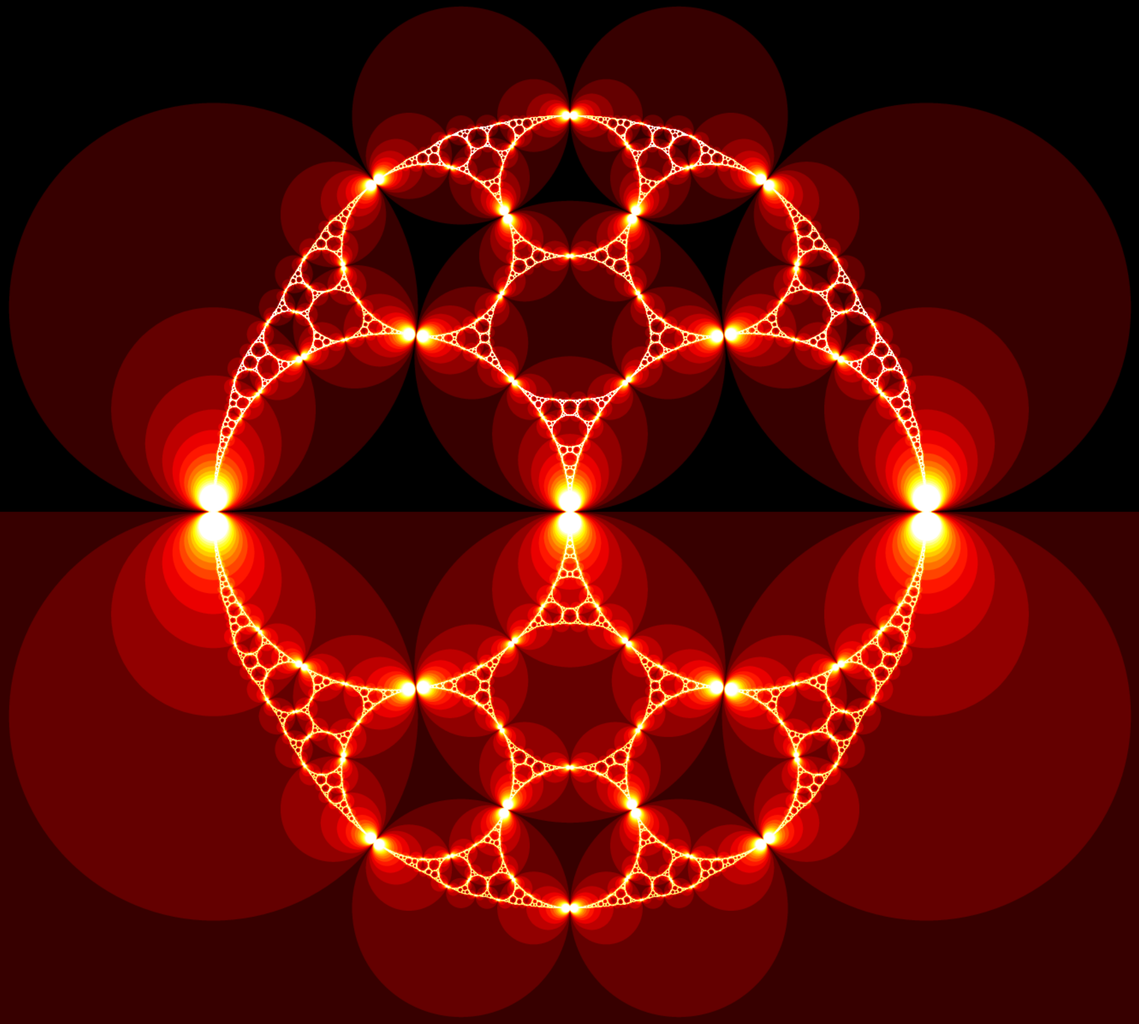
Quantum logics for expressing and proving the correctness of quantum programs

Bergfeld, J.M.

QUANTUM LOGICS FOR EXPRESSING AND PROVING THE CORRECTNESS OF QUANTUM PROGRAMS

J.M. Bergfeld

Jort Martinus Bergfeld



QUANTUM LOGICS FOR EXPRESSING AND PROVING THE CORRECTNESS OF QUANTUM PROGRAMS

Quantum logics for expressing and proving the correctness of quantum programs

Jort Martinus Bergfeld

Quantum logics for expressing and proving the correctness of quantum programs

ILLC Dissertation Series DS-2019-02

INSTITUTE FOR LOGIC, LANGUAGE AND COMPUTATION

For further information about ILLC-publications, please contact

Institute for Logic, Language and Computation
Universiteit van Amsterdam
Science Park 107
1098 XG Amsterdam
phone: +31-20-525 6051
e-mail: illc@uva.nl
homepage: http://www.illc.uva.nl/

The research of this author has been made possible by VIDI grant 639.072.904 of the Netherlands Organization for Scientific Research (NWO).

Cover design by Jort Bergfeld, inspired by Indra's Pearls - Mumford, Series and Wright, Cambridge University Press 2002.
Printed and bound by Ipskamp Drukkers.

ISBN: 978–94–028–1467–5

Quantum logics for expressing and proving the correctness of quantum programs

Academisch Proefschrift

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties ingestelde
commissie, in het openbaar te verdedigen in de Agnietenkapel
op donderdag 16 mei 2019, te 10.00 uur

door

Jort Martinus Bergfeld

geboren te Sint Maarten

Promotor:	Prof. dr. S.J.L. Smets	Universiteit van Amsterdam
Co-promotor:	Dr. J. Sack	California State University Long Beach
Overige leden:	Prof. dr. J.F.A.K. van Benthem	Stanford University
	Prof. dr. R. Giuntini	Università di Cagliari
	Prof. dr. Y. Venema	Universiteit van Amsterdam
	Dr. C. Schaffner	Universiteit van Amsterdam
	Dr. A. Kissinger	Radboud Universiteit

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Voor Berwin Danesh

mijn kleine lieve wonder

Contents

Word of thanks **xi**

1 Introduction **1**
1.1 Relating algebraic and spatial quantum structures 3
1.2 Designing hybrid and probabilistic quantum logics (QHL and PLQP) 5
1.3 Axiomatising quantum logics (QHL and PLQP) 6
1.4 Decidability for a class of Hilbert space based quantum logics . . 7
1.5 Overview of the thesis 8
1.6 Acknowledgement of intellectual contributions 9

2 Preliminaries **11**
2.1 Quantum mechanics 11
2.1.1 The state space 11
2.1.2 Quantum transformations 15
2.1.3 Quantum measurements 16
2.1.4 Multi-partite systems. 17
2.2 Quantum logic 19
2.2.1 Standard quantum logic 20
2.2.2 Píron lattice 22
2.2.3 Modal logic approach 24
2.2.4 Probabilistic logic 35
2.2.5 Duality 37
2.3 Quantum information theory 39
2.3.1 Quantum computation algorithms 39
2.3.2 Quantum communication protocols 44

3 Duality for the logic of quantum actions **47**
3.1 The Categories 48
3.1.1 Categories of Piron Lattices 48

3.1.2 Categories of Quantum Dynamic Frames 51
3.2 Dualities 58
3.2.1 From Piron Lattices to Quantum Dynamic Frames 58
3.2.2 From Quantum Dynamic Frames to Piron Lattices 61
3.2.3 Natural Isomorphisms of the Functors 64
3.2.4 Mayet's Condition 65

4 Completeness of a quantum hybrid logic 67
4.1 Quantum hybrid logic 68
4.1.1 Syntax 68
4.1.2 Frame and model 68
4.1.3 Semantics 71
4.2 Dynamic operators 72
4.3 Complete deductive system 73
4.3.1 Deductive system 73
4.3.2 Completeness 76

5 Probabilistic logic for quantum programs 79
5.1 Probabilistic Quantum Structure 80
5.1.1 Maps between bases and states 81
5.1.2 Agents and Separability 82
5.2 Probablistic quantum logic 83
5.2.1 Syntax 83
5.2.2 Semantics 84
5.2.3 Abbreviations 85
5.3 Deductive system 87
5.3.1 Deducible basic properties 92
5.3.2 Deducible probabilistic properties 98
5.3.3 Deducible properties of a basis. 100
5.4 Examples 107
5.4.1 Example 1: Quantum Leader Election 107
5.4.2 Example 2: BB84 110

6 PLQP & Company: Decidable Logics for Quantum Algorithms 115
6.1 Probabilistic Logic of Quantum Programs 116
6.2 Applying PLQP to the Quantum Search Algorithm 121
6.3 Decidability Proof 123
6.3.1 Proof Recipe, the Core Idea 123
6.3.2 Proof Recipe, Precisely and Generally 126
6.3.3 Application of Our Recipe to PLQP 129
6.3.4 More Applications of Our Recipe 131

7 Conclusions **135**
7.1 Summary 135
7.2 Future work 136

Bibliography **139**

Samenvatting **149**

Abstract **153**

Word of thanks

In the past eight and a half year of my thesis research and writing I have met many many people[1] who have supported me either academically or personally (or both), and with their help I have grown as a person. Although I completely lack the ability to find the right words to express my thanks, in the following pages I still provide a humble attempt to show my gratitude to the following people.

First of all, my promotor and supervisor Sonja Smets. Thank you for giving me the chance to do this research. You have supported personally, especially in the beginning when I had to move to Groningen without any financial reserve. Your knowledge of the field is amazing and you have always been able to point to relevant literature and good conferences. Moreover, each seminar and conference you organised yourself became a joy with lively discussions and always a nice dinner to end.

Secondly, my co-promotor Joshua Sack. Our in-depth mathematical discussions were of great value to me and you were always ready to help me with my articles and the last years with my very slow thesis writing. Without your continuing support during this last years, I would not have finished this thesis.

The doctoral committee Johan van Benthem, Yde Venema, Roberto Giuntini, Christian Schaffner and Aleks Kissinger. Thank you so much for your time and effort to actually read my thesis. I am looking forward to your questions and the following discussion during the defence.

My “official” promotors Rineke Verbrugge and Yde Venema, during the time Sonja was not yet a full professor and could not be my promotor herself. Yde, we have known each other since my bachelor years in mathematics. Your classes on modal logic were what inspired me to pursue mathematical logic as my main field of interest and your encouragements gave me the last push I needed to apply

[1] I gave up on an attempt to list all of you, and therefore most of you are now simply called colleagues. Colleagues should be taken in the broadest sense of the word and includes also the great supporting staff and those who I have met at the conferences, workshops, seminars and summer schools.

for this PhD project. Rineke, with each conversation we had I felt your kindness and warmth. I cannot thank you enough for providing a desk in the University of Groningen when circumstances forced me back from Haarlem to Groningen. This desk has led not only to a finished thesis, but to far much greater joy and happiness in my life.

My research's team members and co-authors Alexandru Baltag, Kohei Kishida, Shengyang Zhong and Nina Gierazimcuk. Kohei, the first time you walked into our office, you immediately started to dance. I have enjoyed and learned a lot from your knowledge of category theory and you have helped me greatly with my academic writing. Shengyang, you're kind, hard-working and disciplined. You have solved a key problem that I had with my completeness proof. You have also done a much better job writing your thesis, and thinking about you has inspired me to continue working on my thesis. Alexandru, you are almost the opposite of me: full of energy, loud and so, so fast, and for that, I have enjoyed your company all the more. You have lighten up every seminar discussion and was the story teller at the dinners. You have done, what I'm sure secretly every researcher wants to do: you replied to a reviewers comments to the editor filled with emotion and indignation. Nina, our research paths separated soon, but I'm glad we had such nice personal conversations during the many seminars and dinners.

My colleagues at the University of Groningen. I came alone to Groningen, knowing nobody, but from the very start never felt alone. There were the daily lunches, 15 o'clock coffee time and the many many dinners together. I remember one morning asking one of you to go to the cinema with me, and by the time it was evening the group had expanded to 10 people without a single effort. The help I got with moving to my new house was amazing. But my most precious memory is the magnificent weekend in a cottage in Drenthe with a few of you.

My colleagues at the University of Amsterdam. Logic and Amsterdam are connected with each other. The diversity of all the research in logic is amazing and I have enjoyed seeing all of your work. I have enjoyed our little basketball team and the days we could play against each other. The many trips to conferences and seminars were fun and relaxing thanks to you. I also dearly remember my bicycle trip to Venezia. Knowing and meeting some locals made it into a very special stay, which otherwise would have been ruined by too much tourism.

My paranimfs. Karolina, I am so grateful I could play Brahm's piano and cello sonata with you, it filled my body with pure lightness. My dear brother Isidoor, thank you for all the conversations about music, movies and life and all the times you have been there for me.

My family, thank you for all the love and care you have given me. Mama, you have raised me into a capable, independant and responsible man. You have taught me to enjoy nature and be thankful for the small things. Papa, thank you for making me interested in technical stuff, from lego to computers. You also have given me and repaired so many bicycles for me, and nothing can make me happier than a good long cycle trip. Marije, thank you for pushing me out of my comfort zone from time to time and your incredible support during the rougher times of high school.

My love, life and wife Mahya. Everything in life became more beautiful when you arrived. I feel more passion and see more colour. I can hardly recognise my life from before, in the past three years we have met, were engaged, married and got our first son. All such enormous amazing moments that have shaped me and will be in my heart forever. Your love drives me to become better each day. We have met because I was still writing this thesis, and this thesis has been finished thanks to your continuing support.

And thank you Berwin, my innocent son. In you I can see the reflection of my happiness, the beauty of my wife and the joy of life.

Gorgan
March, 2019.

Jort Martinus Bergfeld

Chapter 1

Introduction

In the first half of the twentieth century physicists discovered that elementary particles do not obey the classical Newtonian laws, instead obeying different laws. These laws are now known as the laws of quantum mechanics. Quantum mechanics has a tremendous influence on information theory and computer science, leading to new research areas called quantum information theory and quantum computation.

Incorporating quantum mechanics into information theory has led to new communication protocols that achieve goals deemed to be impossible by using classical computational techniques. For example, the quantum leader election protocol [47, 98] is a method for selecting exactly one of n many members, giving each member equal chance of being selected. This is analogous to establishing a fair n-sided die, and such selections are important for distributive systems. If each member in a distributive system is anonymous, no general classical algorithm exists that solves the leader election problem in bounded time and with zero errors. As another example, we can look at the BB84 quantum key distribution protocol [21], a secure distribution key protocol. Although still susceptible to some attacks [106], once the BB84 protocol safely finishes, the distributed key guarantees safety for eternity, unlike classical key distribution schemes.

Many computer programs also benefit from incorporating quantum mechanical techniques. For example, Grover's search algorithm [63] is an algorithm that looks for a key in an unsorted database and is proven to be faster than any classical algorithm. Shor's factoring algorithm [95] is an algorithm that factorises an integer into its prime factors. This algorithm runs in bounded error quantum polynomial time, whereas any known classical algorithm runs in exponential time.

Similar as for classical computing, logic plays a fundamental role in the theory of quantum computing. The role of logic becomes central when we look at the design of quantum programs, especially when we look at their specification and verification. While quantum computation has its own logical system of so-called quantum circuits formulated directly in the language of quantum mechanics, there are other logical systems that operate on a higher level of abstraction. Quantum logic, which was originally used to clarify properties of quantum physics [30], has developed into a broader field, with many logics addressing algebraic structures of quantum systems [39, 44]. A significant recent development is the strengthening of quantum logic to be able to address quantum computation [51]. This coincides with the development to formalize the semantics of quantum programs [48] and the development of model checkers and verification tools for quantum systems [61, 57, 105].

While the above logical systems are of interest, it was by further work of a number of researchers that the connection to modal logic and other systems commonly used in theoretical computer science (dynamic logic and Hoare logic) was made. Robert Goldblatt introduced orthologic and orthomodular logic for orthoframes and orthomodular lattices respectively [62]. Orthomodular lattices [74] are more general algebraic structures than Píron lattices [86], which are more traditional quantum structures, as they are strongly related to Hilbert spaces. Alexandru Baltag and Sonja Smets introduced the logic for quantum actions [10], a propositional dynamic logic (PDL) on quantum dynamic frames. PDL is traditionally used for the verification of classical computer programs and quantum dynamic frames were designed to be dual to Píron lattices. Yet another line of research was initiated by Samson Abramsky and Bob Coecke. They introduced categorical quantum logic [1, 2]. Other work exists; see for example Maria Dalla Chiara and Roberto Giuntini's book on sharp and unsharp quantum logics [44] and the work by Chadha et al. [37, 38] and Mateus et al. [78].

This thesis is positioned at the interface between quantum logic and quantum computation. While building on a long tradition of research in quantum logic (see [44, 76]), this thesis contributes to the field in the following four themes.

- Many logics are designed to reason about specific physical structures. We can choose to use direct abstractions of Hilbert spaces, or we can use algebraic structures with properties which characterise the quantum properties of Hilbert spaces. *Relating these different quantum structures* is important to show where these structures are positioned. Not all quantum structures capture all properties of Hilbert spaces. Although quantum dynamic frames are designed to be equivalent to Píron lattices, in this thesis we provide a formal proof and extend this result to a duality result by considering two different types of morphisms.

- We *design two new logical systems.* Both systems are based on the propositional dynamic quantum logic research of Alexandru Baltag and Sonja Smets. One of which, called *Quantum Hybrid Logic (QHL)*, adds nominals, which provide the power to express atoms and bases, but also opens the door to a complete axiomatisation. The other one, called *Probabistic Logic for Quantum Programs (PLQP)* adds probabilities to extend the logic's expressive power and is able to reason about certain quantum communication protocols.

- In order to design a logic that is fit to reason about quantum structures, one would benefit from a deductive system. We *axiomatise QHL and PLQP*, the two quantum logics described above. One of these two is shown to be complete. The other one is used to prove the correctness of certain quantum information protocols.

- Being able to prove the correctness of a protocol is great, but one could wonder whether or not we can always find such a proof. In the last part of this thesis we show that a class of Hilbert space based quantum logics, which includes the Probabilistic Logic for Quantum Programs, is *decidable*, meaning there is a deterministic procedure to decide whether or not a formula is true.

These themes are discussed in more details in the following sections.

1.1 Relating algebraic and spatial quantum structures

There is a long tradition of investigating dualities between algebraic structures and "spatial" structures, showing that categories of certain algebras and of certain spaces are equivalent to each other, except that they have opposite directions of morphisms. A classic example is the Stone duality between Boolean algebras and fields of sets [97]; see [73] for the Stone duality and vast extensions thereof. For dualities seen in modal logic, such as the one between complete atomic Boolean algebras with operators and Kripke frames, see [32, Chapter 5] and [100, Section 5].[1] In Chapter 3 we build further on this tradition and study the duality of two different quantum structures, *Píron lattices* [86] and *quantum dynamic frames* [10], which are abstractions of Hilbert spaces. Hilbert spaces are among the standard tools for representing quantum systems, and these abstractions highlight essential properties of quantum systems.

Píron lattices provide an algebraic perspective on Hilbert spaces and focus on *testable properties* of the physical system. Testable properties of a physical system can be represented as closed linear subspaces of a Hilbert space, with the one-dimensional subspaces being the states of the system. These states form the atoms of an atomic lattice of closed linear subspaces. A Píron lattice is such a lattice with the appropriate constraints for it to capture the abstract structure of a generalized

[1] While duality plays a crucial role both in Kripke semantics and in locale theory [73], the two fields use the term "frame" to mean quite different structures. In this thesis we always use "frame" in line with the terminology of Kripke semantics.

Hilbert space [86]; a Píron lattice that satisfies “Mayet’s condition” [80] captures the structure of an infinite dimensional Hilbert space over the complex numbers, reals, or quaternions. Such lattices highlight the algebraic properties of a physical system, where joins and meets correspond to the disjunction and conjunction of the properties being tested, and orthocomplementation corresponds to the negation of the property. This sets the foundation for an algebraic semantics of quantum logic. However, on the surface, this logical structure is static and timeless: to express transformations we need to combine several basic operators in a non-intuitive way.

Quantum dynamic frames provide a *dynamic* perspective on quantum systems. The basic ingredients are states which are related to each other via actions that transform the system from one state to another. In this way a quantum dynamic frame is a type of labelled transition system [10]. Relations are constructed from atomic actions that are either projections (corresponding to tests) or unitary evolutions (reversible actions). These quantum dynamic frames are used for reasoning about quantum programs via the “logic of quantum programs” [11], a natural extension of Hoare logic and propositional dynamic logic, which are used for reasoning about classical programs [65].

Given that Píron lattices focus on testable properties and appear to be static and quantum dynamic frames focus on states and actions and are dynamic, it might seem that these two approaches are scarcely related. We show in Chapter 3 that these two approaches are categorically dual to each other, that is, the category of one is equivalent to the dual (opposite) category of the other. A first step was given in [10], where it was observed that a quantum dynamic frame gives rise to a Píron lattice and vice versa. This relationship concerns just the objects of the categories. We provide a detailed and complete proof of this observation. We provide a full categorical structure for both Píron lattices and quantum dynamic frames, and show that these categories are dual to each other. For each of the frames and the lattices, we consider two types of morphisms. One type is the one defined by Moore [81] for two simpler categories: state spaces (symmetric antireflexive frames that separate points) and property lattices (complete atomistic orthocomplemented lattices). These categories are weaker than the ones we consider in this chapter as they do not capture superpositions which are important to quantum theory. However, the definition of the morphisms used by Moore can be used for our categories as well. We also define stronger types of morphisms for both the Píron lattices and quantum dynamic frames. As these morphisms are strictly stronger than Moore’s, we refer to them as *strong* and we refer to the Moore morphisms as *weak*. Both Píron lattice morphisms act directly on properties, while both quantum dynamic frame morphisms act directly on states. These two types of morphisms are dual to each other (have reverse arrows), as is noted in the morphism of state property spaces discussed in [3].

Our duality result in Chapter 3 shows that quantum dynamic frames and Píron lattices form categories that are essentially the same (except for the direction of morphisms). We also show that this relation can be restricted to the objects satisfying Mayet's condition. As Píron lattices satisfying Mayet's condition have already been shown to be equivalent to Hilbert spaces, this result clarifies the close relationship that quantum dynamic frames have with Hilbert spaces. The structures of both quantum dynamic frames and Píron lattices are each a focal point of quantum logic, and hence our duality adds a new perspective to the formal relation between these different quantum structures.

1.2 Designing hybrid and probabilistic quantum logics (QHL and PLQP)

In Chapter 4 we introduce a quantum hybrid logic (QHL), which means that next to the standard operators of intersection, quantum join and orhtocomplementation we add a special set of proposition letters called nominals, which refer to singleton states or atoms. This is the first attempt (as far as the author is aware) to use hybrid logic to reason about quantum structures. The syntax of this logic is in fact equivalent to standard hybrid logic (with down arrow) [5], but the standard deductive system is extended with four new axioms that are used to capture the properties of a quantum Kripke model which have been introduced by Zhong [107]. As quantum Kripke models are equivalent to quantum dynamic frames [107], one could consider this logic to be an extension of the logic for quantum actions, introduced by Alexandru Baltag and Sonja Smets [10]. Indeed, in Chapter 4 we show that all operators of the logic for quantum actions are in fact expressible in this quantum hybrid logic

Quantum information theory gives us a natural reason to introduce nominals. Many quantum protocols require an orthogonal basis (that is, a measurement) to be fixed. We could achieve this by adding constants to the language. However, the specific choice of the basis is not important, only the relation to, for example, the initial state of a protocol. For some quantum cryptographic protocols, it is in fact important that one can choose several bases, and as such, a more flexible way to define a basis is desirable. The nominals allow us to express in an efficient way what a basis is, without the need to fix a basis beforehand.

The main goal of this logic is to express and prove the correctness of quantum protocols. As these are all defined on finite dimensional Hilbert spaces, we limit our attention to finite dimensional quantum Kripke frames in Chapter 4, in order to provide a completeness result.

The new logical system that we introduce for quantum reasoning in Chapter 5 and Chapter 6 is based on combining already existing formalisms of quantum logic, modal logic and probability logic. This gives us a Probabilistic Logic of Quantum Programs (PLQP), that extends a version [12] of the older Logic of Quantum Program (LQP), introduced in [11] and developed in [12, 13, 15, 14]. While the original version in [11] contains *dynamic modalities* $[\pi]$ (for quantum programs π) as well as *spatial modalities* (to talk about subsystems and local information), the later ones were replaced in [12] with "epistemic" modalities K_I (capturing the information that is 'known' to subsystem I, i.e. it is carried by the local state of subsystem I). In addition to the dynamic and epistemic modalities, the logic PLQP presented in Chapter 5 and Chapter 6 is endowed with a *probabilistic modality*, capturing the probability that a given test (of a quantum-testable property) will succeed. This is a novel feature, that greatly enhances the expressivity of the logic, allowing us to use it for the verification of probabilistic quantum algorithms.

Although very similar there exists certain differences between the languages introduced in Chapter 5 and Chapter 6. One of the differences between these languages is the fact that the language in Chapter 5 simplifies the formulas for locality to describe full separability with respect to a given set of components. This simplification of the language allows us to highlight the basic properties in the proof system that are essential to the properties of bases of a finite dimensional Hilbert space.

1.3 Axiomatising quantum logics (QHL and PLQP)

There is a large literature on axiomatising logics for classical computation. These include Hoare Logic [68], Propositional dynamic logic [59], other dynamic logics [65], and temporal logics [69], and they aid in proving correctness of protocols and programs. With the increased prospects of quantum devices and computers, there is a growing interest in (axiomatising) quantum logics.

In Chapter 4, we provide a completeness result for the quantum hybrid logic discussed above with respect to quantum Kripke frames of dimension at most n. As the language is very similar to standard hybrid logic, this result builds on a completeness result for a large class of hybrid logics [32, 31]. We show that part of our quantum hybrid logic falls inside this class for which the completeness result applies, while another part of our logic needs additional work to prove completeness.

Chapter 5 lays a foundation for an axiomatization of the probabilistic logic for quantum programs (PLQP) discussed above. In the non-probabilistic setting, a sound axiomatization that is relevant to our work was developed in [11] for the *Logic of Quantum Programs*, a quantum analogue of the propositional dynamic logic, which was used to prove the correctness of the Quantum teleportation protocol and the Quantum Secret Sharing protocol. But the logic of quantum programs could not express quantities, and could only account for the correctness of qualitative properties of algorithms and protocols considered.

The proof system introduced in Chapter 5 is shown to be sound, and we use it to prove the properties of the Quantum Leader Election protocol of [47] and the BB84 quantum key distribution protocol [21, 22]. These two protocols are just examples of what our system can prove, and we are sure there are many others. But our logic also lays a foundation for the further development in axiomatizing logics for quantum systems, particularly those that involve probability.

There have been other developments in designing axiomatizations of quantum logics, some of which have been shown to be complete. In [62], Goldblatt developed a complete axiomatizion of orthologic and orthomodular quantum logic. There has also been the development of a Gentzen style proofs systems for orthologic [85]. In [92], Selinger uses a graphical language to axiomatize properties for dagger compact closed categories, and shows in [93, 94] that this axiomatic system is also complete with respect to finite-dimensional Hilbert spaces. In [2], Abramsky and Coecke use a diagrammatic axiomatization for categorical quantum logic to prove the correctness of Quantum Teleportation, Logic Gate Teleportation, and Entanglement Swapping protocols. Further work on the graphical calculi includes Coecke and Kissinger's book [40] and the recent work on the zx and zw calculi [64, 72]. An axiomatization of a quantum logic that involves probabilities is given in [79].

The completeness result in Chapter 4 separates itself from previous completeness results for quantum logics, as we show completeness for a dynamic quantum logic that builds on the work of [11], and can be viewed as a quantum analogue of propositional dynamic logic. Similarly, the logic in Chapter 5, that builds on the same work of [11], can be viewed as a probabilistic quantum analogue of propositional dynamic logic.

1.4 Decidability for a class of Hilbert space based quantum logics

Investigations into the decidability of logical systems play an important role in computer science and automated reasoning. To prove that a logical system is decidable essentially means that there exists an effective procedure to answer the question whether a formula is valid (or satisfiable) or not. While we see a long history of work on the decidability of various logical systems within the area of Logic and Computer Science, not many results are known about the decidability of quantum logics. One of the reasons for this is that the investigations into the decidability of logical systems are typically triggered by the design of automated reasoning systems. In the context of quantum reasoning and quantum logic, one would expect that similar decidability questions would be triggered and motivated by the research in the area of quantum computing. However, traditional quantum logics were not designed to be directly applicable to quantum algorithms. One can observe that the original quantum logics were built in order to capture the properties of *single* quantum systems living in an *infinite-dimensional* Hilbert space. In contrast, the logics that are of interest for quantum computing focus mainly on *compound* systems living in *finite-dimensional* spaces.

Motivated by the work in quantum computing, we give a general method for showing the decidability for a whole variety of quantum logics, including in particular the logic considered in Chapter 6. The idea behind our method comes from the work of Dunn et. al. in [50], who translated standard quantum logic over finite-dimensional spaces into (the equational fragment of) the first-order theory of real numbers (which is known to be decidable due to A. Tarski's famous theorem [99]). We extend this method to cover a wider range of quantum logics, such as the one considered in Chapter 6.

1.5 Overview of the thesis

This thesis is organised as follows. In Chapter 2, we give an overview of the development of quantum logic and quantum information theory. As it is impossible to give an overview of all past developments, we will only focus on those lines of research relevant for this thesis. In Section 2.1, we discuss a standard Hilbert space model of quantum mechanics. In Section 2.2, we give an overview of some classical, that is non-quantum, logics and some quantum logics relevant for this thesis, as well as some key concepts of logic in general that one needs to understand for this thesis. In Section 2.3, we provide examples of quantum programs and quantum communication protocols. For all of these examples, we will express their correctness in a quantum logic in later chapters, and for some of these we will also prove their correctness.

In Chapter 3, we show a duality between two approaches to represent quantum structures abstractly and to model the logic and dynamics therein. One approach puts forward a "quantum dynamic frame" [10], a labelled transition system whose transition relations are intended to represent projections and unitaries on a (generalized) Hilbert space. The other approach considers a "Píron lattice" [86], which characterizes the algebra of closed linear subspaces of a (generalized) Hilbert space. We define categories of these two sorts of structures and show a duality between them. This result establishes, on one direction of the duality, that quantum dynamic frames represent quantum structures correctly; on the other direction, it gives rise to a representation of dynamics on a Píron lattice.

In Chapter 4, we introduce a quantum hybrid logic, which is shown to be sound and complete with respect to finite dimensional quantum models, i.e. quantum Kripke models of dimension at most n for a fixed $n \in \mathbb{N}$. While the syntax of our logical system is equivalent to standard hybrid logic, the deductive system is extended with quantum axioms that capture the properties of a quantum Kripke model.

In Chapter 5, we present a sound axiomatization for a probabilistic modal dynamic logic of quantum programs. The logic can express whether a state is separable or entangled, information that is local to a subsystem of the whole quantum system, and the probability of positive answers to quantum tests of certain properties. The power of this axiomatization is demonstrated with proofs of properties concerning bases of a finite dimensional Hilbert space, composite systems, entangled and separable states, and with proofs of the correctness of two probabilistic quantum protocols (the quantum leader election protocol and the BB84 quantum key distribution protocol).

In Chapter 6, we introduce a probabilistic modal (dynamic and epistemic) quantum logic PLQP for reasoning about quantum algorithms. We illustrate its expressivity by using the logic to encode the correctness of the well-known quantum search algorithm, as well as of a quantum protocol known to solve one of the paradigmatic tasks from classical distributed computing: the leader election problem. We also provide a general method (extending an idea employed in the decidability proof in [50]) for proving the decidability of a range of quantum logics, interpreted on finite-dimensional Hilbert spaces. We give general conditions for the applicability of this method, and in particular we apply it to prove the decidability of PLQP.

1.6 Acknowledgement of intellectual contributions

The Chapters 3–6 are all based on articles, three of which have been published.

- Chapter 3 is based on the article published in [25]: Jort Bergfeld, Kohei Kishida, Joshua Sack and Shengyan Zhong. Duality for the Logic of Quantum Actions. *Studia Logica*, 103(4):781–805, 2015.

- Chapter 4 is based on an unpublished preprint written by the author of this thesis.

- Chapter 5 is based on the article published in [26]: Jort Bergfeld and Joshua Sack. Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs. *Soft Computing*, 21(6):1421–1441, 2017.

- Chapter 6 is based on the article published in [8]: Alexandru Baltag, Jort Bergfeld, Joshua Sack, Sonja Smets and Shengyang Zhong. PLQP & company: Decidable logics for quantum algorithms. *International Journal of Theoretical Physics*, 53(10):3628–3647, 2014.

Chapter 2

Preliminaries

In this chapter we discuss the preliminaries necessary to understand the main contributions in this thesis. We discuss one of the standard models of quantum mechanics: the Hilbert space model. Next we review some traditional logics by Birkhoff/von Neumann and Goldblatt, as well as a quantum logic based on propositional dynamic logic. We then discuss some protocols in quantum computation as well as several quantum communication protocols.

2.1 Quantum mechanics

The field of quantum mechanics is too big to be fully reviewed in this thesis, so instead of giving an overview of all the details I will only cover the main points necessary to understand this thesis. For a broader overview of the field see for example [6]. The reader is expected to have some knowledge of complex vector spaces. See for example [104].

The origin of quantum mechanics, which indicates the point of divergence from classical physics, has been triggered by the experimental discovery of certain phenomena (e.g. black body radiation) which could not be accounted for in the available classical paradigm. Several theories have been proposed to explain these experimental results, all of which are essentially the same quantum theory. These theories are based on a set of postulates, from which the entire quantum theory follows. The postulates in this section are taken from [84].

2.1.1 The state space

The mathematical arena in which quantum mechanics is played is called a Hilbert space. Let us recall the relevant definitions for a Hilbert space. (Taken from [42].) First we give the definition for an inner product space.

Definition 2.1.1 (Inner product space)**.** A structure $\mathcal{V} = (V, +, \cdot, \langle \cdot \mid \cdot \rangle)$ is a *complex inner product space* if

1. $(V, +, \cdot)$ is a vector space over the field of complex numbers, and

2. $\langle \cdot \mid \cdot \rangle$ is an *inner product*, that is, a function $\langle \cdot \mid \cdot \rangle : V \times V \to \mathbb{C}$ such that for all $x, y, z \in V$ and $\lambda \in \mathbb{C}$ we have

   (a) *conjugate symmetry:* $\langle x \mid y \rangle = \overline{\langle y \mid x \rangle}$,

   (b) *linearity in the second argument*[1]*:* $\begin{array}{r} \langle x \mid y + z \rangle = \langle x \mid y \rangle + \langle x \mid z \rangle \,, \\ \langle x \mid \lambda y \rangle = \lambda \langle x \mid y \rangle \,, \text{ and} \end{array}$

   (c) *positive definiteness:* $\begin{array}{l} \langle x \mid x \rangle \geq 0, \\ \langle x \mid x \rangle = 0 \text{ iff } x = 0. \end{array}$

We usually denote an inner product space with the vector space V, as we assume that there will be no confusion about which inner product structure is used. Each inner product induces a norm, sometimes called the *inner product norm*, given by

$$\|x\| = \sqrt{\langle x \mid x \rangle}.$$

We can now give the definition of a complete inner product space.

Definition 2.1.2 (Complete inner product space)**.**

- A sequence $\langle\!\langle x_k \rangle\!\rangle_k$ in V is *Cauchy* iff for every $\epsilon > 0$ there exists an $N_\epsilon \in \mathbb{N}$ such that for all $n, m > N_\epsilon$ we have $\|x_n - x_m\| < \epsilon$.

- A sequence $\langle\!\langle x_k \rangle\!\rangle_k$ in V *converges* to a vector $x \in V$ iff $\lim_{k \to \infty} \|x_n - x\| = 0$.

- An inner product space V is *complete* iff every Cauchy sequence converges to some vector in V.

This leads us to the definition of a Hilbert space.

Definition 2.1.3 (Hilbert space)**.** A *Hilbert space* is a complete inner product space.

Now we can state the first postulate of quantum mechanics. Note that a *unit vector* is a vector x with norm one, i.e. $\|x\| = 1$.

Postulate 1 ([84])**.** Associated to any isolated physical system is a complex vector space with an inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

[1] Some prefer to have linearity in the first argument, which would lead to conjugate linearity in the second argument.

Given a state vector $|\phi\rangle$ we obtain the *density operator* corresponding to $|\phi\rangle$ by taking the matrix $|\phi\rangle\langle\phi|$. These are called *pure state*. Sometimes we do not know in which pure state the system is, but we do know that with probability p_i the system is in pure state $|\phi_i\rangle$. Then we can describe the *mixed state* by taking the density operator $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$.

Let us discuss some important concepts in a Hilbert space.

Definition 2.1.4 (Orthogonality)**.** Let $\mathcal{H}$ be a complex Hilbert space. Two vectors $x, y \in \mathcal{H}$ are *orthogonal*, denoted by $x \perp y$, iff $\langle x \mid y\rangle = 0$. Given a subset $X \subseteq \mathcal{H}$ the *orthocomplement* of X, denoted by $\sim\!X$, is given by

$$\sim\!X \stackrel{\text{def}}{=} \{y \in \mathcal{H} \mid y \perp x \text{ for all } x \in X\}.$$

Two subsets $X, Y \subseteq \mathcal{H}$ are *orthogonal*, denoted by $X \perp Y$, iff $x \perp y$ for all $x \in X$ and $y \in Y$. A subset $X \subseteq \mathcal{H}$ is a *closed linear subspace* iff $X = \sim\sim\!X$.

As we will discuss below, in quantum mechanics the outcome of any experiment that we can perform will correspond to some closed linear subspace of a Hilbert space. Therefore when combining two (closed linear) subsets $K, L \subseteq \mathcal{H}$, we are normally not interested in the union of the two sets, but in the smallest closed linear subset containing both sets, which we call the quantum join.

Definition 2.1.5. Let $\mathcal{H}$ be a complex Hilbert space and let $K, L \subseteq \mathcal{H}$ be two subsets. The *quantum join* of K and L, denoted by $K \sqcup L$, is given by

$$K \sqcup L \stackrel{\text{def}}{=} \sim\sim\!(K \cup L).$$

Whenever relevant, we often identify a state vector $|\phi\rangle$ with the singleton set $\{|\phi\rangle\}$. For example, we write $|\phi\rangle \sqcup |\psi\rangle$ instead of $\{|\phi\rangle\} \sqcup \{|\psi\rangle\}$. Now we give the definition of an orthonormal basis.

Definition 2.1.6 (Basis)**.** Let $\mathcal{H}$ be a Hilbert space and let I be an index set. A set $\{|\phi_i\rangle\}_{i\in I}$ of vector states $|\phi_i\rangle \in \mathcal{H}$ is called a *basis* iff

1. $\bigsqcup_I |\phi_i\rangle = \mathcal{H}$, and
2. $\bigsqcup_J |\phi_j\rangle \neq \mathcal{H}$ for any proper subset $J \subsetneq I$.

A basis $\{|\phi_i\rangle\}_{i\in I}$ is called *normal* iff $\||\phi\rangle\| = 1$ for all $i \in I$. A basis is called *orthogonal* iff $|\phi_i\rangle \perp |\phi_j\rangle$ for all $i \neq j \in I$. A basis is called *orthonormal* iff it is both orthogonal and normal.

The Hilbert space $\mathcal{H}$ has *dimension* n iff the index set I of a basis has size n, i.e. $|I| = n$.

Given a finite dimension n, a complex Hilbert space is isomorphic to $\mathbb{C}^n$, the complex n-dimensional vector space. In quantum information theory we almost always work in a finite dimensional complex Hilbert space. If $\{|\psi_i\rangle\}_i$ is an orthonormal basis, then we can rewrite $|\phi\rangle$ as

$$|\phi\rangle = \sum_i \langle\psi_i \mid \phi\rangle\, |\psi_i\rangle\,.$$

The basic elements of quantum information theory are called *qubits*, which is short for quantum bits. These are described by a unit vector in a 2-dimensional complex Hilbert space, thus $\mathbb{C}^2$. The standard basis is given by

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

Here $|0\rangle$ and $|1\rangle$ correspond to the classical states of a bit 0 and 1. Any other unit vector of the form $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, with $\alpha, \beta \neq 0$ is said to be in a superposition of $|0\rangle$ and $|1\rangle$.[2] Another very common basis is called the Hadamard basis, given by $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Before we continue to discuss quantum transformations, let us discuss a structure that is very similar to a Hilbert space, but that is more general. Some quantum structures we discuss in this thesis do not capture all properties of quantum mechanics, instead they capture all properties of a generalised Hilbert space as presented in the following definition.

Definition 2.1.7 (Generalised Hilbert space)**.** A *generalised Hilbert space* is a module V over a division ring K, with an involution $(\_)^* : K \to K$ such that for $k, l \in K$ we have

$$\begin{aligned}(k^*)^* &= k\\ (k \cdot l)^* &= l^* \cdot k^*\end{aligned}$$

and a Hermitian product $\langle \_, \_\rangle : V \times V \to K$ such that for $x, y, z \in V$ and $k \in K$ we have

$$\begin{aligned}\langle x + ky, z\rangle &= \langle x, z\rangle + k\langle x, y\rangle\\ \langle x, y\rangle^* &= \langle y, x\rangle\\ \langle x, x\rangle = 0 &\Leftrightarrow x = 0\end{aligned}$$

and such that for any $M \subseteq V$ we have

$$\sim\! M + \sim\sim\! M = V.$$

[2] In Subsection 2.1.3 we will explain that α and β correspond to the probability of measuring $|0\rangle$ and $|1\rangle$ respectively.

2.1.2 Quantum transformations

Transformations within a closed quantum system are described by unitary transformations. Let us recall the relevant definitions of linear algebra.

Definition 2.1.8 (Adjoint operator)**.** Let $\mathcal{H}$ be a complex Hilbert space and let $A : \mathcal{H} \to \mathcal{H}$ be a continuous linear operator on $\mathcal{H}$. The *adjoint operator* of A denoted by $A^\dagger$ is the unique continuous linear operator $A^\dagger : \mathcal{H} \to \mathcal{H}$ such that for all $x, y \in \mathcal{H}$ we have

$$\langle Ax \mid y \rangle = \langle x \mid A^\dagger y \rangle \,.$$

Existence and uniqueness of the adjoint operator follows from the Riesz representation theorem [89, 90].

Definition 2.1.9. Let $\mathcal{H}$ be a complex Hilbert space. A continuous linear operator $U : \mathcal{H} \to \mathcal{H}$ is called a *unitary transformation* iff $UU^\dagger = I$, where I denotes the identity operator.

With these definitions we can state the second postulate concerning transformations.

Postulate 2 ([84])**.** The evolution of a *closed* quantum system is described by a *unitary transformation.* That is, the state $|\psi_1\rangle$ of the system at time t_1 relates to the state $|\psi_2\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi_2\rangle = U\,|\psi_1\rangle \,.$$

The above postulate assumes a discrete time. We can reformulate this postulate for continuous time using the Schrödinger equation:

$$i\hbar \frac{d\,|\phi\rangle}{dt} = H\,|\phi\rangle \,,$$

where $\hbar$ is *Planck's constant*, a physical constant, and H is the Hamiltonian, a fixed Hermitian operator. Although some applications in quantum information theory consider the time needed for an operation to be performed, especially in quantum cryptology, most applications simple assume each transformation is finished in a fixed amount of time.

From $UU^\dagger = I$ we can show that a unitary transformation respects the inner product:

$$\langle U\psi \mid U\phi \rangle = \langle U^\dagger U\psi \mid \phi \rangle = \langle \psi \mid \phi \rangle \,.$$

As a consequence, we cannot copy qubits, or any other type of quantum information, which we will show in Theorem 2.1.12. Also note that all unitary transformations are invertible.

We define a special unitary transformation called the Hadamard transformation, which we denote with H.[3] The Hadamard transformation sends the standard basis to the Hadamard basis, more precise, H is defined by $H\left|0\right\rangle = \left|+\right\rangle$ and $H\left|1\right\rangle = \left|-\right\rangle$, that is

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

Note that the Hadamard matrix is its own inverse and adjoint.

2.1.3 Quantum measurements

In this subsection we go over the presentation that is most often used in quantum theory of how measurements are performed on quantum systems.

Definition 2.1.10 (Projections)**.** Let $\mathcal{H}$ be a complex Hilbert space. An operator $P : \mathcal{H} \to \mathcal{H}$ is called a *projection* iff $P = PP^\dagger$, or equivalently, iff P is self-adjoint ($P = P^\dagger$) and idempotent ($P = P^2$).

For each projection P we find that the image $\Im(P)$ is a closed linear subspace. Conversely, if $X \subseteq \mathcal{H}$ is a closed linear subspace, then we can define a projection whose image is X by $P_X\left|\phi\right\rangle = \left|\psi\right\rangle$ where $\left|\psi\right\rangle \in X$ and $\|\langle \phi \mid \psi\rangle\| \geq \|\langle \phi \mid \chi\rangle\|$ for all $\left|\chi\right\rangle \in X$. Two projections P and Q are orthogonal if their corresponding closed linear subspaces are orthogonal.

Postulate 3 ([84])**.** Quantum measurements are described by a collection $\{P_n\}$ of *orthogonal projections* such that

$$\bigsqcup_n \Im(P_n) = \mathcal{H}. \tag{2.1}$$

The index n refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $\left|\phi\right\rangle$ immediately before the measurement then the probability that result n occurs is given by

$$p(n) = \left\|P_n\left|\phi\right\rangle\right\|^2,$$

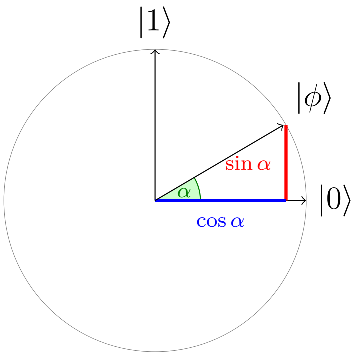
and the state of the system after the measurement is

$$\frac{P_n\left|\phi\right\rangle}{\left\|P_n\left|\phi\right\rangle\right\|}.$$

As a consequence of (2.1) and the orthogonality of the P_n, the probabilities will sum to one:

$$\sum_n p(n) = \sum_n \left\|P_n\left|\phi\right\rangle\right\|^2 = 1.$$

[3] We no longer need to refer to the Hamiltonian, and therefore from now on H will refer to the Hadamard transformation.



If we measure a qubit $|\phi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$ using the standard basis $\{|0\rangle, |1\rangle\}$, then the probability of changing into $|0\rangle$ is $|\cos\alpha|^2$ and the probability of changing into $|1\rangle$ is $|\sin\alpha|^2$.

Figure 2.1: A qubit is measured at an angle

Postulate 3 can be stated more generally, allowing different types of measurement operators than just orthogonal projection, see for example [84]. However, we only consider measurements using orthogonal projections in this thesis, as these are strong enough to describe all quantum protocols under consideration.

In section 2.1.2 we stated that all quantum transformations are unitary transformations, yet it is important to note that a projection is not a unitary transformation. However, in this thesis we consider the measurement device to be outside the quantum system to be measured. So we do not consider a measurement as a quantum transformation, but as a way to extract classical information from a quantum system, e.g. the index n of P_n, and the state changes as a price that we have to pay for this information. We could consider a larger closed quantum system enclosing both the measurement device and the system to be measured; then a measurement would be described by a unitary transformation.[4]

Figure 2.1. illustrates an example of a quantum measurement, i.e. the measurement of a qubit in the standard basis.

2.1.4 Multi-partite systems.

In this subsection we describe how an individual quantum system can be composed of different parts or subsystems.

Definition 2.1.11 (Tensor product)**.** Let V and W be two inner product spaces. The *tensor product*, denoted by $V \otimes W$, is constructed by taking the equivalence classes over the set of formal sums over the cartesian product

$$F(V \times W) \overset{\text{def}}{=} \{\sum_{i=0}^{n} \lambda_i (v_i \otimes w_i) \mid \lambda_i \in \mathbb{C}, v_i \in V, w_i \in W \text{ and } n \in \mathbb{N}\}.$$

under the equivalence relation defined by

[4] This problem is commonly referred to as the measurement problem. Several different solutions to the measurement problem have been proposed, see for example [35, 91, 4].

1. $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$,
2. $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$, and
3. $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$.

The inner product of the tensor product $V \otimes W$ is defined by

$$\langle v_1 \otimes w_1 \mid v_2 \otimes w_2 \rangle_{V \otimes W} = \langle v_1 \mid v_2 \rangle_V \langle w_1 \mid w_2 \rangle_W ,$$

and then expanded linearly to all elements of $V \otimes W$.

Given a unitary transformation $U_1 : V \to V$ and $U_2 : W \to W$ the tensor product of two unitary transformation is given by putting $U_1 \otimes U_2(v \otimes w) = U_1(v) \otimes U_2(w)$ for all $v \in V$ and $w \in W$ and then expanded linearly to all elements of $V \otimes W$.

Postulate 4 ([84])**.** The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system i is prepared to be in the state $|\phi_i\rangle$, then the joint state of the total system is $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$.

Note that we omit $\otimes$ whenever possible, thus $|\phi\rangle \otimes |\psi\rangle$ is written as $|\phi\rangle |\psi\rangle$ or sometimes we even write $|\phi\psi\rangle$.

As mentioned before, the requirement for unitary transformations to respect the inner product implies that a unitary transformation cannot copy elements of a Hilbert space. The following illustrates what this means.

Theorem 2.1.12 (No-cloning theorem [49, 103])**.** *Let $\mathcal{H}$ be a complex Hilbert space. Then there exists no unitary transformation U on $\mathcal{H} \otimes \mathcal{H}$ such that $U(|\phi e\rangle) = |\phi\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}$, where $|e\rangle \in \mathcal{H}$ is some fixed unit vector.*

Proof. Suppose towards a contradiction that we have a unitary transformation U^* and some fixed unit vector $|e\rangle \in \mathcal{H}$ such that $U^* |\phi e\rangle = |\phi\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}$. Take any two unit vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ such that $\langle \phi \mid \psi \rangle \neq 0, 1$. Then we have $U^* |\phi e\rangle = |\phi\phi\rangle$ and $U^* |\psi e\rangle = |\psi\psi\rangle$. If we take the inner product we find

$$\begin{aligned} \langle \phi e \mid \psi e \rangle_{\mathcal{H} \otimes \mathcal{H}} &= \langle \phi \mid \psi \rangle_{\mathcal{H}} \langle e \mid e \rangle_{\mathcal{H}} = \langle \phi \mid \psi \rangle_{\mathcal{H}} , \text{ and} \\ \langle \phi\phi \mid \psi\psi \rangle_{\mathcal{H} \otimes \mathcal{H}} &= \langle \phi \mid \psi \rangle_{\mathcal{H}} \langle \phi \mid \psi \rangle_{\mathcal{H}} = \langle \phi \mid \psi \rangle_{\mathcal{H}}^2 . \end{aligned}$$

As U^* preserves the inner product we find $\langle \phi \mid \psi \rangle = \langle \phi \mid \psi \rangle^2$, which contradicts our assumption that $\langle \phi \mid \psi \rangle \neq 0, 1$. □

Let us give one example of a unitary transformations that acts on more than one qubit. The controlled not gate is given by

$$\text{CNOT}(|x\rangle |y\rangle) \stackrel{\text{def}}{=} |x\rangle |y \oplus x\rangle ,$$

where $\oplus$ is the XOR operator. As a classical gate, that is $\mathrm{CNOT}(x, y) = (x, y \oplus x)$, this gate can be used to copy x by taking $y = 0$. Even as a quantum gate, if we take $|y\rangle = |0\rangle$, this gate will copy $|x\rangle$ if it is either $|0\rangle$ or $|1\rangle$. But now consider the superposition $|x\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then we find

$$\begin{aligned} &\mathrm{CNOT}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle) = \mathrm{CNOT}(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) \\ =&\frac{1}{\sqrt{2}}(\mathrm{CNOT}(|00\rangle) + \mathrm{CNOT}(|10\rangle))) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

This is clearly not a copy of $|x\rangle$, because the two qubits are entangled. Moreover, we can use the equalities $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$ to obtain

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|--\rangle + |++\rangle).$$

Measuring $|x\rangle = |+\rangle$ in the basis $\{|-\rangle, |+\rangle\}$ will always have $|+\rangle$ as outcome, whereas measuring the first qubit of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the same basis has a 50% chance of collapsing the first qubit to $|-\rangle$.

2.2 Quantum logic

Now that we reviewed the basics of quantum mechanics, we will turn our attention to quantum logic, the mathematical tool we want to use to analyse quantum protocols. Although Hilbert spaces have proven to be very successful as a model for quantum mechanics, from a logical point of view a higher-level of abstraction that allows us to reason about physical properties and propositions is required. In classical physics, a property P is a subset of the state space S. A testable proposition is a property for which there exists an experiment that decides with certainty whether the current state of the system is in P or in the complement $S \setminus P$. In classical physics, if P is a testable property, so is the complement $S \setminus P$. In quantum mechanics, we represent a testable property P not by a subset of the state space S, but by a closed linear subspace in a Hilbert space $\mathcal{H}$. Doing this indicates that we deviate from the classical scenario, because we can no longer say that an experiment can decide with certainty on whether the current state of the system is such that P or its classical (set-theoretic) complement is true. The classical complement of a testable property is not guaranteed to be a testable property (i.e. a closed linear subspace of $\mathcal{H}$). In contrast the orthocomplement $P^\perp$ is a testable property. One should note that singleton states, represented by a vector $|\phi\rangle$ are not testable properties, because a measurement cannot distinguish between $|\phi\rangle$ and $\lambda|\phi\rangle$ for a non-zero $\lambda \in \mathbb{C}$. It does not make sense to distinguish between for example the states $|0\rangle$ and $-|0\rangle$ if these states behave completely similar. This is where quantum logic comes in.

2.2.1 Standard quantum logic

In 1932 John von Neumann wrote an influential piece of work on the mathematical and logical foundations of quantum mechanics [101]. The notes on quantum logic presented in this book were expanded to a full quantum logic in 1936 by Garrett Birkhoff and John von Neumann [30].

Given a Hilbert space $\mathcal{H}$, Birkhoff and von Neumann take the one-dimensional subspaces of a Hilbert space as the set of states. The testable properties are the closed linear subspaces. Based on the set of testable properties we can build a lattice structure. These testable properties form a lattice, where the join is the quantum join and the meet is the intersection. If based on classical mechanics the lattice would have been Boolean, but due to the nature of quantum mechanics, this lattice does not satisfy the distributive law:

$$P \wedge (Q \sqcup R) = (P \wedge Q) \sqcup (P \wedge R). \tag{2.2}$$

Before we give a counterexample for (2.2) let us introduce some notation: for a vector $v \in \mathcal{H}$ let us denote the one-dimensional subspace generated by v with $\overline{v}$. For a set of vectors $X \subseteq \mathcal{H}$, the smallest closed linear subspace containing X (or generated by X) is denoted with $\overline{X}$.

As a counter example for (2.2), take $P = \overline{|+\rangle}$, $Q = \overline{|0\rangle}$ and $R = \overline{|1\rangle}$. We have seen that $|+\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$, and $\overline{|0\rangle} \sqcup \overline{|1\rangle}$ is basically the set of all superpositions of $|0\rangle$ and $|1\rangle$. So the left-hand side of (2.2) equals $\overline{|+\rangle}$. But on the right-hand side of (2.2), both $\overline{|+\rangle} \wedge \overline{|0\rangle}$ and $\overline{|+\rangle} \wedge \overline{|1\rangle}$ are equal to the empty set, and therefore the quantum join also equals the empty set.

Instead of the distributive law, Birkhoff and von Neumann showed that a finite dimensional lattice satisfied a weaker law, called the modular law:

$$P \leq R \implies P \sqcup (Q \wedge R) = (P \sqcup Q) \wedge R.$$

On infinite Hilbert spaces this law fails, but Husimi noted that the orthomodular law is respected in every Hilbert space [71]:

$$P \leq Q \implies P \sqcup ({\sim}P \wedge Q) = Q.$$

Let us discuss a slightly different flavour of this standard quantum logic, which is closer related to the logics discussed in this thesis. In this flavour, the logic expresses properties of a quantum system, by using *sentences* (or propositions) ϕ which refer to a closed linear subspace of the given Hilbert space. Sentences are constructed recursively from *atomic sentences* using *sentential connectives.* Atomic sentences are the simplest sentences with no internal structure subject to the analysis of the logic. To what subspace such a sentence p refers can vary. We use a specific sentence $\bot$ to denote any contradiction, i.e., the 0-dimensional subspace $\{\vec{0}\}$. Sentential connectives are operators on sentences that take simpler sentences as arguments and return new, more complex sentences. The grammar of the language of standard quantum logic can be given in the following BNF-format:

$$\phi ::= p \mid \bot \mid {\sim}\phi \mid \phi \wedge \phi \mid \phi \sqcup \phi \tag{2.3}$$

This language is built up from a given set $V_{\mathcal{T}}$ of *propositional variables* and a set $C_{\mathcal{T}}$ of *propositional constants.* In particular $V_{\mathcal{T}}$ contains the atomic sentences p and we work for now with only one propositional constant $\bot$, hence $C_{\mathcal{T}} = \{\bot\}$. The basic set of atomic sentences and constants will be denoted as $A_{\mathcal{T}} = V_{\mathcal{T}} \cup C_{\mathcal{T}}$. We then use our grammar to build more complex sentences from $A_{\mathcal{T}}$ via application of the given quantum connectives. The quantum negation ${\sim}\phi$ will below be interpreted as the orthocomplement of the subspace of ϕ; the conjunction $\phi \wedge \psi$ is used to refer to the intersection of the subspaces ϕ and ψ; and the quantum disjunction $\phi \sqcup \psi$ is used for the closure of the span of the union of ϕ and ψ.

To set the details of our semantics, we first fix a Hilbert space $\mathcal{H}$ and write Σ for the set of (pure) states, i.e. the rays or one-dimensional subspaces of $\mathcal{H}$. In this semantics we associate each sentence ϕ with a subset $[\![\phi]\!] \subseteq \Sigma$, which gives it an interpretation. As such $s \in [\![\phi]\!]$ means that ϕ is *the case at* state $s \in \Sigma$, or that s *satisfies* ϕ.

In standard quantum logic, $[\![\phi]\!]$ is typically taken to be a "closed linear subspace" of $\mathcal{H}$. Here we use scare quotes because, strictly speaking, $[\![\phi]\!] \subseteq \Sigma$ is a different type of object than closed linear subspace $T \subseteq \mathcal{H}$; yet we henceforth refrain from stressing the type difference when the correspondence is obvious. To denote this correspondence, given any non-zero vector $v \in \mathcal{H}$, we write $\tilde{v}$ for the ray that v belongs to. Moreover, given any subset $A \subseteq \mathcal{H}$ that is closed under scalar multiplication, we write $\widetilde{A}$ for the corresponding subset of Σ, i.e., $\widetilde{A} = \{\, \tilde{v} \in \Sigma \mid v \in A \,\}$; on the other hand, given any subset $S \subseteq \Sigma$, we write $\overline{S}$ for the corresponding subset of $\mathcal{H}$, that is, $\overline{S} = \{\, v \in \mathcal{H} \mid \tilde{v} \in S \,\} \cup \{\vec{0}\}$, which is closed under scalar multiplication.[5]

In our semantics, we define interpretations $[\![\phi]\!] \subseteq \Sigma$ for all the sentences ϕ recursively, i.e. along the recursive syntactic construction of ϕ. First we semantically interpret each atomic sentence $p \in A_{\mathcal{T}}$ by a closed linear subspace $[\![p]\!] \subseteq \Sigma$ of $\mathcal{H}$ (or, strictly speaking, a subset of Σ such that $\overline{[\![p]\!]}$ is a closed linear subspace of $\mathcal{H}$) of any dimension.[6]

Definition 2.2.1. An *assignment* is a function $[\![\cdot]\!] : A_{\mathcal{T}} \to \mathcal{P}(\Sigma)$, where $\mathcal{P}(\Sigma)$ is the powerset of Σ, such that $\overline{[\![p]\!]}$ is a closed linear subspace of $\mathcal{H}$ for every $p \in A_{\mathcal{T}}$.

Since we intend $\bot$ to refer to contradiction, we further require that assignments satisfy

[5] Note that $\overline{\varnothing} = \{\vec{0}\}$, so that $\varnothing$ as a subset of Σ corresponds to the 0-dimensional subspace $\{\vec{0}\} \subseteq \mathcal{H}$ rather than $\varnothing$ as a subset of $\mathcal{H}$.

[6] We often use p in such a way that p is the case at exactly one state, in which case $[\![p]\!]$ is a singleton consisting of that state. Yet, in general, $[\![p]\!]$ is any (set of states that corresponds to a) closed linear subspace, so that p may be the case at several (or no) states.

1. $[\![\bot]\!] = \varnothing = \widetilde{\{\vec{0}\}} \subseteq \Sigma$ (corresponding to the 0-dimensional subspace $\{\vec{0}\} \subseteq \mathcal{H}$).

Now, given an assignment of $[\![p]\!]$ to all $p \in A_{\mathcal{T}}$, we extend it to all the sentences ϕ recursively, with the inductive clause for the quantum connectives as follows:

2. $[\![\sim\phi]\!] = \sim[\![\phi]\!]$, the orthocomplement of $[\![\phi]\!]$ (or its corresponding subset of Σ);

3. $[\![\phi \wedge \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$;

4. $[\![\phi \sqcup \psi]\!] = [\![\phi]\!] \sqcup [\![\psi]\!] = \sim(\sim[\![\phi]\!] \cap \sim[\![\psi]\!])$, the closure of the span of $[\![\phi]\!] \cup [\![\psi]\!]$.

This gives an interpretation $[\![\phi]\!]$ for all the sentences ϕ in the quantum logic with $\sim$, $\wedge$, $\sqcup$.

Decidability of standard quantum logic

To prove that a logical system is decidable essentially means that there exists an effective procedure to answer the question whether a formula is valid (or satisfiable) or not. Given a quantum logic (including its syntax and Hilbert space semantics) to reason about a specific quantum system, we can ask if a given formula in the logic is valid, i.e. true no matter which state the system may be in. For instance, $P \sqcup \sim P$ refers to the whole space and hence is valid, irrespectively of which subspace P may refer to. Thus, the family of valid formulas captures the inherent features that $\sim$, $\wedge$, and $\sqcup$ show in the given logic.

One can also regard formulas as terms for subspaces and consider valid equations among them; e.g., we have $P \sqcup Q = \sim(\sim P \wedge \sim Q)$ regardless of which subspaces P and Q may refer to. The decidability result by Dunn et al. [50] concerns such equational theories. They translated standard quantum logic over finite-dimensional spaces into (the equational fragment of) the first-order theory of real numbers, which is known to be decidable due to A. Tarski's famous theorem [99].

Theorem 2.2.2 (Dunn et al. [50])**.** *Given a* finite-dimensional *Hilbert space $\mathcal{H}$, the family of equations (among terms for closed linear subspaces of $\mathcal{H}$) that are valid in $\mathcal{H}$ is decidable, in the sense that there is an effective procedure that, given any equation, decides whether it is valid in $\mathcal{H}$ or not.*

2.2.2 Píron lattice

Birkhoff and von Neumann started with a Hilbert space, then they generated a lattice structure and showed some properties. Píron took a different approach and asked the following question: if we start from a lattice structure, what properties does the lattice need to posses to become a quantum lattice, that is, a lattice that is formed by the closed linear subspaces of a Hilbert space?

Before we look into the work of Píron, let us first make a remark about the notation. In Chapter 3 we will establish a categorical duality result between Piron lattices and the relational structures called Quantum dynamic frames[7].

It will be important to distinguish between operators and elements in Píron lattices and Quantum dynamic frames. Therefore we use small letters $p, q, \dots$ for elements in Píron lattices, which correspond to testable properties P in Hilbert spaces (and Quantum dynamic frames). The orthocomplement is denoted with $p^{\perp}$ (instead of $\sim P$) and the quantum join is denoted with $p \vee q$ (instead of $P \sqcup Q$).

The properties that Píron defined are as follows.

Definition 2.2.3. A *bounded lattice* $\mathfrak{L}$ is a lattice with a greatest element I ("top") and a least element O ("bottom"). An *ortholattice* $\mathfrak{L}$ is a bounded lattice $(L, \leq)$ that satisfies (1) below. An *orthomodular lattice* $\mathfrak{L}$ is an ortholattice $(L, \leq, -^{\perp})$ that satisfies (2). A *propositional system* $\mathfrak{L}$ is an orthomodular lattice $(L, \leq, -^{\perp})$ that satisfies (3)–(5). Lastly, a *Piron lattice* $\mathfrak{L}$ is a propositional system $(L, \leq, -^{\perp})$ that satisfies (6).

1. **Orthocomplement:** The lattice $\mathfrak{L}$ is equipped with a map $-^{\perp} : L \to L$ such that
   (a) $p^{\perp\perp} = p$;
   (b) $p \leq q$ implies $q^{\perp} \leq p^{\perp}$;
   (c) $p \wedge p^{\perp} = O$ and $p \vee p^{\perp} = I$.
2. **Weak Modularity:** $q \leq p$ implies $p[q] = q$, where $p[q] := p \wedge (p^{\perp} \vee q)$.
3. **Completeness:** For any $A \subseteq L$, its meet $\bigwedge A$ and join $\bigvee A$ are in L.

Call $a \in L$ an *atom* if $a \neq O$ and either $p = O$ or $p = a$ holds for every $p \in L$ such that $p \leq a$. Write $\mathrm{At}(\mathfrak{L})$ for the set of atoms of $\mathfrak{L}$.

4. **Atomicity:** For any $p \neq O$, there is an $a \in \mathrm{At}(\mathfrak{L})$ such that $a \leq p$.
5. **Covering Law:** If $a \in \mathrm{At}(\mathfrak{L})$ and $a \not\leq p^{\perp}$ then $p[a] \in \mathrm{At}(\mathfrak{L})$.[8]
6. **Superposition Principle:** For any two distinct $a, b \in \mathrm{At}(\mathfrak{L})$, there is a $c \in \mathrm{At}(\mathfrak{L})$, distinct from both a and b, such that $a \vee c = b \vee c = a \vee b$.[9]

[7] A categorical duality is a contravariant equivalence, and this standard definition is reviewed in more detail in Section 2.2.5. A quantum dynamic frame is a quantum analog of a labelled transition system, and a precise definition will be given in Section 2.2.3.

[8] In an orthomodular lattice, this statement of the Covering Law is equivalent to that in [86]. See [86] or [20] for proofs.

[9] Usually a Piron lattice is defined with the property called irreducibility instead of (6); see, for example, [102]. Yet a propositional system satisfies (6) iff it is irreducible.

We say that a Píron lattice $\mathfrak{L}$ is realisable by a Hilbert space, if there exists a Hilbert space, such that the lattice of closed linear subspaces is isomorphic with the Píron lattice $\mathfrak{L}$. Píron showed the following theorem.

Theorem 2.2.4 (Píron [86])**.** *Each Píron lattice of dimension at least 4 can be realised by a generalized Hilbert space.*

A generalized Hilbert space is not exactly a Hilbert space. Solér [83] and Mayet [80] formulated an additional condition under which the Píron lattice is realisable by a Hilbert space (over the complex numbers, the reals or the quartonians). However, Mayet's condition requires the Píron lattice to have infinite height, and hence the corresponding Hilbert space to have infinite dimension, making it impractical for many applications in quantum information theory. See [3] for a more in depth review of the relationship between Píron lattices and Hilbert spaces.

2.2.3 Modal logic approach

Modal logic

Modal logic is a language for reasoning about relational structures. It is a good choice that balances being intuitive and expressive with nice complexity properties. For example, modal logics are the bisimulation invariant fragment of first order logic [23, 24]. We only review the basic definitions to provide the notation used in this thesis. An overview of modal logic can be found in [32].

Let us define a standard modal logic. Let *Prop* be a set of proposition letters.

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \Box\phi,$$

where $p \in \mathsf{Prop}$. The box operator $\Box\phi$ can mean many things, like "at the next step ϕ holds", "somewhere in the future ϕ holds" or "ϕ is known". In our quantum setting $\Box\phi$ usually means ϕ holds at all non-orthogonal states, that is, after any measurement ϕ still holds.

The semantics is given on Kripke frames, that is, a pair $\mathcal{F} = (S, R)$, where S is a set of states and $R \subseteq S \times S$ is a relation. A Kripke model is a Kripke frame paired with a valuation $V : \mathsf{Prop} \to \mathcal{P}(S)$, where $V(p)$ is the set of states where p holds.

$$\begin{aligned}
\mathfrak{M}, s &\vDash p && \Leftrightarrow s \in V(p)\\
\mathfrak{M}, s &\vDash \neg\phi && \Leftrightarrow \mathfrak{M}, s \nvDash \phi\\
\mathfrak{M}, s &\vDash \phi \wedge \psi && \Leftrightarrow \mathfrak{M}, s \vDash \phi \text{ and } \mathfrak{M}, s \vDash \psi\\
\mathfrak{M}, s &\vDash \Box\phi && \Leftrightarrow \text{if } (s,t) \in R, \text{ then } \mathfrak{M}, t \vDash \phi.
\end{aligned}$$

If a formula ϕ is true at every state in $\mathfrak{M}$, we say ϕ is valid in $\mathfrak{M}$ and write $\mathfrak{M} \vDash \phi$. If ϕ is valid in all Kripke models $\mathfrak{M}$, then we say ϕ is valid and write $\vDash \phi$. Lastly, if ϕ is true in every model based on $\mathcal{F}$, then ϕ is valid on $\mathcal{F}$ and we write $\mathcal{F} \vDash \phi$.

Hybrid logic

Arthur Prior introduced hybrid logic [87]. Compared to modal logic, hybrid logic is more expressive, at the cost of losing some desirable properties that standard modal logic has. For example, hybrid logic is no longer bisimilation invariant. The logic we use in this thesis is more related to the hybrid language introduced by Patrick Blackburn and Jerry Seligman [33]. Hybrid logic is a modal logic where we can name states with nominals. The idea is to sort the proposition letters into two groups: "normal" proposition letters, that act the same as proposition letters in modal logic, and nominals, that are used to name states in the sense that they are true at exactly one single state.

Introducing names for states is quite natural for quantum modal logics. We have seen that Píron lattices are atomic, which implies they have "smallest" elements called atoms just above $\bot$, that is, there are no elements smaller than atoms other than $\bot$. In Kripke models these atomic elements correspond to single states, so nominals allow us to refer to atoms. We can use these nominals to express properties like a basis, or to define what a projector or unitary transformation actually does.

Let us define a standard hybrid logic, which extends the standard modal language with nominals i, variables x, $@_i$-operators to state that a formula holds at state i and $\downarrow x.$-operators which name the current state with x. Let Prop, Nom and Var be three countable and pairwise disjoint sets of proposition letters.

$$\phi ::= p \mid i \mid x \mid \neg\phi \mid \phi \wedge \phi \mid \Box\phi \mid @_k\phi \mid \downarrow x.\phi,$$

where $p \in \mathsf{Prop}$, $i \in \mathsf{Nom}$, $x \in \mathsf{Var}$ and $k \in \mathsf{Nom} \cup \mathsf{Var}$. A formula ϕ is called *closed* if for all $x \in \mathsf{Var}$ all occurrences of x in ϕ only appear under the scope of a down arrow $\downarrow x.(\cdot)$. The Hybrid Language $\mathcal{HL}$ is the collection of all closed formulas.

The models for hybrid logics are Kripke models $\mathfrak{M} = (S, R, V)$, where V is a valuation function $V : \mathsf{Prop} \cup \mathsf{Nom} \to \mathcal{P}S$ with the additional condition that for all $i \in \mathsf{Nom}$ we have $V(i) = \{s\}$ for some $s \in S$. In words, each nominal i holds at precisely one state s. The semantics for the hybrid operators is given by

- $\mathfrak{M}, s \vDash i$ iff $V(i) = \{s\}$,
- $\mathfrak{M}, s \vDash x$ iff $V(x) = \{s\}$,
- $\mathfrak{M}, s \vDash @_k\phi$ iff $\mathfrak{M}, t \vDash \phi$, where $V(k) = \{t\}$, and
- $\mathfrak{M}, s \vDash \downarrow x.\phi$ iff $\mathfrak{M}[V(x) := \{s\}], s \vDash \phi$, where $\mathfrak{M}[V(x) := \{s\}]$ is the model obtained by extending the valuation V of $\mathfrak{M}$ by putting $V(x) := \{s\}$.

With nominals we can define frame properties that cannot be defined in the standard modal language. For example, superposition is defined by $\Diamond\Diamond i$, i.e. each state is reachable from each other state in at most two steps. This implies that the frame is connected, which we know cannot be defined in the standard modal language (See [32, p.437]).

Although we can name states with nominals, in general we cannot assume that all states are named. In fact, in most cases we cannot name all states, because the model will be uncountably large. For example, the set of one-dimensional subspaces of a two dimensional complex vector space is uncountable. So the quantum bit is already modelled by an uncountably large Kripke model. Therefore it is convenient to be able to name states on the fly using $\downarrow x.\phi$, because to define a projection we not only need to speak about the properties of the current state, but also about the properties of the projections of the current state. Note that we can safely assume the current state is named, for example, $i \to \Box\Diamond i$ defines symmetry, but we cannot assume each state reachable from the current state is also named.

Soundness and completeness One goal of this thesis is to make a step towards an automated reasoning system about quantum computation. The choice of our logical systems are therefore not only motivated by their expressibility and intuitiveness, but also by computational considerations. The logics should be expressive enough to be able to handle the algorithms and protocols we wish to consider, but also simple enough for a computer to automatically check the correctness.

We will discuss two important parts of the logic: the semantics and the (syntactical) deductive system. Given a logic $\mathcal{L}$, the semantics for a given model $\mathfrak{M}$ decides whether or not a formula $\phi \in \mathcal{L}$ holds at a given state $s \in \mathfrak{M}$, denoted by $\mathfrak{M}, s \vDash \phi$. If a formula holds at every state in a model, we write $\mathfrak{M} \vDash \phi$. And if a formula holds at every state in every model we call the formula valid and write $\vDash \phi$. The deductive system provides a way to deduce formulas (from axioms) purely based on syntactical considerations. If we can deduce a formula ϕ from the axioms, we write $\vdash \phi$.

Ideally, we would like the semantics and deductive system to correspond to each other, that is $\vdash \phi$ iff $\vDash \phi$. In practice, however, we find many examples which do not satisfy this equation. Soundness, if $\vdash \phi$ then $\vDash \phi$, can be considered a minimal requirement for any formal logical system. It states that any formula we prove is actually valid. A logical system that proves formulas that are not valid, would be rather silly to consider, as it destroys the whole point of a formal proof system. Therefore every formal logic should be sound, and in particular every logic considered in this thesis is sound.

The other direction is called completeness, if $\vDash \phi$ then $\vdash \phi$. Completeness ensures that any tautology, a formula valid in all models under consideration, can be proven within the formal proof system. In addition, if a deductive system is complete, then adding any valid axiom will not increase its deductive power.

In many cases, we are only interested in models with certain properties. Often we restrict ourself to a class of models and then say that a system is sound and complete with respect to this class of models.

Completeness of hybrid logic Let us now show a known completeness result for hybrid logic. Let us first discuss some known lemmas and theorems in hybrid logic, all of which can be found in [32]. For the first lemma we first need to provide definitions for a pure formula and a named model.

Definition 2.2.5 (Pure formula)**.** A formula is called *pure*, if all its atoms are nominals, i.e. no variables and proposition letters occur in the formula. A formula ψ is called an *instance* of ϕ if there is a function $f : \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var} \to \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var}$ such that ψ can be obtained from ϕ by replacing all occurrences of $a \in \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var}$ by $f(a)$. With a *pure instance* ψ of ϕ we mean ψ is a pure formula and an instance of ϕ.

Note that a pure formula does not contain any variables and therefore cannot contain any down arrows either.

Definition 2.2.6 (Named model)**.** A model is called *named* if all states are named by a nominal.

The following lemma explains a connection between validity of a pure formula on a frame and being valid in a named model based on that frame.

Lemma 2.2.7 ([32, Lemma 7.22])**.** *Let $\mathcal{F} = (S, R)$ and let $\mathfrak{M} = (S, R, V)$ be a named model based on $\mathcal{F}$. Let ϕ be a pure formula. Suppose that for all pure instances ψ of ϕ we have $\mathfrak{M} \models \psi$. Then $\mathcal{F} \models \phi$.*

Several complete deductive systems exist for hybrid logic. We will discuss a small variation on the deductive system given in [32], using an axiom from [31] to handle the down arrow $\downarrow x.\phi$. In Figure 2.2 we give the rules, where σ is a function $\sigma : \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var} \to \mathcal{HL}(@, \downarrow)$ such that nominals are sent to nominals and variables are sent to variables, that is, $\sigma|_{\mathsf{Nom}} : \mathsf{Nom} \to \mathsf{Nom}$ and $\sigma|_{\mathsf{Var}} : \mathsf{Var} \to \mathsf{Var}$. The formula ϕ^σ is obtained from ϕ by uniformly replacing all occurrences of $a \in \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var}$ by $\sigma(a)$. In Figure 2.3 we state the axioms.

We can prove completeness without the Name and Paste rules using an ordinary canonical model construction. However, with the Name and Paste rules we can build a *named* canonical model. With Lemma 2.2.7 in mind, we can see why a named canonical model leads to a more powerful completeness result. If we add a pure formula ϕ to the list of axioms, by construction we have $\mathfrak{M} \models \phi$, where $\mathfrak{M}$ is the named canonical model. By Lemma 2.2.7, we now also have $\mathcal{F} \models \phi$, where $\mathcal{F}$ is the canonical frame. If ϕ characterises a frame property P, that is, $\mathcal{F} \models \phi$ iff $\mathcal{F}$ has property P, then the named canonical model will automatically

Rules	
MP	$\vdash \phi \to \psi, \vdash \phi \implies \vdash \psi$
Subst	$\vdash \phi \implies \vdash \phi^\sigma$
Gen$_@$	$\vdash \phi \implies \vdash @_i\phi$
Gen$_\Box$	$\vdash \phi \implies \vdash \Box\phi$
Name	$\vdash i \to \phi \implies \vdash \phi$ if i does not occur in ϕ
Paste	$\vdash @_i\Diamond j \land @_j\phi \implies \vdash @_i\Diamond\phi$ if $i \neq j$ and j does not occur in ϕ

Figure 2.2: Rules of $\mathcal{HL}$.

Axioms	
CT	All classical tautologies
$K_\Box$	$\vdash \Box(p \to q) \to \Box p \to \Box q$
$K_@$	$\vdash @_i(p \to q) \to @_i p \to @_i q$
Selfdual$_@$	$\vdash @_i p \leftrightarrow \neg @_i \neg p$
Ref$_@$	$\vdash @_i i$
Agree	$\vdash @_i @_j p \leftrightarrow @_j p$
Intro	$\vdash i \to (p \leftrightarrow @_i p)$
DA	$\vdash @_i(\downarrow x.\phi \leftrightarrow \phi[x := i])$

Figure 2.3: Standard axioms of $\mathcal{HL}$.

also satisfy property P. So we do not just obtain completeness of standard hybrid logic with respect to the class of all Kripke frames, but also completeness of standard hybrid logic extended with pure formulas with respect to the class of all frames characterised by these pure formulas. This will make our lives a lot easier in Chapter 4.

We will therefore discuss an alternative canonical model construction that leads to a named canonical model, which is discussed in [32]. To achieve this named canonical model we need the concept of a named maximal consistent subset. A maximal consistent subset (MCS) Γ is called *named* if there is an $k \in \Gamma$ for some $k \in \mathsf{Nom}$. The following lemma introduces a class of named maximal consistent subsets Δ_i induced by an arbitrary MCS Γ, and shows some desirable properties. Later on, this class of named MCS's will be used as the set of states of our named canonical model.

Lemma 2.2.8 ([32, Lemma 7.24])**.** *Let Γ be a maximal consistent subset (MCS). For every nominal i, let Δ_i be $\{\phi \mid @_i\phi \in \Gamma\}$. Then*

1. *For every nominal i, Δ_i is an MCS that contains i.*
2. *For all nominals i and j, if $i \in \Delta_j$, then $\Delta_j = \Delta_i$.*
3. *For all nominals i and j, $@_i\phi \in \Delta_j$ iff $@_i\phi \in \Gamma$.*
4. *If k is a name for Γ, then $\Gamma = \Delta_k$.*

Let Σ be a set of consistent formulas. Our goal is to obtain a canonical model $\mathfrak{M}_\Sigma$ in which each state is a maximal consistent subset of quantum hybrid formulas (MCS) of the form Δ_i as described in the above lemma, and $\mathfrak{M}_\Sigma, \Delta_i \vDash \Sigma$ for some $i \in \mathsf{Nom}$. If we simply extend Σ to a standard MCS Γ we are faced with two problems. First we need Γ to be named, that is a $k \in \mathsf{Nom}$ such that $k \in \Gamma$ and therefore $\Gamma = \Delta_k$. This will be achieved with the help of the Name rule.

Second, we need there to be enough Δ_i inside our MCS Γ, so that we can prove the existence lemma. For this we need Γ to be pasted. A MCS Γ is called *pasted* if for every $@_i\Diamond\phi \in \Gamma$ there exists a nominal $j \in \mathsf{Nom}$ such that $@_i\Diamond j \wedge @_j\phi \in \Gamma$. This second property is achieved with the help of the Paste rule. The following lemma is an alternative Lindenbaum lemma that establishes that each consistent set of formulas Σ can be extended to a named and pasted MCS Γ.

Lemma 2.2.9 (Lindenbaum lemma [32, Lemma 7.25])**.** *Let Nom' be a (countably) infinite collection of nominals disjoint from Nom, and let $\mathcal{HL}'$ be the language obtained by adding these new nominals to $\mathcal{HL}$. Then every $\mathcal{HL}$-consistent set of formulas Σ in $\mathcal{HL}$ can be extended to a named and pasted $\mathcal{HL}'$-MCS in language $\mathcal{HL}'$.*

Now we can define the canonical model that we will use in the completeness result.

Definition 2.2.10 (Canonical model [32, Definition 7.26])**.** Let Γ be a named and pasted MCS. The named canonical model $\mathfrak{M}_\Gamma$ yielded by Γ is given by $\mathfrak{M}_\Gamma = (S_\Gamma, R_\Gamma, V_\Gamma)$, where the set of states is given by $S_\Sigma = \{\Delta_i \mid i \in \mathsf{Nom}\}$. The relation R_Γ is the standard canonical relation, so $\Delta_i \not\perp \Delta_j$ iff $\phi \in \Delta_j$ for every $\Box\phi \in \Delta_i$. The valuation V_Σ is given by $V(\phi) = \{\Delta_i \mid \phi \in \Delta_i\}$.

Because we require Γ to be pasted, for every $@_i\Diamond\phi \in \Gamma$ we have a nominal j that witnesses the existence of a named successor that satisfies ϕ, that is, $@_i\Diamond j \wedge @_j\phi \in \Gamma$. This leads to the existence lemma.

Lemma 2.2.11 (Existence lemma [32, Lemma 7.27])**.** *Let Γ be a named and pasted MCS and let $\mathfrak{M} = (S, R, V)$ be the named canonical model yielded by Γ. Suppose $\Delta_i \in S$ and that $\Diamond\phi \in \Delta_i$. Then there is a $j \in \mathsf{Nom}$ such that $\Delta_i R \Delta_j$ and $\phi \in \Delta_j$.*

The following truth lemma is a natural consequence of the existence lemma.

Lemma 2.2.12 (Truth lemma [32, Lemma 7.28])**.** *Let Γ be a named and pasted MCS, let $\mathfrak{M} = (S, R, V)$ be the named canonical model yielded by Γ and let $\Delta_i \in S$. Then for all formulas ϕ we have $\mathfrak{M}, \Delta_i \models \phi$ iff $\phi \in \Delta_i$.*

Note that we need a slightly different proof for the Truth lemma than the one presented in [32], as they do not discuss the down arrow. However, as noted in [31], it is easy to see that the only axiom involving the down arrow (Figure 2.3-DA) will take care of formulas of the form $\downarrow x.\phi$ in the inductive proof of the Truth Lemma. From the above lemmas we can deduce the desired completeness result.

Theorem 2.2.13 (Completeness [32, Theorem 7.29])**.** *Every consistent set of formulas Σ in language $\mathcal{HL}$ is satisfiable in a countable named model. Moreover, if Π is a set of pure formulas and $\mathcal{HL}(\Pi)$ is the hybrid logic obtained by adding all formulas in Π as axioms, then every consistent set of formulas Σ in language $\mathcal{HL}(\Pi)$ is satisfiable in a countable named model based on a frame which validates every formula in Π.*

Note that we are especially interested in the "moreover" part of the above theorem in Chapter 4, as this allows us to build a canonical model based on a quantum frame, rather than an ordinary Kripke frame.

Orthologic

Goldblatt introduced a quantum logic with Kripke style semantics [62] in which the orthogonal relation, denoted by $\sim$, plays a key role. For a set of propositions Prop the set of well formed formulas is given by

$$\phi ::= p \mid \phi \wedge \phi \mid {\sim}\phi.$$

where $p \in \mathsf{Prop}$. The set of all well formed formulas is denoted by Form. As we will see below, the special symbol $\sim$ is a modal operator, similar to $\Box$. Goldblatt also introduced a proof system.We will not give the entire proof system here, but as an example we state the axioms and the rule concerning $\wedge$

$$\begin{aligned}&\phi \wedge \psi \vdash \phi\\ &\phi \wedge \psi \vdash \psi\\ &\text{if } \phi \vdash \psi \text{ and } \phi \vdash \chi, \text{ then } \phi \vdash \psi \wedge \chi\end{aligned}$$

For formulas $\phi, \psi \in$ Form we write $\phi \vdash \psi$ if there is a finite list of axioms and applications of rules, where the last equation is $\phi \vdash \psi$ and the premisses of every applied rule appear earlier in the list.

The model is based on a special type of Kripke frame, called an orthoframe. An orthoframe is a pair $(\Sigma, \perp)$, where Σ is a set of states and $\perp$ is an orthogonality relation on Σ, i.e. $\perp$ is irreflexive and symmetric. Using this relation we can define the orthocomplement ${\sim}S$ of a set $S \subseteq \Sigma$ by

$${\sim}S := \{t \in \Sigma \mid t \perp S\} = \{t \in \Sigma \mid \forall s \in S \text{ we have } t \perp s\}.$$

We call a set $P \subseteq \Sigma$ biorthogonally closed or testable iff $P = {\sim}{\sim}P$. Note that if we have a Hilbert space $\mathcal{H}$ and build an orthoframe by taking Σ as the set of one-dimensional subspaces of $\mathcal{H}$ and $\perp$ as expected, then $P \subseteq \Sigma$ is testable iff P is a testable property or a closed linear subspace.

A function $V : \mathsf{Prop} \longrightarrow \mathcal{P}\Sigma$ is a valuation if $V(p) \subseteq \Sigma$ is testable for every $p \in \mathsf{Prop}$. We extend V to $\mathcal{V}$: Form $\longrightarrow \mathcal{P}\Sigma$ by $\mathcal{V}(\phi \wedge \psi) = \mathcal{V}(\phi) \cap \mathcal{V}(\psi)$ and $\mathcal{V}({\sim}\phi) = {\sim}\mathcal{V}(\phi)$. We call the triple $(\Sigma, \perp, \mathcal{V})$ an orthomodel. With the valuation $\mathcal{V}$ we have a natural interpretation for formulas in Form: for any $s \in \Sigma$ and $\phi \in$ Form

$$s \vDash \phi \Leftrightarrow \phi \in \mathcal{V}(\phi).$$

We say ϕ holds at s if $s \vDash \phi$. We write $\phi \vDash \psi$ if for every orthomodel $(\Sigma, \perp, \mathcal{V})$ and every state $s \in \Sigma$ we have $\Sigma, s \vDash \phi$ implies $\Sigma, s \vDash \psi$. Goldblatt proved his proof system is both sound and complete.

Although orthomodels are able to represent quantum systems, not every orthomodel is a quantum system. We call an orthomodel a quantum orthomodel if the model respects the orthomodular law introduced by Birkhoff and von Neumann, that is $\phi \wedge ({\sim}\phi \vee (\phi \wedge \psi)) \vDash \psi$ is valid in the model. If we restrict our attention to quantum orthomodels, we have to weaken the definition of $\phi \vDash \psi$: for all quantum orthomodels $(\Sigma, \perp, V)$, whenever $\Sigma, s \vDash \phi$ we have $\Sigma, s \vDash \psi$. As this is a much weaker requirement, the relation $\vDash$ will contain many more pairs $\phi \vDash \psi$. Therefore the original proof system is no longer complete. Goldblatt also introduced a quantum proof system, in particular he added an axiom representing the orthomodular law introduced by Birkhoff and von Neumann, and he showed completeness between these new quantum relations.

Logic for quantum actions

In [9] Alexandru Baltag and Sonja Smets take classical propositional dynamic logic (PDL, [65]) and combine this with ideas from Goldblatt's orthologic to create a quantum propositional dynamic logic called the logic for quantum actions (LQA). The great benefit of LQA is that dynamic quantum operators are directly represented in the language. For a set of testable properties $\mathcal{T}$ and a set of uniform transformations $\mathcal{U}$, the syntax is given by

$$\begin{aligned} \phi &::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid [\pi]\phi \\ \pi &::= \top \mid P? \mid U \mid \pi^{\dagger} \mid \pi \cup \pi \mid \pi ; \pi . \end{aligned}$$

Here p is a proposition letter, $[\pi]\phi$ intuitively means the weakest precondition which ensures we obtain ϕ after applying program π, $P \in \mathcal{T}$ is a testable property, $U \in \mathcal{U}$ is a unitary transformation, $\pi^{\dagger}$ is the adjoint of π, $\pi \cup \pi'$ is the random choice between program π or π' and $\pi;\pi'$ is sequential composition.

A dynamic frame is a set of states Σ together with a set of relations $\{\xrightarrow{P?}\}_{P\in\mathcal{T}}$ and a set of relations $\{\xrightarrow{U}\}_{U\in\mathcal{U}}$. Note that using the test relations $\{\xrightarrow{P?}\}_{P\in\mathcal{T}}$ we can define an orthogonal relation $\perp$ by

$$x \perp y \Leftrightarrow \text{ there exists no testable } P \in \mathcal{T} \text{ such that } x \xrightarrow{P?} y.$$

So far the definition of LQA is basically the same as classical PDL. The main difference are the tests $P?$. In classical PDL it is assumed that any $P \subseteq \Sigma$ is testable and that the corresponding relation $\xrightarrow{P?}$ is the diagonal on P, that is $x \xrightarrow{P?} y$ implies $x = y \in P$. So classical tests only check if a state x is already in P and do not change the state. In LQA only orthogonally closed properties $P = {\sim}{\sim}P$ are testable and the corresponding relation $\xrightarrow{P?}$ is assumed to be a partial function $f : \Sigma \longrightarrow P$. This means that in LQA we cannot test every property and if a state lies outside the tested property P, a successful test changes the current state to a state inside P.

Baltag and Smets also introduced several frame properties to ensure that these Kripke frames correspond to quantum systems. These properties are motivated by the axiomatic approach by Píron [86], and the duality result given in Chapter 3 will ensure each quantum dynamic frame is indeed realisable by a generalized Hilbert space.

Definition 2.2.14. A *quantum dynamic frame* $\mathfrak{F}$ is a tuple $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ such that Σ is a set, $\mathcal{L} \subseteq \mathcal{P}(\Sigma)$, and $\xrightarrow{P?} \subseteq \Sigma \times \Sigma$ for each $P \in \mathcal{L}$, and that satisfies the following, where $\rightarrow = \bigcup_{P\in\mathcal{L}} \xrightarrow{P?}$:

1. $\mathcal{L}$ is closed under arbitrary intersection.

2. $\mathcal{L}$ is closed under orthocomplement, where the orthocomplement of $A \subseteq \Sigma$ is ${\sim}A := \{s \in \Sigma \mid s \not\rightarrow t \text{ for all } t \in A\}$.

3. **Atomicity:** For any $s \in \Sigma$, $\{s\} \in \mathcal{L}$.

4. **Adequacy:** For any $s \in \Sigma$ and $P \in \mathcal{L}$, if $s \in P$, then $s \xrightarrow{P?} s$.

5. **Repeatability:** For any $s, t \in \Sigma$ and $P \in \mathcal{L}$, if $s \xrightarrow{P?} t$, then $t \in P$.

6. **Self-Adjointness:** For any $s, t, u \in \Sigma$ and $P \in \mathcal{L}$, if $s \xrightarrow{P?} t \to u$, then there is a $v \in \Sigma$ such that $u \xrightarrow{P?} v \to s$.

7. **Covering Property:** Suppose $s \xrightarrow{P?} t$ for $s, t \in \Sigma$ and $P \in \mathcal{L}$. Then, for any $u \in P$, if $u \neq t$ then $u \to v \not\to s$ for some $v \in P$; or, contrapositively, $u = t$ if $u \to v$ implies $v \to s$ for all $v \in P$.

8. **Proper Superposition:** For any $s, t \in \Sigma$ there is a $u \in \Sigma$ such that $s \to u \to t$.

The main benefit of LQA is the explicit syntax for dynamic operators. This makes LQA much more suitable to design and verify quantum programs. Moreover, LQA has the classical negation $\neg$ alongside the orthocomplement $\sim$, whereas the logics by Birkhoff and von Neumann and Goldblatt only have the orthocomplement.

Zhong's quantum Kripke frame. In [107], Shengyang Zhong provided an equivalent definition of a quantum dynamic frame that is worth discussing, because we will use this alternative definition later on in Chapter 4.

Definition 2.2.15 (Zhong's quantum Kripke frame [107])**.** A *quantum Kripke frame* is a Kripke frame $\mathcal{F} = (\Sigma, \to)$ such that

1. $s \to s$ for every $s \in \Sigma$. *(reflexive)*

2. $s \to t$ implies that $t \not\to s$, for any $s, t \in S$. *(symmetry)*

3. For any $s, t \in \Sigma$, if $s \neq t$, then there exists a $w \in \Sigma$ such that $w \to s$ and $w \not\to t$. *(separation)*

4. For every $P \subseteq \Sigma$ such that $\sim\sim P = P$, if $s \in \Sigma \setminus \sim P$, then there exists a $s' \in \Sigma$ which is an approximation of s in P, that is, $s' \in P$ and $s \to w$ iff $s' \to w$ for all $w \in P$. *(existence of approximation)*

5. For any $s, t \in \Sigma$ there exists a $w \in \Sigma$ such that $s \to w \to t$. *(superposition)*

In Theorem 2.7.25 of [107] Zhong proves the equivalence of a quantum Kripke frame (Definition 2.2.15) and a quantum dynamic frame (Definition 2.2.14).

Logic for quantum programs

All logics discussed so far can only express single systems, thus in essence only reason about one single qubit or about a mutli-partite system about which we cannot say anything of the different components. As most quantum programs and protocols use several qubits we need to extend the language to multi-partite systems in which we can describe the subsystems. Normally if we want to talk about a quantum system that is build up from several subsystems we take the tensor product construction. However, in 1979 Foulis and Randall proved there is no "tensor" construction for quantum logics, which would have the same desired properties as Hilbert spaces [60]. We can address the problem by applying the tensor product to the state space only, instead of the entire logic. Baltag and Smets have also investigated logics for multi-partite systems, where the state space is a tensor product of Hilbert spaces [11]. This logic is called the Logic of Quantum Programs (LQP).

We present here a slight variation of LQP, using a "quantum" knowledge operator K_I [13]. For the modality K_I, fix a set of natural numbers N, using $i \in N$ as indices for Hilbert spaces $\mathcal{H}_i$ that compose the system $\mathcal{H} = \bigotimes_{i \in N} \mathcal{H}_i$. (Typically $\mathcal{H}_i = \mathbb{C}^2$, but not necessarily.) So each subset $I \subseteq N$ is intended to refer to the subsystem composed of the basic components $\mathcal{H}_i$ with $i \in I$, that is, $\mathcal{H}_I = \bigotimes_{i \in I} \mathcal{H}_i$. In this setting $K_I \phi$ means that "(the local state of) *subsystem I carries the information that ϕ is (globally) the case*".

For the semantics of our "local-information modalities" K_I, we should think of the Hilbert space $\mathcal{H} = \bigotimes_{i \in N} \mathcal{H}_i$ as divided into a principal subsystem $\mathcal{H}_I = \bigotimes_{i \in I} \mathcal{H}_i$ and its "environment" $\mathcal{H}_{N \setminus I} = \bigotimes_{i \in N \setminus I} \mathcal{H}_i$. Then $K_I \phi$ is supposed to mean that *the subsystem I carries the information that ϕ*. This idea can be made precise using the density-operator formalism. For any unit vector $v \in s$, the pure state s of the global system N can be alternatively described by the corresponding density operator ρ_v^N. The so-called *reduced density operator $s_I =$* $\mathrm{tr}_{N \setminus I}(\rho_v)$, obtained by taking the partial trace $\mathrm{tr}_{N \setminus I}$ over the environment $N \setminus I$, is typically a *mixed state*, which describes *the "state" s_I of the sub-system I* (when the global system is in state s). The relation of *I-indistinguishability* between global states s, t can thus be defined by putting:

$$s \sim_I t \iff s_I = t_I \iff tr_{N \setminus I}(\rho_v) = tr_{N \setminus I}(\rho_v) \text{ for unit vector } v \in s, w \in t.$$

Essentially, $s \sim_I t$ means that the global states s and t are "locally the same from the viewpoint of I". The indistinguishability relation can be alternatively characterized in terms of *I-remote* actions: these are unitary transformations $U : \mathcal{H} \to \mathcal{H}$ having the property that $U = \mathrm{Id}_I \otimes V$, where $\mathrm{Id}_I : \mathcal{H}_I \to \mathcal{H}_I$ is the identity map on subsystem I and $V : \mathcal{H}_{N \setminus I} \to \mathcal{H}_{N \setminus I}$ is some unitary transformation on its environment. Then it follows that

$$s \sim_I t \iff t = U(s) \text{ for some } I\text{-remote } U.$$

Axioms	
Kripke Axiom	$[\pi](p \to q) \to ([\pi]p \to [\pi]q)$
Testability Axiom	$\Box p \to [q?]p$
Partial Functionality	$\neg[p?]q \to [p?]\neg q$
Adequacy	$p \wedge q \to \langle p?\rangle q$
Repeatability	$T(p) \to [p?]p$
Proper Superpositions	$\langle\pi\rangle\Box\Box p \to [\pi']p$
Unitary Functionality	$\neg[U]q \leftrightarrow [U]\neg q$
Unitary Bijectivity 1	$p \leftrightarrow [U; U^{\dagger}]p$
Unitary Bijectivity 2	$p \leftrightarrow [U^{\dagger}; U]p$
Adjointness	$p \to [\pi]\Box\langle\pi^{\dagger}\rangle\Diamond p$

Figure 2.4: Some sound axioms of the logic for quantum programs.

Now, using the I-indistinguishability relation, we can define an "epistemic" modality K_I in the way that is standard in epistemic modal logic: i.e., we can say that *subsystem I "knows" (it carries the information) that ϕ is the case in state* s iff ϕ is the case in all the states that are I-indistinguishable from s. More formally,

$$s \in \llbracket K_I\phi \rrbracket \begin{array}{l} \iff t \in \llbracket \phi \rrbracket \text{ for every } t \sim_I s \\ \iff U(s) \in \llbracket \phi \rrbracket \text{ for every } I\text{-remote } U \end{array}$$

Or we can put this as follows: I-remote unitary transformations are symmetries that tinker with the environment alone, leaving anything in the principal subsystem I intact; so I locally carries the information that ϕ iff ϕ is invariant under those symmetries.

In [11], Baltag and Smets proposed several sound axioms, the axioms for single system are stated in Figure 2.4. Beside these axioms, they also provided axioms for multi-partite systems, which are less relevant for this thesis. With these axioms, Baltag and Smets prove the correctness of teleportation and quantum secret sharing. On a critical note, LQP cannot express any classical communication nor any classical knowledge of agents, which for many communication protocols is a crucial ingredient. To extend the quantum setting with classical components, Baltag and Smets have recently designed a different system that deals with the classical-quantum interaction [17]. However in this thesis we restrict our attention to the pure quantum setting.

2.2.4 Probabilistic logic

Probabilities arise quite naturally in quantum mechanics, as measuring a qubit that is in a superposition state will have a non-deterministic outcome. While there is a strong tradition in quantum logics that connects to many-valued logics in the algebraic logic tradition, the connection to traditional probabilistic logics having their own specific proof theory and semantics is not often addressed. In Chapter 5 we introduce a quantum logic with probabilities partially based on the work by Fagin, Halpern and Megiddo [54]. Their work considers probabilistic statements and linear inequalities, for example, $3\,\mathrm{Pr}(\phi) \leq 1$ would mean the probability that ϕ is true is less than or equal to $\frac{1}{3}$.

More precisely, given a modal language $\mathcal{L}$ containing the symbol $\mathtt{tt}$ to denote truth, i.e. a formula which is always true. We add formulas of the form $t \geq \rho$, where t is a term, that is

$$\begin{aligned} \phi ::=& p \mid \mathtt{tt} \mid \neg\phi \mid \phi \wedge \phi \mid \Box\phi \mid t \geq \rho \\ t ::=& \rho\,\mathrm{Pr}(\phi) \mid t + t \end{aligned}$$

where $p \in \mathsf{Prop}$ is a proposition letter and $\rho \in \mathbb{Q}$. Given a Kripke model $\mathfrak{M} = (S, R, V)$, the semantics of all standard modal formulas are given as before. Let us consider a probability function $f : \mathcal{P}(S) \to [0,1]$ such that $f(S) = 1$ and $f(A \cup B) = f(A) + f(B)$ if $A \cap B = \emptyset$. We can extend f to terms by putting $f(\rho\,\mathrm{Pr}(\phi)) = \rho \cdot f([\![\phi]\!])$ and $f(t + t') = f(t) + f(t')$. We then say $t \geq \rho$ is true if $f(t) \geq \rho$ holds in a natural way.

Although several other works on probabilistic logic have appeared, Fagin, Halpern and Megiddo [54] were the first to introduce a sound and complete proof system. This deductive system can be split into two parts: one about linear inequalities and the other about probabilities. The axioms for linear inequalities are as follows:

I1	$t \geq \beta \leftrightarrow t + 0\,\mathrm{Pr}(\phi) \geq \beta$
I2	$\sum_{k=1}^{n} \alpha_k \,\mathrm{Pr}(\phi_k) \geq \beta \to \sum_{k=1}^{n} \alpha_{j_k} \,\mathrm{Pr}(\phi_{j_k}) \geq q\beta$ for any permutation $j_1, \ldots, j_n$ of $1, \ldots, n$
I3	$\sum_{k=1}^{n} \alpha_k \,\mathrm{Pr}(\phi_k) \geq \beta \wedge \sum_{k=1}^{n} \alpha'_k \,\mathrm{Pr}(\phi_k) \geq \beta'$ $\to \sum_{k=1}^{n} (\alpha_k + \alpha'_k) \,\mathrm{Pr}(\phi_k) \geq (\beta + \beta')$
I4	$t \geq \beta \leftrightarrow dt \geq d\beta$ if $d > 0$
I5	$t \geq \beta \vee t \leq \beta$
I6	$t \geq \beta \to t \geq \gamma$ if $\beta > \gamma$

All these axioms appear in our deductive system of a probabilistic quantum logic. For classical probabilities we have the following axioms:

P1	$\mathrm{Pr}(\mathtt{tt}) = 1$
P2	$\mathrm{Pr}(\phi) \geq 0$
P3	$\mathrm{Pr}(\phi \wedge \psi) + \mathrm{Pr}(\phi \wedge \neg\psi) = \mathrm{Pr}(\phi)$.
P4	$(\phi \equiv \psi) \to \mathrm{Pr}(\phi) = \mathrm{Pr}(q)$

Axioms P1, P2, and P4 also hold when we interpret Pr as a quantum probability. However, P3 needs to be adjusted in the quantum context, because the complement in classical logic is exchanged for the orhtocomplement in quantum logic. Also, quantum probability has more structure than classical probability, so three more axioms are needed to fully characterize quantum probability, which we will do in Chapter 5.

2.2.5 Duality

Duality is a notion from category theory. To understand duality let us first go over some basic definitions in category theory. For a more detailed overview of category theory, see for example [77]. After we have defined duality, we will discuss some duality results related to quantum logic.

Category theory

Definition 2.2.16 (Category)**.** A category $\mathcal{C}$ consists of objects $\mathsf{Obj}(\mathcal{C})$, morphisms $\mathsf{Mor}(\mathcal{C})$ and a way to compose morphisms ($\circ$). Each category has to satisfy the following properties:

- (*composition*) If $f : X \to Y$ and $g : Y \to Z$, then there exists a morphism $g \circ f : X \to Z$.
- (*associativity*) $f \circ (g \circ h) = (f \circ g) \circ h$.
- (*identity*) For all objects $X \in \mathsf{Obj}(\mathcal{C})$ there exists an identity morphism $1_X : X \to X$ such that for each $f : X \to Y$ and $g : Y \to X$ we have $f \circ 1_X = f$ and $1_X \circ g = g$.

Examples of categories are sets with functions, Hilbert spaces with unitary transformations or the natural numbers with inequality ($\leq$). A morphism $f : X \to Y$ is called an *isomorphism* if there exists a $g : Y \to X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$. Each category $\mathcal{C}$ has a dual category $\mathcal{C}^{\mathsf{Op}}$, where the arrows of each morphism are reversed. Thus a morphism $f : X \to Y$ in $\mathcal{C}^{\mathsf{Op}}$ means f is a morphism in $\mathcal{C}$ from Y to X.

Given two categories $\mathcal{C}$ and $\mathcal{D}$ we can define a functor, which is like a function or morphism between categories.

Definition 2.2.17 (Covariant functor)**.** A functor $F : \mathcal{C} \to \mathcal{D}$ is a function that sends each object $X \in \mathsf{Obj}(\mathcal{C})$ to an object $F(X) \in \mathsf{Obj}(\mathcal{D})$, sends each morphism $f : X \to Y$ in $\mathsf{Mor}(\mathcal{C})$ to a morphism $F(f) : F(X) \to F(Y)$ in $\mathsf{Mor}(\mathcal{D})$, and preserves identity and composition, that is:

- (*preserves identity*) For each $X \in \mathsf{Obj}(\mathcal{C})$, the identity 1_X is send to $1_{F(X)}$.
- (*preserves composition*) $F(f \circ g) = F(f) \circ F(g)$.

A functor that satisfies the above conditions is called *covariant*. A variation of a covariant functor is the *contravariant* functor, which reverses the direction of morphisms. Thus $f : X \to Y$ is send to $F(f) : F(Y) \to F(X)$ and $F(f \circ g) = F(g) \circ F(f)$.

Given two functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{D}$, with the same domain category and range category, we can define a function from F to G called a natural transformation.

Definition 2.2.18 (Natural transformation)**.** A natural transformation $\eta : F \to G$ is a family of morphisms $\{\eta_X : F(X) \to G(X)\}_{X \in \mathsf{Obj}(\mathcal{C})}$ in $\mathsf{Mor}(\mathcal{D})$ such that for each $f : X \to Y$ in $\mathsf{Mor}(\mathcal{C})$ we have $G(f) \circ \eta_X = \eta_Y \circ F(f)$. That is

$$\begin{tikzcd}
X \arrow[d, "f"'] & & F(X) \arrow[r, "\eta_X"] \arrow[d, "F(f)"] & G(X) \arrow[d, "G(f)"] \\
Y & \Longrightarrow & F(Y) \arrow[r, "\eta_Y"'] & G(Y)
\end{tikzcd}$$

If η_X is an isomorphism for each $X \in \mathsf{Obj}(\mathcal{C})$, then we say that F and G are *isomorphic*.

We call two categories $\mathcal{C}$ and $\mathcal{D}$ *equivalent* if we have two covariant functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $F \circ G$ is isomorphic to the identity functor $1_{\mathcal{D}}$ and $G \circ F$ is isomorphic to $1_{\mathcal{C}}$. We call two categories $\mathcal{C}$ and $\mathcal{D}$ *dual* if we have two contravariant functors with the same property.

A quantum duality

The duality result between Piron lattices and quantum dynamic frames presented in Chapter 3 of this thesis builds on an earlier duality result by David Moore [81]. He showed that a duality result can be obtained between the category of state spaces (**State**) and the category of property lattices (**Prop**). These are more general structures than quantum dynamic frames and Píron Lattices respectively and therefore captures only some properties of quantum mechanics.

An object in **State** is a pair $(S, \perp)$, where S is a set of states and $\perp$ is an orthogonal relation between states which satisfies the following three conditions:

SO1 if $s \perp t$, then $t \perp s$,

SO2 if $s \perp t$, then $s \neq t$, and

SO3 if $s \neq t$, then there exists a $u \in S$ such that $s \perp u$ and $t \not\perp u$.

Given a state space $(S, \perp)$ and a set of states $A \subseteq S$, we define $A^\perp := \{s \in S \mid s \perp t \text{ for all } t \in A\}$. If $A^{\perp\perp} = A$, then A is called biorthogonally closed. A morphism from $(S_1, \perp_1)$ to $(S_2, \perp_2)$ is a partially defined map $f : S_1 \setminus K_1 \to S_2$ such that

SM1 $K_1 \cup f^{-1}(B_2)$ is biorthogonally closed in S_1 for each biorthogonally closed $B_2 \subseteq S_2$.

The set K_1 is called the kernel of f and is necessarily biorthogonally closed.

An object in **Prop** is a lattice $(L, \leq, -^{\perp})$ which satisfies the following six conditions:

PO1 there exists a maximal element $1 \in L$,

PO2 the greatest lower bound $\bigwedge A$ of an arbitrary non-empty family A exists,

PO3 $a = \bigwedge\{p^{\perp} \mid p \leq a^{\perp}, p \text{ an atom}\}$ for each $a \in L$,

PO4 $a^{\perp\perp} = a$ for each $a \in L$,

PO5 if $a \leq b$, then $b^{\perp} \leq a^{\perp}$, and

PO6 $a \wedge a^{\perp} = 1^{\perp}$ for each $a \in L$,

where an atom is an element $p \neq 1'$ such that if $x < p$, then $x = 1'$ or $x = p$. A morphism from $(L_1, \leq_1, -^{\perp_1})$ and $(L_2, \leq_2, -^{\perp_2})$ is a map $h : L_1 \to L_2$ such that

PM1 $h(\bigwedge_1 A) = \bigwedge_2 h[A]$ for any $A \subseteq L_1$, and

PM2 if b is an atom of L_2, then there exists an atom a of L_1, such that $b \leq_2 h(a)$.

Moore showed the categories **State** and **Prop** are equivalent in [81].

2.3 Quantum information theory

Quantum information theory aims to utilize the properties specific to quantum mechanics to create information theorectic and computational tools that can advance the investigations in a number of fields, including computer science, communication theory, network theory, cryptography, etc. The goal is to improve security of cryptographic protocols, speed up computations and improve efficiency of codecs.

2.3.1 Quantum computation algorithms

In this subsection we will discuss several quantum algorithms. Quantum computation is believed to exponentially speed up classical computation. The main benefit for quantum computation is the combination of superposition and entanglement. This allows us in some special cases to perform a special kind of parallel computing called quantum parallelism.

Deutsch algorithm. The simplest example to illustrate quantum parallelism is the Deutsch-algorithm [45]. Over the years several improvements have been made to this algorithm. We will present the Deutsch-algorithm as it can be found in [84], where the reader can also find a historical overview of the improvements. The problem is as follows: suppose we are given a classical function f which sends one bit to one bit. Can we determine whether the function is balanced, i.e. both 0 and 1 are in the image, or constant, i.e. either 0 and 1 are both sent to either 0 or both are sent to 1. With a classical computer we can decide this only by first calculating $f(0)$ and then $f(1)$, which gives a full description of the function and therefore we know whether f is balanced or constant.

With a quantum computer we can do better, we can apply the function f only once and still be able to decide whether f is balanced or constant. However, as f is not necessarily invertible, we first have to find a unitary transformation that characterizes f. The unitary transformation is denoted with U_f and acts as follows

$$U_f(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle\,.$$

It is easy to check that this transformation is unitary. If we simply apply U_f to the superposition

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle),$$

we get

$$\frac{1}{\sqrt{2}}(|0f(0)\rangle + |1f(1)\rangle).$$

So, if we measure the first qubit in the standard basis, we have a 50% chance the second qubit collapses to $f(0)$ and a 50% chance it collapses to $f(1)$. The solution is to put both input qubits in a superposition, that is,

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

For readability we use the notation $\overline{x} = x \oplus 1$. After applying U_f we get

$$\frac{1}{2}(|0f(0)\rangle - |0\overline{f(0)}\rangle + |1f(1)\rangle - |1\overline{f(1)}\rangle).$$

We can now rewrite the formula depending on whether f is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$):

$$\begin{aligned}
&\frac{1}{2}((|0\rangle + |1\rangle)\,|f(0)\rangle - (|0\rangle + |1\rangle)\,|\overline{f(0)}\rangle) \text{ if } f \text{ is constant, or}\\
&\frac{1}{2}((|0\rangle - |1\rangle)\,|f(0)\rangle - (|0\rangle - |1\rangle)\,|\overline{f(0)}\rangle) \text{ if } f \text{ is balanced.}
\end{aligned}$$

After applying the Hadamard transformation on the first qubit ($H \otimes I$) we get

$$\frac{1}{\sqrt{2}} |0\rangle \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) \text{ if } f \text{ is constant, or}$$
$$\frac{1}{\sqrt{2}} |1\rangle \left(|f(0)\rangle - |\overline{f(0)}\rangle\right) \text{ if } f \text{ is balanced.}$$

So if we measure the first qubit in the standard basis, the outcome is $|0\rangle$ if the function is constant and $|1\rangle$ if the function is balanced.

The efficiency of the Deutsch algorithm is compromised by the fact that we use two input qubits. Clearly there is a classical alternative with two input bits that does an even better job: simply apply the function f twice in parallel. However, in 1992 David Deutsch and Richard Jozsa published a generalization called the Deutsch-Jozsa algorithm [46]. This algorithm decides whether a function f from $\{0,1\}^{2n}$ to $\{0,1\}$ is balanced or constant with only one application of f. Here we only need $2n+1$ input qubits, which is better than any known classical algorithm.

The Deutsch-algorithm was the first algorithm that shows that quantum computations are potentially more efficient than classical computations.

Grover's search algorithm. Grover's search algorithm was first published in [63] under the title "Quantum mechanics helps in searching for a needle in a haystack". And that is exactly what the algorithm does: it searches for a particular data point in a large (random) data set. Assume we have a data set of N points, where we normally assume $N = 2^n$ for some $n \in \mathbb{N}$, and suppose we have a function $f : N \to \{0,1\}$ called a selection function. Our goal is to find an $x \in N$ such that $f(x) = 1$. The best classical solution, given that the data set is randomly ordered, is to randomly select an $x \in N$ and check whether $f(x) = 1$ or not. This will lead to an average of $\frac{N}{2}$ calculations. A quantum computer can reduce this to about $\sqrt{N}$ calculation steps. The procedure is as follows (See Figure 2.5 for a graphical representation of these steps).

1. Initialize first state $|\phi_0\rangle$ as the superposition of all possible solutions, that is
$$|\phi_0\rangle = \sum_{i=1}^{N} \frac{1}{\sqrt{N}} |i\rangle$$

2. Flip the sign of the amplitudes of correct solutions, thus if $|\phi_{k-1}\rangle = \sum_{i=1}^{N} a_i |i\rangle$, then
$$|\phi_k\rangle = \sum_{i=1}^{N} (-1)^{f(i)} a_i |i\rangle .$$

   This operation does not change the probability of measuring the outcomes; after all, squaring a negative number makes it positive again. But it does change the average amplitude, which we can "obtain" using the following unitary.

$$U_a |\phi\rangle = (\frac{1}{N} \sum_{i,j=1}^{N} |i\rangle \langle j|)(\sum_{k=1}^{N} a_k |k\rangle) = \frac{1}{N} \sum_{i,j,k=1}^{N} a_k |i\rangle \langle j \mid k\rangle = \sum_{i=1}^{N} (\frac{1}{N} \sum_{k=1}^{N} a_k) |i\rangle .$$

Therefore we can apply step 3 below.

3. Flip all amplitudes around the average.

$$|\phi_k\rangle = (2U_a - I) |\phi_{k-1}\rangle .$$

4. Iterate step 2 and 3 about $\frac{\pi}{4}\sqrt{N}$ times. Repeating the steps $\frac{\pi}{4}\sqrt{N}$ ensures the difference between the probability of finding the correct solution and the probability of finding a wrong solution is maximal.

5. Measure $|\phi_k\rangle$ in the standard basis. The probability of finding a particular element is the square of the amplitude, which makes the difference between the correct solution and other elements even more pronounced. In most cases the probability of finding the correct solution is over 90%.

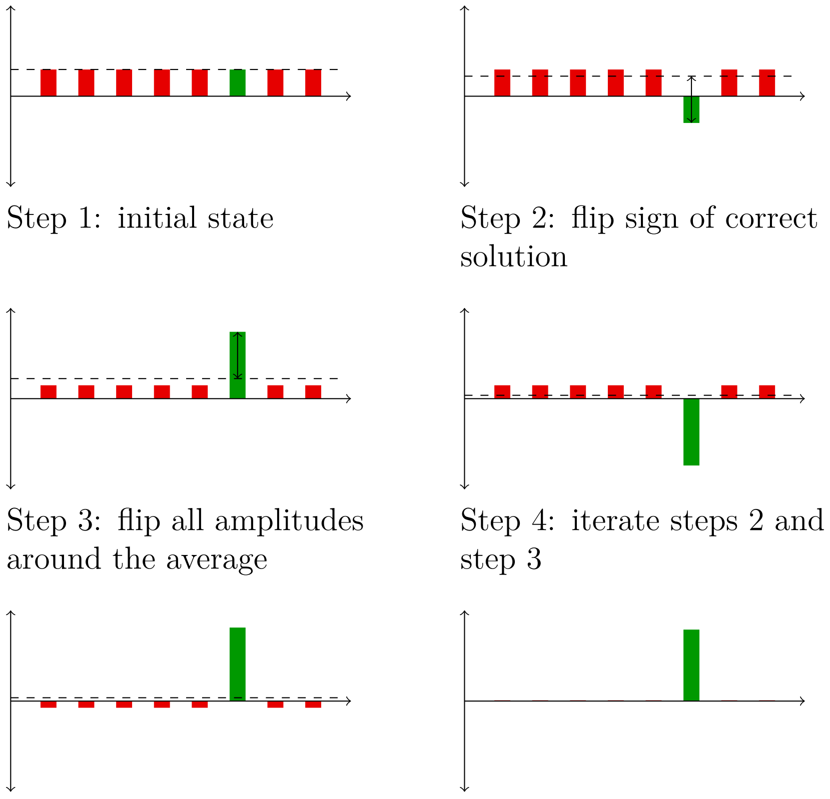
Note that Grover's search algorithm quadratically speeds-up the search process. This is not as impressive or important as an exponential speed-up, but this speed-up has been mathematically proven, whereas most other quantum algorithms only speed-up the best currently known classical counterpart.

Final remarks. Several other quantum algorithms exist. One of the most interesting ones was published by Peter Shor in 1994 [95]. He discovered an algorithm that factors integers into prime numbers in polynomial time[10]. At this moment no polynomial classical algorithm is known and for this reason quantum computers are believed to exponentially speed up computation. Although this is very impressive, the speed-up of Shor's factoring algorithm remains unproven.

Quantum computers also have some limitations: in 1973 Holevo proved a surprising upper bound for quantum information [70]. While we will not discuss this result here, we can mention that as a consequence of this bound we cannot transmit more information with n qubits than with n classical bits.

To summarize, we currently know algorithms that potentially make quantum computers exponentially faster than classical computers. However, it has never been proven that there exist no classical polynomial time algorithm that factors integers. On the other hand, we do know algorithms that quadratically speed-up classical computation.

[10] Actually, it is called bounded error quantum polynomial time (BQP)



Step 1: initial state

Step 2: flip sign of correct solution

Step 3: flip all amplitudes around the average

Step 4: iterate steps 2 and step 3

Step 5: measure the qubit

Figure 2.5: Grover's search algorithm explained in pictures.

2.3.2 Quantum communication protocols

Shor's fast factoring algorithm creates great complications for the security of classical communication as this algorithm breaks most electronic cryptographic protocols currently in use[11]. On the other hand, the main limitations in quantum computers caused by the fact that qubits collapse after measurements and the no-cloning theorem, are actually great benefits for cryptology. By cleverly using these properties one can develop protocols that can detect eavesdroppers on an insecure communication channel. For example, in 1984 Bennett and Brassard invented what is now called the BB84 protocol [21].

BB84. In the BB84 protocol there are two parties, traditionally called Alice and Bob. Alice and Bob want to establish a shared secret key. This key is just a random string of 0's and 1's, which then can be used to encrypt a message by simple addition (bitwise XOR).

Alice starts the protocol by creating two random bit strings of the same length, for example by tossing a coin. Then the first bit string decides what bits to send and the second bit string decides in what basis to send: either $A = \{|0\rangle, |1\rangle\}$ or $B = \{|-\rangle, |+\rangle\}$. Remember that $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is a "perfect" superposition of $|0\rangle$ and $|1\rangle$, thus measuring $|-\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ has a probability of 50% for both $|0\rangle$ and $|1\rangle$ as outcome.

Bob does not know what basis Alice used to send the bits. So after he receives a qubit he randomly selects a basis by tossing a coin and measures the qubits in this basis. If he uses the same basis as Alice used to send the bit, then Bob measures the bit Alice send. If he uses the other basis, he will measure the sent bit only 50% of the time.

After Alice has sent all bits, she and Bob publicly announce which basis they used for every bit. Then they delete all bits where they used a different basis. Now they should both have the same random bit string. See table 2.1 for an example.

Let us discuss two possible attacks on the protocol by an eavesdropper Eve. As Eve cannot copy the qubits, she can only measure the qubits or apply a unitary transformation and send the result on to Bob, or possibly send a newly made qubit. Let us analyse the case where Eve decides to act as Bob, thus she randomly selects one of the two above mentioned bases and measures the qubit. Afterwards she sends the qubit on to Bob. If she uses the same basis as Alice, the outcome of the measurements is the correct bit and Eve sends the qubit from Alice unaltered to Bob. On the other hand, if Eve chooses the wrong basis, not only has she a 50% chance to measure the wrong bit, the qubit from Alice has changed. Now if Bob measures the qubit in the same basis as Alice (50% chance) he has a 50% chance the outcome is wrong. Thus in total 12,5% of the final

[11] There are several proposals for cryptographic protocols that are still considered safe even if a large quantum computer would be build, see for example [27].

Alice										
Random bits	0	1	1	0	1	1	1	0	1	0
Random bases	A	A	B	A	A	A	B	A	B	B
Sends	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Bob										
Random bases	B	A	B	B	A	B	A	A	B	B
Observes	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
Bits	0	1	1	1	1	0	1	0	1	0
Bases agree		✓	✓		✓			✓	✓	✓
Final bits		1	1		1			0	1	0

Table 2.1: An example of the BB84 protocol. (Example taken from [104].)

bit strings Alice and Bob have is different. There is a very easy way to discover Eve's attack: Alice and Bob can exchange half of the remaining bits on a public channel. If too many bits differ, it is very probable Eve was eavesdropping.

There is also a different attack: Eve could apply a unitary transformation. For example, let us consider CNOT discussed in section 2.3.1. If Alice uses basis A, then CNOT will create an exact copy. On the other hand, if Alice uses basis B, the transformation CNOT will create an entangled pair and Bob will measure the wrong bit 50% of the time and we will end up with the same error rate as in the measurement attack. So after Alice and Bob compare half of the remaining bits they will in most cases detect Eve.

In fact, Biham, Boyer, Boykin and Mor proved that BB84 is secure against any measurement or unitary transformation attack in the sense that Eve always introduces errors if she learns information about the key [28]. However, this proof does require that Alice and Bob have an authenticated classical channel, or equivalently that Eve cannot disturb the classical channel. This is in general assumed in quantum security proofs. This means safety holes introduced by the classical channel are ignored.

If we do not assume a secure classical channel there is an obvious attack: the man in the middle attack [106]. In this attack Eve controls both the quantum channel and the classical channel. She completely acts like Bob towards Alice and as Alice towards Bob. As Alice and Bob cannot detect who there talking to, they will not detect Eve. This attack is very plausible as quantum computers break many, if not all, classical encryption schemes. On the other hand, there is still a big advantage of BB84 over most classical protocols. As the shared key of Alice and Bob at the end of the protocol is a completely random bitstring, the message encrypted with this bitstring will be secure if the eavesdropper failed to break the key while the protocol was in progress. In a classical protocol an eavesdropper could simple record all communication, including the encrypted message, and then simply break the key even years after the message has been sent. So a quantum protocol can in the very least limit the time an eavesdropper has to break the key.

Many variations on the BB84 protocol exist. For example, the EPR protocol introduced by Artur K. Ekert in 1991 [52] is a variation on the BB84 protocol. In this protocol Alice prepares n pairs of entangled qubits and sends one of each pair to Bob. After receiving all of them they both randomly measure their qubits in one of three possible bases. After finishing measuring the qubits they publicly compare the bases they used to measure the qubits and throw away the qubits measured in different bases. Then, in order to detect a possible eavesdropper, they compare half of the remaining bits and check if Bell's inequalities (See [19]) are respected. If so, it is very likely an eavesdropper was listening in. If the inequalities are violated the obtained bit string is safe and can be used to encode messages.

Quantum leader election. The Quantum Leader Election protocol is a method for selecting exactly one of n many members, giving each member an equal chance of being selected. This is analogous to establishing a fair n-sided die, and such selections are important for distributive systems. There exists several ways to solve this problem using quantum theory, e.g. [47, 98]. The ones given in [98] consider the quantum leader election protocol in anonymous networks. In these protocols each agent is a different node in a network, but has the same identifier, and is therefore anonymous. Communication plays a key role in these protocols, where the protocol takes several rounds to complete. The one given in [47] is the quantum equivalent of a fair coin, where each agent, although strictly speaking not necessarily, might be in the same room and only requires one measurement.

As we do not explicitly model communciation we will only discuss the protocol given in [47]. Given a set N of agents, the protocol assigns a quantum bit (a two dimensional Hilbert space) to each agent $i \in N$ together with a basis $\{|0\rangle_i, |1\rangle_i\}$. Then the following state, called the W-state, is considered:

$$\sum_{i\in N} \frac{1}{\sqrt{N}} \left(\bigotimes\nolimits^{\mathfrak{M}}_{j\in N\setminus\{i\}} |0\rangle_j \right) \otimes^{\mathfrak{M}} |1\rangle_i \,.$$

This state entangles the qubits in such a way that, after one of the agents measure their qubit in the standard basis $\{|0\rangle_i, |1\rangle_i\}$, the state will collapse to a state where only one agent will measures $|1\rangle_i$ and all other agents measure $|0\rangle_i$, where each agent has the same probability to measure $|1\rangle_i$. The agent who measures $|1\rangle_i$ is then considered to be the newly selected leader.

Chapter 3

Duality for the logic of quantum actions

Summary: In this chapter we show a duality between two approaches to represent quantum structures abstractly and to model the logic and dynamics therein. One approach puts forward a “quantum dynamic frame” [10], a labelled transition system whose transition relations are intended to represent projections and unitaries on a (generalized) Hilbert space. The other approach considers a “Piron lattice” [86], which characterizes the algebra of closed linear subspaces of a (generalized) Hilbert space. We define categories of these two sorts of structures and show a duality between them. This result establishes, on one direction of the duality, that quantum dynamic frames represent quantum structures correctly; on the other direction, it gives rise to a representation of dynamics on a Piron lattice.

Background: This chapter relates Píron lattices, discussed in Chapter 2.2.2, to quantum Kripke frames, discussed in Chapter 2.2.3. The definitions of the morphisms in this Chapter are largely based on the work by David Moore, who showed several duality results on structures closely related to quantum structures, which are discussed in Chapter 2.2.5. As duality is a technique from category theory, some background knowledge on category theory is assumed, which can be found in Chapter 2.2.5.

This chapter is organised as follows. We define two categories of Piron lattices in Subection 3.1.1, one with homomorphisms defined by Moore, and the other with homomorphisms preserving more structure. We define two categories of quantum dynamic frames in Section 3.1.2, similarly with two sorts of structure-preserving maps. We define functors from the Piron lattices to the quantum dynamic frames in Subsection 3.2.1, and the opposite ones in Subsection 3.2.2. These then form dualities, which will be proven in Subsection 3.2.3, and, in Subsection 3.2.4, we restrict these dualities to the categories of objects satisfying Mayet’s condition.

3.1 The Categories

In this section, we define categories of Piron lattices and of quantum dynamic frames.[1] In fact we provide two categories, $\mathbb{L}_w$ and $\mathbb{L}_s$, of Piron lattices, and also two categories, $\mathbb{F}_w$ and $\mathbb{F}_s$, of quantum dynamic frames. In each case the two categories share the same objects, but one (viz., $\mathbb{L}_w$ or $\mathbb{F}_w$) has more morphisms than the other (viz., $\mathbb{L}_s$ or $\mathbb{F}_s$); or, in other words, morphisms in the former preserve less structure than ones in the latter.

3.1.1 Categories of Piron Lattices

Any Hilbert space $\mathcal{H}$ gives rise to a lattice $(L, \leq)$, where L is the family of closed linear subspaces and $\leq$ is set-inclusion $\subseteq$; moreover, the orthocomplement in $\mathcal{H}$ gives a map $-^{\perp} : L \to L$. Piron [86] axiomatized lattices $(L, \leq, -^{\perp})$ that arise from Hilbert spaces in this way—lattices satisfying his axioms (in Definition 3.1.1 below) are now called Piron lattices. As he proved, Piron lattices of height at least 4 correspond to (generalized) Hilbert spaces of dimension at least 4. In this section we define two categories, $\mathbb{L}_w$ and $\mathbb{L}_s$, of Piron lattices. They share the same objects, but $\mathbb{L}_w$ has more morphisms than $\mathbb{L}_s$.

Piron Lattices

Next we provide a set of axioms of a Piron lattice. Lattices satisfying certain subsets of the axioms have useful names as shown in the following definition.

Definition 3.1.1. A *bounded lattice* is a lattice with a greatest element I ("top") and a least element O ("bottom"). An *ortholattice* $\mathfrak{L}$ is a bounded lattice $(L, \leq)$ that satisfies (1) below. An *orthomodular lattice* $\mathfrak{L}$ is an ortholattice $(L, \leq, -^{\perp})$ that satisfies (2). A *propositional system* $\mathfrak{L}$ is an orthomodular lattice $(L, \leq, -^{\perp})$ that satisfies (3)–(5). Lastly, a *Piron lattice* $\mathfrak{L}$ is a propositional system $(L, \leq, -^{\perp})$ that satisfies (6).

1. **Orthocomplement:** $\mathfrak{L}$ is equipped with a map $-^{\perp} : L \to L$ such that
   (a) $p^{\perp\perp} = p$;
   (b) $p \leq q$ implies $q^{\perp} \leq p^{\perp}$;
   (c) $p \wedge p^{\perp} = O$ and $p \vee p^{\perp} = I$.
2. **Weak Modularity:** $q \leq p$ implies $p[q] = q$, where $p[q] := p \wedge (p^{\perp} \vee q)$.
3. **Completeness:** For any $A \subseteq L$, its meet $\bigwedge A$ and join $\bigvee A$ are in L.

Call $a \in L$ an *atom* if $a \neq O$ and either $p = O$ or $p = a$ holds for every $p \in L$ such that $p \leq a$. Write $\mathrm{At}(\mathfrak{L})$ for the set of atoms of $\mathfrak{L}$.

[1] See [7] for an exposition of category theory.

4. **Atomicity:** For any $p \neq O$, there is an $a \in \mathrm{At}(\mathfrak{L})$ such that $a \leq p$.

5. **Covering Law:** If $a \in \mathrm{At}(\mathfrak{L})$ and $a \not\leq p^\perp$ then $p[a] \in \mathrm{At}(\mathfrak{L})$.[2]

6. **Superposition Principle:** For any two distinct $a, b \in \mathrm{At}(\mathfrak{L})$, there is a $c \in \mathrm{At}(\mathfrak{L})$, distinct from both a and b, such that $a \vee c = b \vee c = a \vee b$.[3]

Atoms are meant to correspond to one-dimensional subspaces, or rays, of a Hilbert space; so they satisfy, for instance:

7. $a \not\leq p$ iff $a \wedge p < a$ iff $a \wedge p = O$, for any atom a.

The fact that closed linear subspaces in general are certain sets of rays is expressed in Piron lattices by

Proposition 3.1.2. *Let $\mathfrak{L}$ be an orthomodular lattice satisfying Completeness and Atomicity. Then $\mathfrak{L}$ is* atomistic*, meaning that every $p \in L$ has $p = \bigvee [\![p]\!]$, where $[\![p]\!] := \{a \in \mathrm{At}(\mathfrak{L}) \mid a \leq p\}$.*

Proof. First observe that $p = q$ if both $q \leq p$ and $[\![p]\!] \subseteq [\![q]\!]$, as follows. Suppose the antecedents. $[\![p]\!] \subseteq [\![q]\!]$ means that, for any $a \in \mathrm{At}(\mathfrak{L})$, if $a \leq p$ then $a \leq q$, which implies $a \not\leq q^\perp$, for otherwise $a \leq q \wedge q^\perp = O$. Therefore no $a \in \mathrm{At}(\mathfrak{L})$ satisfies $a \leq p \wedge q^\perp$, that is, $p \wedge q^\perp = O$, i.e., $p^\perp \vee q = I$. Hence $p = p \wedge (p^\perp \vee q) = q$ by $q \leq p$ and Weak Modularity.

Let $q = \bigvee [\![p]\!]$. Then it holds that both $q \leq p$ and $[\![p]\!] \subseteq [\![q]\!]$. Here $\bigvee [\![p]\!] \leq p$ because $a \leq p$ for all $a \in [\![p]\!]$; and if $a \in [\![p]\!]$ then $a \leq \bigvee [\![p]\!]$. □

The connective $p[q] := p \wedge (p^\perp \vee q)$ defined in (2) of Definition 3.1.1 is sometimes called the "Sasaki projection" [41]. The monotone map $p[-] : L \to L$ expresses, in Hilbert-space terms, the direct-image[4] operation under the projector onto the subspace p; this should make the conceptual meaning of (2) and (5) of Definition 3.1.1 transparent. There are many properties an expression of projectors must satisfy, we list some of them below.

8. $p[q] = p \wedge (p^\perp \vee q) \leq p$.

9. $p[a] \wedge a^\perp = p \wedge (p^\perp \vee a) \wedge a^\perp = (p \wedge a^\perp) \wedge (p \wedge a^\perp)^\perp = O$.

10. If $q \leq p^\perp$ then $p[q] = p \wedge (p^\perp \vee q) = p \wedge p^\perp = O$.

Lemma 3.1.3. *For any $a, b \in \mathrm{At}(\mathfrak{L})$, $a \not\leq b^\perp$ is equivalent to $b[a] = b$ and to*

[2] In an orthomodular lattice, this statement of the Covering Law is equivalent to that in [86]. See [86] or [20] for proofs.

[3] Usually a Piron lattice is defined with the property called irreducibility instead of (6); see, for example, [102]. Yet a propositional system satisfies (6) iff it is irreducible.

[4] Because of the view of Sasaki projection as a direct-image, we use the notation standardly used for such. On page 56, we define direct-image for arbitrary functions.

(a) $p[a] = b$ *for some* $p \in L$.

Proof. If $a \not\leq b^\perp$, then $b[a] \neq O$ by the Covering Law, whereas $b[a] \leq b$ by (8) for atom b, and hence $b[a] = b$. Also, $b[a] = b$ obviously implies (a). Finally, if (a) $p[a] = b$, then $a \not\leq b^\perp$, for otherwise $b \leq a^\perp$ and (9) would imply $b = b \wedge a^\perp = p[a] \wedge a^\perp = O$ for atom b. □

In an ortholattice $\mathfrak{L}$, define $[p]q := p^\perp \vee (p \wedge q) = (p[q^\perp])^\perp$, the so-called "Sasaki hook", obtaining a monotone map $[p]- : L \to L$. This expresses the inverse-image operation under the projector onto p.[5] In fact, Weak Modularity amounts to the adjunction[6] formed by direct image $p[-]$ and inverse image $[p]-$ (just as in $f[-] \dashv f^{-1}[-]$ for any function f):

Theorem 3.1.4 (Coecke and Smets [41])**.** *An ortholattice* $\mathfrak{L}$ *satisfies Weak Modularity iff every* $p[-]$ *is left adjoint to* $[p]-$ *(written* $p[-] \dashv [p]-$*).*

$-[-]$ and $[-]-$ are also meant to generalize conjunction and implication (classical logic has $p \wedge - \dashv p \Rightarrow -$ for classical implication $\Rightarrow$). They are supposed to mean, respectively, the following:

- $p[q]$: We may have moved to the current state by testing whether p or not (and receiving the answer "Yes") when q was the case.

- $[p]q$: If we test p and receive the answer "Yes", then q will be the case.

These may help make sense of the unit and counit laws of the adjunction, $q \leq [p](p[q])$ and $p[[p]q] \leq q$. In fact, it is useful to observe that Weak Modularity amounts to the equalities among the following six terms.

$$\begin{array}{rcl}
p[[p]q] & \overset{\text{def}}{=} & p \wedge (p^\perp \vee (p^\perp \vee (p \wedge q))) \\
 & & \| \\
p[p \wedge q] & \overset{\text{def}}{=} & p \wedge (p^\perp \vee (p \wedge q)) \\
{\scriptsize \begin{array}{c}\text{Weak}\\ \text{Modularity}\end{array}} \rotatebox{-90}{$\leq$} & \leqq & \| \,{\scriptsize \text{def}} \\
p \wedge q & & p \wedge [p]q
\end{array} \tag{3.11}$$

[5] Here inverse images are meant to include the kernel.

[6] An *adjunction* between two partially ordered sets $(S_1, \leq_1)$ and $(S_2, \leq_2)$ (often called a *Galois connection*) is a pair of monotone maps $L : S_1 \to S_2$ and $R : S_2 \to S_1$ such that $L(x) \leq_2 y$ iff $x \leq_1 R(y)$ for all $x \in S_1$ and $y \in S_2$, or, equivalently, for which the "unit" law $x \leq_1 RL(x)$ and the "counit" law $LR(y) \leq_2 y$ hold. Such L and R are called *left* and *right adjoints* to each other. In fact, adjunction is defined for categories $\mathbb{C}$, $\mathbb{D}$ and functors $L : \mathbb{C} \to \mathbb{D}$ and $R : \mathbb{D} \to \mathbb{C}$ in general, by requiring certain conditions (that hold trivially in the case of posets) on the correspondence between morphisms $f : L(C) \to D$ and $g : C \to R(D)$, or on natural transformations $\eta : 1_{\mathbb{C}} \to RL$ (unit) and $\epsilon : LR \to 1_{\mathbb{D}}$ (counit). See [7, Definition 9.6 and Proposition 10.1]. We mention a general adjunction in Theorem 3.2.24.

Morphisms of Piron Lattices

There are options as to how to define morphisms of Piron lattices. The first one is due to Moore [81, 82].

Definition 3.1.5. A function $h : L_1 \to L_2$ is a *weak homomorphism between two Piron lattices* $(L_1, \leq_1, -^{\perp_1})$ and $(L_2, \leq_2, -^{\perp_2})$ if the following hold:

12. $h(\bigwedge_1 A) = \bigwedge_2 h[A]$ for any $A \subseteq L_1$.

13. *(Moore's condition)* if b is an atom of L_2, then there exists an atom a of L_1, such that $b \leq_2 h(a)$.

These homomorphisms form a category [81, 82]: the composition of two weak homomophisms is again a weak homomorphism, and the identity map is the identity. Let us write $\mathbb{L}_w$ for this category of Piron lattices and weak homomorphisms. As a second option we consider the smaller class of morphisms that also preserve orthocomplement, and as a consequence preserve arbitrary joins including the bottom.

Definition 3.1.6. A weak homomorphism $k : L_1 \to L_2$ is a *strong homomorphism between Piron lattices* $(L_i, \leq_i, -^{\perp_i})$ $(i = 1, 2)$ if k moreover satisfies

14. $k(p^{\perp_1}) = k(p)^{\perp_2}$ for all $p \in L_1$.

Clearly, the composition of two strong homomorphisms also preserves the orthocomplement, and the identity map is a strong homomorphism; so Piron lattices and strong homomorphisms form a subcategory, $\mathbb{L}_s$, of $\mathbb{L}_w$ that is "wide" in the sense of sharing all the objects. Note that strong homomorphisms preserve I, O, $\vee$, $-[-]$ and $[-]-$, since they preserve $\wedge$ and $-^{\perp}$.

3.1.2 Categories of Quantum Dynamic Frames

We now proceed to define two categories $\mathbb{F}_w$ and $\mathbb{F}_s$ for quantum dynamic frames. Similarly to the Piron lattice categories we defined earlier, they have the same objects and only differ in their morphisms.

Quantum Dynamic Frames

Any Hilbert space $\mathcal{H}$ gives rise to a Kripke frame: a tuple $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ where Σ is the set of rays in $\mathcal{H}$; $\mathcal{L}$ is the family of closed linear subspaces of $\mathcal{H}$, with each subspace expressed as a set of rays; and, for each closed linear subspace $P \in \mathcal{L}$, $\xrightarrow{P?}$ is the relation on Σ such that $s \xrightarrow{P?} t$ iff the projection of s onto P in $\mathcal{H}$ is t. With these projections we can also define the non-orthogonality relation: s is not orthogonal to t, written $s \to t$, iff $s \xrightarrow{P?} t$ for some $P \in \mathcal{L}$. So s is orthogonal to t iff $s \not\to t$. Then we can furthermore define the orthocomplement $\sim\! A$ of any subset $A \subseteq \Sigma$: $s \in \sim\! A$ iff $s \not\to t$ for all $t \in A$.

The axioms of a quantum dynamic frame given by Baltag and Smets [10] aim at characterizing Kripke frames $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ that can be abstracted away from Hilbert spaces in this manner.

Definition 3.1.7. A *quantum dynamic frame* $\mathfrak{F}$ is a tuple $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ such that Σ is a set, $\mathcal{L} \subseteq \mathcal{P}(\Sigma)$, and $\xrightarrow{P?} \subseteq \Sigma \times \Sigma$ for each $P \in \mathcal{L}$, and that satisfies the following, where $\to = \bigcup_{P\in\mathcal{L}} \xrightarrow{P?}$:

15. $\mathcal{L}$ is closed under arbitrary intersection.

16. $\mathcal{L}$ is closed under orthocomplement, where the orthocomplement of $A \subseteq \Sigma$ is $\sim\! A := \{s \in \Sigma \mid s \not\to t \text{ for all } t \in A\}$.

17. **Atomicity:** For any $s \in \Sigma$, $\{s\} \in \mathcal{L}$.

18. **Adequacy:** For any $s \in \Sigma$ and $P \in \mathcal{L}$, if $s \in P$, then $s \xrightarrow{P?} s$.

19. **Repeatability:** For any $s, t \in \Sigma$ and $P \in \mathcal{L}$, if $s \xrightarrow{P?} t$, then $t \in P$.

20. **Self-Adjointness:** For any $s, t, u \in \Sigma$ and $P \in \mathcal{L}$, if $s \xrightarrow{P?} t \to u$, then there is a $v \in \Sigma$ such that $u \xrightarrow{P?} v \to s$.

21. **Covering Property:** Suppose $s \xrightarrow{P?} t$ for $s, t \in \Sigma$ and $P \in \mathcal{L}$. Then, for any $u \in P$, if $u \neq t$ then $u \to v \not\to s$ for some $v \in P$; or, contrapositively, $u = t$ if $u \to v$ implies $v \to s$ for all $v \in P$.

22. **Proper Superposition:** For any $s, t \in \Sigma$ there is a $u \in \Sigma$ such that $s \to u \to t$.

The above definition differs from the one given in [10] in three ways. First, we have added (16), since (15) and (17)–(22) do not ensure (16).[7] Secondly, the axiom called Mayet's condition is part of the definition in [10], but we treat it as an additional axiom; we will discuss it in Section 3.2.4. Lastly, and perhaps most importantly, even though frames have unitary operators as part of their structure in [10], they do not in our definition. We will show how we deal with unitaries in Subsection 3.1.2.

The following series of lemmas show some basic properties of quantum dynamic frames. They will be used to show the duality result later on, but will also help with conceptual understanding of Definition 3.1.7. We start with one of the fundamental properties of the relation $\to$, which expresses non-orthogonality.

[7] For a counterexample, take an arbitrary Hilbert space $\mathcal{H}$ of dimension greater than 2; let Σ be the set of one-dimensional subspaces; let $\mathcal{L}$ consist exactly of $\varnothing$, Σ, and all singletons $\{s\} \subseteq \Sigma$; and let relations $\xrightarrow{\{s\}?}$ be the obvious ones. Since $s \to t$ iff $s \xrightarrow{\{t\}?} t$, it is easy to verify that $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ satisfies (15), (17)–(22) but not (16).

Lemma 3.1.8. *$\to$ is reflexive and symmetric.*

Proof. By Atomicity and Adequacy, $s \xrightarrow{\{s\}?} s$. So, assuming $s \to t$, we have $s \xrightarrow{\{s\}?} s \to t$. By Self-Adjointness, there is a $u \in \Sigma$ such that $t \xrightarrow{\{s\}?} u \to s$. By Repeatability, $u \in \{s\}$, so $u = s$. This means that $t \xrightarrow{\{s\}?} s$, so $t \to s$. □

This justifies writing $s \perp t$ and $s \not\perp t$ for $s \nrightarrow t$ and $s \to t$, our expression of the symmetric relations of orthogonality and non-orthogonality. Note that $s \perp t$ iff $s \in {\sim}\{t\}$, since ${\sim}A = \{s \in \Sigma \mid s \perp t \text{ for all } t \in A\}$.

An important consequence of Lemma 3.1.8 is the following. Let us define the modal operators $\Box, \Diamond : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ using $\to$ as accessibility; i.e.,

$$\begin{aligned}\Box A &= \{s \in \Sigma \mid t \in A \text{ whenever } s \to t\},\\ \Diamond A &= \{s \in \Sigma \mid s \to t \text{ for some } t \in A\} = \neg\Box\neg A,\end{aligned}$$

where $\neg$ is the set complement $\Sigma \setminus -$. Clearly, $\Box$ and $\Diamond$ are monotone, and

$${\sim}A = \{s \in \Sigma \mid t \notin A \text{ whenever } s \not\perp t\} = \Box\neg A = \neg\Diamond A.$$

Then Lemma 3.1.8 implies the following proposition. There, (23) and (24) are the modal-logical expressions of reflexivity and symmetry, respectively; (25) is another way of putting (24), and entails (26) immediately. (27) is by a classic result in [29]; also see [62] for "orthologic", the logic of ortholattices, and its modal-logical representation.

Proposition 3.1.9. *The monotone maps $\Box, \Diamond : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ satisfy:*

23. *$\Box A \subseteq A \subseteq \Diamond A$ for every $A \subseteq \Sigma$.*

24. *$A \subseteq \Box\Diamond A = {\sim}{\sim}A$ for every $A \subseteq \Sigma$.*

25. *$\Diamond \dashv \Box$.*

26. *$\Box\Diamond\Box = \Box$, i.e., ${\sim}{\sim}{\sim} = {\sim}$.*

27. *Moreover, $\mathcal{L}_{\sim\sim} = \{A \subseteq \Sigma \mid {\sim}{\sim}A = A\} = \{{\sim}A \mid A \subseteq \Sigma\}$ forms an ortholattice with the top Σ, the bottom $\varnothing$, orthocomplement $\sim$, $\wedge = \cap$ and $\vee = \sqcup$, which is defined by $A \sqcup B = {\sim}{\sim}(A \cup B) = \Box(\Diamond A \cup \Diamond B) = {\sim}({\sim}A \cap {\sim}B)$ for any $A, B \subseteq \Sigma$.*

Indeed, as we will show (in Proposition 3.1.18), $\mathcal{L}_{\sim\sim} = \mathcal{L}$. Its "$\subseteq$" part is easily obtained by (15)–(17):

Lemma 3.1.10. *For any $A \subseteq \Sigma$, ${\sim}A = \bigcap_{t \in A} {\sim}\{t\} \in \mathcal{L}$.*

For the "$\supseteq$" part, we need to reflect upon $\xrightarrow{P?}$, which purports to express a projector on Hilbert spaces. We show that it is a partial function (Corollary 3.1.13) and that $s \xrightarrow{P?} t$ means that t is the closest state to s inside P, in the sense that s and t are orthogonal to the same states in P (Proposition 3.1.15).

Lemma 3.1.11. *$s \xrightarrow{P?} t$ implies*

28. $t \in P$ and, for all $u \in P$, if $t \not\to u$ then $s \not\to u$.

Proof. Suppose $s \xrightarrow{P?} t$. By Repeatability, $t \in P$. Assume $t \not\to u$ for $u \in P$. Then, by $s \xrightarrow{P?} t \to u$, Self-Adjointness yields $v \in \Sigma$ such that $u \xrightarrow{P?} v \to s$. Since $u \in P$ and, by Lemma 3.1.8, $u \to w$ implies $w \to u$ for all $w \in P$, the Cover Property (with $u \xrightarrow{P?} v$) implies $u = v$. So $v \to s$ yields $s \not\to u$. □

Combining this with the Covering Property, we have

Lemma 3.1.12. *$s \xrightarrow{P?} v$ implies that v is the unique $t \in \Sigma$ satisfying* (28)*.*

Corollary 3.1.13. *$\xrightarrow{P?}$ is a partial function for each $P \in \mathcal{L}$.*

Lemma 3.1.14. *If $s \to u$ for some $u \in P$, then $s \xrightarrow{P?} t \to u$ for some unique $t \in P$.*

Proof. Suppose $s \to u$ for some $u \in P$. Then $u \xrightarrow{P?} u \to s$ by Adequacy and the symmetry of $\to$. Hence by Self-Adjointness $s \xrightarrow{P?} t \to u$ for some $t \in P$. The uniqueness is by Corollary 3.1.13. □

Proposition 3.1.15. *$s \xrightarrow{P?} t$ is equivalent to each of* (28) *and*

(a) $t \in P$ and, for all $u \in P$, $t \not\to u$ iff $s \not\to u$.

Proof. (a) obviously implies (28). We then show (28) implies $s \xrightarrow{P?} t$. Suppose (28). Then $s \not\to t$ since $t \not\to t$ by Lemma 3.1.8. So Lemma 3.1.14 yields $v \in P$ such that $s \xrightarrow{P?} v$, where $v = t$ by Lemma 3.1.12 since t satisfies (28).

Lastly, to show $s \xrightarrow{P?} t$ implies (a), suppose $s \xrightarrow{P?} t$. Then the assertion $t \in P$ and the "only if" part of (a) are Lemma 3.1.11; so, for the "if", assume $s \not\to u$ for $u \in P$. By Lemma 3.1.14, there is a $v \in \Sigma$ such that $s \xrightarrow{P?} v \not\to u$. But $s \xrightarrow{P?} t$ and Corollary 3.1.13 imply $v = t$ and so $t \not\to u$. □

This characterization of $\xrightarrow{P?}$ leads to the characterization of $\mathcal{L}$ as the family $\mathcal{L}_{\sim\sim}$ of fixed points of $\sim\sim$. First, writing $s \sqcup t$ for $\{s\} \sqcup \{t\} = \sim\sim\{s, t\} = \Box\Diamond\{s, t\}$, observe

Lemma 3.1.16. *Suppose $s \xrightarrow{P?} t \in P$ and that there is no $u \in s \sqcup t$ such that $s \to u \in \sim P$. Then $s = t$.*

Proof. By (24), $s, t \in \{s, t\} \subseteq {\sim}{\sim}\{s, t\} = s \sqcup t$; so $t \xrightarrow{s \sqcup t?} t$ by Adequacy. It is therefore enough by the Covering Property to show that $u \to t$ for all $u \in s \sqcup t$ such that $s \to u$. Fix such u; by the supposition, $u \notin {\sim}P$, i.e., $u \in \neg{\sim}P = \Diamond P$. Hence Lemma 3.1.14 yields some $v \in P$ such that $u \xrightarrow{P?} v$ and so $u \to v$. Then $u \in s \sqcup t = \Box\Diamond\{s, t\}$ implies $v \in \Diamond\{s, t\}$, i.e., either $v \to s$ or $v \to t$; this entails $u \to t$, since Proposition 3.1.15 with $s \xrightarrow{P?} t \in P$ and $u \xrightarrow{P?} v \in P$ implies that $v \not\to s$ iff $v \not\to t$ iff $u \not\to t$. □

Lemma 3.1.17. *${\sim}{\sim}P = P$ for every $P \in \mathcal{L}$.*

Proof. (24) implies $P \subseteq {\sim}{\sim}P$. Also, ${\sim}{\sim}P = \Box\Diamond P \subseteq \Diamond P$ by (23). Fix any $s \in {\sim}{\sim}P \subseteq \Diamond P$. Then Lemma 3.1.14 yields $t \in P$ with $s \xrightarrow{P?} t \in P$, whereas $s \in {\sim}{\sim}P$ means that $s \to u \in {\sim}P$ for no u. Hence Lemma 3.1.16 implies $s = t \in P$. □

This and Lemma 3.1.10, combined with Proposition 3.1.9, establish

Proposition 3.1.18. *$\mathcal{L} = \{A \subseteq \Sigma \mid {\sim}{\sim}A = A\} = \{{\sim}A \mid A \subseteq \Sigma\}$, and it forms an ortholattice $(\mathcal{L}, \subseteq, \cap, \sqcup, \Sigma, \varnothing, {\sim})$.*

The following import of Propositions 3.1.18 and 3.1.15 is worth observing. That is, when orthogonality $\perp$ is abstracted from a quantum dynamic frame, $\perp$ gives back $\mathcal{L}$ and $\xrightarrow{P?}$ using $\sim$. Here is another characterization of $\xrightarrow{P?}$, using the frame version of the Sasaki projection $P[Q] := P \cap ({\sim}P \sqcup Q)$.

Proposition 3.1.19. *$s \xrightarrow{P?} t$ iff $P[\{s\}] = \{t\}$.*

Proof. Recall from Proposition 3.1.15 that $s \xrightarrow{P?} t$ iff (28). Observe

$$\begin{aligned}
(28) \iff{}& t \in P \text{ and, for all } u \in P,\ u \perp s \text{ implies } t \perp u \\
\iff{}& t \in P \text{ and } t \perp u \text{ for all } u \in P \cap {\sim}\{s\} \\
\iff{}& t \in P \cap {\sim}(P \cap {\sim}\{s\}) \\
\iff{}& t \in P \cap ({\sim}P \sqcup \{s\}) = P[\{s\}] \qquad \text{(by Lemma 3.1.17).}
\end{aligned}$$

So $P[\{s\}] = \{t\}$ implies (28) and so $s \xrightarrow{P?} t$. On the other hand, if $s \xrightarrow{P?} t$ and (28), then Lemma 3.1.12 implies $P[\{s\}] = \{t\}$. □

Morphisms of Quantum Dynamic Frames

We discuss two options for morphisms on quantum dynamic frames. The first option is due to Moore [81]. First, given a partial function $f : \Sigma_1 \rightharpoonup \Sigma_2$ and any $A \subseteq \Sigma_2$, define the "weakest preimage" of A under f as

$$f^{-1}[A] := \{s \in \Sigma_1 \mid \text{either } f(s) \text{ is undefined or defined and } f(s) \in A\},^{8}$$

and observe that $f^{-1}[-] : \mathcal{P}(\Sigma_2) \to \mathcal{P}(\Sigma_1)$ is right adjoint to the direct-image operation $f[-] : \mathcal{P}(\Sigma_1) \to \mathcal{P}(\Sigma_2) :: B \mapsto \{f(s) \mid s \in B \text{ and } f(s) \text{ is defined}\}$.

Definition 3.1.20. A partial function $f : \Sigma_1 \rightharpoonup \Sigma_2$ is a *weak map between quantum dynamic frames* $(\Sigma_i, \mathcal{L}_i, \{\xrightarrow{P?}_i\}_{P\in\mathcal{L}_i})$ $(i = 1, 2)$ if $f^{-1}[-]$ "preserves testability", meaning that $f^{-1}[P] \in \mathcal{L}_1$ for all $P \in \mathcal{L}_2$,

Quantum dynamic frames and weak maps form a category, $\mathbb{F}_w$, where identity maps are identity morphisms. Another option of morphisms is bounded morphisms, a familiar concept in modal logic (see [32]). These maps preserve the structure of quantum dynamic frames in the sense of preserving all modal formulas.

Definition 3.1.21. A function $g : \Sigma_1 \to \Sigma_2$ is a *strong map between two quantum dynamic frames* $(\Sigma_i, \mathcal{L}_i, \{\xrightarrow{P?}_i\}_{P\in\mathcal{L}_i})$ $(i = 1, 2)$ if g is a bounded morphism with respect to $\to_i$, that is,

29. if $s \to_1 t$, then $g(s) \to_2 g(t)$; and

30. if $g(s) \to_2 t$, then there exists $u \in \Sigma_1$ such that $g(u) = t$ and $s \to_1 u$.

It is easy to see that identity maps are strong maps and that strong maps are composable. So quantum dynamic frames and strong maps form a category, $\mathbb{F}_s$. (It may be interesting to observe that every strong map with a nonempty domain is surjective by Proper Superposition.)

Bounded morphisms can be characterized by the $\Box$ operator as follows, a characterisation commonly found in modal logic. A proof is found, e.g., in [32] (see the proofs of Proposition 5.51 (iv) and Proposition 5.52 (iv) in [32]).

Proposition 3.1.22. *A function $g : \Sigma_1 \to \Sigma_2$ is a bounded morphism (with respect to $\to_i$) if and only if g^{-1} commutes with $\Box$, in the sense that, for all $B \subseteq \Sigma_2$, $g^{-1}\Box_2 B = \Box_1 g^{-1} B$.*

An immediate consequence is

Proposition 3.1.23. *g^{-1} of any strong map $g : \Sigma_1 \to \Sigma_2$ preserves $\sim$ (and therefore $\sqcup$ and $-[-]$ as well).*

Proof. g^{-1} preserves $\neg$ since g is a total function, and preserves $\Box$ by Proposition 3.1.22. So g^{-1} preserves $\sim\, = \Box\neg$. □

This in turn immediately shows that $\mathbb{F}_s$ is a wide subcategory of $\mathbb{F}_w$.

Proposition 3.1.24. *Every strong map $g : \Sigma_1 \to \Sigma_2$ is a weak map.*

[8] The notation $f^{-1}[-]$ disagrees with the definition that may be more standard, in which $f^{-1}[A]$ does not contain the "kernel" of f. Our $f^{-1}[A]$ contains the kernel.

Proof. If $P \in \mathcal{L}_2$, then $\sim\sim P = P$ by Lemma 3.1.17, and so Proposition 3.1.23 implies $\sim\sim g^{-1}[P] = g^{-1}[\sim\sim P] = g^{-1}[P]$, which means that $g^{-1}[P] \in \mathcal{L}_1$ by Proposition 3.1.18. □

One may wonder how much structure of quantum dynamic frames is preserved by morphisms of $\mathbb{F}_w$ or of $\mathbb{F}_s$, since the definition of $\mathbb{F}_w$-morphism does not involve $\xrightarrow{P?}$, and that of $\mathbb{F}_s$-morphism involves neither $\mathcal{L}$ nor $\xrightarrow{P?}$. The following should give some reassurance:

Proposition 3.1.25. *Given quantum dynamic frames* $(\Sigma_i, \mathcal{L}_i, \{\xrightarrow{P?}_i\}_{P\in\mathcal{L}_i})$ *for* $i = 1, 2$, *any function* $g : \Sigma_1 \to \Sigma_2$ *is an isomorphism in* $\mathbb{F}_s$, *iff* (a)–(c) *below hold, and iff* (a) *and* (d) *hold.*

(a) g *is a bijection.*

(b) For any $A \subseteq \Sigma_1$, $A \in \mathcal{L}_1$ *iff* $g[A] \in \mathcal{L}_2$.

(c) For any $s, t \in \Sigma_1$ *and* $P \in \mathcal{L}_1$, $s \xrightarrow{P?} t$ *iff* $g(s) \xrightarrow{g[P]?} g(t)$.

(d) For any $s, t \in \Sigma_1$, $s \to t$ *iff* $g(s) \to g(t)$.

Proof. For "only if" of the first "iff", take an isomorphism g of $\mathbb{F}_s$. (a) is obvious, and (b) is by Proposition 3.1.24. (c) holds because Propositions 3.1.19 and 3.1.23 (along with (a)) imply that $s \xrightarrow{P?} t$ iff $P[\{s\}] = \{t\}$ iff $g[P][\{g(s)\}] = \{g(t)\}$ iff $g(s) \xrightarrow{g[P]?} g(t)$.

"If" of the first "iff" and the second "iff" are straightforward. □

The characterization in terms of (a)–(c) makes it clear that $\mathbb{F}_s$ provides the right notion of isomorphism for $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$. In contrast, isomorphisms in $\mathbb{F}_w$ are rather too weak.[9]

In addition, functions $g : \Sigma \to \Sigma$ satisfying (a) and (d) correspond to unitary and antiunitary operators on the Hilbert space corresponding to Σ, as implied by Wigner's theorem.[10] (In fact, (a) and (d) for $g : \Sigma \to \Sigma$ define "unitaries" in [10].) This justifies our omission of unitaries from the structure of objects, since unitaries can be recovered as automorphisms.

[9] Consider the quantum dynamic frame $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ of a two-dimensional Hilbert space. $\mathcal{L}$ consists of $\varnothing$, Σ and all the singletons. This means that any arbitrary permutation on Σ, regardless of $\xrightarrow{P?}$, is an isomorphism in $\mathbb{F}_w$.

[10] For a short proof of this theorem, see Section 4 of [56]. For more about the significance of this theorem to theoretic physics, see Section 3-2 of [86].

3.2 Dualities

In this section we show the dualities between the categories of Piron lattices and those of quantum dynamic frames. In general, a *duality* between two categories $\mathbb{C}$ and $\mathbb{D}$ is a pair of contravariant functors $F : \mathbb{C}^{\mathrm{op}} \to \mathbb{D}$ and $G : \mathbb{D}^{\mathrm{op}} \to \mathbb{C}$, such that $F \circ G$ is naturally isomorphic to the identity functor $1_{\mathbb{D}}$ on $\mathbb{D}$ and $G \circ F$ is naturally isomorphic to the identity functor $1_{\mathbb{C}}$ on $\mathbb{C}$.[11] Here we first define contravariant functors between $\mathbb{F}_w$ and $\mathbb{L}_w$ and between $\mathbb{F}_s$ and $\mathbb{L}_s$, and then show that they form dualities between the corresponding pairs of categories.

3.2.1 From Piron Lattices to Quantum Dynamic Frames

In this subsection, we define a contravariant functor $F : {\mathbb{L}_w}^{\mathrm{op}} \to \mathbb{F}_w$. Its restriction to $\mathbb{L}_s$ gives another functor $F_s : {\mathbb{L}_s}^{\mathrm{op}} \to \mathbb{F}_s$; we may write F_w for F when the distinction needs emphasizing.

Mapping of Objects

Recall that, given any Piron lattice $\mathfrak{L} = (L, \leq, -^{\perp})$, we write $\mathrm{At}(\mathfrak{L})$ for its set of atoms and $[\![p]\!] = \{a \in \mathrm{At}(\mathfrak{L}) \mid a \leq p\}$ for every $p \in L$. Now define $F(\mathfrak{L})$ to be the structure $(\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P \in \mathcal{L}})$ given by

- $\Sigma = \mathrm{At}(\mathfrak{L})$;
- $\mathcal{L} = \{[\![p]\!] \subseteq \Sigma \mid p \in L\}$;
- for each $[\![p]\!] \in \mathcal{L}$, the relation $\xrightarrow{[\![p]\!]?} \subseteq \Sigma \times \Sigma$ such that, for any $a, b \in \mathrm{At}(\mathfrak{L})$, $a \xrightarrow{[\![p]\!]?} b$ iff $p[a] = b$.

Fixing an arbitrary Piron lattice $\mathfrak{L} = (L, \leq, -^{\perp})$ (for the duration of this subsubsection), we are going to show that $F(\mathfrak{L})$ actually forms a quantum dynamic frame, that is, we will verify that it satisfies the axioms (15)–(22) of a quantum dynamic frame one by one. It is useful to rewrite Lemma 3.1.3 as (31), as well as to observe (32):

31. $a \to b$ if and only if $a \not\leq b^{\perp}$, for any $a, b \in \mathrm{At}(\mathfrak{L})$.
32. Since $a \wedge a^{\perp} = O$, (7) implies $a \not\leq a^{\perp}$, and so $a \to a$ by (31).

Observe that $[\![-]\!]$ is in fact a monotone map preserving a lot of structure.

[11] Given two functors $F_1, F_2 : \mathbb{C} \to \mathbb{D}$, a natural transformation η from F_1 to F_2 is a family of morphisms $\eta_X : F_1(X) \to F_2(X)$ for all objects X of $\mathbb{C}$ such that for any morphism $f : X \to Y$ of $\mathbb{C}$, $\eta_Y \circ F_1(f) = F_2(f) \circ \eta_X$. Then η is moreover called a *natural isomorphism* if each component η_X is an isomorphism of $\mathbb{D}$.

Lemma 3.2.1. $\llbracket - \rrbracket : L \to \mathcal{P}(\Sigma)$ *is an order embedding.*

Proof. $\llbracket p \rrbracket \subseteq \llbracket q \rrbracket$ implies $p = \bigvee \llbracket p \rrbracket \leq \bigvee \llbracket q \rrbracket = q$ by Proposition 3.1.2, whereas $p \leq q$ obviously entails $\llbracket p \rrbracket \subseteq \llbracket q \rrbracket$. □

Lemma 3.2.2. $\llbracket - \rrbracket : L \to \mathcal{P}(\Sigma)$ *preserves all meets and orthocomplement.*

Proof. $\llbracket \bigwedge_{i \in I} p_i \rrbracket = \bigcap_{i \in I} \llbracket p_i \rrbracket$ because, for any $a \in \mathrm{At}(\mathfrak{L})$,

$$\begin{aligned} a \leq \bigwedge_{i \in I} p_i &\iff a \leq p_i \text{ for all } i \in I \\ &\iff a \in \llbracket p_i \rrbracket \text{ for all } i \in I \iff a \in \bigcap_{i \in I} \llbracket p_i \rrbracket. \end{aligned}$$

$\llbracket p^\perp \rrbracket = {\sim}\llbracket p \rrbracket$ because, for any $a \in \mathrm{At}(\mathfrak{L})$,

$$\begin{aligned} a \leq p^\perp &\iff \bigvee \llbracket p \rrbracket = p \leq a^\perp && \text{(by Proposition 3.1.2)} \\ &\iff b \leq a^\perp, \text{ i.e., } a \leq b^\perp, \text{ for all } b \in \llbracket p \rrbracket \\ &\iff a \not\twoheadrightarrow b \text{ for all } b \in \llbracket p \rrbracket && \text{(by (31))} \\ &\iff a \in {\sim}\llbracket p \rrbracket && \square \end{aligned}$$

Lemma 3.2.3. *$F(\mathfrak{L})$ satisfies* (15), (16), (17) *Atomicity,* (18) *Adequacy, and* (19) *Repeatability.*

Proof. (15) and (16) are by Lemma 3.2.2. Let $a, b \in \mathrm{At}(\mathfrak{L})$ and $\llbracket p \rrbracket \in \mathcal{L}$. (17): $\{a\} = \llbracket a \rrbracket \in \mathcal{L}$. (18): If $a \in \llbracket p \rrbracket$, i.e. $a \leq p$, then Weak Modularity implies $p[a] = a$, i.e., $a \xrightarrow{\llbracket p \rrbracket ?} a$. (19): If $a \xrightarrow{\llbracket p \rrbracket ?} b$, then (8) means that $b = p[a] \leq p$, i.e., $b \in \llbracket p \rrbracket$. □

Lemma 3.2.4. *$F(\mathfrak{L})$ satisfies* (20) *Self-Adjointness: Given any $a, b, c \in \mathrm{At}(\mathfrak{L})$ and $\llbracket p \rrbracket \in \mathcal{L}$, suppose $a \xrightarrow{\llbracket p \rrbracket ?} b \to c$. Then $c \xrightarrow{\llbracket p \rrbracket ?} d \to a$ for some $d \in \mathrm{At}(\mathfrak{L})$.*

Proof. $b \leq p$ and $b \not\leq c^\perp$ by Lemma 3.2.3 (19) and by (31); hence $p \not\leq c^\perp$ and so $c \not\leq p^\perp$. Hence $p[c]$ is an atom by the Covering Law. While $c \xrightarrow{\llbracket p \rrbracket ?} p[c]$ by definition, we claim $p[c] \to a$.

Suppose that $p[c] \not\to a$; Then (31) implies $p[c] \leq a^\perp$ and so $a \leq (p[c])^\perp = [p]c^\perp$. This implies, since $a \xrightarrow{\llbracket p \rrbracket ?} b$, that $b = p[a] \leq p[[p]c^\perp] \leq c^\perp$ by (3.11). So (31) implies $b \not\to c$, contradicting $b \to c$. □

Lemma 3.2.5. *$F(\mathfrak{L})$ satisfies* (21) *Covering Property: Given any $a, b, c \in \mathrm{At}(\mathfrak{L})$ and $\llbracket p \rrbracket \in \mathcal{L}$, suppose $a \xrightarrow{\llbracket p \rrbracket ?} b$, $c \neq b$ and $c \in \llbracket p \rrbracket$. Then $c \to d \not\twoheadrightarrow a$ for some $d \in \llbracket p \rrbracket$.*

Proof. Since $c \neq b$ are both atoms, $c \not\leq b$, and so $b^{\perp}[c]$ is an atom by the Covering Law. By definition, $c \xrightarrow{[\![b^{\perp}]\!]?} b^{\perp}[c]$ and so $c \to b^{\perp}[c]$. We claim $b^{\perp}[c] \in [\![p]\!]$ and $b^{\perp}[c] \leq a^{\perp}$, which implies $b^{\perp}[c] \not\to a$ by (31).

Since $b = p[a] \leq p$ by (8) and $c \leq p$ by supposition, $b^{\perp}[c] = b^{\perp} \wedge (b \vee c) \leq b \vee c \leq p$, and so $b^{\perp}[c] \in [\![p]\!]$. Also, $b^{\perp}[c] \leq b^{\perp} = (p[a])^{\perp} = [p]a^{\perp}$ by (8). Therefore $b^{\perp}[c] \leq p \wedge [p]a^{\perp} \leq a^{\perp}$ by (3.11). □

Lemma 3.2.6. *Given any $a, b \in \mathrm{At}(\mathfrak{L})$, there is a $c \in \mathrm{At}(\mathfrak{L})$ such that $a \not\leq c^{\perp}$ and $c \not\leq b^{\perp}$. So, by* (31), *$F(\mathfrak{L})$ satisfies* (22) *Proper Superposition.*

Proof. If $a \not\leq b^{\perp}$ then $c = a$ works by (32); so assume $a \leq b^{\perp}$. It follows that $a \neq b$ by (32). So, by the Superposition Principle, there is a $c \in \mathrm{At}(\mathfrak{L})$ such that $c \neq a$, $c \neq b$ and $a \vee b = a \vee c = b \vee c$. Then observe $a \not\leq c^{\perp}$, for otherwise $a \leq b^{\perp} \wedge c^{\perp} = (b \vee c)^{\perp} = (a \vee b)^{\perp} = a^{\perp} \wedge b^{\perp}$, contradicting (32). Similarly, from $b \leq a^{\perp}$ we have $b \not\leq c^{\perp}$, i.e., $c \not\leq b^{\perp}$. □

Lemmas 3.2.3 through 3.2.6 establish

Theorem 3.2.7. *$F(\mathfrak{L})$ is a quantum dynamic frame.*

Mapping of Morphisms

To define how F acts on morphisms, we start with the following observation. Given an $\mathbb{L}_w$-morphism $h : L_1 \to L_2$, since h preserves all meets, by the adjoint functor theorem there is a monotone map,

$$\ell_h : L_2 \to L_1 :: y \mapsto \bigwedge_{y \leq_2 h(x)} x,$$

that is left adjoint to h as a monotone map, $\ell_h \dashv h$, that is, for any $x \in L_1$ and $y \in L_2$, $\ell_h(y) \leq_1 x$ iff $y \leq_2 h(x)$. Moreover observe

Lemma 3.2.8. *Let $h : L_1 \to L_2$ be an $\mathbb{L}_w$-morphism. Then ℓ_h maps each atom to either an atom or O_1.*

Proof. For each $b \in \mathrm{At}(L_2)$, (13) yields $a \in \mathrm{At}(L_1)$ such that $b \leq_2 h(a)$, which by $\ell_h \dashv h$ implies $\ell_h(b) \leq_1 a$, so $\ell_h(b)$ is either an atom or O_1. □

We define $F(h) : F(L_2) \rightharpoonup F(L_1)$ for any $\mathbb{L}_w$-morphism $h : L_1 \to L_2$ to be the restriction of ℓ_h to the atoms of L_2 that ℓ_h maps to atoms of L_1.

Lemma 3.2.9. *Given any $\mathbb{L}_w$-morphism $h : L_1 \to L_2$, $F(h) : F(L_2) \rightharpoonup F(L_1)$ has $F(h)^{-1}[[\![p]\!]] = [\![h(p)]\!]$ for any $[\![p]\!] \in \mathcal{L}_1$ of $F(L_1)$.*

Proof. Lemma 3.2.8 and $\ell_h \dashv h$ imply

$$\begin{aligned} F(h)^{-1}[[\![p]\!]] &= \{b \in \mathrm{At}(L_2) \mid \text{either } \ell_h(b) = O_1 \text{ or } \ell_h(b) \in [\![p]\!]\} \\ &= \{b \in \mathrm{At}(L_2) \mid \ell_h(b) \leq_1 p\} \\ &= \{b \in \mathrm{At}(L_2) \mid b \leq_2 h(p)\} = [\![h(p)]\!]. \end{aligned}$$

□

Proposition 3.2.10. *(a) For any $\mathbb{L}_w$-morphism h, $F(h)$ is an $\mathbb{F}_w$-morphism.*

(b) F preserves identity morphisms and composition.

Proof. (a) $F(h)^{-1}[-]$ preserves testability since Lemma 3.2.9 means that, for any $[\![p]\!] \in \mathcal{L}_1$, $F(h)^{-1}[[\![p]\!]] = [\![h(p)]\!] \in \mathcal{L}_2$.

(b) For any Piron lattice L, we have $\ell_{1_L}(y) = \bigwedge_{y \leq x} x = y$, that is, $F(1_L) = 1_{F(L)}$. Given any two weak homomorphisms $h_1 : L_1 \to L_2$ and $h_2 : L_2 \to L_3$, we have $F(h_2 \circ h_1) = F(h_1) \circ F(h_2)$ because $\ell_{h_i} \dashv h_i$ implies

$$(\ell_{h_1} \circ \ell_{h_2})(y) = \bigwedge_{\ell_{h_2}(y) \leq_2 h_1(x)} x = \bigwedge_{y \leq_3 h_2 \circ h_1(x)} x = \ell_{h_2 \circ h_1}(y). \qquad \square$$

This and Theorem 3.2.7 mean that F is a contravariant functor from $\mathbb{L}_w$ to $\mathbb{F}_w$. We define another functor F_s by restricting F to $\mathbb{L}_s$. Then we have $F_s : {\mathbb{L}_s}^{\mathrm{op}} \to \mathbb{F}_s$, since F_s lands in $\mathbb{F}_s$, as in Proposition 3.2.12.

Lemma 3.2.11. *Let $k : L_1 \to L_2$ be an $\mathbb{L}_s$-morphism and suppose* $\mathrm{At}(L_2) \neq \varnothing$. *Then ℓ_k maps atoms to atoms.*

Proof. Since $p \leq k \circ \ell_k(p)$ by $\ell_k \dashv k$, $\ell_k(p) = O_1$ implies $p \leq k \circ \ell_k(p) = k(O_1) = O_2$. Thus, for any $b \in \mathrm{At}(L_2)$, $\ell_k(b) \neq O_1$, and so $\ell_k(b) \in \mathrm{At}(L_1)$ by Lemma 3.2.8. □

Proposition 3.2.12. *For any $\mathbb{L}_s$-morphism k, $F(k)$ is an $\mathbb{F}_s$-morphism.*

Proof. Given any strong homomorphism $k : L_1 \to L_2$, we prove (29) and (30) of Definition 3.1.21 for $F(k) : F(L_2) \to F(L_1)$. (29): Observe that, since k preserves $-^{\perp}$ and $\ell_k \dashv k$, any $b \in \mathrm{At}(L_2)$ has $b \leq_2 k \circ \ell_k(b) = k \circ \ell_k(b)^{\perp\perp} = k(\ell_k(b)^{\perp})^{\perp}$ and so $k(\ell_k(b)^{\perp}) \leq_2 b^{\perp}$. Hence $\ell_k(b_0) \leq_1 \ell_k(b_1)^{\perp}$ for $b_0, b_1 \in \mathrm{At}(L_2)$ implies, by $\ell_k \dashv k$, that $b_0 \leq_2 k(\ell_k(b_1)^{\perp}) \leq_2 {b_1}^{\perp}$. Thus, by (31), $b_0 \to_2 b_1$ implies $F(k)(b_0) = \ell_k(b_0) \to_1 \ell_k(b_1) = F(k)(b_1)$.

(30): Suppose $F(k)(b) \to_1 a$ for $b \in \mathrm{At}(L_2)$ and $a \in \mathrm{At}(L_1)$. Then $\ell_k(b) = F(k)(b) \not\leq_1 a^{\perp}$ by (31), and so $b \not\leq_2 k(a^{\perp}) = k(a)^{\perp}$ because $\ell_k \dashv k$ and k preserves $-^{\perp}$. Therefore, by the Covering Law, $k(a)[b] \in \mathrm{At}(L_2)$, so $b \xrightarrow{[\![k(a)[b]]\!]?}_2 k(a)[b]$ and hence $b \to_2 k(a)[b]$. Moreover, (8) implies $k(a)[b] \leq_2 k(a)$ and so $\ell_k(k(a)[b]) \leq_1 a$ by $\ell_k \dashv k$. But, because $\ell_k(k(a)[b])$ is an atom by Lemma 3.2.11, $F(k)(k(a)[b]) = \ell_k(k(a)[b]) = a$. □

3.2.2 From Quantum Dynamic Frames to Piron Lattices

In this subsection, we define a contravariant functor $G_w = G : {\mathbb{F}_w}^{\mathrm{op}} \to \mathbb{L}_w$, and obtain another $G_s : {\mathbb{F}_s}^{\mathrm{op}} \to \mathbb{L}_s$ as the restriction to $\mathbb{F}_s$.

Mapping of Objects

Given any quantum dynamic frame $\mathfrak{F} = (\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P \in \mathcal{L}})$, we define $G(\mathfrak{F})$ as $(\mathcal{L}, \subseteq, \sim)$. We will show that this $G(\mathfrak{F})$ forms a Piron lattice, that is, we will verify that it satisfies (1)–(6). In Proposition 3.1.18, we established that any $G(\mathfrak{F})$ is an ortholattice; so we carry on to show that $G(\mathfrak{F})$ satisfies the other axioms of a Piron lattice, (2)–(6). We will use the laws of ortholattice as well as the laws in Proposition 3.1.9 without particular reference.

Lemma 3.2.13. *$G(\mathfrak{F})$ satisfies* (2) *Weak Modularity: if $Q \subseteq P$ for any $Q, P \in \mathcal{L}$, then $P[Q] = Q$.*

Proof. $Q \subseteq P$ implies $Q \subseteq P[Q]$ in any ortholattice. For $P[Q] \subseteq Q$, first observe $P[Q] = P \cap \Box\neg(P \cap \Box\neg Q) \subseteq P \cap (\neg P \cup \Diamond Q) = P \cap \Diamond Q$. Fix $s \in P[Q] \subseteq P \cap \Diamond Q$; so $s \in P$, and Lemma 3.1.14 yields some $t \in Q$ with $s \xrightarrow{Q?} t$. Then $s = t \in Q$ by Lemma 3.1.16, since there is no $u \in s \sqcup t$ such that $s \to u \in {\sim}Q$, as follows. $s \in P$ and $t \in Q \subseteq P$ imply $s \sqcup t \subseteq P$, where $\sqcup$ is the join of $\mathcal{L}$. Therefore $s \in P[Q] \subseteq {\sim}P \sqcup Q = {\sim}(P \cap {\sim}Q)$ implies $(s \sqcup t) \cap {\sim}Q \subseteq P \cap {\sim}Q \subseteq {\sim}\{s\}$, that is, $(s \sqcup t) \cap \Diamond\{s\} \cap {\sim}Q = \varnothing$. □

Thus $G(\mathfrak{F})$ is an orthomodular lattice; it will be useful shortly to note that $G(\mathfrak{F})$ therefore satisfies the following consequence of (3.11):

33. $p^{\perp} \vee (p[q]) = (p \wedge [p]q^{\perp})^{\perp} = (p \wedge q^{\perp})^{\perp} = p^{\perp} \vee q$.

Lemma 3.2.14. *$G(\mathfrak{F})$ satisfies* (3) *Completeness and* (4) *Atomicity.*

Proof. (3): $\mathcal{L}$ has all meets by (15). Given any $\{P_i \in \mathcal{L}\}_{i \in I}$, ${\sim}{\sim}\bigcup_{i \in I} P_i$ is its join in $\mathcal{L}$, because, for every $Q \in \mathcal{L}$,

$$P_i \subseteq Q \text{ for all } i \in I \iff \bigcup_{i \in I} P_i \subseteq Q \iff {\sim}{\sim}\bigcup_{i \in I} P_i \subseteq Q.$$

Here "$\Leftarrow$" of the second equivalence is by $\bigcup_{i \in I} P_i \subseteq {\sim}{\sim}\bigcup_{i \in I} P_i$; "$\Rightarrow$" is because ${\sim}{\sim}$ is monotone and ${\sim}{\sim}Q = Q$. Thus $\mathcal{L}$ has all joins.

(4): By (17), singletons $\{s\} \in \mathcal{L}$ serve as atoms. □

Lemma 3.2.15. *$G(\mathfrak{F})$ satisfies* (5) *the Covering Law: if $\{s\} \not\subseteq P \in \mathcal{L}$, then $({\sim}P)[\{s\}]$ is a singleton.*

Proof. Since $s \in \neg P = \neg{\sim}{\sim}P = \Diamond{\sim}P$, Lemma 3.1.14 yields $t \in {\sim}P$ with $s \xrightarrow{{\sim}P?} t$, which implies $({\sim}P)[\{s\}] = \{t\}$ by Proposition 3.1.19. □

Lemma 3.2.16. *Suppose $s \neq t$ and $u \neq s$ for $s, t \in \Sigma$ and $u \in s \sqcup t$. Then $s \sqcup u = s \sqcup t$.*

Proof. Since $\sqcup$ is the join in $\mathcal{L}$, $s, u \in s \sqcup t$ implies $s \sqcup u \subseteq s \sqcup t$, and so

$$({\sim}\{s\})[\{u\}] = {\sim}\{s\} \cap (s \sqcup u) \subseteq {\sim}\{s\} \cap (s \sqcup t) = ({\sim}\{s\})[\{t\}].$$

Yet, by $s \neq u$ and $s \neq t$, Lemma 3.2.15 implies that both $({\sim}\{s\})[\{u\}]$ and $({\sim}\{s\})[\{t\}]$ are singletons. Therefore $({\sim}\{s\})[\{u\}] = ({\sim}\{s\})[\{t\}]$. Hence (33) implies

$$s \sqcup u = \{s\} \sqcup (({\sim}\{s\})[\{u\}]) = \{s\} \sqcup (({\sim}\{s\})[\{t\}]) = s \sqcup t. \qquad \square$$

Lemma 3.2.17. *$G(\mathfrak{F})$ satisfies* (6) *the Superposition Principle: If $s, t \in \Sigma$ are distinct, then there is a $u \in \Sigma$ distinct from s and t with $s \sqcup u = t \sqcup u = s \sqcup t$.*

Proof. By Lemma 3.2.16, it is enough to find some $u \in s \sqcup t$ distinct from s and t. We consider two cases: Case 1: $s \not\perp t$. Since $s \xrightarrow{s \sqcup t?} s \neq t \in s \sqcup t$ (by Adequacy), the Covering Property yields some $u \in s \sqcup t$ such that $u \not\to s$, which implies $u \neq s$ by $s \to s$ (Lemma 3.1.8) and $u \neq t$ by $t \to s$.

Case 2: $s \perp t$. Proper Superposition yields $v \in \Sigma$ such that $s \to v \to t$. Then $v \in \Diamond\{t\} \subseteq \Diamond(s \sqcup t)$, so Lemma 3.1.14 yields $u \in s \sqcup t$ with $v \xrightarrow{s \sqcup t?} u$. Since $s, t \in s \sqcup t$, therefore by Proposition 3.1.15 $s \to v \to t$ implies $s \to u \to t$, which means that $s \neq u \neq t$ because $s \not\to t$. $\square$

By Lemmas 3.2.13, 3.2.14, 3.2.15 and 3.2.17 as well as Proposition 3.1.18, we have

Theorem 3.2.18. *$G(\mathfrak{F})$ is a Piron lattice.*

Mapping of Morphisms

Here we define how G acts on morphisms. Given an $\mathbb{F}_w$-morphism $f : \Sigma_1 \rightharpoonup \Sigma_2$, we can define $G(f) : \mathcal{L}_2 \to \mathcal{L}_1$ as $f^{-1}[-]$ (restricted to $\mathcal{L}_2$), because f being an $\mathbb{F}_w$-morphism means that $G(f)(P) \in \mathcal{L}_1$ for all $P \in \mathcal{L}_2$. Then $G : {\mathbb{F}_w}^{\mathrm{op}} \to \mathbb{L}_w$ is a functor, by Theorem 3.2.18 and

Proposition 3.2.19. *(a) For an $\mathbb{F}_w$-morphism f, $G(f)$ is an $\mathbb{L}_w$-morphism.*

(b) G preserves identity morphisms and composition.

Proof. (a): $f^{-1}[-] : \mathcal{P}(\Sigma_2) \to \mathcal{P}(\Sigma_1)$, as a right adjoint, preserves all intersections. So $G(f)$ preserves all meets. Moore's condition holds since it amounts to the triviality that, for every $s \in \Sigma_1$, there is a $t \in \Sigma_2$ such that either $f(s)$ is undefined or else $f(s) = t$. (b) follows simply because $f \mapsto f^{-1}[-]$ is a powerset functor (from the category of partial functions). $\square$

We define a functor $G_s : {\mathbb{F}_s}^{\mathrm{op}} \to \mathbb{L}_s$ as the restriction of G to $\mathbb{F}_s$, since it lands in $\mathbb{L}_s$ by Proposition 3.1.23.

3.2.3 Natural Isomorphisms of the Functors

Now that we have described the two pairs of functors, $F : \mathbb{L}_w{}^{\mathrm{op}} \to \mathbb{F}_w$ and $G : \mathbb{F}_w{}^{\mathrm{op}} \to \mathbb{L}_w$ on the one hand and $F_s : \mathbb{F}_s{}^{\mathrm{op}} \to \mathbb{L}_s$ and $G_s : \mathbb{F}_s{}^{\mathrm{op}} \to \mathbb{L}_s$ on the other, we are ready to prove that each pair forms a duality.

For a set Σ, write $\eta_\Sigma : \Sigma \to \mathcal{P}(\Sigma) :: s \mapsto \{s\}$. Then, for any quantum dynamic frame $\mathfrak{F} = (\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$, it is straightforward to check that $FG(\mathfrak{F}) = (\Sigma', \mathcal{L}', \{\xrightarrow{Q?}\}_{Q\in\mathcal{L}'})$ consists of $\Sigma' = \eta_\Sigma[\Sigma]$, $\mathcal{L}' = \{\eta_\Sigma[P] \mid P \in \mathcal{L}\}$, and $\eta_\Sigma(s) \xrightarrow{\eta_\Sigma[P]?} \eta_\Sigma(t)$ iff $s \xrightarrow{P?} t$ (by Proposition 3.1.19). So, defining $\eta_{\mathfrak{F}} := \eta_\Sigma$, Proposition 3.1.25 implies

Lemma 3.2.20. *Each $\eta_{\mathfrak{F}} : \mathfrak{F} \to FG(\mathfrak{F})$ is an isomorphism in $\mathbb{F}_s$.*

Furthermore,

Lemma 3.2.21. *η is a natural transformation from $1_{\mathbb{F}_w}$ to $F_w \circ G_w$.*

Proof. Given an $\mathbb{F}_w$-morphism $f : \mathfrak{F}_1 \rightharpoonup \mathfrak{F}_2$, we have $G(f) = f^{-1}[-]$, and its left adjoint $\ell_{G(f)}$ has $\ell_{G(f)}(\{s\}) = \bigcap_{s\in f^{-1}[P], P\in\mathcal{L}_2} P$. If $f(s)$ is undefined, then $s \in f^{-1}[\varnothing]$ for $\varnothing \in \mathcal{L}_2$, and so $\ell_{G(f)}(\{s\}) = \varnothing$. If $f(s)$ is defined, then $s \in f^{-1}[P]$ iff $f(s) \in P$, whereas $\{f(s)\} \in \mathcal{L}_2$ by Lemma 3.2.3 (17); thus $\ell_{G(f)}(\{s\}) = \{f(s)\}$. Therefore $FG(f)(\{s\})$ is $\{f(s)\}$ if $f(s)$ is defined and otherwise undefined. This clearly makes $FG(f) \circ \eta_{\mathfrak{F}_1} = \eta_{\mathfrak{F}_2} \circ f$. □

Thus, η is a natural isomorphism both from $1_{\mathbb{F}_w}$ to $F_w \circ G_w$ and from $1_{\mathbb{F}_s}$ to $F_s \circ G_s$. On the other hand, given any Piron lattice $\mathfrak{L} = (L, \leq, -^\perp)$, write $GF(\mathfrak{L}) = (\mathcal{L}, \subseteq, \sim)$ and define $\tau_{\mathfrak{L}} : \mathfrak{L} \to GF(\mathfrak{L})$ by $[\![-]\!] : L \to \mathcal{L}$.

Lemma 3.2.22. *Each $\tau_{\mathfrak{L}} : \mathfrak{L} \to GF(\mathfrak{L})$ is an isomorphism in $\mathbb{L}_s$.*

Proof. Lemma 3.2.1 means, because $[\![-]\!]$ is onto $\mathcal{L} = \{[\![p]\!] \mid p \in L\}$, that $\tau_{\mathfrak{L}}$ is an order isomorphism; so $\tau_{\mathfrak{L}}$ satisfies (12) and (13). Also, it satisfies (14) by Proposition 3.2.2. Hence $\tau_{\mathfrak{L}}$ is an isomorphism in $\mathbb{L}_s$ and so in $\mathbb{L}_w$. □

Lemma 3.2.23. *τ is a natural transformation from $1_{\mathbb{L}_w}$ to $G_w \circ F_w$.*

Proof. Given any $h : \mathfrak{L}_1 \to \mathfrak{L}_2$, Lemma 3.2.9 implies

$$GF(h) \circ \tau_{\mathfrak{L}_1}(p) = GF(h)([\![p]\!]) = F(h)^{-1}[[\![p]\!]] = [\![h(p)]\!] = \tau_{\mathfrak{L}_2} \circ h(p).$$

□

Thus τ is a natural isomorphism both from $1_{\mathbb{L}_w}$ to $G_w \circ F_w$ and from $1_{\mathbb{L}_s}$ to $G_s \circ F_s$. Moreover, it is easy to check that $F\tau_{\mathfrak{L}} \circ \eta_{F\mathfrak{L}} :: a \ (\in \mathrm{At}(\mathfrak{L})) \mapsto \{a\} = [\![a]\!] \mapsto \bigwedge_{[\![a]\!]\subseteq[\![p]\!]} p = a$ and that $G\eta_{\mathfrak{F}} \circ \tau_{G\mathfrak{F}} :: P \ (\in \mathcal{L}) \mapsto [\![P]\!] \mapsto \eta_{\mathfrak{F}}{}^{-1}[[\![P]\!]] = \{s \in \Sigma \mid \{s\} \in [\![P]\!]\} = P$; thus $F\tau \circ \eta_F = 1_F$ and $G\eta \circ \tau_G = 1_G$. Therefore we have established

Theorem 3.2.24. *(F, G, η, τ) and (F_s, G_s, η, τ) form dualities between $\mathbb{F}_w$ and $\mathbb{L}_w$ and between $\mathbb{F}_s$ and $\mathbb{L}_s$, respectively. Moreover, $G \dashv F$ with η unit and τ counit, where we write $F : \mathbb{L}^{\mathrm{op}} \to \mathbb{F}$ and $G : \mathbb{F} \to \mathbb{L}^{\mathrm{op}}$.*

3.2.4 Mayet's Condition

The duality result we have just proven extends to certain (full) subcategories of $\mathbb{L}_w$, $\mathbb{L}_s$, $\mathbb{F}_w$ and $\mathbb{F}_s$; namely, the categories of Piron lattices and quantum dynamic frames that satisfy the property called *Mayet's condition* [80]. As mentioned in the introduction, this condition added to a Piron lattice captures the structure of an infinite dimensional Hilbert space over the complex numbers, reals, or quaternions.

Definition 3.2.25. By a *strong automorphism*, let us mean an isomorphism, either of $\mathbb{L}_s$ or of $\mathbb{F}_s$, on the same object. A Piron lattice $\mathfrak{L} = (L, \leq, -^{\perp})$ is said to satisfy Mayet's condition if there is a strong automorphism $k : L \to L$ such that

34. there is a $p \in L$ such that $k(p) < p$, and

35. there is a $q \in L$ such that there are at least two distinct atoms below q and $k(r) = r$ for all $r \leq q$.

A quantum dynamic frame $\mathfrak{F} = (\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ is said to satisfy Mayet's condition if there is a strong automorphism $g : \Sigma \to \Sigma$ such that

36. there is a $P \in \mathcal{L}$ such that $g^{-1}[P] \subset P$, and

37. there is a $Q \in \mathcal{L}$ that has at least two distinct elements and such that $g(s) = s$ for all $s \in Q$.

Using this condition let us define a full subcategory $\mathbb{L}_w^M$ (respectively, $\mathbb{L}_s^M$, $\mathbb{F}_w^M$ or $\mathbb{F}_s^M$) of $\mathbb{L}_w$ (respectively, $\mathbb{L}_s$, $\mathbb{F}_w$ or $\mathbb{F}_s$); that is, the objects of $\mathbb{L}_w^M$ are the objects of $\mathbb{L}_w$ satisfying Mayet's condition, whereas any pair of objects $\mathfrak{L}_1$, $\mathfrak{L}_2$ of $\mathbb{L}_w^M$ has the same set of morphisms as it has in $\mathbb{L}_w$. Then $\mathbb{L}_w^M$ and $\mathbb{L}_s^M$ are dual to $\mathbb{F}_w^M$ and to $\mathbb{F}_s^M$, respectively, which follows from

Proposition 3.2.26. *A Piron lattice $\mathfrak{L}$ satisfies Mayet's condition iff $F(\mathfrak{L})$ satisfies Mayet's condition. A quantum dynamic frame $\mathfrak{F}$ satisfies Mayet's condition iff $G(\mathfrak{F})$ satisfies Mayet's condition.*

Proof. We first show the two "only if" parts. Suppose $\mathfrak{L} = (L, \leq, -^{\perp})$ satisfies Mayet's condition and let $k : L \to L$ be a strong automorphism that satisfies (34) and (35). While $F(k)$ is a strong automorphism, it satisfies (36) and (37) as follows. We have $p, q \in L$ as in (34) and (35). Then $F(k)^{-1}[[\![p]\!]] = [\![k(p)]\!] \subset [\![p]\!]$ by Lemmas 3.2.9 and 3.2.1. By (35), $[\![q]\!]$ has at least two elements; also each $s \in [\![q]\!]$ has $s = k(s)$, which implies by $\ell_k \dashv k$ that $\ell_k(s) \leq s$ and so $F(k)(s) = \ell_k(s) = s$ by Lemma 3.2.11.

Suppose $\mathfrak{F} = (\Sigma, \mathcal{L}, \{\xrightarrow{P?}\}_{P\in\mathcal{L}})$ satisfies Mayet's condition and let $g : \Sigma \to \Sigma$ be a strong automorphism that satisfies (36) and (37). While $G(g)$ is a strong automorphism, it satisfies (34) and (35) as follows. (36) means that there is a $P \in \mathcal{L}$ such that $G(g)(P) = g^{-1}[P] \subset P$. We have Q as in (37); then it contains two dinstinct singletons, and $R \subseteq Q$ implies $G(g)(R) = g^{-1}(R) = R$ since g restricted to Q is the identity.

Now the "if" parts follow from the "only if" parts because Mayet's condition is stable under isomorphisms in $\mathbb{L}_s$ and in $\mathbb{F}_s$. For the first "if", for instance, if $F(\mathfrak{L})$ satisfies Mayet's condition, then by the second "only if" $GF(\mathfrak{L})$ satisfies it as well, and so does $\mathfrak{L}$. □

It immediately follows from this fact that the functors F_w, G_w, F_s, and G_s restrict to the subcategories $\mathbb{L}_w^M$, $\mathbb{L}_s^M$, $\mathbb{F}_w^M$ and $\mathbb{F}_s^M$, and moreover, by Theorem 3.2.24 (and the fullness of these subcategories),

Theorem 3.2.27. *The pair (F_w^M, G_w^M) forms a duality between $\mathbb{F}_w^M$ and $\mathbb{L}_w^M$ and the pair (F_s^M, G_s^M) forms a duality between $\mathbb{F}_s^M$ and $\mathbb{L}_s^M$.*

Chapter 4

Completeness of a quantum hybrid logic

Summary: In this chapter we introduce a quantum hybrid logic, which is shown to be sound and complete with respect to finite dimensional quantum models, i.e. quantum Kripke models of dimension at most n for a fixed $n \in \mathbb{N}$. While the syntax of our logical system is equivalent to standard hybrid logic, the deductive system is extended with quantum axioms that capture the properties of a quantum Kripke model.

Background: In this chapter we will introduce a sound and complete axiomatisation for quantum Kripke frames (Definition 2.2.15), which were introduced by Shengyang Zhong in [107]. In the same publication Zhong showed that these quantum Kripke frames are equivalent to quantum dynamic frames (Definition 2.2.14), introduced by Smets and Baltag (Chapter 2.2.3). In Chapter 3 we have shown in Theorem 3.2.24 that quantum dynamic frames, and therefore quantum Kripke frames, are dual to Píron lattices (Definition 2.2.3). By Theorem 2.2.4, this means that each quantum Kripke frame is realisable by a generalized Hilbert space. This validates our claim that the language introduced in this chapter is a quantum logic.

One key difference with the framework presented in this chapter and the frameworks from previous work is that we only consider finite structures. In the research area that deals with quantum information and quantum computation we normally only work with Hilbert spaces of finite dimension. For a fixed dimension $n \in \mathbb{N}$, all complex Hilbert spaces of dimension n are equivalent to the Hilbert space $\mathbb{C}^n$. In fact, we normally only consider qubits, that is, vectors in the complex vector space $\mathbb{C}^2$ of dimension 2. If we have N qubits, this becomes a vector in the tensor product $\bigotimes_N \mathbb{C}^2$. For many practical purposes, the limitation to focus only on finite dimensional frames is acceptable.

The language introduced in this chapter is based on hybrid logic (Chapter 2.2.3). Our completeness result heavily depends on a previously obtained completeness results in Hybrid logic,which is described in more detail in Chapter 2.2.3. In this chapter we extend the normal hybrid logic with several axioms. Most of these axioms are pure formulas, that is, they only contain nominals as their atoms. By Theorem 2.2.13, this new language will then be sound and complete with respect to all frames validating the new pure axioms.

The chapter is organised as follows. In Section 4.1, we discuss the syntax and semantics of a quantum hybrid logic and an equivalent definition of a (finite dimensional) quantum Kripke frame. In Section 4.2, we show that our quantum hybrid logic can express the dynamic operators of the logic of quantum actions (see Chapter 2.2.3) and as a consequence is as expressive as the logic of quantum actions. In Section 4.3, we introduce the deductive system and show completeness.

4.1 Quantum hybrid logic

4.1.1 Syntax

Let Prop, Nom and Var be three countable and pairwise disjoint sets of proposition letters. The set of all hybrid formulas is given by

$$\phi ::= p \mid i \mid x \mid \neg\phi \mid \phi \wedge \phi \mid \Box\phi \mid @_k\phi \mid {\downarrow}x.\phi,$$

where $p \in \mathsf{Prop}$, $i \in \mathsf{Nom}$, $x \in \mathsf{Var}$ and $k \in \mathsf{Nom} \cup \mathsf{Var}$. A formula ϕ is called *closed* if for all $x \in \mathsf{Var}$ all occurrences of x in ϕ only appear under the scope of a down arrow ${\downarrow}x.(\cdot)$. The "Quantum" Hybrid Language ($\mathcal{QHL}$) is the collection of all closed formulas.

4.1.2 Frame and model

Given a set of states S and a (non-orthogonality) relation $\not\perp \subseteq S \times S$, we write $s \not\perp t$ instead of $(s,t) \in \not\perp$ and $s \perp t$ otherwise. For any $P \subseteq S$ we write ${\sim}P$ for the set $\{s \in S \mid s \perp t \text{ for all } t \in P\}$. With $\mathcal{T}$ we denote the set of testable properties, that is $\mathcal{T} = \{P \subseteq S \mid P = {\sim}{\sim}P\}$.

Definition 4.1.1 (Quantum Kripke Model of finite dimension)**.** Let n be a positive integer. A *Quantum Kripke Frame of dimension at most* n (QKF$_n$) $\mathcal{F}$ is a pair $(S, \not\perp)$ consisting of a set of states S and a non-orthogonality relation $\not\perp \subseteq S \times S$ such that:

1. $s = t$ iff $s \not\perp u$ implies $u \not\perp t$ for all $u \in S$, *(separation)*

2. for all $s, t \in S$ there exists a $u \in S$ such that $s \not\perp u \not\perp t$. *(superposition)*

3. for every multi-subset $\{s_1, \cdots s_{n+1}\} \subseteq S$ of $n+1$ (possibly non-distinct) states we have $s_i \not\perp s_j$ for some $i \neq j$, *(maximum basis)*

4. for every finite $P \subseteq_\omega S$ and $s \in S \setminus {\sim}P$ there exists a $t \in {\sim}{\sim}P$ such that $s \not\perp u$ iff $t \not\perp u$ for all $u \in {\sim}{\sim}P$, *(finite cover law)*

A *Quantum Kripke Model of dimension at most* n (QKM$_n$) is a pair $\mathfrak{M} = (\mathcal{F}, V)$ consisting of a QKF$_n$ $\mathcal{F}$ and a valuation $V : \mathsf{Prop} \cup \mathsf{Nom} \cup \mathsf{Var} \to \mathcal{P}(S)$ such that $|V(i)| = 1$ for all $i \in \mathsf{Nom}$.

For the remainder of this section let us fix a positive integer n. Given a quantum Kripke model $\mathfrak{M}$ of dimension at most n (QKM$_n$), we say a state $s \in S$ is *named* by $i \in \mathsf{Nom}$ if $V(i) = \{s\}$. We say the model $\mathfrak{M}$ is *named* if all states $s \in S$ are named.

We will now prove certain properties of quantum Kripke models of dimension at most n. Our definition of a QKF$_n$ differs from Zhong's original definition (Definition 2.2.15) in several ways: We have combined the two conditions "symmetry" and "separation" into one separation condition. His "existence of approximation" condition is restated as the "cover law" and "reflexivity" follows from our new condition "maximum basis". However, aside from the finite dimension these two definitions are equivalent. The following lemma shows a QKF$_n$ is reflexive, symmetric and separated.

Lemma 4.1.2. *Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n (QKF$_n$). Then $\not\perp$ is reflexive, symmetric and separated, that is:*

1. *$s \not\perp s$ for all $s \in S$,* *(reflexivity)*
2. *$s \not\perp t$ iff $t \not\perp s$ for all $s, t \in S$,* *(symmetry)*
3. *$s \neq t$ iff $s \not\perp u$ and $u \perp t$ for some $u \in S$,* *(alternative separation)*

Proof. Note that the alternative separation in this lemma is simply the contrapositive of separation (Definition 4.1.1-1).

To show reflexivity, take any $s \in S$ and let $\{s_1, \ldots, s_{n+1}\} \subseteq S$ be the multisubset where $s_i = s$ for every $1 \leq i \leq n + 1$. Then by *maximum basis* (Definition 4.1.1-3) we have $s_i \not\perp s_j$ for some $i \neq j$, but in this case this means $s \not\perp s$.

To show symmetry, take any $s, t \in S$. We have $s = s$, so by separation (Definition 4.1.1-1), we have $s \not\perp u$ implies $u \not\perp s$ for all $u \in S$, so in particular we get $s \not\perp t$ implies $t \not\perp s$. Similarly, from $t = t$ we get $t \not\perp s$ implies $s \not\perp t$, so we get $s \not\perp t$ iff $t \not\perp s$. □

The following lemma collects some properties of the orthocomplement.

Lemma 4.1.3. *Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n (QKF$_n$). The following statements hold.*

1. *If $P \subseteq Q$, then ${\sim}Q \subseteq {\sim}P$.*

2. *$P \subseteq {\sim}{\sim}P$ for all $P \subseteq S$.*

3. *${\sim}P = {\sim}{\sim}{\sim}P$ for all $P \subseteq S$.*

Proof. 1. Suppose $P \subseteq Q$ and suppose $s \in {\sim}Q$. Then $s \perp t$ for all $t \in Q$. Since $P \subseteq Q$ this implies $s \perp t$ for all $t \in P$ and therefore $s \in {\sim}P$.

2. For all $t \in {\sim}P$ we have $t \perp s$ for all $s \in P$. Therefore, by symmetry (Lemma 4.1.2-2), for any $s \in P$ we have $s \perp t$ for all $t \in {\sim}P$ and so $s \in {\sim}{\sim}P$ for all $s \in P$.

3. By Lemma 4.1.3-2 we already have ${\sim}P \subseteq {\sim}{\sim}{\sim}P$. Moreover, by Lemma 4.1.3-2 we also know $P \subseteq {\sim}{\sim}P$, which by Lemma 4.1.3-1 implies ${\sim}{\sim}{\sim}P \subseteq {\sim}P$.

□

The orthocomplement can be regarded as a negation in quantum structures. We introduce the quantum join $\sqcup$ as the dual of $\cap$ with respect to $\sim$, that is, $(P \sqcup Q) := {\sim}({\sim}P \cap {\sim}Q)$ for all subsets $P, Q \subseteq S$, where S is the set of states. The following lemma collects some properties of the quantum join.

Lemma 4.1.4. *Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n (QKF_n). The following statements hold.*

1. *$P \sqcup Q = {\sim}{\sim}(P \cup Q)$ for all $P, Q \subseteq S$.*

2. *$P \subseteq P \sqcup Q$ for all $P, Q \subseteq S$.*

3. *If $P, Q \subseteq R$, then $P \sqcup Q \subseteq {\sim}{\sim}R$.*

Proof. 1. For this statement it is enough to show ${\sim}(P \cup Q) = ({\sim}P \cap {\sim}Q)$. From $P \subseteq (P \cup Q)$ we get ${\sim}(P \cup Q) \subseteq {\sim}P$ by Lemma 4.1.3-1. Similar we get ${\sim}(P \cup Q) \subseteq {\sim}Q$, and therefore ${\sim}(P \cup Q) \subseteq ({\sim}P \cap {\sim}Q)$.

For the other direction, suppose $s \in ({\sim}P \cap {\sim}Q)$, then $s \perp t$ for all $t \in P$ and $s \perp t$ for all $t \in Q$. Therefore $s \perp t$ for all $t \in (P \cup Q)$, which by definition means $s \in {\sim}(P \cup Q)$.

2. $P \subseteq (P \cup Q)$, so by Lemma 4.1.3-2 we have $P \subseteq {\sim}{\sim}P$ and by applying Lemma 4.1.3-1 twice we get ${\sim}{\sim}P \subseteq {\sim}{\sim}(P \cup Q)$, so by transitivity $P \subseteq {\sim}{\sim}(P \cup Q)$. By Lemma 4.1.4-1 we have ${\sim}{\sim}(P \cup Q) = (P \sqcup Q)$, and therefore $P \subseteq (P \sqcup Q)$.

3. Suppose $P, Q \subseteq R$, then $(P \cup Q) \subseteq R$. Therefore by Lemma 4.1.3-1 we have ${\sim}{\sim}(P \cup Q) \subseteq {\sim}{\sim}R$, which by Lemma 4.1.4-1 implies $(P \sqcup Q) \subseteq {\sim}{\sim}R$.

□

The following lemma establishes that each subset of the set of states $P \subseteq S$ has a finite basis for its orthocomplement closure $\sim\sim P$.

Lemma 4.1.5. *Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n (QKF$_n$). For every (non-empty) subset $P \subseteq S$ there exists a finite subset $P_\omega \subseteq S$ such that $\sim\sim P_\omega = \sim\sim P$.*

Proof. If P is the empty set, the statement is trivial. Suppose P is non-empty. We will construct P_ω inductively with at most n steps. Let P_ω^0 be the empty set. For the inductive step, suppose P_ω^m is defined such that P_ω^m has m states, which are pairwise orthogonal, that is, $s \perp t$ for all $s, t \in P_\omega^m$. We now consider the following two cases.

- Suppose $(\sim P_\omega^m \cap \sim\sim P) \neq \emptyset$. Take any $s \in (\sim P_\omega^m \cap \sim\sim P)$ and let $P_\omega^{m+1} = (P_\omega^m \cup \{s\})$.
- Suppose $(\sim P_\omega^m \cap \sim\sim P) = \emptyset$, the construction terminates and we let $P_\omega = P_\omega^m$.

Note that by construction and by symmetry (Lemma 4.1.2-2) each set P_ω^m indeed consists of m states that are pairwise orthogonal. Therefore by maximum basis (Definition 4.1.1-3) P_ω^{n+1} cannot exist and the construction must terminate after at most n steps.

We claim $\sim\sim P_\omega = \sim\sim P$. Suppose not, then there exists an $s \in \sim\sim P$ such that $s \notin \sim\sim P_\omega$. Therefore there exists a $t \in \sim P_\omega$ such that $s \not\perp t$, so $t \in S \setminus \sim(P_\omega \cup \{s\})$. By the finite cover law (Definition 4.1.1-4) there exists a $u \in \sim\sim(P_\omega \cup \{s\})$ such that $t \perp v$ iff $u \perp v$ for all $v \in \sim\sim(P_\omega \cup \{s\})$. As $\sim\sim P_\omega \subseteq \sim\sim(P_\omega \cup \{s\})$ and $t \in \sim P_\omega$, we know $u \perp v$ for all $v \in P_\omega$. As $\sim\sim(P_\omega \cup \{s\}) \subseteq \sim\sim P$ we know $u \in \sim\sim P$. Therefore $u \in (\sim P_\omega \cap \sim\sim P) \neq \emptyset$, which contradicts the construction of P_ω. □

Corollary 4.1.6. *Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n (QKF$_n$). Then $\mathcal{F}$ satisfies the infinite cover law, which is:*

6. *for every $P \subseteq S$ and $s \in S \setminus \sim P$ there exists a $t \in \sim\sim P$ such that $s \not\perp u$ iff $t \not\perp u$ for all $u \in \sim\sim P$,* *(infinite cover law)*

4.1.3 Semantics

Definition 4.1.7. Given a Quantum Kripke Model $\mathfrak{M} = (S, \not\perp, V)$ of dimension at most n (QKM$_n$), we inductively define for $p \in \mathsf{Prop}$, $i \in \mathsf{Nom}$ and $x \in \mathsf{Var}$

- $\mathfrak{M}, s \vDash p$ iff $s \in V(p)$,
- $\mathfrak{M}, s \vDash i$ iff $V(i) = \{s\}$,
- $\mathfrak{M}, s \vDash x$ iff $V(x) = \{s\}$,

- $\mathfrak{M}, s \vDash \neg\phi$ iff $\mathfrak{M}, s \nvDash \phi$,
- $\mathfrak{M}, s \vDash \phi \wedge \psi$ iff $\mathfrak{M}, s \vDash \phi$ and $\mathfrak{M}, s \vDash \psi$,
- $\mathfrak{M}, s \vDash \Box\phi$ iff for all $t \in S$ if $s \not\perp t$ then $\mathfrak{M}, t \vDash \phi$,
- $\mathfrak{M}, s \vDash @_k\phi$ iff $\mathfrak{M}, t \vDash \phi$, where $V(k) = \{t\}$, and
- $\mathfrak{M}, s \vDash \downarrow x.\phi$ iff $\mathfrak{M}[V(x) := \{s\}], s \vDash \phi$, where $\mathfrak{M}[V(x) := \{s\}]$ is the model obtained by extending the valuation V of $\mathfrak{M}$ by putting $V(x) := \{s\}$.

We write $\llbracket\phi\rrbracket := \{s \in S \mid \mathfrak{M}, s \vDash \phi\}$. Moreover, we write $\mathfrak{M} \vDash \phi$ iff $\mathfrak{M}, s \vDash \phi$ for all $s \in S$, and for a QKF$_n$ $\mathcal{F} = (S, \not\perp)$, we write $\mathcal{F} \vDash \phi$ iff $\mathfrak{M} = (S, \not\perp, V) \vDash \phi$ for every valuation V on $\mathcal{F}$.

Lemma 4.1.8. *Given a Quantum Kripke Model $\mathfrak{M} = (S, \not\perp, V)$ of dimension at most n (QKF$_n$), for all ϕ we have $\llbracket\Box\neg\phi\rrbracket = {\sim}\llbracket\phi\rrbracket$, and as a consequence $\llbracket\Box\Diamond\phi\rrbracket = {\sim}{\sim}\llbracket\phi\rrbracket$.*

Proof. Suppose $s \in \llbracket\Box\neg\phi\rrbracket$. Then by definition for every $t \in S$ such that $s \not\perp t$ we have $t \in \llbracket\neg\phi\rrbracket$, which is equivalent to $t \notin \llbracket\phi\rrbracket$. Therefore $s \perp t$ for all $t \in \llbracket\phi\rrbracket$, which by definition means $s \in {\sim}\llbracket\phi\rrbracket$. Similarly, if $s \in {\sim}\llbracket\phi\rrbracket$, then $s \in \llbracket\Box\neg\phi\rrbracket$. □

4.2 Dynamic operators

In this section we will show $\mathcal{QHL}$ can express dynamic operators similar to tests as can be found in the logic for quantum actions [10].

Let $\mathcal{F} = (S, \not\perp)$ be a quantum Kripke frame of dimension at most n. Let $\mathcal{T} := \{P \subseteq S \mid {\sim}{\sim}P = P\}$ be the set of testable properties. We define a new relation R_P for each $P \in \mathcal{T}$ in the following way.

$$R_P := \{(s,t) \in \not\perp \mid t \in P \text{ and } s \not\perp u \text{ iff } t \not\perp u \text{ for all } u \in P\}.$$

These relations R_P correspond to the projectors onto subspaces P in Hilbert spaces. Therefore these relations must be partial functions.

Lemma 4.2.1. *The relation R_P is a partial function for each $P \in \mathcal{T}$.*

Proof. Let $P \in \mathcal{T}$ and suppose towards a contradiction $(s,t) \in R_P$ and $(s,t') \in R_P$ for some $t \neq t'$. By *separation*, there is a $u \in S$ such that $t \not\perp u$ and $t' \perp u$. By definition of R_P, both $t \in P$ and $t' \in P$. Therefore $u \in S \setminus {\sim}P$. By Corollary 4.1.6, there exists a $v \in P$ such that $v \not\perp w$ iff $u \not\perp w$ for all $w \in P$. Thus we have $v \not\perp t$ and $v \perp t'$. By definition of R_P we have $s \not\perp v$ and $s \perp v$, a contradiction. □

Rules	
MP	$\vdash \phi \to \psi, \vdash \phi \implies \vdash \psi$
Subst	$\vdash \phi \implies \vdash \phi^\sigma$
Gen$_@$	$\vdash \phi \implies \vdash @_i\phi$
Gen$_\Box$	$\vdash \phi \implies \vdash \Box\phi$
Name	$\vdash i \to \phi \implies \vdash \phi$ if i does not occur in ϕ
Paste	$\vdash @_i\Diamond j \land @_j\phi \implies \vdash @_i\Diamond\phi$ if $i \neq j$ and j does not occur in ϕ

Figure 4.1: Rules of $\mathcal{QHL}(@,\downarrow)$.

We introduce a new abbreviation for a dynamic operator.

$$\langle\phi?\rangle\psi := \downarrow x.\Diamond\downarrow y.(\psi \land \Box\Diamond\phi \land \Box(\Box\Diamond\phi \to \Diamond x) \land @_x\Box(\Box\Diamond\phi \to \Diamond y))$$

In the following lemma we show that the semantics of $\langle p?\rangle q$ is connected to the relations R_P with $P \in \mathcal{T}$.

Lemma 4.2.2. *Let $\mathfrak{M} = (S, \not\perp, V)$ be a quantum Kripke model of dimension at most n. Then we have*

$$\mathfrak{M}, s \vDash \langle\phi?\rangle\psi \textit{ iff } (s,t) \in R_P \textit{ for some } t \in S \textit{ and } \mathfrak{M}, t \vDash \psi, \textit{ where } P = \sim\sim[\![\phi]\!].$$

Proof. Suppose $\mathfrak{M}, s \vDash \langle\phi?\rangle\psi$. Then there exists a $t \in S$ such that $s \not\perp t$ and $\mathfrak{M}, t \vDash \psi$ and

$$\mathfrak{M}[V(x) = \{s\}, V(y) = \{t\}], t \vDash \Box\Diamond\phi \land \Box(\Box\Diamond\phi \to \Diamond x) \land @_x\Box(\Box\Diamond\phi \to \Diamond y),$$

that is, if we let $P = \sim\sim[\![\phi]\!]$, then $t \in P$ and $t \not\perp u$ iff $s \not\perp u$ for all $u \in P$, or in other words, $(s,t) \in R_P$.

Suppose there exists a $t \in S$ such that $(s,t) \in R_P$ and $\mathfrak{M}, t \vDash \psi$, where $P = \sim\sim[\![\phi]\!]$. Then by definition of R_P we have

$$\mathfrak{M}[V(x) = \{s\}, V(y) = \{t\}], t \vDash \Box\Diamond\phi \land \Box(\Box\Diamond\phi \to \Diamond x) \land @_x\Box(\Box\Diamond\phi \to \Diamond y).$$

In other words, $\mathfrak{M}, s \vDash \langle\phi?\rangle\psi$. □

4.3 Complete deductive system

4.3.1 Deductive system

We have all rules (Figure 4.1) and axioms (Figure 4.2) of $\mathcal{HL}(@,\downarrow)$ as can be found in the first axiomatisation of [31, Section 5, Figure 3] (Blackburn et. al. "Pure Extensions, Proof Rules, and Hybrid Axiomatics"). Moreover, we have four axioms to characterise each of the four properties of a quantum Kripke frame of

Axioms	
CT	All classical tautologies
$K_\Box$	$\vdash \Box(p \to q) \to \Box p \to \Box q$
$K_@$	$\vdash @_i(p \to q) \to @_i p \to @_i q$
Selfdual$_@$	$\vdash @_i p \leftrightarrow \neg @_i \neg p$
Ref$_@$	$\vdash @_i i$
Agree	$\vdash @_i @_j p \leftrightarrow @_j p$
Intro	$\vdash i \to (p \leftrightarrow @_i p)$
DA	$\vdash @_i(\downarrow x.\phi \leftrightarrow \phi[x := i])$

Figure 4.2: Standard axioms of $\mathcal{QHL}$.

Axioms for quantum Kripke frames	
Separation	$\vdash i \leftrightarrow \Box\Diamond i$
Superposition	$\vdash \Diamond\Diamond i$
Maximum basis	$\vdash \bigvee_{1 \leq i \neq j \leq n+1} @_i \Diamond j$
Cover law	$\vdash @_i \Diamond p \to @_i \Diamond \downarrow x. \left(\begin{array}{r} \Box\Diamond p \wedge \Box(\Box\Diamond p \to \Diamond i) \\ \wedge\ @_i \Box(\Box\Diamond p \to \Diamond x) \end{array} \right)$

Figure 4.3: Axioms for finite quantum Kripke frames.

dimension at most n (Figure 4.3). We refer to this deductive system as $\mathcal{QHL}_n$ (finite quantum hybrid logic).

Some properties of QKF_n are defined by some of the axioms in Figure 4.3. Let us recall the definition of *frame definability.*

Definition 4.3.1 (Frame definability)**.** A modal fromula ϕ *defines* (or *characterises*) a class of frames $\mathcal{K}$, if for all frames $\mathcal{F}$, $\mathcal{F}$ is in $\mathcal{K}$ iff $\mathcal{F} \vDash \phi$.

The following lemma establishes that the first three axioms in Figure 4.3 characterise the first three properties of a quantum Kripke frame of dimension at most n in Definition 4.1.1.

Lemma 4.3.2. *The axioms Separation, Superposition and Maximum basis characterise their corresponding properties from Definition 4.1.1.*

Proof. For Separation ($\vdash i \leftrightarrow \Box\Diamond i$), suppose $\mathcal{F} = (S, \not\perp)$ satisfies *separation*, so $s = t$ iff $s \not\perp u$ implies $u \not\perp t$ for all $u \in S$. Let V be some valuation on $\mathcal{F}$ and let $\mathfrak{M} = (S, \not\perp, V)$. Suppose $\mathfrak{M}, s \vDash i$. As we have $s = s$, we have $s \not\perp u$ implies $u \not\perp s$ for all $u \in S$, so we have $\mathfrak{M}, s \vDash \Box\Diamond i$ as required.

Suppose $\mathfrak{M}, s \vDash \Box\Diamond i$. Then $\mathfrak{M}, u \vDash \Diamond i$ for all $s \not\perp u$. As $V(i) = \{t\}$ for some $t \in S$, we have $u \not\perp t$ for all $s \not\perp u$, so we have $s = t$ and therefore $\mathfrak{M}, s \vDash i$. In conclusion, if $\mathcal{F}$ satisfies separation, then $\mathcal{F} \vDash i \leftrightarrow \Box\Diamond i$.

Now suppose $\mathcal{F} \vDash i \leftrightarrow \Box\Diamond i$. Suppose for some $s, t \in S$ we have $s = t$. Let V be any valuation on $\mathcal{F}$ such that $V(i) = \{s\} = \{t\}$ and let $\mathfrak{M} = (S, \not\perp, V)$. Then $\mathfrak{M}, s \vDash i$ and therefore $\mathfrak{M}, s \vDash \Box\Diamond i$. Thus for every $s \not\perp u$ we have $\mathfrak{M}, u \vDash \Diamond i$. Since $V(i) = \{t\}$, we have $s \not\perp u$ implies $u \not\perp t$ as required.

Suppose for some $s, t \in S$ we have $s \not\perp u$ implies $u \not\perp t$ for all $u \in S$. Let V be any valuation on $\mathcal{F}$ such that $V(i) = \{t\}$ and let $\mathfrak{M} = (S, \not\perp, V)$. Then we have $\mathfrak{M}, s \vDash \Box\Diamond i$. Therefore we have $\mathfrak{M}, s \vDash i$, which implies $V(i) = \{s\}$. But this implies $s = t$ as required. In conclusion, $\mathcal{F} \vDash i \leftrightarrow \Box\Diamond i$ implies $\mathcal{F}$ satisfies separation.

For Superposition ($\Diamond\Diamond i$), suppose $\mathcal{F} = (S, \not\perp)$ satisfies *superposition*, so for every $s, t \in S$ there exists a $u \in S$ such that $s \not\perp u$ and $u \not\perp t$. Let V be any valuation for $\mathcal{F}$. We know $V(i) = \{t\}$ for some $t \in S$. For any $s \in S$ there exists a $u \in S$ such that $s \not\perp u$ and $u \not\perp t$. So $\mathcal{F}, V, u \vDash \Diamond i$ and $\mathcal{F}, V, s \vDash \Diamond\Diamond i$. Because $s \in S$ was an arbitrary state, we get $\mathcal{F}, V \vDash \Diamond\Diamond i$.

Suppose for some $\mathcal{F} = (S, \not\perp)$ there are s, t such that there exists no $u \in S$ such that $s \not\perp u$ and $u \not\perp t$. Let V be such that $V(i) = \{t\}$. Then we have $\mathcal{F}, V, s \vDash \neg\Diamond\Diamond i$.

For Maximum basis ($\vdash \bigvee_{1 \leq i \neq j \leq n+1} @_i\Diamond j$), suppose $\mathcal{F} = (S, \not\perp)$ satisfies *maximum basis*, so for every multi-subset $X \subseteq S$ of $n + 1$ (possibly non-distinct) states there exists $s \neq t \in X$ such that $s \not\perp t$. For some valuation V on $\mathcal{F}$ let $I \subseteq \mathsf{Nom}$ be any set of $n + 1$ nominals and let us define the multi-subset $X = \{s_i \mid i \in I \text{ and } V(i) = \{s\}$. By *maximum basis* there are $i \neq j \in I$ such that $s_i \not\perp s_j$ and therefore $\mathcal{F}, V, s_i \vDash \Diamond j$ and by definition of $@_i\phi$ we have $\mathcal{F}, V \vDash @_i\Diamond j$. By propositional reasoning we get $\mathcal{F}, V \vDash \bigvee_{i \neq j \in I} @_i\Diamond j$.

Suppose for some $\mathcal{F} = (S, \not\perp)$ there is a multi-subset $\{s_1, \ldots, s_{n+1}\} \subseteq S$ such that $s_i \perp s_j$ for all $i \neq j$. Let $I \subseteq \mathsf{Nom}$ be a subset of $n + 1$ nominals and let V be a valuation such that $V(i) = s_i$ for all $i \in I$. Then we have $\mathcal{F}, V, s_i \vDash \neg\Diamond j$ for all $i \neq j \in I$. Therefore we have $\mathcal{F}, V \vDash \bigwedge_{i \neq j \in I} \neg @_i\Diamond j$, which is equivalent to $\mathcal{F}, V \vDash \neg \bigvee_{i \neq j \in I} @_i\Diamond j$. □

The following theorem establishes all rules and axioms are sound with respect to quantum Kripke frames of dimension at most n.

Theorem 4.3.3 (Soundness). *The rules in Figure 4.1 and the axioms in Figure 4.2 and Figure 4.3 are sound with respect to the class of all quantum Kripke frames of dimension at most n (QKF$_n$).*

Proof. The rules in Figure 4.1 and the axioms in Figure 4.2 are standard hybrid logic rules and axioms and are sound with respect to every class of hybrid logic frames. The soundness of the axioms Separation, Superposition and Maximum basis from Figure 4.3 are established in Lemma 4.3.2. What is left to show is the soundness of the axiom Cover law.

Let $\mathfrak{M} = (S, \not\perp, V)$ be a quantum Kripke model of dimension at most n and suppose $\mathfrak{M}, s \vDash @_i\Diamond p$. Without loss of generality, assume $V(i) = \{s\}$, so $\mathfrak{M}, s \vDash$

$\Diamond p$. Let $P = [\![p]\!]$, then there exists a $t \in P$ such that $s \not\perp t$, which is equivalent to $s \in S \setminus {\sim}P$. By Corollary 4.1.6, there exists a $u \in {\sim\sim}P$ such that $s \not\perp v$ iff $u \not\perp v$ for all $v \in {\sim\sim}P$. As $u \in {\sim\sim}P$ and $u \not\perp u$ by Lemma 4.1.2-1 we have $s \not\perp u$. By Lemma 4.1.8 we have $[\![\Box\Diamond p]\!] = {\sim\sim}P$, so we get

$$\mathfrak{M}, s \vDash @_i \Diamond{\downarrow}x.(\Box\Diamond p \wedge \Box(\Box\Diamond p \to \Diamond i) \wedge @_i\Box(\Box\Diamond p \to \Diamond x)).$$

□

4.3.2 Completeness

We will now show that $\mathcal{QHL}$ is complete. We will extend the completeness result discussed in Chapter 2.2.3. Let us briefly repeat the key steps of the proof.

Let Σ be a set of consistent formulas. Our goal is to obtain a canonical model $\mathfrak{M}_\Sigma$ in which each state is a maximal consistent subset of quantum hybrid formulas (MCS), each state is named by an $i \in \mathsf{Nom}$ and $\mathfrak{M}_\Sigma, s \vDash \Sigma$ for some state s.

We need a special type of MCS in order to obtain our completeness result. A MCS Γ is called *named* if there is an $i \in \Gamma$ for some $i \in \mathsf{Nom}$. A MCS Γ is called *pasted* if for every $@_i\Diamond\phi \in \Gamma$ there exists a nominal $j \in \mathsf{Nom}$ such that $@_i\Diamond j \wedge @_j\phi \in \Gamma$.

By the extended Lindenbaum lemma (Lemma 2.2.9) we can extend Σ to a named and pasted MCS Γ_Σ. From this Γ_Σ we can obtain a MCS named by i for each $i \in \mathsf{Nom}$. Let us define Δ_i by

$$\Delta_i := \{\phi \mid @_i\phi \in \Gamma_\Sigma\}.$$

Note we have the axiom $@_i i$, and since any MCS contains all axioms, we will have $i \in \Delta_i$. Moreover, since Γ_Σ is named, by Lemma 2.2.8 there exists a $k \in \mathsf{Nom}$ such that

$$\Gamma_\Sigma = \Delta_k. \tag{4.1}$$

The set of states of the canonical model $\mathfrak{M}_\Sigma$ will be $S_\Sigma = \{\Delta_i \mid i \in \mathsf{Nom}\}$. The relation $\not\perp_\Sigma$ is the standard canonical relation, so $\Delta_i \not\perp \Delta_j$ iff $\phi \in \Delta_j$ for every $\Box\phi \in \Delta_i$. The valuation V_Σ is given by $V(\phi) = \{\Delta_i \mid \phi \in \Delta_i\}$. Note that by Lemma 2.2.8 we have $j \in \Delta_i$ iff $\Delta_i = \Delta_j$, thus $|V(i)| = 1$ for all nominals $i \in \mathsf{Nom}$.

Theorem 4.3.4 (Completeness)**.** *A set of formulas Σ is $\mathcal{QHL}_n$ consistent iff Σ is satisfiable in a quantum Kripke model of dimension at most n (QKM$_n$).*

Proof. The direction from right to left follows from soundness (Theorem 4.3.3). For the left to right direction, suppose a set of formulas Σ is $\mathcal{QHL}_n$ consistent. Following the steps described above we obtain a named canonical model $\mathfrak{M} =$

(S, R, V), where S is a set of $\mathcal{QHL}_n$ maximal consistent sets of formulas[1], the model $\mathfrak{M}$ is a Hybrid logic model, that is $|V(i)| = 1$ for each $i \in \mathsf{Nom}$, and each $s \in S$ is named by some $i \in \mathsf{Nom}$. Moreover, by (4.1) there is an $s \in S$ such that $\Sigma \subseteq s$ and, because $\mathfrak{M}$ satisfies the truth lemma (Lemma 2.2.12), we have:

$$\mathfrak{M}, s \vDash \phi \text{ for all } \phi \in \Sigma.$$

We will now show $\mathfrak{M}$ is a quantum Kripke model of dimension at most n, that is, we will show $\mathfrak{M}$ satisfies all four properties of Definition 4.1.1.

A *pure formula* is a formula in which the only atomic proposition letters occurring are nominals (see Definition 2.2.5). The axioms Separation, Superposition and Maximum basis are all pure formulas, and by Theorem 2.2.13 the model $\mathfrak{M}$ satisfies their characteristic properties, which by Lemma 4.3.2 are *separation*, *superposition* and *maximum basis* (properties 1–3) of Definition 4.1.1.

To prove $\mathfrak{M}$ satisfies the *finite cover law* (Definition 4.1.1-4), suppose for some finite subset $P \subset_\omega S$ we have $s \in S \setminus {\sim}P$. By definition this means there exists a $v \in P$ such that $s \not\perp v$. Given that $\mathfrak{M}$ is named, s is named by some $i \in \mathsf{Nom}$ and each $p \in P$ is named by some $i_p \in \mathsf{Nom}$. Let $\phi := \bigvee_{p \in P} i_p$, then $[\![\phi]\!] = P$. As $v \in P$, we note that $\mathfrak{M}, v \vDash \phi$ and by Lemma 4.1.8 note that $[\![\Box\Diamond\phi]\!] = {\sim}{\sim}P$.

We have $\mathfrak{M}, v \vDash \phi$ and therefore $\mathfrak{M}, s \vDash \Diamond\phi$, so given that $V(i) = \{s\}$ we conclude $\mathfrak{M}, s \vDash @_i\Diamond\phi$. Thus by modus ponens $\mathfrak{M}, s \vDash @_i\Diamond{\downarrow}x.(\Box\Diamond\phi \wedge \Box(\Box\Diamond\phi \rightarrow \Diamond i) \wedge @_i(\Box\Diamond\phi \rightarrow \Diamond x))$. Therefore there exists a $t \in S$ such that

- $\mathfrak{M}[V(x) := \{t\}], t \vDash \Box\Diamond\phi$, that is, $t \in {\sim}{\sim}P$, and
- $\mathfrak{M}[V(x) := \{t\}], t \vDash \Box(\Box\Diamond\phi \rightarrow \Diamond i)$, that is, for all $u \in S$ such that $t \not\perp u$, if $u \in {\sim}{\sim}P$ then $u \not\perp s$, and
- $\mathfrak{M}[V(x) := \{t\}], s \vDash \Box(\Box\Diamond\phi \rightarrow \Diamond x)$, that is, for all $u \in S$ such that $s \not\perp u$, if $u \in {\sim}{\sim}P$ then $u \not\perp t$.

Combining and rewriting the above three statements we see that there exists a $t \in {\sim}{\sim}P$ such that $s \not\perp u$ iff $t \not\perp u$ for all $u \in {\sim}{\sim}P$. In conclusion, $\mathfrak{M}$ satisfies property 4 of definition 4.1.1. □

[1] Note that S is not the set of *all* $\mathcal{QHL}_n$ maximal consistent sets of formulas.

Chapter 5

Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs

Summary: In this chapter we present a sound axiomatization for a probabilistic modal dynamic logic of quantum programs. The logic can express whether a state is separable or entangled, information that is local to a subsystem of the whole quantum system, and the probability of positive answers to quantum tests of certain properties. The power of this axiomatization is demonstrated with proofs of properties concerning bases of a finite dimensional Hilbert space, composite systems, entangled and separable states, and with proofs of the correctness of two probabilistic quantum protocols (the quantum leader election protocol and the BB84 quantum key distribution protocol).

Background: This chapter introduces a sound axiomatisation for a probabilistic quantum logic. The logic is based on the logic for quantum programs introduced by Baltag and Smets, which we discuss in Chapter 2.2.3. The logic presented in this chapter is closely related to the probabilistic logic presented in Chapter 6. The axiomatisation starts from the deductive system for probabilistic logic introduced by Fagin and Halpern, which we discuss in Chapter 2.2.4, and several sound axioms proposed by Baltag and Smets, which are discussed in Chapter 2.2.3, in particular Figure 2.4.

This chapter is organized as follows. In Section 5.1, we introduce probabilistic quantum structures, the basic structures for our semantics, which are mild abstractions of Hilbert spaces. In Section 5.2, we introduce the syntax and semantics for our probabilistic logic of quantum programs. We then present in Section 5.3 the deductive system and prove some properties in our language, including properties concerning orthonormal bases. In Section 5.4 we prove the correctness of the quantum leader election protocol and the BB84 protocol.

5.1 Probabilistic Quantum Structure

Let $\mathcal{H}$ be a finite dimensional Hilbert space with an orthonormal basis $\vec{B} = (\vec{b}_0, \ldots, \vec{b}_{n-1})$. Let $V_{\vec{B}}$ denote the set of all functions $f : \vec{B} \to \mathbb{C}$. It is well known that there is a bijective correspondence between the vectors in $\mathcal{H}$ and the elements of $V_{\vec{B}}$ given by mapping every $\vec{v}$ in $\mathcal{H}$ to the function $\vec{b}_i \mapsto \langle \vec{v}, \vec{b}_i \rangle$. A *state* of $\mathcal{H}$ is a one-dimensional subspace s of $\mathcal{H}$. We represent the states of $\mathcal{H}$ by a subset of $V_{\vec{B}}$, each representing a canonical representative of the one-dimensional subspace. This subset is the set of complex probability mass function defined as follows.

Definition 5.1.1 (Complex probability mass functions)**.** Let $B = \{b_i \mid 0 \leq i < n\}$ for some positive $n \in \mathbb{N}$ be an ordered set (which we call an *ordered basis*). A function $f : B \to \mathbb{C}$ is called a *complex probability mass function* on B if

1. there exists an $i \in n$ such that
   (a) $f(b_j) = 0$ for all $j < i$, and
   (b) $f(b_i) \in (0, 1] \subset \mathbb{R}$,
2. $|f(b_i)|^2 \in [0, 1]$ for all $i \in n$, and
3. $\sum_{i \in N} |f(b_i)|^2 = 1$.

Let S_B denote the set of all complex probability mass functions on B.

Note that if f is a complex probability mass function, the function $f^2 : B \to [0, 1]$ is a (real) probability mass function. In this sense, a complex probability mass function can be seen as an appropriate "square root" of a probability mass function.

Every function $f \in V_{\vec{B}}$ can be converted into a function in $S_{\vec{B}}$ as follows.

Definition 5.1.2 (Strong normalization)**.** Let $B = \{b_i \mid 0 \leq i < n\}$ for some positive $n \in \mathbb{N}$ be an ordered basis. For every non-zero function $f : B \to \mathbb{C}$, where $c = f(b_i)$ for the smallest i such that $f(b_i) \neq 0$, we define the *strong normalization* $\mathsf{sn}(f)$ of f by

$$\mathsf{sn}(f) : b \mapsto \frac{\overline{c}}{\sqrt{\sum_i |\overline{c} \cdot f(b_i)|^2}} f(b),$$

where $\overline{c}$ is the complex conjugate of c.

It is easy to see that the strong normalization transforms any non-zero function $f : \vec{B} \to \mathbb{C}$ into a complex probability mass function. The set of complex probability mass functions is identified with the set of states of a Hilbert space by the following proposition.

Proposition 5.1.3. *Let $\mathcal{H}$ be a Hilbert space with $\vec{B} = \{\vec{b_0}, \ldots, \vec{b_{n-1}}\}$ an ordered orthonormal basis. The following both hold.*

1. *Given a complex probability mass function $f : \vec{B} \to \mathbb{C}$, there exists a unique unit vector $\vec{v}$ in $\mathcal{H}$, such that for each j, $f(\vec{b_j}) = \langle \vec{v}, \vec{b_j} \rangle$.*

2. *Given any state s of $\mathcal{H}$, there is a* unique *unit vector $\vec{v}$ in s, such that the function $f_{\vec{v}} = \langle \vec{v}, \cdot \rangle : \vec{B} \to \mathbb{C}$ is a complex probability mass function over the ordered orthonormal basis $\vec{B}$.*

Proof. 1. Given $f \in S_{\vec{B}}$, we define the vector $\vec{v}$ to be

$$\vec{v} = \sum_{j \in n} f(\vec{b_j})\vec{b_j}.$$

Since the basis $\vec{B}$ is orthonormal, it is easy to see that $f(\vec{b_j}) = \langle \vec{v}, \vec{b_j} \rangle$. By condition 3 of the definition of a complex probability mass function, $\vec{v}$ is a unit vector.

2. Let s be a one-dimensional subspace of $\mathcal{H}$, and let $\vec{w}$ be any non-zero vector in s. We identify $\vec{w}$ with a non-zero function in $f_{\vec{w}} \in V_{\vec{B}}$. Let $\vec{v}$ be a vector corresponding to $\mathsf{sn}(f_{\vec{w}})$. As $\vec{v}$ only differs from $\vec{w}$ by a constant multiple, $\vec{v} \in s$. Furthermore, as $\mathsf{sn}(f_{\vec{w}})$ is a complex probability mass function, $\vec{v}$ is a unit vector. To see that $\vec{v}$ is unique, we observe that for any complex number $c \neq 1$ and any complex probability mass function f, the function $c \cdot f : \vec{b} \mapsto c \cdot f(\vec{b})$ is not a complex probability mass function. □

Because every state can be represented by a complex probability mass function, we will use the term *state* to mean either a one-dimensional subspace or a complex probability mass function. We will also use the same notation for both concepts. Also, throughout this chapter, we will identify each natural number $n \in \mathbb{N} \overset{\text{def}}{=} \{0, 1, 2, \dots\}$ with the set $\{0, 1, \dots, n-1\}$ of elements preceding it. If we write $i < N$ without a lower bound, we intend for i to range from $i = 0$ to $i = N - 1$.

5.1.1 Maps between bases and states

We require the basis to be ordered so that we can have a canonical representation of each state via a vector representative of its one-dimensional subspace (for the same reason, vectors are written as ordered tuples, also assuming an order to its basis). Were we to reorder the basis elements, we could then map each vector representative in the original ordering to its unique corresponding representative in the new order (this mapping is, in this context, an identity map on states). This concept is generalized to change of basis maps as follows.

Definition 5.1.4 (change-of-basis isomorphism)**.** Let $B = \{b_i \mid i < d_B\}$ and $C = \{c_i \mid i < d_C\}$ be two ordered basis (where C could be a reordering of B).

A function $h : S_B \to S_C$ is a *change-of-basis isomorphism* iff there is a bijection $\eta : C \to B$ (which implies $d_B = d_C$) such that for all $s \in S_B$ and for all $i < d_C$

$$h(s)(c_i) = \mathsf{sn}(s \circ \eta)(c_i).$$

We call h an *order isomorphism* if in addition $\eta(c_i) = b_i$ for all $i < d_C$. We write $B \cong C$ and $S_B \cong S_C$ if there is an order isomorphism between S_B and S_C. We write $s \cong t$ for $s \in S_B$ and $t \in S_C$ if there is an order isomorphism $h : S_B \to S_C$, such that $h(s) = t$.

The tensor product of two ordered bases is the Cartesian product of the elements ordered by the dictionary order.

Definition 5.1.5 (Tensor product)**.** The *tensor product* of two ordered bases $B = (b_0, \dots, b_{n-1})$ and $C = (c_0, \dots, c_{m-1})$ is $D = (d_0, \dots, d_{nm-1})$, such that $d_k = (b_i, c_j)$ where $i = \lfloor k/m \rfloor$ and $j = k \mod m$. The tensor product of $s \in S_B$ and $t \in S_C$, denoted $s \otimes t$, is given by

$$(s \otimes t)(b_i, c_j) = s(b_i) \cdot t(c_j).$$

It is easy to see that in general $(s \otimes t) \otimes r \cong s \otimes (t \otimes r)$. As the tensor product is associative given our strictest notion of isomorphism, we will ignore internal parentheses when taking tensor products of more than two bases.

5.1.2 Agents and Separability

In most communication protocols we have several agents who are in control of part of the (quantum) system, but not the whole. The following definitions describe formally how a probabilistic quantum model is build up from its submodel.

Definition 5.1.6 (multi-agent PQM and components)**.** Let $N = \{0, \dots, N-1\}$ be a finite set of agents. An *N-Probabilistic Quantum Model (N-PQM)* is a tuple $\mathfrak{M} = (B_0, \dots, B_{N-1})$ of ordered bases. Let $I \subseteq N$. Then $\mathfrak{M}_I \overset{\text{def}}{=} \{B_i \mid i \in I\}$ is said to be a *component* of $\mathfrak{M}$.

If $I = \{x_1, \dots, x_m\} \subseteq N$ for some $m < N$ (where (x_i) is strictly increasing), we write $\bigotimes \mathfrak{M}_I = B_{x_1} \otimes B_{x_2} \otimes \cdots \otimes B_{x_m}$. We write $S_I^{\mathfrak{M}}$ (or S_I if $\mathfrak{M}$ is understood from context) for $S_{\bigotimes \mathfrak{M}_I}$, and S (or $S^{\mathfrak{M}}$) for S_N (or $S_N^{\mathfrak{M}}$). In what follows, given a finite ordered set $J = \{x_1, \dots, x_m\}$ for some $m < N$, where the sequence (x_i) is strictly increasing, we use the notation $(b_i)_{i \in J}$ for the tuple $(b_{x_1}, \dots, b_{x_m})$.

Definition 5.1.7 (Tensor product of Agent components)**.** Let $\mathfrak{M} = (B_0, \dots, B_{N-1})$ be an N-PQM, and let $I, J \subseteq N$, such that $I \cap J = \emptyset$. The *$\mathfrak{M}$-tensor product* $\mathfrak{M}_I \otimes^{\mathfrak{M}} \mathfrak{M}_J$ is defined to be $\mathfrak{M}_{I \cup J}$, but where for each $s \in S_I$ and $t \in S_J$, we have for each sequence (x_i) with $b_{x_i} \in B_i$ that

$$(s \otimes^{\mathfrak{M}} t)((b_{x_i})_{i \in I \cup J}) = s((b_{x_i})_{i \in I}) \cdot t((b_{x_j})_{j \in J}).$$

Given sets $X \subseteq S_I$ and $Y \subseteq S_J$, let $X \otimes^{\mathfrak{M}} Y \overset{\text{def}}{=} \{x \otimes^{\mathfrak{M}} y \mid x \in X, y \in Y\}$.

Note that although $\otimes$ is not commutative, $\otimes^{\mathfrak{M}}$ is. Also note that $\otimes^{\mathfrak{M}}$ is associative; hence we generally omit parentheses.

Definition 5.1.8 (Separable and entangled states)**.** Given an N-PQM $\mathfrak{M}$, a set $J \subseteq N$, a partition $\Pi = \{X_1, \dots, X_k\}$ of N, and a state $s \in S^{\mathfrak{M}}$, we say than

- s is $\mathfrak{M}$*-separable in* J if there exist $s_J \in S_J$ and $s_{N\setminus J} \in S_{N\setminus J}$ such that $s \cong s_J \otimes^{\mathfrak{M}} s_{N\setminus J}$. If s is not $\mathfrak{M}$-separable in J we say that s is $\mathfrak{M}$*-entangled in* J.
- s is $\mathfrak{M}$*-separable in* Π if there exists $s_i \in S_{X_i}$ such that $s \cong s_1 \otimes^{\mathfrak{M}} \cdots \otimes^{\mathfrak{M}} s_k$. If s is not $\mathfrak{M}$-separable in Π we say that s is $\mathfrak{M}$*-entangled in* Π. If $\mathfrak{M}$ is separable in $\{\{i\} \mid i \in N\}$, we say $\mathfrak{M}$ is *fully separable.*

Separability will play an important role in the semantics of the logic we define in the next section.

5.2 Probablistic quantum logic

In this section, we define the syntax and semantics of our language, and provide some useful syntactic abbreviations.

5.2.1 Syntax

Let N be a set of agents and let Prop be a (countable) set of proposition letters denoted with $p, q, \dots$. The language is three-sorted, with formulas ϕ, programs α, and probability terms t, and is defined by

$$\begin{aligned}
\phi &::= p \mid \neg\phi \mid \phi \wedge \phi \mid [\alpha]\phi \mid \mathrm{At}(\phi) \mid \mathsf{Sep}(\phi) \mid \phi_I \mid t \geq \rho \\
\alpha &::= \phi? \mid \alpha \cup \alpha \mid \alpha ; \alpha \\
t &::= \rho \Pr(\phi) \mid t + t
\end{aligned}$$

where $p \in \mathsf{Prop}$, $I \subseteq N$, and $\rho \in \mathbb{Q}$. The set of formulas ϕ is denoted by $\mathcal{L}_N$, and the set of terms t is denoted by Terms.

We have the standard logical connectives $\neg\phi, \phi \wedge \psi$ and $[\alpha]\phi$ with the meaning *not* ϕ, ϕ *and* ψ and *after any successful execution of program* α, ϕ *holds* respectively.

Here the programs α are $\phi?$, *a quantum test whether or not* ϕ *holds*; $\alpha \cup \beta$, *an arbitrary choice between two programs* α *and* β; and $\alpha; \beta$, *the sequential execution of two programs* α *and* β.

We also have three non-standard, but useful connectives. $\mathrm{At}(\phi)$ intuitively means that ϕ *is only true at one and only one state.* $\mathsf{Sep}(\phi)$ means intuitively that all states making ϕ true *are separable into each agent*, that is, these states are of the form $\bigotimes^{\mathfrak{M}}_{i<N} s_{\{i\}}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. ϕ_I intuitively represents *the information that the local system I has about ϕ*, that is, if any measurment that can be performed within the local system I cannot refute ϕ, then ϕ_I true.

Lastly, we have $t \geq \rho$, which intuitively means *the probability of t is greater than or equal to ρ*. Here t is a linear combination of $\Pr(\phi)$, the *probability that a test for ϕ is successful*.

We have chosen the language to express several examples in the simplest way. However, one could easily imagine ways to extend the expressibility of this language. For example, we could extend this language with unitary operators $\alpha ::= U \mid U^\dagger$, however we do not use these operators in the examples we discuss.

5.2.2 Semantics

The semantics is defined with respect to an N-PQM $\mathfrak{M}$. We will make use of the following concepts. We first observe that from just an ordered basis $B = \{b_0, \ldots, b_{n-1}\}$ we can recover the Hilbert space structure, such as the inner product, as follows. For any two states $s, t \in S_B$, we define the *inner product* of s and t to be

$$\langle s, t \rangle \overset{\text{def}}{=} \sum_{i=0}^{n-1} \overline{s(b_i)} t(b_i) \tag{5.1}$$

where in general $\overline{z}$ is the complex conjugate of z. Then $R \overset{\text{def}}{=} \{(s,t) \mid \langle s, t \rangle \neq 0\}$ relates any two states that are non-orthogonal. We define the orthocomplement of a set of states X by

$$\sim\!X \overset{\text{def}}{=} \{s \in S \mid (s, x) \notin R \text{ for all } x \in X\}$$

and let $\mathcal{T} \overset{\text{def}}{=} \{P \subseteq S \mid P = \sim\sim\!P\}$ be the set of *testable properties*. For each $P \in \mathcal{T}$ we then let

$$R_P \overset{\text{def}}{=} \left\{(s,t) \in S^2 \middle| t \in P \text{ and } \mid \langle s, u \rangle|^2 < |\langle s, t \rangle|^2 \text{ for all } u \in P \setminus \{t\}\right\}.$$

Note that each $P \in \mathcal{T}$ corresponds to a linear closed subspace in a Hilbert space and that the relation R_P in fact corresponds to the projection onto the subspace P. It is easy to see that each singleton is testable, and hence that $R = \bigcup_{P \in \mathcal{T}} R_P$.

Given an N-PQM $\mathfrak{M}$ with carrier set $S = S_{\bigotimes \mathfrak{M}}$ and a valuation $V : \mathsf{Prop} \to \mathcal{P}S$, we interpret formulas by a function $[\![\cdot]\!]^{\mathfrak{M}} : \mathcal{L}_N \to \mathcal{P}S$, we interpret each program α by a relation $R_\alpha^{\mathfrak{M}} \subseteq S \times S$, and we interpret probability terms by a family of functions $[\![\cdot]\!]_s^{\mathfrak{M}} : \text{Terms} \to \mathbb{R}$ for each $s \in S$ as follows (we typically omit the superscript when it is understood by context). To interpret formulas ϕ:

$$\begin{aligned}
[\![p]\!] &\stackrel{\text{def}}{=} V(p),\\
[\![\neg\phi]\!] &\stackrel{\text{def}}{=} S \setminus [\![\phi]\!],\\
[\![\phi \wedge \psi]\!] &\stackrel{\text{def}}{=} [\![\phi]\!] \cap [\![\psi]\!],\\
[\![[\alpha]\phi]\!] &\stackrel{\text{def}}{=} \{s \in S \mid R_\alpha(s) \subseteq [\![\phi]\!]\},\\
[\![\mathrm{At}(\phi)]\!] &\stackrel{\text{def}}{=} \begin{cases} S & \text{if } [\![\phi]\!] = \{s\} \text{ for some } s \in S,\\ \emptyset & \text{otherwise,}\end{cases}\\
[\![\mathsf{Sep}(\phi)]\!] &\stackrel{\text{def}}{=} \begin{cases} S & \text{if } [\![\phi]\!] \subseteq \{s \in S \mid s = \bigotimes^{\mathfrak{M}}_{i\in N} s_{\{i\}}\},\\ \emptyset & \text{otherwise,}\end{cases}\\
[\![\phi_I]\!] &\stackrel{\text{def}}{=} \left\{ s_I \otimes^{\mathfrak{M}} s_{N\setminus I} \;\middle|\; (s_I \otimes^{\mathfrak{M}} t_{N\setminus I}) \in [\![\phi]\!] \text{ for some } t_{N\setminus I} \right\},\\
[\![t \geq \rho]\!] &\stackrel{\text{def}}{=} \{s \in S \mid [\![t]\!]_s \geq \rho\}.
\end{aligned}$$

To interpret programs α:

$$\begin{aligned}
R_{\phi?} &\stackrel{\text{def}}{=} R_P, \text{ where } P = {\sim}{\sim}[\![\phi]\!],\\
R_{\alpha\cup\beta} &\stackrel{\text{def}}{=} R_\alpha \cup R_\beta,\\
R_{\alpha;\beta} &\stackrel{\text{def}}{=} R_\alpha; R_\beta.
\end{aligned}$$

To interpret terms t:

$$\begin{aligned}
[\![\rho\,\mathrm{Pr}(\phi)]\!]_s &\stackrel{\text{def}}{=} \rho \sum_{t\in R_P(s)} |\langle s,t\rangle|^2, \text{ where } P = {\sim}{\sim}[\![\phi]\!],\\
[\![t_1 + t_2]\!]_s &\stackrel{\text{def}}{=} [\![t_1]\!]_s + [\![t_2]\!]_s.
\end{aligned}$$

5.2.3 Abbreviations

With this language we can express many notions in quantum mechanics. Some are so important and natural to use, we introduce abbreviations for them (Figure 5.1). We have the standard abbreviations $\mathtt{tt}, \mathtt{ff}$ and $\vee$. Note that if $[\neg\phi?]\mathtt{ff}$ holds in a state s, then any test from s will result in a state with property ϕ, or equivalently, any non-orthogonal state has property ϕ. We abbreviate $[\neg\phi?]\mathtt{ff}$ using $\Box\phi$, where $\Box$ can be viewed as the modal operator for the non-orthogonality relation R. We abbreviate ${\sim}\phi$ by $\Box\neg\phi$ for the following reason. The orthocomplement of ϕ, denoted by ${\sim}\phi$, is true at any state s that is orthogonal to the set of states that make ϕ true. Equivalently, every state that makes ϕ true is orthogonal to s, and hence every state non-orthogonal to s makes $\neg\phi$ true. This means that $\Box\neg\phi$ is true at s. With the orthocomplement we can also define the quantum join: $\phi \sqcup \psi \stackrel{\text{def}}{=} {\sim}({\sim}\phi \wedge {\sim}\psi)$. The quantum join $\phi \sqcup \psi$ can be thought of as the smallest testable property containing ϕ and ψ.

$\mathtt{ff}$	$\overset{\text{def}}{=} p \wedge \neg p$	$\forall\phi$	$\overset{\text{def}}{=} \Box\Box\phi$
$\mathtt{tt}$	$\overset{\text{def}}{=} \neg\mathtt{ff}$	$\exists\phi$	$\overset{\text{def}}{=} \Diamond\Diamond\phi$
$\langle\alpha\rangle\phi$	$\overset{\text{def}}{=} \neg[\alpha]\neg\phi$	$(\phi \leq \psi)$	$\overset{\text{def}}{=} \forall(\phi \rightarrow \psi)$
$\Box\phi$	$\overset{\text{def}}{=} [\neg\phi?]\mathtt{ff}$	$(\phi \equiv \psi)$	$\overset{\text{def}}{=} \forall(\phi \leftrightarrow \psi)$
$\Diamond\phi$	$\overset{\text{def}}{=} \neg\Box\neg\phi$	$\phi \perp \psi$	$\overset{\text{def}}{=} \phi \leq {\sim}\psi$
${\sim}\phi$	$\overset{\text{def}}{=} \Box\neg\phi$	$T(\phi)$	$\overset{\text{def}}{=} {\sim}{\sim}\phi \equiv \phi$
$\phi \vee \psi$	$\overset{\text{def}}{=} \neg(\neg\phi \wedge \neg\psi)$	$I(\phi)$	$\overset{\text{def}}{=} (\phi \equiv \phi_I)$
$\phi \sqcup \psi$	$\overset{\text{def}}{=} {\sim}({\sim}\phi \wedge {\sim}\psi)$		

Figure 5.1: Abbreviations for formulas

$\sum_{k=1}^{n} a_k \Pr(\phi_k)$	$\overset{\text{def}}{=} a_1 \Pr(\phi_1) + \cdots + a_n \Pr(\phi_n)$		
$\rho \sum_{k=1}^{n} a_k \Pr(\phi_k)$	$\overset{\text{def}}{=} \sum_{k=1}^{n} \rho a_k \Pr(\phi_k)$		
$t < \rho$	$\overset{\text{def}}{=} \neg(t \geq \rho)$	$t_1 \geq t_2$	$\overset{\text{def}}{=} t_1 - t_2 \geq 0$
$t_1 \geq t_2$	$\overset{\text{def}}{=} t_2 - t_1 \geq 0$	$t_1 = t_2$	$\overset{\text{def}}{=} t_1 - t_2 = 0$
$t \leq \rho$	$\overset{\text{def}}{=} -t \geq -\rho$	$\langle\phi?\rangle_{=\rho}\psi$	$\overset{\text{def}}{=} \Pr(\phi) = \rho \wedge \langle\phi?\rangle\psi$
$t = \rho$	$\overset{\text{def}}{=} t \geq \rho \wedge t \leq \rho$	$\langle\phi?\rangle_{>\rho}\psi$	$\overset{\text{def}}{=} \Pr(\phi) > \rho \wedge \langle\phi?\rangle\psi$

Figure 5.2: Probabilistic abbreviations

Our quantum models satisfy the superposition principle: every state can reach any other state in two non-orthogonal steps, that is $R; R = S \times S$. This gives us the power to express that a formula is valid in a model: $\forall\phi \overset{\text{def}}{=} \Box\Box\phi$ is true at a state iff ϕ is true at every state in the model. With this global modality we can express many relations between formulas that are globally true, such as inequality: $(\phi \leq \psi) \overset{\text{def}}{=} \forall(\phi \rightarrow \psi)$, equality: $(\phi \equiv \psi) \overset{\text{def}}{=} \forall(\phi \leftrightarrow \psi)$, and orthogonal formulas: $(\phi \perp \psi) \overset{\text{def}}{=} (\phi \leq {\sim}\psi)$.

As can be seen from the definition of the semantics, the logical operators for probability $\Pr(\phi)$ and for tests $\phi?$ are only meaningful if the formula ϕ is testable. Noting that every testable property is closed under taking double orthocomplement, we can express testability by $T(\phi) \overset{\text{def}}{=} (\phi \equiv {\sim}{\sim}\phi)$.

Similarly, in a multi-agent setting, the formula ϕ must be separable in I for ϕ_I to represent the information I has about ϕ (that is, *I's local state*). We say that ϕ is *I-local* if $I(\phi) \overset{\text{def}}{=} (\phi \equiv \phi_I)$, that is, the truth of ϕ is fully determined by the local state of I.

In Figure 5.2 we have abbreviations concerning probabilities. All but the last two are standard abbreviations for terms and pure probabilistic formulas taken from [54, p. 83]. Concerning the last two, we are often interested in the probability of successfully testing ϕ as well as the outcome of a successful test. We abbreviate this with the formulas $\langle\phi?\rangle_{=\rho}\psi$ and $\langle\phi?\rangle_{>\rho}\psi$.

$$\begin{array}{|lll|}\hline \text{MP} & \dfrac{\phi \quad \phi \to \psi}{\psi} & \text{(modus ponens)} \\ \text{Nec} & \dfrac{\phi}{[\alpha]\phi} & \text{(necessitation)} \\ \text{US} & \dfrac{\phi}{\phi^{\sigma}} \text{ for some } \sigma : \mathsf{Prop} \to \mathcal{L}_N & \text{(substitution)} \\ \hline \end{array}$$

Figure 5.3: Rules

5.3 Deductive system

Our deductive proof system contains three rules (Figure 5.3), where ϕ^{σ} is obtained from ϕ by replacing all occurrences of p with $\sigma(p)$, and a list of axioms (Figure 5.4), divided into the following five categories: standard propositional dynamic logic axioms, standard axioms about linear inequalities, basic axioms for quantum systems, probabilistic axioms for quantum systems and axioms for quantum systems concerning atoms and separability.

A proof for ϕ is a finite sequence of formulas, such that the last formula is ϕ and every formula is either an axiom listed below or obtained by applying an inference rule to (a) formula(s) appearing earlier in the sequence.

The three rules in Figure 5.3 are standard, but we can deduce some non-standard rules concerning the abbreviations $\forall$, $\leq$, $\equiv$ and $T(\cdot)$, which will be given in Lemma 5.3.3.

The axioms for programs and for linear inequalities are standard, so we will only discuss the axioms in the last three categories.

Basic axioms for quantum systems. The first axiom Q1 states that equivalent formulas have equivalent tests. The second axiom Q2 expresses that by design when we test for a formula ϕ we actually test for the smallest closed linear subset containing $[\![\phi]\!]$, that is $\sim\sim\phi$.

For the axioms Q3 to Q9 one should remember that $\Box$ corresponds to the non-orthogonality relation and $[p?]$ corresponds to the projection onto P, where $P = \sim\sim[\![p]\!]$.

Axiom Q3 is related to the superposition principle, which is the principle that for every two states there is a third state that is non-orthogonal to both of them (or any two states can reach each other by two non-orthogonal steps).

Axiom Q4 states that if a successful test for p results in a state satisfying q, then the state is non-orthogonal to $[\![q]\!]$, so we can successfully test for q. Axiom Q5 corresponds to the fact that each projection is a partial function.

A successful test for a testable property P always results in a state inside P. When inquiring about a property Q that is not testable, our framework tests

Axioms for programs	
PL	All propositional tautologies
K$[\alpha]$	$[\alpha](p \rightarrow q) \rightarrow ([\alpha]p \rightarrow [\alpha]q)$
PDL1	$[\alpha;\beta]p \leftrightarrow [\alpha][\beta]p$
PDL2	$[\alpha \cup \beta]p \leftrightarrow [\alpha]p \wedge [\beta]p$
Axioms for linear inequalities	
I1	$t \geq \beta \leftrightarrow t + 0\,\mathrm{Pr}(\phi) \geq \beta$
I2	$\sum_{k=1}^{n} \alpha_k \,\mathrm{Pr}(\phi_k) \geq \beta \rightarrow \sum_{k=1}^{n} \alpha_{j_k} \,\mathrm{Pr}(\phi_{j_k}) \geq q\beta$ for any permutation $j_1, \ldots, j_n$ of $1, \ldots, n$
I3	$\sum_{k=1}^{n} \alpha_k \,\mathrm{Pr}(\phi_k) \geq \beta \wedge \sum_{k=1}^{n} \alpha'_k \,\mathrm{Pr}(\phi_k) \geq \beta'$ $\rightarrow \sum_{k=1}^{n} (\alpha_k + \alpha'_k) \,\mathrm{Pr}(\phi_k) \geq (\beta + \beta')$
I4	$t \geq \beta \leftrightarrow dt \geq d\beta$ if $d > 0$
I5	$t \geq \beta \vee t \leq \beta$
I6	$t \geq \beta \rightarrow t \geq \gamma$ if $\beta > \gamma$
Basic axioms for quantum systems	
Q1	$(p \equiv q) \rightarrow ([p?]r \leftrightarrow [q?]r)$
Q2	$[p?]q \leftrightarrow [{\sim}{\sim}p?]q$
Q3	$\Box\Box p \leftrightarrow \Box\Box\Box p$
Q4	$\langle p? \rangle q \rightarrow \langle q? \rangle \mathtt{tt}$
Q5	$\langle p? \rangle q \rightarrow [p?]q$
Q6	$[p?]{\sim}{\sim}p$
Q7	$p \rightarrow (q \rightarrow \langle p? \rangle q)$
Q8	$p \rightarrow [q?]\Box\langle q? \rangle \Diamond p$
Q9	$T(p) \wedge T(q) \rightarrow (\langle p? \rangle q \leftrightarrow (\Diamond p \wedge \Box(p \rightarrow \Diamond(p \wedge q))))$
Probabilistic axioms for quantum systems	
P1	$\mathrm{Pr}(\mathtt{tt}) = 1$
P2	$\mathrm{Pr}(p) \geq 0$
P3	$\mathrm{Pr}(p) = 0 \leftrightarrow {\sim}p$
P4	$(p \equiv q) \rightarrow \mathrm{Pr}(p) = \mathrm{Pr}(q)$
P5	$(p \perp q) \rightarrow \mathrm{Pr}(p \sqcup q) = \mathrm{Pr}(p) + \mathrm{Pr}(q)$
P6	$((p \perp q) \wedge \exists p \wedge \exists q) \rightarrow \exists(\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q)$
P7	$(p \leq q) \wedge \langle q? \rangle_{=\rho}(\mathrm{Pr}(p) = \tau) \rightarrow (\mathrm{Pr}(p) = \rho\tau)$
Axioms for atoms and separability	
A1	$(\mathrm{At}(p) \wedge (q \not\equiv \mathtt{ff}) \wedge (q \leq p)) \rightarrow (q \equiv p)$
A2	$\mathrm{At}(p) \rightarrow (\exists(p \wedge q) \leftrightarrow (p \leq q))$
A3	$(\mathrm{At}(p) \wedge (p \leq \Diamond q) \wedge T(q)) \rightarrow \mathrm{At}((p \sqcup {\sim}q) \wedge q)$
A4	$\mathsf{Sep}(p) \rightarrow (\mathrm{At}(p) \leftrightarrow (\exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})))$
A5	$\mathsf{Sep}(p) \wedge \mathsf{Sep}(q) \wedge \mathrm{At}(p) \wedge \mathrm{At}(q) \rightarrow ((p \equiv q) \leftrightarrow \bigwedge_{i<N}(p_{\{i\}} \equiv q_{\{i\}}))$
A6	$\mathsf{Sep}(p) \wedge \mathsf{Sep}(q) \rightarrow (\bigvee_{i<N}(p_{\{i\}} \perp q_{\{i\}}) \rightarrow (p \perp q))$

Figure 5.4: Axioms for quantum systems

for the smallest testable property containing Q. Axiom Q6 corresponds to these facts, where $\sim\sim p$ corresponds to the smallest testable property containing p.

If $s \in P$, then the projection is reflexive on s, that is, $(s, s) \in R_P$. So if a state makes p true, a successful test for p always ends up in the same state. This is captured by axiom Q7.

Axiom Q8 corresponds to the self-adjointness of projections with respect to the inner product, that is,

$$\langle \mathrm{Proj}_P(s), t\rangle = \langle s, \mathrm{Proj}_P(t)\rangle,$$

where $\mathrm{Proj}_P(s)$ is the projection of vector s onto the space P (sR_Pt where $t = \mathsf{sn}(\mathrm{Proj}_P(s))$). In non-probabilistic terms, this means that if the projection of s onto P is non-orthogonal to a state t, then the projection of t onto P is non-orthogonal to s.

The projection t of a state s onto P should be the closest state to s that is inside P. This can be expressed by: $(s, t) \in R_P$ iff for all $u \in P$ we have uRs iff uRt. This statement is partially captured by axiom Q9: looking at the right-to-left part of the biconditional, if a state s is non-orthogonal to a state satisfying p, and if all states satisfying p that are non-orthogonal to s are also non-orthogonal to a state satisfying $p \wedge q$, then the property $p \wedge q$ is "close to s", and a successful test for p at state s results in a state that satisfies q.

Probabilistic axioms for quantum systems. Axiom P1 and P2 are standard probability axioms ensuring the probability values are in the interval $[0, 1]$. Axiom P3 establishes the correspondence between orthogonality and zero probability.

Equivalent formulas should have equal probabilities, which is captured by axiom P4. Normally we can add the probabilities of disjoint sets, but in quantum systems we need the sets to be orthogonal.

Axiom P6 is the probabilistic version of the superposition statement. If p and q are orthogonal we can superpose them into a state with probability ρ to p and probability $1 - \rho$ to q. Axiom P7 relates to conditional probabilities: the probability of $p \wedge q$ is equal to the probability of p given q (which is τ in the axiom) times the probability of q (which is ρ in the axiom).

Axioms for atoms and separability. Atoms are the smallest non-empty sets, therefore any non-empty set smaller than an atom is equal to that atom. This is captured by axiom A1. As atoms are singleton states, a formula ϕ is satisfied at this state if and only if the atom implies ϕ. This is reflected by axiom A2.

For singleton states s that are non-orthogonal to a testable property Q, we have $(s, t) \in R_Q$ iff $\{t\} = (\{s\} \sqcup \sim Q) \cap Q$. In other words the projection of an atom is again an atom. This is captured by axiom A3.

Axiom A4 provides a characterisation of an atom under the condition that the formula is separable. Axiom A5 asserts that two fully separable atoms are equivalent if and only if each of their local components are equivalent. Axiom A6 expresses the fact that two fully separable properties are orthogonal if one of their local components are orthogonal.

Theorem 5.3.1. *The rules in Figure 5.3 and the axioms in Figure 5.4 are sound with respect to multi-agent probabilistic quantum models (N-PQM).*

Proof. Many of the axioms are standard from the literature. For example, PL, K, PDL1, and PDL2 are from propositional dynamic logic (see for example [65]). The axioms I1–I6 are from [53]. The axioms P1 P2 and variations of P4 are common among probability logics (see for example [53]). The axioms Q4–Q8 are from [10] and [96]. The validity of some others may be obvious from the discussion above. We now prove the soundness of select axioms.

Q9: Suppose p and q are testable, i.e. $[\![p]\!] = {\sim}{\sim}[\![p]\!]$ and $[\![q]\!] = {\sim}{\sim}[\![q]\!]$. Let $s \in [\![\langle p?\rangle q]\!]$. Then, by definition of $R_{[\![p]\!]}$ there exists a $t \in S$ such that $(s,t) \in R_{[\![p]\!]}$ and $t \in [\![p]\!]$; since $s \in [\![\langle p?\rangle q]\!]$, it also holds that $t \in [\![q]\!]$. As $[\![p \wedge q]\!] = [\![p]\!] \cap [\![q]\!]$, we have $t \in [\![p \wedge q]\!]$. As $R_{[\![p]\!]}$ corresponds to the projection onto $[\![p]\!]$, we know each state $u \in [\![p]\!]$ that is non-orthogonal to s is also non-orthogonal to t. Since $t \in [\![p \wedge q]\!]$, this means that $s \in [\![\Diamond p \wedge \Box(p \rightarrow \Diamond(p \wedge q))]\!]$.

Now suppose $s \in [\![\Diamond p \wedge \Box(p \rightarrow \Diamond(p \wedge q))]\!]$. Then we have $s \in [\![\Diamond p]\!]$, so s is non-orthogonal to $[\![p]\!]$, and therefore we have $(s,t) \in R_{[\![p]\!]}$ for some unique $t \in [\![p]\!]$. Then since $s \in [\![\Box(p \rightarrow \Diamond(p \wedge q))]\!]$, we know that $t \in [\![\Diamond(p \wedge q)]\!]$; thus there exists a $u \in [\![p \wedge q]\!] = [\![p]\!] \cap [\![q]\!]$, such that tRu. Now

$${\sim}{\sim}[\![p \wedge q]\!] = {\sim}{\sim}([\![p]\!] \cap [\![q]\!]) = {\sim}{\sim}[\![p]\!] \cap {\sim}{\sim}[\![q]\!] = [\![p]\!] \cap [\![q]\!] = [\![p \wedge q]\!].$$

Suppose towards a contradiction $t \notin [\![q]\!]$. Since $t \notin [\![p \wedge q]\!] = {\sim}{\sim}[\![p \wedge q]\!]$, we know there exists a $v \in {\sim}[\![p \wedge q]\!]$ such that tRv. Therefore v is non-orthogonal to $[\![p]\!]$, so there exists a unique $w \in [\![p]\!]$ such that $(v,w) \in R_{[\![p]\!]}$.

Now w (as the projection of v onto $[\![p]\!]$) can be characterized by being the element of $[\![p]\!]$ where vRu iff wRu for all $u \in [\![p]\!]$ (see, for example, [25, Proposition 2.15]). So we have wRx iff vRx for all $x \in [\![p]\!] \supset [\![p \wedge q]\!]$, and therefore we have $w \in [\![p]\!] \cap {\sim}[\![p \wedge q]\!]$. We also have wRt, which implies wRs (because t is the projection of s onto $[\![p]\!]$). Since $s \in [\![\Box(p \rightarrow \Diamond(p \wedge q))]\!]$ we have $w \in [\![\Diamond(p \wedge q)]\!]$, contradicting the fact that $w \in {\sim}[\![p \wedge q]\!]$. Thus $t \in [\![q]\!]$ and $s \in [\![\langle p?\rangle q]\!]$.

P6: Let $s \in [\![((p \perp q) \wedge \exists p \wedge \exists q)]\!]$. Let $x \in [\![p]\!]$ and $y \in [\![q]\!]$. Since $s \in [\![p \perp q]\!]$, $[\![p]\!] \subseteq [\![{\sim}q]\!]$, and hence $[\![p]\!]$ and $[\![q]\!]$ are orthogonal, and hence $\langle x, y\rangle = 0$. Consider the vector $z = \sqrt{\rho}x + \sqrt{(1-\rho)}y$. One can easily check that $z = \mathsf{sn}(z)$, and is hence in S. Furthermore, as $y \perp x$, the projection of z onto ${\sim}{\sim}[\![p]\!]$ is the vector $\sqrt{\rho}x$, whose normalization is $x \in [\![p]\!]$, and hence $z \in [\![\langle p?\rangle p]\!]$. The probability of projecting onto ${\sim}{\sim}[\![p]\!]$ is then $|\langle z, x\rangle|^2 = \rho$; thus $z \in [\![\langle p?\rangle_{=\rho} p]\!]$. We can similarly show that $z \in [\![\langle q?\rangle_{=1-\rho} q]\!]$. Therefore $z \in [\![\langle p?\rangle_{=\rho} p \wedge \langle q?\rangle_{=1-\rho} q]\!]$, and thus $s \in [\![\exists(\langle p?\rangle_{=\rho} p \wedge \langle q?\rangle_{=1-\rho} q)]\!]$, as desired.

P7: Let $Q = \sim\sim[\![q]\!]$ and $P = \sim\sim[\![p]\!]$. Suppose $s \in [\![(p \leq q) \wedge \langle q?\rangle_{=\rho}(\mathrm{Pr}(p) = \tau)]\!]$. Because $s \in [\![p \leq q]\!]$, we have that $[\![p \leq q]\!] \neq \emptyset$, and thus $[\![p]\!] \subseteq [\![q]\!]$, giving us $P \subseteq Q$. Also, $s \in [\![\langle q?\rangle_{=\rho}(\mathrm{Pr}(p) = \tau)]\!]$ and hence there exists a t, such that sR_Qt, $|\langle s,t\rangle|^2 = \rho$, and $t \in [\![\mathrm{Pr}(p) = \tau)]\!]$. Then there exists a $u \in P$, such that tR_Pu and $|\langle t,u\rangle|^2 = \tau$.

Now let $\eta = \langle s,t\rangle t$ be the actual vector when projecting s onto Q. Let $\xi = \langle \eta, u\rangle u$ be the actual vector when projecting η onto P. Let $\omega = \langle s,v\rangle v$ be the actual vector when projecting s onto P. Since $P \subseteq Q$, $\xi = \omega$ (to see this, one can change the basis so that P is the span of a subset of the basis elements, Q the span of a larger subset of the basis elements, and then project by removing the coefficients for basis elements not in the set we are projecting onto). Thus $u = v$ and $\langle \eta, u\rangle = \langle s,u\rangle$. Expanding η, we have $\overline{\langle s,t\rangle}\langle t,v\rangle = \langle s,u\rangle$. Hence $\rho\tau = |\langle s,t\rangle|^2|\langle t,v\rangle|^2 = |\langle s,u\rangle|^2$ is the probability of projecting s onto P. Hence $s \in [\![\mathrm{Pr}(p) = \rho\tau]\!]$.

A4: First, we claim that for any $\emptyset \subsetneq I \subsetneq N$ and any p we have $[\![T(p_I) \wedge \exists p_I]\!] = S$ (where S is the whole state space) if and only if it holds that $[\![p_I]\!] = \{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ for some fixed $s_I \in S_I$. Before we prove this claim, let us show the soundness of A4 with this claim.

Suppose we have that $s \in [\![\mathsf{Sep}(p) \wedge \mathrm{At}(p)]\!]$. Then $[\![\mathsf{Sep}(p) \wedge \mathrm{At}(p)]\!] = S$. Then $[\![p]\!] = \{\bigotimes^{\mathfrak{M}}_{i<N} s_{\{i\}}\}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. Therefore we have $[\![p_{\{i\}}]\!] = \{s_{\{i\}}\} \otimes^{\mathfrak{M}} S_{N\setminus\{i\}}$, and thus by the claim, $p_{\{i\}}$ is testable, i.e. $[\![T(p_{\{i\}})]\!] = S$ for each $i < N$. Because p is an atom, we also know that $[\![\exists p]\!] = S$. Thus $s \in [\![\exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!]$.

Now suppose $s \in [\![\mathsf{Sep}(p) \wedge \exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!]$. Then we have $[\![\mathsf{Sep}(p) \wedge \exists p \wedge \bigwedge_{i<N} T(p_{\{i\}})]\!] = S$. From $[\![\exists p]\!] = S$ we deduce $[\![p]\!] \neq \emptyset$. By $[\![\mathsf{Sep}(p)]\!] = S$ we know $[\![p]\!] \subseteq \bigcap_{i<N} [\![p_{\{i\}}]\!]$. By the claim we know $\bigcap_{i<N} [\![p_{\{i\}}]\!] = \{\bigotimes^{\mathfrak{M}}_{i<N} s_{\{i\}}\}$ for some $s_{\{i\}} \in S_{\{i\}}$ for each $i < N$. Combining these results we know $[\![p]\!] = \{s\}$, and therefore p is an atom, i.e. $[\![\mathrm{At}(p)]\!] = S$. Therefore, $s \in [\![\mathrm{At}(p)]\!]$.

To prove the claim, we first note that if $[\![T(q)]\!] = S$, we have $[\![q]\!] = \sim\sim[\![q]\!]$. Therefore if $s, t \in [\![q]\!]$ we also have $\sqrt{\rho}s + \sqrt{1-\rho}t \in [\![q]\!]$ for any $\rho \in [0,1]$, because any state that is orthogonal to both s and t is also orthogonal to $\sqrt{\rho}s + \sqrt{1-\rho}t$, so we find $\sqrt{\rho}s + \sqrt{1-\rho}t \in \sim\sim\{s,t\} \subseteq \sim\sim[\![q]\!] = [\![q]\!]$.

By definition of $[\![p_I]\!]$, any $s \in [\![p_I]\!]$ is of the form $s_I \otimes^{\mathfrak{M}} s_{N\setminus I}$. Suppose $s_I \otimes^{\mathfrak{M}} s_{N\setminus I}, t_I \otimes^{\mathfrak{M}} t_{N\setminus I} \in [\![p_I]\!]$ such that $s_I \neq t_I$. Without loss of generality we may also assume $s_{N\setminus I} \neq t_{N\setminus I}$, because if $s_I \otimes^{\mathfrak{M}} s_{N\setminus I} \in [\![p_I]\!]$, then $s_I \otimes^{\mathfrak{M}} s'_{N\setminus I} \in [\![p_I]\!]$ for any other $s'_{N\setminus I} \in S_{N\setminus I}$. If we look at the sum $\sqrt{\rho}(s_I \otimes^{\mathfrak{M}} s_{N\setminus I}) + \sqrt{1-\rho}(t_I \otimes^{\mathfrak{M}} t_{N\setminus I})$, with $\rho \neq 0, 1$, it is not hard to see that this sum is not equal to $u_I \otimes^{\mathfrak{M}} u_{N\setminus I}$ for any $u_I \in S_I$ and $u_{N\setminus I} \in S_{N\setminus I}$. In other words, $\sqrt{\rho}(s_I \otimes^{\mathfrak{M}} s_{N\setminus I}) + \sqrt{1-\rho}(t_I \otimes^{\mathfrak{M}} t_{N\setminus I}) \notin [\![p_I]\!]$.

Combining the above two results, we have that if $[\![p_I]\!] \neq \emptyset$ and $[\![T(p_I)]\!] = S$, then $[\![p_I]\!] = \{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ for some fixed $s_I \in S_I$.

For the other direction, we have that $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ is isomorphic to $S_{N\setminus I}$,

1	$\mathtt{tt}$	PL
2	$\mathtt{tt} \to (p \to \langle \mathtt{tt}?\rangle p)$	Q7 + US
3	$p \to \langle \mathtt{tt}?\rangle p$	MP(1,2)
4	$\langle \mathtt{tt}?\rangle p \to \Diamond p$	(5.3) + US
5	$p \to \Diamond p$	PL(3,4)
6	$\langle \mathtt{tt}?\rangle p \to [\mathtt{tt}?]p$	Q5 + US
7	$p \to [\mathtt{tt}?]p$	PL(3,6)
8	$[\mathtt{tt}?]p \to p$	PL(3) + US
9	$\langle \mathtt{tt}?\rangle p \to p$	PL(7) + US
10	$p \to [\mathtt{tt}?]\Box\langle \mathtt{tt}?\rangle \Diamond p$	Q8 + US
11	$p \to \Box\Diamond p$	PL(8,9,10) + US

Figure 5.5: A proof of $\vdash p \to \Diamond p$ and $\vdash p \to \Box\Diamond p$.

because every vector in the space spanned by $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ is a constant multiple of an element of $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$. Hence $\{s_I\} \otimes^{\mathfrak{M}} S_{N\setminus I}$ represents a subspace, and is therefore bi-orthogonally closed. Every topologically closed linear subspace is bi-orthogonally closed [30], and it is well-known that every subspace of a finite dimensional Hilbert space is isomorphic to $\mathbb{C}^n$ and therefore topologically closed. This finishes the proof of the claim. □

5.3.1 Deducible basic properties

We will now use our system to deduce several properties that are standard in most quantum logics, like weak modularity. In the first lemma we will show the connection between projections ($\langle\phi?\rangle$) and non-orthogonality ($\Diamond$). Also we show non-orthogonality is both reflexive and symmetric.

Lemma 5.3.2. *The following formulas are deducible.*

$$\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p \tag{5.2}$$

$$\vdash \langle p?\rangle q \to \Diamond q \tag{5.3}$$

$$\vdash p \to \Diamond p \qquad \textit{(reflexivity)} \tag{5.4}$$

$$\vdash p \to \Box\Diamond p \qquad \textit{(symmetry)} \tag{5.5}$$

Proof. To prove $\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p$, we first observe that $\vdash p \equiv \neg\neg p$. Then using universal substitution on Q1 and propositional logic, we obtain $\vdash \neg[p?]\mathtt{ff} \leftrightarrow \neg[\neg\neg p?]\mathtt{ff}$, which is precisely what $\vdash \langle p?\rangle \mathtt{tt} \leftrightarrow \Diamond p$ abbreviates.

To prove $\vdash \langle p?\rangle q \to \Diamond q$, observe by axiom Q4 that $\vdash \langle p?\rangle q \to \langle q?\rangle \mathtt{tt}$, where the right side is equivalent to $\Diamond q$. The proofs for $\vdash p \to \Diamond p$ and $\vdash p \to \Box\Diamond p$ can be found in Figure 5.5. □

With a proof of reflexivity, we can deduce the following four bidirectional rules (each column has both directions):

Lemma 5.3.3. *The following rules hold true:*

$$\frac{\vdash p}{\vdash \forall p} \qquad \frac{\vdash p \to q}{\vdash p \leq q} \qquad \frac{\vdash p \leftrightarrow q}{\vdash p \equiv q} \qquad \frac{\vdash p \leftrightarrow {\sim}{\sim}p}{\vdash T(p)}$$

$$\frac{\vdash \forall p}{\vdash p} \qquad \frac{\vdash p \leq q}{\vdash p \to q} \qquad \frac{\vdash p \equiv q}{\vdash p \leftrightarrow q} \qquad \frac{\vdash T(p)}{\vdash p \leftrightarrow {\sim}{\sim}p}$$

Proof. The upper row follows from two applications of necessitation; the lower row follows from reflexivity (Lemma 5.3.2-(5.4), which is equivalent to $\vdash \Box p \to p$). □

Throughout this text we will often apply the above lemma without reference. The following lemma states that every atom is non-empty.

Lemma 5.3.4. *The following formula is deducible.*

$$\vdash \exists p \leftrightarrow (p \not\equiv \mathtt{ff}).$$

As a consequence $\vdash \mathrm{At}(p) \to (p \not\equiv \mathtt{ff})$.

Proof. $p \not\equiv \mathtt{ff}$ abbreviates $\neg\Box\Box(p \leftrightarrow \mathtt{ff})$, which is equivalent to $\Diamond\Diamond((p \wedge \neg\mathtt{ff}) \vee (\neg p \wedge \mathtt{ff}))$. By standard modal reasoning, this is equivalent to $\Diamond\Diamond p$, or in abbreviated form $\exists p$.

We have $\vdash p \leq \mathtt{tt}$, so by $\mathsf{A2}$ we have $\vdash \mathrm{At}(p) \to \exists(p \wedge \mathtt{tt})$ and as we have $\vdash p \equiv (p \wedge \mathtt{tt})$ we have $\vdash \mathrm{At}(p) \to (p \not\equiv \mathtt{ff})$. □

The following lemma collects several properties of the orthocomplement, in particular the three defining properties $p \leq {\sim}{\sim}p$, $p \leq q$ implies ${\sim}q \leq {\sim}p$, and $(p \wedge {\sim}p) \equiv \mathtt{ff}$. Note that the first property $p \leq {\sim}{\sim}p$ is weaker than the standard property found in many quantum logics $p \equiv {\sim}{\sim}p$, but the latter only holds in quantum models that only consider testable properties.

Lemma 5.3.5 (Orthocomplement)**.** *The following formulas are deducible.*

$$\vdash p \leq {\sim}{\sim}p \tag{5.6}$$

$$\vdash (p \leq q) \to ({\sim}q \leq {\sim}p) \tag{5.7}$$

$$\vdash (p \wedge {\sim}p) \equiv \mathtt{ff} \tag{5.8}$$

$$\vdash {\sim}p \equiv {\sim}{\sim}{\sim}p \tag{5.9}$$

$$\vdash p \perp q \leftrightarrow q \perp p \tag{5.10}$$

Proof. The proofs of these formulas can be found in Figure 5.6. □

As shown in [11], the set of testable properties $\mathcal{T}$ contains all singletons and is closed under taking orthocomplement and intersections. The following lemma establishes the latter property. The former property will be deduced in Lemma 5.3.11, because we first need to show weak modularity.

1	$p \to \Box\Diamond p$	Lem. 5.3.2
2	$p \to \sim\sim p$	Abb.(1)
3	$p \leq \sim\sim p$	Lem. 5.3.3
4	$\Box\Box(p \to q) \to \Box\Box(\neg q \to \neg p)$	ML
5	$\Box\Box(p \to q) \to \Box\Box\Box(\neg q \to \neg p)$	$\mathtt{Q3}$
6	$\Box\Box(p \to q) \to \Box\Box(\Box\neg q \to \Box\neg p)$	ML(5)
7	$(p \leq q) \to (\sim q \leq \sim p)$	Abb.(6)
8	$\Box\neg p \to \neg p$	Lem. 5.3.2
9	$(p \land \Box\neg p) \to \mathtt{ff}$	PL(8)
10	$(p \land \sim p) \equiv \mathtt{ff}$	Lem. 5.3.3
11	$\sim p \leq \sim\sim\sim p$	US(3)
12	$(p \leq \sim\sim p) \to (\sim\sim\sim p \leq \sim p)$	US(7)
13	$(\sim\sim\sim p \leq \sim p)$	MP(3,12)
14	$\sim p \equiv \sim\sim\sim p$	PL(11,13)
15	$(p \leq \sim q) \to (\sim\sim q \leq \sim p)$	US(7)
16	$(p \leq \sim q) \to (q \leq \sim p)$	PL(2,15)
17	$(p \perp q) \to (q \perp p)$	Abb.(16)
18	$(q \perp p) \to (p \perp q)$	US(17)
19	$(p \perp q) \leftrightarrow (q \perp p)$	PL(17,18)

Figure 5.6: A proof of $\vdash p \leq \sim\sim p$, $\vdash (p \leq q) \to (\sim q \leq \sim p)$, $\vdash \sim p \equiv \sim\sim\sim p$, $\vdash (p \leq q) \to (\sim q \leq \sim p)$ and $\vdash (p \perp q) \leftrightarrow (q \perp p)$.

1	$\sim p \equiv \sim\sim\sim p$	(5.9)
2	$T(\sim p)$	Abb.(1)
3	$(p \wedge q) \leq \sim\sim(p \wedge q)$	(5.6)
4	$(p \wedge q) \leq p$	PL
5	$\sim\sim(p \wedge q) \leq \sim\sim p$	(5.7)
6	$\sim\sim(p \wedge q) \leq \sim\sim q$	US(5)
7	$\sim\sim(p \wedge q) \leq (\sim\sim p \wedge \sim\sim q)$	PL(5,6)
8	$(T(p) \wedge T(q)) \rightarrow ((\sim\sim p \wedge \sim\sim q) \equiv (p \wedge q))$	ML
9	$(T(p) \wedge T(q)) \rightarrow (\sim\sim(p \wedge q) \leq (p \wedge q))$	ML(7,8)
10	$(T(p) \wedge T(q)) \rightarrow ((p \wedge q) \equiv \sim\sim(p \wedge q))$	PL(3,9)
11	$(T(p) \wedge T(q)) \rightarrow T(p \wedge q)$	Abb.(10)

Figure 5.7: A proof of $T(\sim p)$ and $\vdash T(p) \wedge T(q) \rightarrow T(p \wedge q)$

Lemma 5.3.6 (Testable properties)**.** *The following formulas are deducible.*

$$\vdash T(\sim p) \tag{5.11}$$

$$\vdash T(p) \wedge T(q) \rightarrow T(p \wedge q) \tag{5.12}$$

Proof. The proof of these formulas can be found in Figure 5.7. □

The following lemma collects several properties of the quantum join. Most of these properties are intuitive when one thinks of the quantum join $p \sqcup q$ as the smallest closed linear subspace containing both p and q. For (5.17), if r is orthogonal to both p and q, then r is orthogonal to each element in the span of p and q, which is the quantum join $p \sqcup q$.

Lemma 5.3.7 (Quantum join)**.** *The following formulas are deducible.*

$$\vdash p \leq (p \sqcup q) \tag{5.13}$$

$$\vdash (p \sqcup q) \equiv (\sim\sim p) \sqcup (\sim\sim q) \tag{5.14}$$

$$\vdash (T(p) \wedge T(q)) \rightarrow (\sim(p \wedge q) \equiv (\sim p \sqcup \sim q)) \tag{5.15}$$

$$\vdash \sim(p \sqcup q) \equiv (\sim p \wedge \sim q) \tag{5.16}$$

$$\vdash ((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q)) \tag{5.17}$$

$$\vdash (p \sqcup \sim p) \equiv \texttt{tt} \tag{5.18}$$

$$\vdash (T(r) \wedge (p \leq r) \wedge (q \leq r)) \rightarrow ((p \sqcup q) \leq r) \tag{5.19}$$

Proof. The proof for the first five formulas can be found in Figure 5.8.

To show $\vdash (p \sqcup \sim p) \equiv \texttt{tt}$, we observe by Lemma 5.3.5-(5.8) that $\vdash (p \wedge \sim p) \equiv \texttt{ff}$. Hence $\vdash \neg(p \wedge \sim p) \equiv \texttt{tt}$. By modal logic, we have that $\vdash \sim(p \wedge \sim p) \equiv \Box\texttt{tt}$. Using necessitation and propositional logic, we have $\vdash \texttt{tt} \equiv \Box\texttt{tt}$. The desired result follows from this and modal logic.

To prove (5.19), we use Lemma 5.3.5-(5.7) to get $\vdash (p \leq r) \rightarrow (\sim r \leq \sim p)$ and $\vdash (q \leq r) \rightarrow \sim r \leq \sim p$, and hence $\vdash (p \leq r) \wedge (q \leq r) \rightarrow (\sim r \leq (\sim p \wedge \sim q))$.

1	$p \leq {\sim}{\sim}p$	Lem 5.3.5
2	$({\sim}p \wedge {\sim}q) \leq {\sim}p$	PL + Lem. 5.3.3
3	${\sim}{\sim}p \leq {\sim}({\sim}p \wedge {\sim}q)$	Lem. 5.3.5 + US
4	$p \leq {\sim}({\sim}p \wedge {\sim}q)$	ML(1,3)
5	$p \leq (p \sqcup q)$	Abb.(4)
6	${\sim}p \equiv {\sim}{\sim}{\sim}p$	Lem. 5.3.5
7	${\sim}({\sim}p \wedge {\sim}q) \equiv {\sim}({\sim}{\sim}{\sim}p \wedge {\sim}{\sim}{\sim}q)$	ML(6)
8	$(p \sqcup q) \equiv ({\sim}{\sim}p \sqcup {\sim}{\sim}q)$	Abb.(7)
9	$(T(p) \wedge T(q)) \rightarrow ({\sim}(p \wedge q) \equiv {\sim}({\sim}{\sim}p \wedge {\sim}{\sim}p))$	ML
10	$(T(p) \wedge T(q)) \rightarrow ({\sim}(p \wedge q) \equiv ({\sim}p \sqcup {\sim}q))$	Abb.(9)
11	$T({\sim}{\sim}({\sim}p \wedge {\sim}q))$	Lem.5.3.6
12	${\sim}{\sim}({\sim}p \wedge {\sim}q) \equiv ({\sim}p \wedge {\sim}q)$	Abb.(11)
13	${\sim}(p \sqcup q) \equiv ({\sim}p \wedge {\sim}q)$	Abb.(12)
14	$(r \perp p) \leftrightarrow \forall(r \rightarrow {\sim}p)$	Abb.
15	$(r \perp q) \leftrightarrow \forall(r \rightarrow {\sim}q)$	Abb.
16	$((r \perp p) \wedge (r \perp q)) \leftrightarrow \forall(r \rightarrow ({\sim}p \wedge {\sim}q))$	PL(14,15)
17	$T({\sim}p \wedge {\sim}q)$	Lem 5.3.6
18	$({\sim}p \wedge {\sim}q) \leftrightarrow {\sim}{\sim}({\sim}p \wedge {\sim}q)$	Lem. 5.3.3(17)
19	$((r \perp p) \wedge (r \perp q)) \leftrightarrow \forall(r \rightarrow {\sim}{\sim}({\sim}p \wedge {\sim}q))$	PL(16,18)
20	$((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q))$	Abb.(19)

Figure 5.8: A proof of $\vdash p \leq p \sqcup q$, $\vdash (p \sqcup q) \equiv ({\sim}{\sim}p \sqcup {\sim}{\sim}q)$, $(T(p) \wedge T(q)) \rightarrow ({\sim}(p \wedge q) \equiv ({\sim}p \sqcup {\sim}q))$, ${\sim}(p \sqcup q) \equiv ({\sim}p \wedge {\sim}q)$, and $\vdash ((r \perp p) \wedge (r \perp q)) \leftrightarrow (r \perp (p \sqcup q))$.

Using Lemma 5.3.5-(5.7) again we have $\vdash (p \leq r) \wedge (q \leq r) \rightarrow {\sim}({\sim}p \wedge {\sim}q) \leq {\sim}{\sim}r$. Adding $T(r)$ to the antecedent, the desired result follows from the previous observation and modal logic. □

We need a more general version of Lemma 5.3.7-(5.17) that considers the quantum join of n formulas instead of just two.

Corollary 5.3.8. *For all finite n and for all sets of formulas $\mathcal{B}$ of size n, the following formula is deducible.*

$$\vdash \bigwedge_{b \in \mathcal{B}} (p \perp b) \rightarrow p \perp \bigsqcup \mathcal{B} \tag{5.20}$$

$$\vdash \exists p \wedge (p \leq \bigsqcup_{b \in \mathcal{B}} b) \rightarrow \bigvee_{b \in \mathcal{B}} (p \not\perp b) \tag{5.21}$$

Proof. We prove this by induction on n. For $n = 1$ the statement holds trivially. Now suppose the statement holds for n. Let $\mathcal{B}$ be a set of formulas of size n and let b_{n+1} be a formula. By the induction hypothesis we have $\vdash (\bigwedge_{b \in \mathcal{B}} p \perp b) \rightarrow (p \perp \bigsqcup \mathcal{B})$. By Lemma 5.3.7-(5.17) we have $\vdash (p \perp b_{n+1}) \wedge (p \perp \bigsqcup \mathcal{B}) \rightarrow (p \perp (\bigsqcup \mathcal{B}) \sqcup b_{n+1})$. Combining the two results gives the desired result.

1	$q \leq ({\sim}p \sqcup q)$	Lem. 5.3.7
2	$(q \leq p) \to (q \leq (p \wedge ({\sim}p \sqcup q)))$	ML(1)
3	$p \to \Diamond p$	Lem. 5.3.2
4	$(q \leq p) \to (q \equiv (p \wedge q))$	ML
5	$T(p) \to ((p \wedge ({\sim}p \sqcup q)) \equiv (p \wedge \Box\neg(p \wedge \Box\neg q)))$	ML
6	$(q \leq p) \to (\Box\neg(p \wedge \Box\neg q) \leftrightarrow \Box(p \to \Diamond(p \wedge q)))$	ML(4)
7	$(q \leq p) \to (p \wedge \Box\neg(p \wedge \Box\neg q) \to \Diamond p \wedge \Box(p \to (\Diamond(p \wedge q))))$	PL(3,6)
8	$(T(p) \wedge T(q) \wedge \Diamond p \wedge \Box(p \to \Diamond(p \wedge q))) \to \langle p?\rangle q$	Q9
9	$(T(p) \wedge T(q) \wedge (q \leq p)) \to ((p \wedge ({\sim}p \sqcup q)) \to \langle p?\rangle q)$	PL(5,7,8)
10	$p \to ([p?]q \to q)$	Q7
11	$\langle p?\rangle q \to [p?]q$	Q5
12	$(p \wedge \langle p?\rangle q) \to q$	PL(10,11)
13	$(T(p) \wedge T(q) \wedge (q \leq p)) \to ((p \wedge ({\sim}p \sqcup q)) \to q)$	PL(9,12)
14	$(T(p) \wedge T(q) \wedge (q \leq p)) \leftrightarrow \forall(T(p) \wedge T(q) \wedge (q \leq p))$	Lem. 5.3.3
15	$(T(p) \wedge T(q) \wedge (q \leq p)) \to ((p \wedge ({\sim}p \sqcup q)) \leq q)$	Nec(13,14)
16	$(T(p) \wedge T(q) \wedge (q \leq p)) \to (q \equiv (p \wedge ({\sim}p \sqcup q)))$	ML(2,15)

Figure 5.9: A proof of $\vdash (T(p) \wedge T(q) \wedge (q \leq p)) \to (q \equiv (p \wedge ({\sim}p \sqcup q)))$.

For (5.21), Note that $\vdash (\exists p \wedge (p \leq \bigsqcup\mathcal{B}) \to (p \not\perp \bigsqcup\mathcal{B})$. Thus by the contrapositive of (5.20), we have $\vdash (\exists p \wedge (p \leq \bigsqcup\mathcal{B}) \to \bigvee_{b\in\mathcal{B}}(p \not\perp b)$. □

One of the main difference between classical logic and quantum logic is the lack of distributivity. Classical models satisfies distributivity $(p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r))$, but quantum models only satisfy a weaker version of distributivity called weak modularity, which we will show in the following lemma.

Lemma 5.3.9 (Weak modularity)**.** *The following formula is deducible.*

$$\vdash T(p) \wedge T(q) \wedge (q \leq p) \to (q \equiv p \wedge ({\sim}p \sqcup q)).$$

Proof. The proof can be found in Figure 5.9. □

We also need the dual of weak modularity, which we will show in the following corollary.

Corollary 5.3.10. *The following formula is deducible.*

$$\vdash T(q) \wedge (p \leq q) \to (q \equiv p \sqcup ({\sim}p \wedge q))$$

Proof. This is basically the dual of Lemma 5.3.9, that is, taking the orthocomplement. See Figure 5.10. □

With weak modularity we can show each atom is testable.

1	$(p \leq q) \to (\sim q \leq \sim p)$	Lem. 5.3.5
2	$T(\sim p)$	Lem. 5.3.6
3	$(\sim q \leq \sim p) \to (\sim q \equiv \sim p \wedge (\sim\sim p \sqcup \sim q))$	Lem. 5.3.9
4	$(p \leq q) \to (\sim\sim q \equiv \sim(\sim p \wedge (p \sqcup \sim q)))$	ML(1,2,3)
5	$(p \leq q) \to (\sim\sim q \equiv (\sim\sim p \sqcup \sim(p \sqcup \sim q)))$	Lem. 5.3.7
6	$(p \leq q) \to (\sim\sim q \equiv (p \sqcup (\sim p \wedge \sim\sim q)))$	Lem. 5.3.7
7	$(T(q) \wedge (p \leq q)) \to (q \equiv p \sqcup (\sim p \wedge q))$	ML(6)

Figure 5.10: A proof of $\vdash (T(q) \wedge (p \leq q)) \to (q \equiv p \sqcup (\sim p \wedge q))$.

Lemma 5.3.11. *The following formula is deducible.*

$$\mathrm{At}(p) \to T(p).$$

Proof. By Lemma 5.3.5 we have $\vdash p \leq \sim\sim p$, and by Lemma 5.3.2-(5.4) we have $\vdash \sim\sim p \leq \Diamond\sim\sim p$. So we can deduce $\vdash p \leq \Diamond\sim\sim p$. By Lemma 5.3.6 we have $\vdash T(\sim\sim p)$. Therefore we can apply axiom A3 and (5.9) to deduce $\vdash \mathrm{At}(p) \to \mathrm{At}((p \sqcup \sim p) \wedge \sim\sim p)$. By Lemma 5.3.7 we have $\vdash (p \sqcup \sim p) \equiv \mathtt{tt}$, so we can deduce $\vdash \mathrm{At}(p) \to \mathrm{At}(\sim\sim p)$. By Lemma 5.3.4 we have $\vdash \mathrm{At}(p) \to (\mathtt{ff} \not\equiv p)$, and we already have $\vdash p \leq \sim\sim p$, so we can deduce $\vdash \mathrm{At}(p) \to (p \equiv \sim\sim p)$ by axiom A1. This is equivalent to the desired result. □

5.3.2 Deducible probabilistic properties

The following lemma collects several deducible properties of probabilistic quantum logic.

Lemma 5.3.12. *The following formulas are deducible:*

$$\vdash \Diamond p \leftrightarrow \Pr(p) > 0 \tag{5.22}$$

$$\vdash \Pr(p) + \Pr(\sim p) = 1 \tag{5.23}$$

$$\vdash \Pr(p) = \Pr(\sim\sim p) \tag{5.24}$$

$$\vdash T(p) \to (p \leftrightarrow \Pr(p) = 1) \tag{5.25}$$

$$\vdash p \to \Pr(p) = 1 \tag{5.26}$$

Proof. The proof of (5.22) is in Figure 5.11.

We now show (5.23). By Lemma 5.3.5 we have $\vdash p \perp \sim p$ and $\vdash p \sqcup \sim p$, and hence by axiom P1, P4 and P5 we obtain the desired result $\vdash \Pr(p) + \Pr(\sim p) = 1$.

We now show (5.24). By uniform substitution in (5.23) we have $\vdash \Pr(\sim p) + \Pr(\sim\sim p) = 1$. From this we can use the inequality axioms to show the second result $\vdash \Pr(p) = \Pr(\sim\sim p)$.

We now show (5.25). Since $T(p)$ abbreviates $p \equiv \sim\sim p$, from the axiom $\vdash \Pr(p) = 0 \leftrightarrow \sim p$ it follows that $\vdash T(p) \to p \leftrightarrow \Pr(\sim p) = 0$. From the inequality

1	$\Pr(p) \neq 0 \leftrightarrow \Diamond p$	P3 + PL
2	$\Pr(p) > 0 \leftrightarrow \Diamond p$	PL(1) + P2

Figure 5.11: A proof of $\vdash \Diamond p \leftrightarrow \Pr(p) > 0$.

axioms and propositional reasoning we obtain the third result $\vdash T(p) \to p \leftrightarrow \Pr(p) = 1$.

We now show (5.26). By Lemma 5.3.5 we also have $\vdash p \to {\sim}{\sim}p$ and $\vdash T({\sim}({\sim}p))$, combining this with $\vdash \Pr(p) = \Pr({\sim}{\sim}p)$ we obtain the last result $\vdash p \to \Pr(p) = 1$. □

The following lemma shows that probability ($\Pr(\cdot)$) is monotone.

Proposition 5.3.13. *The following formula is deducible.*

$$\vdash p \leq q \to \Pr(p) \leq \Pr(q).$$

Proof. First, by (5.6) and modal logic, we have $\vdash p \leq q \to p \leq {\sim}{\sim}q$ and by Lemma 5.3.6, we have $\vdash T({\sim}{\sim}q)$. Therefore by Corollary 5.3.10 we have $\vdash p \leq q \to {\sim}{\sim}q \equiv p \sqcup ({\sim}p \wedge {\sim}{\sim}q)$. Hence by P4, $\vdash p \leq q \to P({\sim}{\sim}q) = P(p \sqcup ({\sim}p \wedge {\sim}{\sim}q))$. Note that $\vdash p \perp ({\sim}p \wedge {\sim}{\sim}q)$, since clearly $\vdash {\sim}p \wedge {\sim}{\sim}q \leq {\sim}p$. Thus by P5, $\vdash \Pr(p \sqcup ({\sim}p \wedge {\sim}{\sim}q)) = \Pr(p) + \Pr({\sim}p \wedge {\sim}{\sim}q)$. By (5.24), $\vdash \Pr(q) = \Pr({\sim}{\sim}q)$. Using inequality axioms, we obtain $\vdash p \leq q \to \Pr(q) = \Pr(p) + \Pr({\sim}p \wedge {\sim}{\sim}q)$. The desired result follows from this and the inequality axioms. □

Axiom P5 only considers a pair of orthogonal states, but can be generalised to a finite set of n pairwise orthogonal states.

Lemma 5.3.14. *For all n, the following formula is deducible.*

$$\vdash \left(\bigwedge_{i<j<n} b_i \perp b_j \right) \to \left(\Pr(\bigsqcup_{i \leq n} b_i) = \sum_{i<n} \Pr(b_i) \right).$$

Proof. We prove this by induction. For $n = 2$, the statement holds by Axiom P5. Now suppose the statement holds for n (IH). Given the induction hypothesis (IH), the proof of

$$\vdash \left(\bigwedge_{i<j<n+1} b_i \perp b_j \right) \to \left(\Pr(\bigsqcup_{i \leq n} b_i) = \sum_{i<n+1} \Pr(b_i) \right).$$

is given in Figure 5.12. □

Using Lemma 5.3.14 we obtain a nice characterisation for the quantum join of a set of orthogonal states involving probabilities, which we show in the following corollary.

1	$\bigwedge_{i<j<n+1}(b_i \perp b_j) \to (b_n \perp \bigsqcup_{i<n} b_i)$	Cor. 5.3.8
2	$\Pr(\bigsqcup_{i<n+1} b_i) = \Pr((\bigsqcup_{i<n} b_i) \sqcup b_n)$	Abb.
3	$(b_n \perp \bigsqcup_{i<n} b_i) \to (\Pr((\bigsqcup_{i<n} b_i) \sqcup b_n) = \Pr(\bigsqcup_{i<n} b_i) + \Pr(b_n))$	P5
4	$\bigwedge_{i<j<n}(b_i \perp b_j) \to \Pr(\bigsqcup_{i<n} b_i) = \sum_{i<n} \Pr(b_i)$	(IH)
5	$\bigwedge_{i<j<n+1}(b_i \perp b_j) \to \Pr(\bigsqcup_{i<n+1} b_i) = \sum_{i<n+1} \Pr(b_i)$	I1–I3

Figure 5.12: A proof of $\vdash (\bigwedge\limits_{i<j<n} b_i \perp b_j) \to (\Pr(\bigsqcup\limits_{i\leq n} b_i) = \sum\limits_{i<n} \Pr(b_i))$.

Corollary 5.3.15. *For all finite n the following formula is deducible.*

$$\vdash \bigwedge_{i<j\leq n} (b_i \perp b_j) \to ((\bigsqcup_{i<n} b_i) \equiv (\sum_{i<n} \Pr(b_i) = 1)).$$

Proof. For $n \geq 2$ we know $\vdash T(\bigsqcup_{i<n} b_i)$ is derivable by Lemma 5.3.6, so by Lemma 5.3.12-(5.25), we have $\vdash (\Pr(\bigsqcup_{i\leq n} b_i) = 1) \leftrightarrow \bigsqcup_{i\leq n} b_i$. By lemma 5.3.14, we know

$$\vdash \left(\bigwedge_{i<j\leq n} b_i \perp b_j\right) \to \Pr(\bigsqcup_{i\leq n} b_i) = \sum_{i\leq n} \Pr(b_i).$$

Combining these results we get our desired result. □

Similar to axiom P5, we can generalise axiom P7 by considering the quantum join of a finite set of formulas.

Lemma 5.3.16. *The following formula is deducible.*

$$\vdash \langle \bigsqcup_{i\leq n} b_i? \rangle_{=\rho} \bigwedge_{i\leq n} (\Pr(b_i) = \rho_i) \to \bigwedge_{i\leq n} (\Pr(b_i) = \rho\rho_i)$$

Proof. By modal logic we have

$$\vdash \langle \bigsqcup_{i\leq n} b_i? \rangle_{=\rho} \bigwedge_{i\leq n} (\Pr(b_i) = \rho_i) \to \bigwedge_{i\leq n} \langle \bigsqcup_{i\leq n} b_i? \rangle_{=\rho} (\Pr(b_i) = \rho_i).$$

By Lemma 5.3.7-(5.13), we also know $\vdash b_i \leq \bigsqcup_{j\leq n} b_j$, so the statement follows from axiom P7 and propositional logic. □

5.3.3 Deducible properties of a basis.

Since the notion of an orthonormal basis is very important in the two protocols that we will discuss in Section 5.4, as well as many other protocols, we discuss the definition of a basis and prove several properties.

Let $\mathfrak{M}$ be an N-PQM and let $\mathcal{B}$ be a finite set of formulas. The set $\mathcal{B}$ is called an orthosubbasis of $\mathfrak{M}$ if the following formula is satisfied in $\mathfrak{M}$:

$$\mathsf{SubBasis}(\mathcal{B}) \overset{\text{def}}{=} \bigwedge_{b\in\mathcal{B}} (b \not\equiv \mathtt{ff}) \wedge \bigwedge_{b\neq b'\in\mathcal{B}} (b \perp b') \wedge (\bigsqcup_{b\in\mathcal{B}} b \equiv \mathtt{tt}).$$

In the following lemma we show that the probabilities of elements in an orthosubbasis $\mathcal{B}$ add up to 1.

Lemma 5.3.17. *For a finite set of formulas $\mathcal{B}$ the following formula is deducible.*

$$\vdash \mathit{SubBasis}(\mathcal{B}) \to \sum_i \Pr(b_i) = 1.$$

Proof. This lemma follows directly from the definition of an orthosubbasis combined with Lemma 5.3.14 and axiom $\mathsf{P1}$. □

An orthosubbasis $\mathcal{B}$ is an orthobasis if any proper superset of $\mathcal{B}$ is not a subbasis. This happens precisely when $\mathcal{B}$ consists only of atoms.

$$\mathsf{Basis}(\mathcal{B}) \overset{\text{def}}{=} \mathsf{SubBasis}(\mathcal{B}) \wedge \bigwedge_{b \in \mathcal{B}} \mathrm{At}(b).$$

We are going to show that each basis has the same number of elements. In order to show this, we will first show that within a quantum join we can replace one atom p by another atom q without changing the quantum join $p \sqcup r$, so long as these two atoms are "close" enough (q is also under the join, but not under r).

Lemma 5.3.18. *The following formula is deducible.*

$$\vdash (\mathrm{At}(p) \wedge \mathrm{At}(q) \wedge T(r) \wedge (q \leq (p \sqcup r)) \wedge (q \nleq r)) \to ((p \sqcup r) \equiv (q \sqcup r))$$

Proof. Let us abbreviate the antecedent with

$$\mathsf{Ant} := \mathrm{At}(p) \wedge \mathrm{At}(q) \wedge T(r) \wedge (q \leq (p \sqcup r)) \wedge (q \nleq r).$$

By Lemma 5.3.7-(5.13), we know $\vdash r \leq (p \sqcup r)$ and together with the assumption $q \leq (p \sqcup r)$ from the antecedent and $\vdash T(p \sqcup r)$ by Lemma 5.3.6, we get $\vdash \mathsf{Ant} \to (q \sqcup r \leq p \sqcup r)$ by Lemma 5.3.7-(5.19). As $\vdash \mathsf{Ant} \to (q \nleq r)$ we get by basic reasoning $\vdash \mathsf{Ant} \to (q \sqcup r \nleq r)$, and by the above $\vdash \mathsf{Ant} \to (p \sqcup r \nleq r)$. Thus $\vdash \mathsf{Ant} \to (p \nleq r)$.

Because $\vdash \mathsf{Ant} \to T(r)$ we have $\vdash \mathsf{Ant} \to (p \nleq r \leftrightarrow p \nleq {\sim}{\sim}r)$. Hence, we have $\vdash \mathsf{Ant} \to (p \nleq {\sim}{\sim}r)$. Unpacking the notation, this is equivalent to $\vdash \mathsf{Ant} \to \exists(p \wedge \Diamond{\sim}r)$. Because $\vdash \mathsf{Ant} \to \mathrm{At}(p)$, we find that $\vdash \mathsf{Ant} \to (\exists(p \wedge \Diamond{\sim}r) \leftrightarrow (p \leq \Diamond{\sim}r))$ by $\mathsf{A2}$. Hence, $\vdash \mathsf{Ant} \to (p \leq \Diamond{\sim}r)$.

Since $\vdash \mathsf{Ant} \to ((q \sqcup r) \leq (p \sqcup r))$, we know that $\vdash \mathsf{Ant} \to (((q \sqcup r) \wedge {\sim}r) \leq ((p \sqcup r) \wedge {\sim}r))$. Applying $\mathsf{A1}$ and $\mathsf{A3}$ we obtain $\vdash \mathsf{Ant} \to (((q \sqcup r) \wedge {\sim}r) \equiv ((p \sqcup r) \wedge {\sim}r))$. Now we can apply weak modularity (Corollary 5.3.10) to get the desired result.

$$\vdash \mathsf{Ant} \to (q \sqcup r) \equiv (r \sqcup ((q \sqcup r) \wedge {\sim}r)) \equiv (r \sqcup ((p \sqcup r) \wedge {\sim}r)) \equiv (p \sqcup r).$$

□

The following lemma uses the previous lemma to establish that a quantum join of n formulas can contain at most n orthogonal states.

Lemma 5.3.19. *For any finite n and any set $\mathcal{B}$ of size n and any set $\mathcal{C}$ of finite size $m > n$, the following is deducible.*

$$\vdash (\bigwedge_{a \in \mathcal{B} \cup \mathcal{C}} \mathrm{At}(a) \wedge \bigwedge_{c \neq c' \in \mathcal{C}} (c \perp c')) \to \bigvee_{c \in \mathcal{C}} (c \not\leq \bigsqcup \mathcal{B}).$$

Proof. We prove this by induction on n. For $n = 1$, the formula follows immediately from A1 and Lemma 5.3.4.

Suppose the formula holds true for any set $\mathcal{B}$ of size smaller than n and any set $\mathcal{C}$ of size bigger than the size of $\mathcal{B}$ (IH). Consider the following formula (which is the negation of the desired formula):

$$\chi \overset{\text{def}}{=} \bigwedge_{a \in \mathcal{B} \cup \mathcal{C}} \mathrm{At}(a) \wedge \bigwedge_{c \neq c' \in \mathcal{C}} (c \perp c')) \wedge \bigwedge_{c \in \mathcal{C}} (c \leq \bigsqcup \mathcal{B}).$$

It suffices to prove $\vdash \chi \to \mathtt{ff}$. Take any order on $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$. We will use Lemma 5.3.18 to replace each b by a c one by one, such that the quantum join remains the same.

First step, remove b_0: By the induction hypothesis (IH) and propositional logic, there exists a $c_0 \in \mathcal{C}$ such that $\vdash \chi \to c_0 \not\leq \bigsqcup \mathcal{B} \setminus \{b_0\}$. Given that $c_0 \leq \bigsqcup \mathcal{B}$, $\mathrm{At}(b_0)$ and $\mathrm{At}(c_0)$ are also provable from χ, we can apply Lemma 5.3.18 and obtain $\vdash \chi \to (\bigsqcup \mathcal{B} \equiv (\bigsqcup(\mathcal{B} \setminus \{b_0\}) \sqcup \{c_0\}))$.

Steps 2–n. Suppose we have a set $\mathcal{C}'$ of l elements such that for $\mathcal{B}' = \{b_l, \ldots, b_{n-1}\}$ we have

$$\vdash \chi \to (\bigsqcup \mathcal{B} \equiv (\bigsqcup \mathcal{B}' \sqcup \bigsqcup \mathcal{C}')).$$

Now we remove b_l and obtain a $c_l \in \mathcal{C} \setminus \mathcal{C}'$ in a completely similar way as in step 1, such that

$$\vdash \chi \to (\bigsqcup \mathcal{B} \equiv (\bigsqcup(\mathcal{B}' \setminus \{b_l\}) \sqcup \bigsqcup(\mathcal{C}' \cup \{c_l\}))).$$

Final step. After n steps we have a set $\mathcal{C}' \subsetneq \mathcal{C}$ such that $\vdash \chi \to (\bigsqcup \mathcal{B} \equiv \bigsqcup \mathcal{C}')$. We know there exists a $c \in \mathcal{C} \setminus \mathcal{C}'$ for which we have $\vdash \chi \to \bigwedge_{c' \in \mathcal{C}'} c \perp c'$ and therefore by Corollary 5.3.8, we have $\vdash \chi \to (c \perp \bigsqcup \mathcal{C}')$, which means $\vdash \chi \to (c \not\leq \bigsqcup \mathcal{B})$. Recall that $c \leq \bigsqcup \mathcal{B}$ is a conjunct of χ. Thus $\vdash \chi \to \mathtt{ff}$. □

Now we can show that each basis contains the same number of atoms.

Theorem 5.3.20. *For any two finite sets of formulas $\mathcal{B}$ and $\mathcal{C}$ such that $|\mathcal{B}| = |\mathcal{C}|$ the following formula is deducible.*

$$\vdash \mathsf{Basis}(\mathcal{B}) \wedge \bigwedge_{c \in \mathcal{C}} \left(\mathrm{At}(c) \wedge \bigwedge_{c' \in \mathcal{C} \setminus \{c\}} (c \perp c') \right) \to \mathsf{Basis}(\mathcal{C}).$$

Proof. We first abbreviate the antecedent with:

$$\mathsf{Ant} := \mathsf{Basis}(\mathcal{B}) \wedge \bigwedge_{c \in \mathcal{C}} \left(\mathrm{At}(c) \wedge \bigwedge_{c' \in \mathcal{C} \setminus \{c\}} (c \perp c') \right).$$

We wish to show that $\vdash \mathsf{Ant} \rightarrow \mathsf{Basis}(\mathcal{C})$. As many conditions for $\mathcal{C}$ to be a basis are already in Ant, it suffices to show that $\vdash \mathsf{Ant} \rightarrow (\bigsqcup \mathcal{C} \equiv \mathtt{tt})$. Since $\vdash \mathsf{Ant} \rightarrow \mathsf{Basis}(\mathcal{B})$, it suffices to show $\vdash \mathsf{Ant} \rightarrow (\bigsqcup \mathcal{C} \equiv \bigsqcup \mathcal{B})$. To prove this, we follow a similar construction as was given in the inductive step for Lemma 5.3.19. We enumerate $\mathcal{B} = \{b_0, \ldots, b_{n-1}\}$, and will replace these elements with elements of $\mathcal{C}$ one by one.

First step, remove b_0: by Lemma 5.3.19, there is a $c_0 \in \mathcal{C}$, such that $\vdash \mathsf{Ant} \rightarrow c_0 \not\leq \bigsqcup \mathcal{B} \setminus \{b_0\}$. Just as we did in the proof of Lemma 5.3.19, we then apply Lemma 5.3.18 and obtain $\vdash \mathsf{Ant} \rightarrow (\bigsqcup \mathcal{B} \equiv (\bigsqcup(\mathcal{B} \setminus \{b_0\}) \sqcup \{c_0\}))$. Note that the only difference between this step and that of the proof of Lemma 5.3.19 is that we applied Lemma 5.3.19 directly rather than used induction. Steps 2–n differ from those of Lemma 5.3.19 in precisely the same way.

In the final step we have obtained a set $\mathcal{C}' \subseteq \mathcal{C}$ such that $\vdash \mathsf{Ant} \rightarrow (\bigsqcup \mathcal{B} \equiv \bigsqcup \mathcal{C}')$ and $|\mathcal{B}| = |\mathcal{C}'|$. But we know that $|\mathcal{C}| = |\mathcal{B}|$ and therefore $\mathcal{C} = \mathcal{C}'$ (thus instead of a contradiction we get the desired result). □

Corollary 5.3.21. *If $\mathfrak{M} \models \mathsf{Basis}(\mathcal{B})$ and $\mathfrak{M} \models \mathsf{Basis}(\mathcal{C})$ then $|\mathcal{B}| = |\mathcal{C}|$.*

For most protocols we do not just require a basis for the whole system, but a basis for each local subsystem. In those cases the basis for the whole system will be the tensor product of the basis for the local subsystems. We will refer to these basis as locally orthogonal (fully) separable orthobasis (LOSB), which can be expressed by

$$\begin{aligned} \mathsf{LOSB}(\mathcal{B}) \stackrel{\text{def}}{=} \mathsf{Basis}(\mathcal{B}) \wedge \bigwedge_{b \in \mathcal{B}} \mathsf{Sep}(b) \wedge \bigwedge_{i<N} \bigwedge_{b \in \mathcal{B}} \bigvee_{c \in \mathcal{B}} (b_{\{i\}} \not\equiv c_{\{i\}}) \\ \wedge \bigwedge_{i<N} \bigwedge_{b \in \mathcal{B}} \bigwedge_{c \in \mathcal{B}} (b_{\{i\}} \equiv c_{\{i\}} \vee b_{\{i\}} \perp c_{\{i\}}). \end{aligned}$$

The second to last conjunct of the four conjuncts asserts that each local component has dimension at least two, and the last conjunct asserts that local components that are not equal must be orthogonal.

The following lemma states that any LOSB $\mathcal{B}$ is the tensor product of its local states.

Lemma 5.3.22. *For a finite set of formulas $\mathcal{B}$, Let $\mathcal{B}^N$ be the set of functions from $\{0, \ldots, N-1\}$ to $\mathcal{B}$. The following formula is deducible:*

$$\vdash \mathit{LOSB}(\mathcal{B}) \rightarrow \bigwedge_{f \in \mathcal{B}^N} \bigvee_{b \in \mathcal{B}} \bigwedge_{i<N} (b_{\{i\}} \equiv f(i)_{\{i\}}).$$

Proof. Let χ be the negation of what we are trying to prove:

$$\chi := \mathsf{LOSB}(\mathcal{B}) \wedge \neg \left(\bigwedge_{f \in \mathcal{B}^N} \bigvee_{b \in \mathcal{B}} \bigwedge_{i<N} (b_{\{i\}} \equiv f(i)_{\{i\}}) \right).$$

It suffices to show that $\vdash \chi \to \mathtt{ff}$. First note that

$$\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} \bigvee_{i<N} (b_{\{i\}} \not\equiv f(i)_{\{i\}})).$$

Furthermore by definition of LOSB and propositional logic, for every $f \in \mathcal{B}^N$ and $b \in \mathcal{B}$,

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to ((b_{\{i\}} \not\equiv f(i)_{\{i\}}) \to (b_{\{i\}} \perp f(i)_{\{i\}})).$$

Thus

$$\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} \bigvee_{i<N} (b_{\{i\}} \perp f(i)_{\{i\}})).$$

By $\mathsf{A6}$ we have $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} \bigwedge_{b \in \mathcal{B}} (b \perp f(i)))$. Then by Lemma 5.3.8, $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (f(i) \perp \bigsqcup \mathcal{B}))$. Written another way, we have $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (\bigsqcup \mathcal{B} \leq {\sim} f(i)))$.

By modal reasoning $\vdash \mathtt{tt} \equiv {\sim}\mathtt{ff}$ and by Lemma 5.3.5-(5.7), $\vdash (\phi \not\equiv \mathtt{ff}) \leftrightarrow ({\sim}\phi \not\equiv \mathtt{tt})$. As for each $i < N$, $f(i) \in \mathcal{B}$ and $f(i) \not\equiv \mathtt{ff}$ is a conjunct of $\mathsf{SubBasis}(\mathcal{B})$ and hence a conjunct of χ, we have that $\vdash \chi \to ({\sim} f(i) \not\equiv \mathtt{tt})$. As $\vdash (\phi \leq \psi) \wedge (\psi \neq \mathtt{tt}) \to (\phi \neq \mathtt{tt})$, we have from this and $\vdash \chi \to (\bigvee_{f \in \mathcal{B}^N} (\bigsqcup \mathcal{B} \leq {\sim} f(i)))$ that $\vdash \chi \to (\bigsqcup \mathcal{B} \neq \mathtt{tt})$. This together with the fact that $\bigsqcup \mathcal{B} = \mathtt{tt}$ is a conjunct of $\mathsf{SubBasis}(\mathcal{B})$ and hence of χ gives us that $\vdash \chi \to \mathtt{ff}$. □

Given two LOSBs $\mathcal{B}$ and $\mathcal{C}$, we can construct a new LOSB $\mathcal{D}$, such that for all $i < N$, either for all $d \in \mathcal{D}$ we have $d_{\{i\}} \equiv b_{\{i\}}$ for some $b \in \mathcal{B}$ or for all $d \in \mathcal{D}$ we have $d_{\{i\}} \equiv c_{\{i\}}$ for some $c \in \mathcal{C}$. The following lemma proves this fact.

Lemma 5.3.23. *Let $\mathcal{B}, \mathcal{C}$ and $\mathcal{D}$ be three sets of proposition letters of equal size, i.e. $|\mathcal{B}| = |\mathcal{C}| = |\mathcal{D}|$. The following formula is deducible:*

$$\vdash \mathit{Ant} \to \mathit{LOSB}(\mathcal{D}).$$

where

$$\mathit{Ant} \overset{def}{=} \mathit{LOSB}(\mathcal{B}) \wedge \mathit{LOSB}(\mathcal{C}) \wedge \bigwedge_{d \in \mathcal{D}} \mathsf{Sep}(d) \wedge \bigwedge_{d \neq d' \in \mathcal{D}} d \not\equiv d'$$
$$\wedge \bigwedge_{i<N} \left((\bigwedge_{d \in \mathcal{D}} \bigvee_{b \in \mathcal{B}} d_{\{i\}} \equiv b_{\{i\}}) \vee (\bigwedge_{d \in \mathcal{D}} \bigvee_{c \in \mathcal{C}} d_{\{i\}} \equiv c_{\{i\}}) \right)$$

Proof. In order to show $\vdash \mathsf{Ant} \to \mathsf{LOSB}(\mathcal{D})$ it suffices to show that $\mathsf{Basis}(\mathcal{D})$, $\bigwedge_{d\in\mathcal{D}} \mathsf{Sep}(d)$,

$$\bigwedge_{i<N} \bigwedge_{d\in\mathcal{D}} \bigwedge_{d'\in\mathcal{D}} \Big((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d'_{\{i\}})\Big), \tag{5.27}$$

and

$$\bigwedge_{i<N} \bigwedge_{d\in\mathcal{D}} \bigvee_{d'\in\mathcal{D}} (d_{\{i\}} \not\equiv d'_{\{i\}}) \tag{5.28}$$

are provable from Ant.

By extracting a conjunct from Ant, we already have $\vdash \mathsf{Ant} \to \bigwedge_{d\in\mathcal{D}} \mathsf{Sep}(d)$.

As an intermediate step, we show that $\vdash \mathsf{Ant} \to \bigwedge_{d\in\mathcal{D}} \mathrm{At}(d)$. By axiom $\mathsf{A4}$ we have $\vdash \mathsf{Ant} \to T(b_{\{i\}})$ and $\vdash \mathsf{Ant} \to T(c_{\{i\}})$ for all $b \in \mathcal{B}$, $c \in \mathcal{C}$ and $i < N$. As Ant asserts the equivalence of each $d_{\{i\}}$ with either $b_{\{i\}}$ or $c_{\{i\}}$, propositional reasoning gives us $\vdash \mathsf{Ant} \to T(d_{\{i\}})$ for all $d \in \mathcal{D}$ and $i < N$. So, by axiom $\mathsf{A4}$, we have $\vdash \mathsf{Ant} \to \mathrm{At}(d)$ for all $d \in \mathcal{D}$.

We next show that (5.27) is provable from Ant. By propositional logic, using the conjunct for $\mathsf{LOSB}(\mathcal{B})$ and for $\mathsf{LOSB}(\mathcal{C})$, we have

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} (\chi(\mathcal{B}) \vee \chi(\mathcal{C})),$$

where

$$\chi(\mathcal{B}) := \bigwedge_{d,d'\in\mathcal{D}} \bigvee_{b,b'\in\mathcal{B}} ((d_{\{i\}} \equiv b_{\{i\}}) \wedge (d'_{\{i\}} \equiv b'_{\{i\}}) \wedge ((b_{\{i\}} \equiv b'_{\{i\}}) \vee (b_{\{i\}} \perp b_{\{i\}}))).$$

Then by modal logic we have

$$\vdash \chi(\mathcal{B}) \to \bigwedge_{d,d'\in\mathcal{D}} ((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d_{\{i\}}))$$

and similarly

$$\vdash \chi(\mathcal{C}) \to \bigwedge_{d,d'\in\mathcal{D}} ((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d_{\{i\}}))$$

Putting these together, we obtain by propositional logic

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} \bigwedge_{d\in\mathcal{D}} \bigwedge_{d'\in\mathcal{D}} \Big((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d'_{\{i\}})\Big)$$

To show $\vdash \mathsf{Ant} \to \mathsf{Basis}(\mathcal{D})$, by Theorem 5.3.20, it remains to show that $\vdash \mathsf{Ant} \to \bigwedge_{d\neq d'\in\mathcal{D}} d \perp d'$. For each $d, d' \in \mathcal{D}$, because $\mathsf{Sep}(d)$ is a conjunct of Ant for each $d \in \mathcal{D}$, and because $\vdash \mathsf{Ant} \to \bigwedge_{d\in\mathcal{D}} \mathrm{At}(d)$, we apply axiom $\mathsf{A5}$ to get

$$\vdash \mathsf{Ant} \to \bigwedge_{d,d'\in\mathcal{D}} ((d \equiv d') \leftrightarrow \bigwedge_{i} (d_{\{i\}} \equiv d'_{\{i\}})).$$

Then

$$\vdash \mathsf{Ant} \to \bigwedge_{d\neq d'\in\mathcal{D}} \bigvee_{i} (d_{\{i\}} \not\equiv d'_{\{i\}}).$$

Because

$$\vdash \mathsf{Ant} \to \bigwedge_{d\in\mathcal{D}} \bigwedge_{d'\in\mathcal{D}} \bigwedge_{i<N} \Big((d_{\{i\}} \equiv d'_{\{i\}}) \vee (d_{\{i\}} \perp d'_{\{i\}})\Big),$$

we have by propositional logic

$$\vdash \mathsf{Ant} \to \bigwedge_{d\neq d'\in\mathcal{D}} \bigvee_{i} (d_{\{i\}} \perp d'_{\{i\}})$$

Thus by axiom $\mathsf{A6}$, $\vdash \mathsf{Ant} \to \bigwedge_{d\neq d'\in\mathcal{D}}(d \perp d')$.

To show (5.28), let us fix an $i < N$ and let $\phi(i, \mathcal{B})$ be

$$\phi(i,\mathcal{B}) := \bigvee_{d\in\mathcal{D}} \bigwedge_{d'\in\mathcal{D}} (d_{\{i\}} \equiv d'_{\{i\}}) \wedge \bigwedge_{d\in\mathcal{D}} \bigvee_{b\in\mathcal{B}} (d_{\{i\}} \equiv b_{\{i\}}).$$

So for a fixed i we assume the negation of (5.28) and we assume all $d \in \mathcal{D}$ are equal to some $b \in \mathcal{B}$ at location i. We wish to show $\vdash \mathsf{Ant} \wedge \phi(i, \mathcal{B}) \to \mathtt{ff}$.

By definition of $\equiv$ and modal reasoning, the first conjunct of $\phi(i, \mathcal{B})$ implies $\bigwedge_{d,d'\in\mathcal{D}}(d_{\{i\}} \equiv d'_{\{i\}})$, that is, all $d \in \mathcal{D}$ are locally equivalent at location i. Combined with the second conjunct we get

$$\vdash \mathsf{Ant} \wedge \phi(i,\mathcal{B}) \to \bigvee_{b\in\mathcal{B}} \bigwedge_{d\in\mathcal{D}} (d_{\{i\}} \equiv b_{\{i\}}).$$

As $\mathsf{LOSB}(\mathcal{B})$ is a conjunct of Ant, we have

$$\bigwedge_{b\in\mathcal{B}} \bigvee_{b'\in\mathcal{B}} (b_{\{i\}} \not\equiv b'_{\{i\}}).$$

Moreover, we have

$$\bigwedge_{b,b'\in\mathcal{B}} \Big((b_{\{i\}} \equiv b'_{\{i\}}) \vee (b_{\{i\}} \perp b'_{\{i\}})\Big).$$

Using propositional reasoning we obtain

$$\vdash \mathsf{Ant} \wedge \phi(i,\mathcal{B}) \to \bigvee_{b\in\mathcal{B}} \bigwedge_{d\in\mathcal{D}} (d_{\{i\}} \perp b_{\{i\}}).$$

By axiom $\mathsf{A6}$, this implies

$$\vdash \mathsf{Ant} \wedge \phi(i,\mathcal{B}) \to \bigvee_{b\in\mathcal{B}} \bigwedge_{d\in\mathcal{D}} (d \perp b).$$

Now we can apply Corollary 5.3.8

$$\vdash \mathsf{Ant} \wedge \phi(i,\mathcal{B}) \to \bigvee_{b\in\mathcal{B}} (b \perp \bigsqcup \mathcal{D}).$$

We have already shown that $\vdash \mathsf{Ant} \to \mathsf{Basis}(\mathcal{D})$, and as $\bigsqcup \mathcal{D} \equiv \mathtt{tt}$ is a conjunct of $\mathsf{Basis}(\mathcal{D})$ we conclude

$$\vdash \mathsf{Ant} \wedge \phi(i,\mathcal{B}) \to \mathtt{ff}.$$

We can show this result for any $i < N$ and replacing $\mathcal{B}$ by $\mathcal{C}$. As a result we get

$$\vdash \mathsf{Ant} \wedge \bigvee_{i<N} \bigvee_{d\in\mathcal{D}} \bigwedge_{d'\in\mathcal{D}} (d_{\{i\}} \equiv d'_{\{i\}}) \to \mathtt{ff}.$$

This is equivalent to the desired result:

$$\vdash \mathsf{Ant} \to \bigwedge_{i<N} \bigwedge_{d\in\mathcal{D}} \bigvee_{d'\in\mathcal{D}} (d_{\{i\}} \not\equiv d'_{\{i\}}).$$

□

5.4 Examples

In this section we will discuss how to express and prove correctness for two quantum protocols: the quantum leader election protocol (Section 5.4.1) and the BB84 quantum key distribution protocol (Section 5.4.2).

5.4.1 Example 1: Quantum Leader Election

The quantum leader election protocol aims to randomly select a leader in a group of agents such that each agent has equal probability to be selected as the leader. There exists several ways to solve this problem using quantum theory, e.g. [47, 98]. The ones given in [98] rely heavily on communication, and as we do not explicitly model communication, we will discuss the version given in [47], which omits explicit communication.

Given a set N of agents, the protocol assigns a quantum bit (a two dimensional Hilbert space) to each agent $i \in N$ together with a basis $\{|0\rangle_i, |1\rangle_i\}$. Then the following state, called the W-state, is considered:

$$\sum_{i\in N} \frac{1}{\sqrt{N}} \left(\bigotimes\nolimits^{\mathfrak{M}}_{j\in N\setminus\{i\}} |0\rangle_j \right) \otimes^{\mathfrak{M}} |1\rangle_i .$$

This state entangles the qubits in such a way that, after the agents measure their qubit, only one agent measures $|1\rangle$ and all other agents measure $|0\rangle$.

In our logic, we express and prove the existence of the W-state, showing that it has the desired probabilistic behaviour. Our formula for correctness applies not only to the case where each agent has a qubit, but where each agent has a Hilbert space with dimension at least 2 (no smaller than a qubit). We could alternatively have enforced the property that each agent has precisely one qubit using as a conjunct

$$\mathsf{LOSB}(\mathcal{B}) \to \bigwedge_{i<N} \bigwedge_{b,c,d\in\mathcal{B}} \Big((b_{\{i\}} \perp c_{\{i\}}) \to \Big((d_{\{i\}} \equiv b_{\{i\}}) \vee (d_{\{i\}} \equiv c_{\{i\}}) \Big) \Big),$$

and the proofs in this section would have been essentially the same.

Let $\mathcal{B}$ be a LOSB. Then an ordered subset $\mathcal{W} = \{W^i \mid i \in N+1\} \subset \mathcal{B}$ is *Quantum Leader Election compatible* (QLE compatible) if the following formula is satisfied (somewhere in) $\mathfrak{M}$:

$$\mathrm{QLE}(\mathcal{W}) \overset{\text{def}}{=} \bigwedge_{i\in N} \left((W^i_{\{i\}} \not\equiv W^N_{\{i\}}) \wedge \bigwedge_{j \in N\setminus i} (W^i_{\{j\}} \equiv W^N_{\{j\}}) \right).$$

We interpret this formula as follows. The last element W^N should be seen as the tensor product $\bigotimes^{\mathfrak{M}}_{i\in N} \mathbf{0}_i$, where $\mathbf{0}_i$ is the qubit for agent i corresponding to the classical bit 0 (one of the basis elements of the qubit). For $i < N$, the element W^i is similarly a tensor product of classical bits, where each component $k \neq i$ is similarly $\mathbf{0}_k$, but where component $k = i$ is $\mathbf{1}_k$ instead. Note that we are interpreting basis elements of the components as classical bits, rather than defining the basis elements of the components with respect to pre-determined classical bits.

The *correctness* of the quantum leader election is expressed by

$$\mathsf{QLE\text{-}Cor}(\mathcal{B}) \overset{\text{def}}{=} \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \left(\mathsf{QLE}(\mathcal{W}) \wedge \exists \bigwedge_{i<N} \Pr(W^i) = \frac{1}{N} \right),$$

where $\mathcal{W} \subset_{N+1} \mathcal{B}$ ranges over all subsets $\{W^0, \dots, W^N\}$ of $\mathcal{B}$ of size $N+1$.

We will first show that for any set $\mathcal{B} = \{b_0, \dots, b_{n-1}\}$ of n pairwise orthogonal properties we have a state that has probability $\frac{1}{n}$ for each property in $\mathcal{B}$. Let us define

$$\mathsf{Ort}(\mathcal{B}) \overset{\text{def}}{=} \bigwedge_{i<n} (T(b_i) \wedge (b_i \not\equiv \mathtt{ff})) \wedge \bigwedge_{i<j<n} b_i \perp b_j.$$

Proposition 5.4.1. *For all $n \geq 1$ and for any set $\mathcal{B} = \{b_0, \dots, b_{n-1}\}$ of n formulas, the following formula is deducible.*

$$\vdash \mathsf{Ort}(\mathcal{B}) \to \exists \left(\bigwedge_{i\in n} \Pr(b_i) = \frac{1}{n} \right).$$

Proof. With induction: for $n = 1$ we have $\vdash \mathsf{Ort}(\mathcal{B}) \to (b \not\equiv \mathtt{ff})$, which by Lemma 5.3.4 implies $\vdash \mathsf{Ort}(\mathcal{B}) \to \exists b$. By Lemma 5.3.12-(5.26), we have $\vdash b \to \Pr(b) = 1$, so we have $\vdash \mathsf{Ort} \to \exists(\Pr(b) = 1)$, which finishes the case $n = 1$.

Induction hypothesis (IH): suppose for n we have

$$\vdash \mathsf{Ort}(\mathcal{B}_n) \to \exists (\bigwedge_{i\in n} \Pr(b_i) = \frac{1}{n}).$$

Let $\mathcal{B}_{n+1} = \mathcal{B}_n \cup \{b_n\}$. In Figure 5.13 we show how to deduce

$$\vdash \mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\bigwedge_{i \leq n+1} \Pr(b_i) = \frac{1}{n+1} \right)$$

□

1	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists b_n$	Lem. 5.3.4
2	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}\right)$	IH
3	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (b_n \perp \bigsqcup_{i\in n} b_i)$	Cor. 5.3.8
4	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}) \leq (\bigsqcup_{i<n} b_i)$	Cor. 5.3.15
5	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to (b_n \perp (\bigwedge_{i<n} \Pr(b_i) = \frac{1}{n})$	ML(3,4)
6	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\langle b_n?\rangle_{=\frac{1}{n+1}} b_n \wedge \langle q?\rangle_{=\frac{n}{n+1}} q\right)$	
	with $q = \bigwedge_{i<n} \Pr(b_i) = \frac{1}{n}$	P6
7	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\Pr(b_n) = \frac{1}{n+1} \wedge \bigwedge_{i<n} \Pr(b_i) = \frac{1}{n+1})\right)$	Lem. 5.3.16
8	$\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists \left(\bigwedge_{i\leq n+1} \Pr(b_i) = \frac{1}{n+1}\right)$	PL(8)

Figure 5.13: A proof of $\mathsf{Ort}(\mathcal{B}_{n+1}) \to \exists(\bigwedge\limits_{i\leq n+1} \Pr(b_i) = \frac{1}{n+1})$.

The following theorem proves the correctness of the quantum leader election.

Theorem 5.4.2. *For any finite set of formulas $\mathcal{B}$, the following formula is deducible: $\vdash$ $\mathsf{QLE\text{-}Cor}(\mathcal{B})$, that is,*

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \left(\mathsf{QLE}(\mathcal{W}) \wedge \exists \bigwedge_{i<N} \Pr(W^i) = \frac{1}{N}\right),$$

where $\mathcal{W} \subset_{N+1} \mathcal{B}$ ranges over all subsets $\{W^0, \ldots, W^N\}$ of $\mathcal{B}$ of size $N+1$.

Proof. For any $\mathcal{W} = \{W^0, \ldots, W^N\} \subset_{N+1} \mathcal{B}$ we can extract conjuncts from $\mathsf{LOSB}(\mathcal{B})$ and apply Lemma 5.3.11 to obtain $\vdash \mathsf{LOSB}(\mathcal{B}) \to \mathsf{Ort}(\mathcal{W})$. It is easy to see that for any $\mathcal{W}' \subset_N \mathcal{W}$, we have that $\vdash \mathsf{Ort}(\mathcal{W}) \to \mathsf{Ort}(\mathcal{W}')$. Thus by this and Proposition 5.4.1, we have for any $\mathcal{W} \subset_{N+1} \mathcal{B}$

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \exists \left(\bigwedge_{i<N} \Pr(W^i) = \frac{1}{N}\right). \tag{5.29}$$

To show that $\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \mathsf{QLE}(\mathcal{W})$, we select any $b \in \mathcal{B}$ to be W^N. Note that

$$\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\{b^i \mid i<N\}\subset\mathcal{B}} \left(\bigwedge_{i<N} (b^i_{\{i\}} \not\equiv W^N_{\{i\}})\right). \tag{5.30}$$

For a given set $\mathcal{V} = \{b^i \mid i < N\} \subset \mathcal{B}$ and each $i < N$, let $f^{\mathcal{V}}_i : \{0, \ldots, N-1\} \to \mathcal{B}$, such that $f^{\mathcal{V}}_i(j) = W^N$ if $i \neq j$ and $f^{\mathcal{V}}_i(i) = b^i$. Then for each $i < N$, we can apply Lemma 5.3.22 using $f^{\mathcal{V}}_i$ to obtain a $W^i \in \mathcal{B}$ such that $W^i_{\{i\}} \equiv b^i_{\{i\}} \not\equiv W^N_{\{i\}}$ and $W^i_{\{j\}} \equiv W^N_{\{j\}}$ for any $j \neq i$. By (5.30) we know that for some $\mathcal{V} \subset \mathcal{B}$ the resulting set $\mathcal{W} = \{W^0, \ldots, W^{N-1}, W^N\}$ will be QLE compatible. Hence, by using Lemma 5.3.22 and (5.30), we obtain $\vdash \mathsf{LOSB}(\mathcal{B}) \to \bigvee_{\mathcal{W}\subset_{N+1}\mathcal{B}} \mathsf{QLE}(\mathcal{W})$. The desired result follows from this, (5.29), and propositional logic. □

5.4.2 Example 2: BB84

The BB84 protocol is designed to provide two agents with the same random bitstring, to be used as a key for both encryption and description. The protocol works as follows: the first agent Alice has the ability to produce qubits in two different basis: $\{|0\rangle, |1\rangle\}$ and $\{|-\rangle, |+\rangle\}$. Alice chooses two equally sized random bitstrings; the first is the message to be sent, the second determines the basis in which each individual bit of the message bitstring is sent. She sends the qubits to Bob, who has choosen a random bitstring as well in order to determine which basis he uses to measure each received qubit. After all qubits have been sent and measured, Alice and Bob publicly compare the basis bitstring they have used to create and measure the qubits respectively. On those positions where the basis bitstring matches, the corresponding bit in the message bitstring should correspond as well. On all other positions, those bits in the message bitstring could be different and are thus discarded. In the end, Alice and Bob have a corresponding random bitstring which is in general about half the size of the random bitstring Alice started with. Of course, this is in the ideal situation where no eavesdropper disturbs the channel. This section proves properties of this ideal situation.

We first need to characterize the message space. Let us fix the number of qubits at N and let $\mathfrak{M}$ be the tensor product of N identical two dimensional quantum models. Let $\mathcal{B}_1$ and $\mathcal{B}_+$ be two LOSB's that are locally probabilistically far apart (PFA), that is

$$\begin{aligned}\mathsf{PFA}(\mathcal{B}_1, \mathcal{B}_+) \stackrel{\text{def}}{=} {} & \mathsf{LOSB}(\mathcal{B}_1) \wedge \mathsf{LOSB}(\mathcal{B}_+) \\ & \wedge \bigwedge_{b\in\mathcal{B}_1} \bigwedge_{c\in\mathcal{B}_+} \bigwedge_{i<N} \Big(b \leq (\Pr(c_{\{i\}}) = \frac{1}{2}) \wedge c \leq (\Pr(b_{\{i\}}) = \frac{1}{2}) \Big)\end{aligned}$$

Intuitively, $\mathcal{B}_1$ represents the N tensor product of the local basis $\{|0\rangle, |1\rangle\}$, and $\mathcal{B}_+$ represents the N tensor product of the local basis $\{|-\rangle, |+\rangle\}$. We introduce two new abbreviations for the remainder of this section:

$$\begin{aligned} m_{\{i\}} \in \{0,1\} &\stackrel{\text{def}}{=} \bigvee_{b\in\mathcal{B}_1} m_{\{i\}} \equiv b_{\{i\}}, \\ m_{\{i\}} \in \{-,+\} &\stackrel{\text{def}}{=} \bigvee_{b\in\mathcal{B}_+} m_{\{i\}} \equiv b_{\{i\}}. \end{aligned}$$

The message space $\mathcal{M}$ of 4^N proposition letters can be defined by requiring each proposition to be locally equivalent either to some $b \in \mathcal{B}_1$ or to some $b \in \mathcal{B}_+$.

$$\mathsf{Mes}(\mathcal{M}) \stackrel{\text{def}}{=} \bigwedge_{m\in\mathfrak{M}} \mathsf{Sep}(m) \wedge \bigwedge_{m\in\mathfrak{M}} \left(\bigwedge_{i<N} \bigvee_{a\in\mathcal{B}_1\cup\mathcal{B}_+} (m_{\{i\}} \equiv a_{\{i\}}) \wedge \bigwedge_{m'\in\mathfrak{M}\setminus\{m\}} (m \not\equiv m') \right).$$

Let k be some element of $\mathcal{M}$. This represents Ann's message and choice of basis for each component.

For any string $s \in \{1,+\}^N$, let s_i denote the i'th coordinate. We define the set of propositions $\mathcal{B}_s \subseteq \mathcal{M}$ by

$$\mathcal{B}_s := \Big\{ b \in \mathcal{M} \;\Big|\; b_{\{i\}} \equiv b'_{\{i\}} \text{ for some } b' \in \mathcal{B}_{s_i}\text{and for all } i < N \Big\}.$$

In words, $\mathcal{B}_s$ is the set of formulas where the i'th coordinate of each element b of $\mathcal{B}_s$ is in $\{0,1\}$ if the i'th coordinate of s is 1, and where the i'th coordinate of b in $\{-,+\}$ otherwise. Note that by Lemma 5.3.23, for each $s \in \{1,+\}^N$ the resulting set $\mathcal{B}_s$ is an LOSB.

Furthermore, given a string $s \in \{1,+\}^N$, define the term-abbreviation:

- $\Pr_s(\phi) \overset{\text{def}}{=} \sum_{b\in\mathcal{B}_s} \Pr(b \wedge \phi)$
- $\Pr_{\mathcal{M}}(\phi) \overset{\text{def}}{=} \sum_{s\in\{1,+\}^N} \frac{1}{2^N} \Pr_s(\phi)$

The term $\Pr_s(\phi)$ represents the probability of ϕ holding true after measuring the state using basis $\mathcal{B}_s$, in the event that ϕ is testable (ϕ needs to be testable for this reading to hold). The term $\Pr_{\mathcal{M}}(\phi)$ represents the probability of ϕ holding true after using a randomly selected one of the 2^N chosen bases of states in $\mathcal{M}$.

The correctness of the BB84 protocol, when there is no eavesdropper, can be expressed by

$$\mathsf{Ant} \to \Pr_{\mathcal{M}}(\mathsf{Match}) = 1,$$

where

$$\mathsf{Ant} \overset{\text{def}}{=} \mathsf{PFA}(\mathcal{B}_1, \mathcal{B}_+) \wedge \mathsf{Mes}(\mathcal{M}) \wedge k$$

and Match states that at those coordinates where the choice of basis of Alice and Bob agree, Bob's measured result agrees with Alice's original message k. Formally this is expressed by

$$\mathsf{Match} \overset{\text{def}}{=} \bigwedge_{i<N} \Big(\mathsf{BasisOf}(k_{\{i\}}) \to \bigvee \{ m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}} \} \Big),$$

where

$$\mathsf{BasisOf}(k_{\{i\}}) = \begin{cases} \bigvee\{m \in \mathcal{M} \mid m_{\{i\}} \in \{0,1\}\} & \text{if } k_{\{i\}} \in \{0,1\}, \\ \bigvee\{m \in \mathcal{M} \mid m_{\{i\}} \in \{-,+\}\} & \text{if } k_{\{i\}} \in \{-,+\}. \end{cases}$$

The probability of Match being equal to 1 reflects that without interference Bob should have received Ann's message perfectly among those coordinates where they used the same basis.

Theorem 5.4.3. *The following formula is deducible.*

$$\vdash \mathsf{Ant} \to \Pr_{\mathcal{M}}(\mathsf{Match}) = 1.$$

Proof. We will first show $\vdash \mathsf{Ant} \to \mathrm{Pr}_s(\mathsf{Match}) = 1$ for all $s \in \{1,+\}^N$. The desired result will then follow from the inequality axioms. By Lemma 5.3.23, we know $\vdash \mathsf{Ant} \to \mathsf{LOSB}(\mathcal{B}_s)$, and therefore by Lemma 5.3.17, $\vdash \mathsf{Ant} \to \sum_{b\in\mathcal{B}_s} \mathrm{Pr}(b) = 1$. So to show that $\mathrm{Pr}_{\mathcal{M}}(\mathsf{Match}) = \sum_{s\in\{1,+\}^N} \frac{1}{2^N} \mathrm{Pr}_s(\mathsf{Match}) = 1$ it is enough to show that $\vdash \mathsf{Ant} \to \mathrm{Pr}(b) = \mathrm{Pr}(b \wedge \mathsf{Match})$ for all $b \in \mathcal{M}$.

Let us define

$$\mathsf{Match_i} \stackrel{\text{def}}{=} \Big(\mathsf{BasisOf}(k_{\{i\}}) \to \bigvee\{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\}\Big)\,.$$

Thus $\mathsf{Match} = \bigwedge_{i<N} \mathsf{Match}_i$. We will show that for each $b \in \mathcal{M}$,

$$\vdash \bigwedge_{i<N} (\mathsf{Ant} \to (\mathrm{Pr}(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i)), \tag{5.31}$$

hence

$$\vdash \mathsf{Ant} \to \Bigg(\mathrm{Pr}(b) = 0 \vee (b \equiv (b \wedge \bigwedge_{i<N} \mathsf{Match}_i))\Bigg)$$

Before we prove (5.31), let us show how to proof the main statement of the theorem. By $\mathsf{P4}$, $\vdash$ $(b \equiv (b \wedge \mathsf{Match}) \to \mathrm{Pr}(b) = \mathrm{Pr}(b \wedge \mathsf{Match})$. By Proposition 5.3.13, $\vdash$ $(\mathrm{Pr}(b \wedge \mathsf{Match}) \leq \mathrm{Pr}(b))$. Thus by $\mathsf{P2}$ and inequality axioms $\vdash \mathrm{Pr}(b) = 0 \to \mathrm{Pr}(b) = \mathrm{Pr}(b \wedge \mathsf{Match})$. Hence, from (5.31) we use these steps to arrive at $\vdash \mathsf{Ant} \to \mathrm{Pr}(b) = \mathrm{Pr}(b \wedge \mathsf{Match})$.

To prove (5.31), let us fix an $i < N$. We will discuss several cases, expressed by the following formulas:

$$\begin{aligned}
\phi &\stackrel{\text{def}}{=} (b_{\{i\}} \equiv k_{\{i\}})\\
\psi &\stackrel{\text{def}}{=} (b_{\{i\}} \not\equiv k_{\{i\}}) \wedge (b_{\{i\}} \in \{0,1\} \leftrightarrow k_{\{i\}} \in \{0,1\})\\
\chi &\stackrel{\text{def}}{=} (b_{\{i\}} \not\equiv k_{\{i\}}) \wedge (b_{\{i\}} \in \{0,1\} \leftrightarrow k_{\{i\}} \notin \{0,1\})
\end{aligned}$$

By propositional logic, we have $\vdash \phi \vee \psi \vee \chi$.

Case ϕ: First note that we have

$$\vdash \mathsf{Ant} \wedge \phi \to b \leq \Big(\mathsf{BasisOf}(k_{\{i\}}) \to \bigvee\{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\}\Big)\,,$$

because $\phi = (b_{\{i\}} \equiv k_{\{i\}})$ ensures $b \in \{m \in \mathcal{M} \mid m_{\{i\}} \equiv k_{\{i\}}\}$. Rewriting, we have $\vdash \mathsf{Ant}\wedge\phi \to (b \equiv (b\wedge\mathsf{Match}_i))$. Hence $\vdash \mathsf{Ant}\wedge\phi \to (\mathrm{Pr}(b) = 0\vee(b \equiv (b\wedge\mathsf{Match}_i))$.

Case ψ: By extracting conjuncts from Ant, we have $\vdash \mathsf{Ant} \wedge \psi \to \mathsf{LOSB}(\mathcal{B}_1) \wedge \mathsf{LOSB}(\mathcal{B}_+)$. Expanding ψ, we have

$$\vdash (\mathsf{Ant} \wedge \psi) \to \Big(b_{\{i\}} \in \{0,1\} \wedge k_{\{i\}} \in \{0,1\}\Big) \vee \Big(b_{\{i\}} \in \{-,+\} \wedge k_{\{i\}} \in \{-,+\}\Big)\,.$$

Thus by propositional logic, $\vdash \mathsf{Ant} \wedge \psi \to (b_{\{i\}} \perp k_{\{i\}})$ for each $i < N$. By axiom $\mathsf{A6}$, $\vdash \mathsf{Ant}\wedge\psi \to (b \perp k)$ and therefore by axiom $\mathsf{P3}$, $\vdash \mathsf{Ant}\wedge\psi \to (k \leq \mathrm{Pr}(b) = 0)$. By Lemma 5.3.2-(5.4), $\vdash \mathsf{Ant} \wedge \psi \to \mathrm{Pr}(b) = 0$. Hence $\vdash \mathsf{Ant} \wedge \psi \to ((\mathrm{Pr}(b) = 0) \vee (b \equiv (b \wedge \mathsf{Match}_i))$.

$\mathsf{Case}\ \chi$: By expanding χ, we have

$$\vdash (\mathsf{Ant} \wedge \chi) \to \Big(b_{\{i\}} \notin \{0,1\} \wedge k_{\{i\}} \in \{0,1\}\Big) \vee \Big(b_{\{i\}} \notin \{-,+\} \wedge k_{\{i\}} \in \{-,+\}\Big)\,.$$

By this and modal logic, we have that $\vdash \mathsf{Ant} \wedge \chi \to (b \leq \neg\mathsf{BasisOf}(k_{\{i\}}))$. Thus $\vdash \mathsf{Ant} \wedge \chi \to (b \leq \mathsf{Match}_i)$, which is equivalent to $\vdash \mathsf{Ant} \wedge \chi(b \equiv b \wedge \mathsf{Match}_i)$. Thus $\vdash \mathsf{Ant} \wedge \chi \to (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$.

Now we have $\vdash \mathsf{Ant} \wedge \omega \to (\Pr(b) = 0 \vee (b \equiv (b \wedge \mathsf{Match}_i))$, for each $\omega \in \{\phi, \psi, \chi\}$. Together with $\vdash \phi \vee \psi \vee \chi$, and repeating for each $i < N$, we have (5.31). $\square$

Chapter 6

PLQP & Company: Decidable Logics for Quantum Algorithms

Summary: In this chapter we introduce a probabilistic modal (dynamic and epistemic) quantum logic PLQP for reasoning about quantum algorithms. We illustrate its expressivity by using it to encode the correctness of the well-known quantum search algorithm. We also provide a general method (extending an idea employed in the decidability proof in [50]) for proving the decidability of a range of quantum logics, interpreted on finite-dimensional Hilbert spaces. We give general conditions for the applicability of this method, and in particular we apply it to prove the decidability of PLQP.

Background: The logical system that we introduce for quantum reasoning in this chapter is similar to the one introduced in Chapter 5 and is based on combining the well-known formalisms of quantum logic, modal logic and probability logic (see Chapter 2). This gives us a Probabilistic Logic of Quantum Programs (PLQP), that extends a version [12] of the older Logic of Quantum Program (LQP), introduced in [11] and developed in [12, 13, 15, 14]. While the original version in [11] had *dynamic modalities* $[\pi]$ (for quantum programs π) as well as *spatial modalities* (to talk about subsystems and local information), the later ones were replaced in [12] with "epistemic" modalities K_I (capturing the information that is 'known' to subsystem I, i.e. it is carried by the local state of subsystem I). In addition to the dynamic and epistemic modalities, the logic PLQP presented in this chapter is endowed with a *probabilistic modality*, capturing the probability that a given test (of a quantum-testable property) will succeed. This is a novel feature, that greatly enhances the expressivity of the logic, allowing us to use it for the verification of probabilistic quantum algorithms.

Let us briefly summarise some notational conventions from Chapter 2.2.1. In standard quantum logic, $[\![\phi]\!]$ is typically taken to be a "closed linear subspace" of $\mathcal{H}$. Here we use scare quotes because, strictly speaking, $[\![\phi]\!] \subseteq \Sigma$ is a different type of object than a closed linear subspace $T \subseteq \mathcal{H}$; yet we henceforth refrain from stressing the type difference when the correspondence is obvious. To denote this correspondence, given any non-zero vector $v \in \mathcal{H}$, we write $\tilde{v}$ for the ray that v belongs to. Moreover, given any subset $A \subseteq \mathcal{H}$ that is closed under scalar multiplication, we write $\widetilde{A}$ for the corresponding subset of Σ, i.e., $\widetilde{A} = \{\, \tilde{v} \in \Sigma \mid v \in A \,\}$; on the other hand, given any subset $S \subseteq \Sigma$, we write $\overline{S}$ for the corresponding subset of $\mathcal{H}$, that is, $\overline{S} = \{\, v \in \mathcal{H} \mid \tilde{v} \in S \,\} \cup \{\vec{0}\}$, which is closed under scalar multiplication.[1]

The structure of this chapter is as follows. In Section 6.1, we introduce the logic PLQP, and give its semantics in terms of finite-dimensional Hilbert space. Next we illustrate this logic's expressive power, by using it to encode the correctness of the quantum search algorithm in Section 6.2. We lay out our recipe for decidability proofs in full generality in Subsection 6.3.1, and then we demonstrate this recipe by applying it to PLQP in Subsection 6.3.3. In the final Subsection 6.3.4, we briefly illustrate how our proof method can be applied to other logics, in particular to quantum logics with propositional (and action) quantifiers, and to logics whose semantics is based on mixed states (as opposed to pure states).

6.1 Probabilistic Logic of Quantum Programs

In Chapter 2.2.1 we introduced the syntax and semantics of standard quantum logic, which can be used to express interesting properties of quantum systems by using the quantum connectives $\sim$, $\wedge$ and $\sqcup$. Yet in the context of quantum logic it is fruitful to consider more connectives besides the given ones, including the classical Boolean connectives. In [15, 16] it has been argued that adding classical connectives allows one to express even more quantum properties than standard quantum logic can. Also, it is often useful to have propositional constants other than $\bot$. For instance, to express the correctness of a quantum communication protocol, we may want an atomic sentence c to invariably refer to (the state $\widetilde{|\beta_{00}\rangle}$ corresponding to) the Bell-state vector $|\beta_{00}\rangle$; then we add to the semantics the constraint $[\![c]\!] = \{\widetilde{|\beta_{00}\rangle}\}$. In this section we build a new vocabulary to introduce PLQP, the Probabilistic Logic of Quantum Programs. PLQP is an extension of the "epistemic" version [12] of the Logic of Quantum Programs (LQP), originally introduced in [11, 13], obtained by adding a probabilistic-test modality.

Syntax The language of this logic consists of two layers, one for sentences ϕ and the other for programs π, and is defined by double recursion.[2] To define

[1] Note that $\overline{\varnothing} = \{\vec{0}\}$, so that $\varnothing$ as a subset of Σ corresponds to the 0-dimensional subspace $\{\vec{0}\} \subseteq \mathcal{H}$ rather than $\varnothing$ as a subset of $\mathcal{H}$.

[2] This allows for some sentences to be constructed using program terms and some program terms to be constructed using sentences.

terms π for programs, we are given a set of *action variables* $V_{\mathcal{U}}$ and a set of *action constants* $C_{\mathcal{U}}$. We use $A_{\mathcal{U}} = V_{\mathcal{U}} \cup C_{\mathcal{U}}$ to denote *atomic action terms*, all of which are intended to refer to unitary transformations. We formally define *sentences* ϕ and *program terms* π of PLQP in the following BNF format, where $p \in A_{\mathcal{T}}$, $u \in A_{\mathcal{U}}$, $I \subseteq N$ for a (fixed) set N of natural numbers, and r is a rational number in $[0, 1]$:

$$\begin{aligned} \phi &::= p \mid \phi \wedge \phi \mid \neg\phi \mid [\pi]\phi \mid K_I\phi \mid \overset{\geqslant r}{\mathrm{Pr}}\,\phi \\ \pi &::= u \mid \phi? \mid \pi;\pi \mid \pi \cup \pi \end{aligned}$$

In addition to the standard propositional connectives for (classical) negation and conjunction, PLQP has *dynamic modalities* $[\pi]$ (one for each program term π), *"epistemic" modalities* K_I (one for each $I \subseteq N$) and *probabilistic modalities* $\mathrm{Pr}^{\geqslant r}$ (one for each rational number $r \in [0, 1]$). Their intended meaning is as follows:

- π is a program (such as a quantum logical gate or a quantum test), and is used to construct sentences via the dynamic modality $[\pi]$.

- u is an atomic action term that refers to a unitary transformation, e.g. a quantum gate such as the Hadamard, CNOT or Toffoli gate.

- $\phi?$ is the program that refers to the successful test of a sentence ϕ.

- $\pi_1;\pi_2$ is the program given by the sequential composition of π_1 and π_2 (applying first π_1 and then π_2).

- $\pi_1 \cup \pi_2$ is the program given by the indeterministic choice between π_1 and π_2 (either π_1 or π_2 is executed).

- Using the dynamic modality $[\pi]$, the sentence $[\pi]\phi$ means that "ϕ *will be the case after* (any successful execution of) π".

- For the modality K_I, fix a set of natural numbers N, using $i \in N$ as indices for Hilbert spaces $\mathcal{H}_i$ that compose the system $\mathcal{H} = \bigotimes_{i\in N} \mathcal{H}_i$. (Typically $\mathcal{H}_i = \mathbb{C}^2$, but not necessarily.) So each subset $I \subseteq N$ is intended to refer to the subsystem composed of the basic components $\mathcal{H}_i$ with $i \in I$, that is, $\mathcal{H}_I = \bigotimes_{i\in I} \mathcal{H}_i$. In this setting $K_I\phi$ means that "(the local state of) *subsystem I carries the information that ϕ is (globally) the case*".

- For a rational number r in the interval $[0, 1]$, $\mathrm{Pr}^{\geqslant r}\,\phi$ means that "*testing property ϕ (on the current state) will succeed with probability* $\geqslant r$".

In this language, we can define additional connectives via the following abbreviations:

$\bot$	$\overset{\text{def}}{=} \phi \wedge \neg\phi$	$\Box\phi$	$\overset{\text{def}}{=} \neg\Diamond\neg\phi$
$\top$	$\overset{\text{def}}{=} \neg\bot$	$E\phi$	$\overset{\text{def}}{=} \Diamond\Diamond\phi$
$\sim\phi$	$\overset{\text{def}}{=} [\phi?]\bot$	$A\phi$	$\overset{\text{def}}{=} \neg E\neg\phi$
$\phi \sqcup \psi$	$\overset{\text{def}}{=} \sim(\sim\phi \wedge \sim\psi)$	$\Pr^{\leqslant r}\phi$	$\overset{\text{def}}{=} \Pr^{\geqslant(1-r)} \sim\phi$
$\phi \vee \psi$	$\overset{\text{def}}{=} \neg(\neg\phi \wedge \neg\psi)$	$\Pr^{<r}\phi$	$\overset{\text{def}}{=} \neg\Pr^{\geqslant r}\phi$
$\phi \to \psi$	$\overset{\text{def}}{=} \neg(\phi \wedge \neg\psi)$	$\Pr^{>r}\phi$	$\overset{\text{def}}{=} \neg\Pr^{\leqslant r}\phi$
$\langle\pi\rangle\phi$	$\overset{\text{def}}{=} \neg[\pi]\neg\phi$	$[\phi?^{\geqslant r}?]\psi$	$\overset{\text{def}}{=} \Pr^{\geqslant r}\phi \to [\phi?]\psi$
$\Diamond\phi$	$\overset{\text{def}}{=} \langle\phi?\rangle\top$		

In particular, classical disjunction $\vee$ is the De Morgan dual of $\wedge$ under classical negation $\neg$, whereas quantum disjunction $\sqcup$ is the De Morgan dual of $\wedge$ under quantum negation $\sim$. For instance, in $\mathbb{C}^2$, let p refer to the state $\widetilde{|0\rangle}$; then $\sim p$ refers to $\widetilde{|1\rangle}$, but $\neg p$ refers to all the states in $\mathbb{C}^2$ except $\widetilde{|0\rangle}$—so, whereas $\sim(p \sqcup \sim p)$ is a contradiction, $\neg(p \vee \sim p)$ refers to all the states where $\widetilde{|0\rangle}$ and $\widetilde{|1\rangle}$ are superposed. We use $\to$ for the classical material implication, and define a series of abbreviations for the opposite and strict versions of the probabilistic operator: $\Pr^{\leqslant r}$, $\Pr^{>r}$, $\Pr^{<r}$. The sentence $\Diamond\phi$ expresses that "the test of whether ϕ is the case or not can succeed", and $\Box$ is the classical dual of $\Diamond$. Similarly $\langle\pi\rangle\phi$ is the classical dual of $\neg[\pi]\neg\phi$. We also introduce a universal modality $A\phi$ and an existential modality $E\phi$; they respectively mean that "ϕ is the case not just in the current state but in every state of the system" and "ϕ is the case in some state of the system". The intended interpretation for the construct $[\phi?^{\geqslant r}]\psi$ is that "if the test of ϕ will succeed with probability $\geqslant r$, then ψ will be the case after any successful execution of the test".[3]

We may refer to $[\pi]$, $\langle\pi\rangle$, $\Box$, $\Diamond$, A, E and K_I as *modalities*, in the spirit of modal logic [34] and in particular of dynamic logic [65] and epistemic logic [67, 55]. All the above introduced syntactic constructs are justified by the semantic conditions we will lay out shortly.

Semantics Just as in Chapter 2.2.1, we fix a Hilbert space $\mathcal{H}$ and take the corresponding state space Σ. An assignment $[\![\cdot]\!]$ assigns subsets of Σ to atomic sentences $p \in A_{\mathcal{T}}$, and binary relations on Σ to atomic action terms $u \in A_{\mathcal{U}}$. The semantics is given by recursively extending such an assignment $[\![\cdot]\!]$ to all sentences and all terms, interpreting each sentence ϕ with a set $[\![\phi]\!] \subseteq \Sigma$ of states, and each program π with a binary relation $[\![\pi]\!] \subseteq \Sigma \times \Sigma$ on states.

Definition 6.1.1. An *assignment* is a function $[\![\cdot]\!]$ from $A_{\mathcal{T}} \cup A_{\mathcal{U}}$ such that

[3] We can also think of $[-?^{\leqslant r}]$, $[-?^{>r}]$, $[-?^{<r}]$, $\langle -?^{\geqslant r}\rangle$, $\langle -?^{\leqslant r}\rangle$, $\langle -?^{>r}\rangle$, and $\langle -?^{<r}\rangle$, but as they play no essential role in this article we omit them here.

- For every $p \in A_{\mathcal{T}}$, $\llbracket p \rrbracket \subseteq \Sigma$ corresponds to a closed linear subspace of $\mathcal{H}$.
- For every $u \in A_{\mathcal{U}}$, $\llbracket u \rrbracket : \Sigma \to \Sigma$ corresponds to a unitary transformation on $\mathcal{H}$.
- Every constant symbol $c \in C_{\mathcal{T}} \cup C_{\mathcal{U}}$ is interpreted as intended, such as in (1).

To extend $\llbracket \cdot \rrbracket$, we interpret classical negation $\neg$ and disjunction $\vee$ classically:[4]

1. $s \in \llbracket \neg\phi \rrbracket$ iff $s \notin \llbracket \phi \rrbracket$, so that $\llbracket \neg\phi \rrbracket = \Sigma \setminus \llbracket \phi \rrbracket$, the Boolean complement of $\llbracket \phi \rrbracket$;
2. $s \in \llbracket \phi \vee \psi \rrbracket$ iff either $s \in \llbracket \phi \rrbracket$ or $s \in \llbracket \psi \rrbracket$, so that $\llbracket \phi \vee \psi \rrbracket = \llbracket \phi \rrbracket \cup \llbracket \psi \rrbracket$.

To formally define the semantics of dynamic modalities $[\pi]$, we introduce π-*transition relations* among states: $s \xrightarrow{\llbracket \pi \rrbracket} t$ means that " the successful execution of program π at state s moves the system to state t". Specifically, for program $u \in A_{\mathcal{U}}$, i.e., the action by the unitary transformation $\llbracket u \rrbracket : \Sigma \to \Sigma$, we have $s \xrightarrow{\llbracket u \rrbracket} t$ iff $\llbracket u \rrbracket(s) = t$. Also, for program $\phi?$, i.e., the test of whether a given sentence ϕ is the case or not, let us write $\mathit{Proj}_{\llbracket \phi \rrbracket} : \mathcal{H} \to \mathcal{H}$ for the projection onto the closed linear subspace of $\mathcal{H}$ that $\overline{\llbracket \phi \rrbracket}$ generates, i.e., $\sim\sim\overline{\llbracket \phi \rrbracket}$; then we set $s \xrightarrow{\llbracket \phi? \rrbracket} t$ iff $\{\, \mathit{Proj}_{\llbracket \phi \rrbracket}(v) \mid v \in s \,\} = t$. We also set $s \xrightarrow{\llbracket \pi_1;\pi_2 \rrbracket} t$ iff $s \xrightarrow{\llbracket \pi_1 \rrbracket} u \xrightarrow{\llbracket \pi_2 \rrbracket} t$ for some $u \in \Sigma$, and $s \xrightarrow{\llbracket \pi_1 \cup \pi_2 \rrbracket} t$ iff either $s \xrightarrow{\llbracket \pi_1 \rrbracket} t$ or $s \xrightarrow{\llbracket \pi_2 \rrbracket} t$.

Now, given the transition relations $\xrightarrow{\llbracket \pi \rrbracket}$, the intended meaning of $[\pi]\phi$ can be formalized in the manner of Hennessy-Milner logic for labelled transition systems [66]:

3. $s \in \llbracket [\pi]\phi \rrbracket \iff t \in \llbracket \phi \rrbracket$ whenever $s \xrightarrow{\llbracket \pi \rrbracket} t$.

Plugging the specific transition relations $\xrightarrow{\llbracket u \rrbracket}$ and $\xrightarrow{\llbracket \phi? \rrbracket}$ above into this, we have:

4. $\llbracket [u]\phi \rrbracket = \{\, s \mid \llbracket u \rrbracket(s) \in \llbracket \phi \rrbracket \,\} = \llbracket u \rrbracket^{-1} \llbracket \phi \rrbracket$.
5. $\llbracket [\phi?]\psi \rrbracket = \{\, s \mid \mathit{Proj}_{\llbracket \phi \rrbracket}(v) \in \overline{\llbracket \psi \rrbracket} \text{ for all } v \in s \,\} = \widetilde{\mathit{Proj}_{\llbracket \phi \rrbracket}}^{-1}[\overline{\llbracket \psi \rrbracket}]$.
6. $\llbracket [\pi_1;\pi_2]\phi \rrbracket = \llbracket [\pi_1][\pi_2]\phi \rrbracket$.
7. $\llbracket [\pi_1 \cup \pi_2]\phi \rrbracket = \llbracket [\pi_1]\phi \wedge [\pi_2]\phi \rrbracket$.

[4] In quantum logic, $\llbracket \phi \rrbracket$ lies in the lattice $L_{\mathcal{H}}$ of closed linear subspaces of $\mathcal{H}$. In contrast, for ϕ containing classical connectives, $\llbracket \phi \rrbracket$ is not in general a closed linear subspace (though it is closed under scalar multiplication and lies in the powerset $\mathcal{P}(\Sigma)$ of Σ). Nevertheless we do not drop the constraint that $\llbracket p \rrbracket$ is a closed linear subspace for any atomic p.

(4) and (5) mean that $[\![[u]\psi]\!]$ and $[\![[\phi?]\psi]\!]$ are the pre-images, or the "weakest preconditions", of $[\![\psi]\!]$ under $[\![u]\!]$ and $\mathit{Proj}_{[\![\phi]\!]}$. It is also worth noting that (5) implies

8. $[\![[\phi?]\psi]\!] = {\sim}[\![\phi]\!] \sqcup ([\![\phi]\!] \cap [\![\psi]\!])$, the so-called "Sasaki hook" from $[\![\phi]\!]$ to $[\![\psi]\!]$.

Moreover, with $\psi = \bot$, by (1) we can verify

9. $[\![[\phi?]\bot]\!] = \{ s \mid \mathit{Proj}_{[\![\phi]\!]}(v) = \vec{0} \text{ for all } v \in s \} = {\sim}[\![\phi]\!]$.

10. $[\![\Diamond\phi]\!] = [\![\langle\phi?\rangle\top]\!] = [\![\neg[\phi?]\bot]\!] = \{ s \mid s \xrightarrow{[\![\phi?]\!]} t \text{ for some } t \in \Sigma \}$.

In addition, we can show

11. $[\![A\phi]\!] = [\![\Box\Box\phi]\!] = \Sigma$ if $[\![\phi]\!] = \Sigma$; otherwise $[\![A\phi]\!] = \varnothing$.[5]

For the semantics of our "local-information modalities" K_I, we should think of the Hilbert space $\mathcal{H} = \bigotimes_{i \in N} \mathcal{H}_i$ as divided into a principal subsystem $\mathcal{H}_I = \bigotimes_{i \in I} \mathcal{H}_i$ and its "environment" $\mathcal{H}_{N \setminus I} = \bigotimes_{i \in N \setminus I} \mathcal{H}_i$. Then $K_I\phi$ is supposed to mean that *the subsystem I carries the information that ϕ.* This idea can be made precise using the density-operator formalism. For any unit vector $v \in s$, the pure state s of the global system N can be alternatively described by the corresponding density operator ρ_v^N. The so-called *reduced density operator* $s_I = \mathrm{tr}_{N \setminus I}(\rho_v)$, obtained by taking the partial trace $\mathrm{tr}_{N \setminus I}$ over the environment $N \setminus I$, is typically a *mixed state*, which describes *the "state" s_I of the sub-system I* (when the global system is in state s). The relation of *I-indistinguishability* between global states s, t can thus be defined by putting:

$$s \sim_I t \iff s_I = t_I \iff tr_{N \setminus I}(\rho_v) = tr_{N \setminus I}(\rho_w) \text{ for unitary } v \in s, w \in t.$$

Essentially, $s \sim_I t$ means that the global states s and t are "locally the same from the viewpoint of I". The indistinguishability relation can be alternatively characterized in terms of *I-remote* actions: these are unitary transformations $\mathcal{U} : \mathcal{H} \to \mathcal{H}$ having the property that $\mathcal{U} = \mathrm{Id}_I \otimes V$, where $\mathrm{Id}_I : \mathcal{H}_I \to \mathcal{H}_I$ is the identity map on subsystem I and $V : \mathcal{H}_{N \setminus I} \to \mathcal{H}_{N \setminus I}$ is some unitary transformation on its environment. Then it follows that

$$s \sim_I t \iff t = \mathcal{U}(s) \text{ for some } I\text{-remote } \mathcal{U}.$$

Now, using the I-indistinguishability relation, we can define an "epistemic" modality K_I in the way that is standard in epistemic modal logic: i.e., we can say that *subsystem I "knows" (it carries the information) that ϕ is the case in state s* iff ϕ is the case in all the states that are I-indistinguishable from s. More formally,

[5] See [11], 499f., for a proof.

12. $s \in [\![K_I\phi]\!] \begin{array}{l} \iff t \in [\![\phi]\!] \text{ for every } t \sim_I s \\ \iff U(s) \in [\![\phi]\!] \text{ for every } I\text{-remote } U \end{array}.$

Or we can put this as follows: I-remote unitary transformations are symmetries that tinker with the environment alone, leaving anything in the principal subsystem I intact; so I locally carries the information that ϕ iff ϕ is invariant under those symmetries.

The probability connective $\mathrm{Pr}^{\geqslant r}$ is interpreted straightforwardly via Born's rule:

13. $s \in [\![\mathrm{Pr}^{\geqslant r}\, \phi]\!] \iff \langle v|\, \mathit{Proj}_{[\![\phi]\!]}\, |v\rangle \geqslant r$ for all unit vectors $v \in s$.

The constraints we have reviewed so far give the semantics of PLQP.

Definition 6.1.2. Given a language $\mathcal{L}$ of PLQP, by an *PLQP model over a Hilbert space* $\mathcal{H}$ (for $\mathcal{L}$) we mean a pair consisting of the set Σ of states in $\mathcal{H}$ and any valuation map $[\![\cdot]\!]$ (for $\mathcal{L}$) that extends an assignment (Definition 6.1.1) and satisfies (3), (1), (4)–(7), (12), (13). We say that a sentence ϕ of $\mathcal{L}$ is *PLQP-valid in* $\mathcal{H}$, and write $\mathcal{H} \vDash_{\mathrm{PLQP}} \phi$, or $\mathcal{H} \vDash \phi$ for short, if ϕ is true everywhere in Σ regardless of the assignments, that is, if $[\![\phi]\!] = \Sigma$ for all PLQP models $(\Sigma, [\![\cdot]\!])$ over $\mathcal{H}$. Lastly, we define the logic $\mathbf{PLQP}_{\mathcal{H}}$, the PLQP (in $\mathcal{L}$) of $\mathcal{H}$, as the set of sentences of $\mathcal{L}$ that are PLQP-valid in $\mathcal{H}$; that is,

$$\mathbf{PLQP}_{\mathcal{H}} = \{\, \phi \in \mathcal{L} \mid [\![\phi]\!] = \Sigma \text{ for all PLQP models } (\Sigma, [\![\cdot]\!]) \text{ over } \mathcal{H}\,\}.$$

6.2 Applying PLQP to the Quantum Search Algorithm

The connectives of PLQP, which we reviewed above in Section 6.1, serve many purposes. In this section, we show that PLQP is expressive enough to capture the correctness of the quantum search algorithm [63].

Let us fix a quantum system $\mathcal{H}$ of $n+1$ qubits, for $n > 2$; we write $N = \{0, \dots, n-1\}$ and $N + 1 = \{0, \dots, n\}$ and use $i \in N + 1$ as indices for qubits. We also write $2 = \{0, 1\}$, so that any $g : N \to 2$ is an assignment of 0 and 1 to the qubits in N. Now, by a *classical state*, we mean $|g\rangle = \otimes_{i \in N} |g(i)\rangle_i$ for any $g : N \to 2$. A unitary operator O on $\mathcal{H}$ is called an *oracle* if there is exactly one classical state $|\widehat{f}\rangle$ such that, for every classical state $|g\rangle$ and $b \in 2$,

$$O(|g\rangle \otimes |b\rangle_n) = \begin{cases} |g\rangle \otimes |1-b\rangle_n & \text{if } g = \widehat{f}, \\ |g\rangle \otimes |b\rangle_n & \text{otherwise.} \end{cases}$$

The quantum search algorithm lets us find such a classical state $|\widehat{f}\rangle$, given an oracle O.

Algorithm and Correctness Criterion The algorithm goes as follows:

i. Set each qubit $i \in N$ in the state $|0\rangle_i$ and the qubit n in $|1\rangle_n$.

ii. Apply the Hadamard gate to each qubit in $N+1$.

iii. (a) Apply the oracle O to $N+1$.
(b) Apply the Hadamard gate to each qubit in N.
(c) Apply to N the conditional phase shift gate P_N, whose matrix representation has $(P_N)_{00} = 1$, $(P_N)_{ii} = -1$ if $0 < i < n$, and $(P_N)_{ij} = 0$ if $i \neq j$.
(d) Apply the Hadamard gate to each qubit in N.

iv. Repeat (iii) k times, where k is the largest natural number less than $\frac{\pi}{4}\sqrt{2^n}$.

v. Measure the qubits in N.

This algorithm is correct if $|g\rangle = |\widehat{f}\rangle$ with probability greater than 0.5, where $|g\rangle$ is the classical state of the qubits in N after measurement. PLQP can express this correctness, when a language $\mathcal{L}_{\mathbf{PLQP}}$ of PLQP has

- For each $i \in N+1$, propositional constants 0_i and 1_i. $[\![0_i]\!]$ (resp., $[\![1_i]\!]$) is the property of being in an i-separated state whose i-local state is generated by $|0\rangle_i$ (resp., $|1\rangle_i$).
- For each $i \in N+1$, an action constant H_i for the i-local action that performs the Hadamard transform on qubit i and does not affect the other qubits.
- An action constant P for the N-local action which performs the conditional phase shift gate on N and whose matrix is $P_N \otimes \mathrm{Id}_n$. Here Id_n is the matrix for the identity map on qubit n and $\otimes$ is the Kronecker product of two matrices.
- An action variable O (we use it to refer to the oracle).

PLQP Expression For any propositional variable $p \in V_{\mathcal{T}}$, let $\mathit{CState}(p)$ be a formula of PLQP stating that if p then the system must be in an N-separated state whose N-local state is classical. Also, let $\mathit{Ora}(O)$ be a formula of PLQP stating that O is an oracle. More precisely, given any $f : N \to 2$ let us write $\underline{f}$ for the sentence $\bigwedge_{i \in N} f(i)_i$, and then

$$\mathit{CState}(p) := Ep \wedge A\Big(p \to \bigvee_{f:N\to 2} \underline{f}\Big),$$

$$\mathit{Ora}(O) := \bigvee_{f:N\to 2} A \left[\begin{array}{c} \big(\underline{f} \wedge 0_n \to [O](\underline{f} \wedge 1_n)\big) \wedge \big(\underline{f} \wedge 1_n \to [O](\underline{f} \wedge 0_n)\big) \\ \wedge \displaystyle\bigwedge_{g:N\to 2, g\neq f} \left(\begin{array}{c} \big(\underline{g} \wedge 0_n \to [O](\underline{g} \wedge 0_n)\big) \\ \wedge \big(\underline{g} \wedge 1_n \to [O](\underline{g} \wedge 1_n)\big) \end{array} \right) \end{array} \right].$$

Note that, since $[\![\bigvee_{f:N\to 2} \underline{f}]\!]$ is not a closed linear subspace, if $[\![\mathit{CState}(p)]\!] = \Sigma$ then all the states in $[\![p]\!]$ are N-separated and there is a single $f : N \to 2$ such that $|f(i)\rangle_i$ generate the N-local states of all the states in $[\![p]\!]$. Now, writing $\mathbf{0} : N \to 2$ for the constant $\mathbf{0} :: i \mapsto 0$ and $[\pi]^k$ for the k-times iteration of $[\pi]$ (for k as in step (iv) of the algorithm), consider

$$\begin{aligned} \mathit{QSA} := \mathit{Ora}(O) \wedge \mathit{CState}(p) \wedge A\Big(p \wedge 0_n \to [O]1_n\Big) \wedge A\Big(p \wedge 1_n \to [O]0_n\Big) \wedge \underline{\mathbf{0}} \wedge 1_n \\ \to [H_0; \cdots ; H_n][O; H_0; \cdots ; H_{n-1}; P; H_0; \cdots ; H_{n-1}]^k P^{>0.5} p. \end{aligned}$$

This formula QSA expresses the correctness of the quantum search algorithm, in the sense that the algorithm is correct for an $(n+1)$-qubit system $\mathcal{H}$ iff QSA is valid in $\mathcal{H}$.

6.3 Decidability Proof

The goal of this section is to provide a general method for proving decidability not just for PLQP but in fact for a wide range of logics of Hilbert spaces. The section proceeds as follows. In subsection 6.3.1, we lay out the core idea of the method in conceptual terms, by illustrating how it works with PLQP in particular. From this illustration, we extract in subsection 6.3.2 a precise lemma that can be applied to show a wider range of logics of Hilbert spaces to be decidable. Then, in subsection 6.3.3, we show how to apply this lemma to the particular case of PLQP, establishing its decidability. We close the section by briefly mentioning, in subsection 6.3.4, other kinds of logics to which the lemma can be applied.

6.3.1 Proof Recipe, the Core Idea

The core idea of our method of proving a given logic of a Hilbert space to be decidable is to rewrite the semantics for the logic entirely (and effectively) in the first-order theory of complex numbers, which is decidable due to Tarski's [99] theorem. In this subsection, we describe how this idea works by taking the case of PLQP as an example. (Our discussion in this subsection is not meant to be a rigorous proof, but rather a conceptual illustration; we turn this illustration into rigorous proofs in subsections 6.3.2 and 6.3.3.)

Let us write $\mathbb{C}$ for the set of complex numbers, $\mathcal{L}_{\mathbb{C}} = (+, \cdot, *, 0, 1)$ for the first-order language of $\mathbb{C}$ with $*$ for the complex conjugate, and $\mathbb{T}_{\mathbb{C}}$ for the theory of $\mathbb{C}$ in $\mathcal{L}_{\mathbb{C}}$, whose decidability follows from Tarski's [99] theorem. The key to our proof method is the following fact, which Dunn et al. [50] also used in an essential step of their proof.

Fact 6.3.1. When $\mathcal{H} \cong \mathbb{C}^n$ is a Hilbert space of dimension $n \in \mathbb{N}$, its closed linear subspaces are exactly the kernels of $n \times n$ complex matrices.

This means the following, for any atomic sentence $p \in A_{\mathcal{T}}$ and any $n \times n$ matrix $\hat{p}$ and n-vector $\vec{v}$ of variables of $\mathcal{L}_{\mathbb{C}}$. For every assignment $[\![\cdot]\!]$ (see Definition 6.1.1), some value of $\hat{p}$ in $\mathbb{C}^{n\times n}$ corresponds to the subspace $\overline{[\![p]\!]}$,[6] in the sense that

$$\vec{v} \in \overline{[\![p]\!]} \iff \hat{p}\vec{v} = \vec{0}, \text{ i.e., } \begin{array}{l} p_{11}v_1 + \cdots + p_{1n}v_n = 0 \\ \wedge \cdots \\ \wedge\, p_{n1}v_1 + \cdots + p_{nn}v_n = 0 \end{array} \tag{6.14}$$

for every value of $\vec{v}$ in $\mathbb{C}^n$. On the other hand, every value of $\hat{p}$ corresponds (in the same sense) to $\overline{[\![p]\!]}$ for some assignment $[\![\cdot]\!]$. Note here that $\hat{p}\vec{v} = \vec{0}$ is a formula of $\mathcal{L}_{\mathbb{C}}$. Then we can expand (6.14) into a decidability proof as follows.

First, here is a proof that p is decidably not valid—even though we hardly need a proof that propositional variables p are never valid, the case still serves as a basis for our decidability proof. From (6.14) it immediately follows that, given any particular $[\![\cdot]\!]$ and any value of $\hat{p}$ that corresponds to $\overline{[\![p]\!]}$, p is true everywhere in $\mathcal{H}$ iff the formula $\hat{p}\vec{v} = \vec{0}$ holds of all values of $\vec{v}$ in $\mathbb{C}^n$; that is,

$$\overline{[\![p]\!]} = \mathcal{H} \iff \forall\vec{v}.\, \vec{v} \in \overline{[\![p]\!]} \iff \forall\vec{v}.\, \hat{p}\vec{v} = \vec{0}.$$

This further implies that p is valid in $\mathcal{H}$, written $\mathcal{H} \vDash p$ (see Definition 6.1.2), iff $\hat{p}\vec{v} = \vec{0}$ holds not just of all values of $\vec{v}$ but moreover of all values of $\hat{p}$ in $\mathbb{C}^{n\times n}$; that is,

$$\begin{aligned} \mathcal{H} \vDash p, \text{ i.e., } \overline{[\![p]\!]} = \mathcal{H} \text{ for all } [\![\cdot]\!] &\iff \forall\vec{v}.\, \hat{p}\vec{v} = \vec{0} \text{ for all values of } \hat{p} \\ &\iff \mathbb{T}_{\mathbb{C}} \vdash \forall\hat{p}\,\forall\vec{v}.\, \hat{p}\vec{v} = \vec{0}. \end{aligned}$$

Due to the quantifiers, $\forall\hat{p}\,\forall\vec{v}.\, \hat{p}\vec{v} = \vec{0}$ is a *closed* sentence of $\mathcal{L}_{\mathbb{C}}$ with no constant symbols except 0; therefore, by the decidability of $\mathbb{T}_{\mathbb{C}}$, it is decidable that the last equivalent does not hold. The upshot is this: The formula $\hat{p}\vec{v} = \vec{0}$ of $\mathcal{L}_{\mathbb{C}}$, regarded as an n-ary formula with variables $\vec{v}$ and particular values of $\hat{p}$ as parameters, defines the subset $\overline{[\![p]\!]}$ of $\mathcal{H}$ to which the parameters correspond;[7] so quantifying over both $\vec{v}$ and $\hat{p}$ gives the closed sentence of $\mathcal{L}_{\mathbb{C}}$ that decides whether p is valid in $\mathcal{H}$ or not (and in this case, it is not).

We extend this case to all the sentences ϕ of a language $\mathcal{L}_{\mathbf{PLQP}}$ of PLQP and not just atomic ones; that is, if for each ϕ we can find an n-ary formula $\phi^\delta(\vec{v}, \bar{x})$ of $\mathcal{L}_{\mathbb{C}}$ that defines $\overline{[\![\phi]\!]} \subseteq \mathcal{H}$ (perhaps with values of $\bar{x}$ as parameters), then we can decide whether ϕ is valid in $\mathcal{H}$ or not by universally quantifying over $\vec{v}$ and $\bar{x}$. Schematically, what we just saw is the left column below, and we extend it

[6] An assignment $[\![\cdot]\!]$ assigns to p a set $[\![p]\!] \subseteq \Sigma$ corresponding to a closed linear subspace of $\mathcal{H}$, and $\overline{[\![p]\!]}$ is that subspace. See p. 116 for more on this notation.

[7] Particular values of $\hat{p}$ as parameters may be undefinable in $\mathcal{L}_{\mathbb{C}}$; but they do not hinder our proof, since in the end we quantify over $\hat{p}$ and obtain closed sentences of $\mathcal{L}_{\mathbb{C}}$.

into the right.

$$\begin{aligned}
\hat{p}\vec{v} = \vec{0}\ &\textit{defines}\ \overline{\llbracket p \rrbracket} \subseteq \mathcal{H}, & \phi^{\delta}(\vec{v},\bar{x})\ &\textit{defines}\ \overline{\llbracket \phi \rrbracket} \subseteq \mathcal{H},\\
\vec{v} \in \overline{\llbracket p \rrbracket} &\iff \mathbb{C} \vDash \hat{p}\vec{v} = \vec{0}, & \vec{v} \in \overline{\llbracket \phi \rrbracket} &\iff \mathbb{C} \vDash \phi^{\delta}(\vec{v},\bar{x}),\\
\overline{\llbracket p \rrbracket} = \mathcal{H} &\iff \mathbb{C} \vDash \forall\vec{v}.\, \hat{p}\vec{v} = \vec{0}, & \overline{\llbracket \phi \rrbracket} = \mathcal{H} &\iff \mathbb{C} \vDash \forall\vec{v}.\, \phi^{\delta}(\vec{v},\bar{x}),\\
\mathcal{H} \vDash p &\iff \mathbb{C} \vDash \forall\hat{p}\,\forall\vec{v}.\, \hat{p}\vec{v} = \vec{0}, & \mathcal{H} \vDash \phi &\iff \mathbb{C} \vDash \forall\bar{x}\,\forall\vec{v}.\, \phi^{\delta}(\vec{v},\bar{x}).
\end{aligned}$$

Here, however, the last step on the right is not quite correct, since ϕ may contain an expression for which parameters cannot be arbitrary. For instance, consider a particular subspace $\overline{\llbracket p \rrbracket}$ and unitary transformation $\llbracket u \rrbracket$, as well as values of $\hat{p}$ and $\hat{u}$ corresponding to them respectively. Then, as we will explain in more detail in subsection 6.3.3, the formula $([u]p)^{\delta}$ that defines $\overline{\llbracket [u]p \rrbracket} \subseteq \mathcal{H}$ is $\hat{p}(\hat{u}\vec{v}) = \vec{0}$, so that

$$\overline{\llbracket [u]p \rrbracket} = \mathcal{H} \iff \mathbb{C} \vDash \forall\vec{v}.\, \hat{p}(\hat{u}\vec{v}) = \vec{0}.$$

Yet it would be a mistake to carry on to say

$$\mathcal{H} \vDash [u]p \iff \mathbb{C} \vDash \forall\hat{u}\,\forall\hat{p}\,\forall\vec{v}.\, \hat{p}(\hat{u}\vec{v}) = \vec{0}, \tag{6.15}$$

because, whereas any value of $\hat{p}$ corresponds to a linear subspace, not every value of $\hat{u}$ is good in the sense of corresponding to a unitary transformation. Still, there is a formula of $\mathcal{L}_{\mathbb{C}}$ defining the range of good values of $\hat{u}$—namely, $\mathcal{U}_n(\hat{x}) := \ulcorner \hat{x}^{\dagger}\hat{x} = \hat{x}\hat{x}^{\dagger} = \mathrm{Id}_n \urcorner$,[8] which states that $\hat{x}$ is an $n \times n$ unitary matrix. Therefore, instead of (6.15), we can correctly have

$$\mathcal{H} \vDash [u]p \iff \mathbb{C} \vDash \forall\hat{u}\,\forall\hat{p}\,(\mathcal{U}_n(\hat{u}) \to \forall\vec{v}.\, \hat{p}(\hat{u}\vec{v}) = \vec{0}).$$

In a more general form, for each sentence ϕ of $\mathcal{L}_{\mathbf{PLQP}}$ we will need a pair of formulas of $\mathcal{L}_{\mathbb{C}}$, written $\phi^{\delta}(\vec{v},\bar{x})$ and $\phi^{\rho}(\bar{x})$, that "interprets" ϕ in the sense that

16. $\phi^{\delta}(\vec{v},\bar{c})$ defines $\overline{\llbracket \phi \rrbracket} \subseteq \mathcal{H}$ with parameters $\bar{c}$ (hence the superscript δ for "*d*efining"), when the values $\bar{c}$ of the variables $\bar{x}$ correspond to the assignment $\llbracket \cdot \rrbracket$, and

17. $\phi^{\rho}(\bar{x})$ defines the range of good values $\bar{c}$ of $\bar{x}$ (hence the superscript ρ for "*r*ange"),

so that

$$\mathcal{H} \vDash \phi \iff \mathbb{C} \vDash \forall\bar{x}\,(\phi^{\rho}(\bar{x}) \to \forall\vec{v}.\, \phi^{\delta}(\vec{v},\bar{x})).$$

We need an effective procedure that yields such an interpreting pair of formulas $\phi^{\delta}(\vec{v},\bar{x})$, $\phi^{\rho}(\bar{x})$ to every sentence ϕ. For this purpose, it is enough by induction to have

[8] We use the quotation marks $\ulcorner\cdot\urcorner$ loosely to identify formulas of $\mathcal{L}_{\mathbb{C}}$ with its scopes, so that the distinction is clearer between the equality sign within formulas of $\mathcal{L}_{\mathbb{C}}$ and an equation among formulas of $\mathcal{L}_{\mathbb{C}}$.

- an effective procedure that yields p^δ and p^ρ to every atomic sentence p;

- for each (n-ary) connective $\boxast$, an effective procedure that, given any ${\phi_i}^\delta$ and ${\phi_i}^\rho$, yields $\boxast(\phi_1, \ldots, \phi_n)^\delta$ and $\boxast(\phi_1, \ldots, \phi_n)^\rho$.

6.3.2 Proof Recipe, Precisely and Generally

In the previous subsection we laid out the core idea of our decidability proof taking PLQP as an example. In this subsection we abstract essential elements from this idea and put them in a more precise form that can be applied more generally to a wider range of logics than just PLQP. First, we generalize the notion of PLQP models to the following.

Definition 6.3.2. Given a language $\mathcal{L}$ (that may be modal or not), by a $\mathbb{C}^n$-*interpretation of* $\mathcal{L}$ we mean a map $[\![\cdot]\!]$ that assigns to each sentence ϕ of $\mathcal{L}$ a subset $[\![\phi]\!] \subseteq \mathbb{C}^n$. Also, given any class $\mathcal{I}$ of $\mathbb{C}^n$-interpretations of $\mathcal{L}$, we say that a sentence ϕ of $\mathcal{L}$ is $\mathcal{I}$-valid, and write $\mathcal{I} \vDash \phi$, if $[\![\phi]\!] = \mathbb{C}^n$ for all $[\![\cdot]\!] \in \mathcal{I}$; moreover, by the logic of $\mathcal{I}$ (in $\mathcal{L}$), we mean the set of $\mathcal{I}$-valid sentences of $\mathcal{L}$.

This definition clearly subsumes that of PLQP models $(\Sigma, [\![\cdot]\!])$ over a Hilbert space $\mathcal{H} \cong \mathbb{C}^n$; each $(\Sigma, [\![\cdot]\!])$ is (isomorphic to) a $\mathbb{C}^n$-interpretation $\overline{[\![\cdot]\!]}$.

Next, we generalize the correspondence between values of variables $\hat{p}$, $\hat{u}$ as parameters and values $[\![p]\!]$, $[\![u]\!]$ of assignments $[\![\cdot]\!]$. In the case of PLQP, take variables $\hat{p}, \hat{u}, \ldots$ of $\mathcal{L}_\mathbb{C}$ for all the atomic expressions $p, u, \ldots$ of $\mathcal{L}_{\mathbf{PLQP}}$, and observe the following (18)–(20). Here we write $\mathrm{var}(\mathcal{L}_\mathbb{C})$ for the set of variables of $\mathcal{L}_\mathbb{C}$. Also, for any $\alpha : \mathrm{var}(\mathcal{L}_\mathbb{C}) \to \mathbb{C}$ and any list $\bar{x} = (x_1, \ldots, x_m)$ of variables of $\mathcal{L}_\mathbb{C}$, we write $\alpha(\bar{x})$ for the list $(\alpha(x_1), \ldots, \alpha(x_m))$.

18. For each assignment $[\![\cdot]\!]$, there is an assignment $\alpha : \mathrm{var}(\mathcal{L}_\mathbb{C}) \to \mathbb{C}$ of values to $\hat{p}, \hat{u}, \ldots$ that corresponds to $[\![\cdot]\!]$. (Indeed there are many, since, for instance, values $c_{11}, \ldots, c_{nn}$ and $2c_{11}, \ldots, 2c_{nn}$ of $\hat{p}$ correspond to the same subspace of $\mathbb{C}^n$.)

19. On the other hand, not every assignment $\alpha : \mathrm{var}(\mathcal{L}_\mathbb{C}) \to \mathbb{C}$ is good in the sense of corresponding to some $[\![\cdot]\!]$. Yet, if α is good, it corresponds to a unique $[\![\cdot]\!]$.

20. Moreover, for any finite list of variables, say $\hat{u}$, there is a formula of $\mathcal{L}_\mathbb{C}$ (i.e., $\hat{x}^\dagger \hat{x} = \hat{x}\hat{x}^\dagger = \mathrm{Id}_n$) that the value $\alpha(\hat{u})$ has to satisfy in order for $\alpha : \mathrm{var}(\mathcal{L}_\mathbb{C}) \to \mathbb{C}$ to be good.

Recall that a *partial function* R from a set X *onto* a set Y is a relation $R \subseteq X \times Y$ such that

- for every $y \in Y$ there is some $x \in X$ with Rxy, and

- for every $x \in X$ there is at most one $y \in Y$ with Rxy,

and that we write $\mathrm{dom}(R) := \{\, x \in X \mid Rxy \text{ for some } y \in Y \,\}$. Then (18) and (19) together mean that the correspondence is a partial function from the set of assignments $\alpha : \mathrm{var}(\mathcal{L}_{\mathbb{C}}) \to \mathbb{C}$ (of values to $\hat{p}, \hat{u}, \ldots$) onto the set of PLQP models $[\![\cdot]\!]$, and moreover that $\mathrm{dom}(R)$, with R for the correspondence, is the set of good assignments α. So we generalize the correspondence as in Definition 6.3.3 below. As preliminary notation, let us write $\mathbb{C}^{\mathrm{var}(\mathcal{L}_{\mathbb{C}})}$ for the set of assignments $\alpha : \mathrm{var}(\mathcal{L}_{\mathbb{C}}) \to \mathbb{C}$. Also, given any $(n+m)$-ary formula $\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ of $\mathcal{L}_{\mathbb{C}}$ and m-tuple $c_1, \ldots, c_m \in \mathbb{C}$, we write $\psi(\mathbb{C}, c_1, \ldots, c_m)$ for the set that $\psi(\bar{x}, \bar{y})$ defines with parameters $\bar{c}$ in place of $\bar{y}$, that is,

$$\psi(\mathbb{C}, c_1, \ldots, c_m) := \{\, (b_1, \ldots, b_n) \in \mathbb{C}^n \mid \mathbb{C} \vDash \psi[b_1, \ldots, b_n, c_1, \ldots, c_m] \,\} \subseteq \mathbb{C}^n.$$

Then we enter the following definition, whose first sentence generalizes (18) and (19) with the part before “such that”, and (20) with the part after.

Definition 6.3.3. Given any class $\mathcal{I}$ of $\mathbb{C}^n$-interpretations, a $\mathbb{C}$*-coding of* $\mathcal{I}$ is a partial function R from $\mathbb{C}^{\mathrm{var}(\mathcal{L}_{\mathbb{C}})}$ onto $\mathcal{I}$ such that, for every finite list of variables $\bar{x} = (x_1, \ldots, x_m) \subseteq \mathrm{var}(\mathcal{L}_{\mathbb{C}})$ of $\mathcal{L}_{\mathbb{C}}$, there is an m-ary formula $\rho_{\bar{x}}(\bar{y})$ of $\mathcal{L}_{\mathbb{C}}$ defining the set $\{\, \alpha(\bar{x}) \in \mathbb{C}^m \mid \alpha \in \mathrm{dom}(R) \,\}$, that is, $\rho_{\bar{x}}(\mathbb{C}) = \{\, \alpha(\bar{x}) \in \mathbb{C}^m \mid \alpha \in \mathrm{dom}(R) \,\}$. Moreover, we say that a $\mathbb{C}$-coding is *effective* if there is an effective procedure of giving such $\rho_{\bar{x}}(\bar{y})$ to any given finite $\bar{x}$.[9]

In the case of PLQP, the correspondence between values of $\hat{p}, \hat{u}, \ldots$ and $[\![\cdot]\!]$ contributes to the decidability proof in combination with an interpretation of sentences ϕ of $\mathcal{L}_{\mathbf{PLQP}}$ in terms of pairs of formulas $\phi^{\delta}(\vec{v}, \bar{x})$, $\phi^{\rho}(\bar{x})$ of $\mathcal{L}_{\mathbb{C}}$. In other words, the essential property we require of the correspondence is to guarantee that the interpretation satisfies (16) and (17); or, in the new notation, with R for the correspondence, (16) and (17) amount respectively to

21. $R(\alpha, [\![\cdot]\!])$ entails $[\![\phi]\!] = \phi^{\delta}(\mathbb{C}, \alpha(\bar{x}))$,

22. $\phi^{\rho}(\mathbb{C}) = \rho_{\bar{x}}(\mathbb{C})$.

Therefore we generalize the PLQP case to Definition 6.3.4 and Lemma 6.3.5. The idea is to use (21) as the essential part of Definition 6.3.4, and, for (22), to show that $\rho_{\bar{x}}(\bar{x})$ plays the role in the proof of Lemma 6.3.5 that $\phi^{\rho}(\bar{x})$ played in subsection 6.3.1. So we first enter

Definition 6.3.4. Fix a finite-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^n$, any class $\mathcal{I}$ of $\mathbb{C}^n$-interpretations of a language $\mathcal{L}$, and any $\mathbb{C}$-coding R of $\mathcal{I}$. Then, for any sentence ϕ of $\mathcal{L}$, we say that a formula $\phi^{\delta}(v_1, \ldots, v_n, \bar{x})$ of $\mathcal{L}_{\mathbb{C}}$ (with a specific tuple of variables $\bar{x}$) *translates* ϕ *in* R, or *is an* R*-translation of* ϕ, if (21) holds for every $\alpha : \mathrm{var}(\mathcal{L}_{\mathbb{C}}) \to \mathbb{C}$ and $[\![\cdot]\!] \in \mathcal{I}$.

[9] The effectiveness of a $\mathbb{C}$-coding R does not assume any such property as recursiveness on R itself.

Then we prove the following lemma, which shows, among other things, that $\rho_{\bar{x}}(\bar{x})$ serves as the desired formula $\phi^{\rho}(\bar{x})$, thereby interpreting ϕ together with $\phi^{\delta}(\vec{v}, \bar{x})$.

Lemma 6.3.5. *Fix a finite-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^n$, any class $\mathcal{I}$ of $\mathbb{C}^n$-interpretations of a language $\mathcal{L}$, and any effective $\mathbb{C}$-coding R of $\mathcal{I}$. Suppose a sentence ϕ of $\mathcal{L}$ has an R-translation. Then it is decidable whether $\mathcal{I} \vDash \phi$ or not.*

Proof. Suppose a formula $\phi^{\delta}(\vec{v}, \bar{x})$ of $\mathcal{L}_{\mathbb{C}}$ translates ϕ in R. This entails both

23. for each $\bar{c} \in \rho_{\bar{x}}(\mathbb{C})$, there is $[\![\cdot]\!] \in \mathcal{I}$ such that $[\![\phi]\!] = \phi^{\delta}(\mathbb{C}, \bar{c})$;

24. for each $[\![\cdot]\!] \in \mathcal{I}$, there is $\bar{c} \in \rho_{\bar{x}}(\mathbb{C})$ such that $[\![\phi]\!] = \phi^{\delta}(\mathbb{C}, \bar{c})$.

To show (23), suppose $\bar{c} \in \rho_{\bar{x}}(\mathbb{C})$. This means that $\bar{c} = \alpha(\bar{x})$ for some $\alpha \in \mathrm{dom}(R)$, i.e., α such that $R(\alpha, [\![\cdot]\!])$ for some $[\![\cdot]\!]$. Hence $[\![\phi]\!] = \phi^{\delta}(\mathbb{C}, \alpha(\bar{x})) = \phi^{\delta}(\mathbb{C}, \bar{c})$ because $\phi^{\delta}(\vec{v}, \bar{x})$ translates ϕ in R. (24) holds because, for any $[\![\cdot]\!]$, there is α such that $R(\alpha, [\![\cdot]\!])$ (since R is onto), and so $[\![\phi]\!] = \phi^{\delta}(\mathbb{C}, \alpha(\bar{x}))$ and $\alpha(\bar{x}) \in \rho_{\bar{x}}(\mathbb{C})$. Then (23) and (24) respectively imply the "⇒" and "⇐" parts of $(*)$ in

$$\begin{aligned} \mathcal{I} \vDash \phi, \text{ i.e., } [\![\phi]\!] = \mathbb{C}^n \text{ for every } [\![\cdot]\!] \in \mathcal{I} \; &\overset{(*)}{\iff} \; \mathbb{C} \vDash \forall \vec{v}.\, \phi^{\delta}(\vec{v}, \bar{c}) \text{ for every } \bar{c} \in \rho_{\bar{x}}(\mathbb{C}) \\ &\iff \; \mathbb{C} \vDash \forall \bar{x}\, (\rho_{\bar{x}}(\bar{x}) \to \forall \vec{v}.\, \phi^{\delta}(\vec{v}, \bar{x})), \end{aligned}$$

and it is decidable, by Tarski's [99] theorem, whether the last equivalent is true or not. □

This finally gives the following, which encapsulates our recipe for decidability proofs.

Lemma 6.3.6. *For every finite-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^n$ and every class $\mathcal{I}$ of $\mathbb{C}^n$-interpretations of a language $\mathcal{L}$, the logic of $\mathcal{I}$ is decidable if*

25. *$\mathcal{L}$ is recursively enumerable;*

26. *there is an effective $\mathbb{C}$-coding R of $\mathcal{I}$;*

27. *the set of atomic sentences of $\mathcal{L}$ is* effectively R-translatable*, meaning that there is an effective procedure that yields an R-translation to any given atomic sentence p of $\mathcal{L}$;*

28. *each (n-ary) connective $\circledast$ of $\mathcal{L}$* effectively preserves R-translatability*, meaning that there is an effective procedure that, given any sentences ϕ_i of $\mathcal{L}$ ($1 \leqslant i \leqslant n$) and any R-translations thereof, yields an R-translation of $\circledast(\phi_1, \ldots, \phi_n)$.*

Proof. If (25)–(28) hold, we can effectively combine the effective procedures into a single effective procedure that, given any sentence ϕ of $\mathcal{L}$, yields a pair of formulas of $\mathcal{L}_{\mathbb{C}}$ that interprets ϕ in $\mathcal{I}$. Hence Lemma 6.3.5 implies Lemma 6.3.6. □

6.3.3 Application of Our Recipe to PLQP

We provided above a general recipe for decidability proofs in the form of Lemma 6.3.6. As an instance of its application, we take $\mathbf{PLQP}(\mathcal{H})$ and prove it decidable; that is, we prove

Theorem 6.3.7. *Let $\mathcal{L}_{\mathbf{PLQP}}$ be a language of PLQP. For any $n \in \mathbb{N}$ and any Hilbert space $\mathcal{H} \cong \mathbb{C}^n$, the logic $\mathbf{PLQP}(\mathcal{H}) = \{\, \phi \in \mathcal{L}_{\mathbf{PLQP}} \mid \mathcal{H} \vDash \phi \,\}$ is decidable.*

By Lemma 6.3.6, it is enough to show (25)–(28) about $\mathcal{L}_{\mathbf{PLQP}}$ and the class $\mathcal{I}$ of ($\mathbb{C}^n$-interpretations corresponding to) PLQP models over $\mathcal{H}$. (25) is clear. For (26), let us fix variables $\vec{v} = (v_1, \ldots, v_n)$ of $\mathcal{L}_{\mathbb{C}}$, and moreover take an effective map from the atomic expressions of $\mathcal{L}_{\mathbf{PLQP}}$ to the $(n \times n)$-tuples of variables of $\mathcal{L}_{\mathbb{C}}$, assigning

- $\hat{p} = (p_{11}, \ldots, p_{ij}, \ldots, p_{nn})$ to each atomic sentence $p \in A_{\mathcal{T}}$ of $\mathcal{L}_{\mathbf{PLQP}}$ and
- $\hat{u} = (u_{11}, \ldots, u_{ij}, \ldots, u_{nn})$ to each atomic action term $u \in A_{\mathcal{U}}$ of $\mathcal{L}_{\mathbf{PLQP}}$,

so that all these variables of $\mathcal{L}_{\mathbb{C}}$ are distinct. Moreover, let $\mathcal{U}_m(\hat{x})$ for $m \in \mathbb{N}$ be a formula of $\mathcal{L}_{\mathbb{C}}$ stating that $\hat{x}$ is an $m \times m$ unitary matrix, that is, $\mathcal{U}_m(\hat{x}) = \ulcorner \hat{x}^\dagger \hat{x} = \hat{x}\hat{x}^\dagger = \mathrm{Id}_m \urcorner$. Now define a relation $R \subseteq \mathbb{C}^{\mathrm{var}(\mathcal{L}_{\mathbb{C}})} \times \mathcal{I}$ so that, for $\alpha : \mathrm{var}(\mathcal{L}_{\mathbb{C}}) \to \mathbb{C}$ and a PLQP model $(\Sigma, [\![\cdot]\!])$, $R(\alpha, [\![\cdot]\!])$ iff

- for each $u \in A_{\mathcal{U}}$, $\mathbb{C} \vDash \mathcal{U}_n[\alpha(\hat{u})]$, that is, $\alpha(\hat{u})$ is a unitary matrix,
- for each $p \in A_{\mathcal{T}}$, $[\![p]\!]$ is the kernel of the matrix $\alpha(\hat{p})$, and
- for each $u \in A_{\mathcal{U}}$, $[\![u]\!]$ is the unitary transformation given by the unitary matrix $\alpha(\hat{u})$.

Then we have (26), as R is clearly an effective $\mathbb{C}$-coding of $\mathcal{I}$ with formulas $\rho_{\bar{x}}(\bar{y})$ given by

- $\rho_{\hat{p}}(\hat{y}) = \ulcorner 0 = 0 \urcorner$ for every propositional variable $p \in V_{\mathcal{T}}$.
- $\rho_{\hat{u}}(\hat{y}) = \mathcal{U}_n(\hat{y})$ for every action variable $u \in V_{\mathcal{U}}$.
- Suitable conditions for constant symbols $c \in C_{\mathcal{T}} \cup C_{\mathcal{U}}$.[10]

[10] For instance, if c is an action constant for the Hadamard gate, $\rho_{\hat{c}}(\hat{y})$ is a formula of $\mathcal{L}_{\mathbb{C}}$ stating that $\hat{y}$ is a matrix corresponding to the gate. Also, even though we defined $\bot$ as an abbreviation $\phi \wedge \neg\phi$ on p. 118, if we treated $\bot$ as a propositional constant for the contradiction, then we would set $\rho_{\hat{\bot}}(\hat{y}) = \ulcorner \hat{y} = \mathrm{Id}_n \urcorner$ for some $n \times n$ matrix $\hat{\bot}$ of variables of $\mathcal{L}_{\mathbb{C}}$, so that $\forall \bar{x}\, (\phi^\rho(\bar{x}) \to \phi^\delta(\vec{v}, \bar{x}))$ for $\phi = \bot$ would be $\forall \hat{\bot}\, (\hat{\bot} = \mathrm{Id}_n \to \hat{\bot}\vec{v} = \vec{0})$. On the other hand, if the interpretation of c has no suitable formula $\rho_{\hat{c}}(\hat{y})$ in $\mathcal{L}_{\mathbb{C}}$ (e.g., if it involves numbers undefinable in $\mathcal{L}_{\mathbb{C}}$), then the interpretation cannot have a $\mathbb{C}$-coding and Lemma 6.3.6 cannot be applied.

- For general $\bar{x}$, write $A = \{\, a \in A_{\mathcal{T}} \cup A_{\mathcal{U}} \mid \bar{x} \cap \hat{a} \neq \varnothing \,\}$ and $B = \{\, a_{ij} \mid a \in A$ but $a_{ij} \notin \bar{x} \,\}$. Then let $\rho_{\bar{x}}(\bar{y})$ be such that $\rho_{\bar{x}}(\bar{x}) = \ulcorner \exists z_1, \ldots, z_m \bigwedge_{a \in A} \rho_{\hat{a}}(\hat{a}) \urcorner$ for $\{z_1, \ldots, z_m\} = B$.

For (27) and (28), given any sentence ϕ of $\mathcal{L}_{\mathbf{PLQP}}$ we write $\mathrm{par}(\phi) = \bigcup\{\, \hat{a} \mid a \in A_{\mathcal{T}} \cup A_{\mathcal{U}}$ occurs in $\phi \,\}$; we use $\mathrm{par}(\phi)$ as the (variables for) parameters in our R-translation $\phi^{\delta}(\vec{v}, \mathrm{par}(\phi))$ of ϕ. Our definition of $\phi^{\delta}(\vec{v}, \mathrm{par}(\phi))$ goes recursively along the construction of ϕ. For atomic $p \in A_{\mathcal{T}}$, we have $\mathrm{par}(p) = \hat{p}$, so let our R-translation of p be $p^{\delta}(\vec{v}, \mathrm{par}(p)) = \ulcorner \hat{p}\vec{v} = \vec{0} \urcorner$; then

Fact 6.3.8. The set $A_{\mathcal{T}}$ of atomic sentences of $\mathcal{L}_{\mathbf{PLQP}}$ is effectively R-translatable.

Proof. The assignment of $\mathrm{par}(p) = \hat{p}$ and $p^{\delta}(\vec{v}, \mathrm{par}(\phi))$ to $p \in A_{\mathcal{T}}$ is clearly effective. For each $p \in A_{\mathcal{T}}$, $p^{\delta}(\vec{v}, \mathrm{par}(p))$ translates p in R because $R(\alpha, [\![\cdot]\!])$ means by definition that $[\![p]\!]$ is the kernel of the matrix $\alpha(\hat{p})$, so that $[\![p]\!] = \{\, \vec{c} \in \mathbb{C}^n \mid \alpha(\hat{p})\vec{c} = \vec{0} \,\} = p^{\delta}(\mathbb{C}, \alpha(\hat{p}))$. □

Thus (27). We then give $\phi^{\delta}(\vec{v}, \mathrm{par}(\phi))$ to compound ϕ recursively and check (28) with each connective of $\mathcal{L}_{\mathbf{PLQP}}$. For the simplest one of $\wedge$, (3) implies that $[\![\phi \wedge \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$ for each PLQP model $[\![\cdot]\!]$. Hence, given $\phi^{\delta}(\vec{v}, \mathrm{par}(\phi))$ and $\phi^{\delta}(\vec{v}, \mathrm{par}(\psi))$, we set

$$(\phi \wedge \psi)^{\delta}(\vec{v}, \mathrm{par}(\phi \wedge \psi)) = \ulcorner \phi^{\delta}(\vec{v}, \mathrm{par}(\phi)) \wedge \psi^{\delta}(\vec{v}, \mathrm{par}(\psi)) \urcorner$$

(which makes sense since $\mathrm{par}(\phi \wedge \psi) = \mathrm{par}(\phi) \cup \mathrm{par}(\psi)$), so that

$$(\phi \wedge \psi)^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\phi \wedge \psi))) = \phi^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\phi))) \cap \psi^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\psi)))$$

for every $\alpha : \mathrm{var}(\mathcal{L}_{\mathbb{C}}) \to \mathbb{C}$. Then we have

Fact 6.3.9. $\wedge$ effectively preserves R-translatability.

Proof. $\mathrm{par}(\phi \wedge \psi) = \mathrm{par}(\phi) \cup \mathrm{par}(\psi)$ and $(\phi \wedge \psi)^{\delta}(\vec{v}, \mathrm{par}(\phi \wedge \psi))$ are given clearly effectively. Moreover, if $R(\alpha, [\![\cdot]\!])$, the hypothesis that $\phi^{\delta}(\vec{v}, \mathrm{par}(\phi))$ and $\psi^{\delta}(\vec{v}, \mathrm{par}(\psi))$ translate ϕ and ψ in R, respectively, implies that

$$\begin{aligned}(\phi \wedge \psi)^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\phi \wedge \psi))) &= \phi^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\phi))) \cap \psi^{\delta}(\mathbb{C}, \alpha(\mathrm{par}(\psi))) \\ &= [\![\phi]\!] \cap [\![\psi]\!] = [\![\phi \wedge \psi]\!].\end{aligned}$$

Thus $(\phi \wedge \psi)^{\delta}(\vec{v}, \mathrm{par}(\phi \wedge \psi))$ interprets $\phi \wedge \psi$ in R. □

Let us take another case; viz., $[\phi?]$, which involves adding new parameters. (8) implies that $[\![[\phi?]\psi]\!] = {\sim}[\![\phi]\!] \sqcup ([\![\phi]\!] \wedge [\![\psi]\!])$. So, writing

$${\sim}F(\vec{v}, \bar{x}) = \ulcorner \forall \vec{w}\, (F(\vec{w}, \bar{x}) \to \langle \vec{v} \rangle\, \vec{w} = 0) \urcorner, \qquad G \sqcup H = \ulcorner {\sim}({\sim}G \wedge {\sim}H) \urcorner$$

for formulas $F(\vec{v},\bar{x})$, G and H of $\mathcal{L}_{\mathbb{C}}$, we set

$$([\phi?]\psi)^\delta(\vec{v},\mathrm{par}([\phi?]\psi)) = \ulcorner{\sim}\phi^\delta(\vec{v},\mathrm{par}(\phi)) \sqcup (\phi^\delta(\vec{v},\mathrm{par}(\phi)) \wedge \psi^\delta(\vec{v},\mathrm{par}(\psi)))\urcorner$$

(which makes sense since $\mathrm{par}([\phi?]\psi) = \mathrm{par}(\phi) \cup \mathrm{par}(\psi)$). Then $[\phi?]$ effectively preserves R-translatability; the proof is similar to the one above for Fact 6.3.9, except that here we need Fact 6.3.8 to make sure $\phi^\delta(\vec{v},\mathrm{par}(\phi))$ translates ϕ in R.

For K_I, (12) implies that $\overline{[\![K_I\phi]\!]} = \{\vec{v} \in \mathcal{H} \mid (\mathrm{Id}_I \otimes \mathcal{U})(\vec{v}) \in \overline{[\![\phi]\!]}$ for all unitary transformations $\mathcal{U}$ on $\mathcal{H}_{N\setminus I}\}$. So, with $\mathcal{H}_{N\setminus I} \cong \mathbb{C}^m$, we take $\hat{y} = (y_{11},\ldots,y_{ij},\ldots,y_{mm})$ and set

$$(K_I\phi)^\delta(\vec{v},\mathrm{par}(K_I\phi)) = \ulcorner\forall\hat{y}\,(\mathcal{U}_m(\hat{y}) \to \phi^\delta((\mathrm{Id}_I \otimes \hat{y})(\vec{v}),\mathrm{par}(\phi)))\urcorner$$

(which makes sense since $\mathrm{par}(K_I\phi) = \mathrm{par}(\phi)$). Then with an obvious routine we can show that K_I effectively preserves R-translatability.

For $\mathrm{Pr}^{\geqslant r}$, rather than using (13) straightforwardly, we observe that it implies

$$v \in \overline{[\![\overset{\geqslant r}{\mathrm{Pr}}\,\phi]\!]} \iff |\,\langle v\rangle\, w|^2 \geqslant r||v||^2||w||^2 \text{ for some non-zero } w \in {\sim\sim}\overline{[\![\phi]\!]}.$$

So we enter the following (which makes sense since $\mathrm{par}(\mathrm{Pr}^{\geqslant r}\,\phi) = \mathrm{par}(\phi)$):[11]

$$(\overset{\geqslant r}{\mathrm{Pr}}\,\phi)^\delta(\vec{v},\mathrm{par}(\overset{\geqslant r}{\mathrm{Pr}}\,\phi)) = \ulcorner\exists\vec{w}\begin{pmatrix} \vec{w} \neq \vec{0} \wedge {\sim\sim}\phi^\delta(\vec{w},\mathrm{par}(\phi)) \\ \wedge\,|\,\langle\vec{v}\rangle\,\vec{w}|^2 \geqslant r||\vec{v}||^2||\vec{w}||^2 \end{pmatrix}\urcorner.$$

Then we can show, again routinely, that $\mathrm{Pr}^{\geqslant r}$ effectively preserves R-translatability.

We can treat other connectives using the rest of the constraints in a similar manner; we list the clauses in Table 6.1. (The second half of Table 6.1 lists connectives definable in PLQP, in case one may choose a different combination of connectives than PLQP, e.g., without ¬.)

And it is routine to check

Fact 6.3.10. Each of the connectives listed above effectively preserves R-translatability.

Thus (28), and therefore, by Lemma 6.3.6, this completes our proof of Theorem 6.3.7.

6.3.4 More Applications of Our Recipe

In Subsection 6.3.3 we applied our decidability-proof recipe to PLQP; yet the recipe covers a much wider range of logics. In this subsection we mention other applications of our method.

[11] In $\mathcal{L}_{\mathbb{C}}$, we write x^2 and $x \geqslant y$ as short for $x \cdot x$ and $\exists z\,(z = z^* \wedge x = y + z^2)$, the latter of which expresses a preorder relation that, when restricted to reals, agrees with the usual order of reals.

$p^\delta(\vec{v}, \mathrm{par}(p))$	$=$	$\ulcorner \hat{p}\vec{v} = \vec{0} \urcorner$
$(\phi \wedge \psi)^\delta(\vec{v}, \mathrm{par}(\phi \wedge \psi))$	$=$	$\ulcorner \phi^\delta(\vec{v}, \mathrm{par}(\phi)) \wedge \psi^\delta(\vec{v}, \mathrm{par}(\psi)) \urcorner$
$(\neg\phi)^\delta(\vec{v}, \mathrm{par}(\neg\phi))$	$=$	$\ulcorner \phi^\delta(\vec{v}, \mathrm{par}(\phi)) \to \vec{v} = \vec{0} \urcorner$
$([u]\phi)^\delta(\vec{v}, \mathrm{par}([u]\phi))$	$=$	$\ulcorner \phi^\delta(\hat{u}\vec{v}, \mathrm{par}(\phi)) \urcorner$
$([\phi?]\psi)^\delta(\vec{v}, \mathrm{par}([\phi?]\psi))$	$=$	$\ulcorner \begin{pmatrix} \sim\phi^\delta(\vec{v}, \mathrm{par}(\phi)) \\ \sqcup\, (\phi^\delta(\vec{v}, \mathrm{par}(\phi)) \wedge \psi^\delta(\vec{v}, \mathrm{par}(\psi)) \end{pmatrix} \urcorner$
$(K_I\phi)^\delta(\vec{v}, \mathrm{par}(K_I\phi))$	$=$	$\ulcorner \forall \hat{y}\, (\mathcal{U}_m(\hat{y}) \to \phi^\delta((\mathrm{Id}_I \otimes \hat{y})(\vec{v}), \mathrm{par}(\phi))) \urcorner$
$(\mathrm{Pr}^{\geqslant r}\, \phi)^\delta(\vec{v}, \mathrm{par}(\mathrm{Pr}^{\geqslant r}\, \phi))$	$=$	$\ulcorner \exists \vec{w} \begin{pmatrix} \vec{w} \neq \vec{0} \wedge \sim\sim\phi^\delta(\vec{w}, \mathrm{par}(\phi)) \\ \wedge \lvert \langle \vec{v} \rangle\, \vec{w} \rvert^2 \geqslant r \Vert \vec{v} \Vert^2 \Vert \vec{w} \Vert^2 \end{pmatrix} \urcorner$
$(\sim\phi)^\delta(\vec{v}, \mathrm{par}(\sim\phi))$	$=$	$\ulcorner \sim\phi^\delta(\vec{v}, \mathrm{par}(\phi)) \urcorner$
$(\phi \sqcup \psi)^\delta(\vec{v}, \mathrm{par}(\phi \sqcup \psi))$	$=$	$\ulcorner \phi^\delta(\vec{v}, \mathrm{par}(\phi)) \sqcup \psi^\delta(\vec{v}, \mathrm{par}(\psi)) \urcorner$
$(\phi \vee \psi)^\delta(\vec{v}, \mathrm{par}(\phi \vee \psi))$	$=$	$\ulcorner \phi^\delta(\vec{v}, \mathrm{par}(\phi)) \vee \psi^\delta(\vec{v}, \mathrm{par}(\psi)) \urcorner$
$(\Diamond\phi)^\delta(\vec{v}, \mathrm{par}(\Diamond\phi))$	$=$	$\ulcorner \sim\phi^\delta(\vec{v}, \mathrm{par}(\phi)) \to \vec{v} = \vec{0} \urcorner$
$(A\phi)^\delta(\vec{v}, \mathrm{par}(A\phi))$	$=$	$\ulcorner \forall \vec{w}\, (\phi^\delta(\vec{w}, \mathrm{par}(\phi))) \urcorner$

Table 6.1: The recursive definition of R-translations $\phi^\delta(\vec{v}, \mathrm{par}(\phi))$ of ϕ

Quantum Versions of Modal Logics with Propositional Quantifiers In quantum reasoning we often say that there are testable properties (closed linear subspaces) or quantum actions (unitary transformations) satisfying such and such properties, and it can be useful to express this idea within a logical language. Thus one may choose to add *propositional quantifiers* (ranging over closed linear subspaces) and *action quantifiers* (ranging over unitary transformations) to the dynamic-logic-style syntax of PLQP, so that the new syntax has

$$\phi ::= \cdots \mid \forall p.\, \phi \mid \forall u.\, \phi$$

for variable symbols $p \in V_\mathcal{T}$ and $u \in V_\mathcal{U}$, and the semantics has

29. $s \in [\![\forall p.\, \phi]\!]$ iff $s \in [\![\phi]\!]'$ for every assignment $[\![\cdot]\!]' \simeq_p [\![\cdot]\!]$,

30. $s \in [\![\forall u.\, \phi]\!]$ iff $s \in [\![\phi]\!]'$ for every assignment $[\![\cdot]\!]' \simeq_u [\![\cdot]\!]$,

where we write $[\![\cdot]\!]' \simeq_a [\![\cdot]\!]$ if $[\![a']\!]' = [\![a']\!]$ for all $a' \in V_\mathcal{T} \cup V_\mathcal{U}$ except possibly a.

This is essentially a quantum (and probabilistic) version of K. Fine's "Modal Logics with Propositional Quantifiers" [58]. But, while most of the classical versions of these logics are undecidable, the *quantum version turns out to be decidable*! Indeed, our general recipe immediately provides a decidability proof for the extended logic; we just need to set

$$(\forall p.\, \phi)^\delta(\vec{v}, \mathrm{par}(\forall p.\, \phi)) = \ulcorner \forall \hat{p}\, (\rho_{\hat{p}}(\hat{p}) \to \phi^\delta(\vec{v}, \mathrm{par}(\phi))) \urcorner,$$
$$(\forall u.\, \phi)^\delta(\vec{v}, \mathrm{par}(\forall u.\, \phi)) = \ulcorner \forall \hat{u}\, (\rho_{\hat{u}}(\hat{u}) \to \phi^\delta(\vec{v}, \mathrm{par}(\phi))) \urcorner$$

and then routinely show that $\forall p$ and $\forall u$ preserve translatability.

The contrast in computational complexity between the classical and the quantum Modal Logics with Propositional Quantifiers is easily explained by noting that *our quantum quantifiers have a restricted range*: the propositional quantifiers range only over linear subspaces (and the action quantifiers over unitary maps). This is natural in a quantum context, since only linear subspaces represent *experimentally meaningful (testable) properties.* In contrast, in the classical versions, the propositional quantifiers range over *all* subsets of the state space, and thus they are essentially *second-order* quantifiers.

Logics for Mixed States All the logics we reviewed in Chapter 2.2.1 and 6.1 were about *pure states*, in the sense that $[\![\phi]\!]$ were sets of pure states. On the other hand, mixed states play a significant role in quantum reasoning, and therefore one may consider a semantics given in terms of mixed states, so that $[\![\phi]\!]$ are then sets of density matrices on $\mathcal{H}$. It is easy to see our recipe for the decidability proof readily extends to such a semantics (although Definition 6.3.2 needs modifying so that $[\![\phi]\!] \subseteq \mathbb{C}^{n\times n}$).

Chapter 7

Conclusions

In this chapter we summarise the results of this thesis and look at possible new directions of research that build on the results of this thesis. In Section 7.1 you will find a summery by themes. In Section 7.2, we discuss new questions and new research directions in the three themes mentioned in the introduction: relating different quantum structures, axiomatising the quantum logics and decidability.

7.1 Summary

Relating algebraic and spatial quantum structures. In Chapter 3, we provided duality results connecting Piron lattices and quantum dynamic frames. We introduced the categories $\mathbb{L}_w$ and $\mathbb{L}_s$ of Píron lattices with weak and strong homomorphisms respectively. We introduced the categories $\mathbb{F}_w$ and $\mathbb{F}_s$ of quantum dynamic frames with weak and strong homomorphisms respectively. We have defined a functor F_w from $\mathbb{L}_w$ to $\mathbb{F}_w$ and a functor G_w from $\mathbb{F}_w$ to $\mathbb{L}_w$. We similarly have functors F_s and G_s between $\mathbb{L}_s$ and $\mathbb{F}_s$. We have shown that (F_s, G_s) forms a duality between categories $\mathbb{L}_s$ and $\mathbb{F}_s$ and that (F_w, G_w) forms a duality between categories $\mathbb{L}_w$ and $\mathbb{F}_w$. We have also shown that these dualities are preserved when restricting these categories to those objects that satisfy Mayet's condition. This result establishes, on one direction of the duality, that quantum dynamic frames represent quantum structures correctly; on the other direction, it gives rise to a representation of dynamics on a Píron lattice.

Desinging new quantum logics. In Chapter 4, we have introduced a quantum hybrid logic and an alternative definition of quantum Kripke frames, which we have shown are equivalent to the original definition of quantum Kripke frames (Definition 2.2.15), except they have finite dimension n. This logic is shown to be at least as expressive as the logic for quantum actions and can express atomic propositions using nominals, allowing us to express, for example, a basis.

In Chapter 5 and Chapter 6, we introduced two logics that build on earlier work on dynamic quantum logic [11, 15, 16], which developed quantum versions of propositional dynamic logic. Those earlier logics could prove the correctness of many non-probabilistic quantum protocols, but they were not suited for those protocols where probabilities play an essential role. The two different versions of the logic PLQP introduced in these chapters overcome this limitation by adding a quantum-probabilistic operator. The version in Chapter 5 adds a separability operator, to discuss important properties of quantum theory, like a particular type of basis. As a consequence, we showed that PLQP can express the correctness of three probabilistic quantum protocols, viz. the BB84 protocal, the quantum search algorithm and a quantum leader election protocol.

Axiomatising quantum logics. In Chapter 4, we have introduced four new axioms to charactarise the properties of a quantum Kripke frame. We showed that these axioms combined with a standard aximatisation of hybrid logic is complete with respect to quantum Kripke frames of dimension at most n.

In Chapter 5, we lay a foundation for an axiomatisation of probabilistic quantum logics in the style of propositional dynamic logic. The axiomatisation provided in this work is powerful enough to prove the correctness of quantum protocols, such as the quantum leader election of [47] and the BB84 quantum key distribution [21]. As probability plays an important role in so many quantum protocols, we expect that our logic can be used and adapted to a much wider range of quantum protocols.

Decidability of a class of Hilbert space based quantum logics. In Chapter 6 we introduce a general proof method to show that a Hilbert space based (quantum) logic is decidable. We use this method to show that PLQP introduced in this chapter is decidable. We believe this result to be of interest for research in both quantum logic and quantum computation, as it shows that quantum logic has a great computational advantage over its classical variants (which are known to be undecidable).

7.2 Future work

How do probabilistic quantum structures relate to each other? The quantum structures discussed in Chapter 3 are concerned with non-probabilistic single quantum systems. Future work may involve forming dualities between algebraic and set theoretic quantum structures that are even richer. Adding probability to the setting may be a useful step to take, and there exist dualities involving probability already, such as [75].

How do quantum structures based on the non-orthogonality relation relate to each other? Another line of future investigation is to develop categories and duality or correspondence results relating to a variation of quantum dynamic frames that do not have parametrized relations, but rather just the non-orthogonality relation.

Can we find a complete axiomatisation for the Probabilstic Logic for Quantum Programs (PLQP)? In Chapter 5, we introduced a sound axiomatisation for PLQP. In Chapter 4, we introduced a complete axiomatisation for Quantum Hybrid Logic (QHL). One could consider to change the syntax of PLQP so that it extends QHL and add to the deductive systems of Chapter 4 the axioms from Chapter 5. This could be the basis for a richer completeness result. Incorporating multi-partite systems will be a greater challenge, as there exists no obvious definition of a tensor product for quantum Kripke models (as shown by Randall and Foulis in [88]).

Can we extend PLQP so that it can express the creation of the W-state? The sound axiomatisation discussed in Chapter 5 may pave the way for more powerful axiomatic systems of stronger logics. For example, an axiomatic analysis of the construction of the W-state is left for future work; such an analysis would benefit from a more powerful logic that explicitly reasons about unitary operations. When involving unitaries for quantum protocols and programs, it would be further beneficial to either characterise commonly used logic gates, such as the Hadamard gate, or to include them as constants.

Can we extend PLQP so that it can express classical and quantum communication? Another potential extension of PLQP is to add the power to explicitly express both the quantum and classical communication involved in various protocols. This may help in expressing important properties of a communication rich variant of the quantum leader election protocol given in [98], as well as the relationships among the classical and quantum communication in the quantum teleportation protocol. This line of work would build further on the idea of a quantum dynamic epistemic logic mentioned in [18] and on the work in [17]. We also hope that future work will clarify the prospects for a complete proof system.

Can we find a more efficient decidability algorithm? The result in Chapter 6 concerns decidability, but one could also be concerned about the actual decision procedures and their complexity. We referred to Tarski's [99] theorem because it was the first to show $\mathbb{T}_{\mathbb{C}}$ to be decidable; yet there have been more efficient procedures proposed for $\mathbb{T}_{\mathbb{C}}$, such as one by Collins [43] (see also [36]), that improve the particular decision procedure Tarski gave. Given the applicability of our logic, it would be of practical value to devise more efficient procedures, or to find useful fragments for which more efficient procedures are available.

Bibliography

[1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th IEEE conference on Logic in Computer Science (LiCS'04)*, pages 415–425. IEEE Press, 2004.

[2] Samson Abramsky and Bob Coecke. Categorical quantum mechanics. In Daniel Lehmann, Kurt Engesser, and Dov M. Gabbay, editors, *Handbook of Quantum Logic and Quantum Structures*, pages 261 – 323. Elsevier, Amsterdam, 2009.

[3] Diederik Aerts. Quantum axiomatics. In Kurt Engesser, Dov M. Gabbay, and Daniel Lehmann, editors, *Handbook of Quantum Logic and Quantum Structures*, pages 79–126. Elsevier Science B.V., Amsterdam, 1st edition, 2009.

[4] Diederik Aerts and Massimiliano Sassoli de Bianchi. The extended bloch representation of quantum mechanics and the hidden-measurement solution to the measurement problem. *Annals of Physics*, 351:975 – 1025, 2014.

[5] C. Areces and Balder ten Cate. Hybrid logic. In Johan Van Benthem Patrick Blackburn and Frank Wolter, editors, *Handbook of Modal Logic*, volume 3 of *Studies in Logic and Practical Reasoning*, chapter 14, pages 821–868. Elsevier, 2007.

[6] Gennaro Auletta and Giorgio Parisi. *Foundations and interpretation of quantum mechanics*. World Scientific, 2001.

[7] Steve Awodey. *Category Theory*. Oxford University Press, 2006.

[8] Alexandru Baltag, Jort Bergfeld, Kohei Kishida, Joshua Sack, Sonja Smets, and Shengyang Zhong. PLQP & company: Decidable logics for quantum algorithms. *International Journal of Theoretical Physics*, 53(10):3628–3647, 2014.

[9] Alexandru Baltag and Sonja Smets. The logic of quantum programs. In Peter Selinger, editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages*, pages 39–56. Turku Centre for Computer Science, 2004.

[10] Alexandru Baltag and Sonja Smets. Complete axiomatizations for quantum actions. *International Journal of Theoretical Physics*, 44(12):2267–2282, 2005.

[11] Alexandru Baltag and Sonja Smets. LQP: the dynamic logic of quantum information. *Mathematical Structures in Computer Science*, 16(3):491–525, 2006.

[12] Alexandru Baltag and Sonja Smets. A dynamic-logical perspective on quantum behavior. *Studia Logica*, 89(2):187–211, 2008.

[13] Alexandru Baltag and Sonja Smets. Correlated knowledge: an epistemic-logic view on quantum entanglement. *International Journal of Theoretical Physics*, 49(12):3005–3021, 2010.

[14] Alexandru Baltag and Sonja Smets. Correlated information: a logic for multi-partite quantum systems. *Electronic Notes in Theoretical Computer Science*, 270(2):3–14, 2011.

[15] Alexandru Baltag and Sonja Smets. Quantum logic as a dynamic logic. *Synthese*, 179(2):285–306, 2011.

[16] Alexandru Baltag and Sonja Smets. The dynamic turn in quantum logic. *Synthese*, 186(3):753–773, 2012.

[17] Alexandru Baltag and Sonja Smets. Reasoning about classical and quantum interaction. Presentation at the Logic Colloquium, Helsinki, August 2015.

[18] Alexandru Baltag and Sonja Smets. Modeling correlated information change: from conditional beliefs to quantum conditionals. *Soft Computing*, 21(1523), 2017.

[19] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[20] Enrico Beltrametti and Gianni Cassinelli. *The Logic of Quantum Mechanics.* Encyclopedia of Mathematics and Its Applications. Addison-Wesley Publishing Company, 1981.

[21] Charles H. Bennett and Giles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. Bangalore, India, 1984.

[22] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, Part 1:7–11, 2014. Theoretical Aspects of Quantum Cryptography – Celebrating 30 years of BB84.

[23] Johan van Benthem. *Modal Correspondence Theory*. PhD thesis, Universiteit van Amsterdam, 1976.

[24] Johan van Benthem. *Modal Logic and Classical Logic*. Bibliopolis, 1983.

[25] Jort M. Bergfeld, Kohei Kishida, Joshua Sack, and Shengyang Zhong. Duality for the logic of quantum actions. *Studia Logica*, 103(4):781–805, August 2015.

[26] Jort Martinus Bergfeld and Joshua Sack. Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs. *Soft Computing*, 21(6):1421–1441, March 2017.

[27] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer-Verlag, 2009.

[28] Eli Biham, Michel Boyer, PO Boykin, and Tal Mor. A proof of the security of quantum key distribution. *Journal of cryptology*, 19:381–439, December 2006.

[29] Garrett Birkhoff. *Lattice Theory*. American Mathematical Society, 3rd edition, 1967.

[30] Garrett Birkhoff and John von Neumann. The Logic of Quantum Mechanics. *The Annals of Mathematics*, 37:823–843, 1936.

[31] Patrick Blackburn and Balder ten Cate. Pure extensions, proof rules, and hybrid axiomatics. *Studia Logica*, 84(2):277–322, 2006.

[32] Patrick Blackburn, Martin de Rijke, and Yde Venema. *Modal Logic*. Cambridge University Press, 2001.

[33] Patrick Blackburn and Jerry Seligman. Hybrid languages. *Journal of Logic, Language and Information*, 4:251–272, 1995.

[34] Patrick Blackburn and Johan Van Benthem. Modal logic: A semantic perspective. In Patrick Blackburn, Johan Van Benthem, and Frank Wolter, editors, *Handbook of modal logic*, pages 1–84. Elsevier, Amsterdam, 2006.

[35] D. Bohm and J. Bub. A proposed solution of the measurement problem in quantum mechanics by a hidden variable theory. *Review of Modern Physics*, 38:453–469, July 1966.

[36] Bob F Caviness and Jeremy R Johnson. *Quantifier elimination and cylindrical algebraic decomposition.* Springer, 1998.

[37] Rohit Chadha, Paulo Mateus, and Amílcar Sernadas. Reasoning about imperative quantum programs. *Electron. Notes Theor. Comput. Sci.*, 158:19–39, May 2006.

[38] Rohit Chadha, Paulo Mateus, Amílcar Sernadas, and Cristina Sernadas. Extending classical logic for reasoning about quantum systems. In Daniel Lehmann, Kurt Engesser, and Dov M. Gabbay, editors, *Handbook of Quantum Logic and Quantum Structures: Quantum Logic*, pages 325–371. Elsevier, 2009.

[39] Maria Luisa Dalla Chiara and Roberto Giuntini. Quantum logics. In Dov M. Gabbay and Franz Guenthner, editors, *Handbook of Philosophical Logic*, pages 129–228. Kluwer Academic Publishers, 2002.

[40] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course In Quantum Theory and Diagrammatic Reasoning.* Cambridge University Press, March 2017.

[41] Bob Coecke and Sonja Smets. The Sasaki hook is not a [static] implicative connective but induces a backward [in time] dynamic one that assigns causes. *International Journal of Theoretical Physics*, 43:1705–1736, 2004.

[42] David W. Cohen. *An Introduction to Hilbert Space and Quantum Logic.* Problem Books in Mathematics. Springer-Verlag, New York, 1989.

[43] George E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In H. Brakhage, editor, *Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975*, pages 134–183, Berlin, 1975. Springer.

[44] Maria Luisa Dalla Chiara, Roberto Giuntini, and Richard Greechie. *Reasoning in quantum theory: sharp and unsharp quantum logics*, volume 22 of *Trends in logic.* Kluwer Acadamic Press, Dordrecht, 2004.

[45] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[46] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.

[47] Ellie D'Hondt and Prakash Panangaden. The computational power of the W and GHZ states. *Quantum Info. Comput.*, 6(2):173–183, March 2006.

[48] Ellie D'Hondt and Prakash Panangaden. Quantum weakest preconditions. *Mathematical Structures in Computer Science*, 16:429–451, 6 2006.

[49] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[50] J. Michael Dunn, Tobias J. Hagge, Lawrence S. Moss, and Zhenghan Wang. Quantum logic as motivated by quantum computing. *The Journal of Symbolic Logic*, 70:353–359, 6 2005.

[51] J. Michael Dunn, Lawrence S. Moss, and Zhenghan Wang. Editors' introduction: The third life of quantum logic: Quantum logic inspired by quantum computing. *Journal of Philosophical Logic*, 42(3):443–459, 2013.

[52] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[53] Ronald Fagin and Joseph Y. Halpern. Reasoning About Knowledge and Probability . *Journal of the ACM*, 41(2):340–367, 1994.

[54] Ronald Fagin, Joseph Y. Halpern, and Nimrod Megiddo. A logic for reasoning about probabilities. *Information and Computation*, 87(1):78–128, 1990.

[55] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about knowledge*. MIT press Cambridge, 1995.

[56] Claude-Alain Faure. An elementary proof of the fundamental theorem of projective geometry (dedicated to Alfred Frölicher). *Geometriae Dedicata*, 90(1):145–151, 2002.

[57] Yuan Feng, Nengkun Yu, and Mingsheng Ying. Model checking quantum Markov chains. *Journal of Computer and System Sciences*, 79(7):1181 – 1198, 2013.

[58] Kit Fine. Propositional quantifiers in modal logic. *Theoria*, 36(3):336–346, 1970.

[59] Michael J. Fischer and Richard E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Sciences*, 18(2):194 – 211, 1979.

[60] D. Foulis and C.H. Randall. Tensor products of quantum logics do not exist. *Notices of the American Mathematical Society*, 26(6), 1979.

[61] Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. QMC: A model checker for quantum systems. In *Proceedings of the 20th international conference on Computer Aided Verification*, CAV '08, pages 543–547, Berlin, Heidelberg, 2008. Springer-Verlag.

[62] Robert I. Goldblatt. Semantic analysis of orthologic. *Journal of Philosophical Logic*, 3(1-2):19–35, 1974.

[63] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325, 1997.

[64] Amar Hadzlhasanovic. *The algebra of entanglement and the geometry of composition*. PhD thesis, University of Oxford, 2017. arXiv:1709.08086.

[65] David Harel, Jerzy Tiuryn, and Dexter Kozen. *Dynamic Logic*. MIT Press, Cambridge, MA, USA, 2000.

[66] Matthew Hennessy and Robin Milner. *On observing nondeterminism and concurrency*. Springer, 1980.

[67] J. Hintikka. *Knowledge and belief: an introduction to the logic of two notions*. Cornell University Press, 1962.

[68] Tony C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, October 1969.

[69] Ian Hodkinson and Mark Reynolds. Temporal logic. In Patrick Blackburn, Johan Van Benthem, and Frank Wolter, editors, *Handbook of Modal Logic*, volume 3 of *Studies in Logic and Practical Reasoning*, chapter 11, pages 655 – 720. Elsevier, 2007.

[70] AS Holevo. Some estimates for information quantity transmitted by quantum communication channel (rus). *Problems of Information Transmission*, 9(3):3–11, 1973.

[71] K. Husimi. Studies on the foundations of quantum mechanics i. In *Proceedings of Physico-Mathematical Society Japan*, volume 9, pages 766–778, 1937.

[72] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics. *arXiv:quant-ph/1705.11151*, February 2018.

[73] Peter T. Johnstone. *Stone spaces*. Cambridge University Press, 1982.

[74] Gudrun Kalmbach. *Orthomodular Lattices*. Acadamic Press, New York, 1983.

[75] D. Kozen, K.G. Larsen, R. Mardare, and P. Panangaden. Stone duality for markov processes. In *Logic in Computer Science (LICS), 2013 28th Annual IEEE/ACM Symposium on*, pages 321–330, June 2013.

[76] Daniel Lehmann, Kurt Engesser, and Dov M. Gabbay, editors. *Handbook of Quantum Logic and Quantum Structures.* Elsevier, Amsterdam, 2007.

[77] Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer verlag, New York, second edition, 1998.

[78] P. Mateus, J. Ramos, A. Sernadas, and C. Sernadas. Temporal logics for reasoning about quantum systems. In I. Mackie and S. Gay, editors, *Semantic Techniques in Quantum Computation*, pages 389–413. Cambridge University Press, 2010.

[79] P. Mateus and A. Sernadas. Weakly complete axiomatization of exogenous quantum propositional logic. *Inf. Comput.*, 204(5):771–794, May 2006.

[80] René Mayet. Some characterizations of the underlying division ring of a Hilbert lattice by automorphisms. *International Journal of Theoretical Physics*, 37:109–114, 1998.

[81] D.J. Moore. Categories of representations of physical systems. *Helvetica Physica Acta*, 68:658–678, 1995.

[82] D.J. Moore. On state spaces and property lattices. *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, 30(1):61–83, 1999.

[83] M.P. Solèr. Characterization of Hilbert spaces by orthomodular spaces. *Communications in Algebra*, 23(1):219–243, 1995.

[84] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2011.

[85] Hirokazu Nishimura. Gentzen methods in quantum logic. In Daniel Lehmann, Kurt Engesser, and Dov M. Gabbay, editors, *Handbook of Quantum Logic and Quantum Structures*, pages 227 – 260. Elsevier, Amsterdam, 2009.

[86] Constantin Piron. *Foundations of Quantum Physics.* W.A. Benjamin Inc., 1976.

[87] Arthur N. Prior. *Past, Present and Future.* Oxford University Press, 1967.

[88] Charles Randall and David Foulis. Tensor products of quantum logics do not exist. *Notices Amer. Math. Soc.*, 26(6), 1979.

[89] Michael Reed and Barry Simon. *Functional Analysis*, volume 1 of *Methods of Modern Mathematical Physics.* Academic Press, first edition edition, January 1980.

[90] Frigyes Riesz. Sur une espèce de géométrie analytique des systèmes de fonctions sommables. *Comptes Rendus de l'Académie des Sciences*, 144:1409–1411, 1907.

[91] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Review of Modern Physics*, 76:1267–1305, Februari 2005.

[92] Peter Selinger. Dagger compact closed categories and completely positive maps: (extended abstract). *Electronic Notes in Theoretical Computer Science*, 170(0):139 – 163, 2007. Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005).

[93] Peter Selinger. Finite dimensional Hilbert spaces are complete for dagger compact closed categories (extended abstract). *Electronic Notes in Theoretical Computer Science*, 270(1):113 – 119, 2011. Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008).

[94] Peter Selinger. Finite dimensional hilbert spaces are complete for dagger compact closed categories. *Logical Methods in Computer Science*, 8:1–12, 2012.

[95] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Shafi Goldwasser, editor, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society Press, 1994.

[96] Sonja Smets and Alexandru Baltag. Logics for Quantum Information Flow, presented at the 18-th European Summer School of Logic, Language and Information. http://www.vub.ac.be/CLWF/SS/slides.html, 2006.

[97] Marshall H. Stone. The theory of representations for Boolean algebras. *Transactions of the American Mathematical Society*, 40:37–111, 1936.

[98] Seiichiro Tani, Hirotada Kobayashi, and Keiji Matsumoto. Exact quantum algorithms for the leader election problem. *ACM Trans. Comput. Theory*, 4(1):1:1–1:24, March 2012.

[99] A. Tarski. *A decision method for elementary algebra and geometry.* RAND Corporation, Santa Monica, 1948.

[100] Yde Venema. Algebras and coalgebras. In Patrick Blackburn, Johan van Benthem, and Frank Wolter, editors, *Handbook of Modal Logic*, volume 3 of *Studies in Logic and Practical Reasoning*, pages 331–426. Elsevier, 2007.

[101] John Von Neumann. *Mathematische grundlagen der quanten-mechanik.* Springer, Berlin, 1932.

[102] Alexander Wilce. Quantum logic and probability theory. http://plato.stanford.edu/archives/fall2012/entries/qt-quantlog/, 2012.

[103] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, October 1982.

[104] Noson S. Yanofsky and Mirco A. Mannucci. *Quantum Computing for Computer Scientists.* Cambridge University Press, New York, 2008.

[105] Mingsheng Ying, Nengkun Yu, Yuan Feng, and Runyao Duan. Verification of quantum programs. *Science of Computer Programming*, 78(9):1679 – 1700, 2013.

[106] W Yong, W Huadeng, L Zhaohong, and H Jinxiang. Man-in-the-middle attack on BB84 protocol and its defence. In *Proceedings 2009 2nd IEEE International Conference on Computer Science and Information Technology ICCSIT 2009*, pages 438–439, 2009.

[107] Shengyang Zhong. *Orthogonality and Quantum Geometry – Towards a Relational Reconstruction of Quantum Theory.* PhD thesis, Universiteit van Amsterdam, 2015.

Samenvatting

In de eerste helft van de twintigste eeuw ontdekten natuurkundigen dat de allerkleinste deeltjes van ons universum de klassieke wetten van Newton niet respecteren, in plaats daarvan volgen ze de wetten die nu bekend staan als de quantum mechanica. Quantum mechanica heeft een enorme invloed gehad op informatie theorie: het toepassen van de nieuwe technieken uit de quantum mechanica heeft geleid tot nieuwe communicatie protocollen die eigenschappen bezitten waarvan men denkt dat ze met klassieke computer technieken onmogelijk zijn. Ook bestaan er quantum computer algoritmes die bewezen sneller zijn dan hun klassieke tegenhangers.

Net zoals logica een fundamentele rol speelt voor klassieke informatie theorie, zal de quantum logica een rol gaan spelen voor quantum informatie theorie. De rol van logica zal belangrijk worden bij het ontwerpen van computer algoritmes, zeker bij het specificiëren en verifiëren. Dit proefschrift concentreert zich op het verband tussen quantum logica en quantum informatie theorie en brengt resultaten in de volgende vier thema's.

Algebraïsche en ruimtelijke structuren relateren. In Hoofdstuk 3 bestuderen we een dualiteit tussen twee verschillende quantum structuren: *Píron tralies* en *dynamische quantum modellen*. Beide zijn abstracties van Hilbert ruimtes, een van de standaard modellen voor het representeren van een quantum systeem. Beide structuren benadrukken andere eigenschappen van een quantum systeem en door ze te verbinden via een dualiteit kunnen we laten zien hoe deze eigenschappen gerelateerd zijn aan elkander.

Píron tralies geven een algebraïsch perspectief op een Hilbert ruimte en de focus ligt met name op de *testbare eigenschappen* van een fysiek quantum systeem. De definitie van een Píron tralie legt zulke beperkingen op een standaard tralie dat het precies de structuur van een algemene Hilbert ruimte[1] representeert. Een Píron tralie die daarnaast ook voldoet aan Mayet's conditie, representeert een

[1] Algemene Hilbert ruimte zijn bijna, maar niet helemaal gelijk aan een Hilbert ruimte.

oneindig dimensionale Hilbert ruimte over de complexe getallen, de reële getallen of de quaternionen. Dynamische quantum modellen zijn een vorm van gemerkte transitie systemen en geven een *dynamisch* perspectief op fysieke quantum systemen.

Om een volledige categorische structuur te creëren, koppelen we zowel Píron tralies als dynamische quantum modellen aan twee verschillende type morfismen. Het eerste type is geïntroduceerd door Moore voor zwakkere structuren die een aantal quantum eigenschappen, zoals superpositie, niet representeren. Het tweede type door onszelf geïntroduceerd is een sterkere variant die meer structuur behoudt.

Ons dualiteitsresultaat in Hoofdstuk 3 laat zien dat de categorieën van Píron tralies en dynamisch quantum modellen in essentie hetzelfde zijn (met uitzondering van de richting van de morfismen). We laten tevens zien dat de dualiteit beperkt kan worden tot objecten die voldoen Mayet's condities. Aangezien het al aangetoond is dat Píron tralies equivalent zijn met Hilbert ruimtes, laat dit resultaat ook de sterke relatie zien tussen dynamische quantum modellen en Hilbert ruimtes. Zowel Píron tralies als dynamische quantum structuren zijn belangrijke structuren in de quantum logica, en ons dualiteitsresultaat laat nieuw licht schijnen op het wiskundige verband tussen deze twee structuren.

Het ontwerpen van hybride en probabilistiche quantum logica's. In dit proefschrift introduceren we twee nieuwe logische systemen: *Quantum Hybride Logica (QHL)* en *Probabilistische Logica voor Quantum Programma's (PLQP).*

In Hoofdstuk 4 introduceren we quantum hybride logica (QHL). Dit betekent dat we naast de "standaard" quantum modale operatoren zoals negatie ($\neg$), doorsnede ($\wedge$) en orthogonaliteit ($\Box$), we een extra verzameling propositie letters hebben, de nominalen, speciaal voor het benoemen van een enkel punt (of atoom) in ons model. De syntax van deze nieuwe logica is in feite exact hetzelfde als de standaard hybride logica (met een hier-pijl operator), maar het deductief systeem wordt uitgebreid met vier nieuwe axioma's die de eigenschappen van de door Zhong geïntroduceerde quantum Kripke modellen representeren. Voor het volledigheidsresultaat moet dat model nog uitgebreid worden met een nieuwe eigenschap, die er voor zorgt dat het model een eindige dimensie heeft. Deze nieuwe eigenschap zorgt er tevens voor dat de QHL het concept van een basis kan uitdrukken.

We laten zien dat de taal de standaard eigenschappen van de quantum logica kan uitdrukken, zoals het orthogonale complement en de quantum vereniging. Aangezien quantum Kripke modellen equivalent zijn aan dynamische quantum modellen, kunnen we deze taal beschouwen als een uitbreiding op de Logica voor Quantum Acties (LQA), die door Baltag en Smets is geïntroduceerd. En inderdaad laten we in Hoofdstuk 4 zien dat alle operatoren van deze logica uitdrukbaar zijn in QHL.

De nieuwe logische systemen voor quantum redeneren die worden geïntroduceerd in Hoofdstuk 5 en Hoofdstuk 6 komen tot stand door de al bestaande systemen voor quantum logica, modale logica en probabilistische logica te combineren. Dit geeft ons een probablistische uitbreiding van de al bestaande Logica van Quantum Programma's (LQP). De taal bevat *dynamische modaliteiten* $[\pi]$ voor quantum programma's π en *epistemische* modaliteiten K_I voor het uitdrukken van de informatie die beschikbaar is voor het subsysteem I. Naast de dynamische en epistemische modaliteiten, voegen we *probabilistische modaliteiten* toe, die de kans uitdrukt dat een gegeven test (van een quantum testbare eigenschap) zal slagen. Dit is een nieuwe aanvulling op de al bestaande logica's die de uitdrukbaarheid van de logica enorm uitbreidt. Hierdoor wordt deze formele taal geschikt voor het verifiëren van probabilistische quantum algoritmes.

In Hoofdstuk 5 drukken we de correctheid uit van het BB84 quantum sleutel protocol en van het quantum leiderverkiezingsprotocol. In Hoofdstuk 6 drukken we de correctheid van Grover's zoekalgoritme uit.

Het axiomatiseren van quantum logica's (QHL en PLQP). In Hoofdstuk 4, geven we een correctheids- en volledigheidsresultaat voor de quantum hybride logica die hierboven beschreven is in de context van quantum Kripke modellen met een dimensie van ten hoogste n. Aangezien de taal zeer veel lijkt op standaard hybride logica, bouwen we verder op een volledigheidsresultaat dat al bestaat voor een grote groep hybride logica's. We laten zien dat een deel van onze quantum hybride logice binnen deze groep valt, terwijl een ander deel extra werk vereist om volledigheid te bewijzen. We laten zien dat drie van de vier nieuwe axioma's een model eigenschap definiëren. Dat wil zeggen, het model bezit een bepaalde eigenschap dan en slechts dan als het model het axioma valideert.

In Hoofdstuk 5 leggen we een fundering voor een axiomatisering van de hierboven beschreven probabilistische logica voor quantum programma's (PLQP). We laten zien dat ons nieuwe bewijssysteem correct is. We bewijzen een lange lijst van lemma's met basis (en minder basis) eigenschappen van quantum theorie, zoals onder andere eigenschappen van het orthogonale complement, de quantum vereniging en een orthogonale basis. Het bewijssysteem samen met deze lange lijst van lemma's gebruiken we vervolgens om de correctheid van het quantum leiderverkiezingsprotocol en het BB84 quantum sleutel distributie protocol te bewijzen. Deze twee protocollen zijn bedoeld als voorbeeld wat met ons system bewezen kan worden, maar we zijn er zeker van dat er meer mogelijk is. Deze logica is enkel bedoeld als eerste stap en vraagt om verder onderzoek naar in het bijzonder probabilistische quantum logica's.

Beslisbaarheid voor een groep van op Hilbert ruimte gebaseerde quantum logica's. In het laatste deel van dit proefschrift laten we zien dat een grote groep op Hilbert ruimte gebaseerde quantum logica's, waaronder de hierboven beschreven Probabilistische Logica voor Quantum Programma's (PLQP), beslisbaar is. Een beslisbaarheidsbewijs voor een logica bestaat in essentie uit het laten zien dat er een effective procedure bestaat om the controleren of een formule valide (of vervulbaar) is of niet.

We laten een algemene methode zien voor het bewijzen van beslisbaarheid voor een groot aantal quantum logica's, waaronder de logica in Hoofdstuk 6. Het idee achter deze methode komt van het werk van Dunn et. al. Zij vertaalde standaard quantum logica over eindig dimensionale ruimtes naar eerste order theorie van reële getallen, die beslibaar is vanwege Tarski's beroemde stelling. We breiden deze methode uit naar een veel grotere groep van quantum logica's, door een inductieve methode te introduceren die checkt of er voor een taal een effectieve vertaling bestaat naar de eerste order theorie van de reële getallen. Simpel gezegd, als een propositionele of atomistische formule effectief vertaald kan worden, en elke n-voudige operator behoud deze effectieve vertaling, dan is de taal als geheel beslisbaar. Deze methode passen we toe op PLQP en daarmee laten we zien dat deze beslisbaar is.

Abstract

In the first half of the twentieth century physicists discovered that elementary particles do not obey the classical Newtonian laws, instead obeying different laws. These laws are now known as the laws of quantum mechanics. Quantum mechanics has a tremendous influence on information theory and computer science. Incorporating quantum mechanics into information theory has led to new communication protocols that achieve goals deemed to be impossible by using classical computational techniques. Quantum mechanics also offers great opportunities for computer science: several alogrithms incorporating quantum mechanical techniques have been proven to be proven faster than any classical algorithm.

Similar as for classical computing, logic plays a fundamental role in the theory of quantum computing. The role of logic becomes central when we look at the design of quantum programs, especially when we look at their specification and verification. This thesis is positioned at the interface between quantum logic and quantum computation and contributes to the field in the following four themes.

Relating algebraic and spatial quantum structures. In Chapter 3 we study the duality of two different quantum structures, *Píron lattices* and *quantum dynamic frames*, which both are abstractions of Hilbert spaces, a standard tool for representing quantum systems. Both structures emphasize different properties of a quantum system and relating them shows how these different properties are connected.

Píron lattices provide an algebraic perspective on Hilbert spaces and focus on *testable properties* of a quantum physical system. A Píron lattice is such a lattice with the appropriate constraints for it to capture the abstract structure of a generalized Hilbert space, which is not exactly, but quite close to a normal Hilbert space. A Píron lattice that satisfies “Mayet’s condition” captures the structure of an infinite dimensional Hilbert space over the complex numbers, reals, or quaternions. Quantum dynamic frames are a type of labelled transition

systems and provide a *dynamic* perspective on quantum systems.

To provide a full categorical structure for both Píron lattices and quantum dynamic frames, we consider two types of morphisms for each of the frames and the lattices. One type is that defined by Moore for two weaker structures that do not capture superposition, an important property of quantum theory: state spaces (symmetric anti-reflexive frames that separate points) and property lattices (complete atomistic orthocomplemented lattices). We also define stronger types of morphisms for both the Píron lattices and quantum dynamic frames. Both Píron lattice morphisms act directly on properties, while both quantum dynamic frame morphisms act directly on states.

Our duality result in Chapter 3 shows that quantum dynamic frames and Píron lattices form categories that are essentially the same (except for the direction of morphisms). We also show that this relation can be restricted to the objects satisfying Mayet's condition. As Píron lattices satisfying Mayet's condition have already been shown to be equivalent to Hilbert spaces, this result clarifies the close relationship that quantum dynamic frames have with Hilbert spaces. The structures of both quantum dynamic frames and Píron lattices are each a focal point of quantum logic, and hence our duality adds a new perspective to the formal relation between these different quantum structures.

Designing hybrid and probabilistic quantum logics (QHL and PLQP). We design two new logical systems: *Quantum Hybrid Logic (QHL)* and *Probabistic Logic for Quantum Programs (PLQP).*

In Chapter 4 we introduce a quantum hybrid logic (QHL), which means that next to the "standard modal operators" of negation (¬), intersection (∧) and non-orthogonality (□), we add a special set of proposition letters called nominals, which refer to singleton states or atoms. The syntax of this logic is in fact equivalent to standard hybrid logic (with down arrow), but the standard deductive system is extended with four new axioms that are used to capture the properties of a quantum Kripke model which have been introduced by Zhong, with one new condition, which states the model has to have finite dimension. The axiom for this extra condition also shows QHL can express the concept of a basis.

We show the language can express standard quantum properties like orthocomplement and quantum join. As quantum Kripke models are equivalent to quantum dynamic frames, one could consider this logic to be an extension of the logic for quantum actions, introduced by Alexandru Baltag and Sonja Smets. Indeed, in Chapter 4 we show that all operators of the logic for quantum actions are in fact expressible in this quantum hybrid logic

The new logical system that we introduce for quantum reasoning in Chapter 5 and Chapter 6 is based on combining already existing formalisms of quantum logic, modal logic and probability logic. This gives us a Probabilistic Logic of Quantum Programs (PLQP), that extends a version of the older Logic of Quan-

tum Program (LQP). The language contains *dynamic modalities* $[\pi]$ (for quantum programs π) as well as "epistemic" modalities K_I (capturing the information that is 'known' to subsystem I, i.e. it is carried by the local state of subsystem I). In addition to the dynamic and epistemic modalities, the logic PLQP presented in Chapter 5 and Chapter 6 is endowed with a *probabilistic modality*, capturing the probability that a given test (of a quantum-testable property) will succeed. This is a novel feature, that greatly enhances the expressivity of the logic, allowing us to use it for the verification of probabilistic quantum algorithms.

In Chapter 5 we express the BB84 protocol and the quantum leader election protocol. In Chapter 6 we express the correctness of the Grover's search algorithm.

Axiomatising quantum logics (QHL and PLQP). In Chapter 4, we provide a soundness and a completeness result for the quantum hybrid logic discussed above with respect to quantum Kripke frames of dimension at most n. As the language is very similar to standard hybrid logic, this result builds on a completeness result for a large class of hybrid logics. We show that part of our quantum hybrid logic falls inside this class for which the completeness result applies, while another part of our logic needs additional work to prove completeness. We show that three of the four new axioms define a frame property. That is, a frame has a certain property if and only if it validates the corresponding axiom.

Chapter 5 lays a foundation for an axiomatization of the probabilistic logic for quantum programs (PLQP) discussed above. The proof system introduced is shown to be sound. We also show a long list of basic and less basic properties of quantum theory concerning orthocomplement, quantum join and orthogonal bases. We use the deductive system and the list of basic properties to prove the properties of a Quantum Leader Election protocol and the BB84 quantum key distribution protocol. These two protocols are just examples of what our system can prove, and we are sure there are many others. But our logic also lays a foundation for the further development in axiomatizing logics for quantum systems, particularly those that involve probability.

Decidability for a class of Hilbert space based quantum logics. In the last part of this thesis we show that a class of Hilbert space based quantum logics, which includes the Probabilistic Logic for Quantum Programs, is *decidable*. To prove that a logical system is decidable essentially means that there exists an effective procedure to answer the question whether a formula is valid (or satisfiable) or not.

We give a general method for showing the decidability for a whole variety of quantum logics, including in particular the logic considered in Chapter 6. The idea behind our method comes from the work of Dunn et. al. who translated standard quantum logic over finite-dimensional spaces into (the equational fragment of) the first-order theory of real numbers, which is known to be decidable due to Tarski's famous theorem. We extend this method to cover a wider range of quantum logics, by showing an inductive way to check if a language can be effectively translated. Basically, if each atomic sentence can be effectively translated to a defining first-order formula and each n-ary operator preserves this translatability, then the language is decidable. The method is applied to the language PLQP, which is therefore shown to be decidable.

Titles in the ILLC Dissertation Series:

ILLC DS-2009-01: **Jakub Szymanik**
Quantifiers in TIME and SPACE. Computational Complexity of Generalized Quantifiers in Natural Language

ILLC DS-2009-02: **Hartmut Fitz**
Neural Syntax

ILLC DS-2009-03: **Brian Thomas Semmes**
A Game for the Borel Functions

ILLC DS-2009-04: **Sara L. Uckelman**
Modalities in Medieval Logic

ILLC DS-2009-05: **Andreas Witzel**
Knowledge and Games: Theory and Implementation

ILLC DS-2009-06: **Chantal Bax**
Subjectivity after Wittgenstein. Wittgenstein's embodied and embedded subject and the debate about the death of man.

ILLC DS-2009-07: **Kata Balogh**
Theme with Variations. A Context-based Analysis of Focus

ILLC DS-2009-08: **Tomohiro Hoshi**
Epistemic Dynamics and Protocol Information

ILLC DS-2009-09: **Olivia Ladinig**
Temporal expectations and their violations

ILLC DS-2009-10: **Tikitu de Jager**
"Now that you mention it, I wonder...": Awareness, Attention, Assumption

ILLC DS-2009-11: **Michael Franke**
Signal to Act: Game Theory in Pragmatics

ILLC DS-2009-12: **Joel Uckelman**
More Than the Sum of Its Parts: Compact Preference Representation Over Combinatorial Domains

ILLC DS-2009-13: **Stefan Bold**
Cardinals as Ultrapowers. A Canonical Measure Analysis under the Axiom of Determinacy.

ILLC DS-2010-01: **Reut Tsarfaty**
Relational-Realizational Parsing

ILLC DS-2010-02: **Jonathan Zvesper**
Playing with Information

ILLC DS-2010-03: **Cédric Dégremont**
The Temporal Mind. Observations on the logic of belief change in interactive systems

ILLC DS-2010-04: **Daisuke Ikegami**
Games in Set Theory and Logic

ILLC DS-2010-05: **Jarmo Kontinen**
Coherence and Complexity in Fragments of Dependence Logic

ILLC DS-2010-06: **Yanjing Wang**
Epistemic Modelling and Protocol Dynamics

ILLC DS-2010-07: **Marc Staudacher**
Use theories of meaning between conventions and social norms

ILLC DS-2010-08: **Amélie Gheerbrant**
Fixed-Point Logics on Trees

ILLC DS-2010-09: **Gaëlle Fontaine**
Modal Fixpoint Logic: Some Model Theoretic Questions

ILLC DS-2010-10: **Jacob Vosmaer**
Logic, Algebra and Topology. Investigations into canonical extensions, duality theory and point-free topology.

ILLC DS-2010-11: **Nina Gierasimczuk**
Knowing One's Limits. Logical Analysis of Inductive Inference

ILLC DS-2010-12: **Martin Mose Bentzen**
Stit, Iit, and Deontic Logic for Action Types

ILLC DS-2011-01: **Wouter M. Koolen**
Combining Strategies Efficiently: High-Quality Decisions from Conflicting Advice

ILLC DS-2011-02: **Fernando Raymundo Velazquez-Quesada**
Small steps in dynamics of information

ILLC DS-2011-03: **Marijn Koolen**
The Meaning of Structure: the Value of Link Evidence for Information Retrieval

ILLC DS-2011-04: **Junte Zhang**
System Evaluation of Archival Description and Access

ILLC DS-2011-05: **Lauri Keskinen**
Characterizing All Models in Infinite Cardinalities

ILLC DS-2011-06: **Rianne Kaptein**
Effective Focused Retrieval by Exploiting Query Context and Document Structure

ILLC DS-2011-07: **Jop Briët**
Grothendieck Inequalities, Nonlocal Games and Optimization

ILLC DS-2011-08: **Stefan Minica**
Dynamic Logic of Questions

ILLC DS-2011-09: **Raul Andres Leal**
Modalities Through the Looking Glass: A study on coalgebraic modal logic and their applications

ILLC DS-2011-10: **Lena Kurzen**
Complexity in Interaction

ILLC DS-2011-11: **Gideon Borensztajn**
The neural basis of structure in language

ILLC DS-2012-01: **Federico Sangati**
Decomposing and Regenerating Syntactic Trees

ILLC DS-2012-02: **Markos Mylonakis**
Learning the Latent Structure of Translation

ILLC DS-2012-03: **Edgar José Andrade Lotero**
Models of Language: Towards a practice-based account of information in natural language

ILLC DS-2012-04: **Yurii Khomskii**
Regularity Properties and Definability in the Real Number Continuum: idealized forcing, polarized partitions, Hausdorff gaps and mad families in the projective hierarchy.

ILLC DS-2012-05: **David García Soriano**
Query-Efficient Computation in Property Testing and Learning Theory

ILLC DS-2012-06: **Dimitris Gakis**
Contextual Metaphilosophy - The Case of Wittgenstein

ILLC DS-2012-07: **Pietro Galliani**
The Dynamics of Imperfect Information

ILLC DS-2012-08: **Umberto Grandi**
Binary Aggregation with Integrity Constraints

ILLC DS-2012-09: **Wesley Halcrow Holliday**
Knowing What Follows: Epistemic Closure and Epistemic Logic

ILLC DS-2012-10: **Jeremy Meyers**
Locations, Bodies, and Sets: A model theoretic investigation into nominalistic mereologies

ILLC DS-2012-11: **Floor Sietsma**
Logics of Communication and Knowledge

ILLC DS-2012-12: **Joris Dormans**
Engineering emergence: applied theory for game design

ILLC DS-2013-01: **Simon Pauw**
Size Matters: Grounding Quantifiers in Spatial Perception

ILLC DS-2013-02: **Virginie Fiutek**
Playing with Knowledge and Belief

ILLC DS-2013-03: **Giannicola Scarpa**
Quantum entanglement in non-local games, graph parameters and zero-error information theory

ILLC DS-2014-01: **Machiel Keestra**
Sculpting the Space of Actions. Explaining Human Action by Integrating Intentions and Mechanisms

ILLC DS-2014-02: **Thomas Icard**
The Algorithmic Mind: A Study of Inference in Action

ILLC DS-2014-03: **Harald A. Bastiaanse**
Very, Many, Small, Penguins

ILLC DS-2014-04: **Ben Rodenhäuser**
A Matter of Trust: Dynamic Attitudes in Epistemic Logic

ILLC DS-2015-01: **María Inés Crespo**
Affecting Meaning. Subjectivity and evaluativity in gradable adjectives.

ILLC DS-2015-02: **Mathias Winther Madsen**
The Kid, the Clerk, and the Gambler - Critical Studies in Statistics and Cognitive Science

ILLC DS-2015-03: **Shengyang Zhong**
Orthogonality and Quantum Geometry: Towards a Relational Reconstruction of Quantum Theory

ILLC DS-2015-04: **Sumit Sourabh**
Correspondence and Canonicity in Non-Classical Logic

ILLC DS-2015-05: **Facundo Carreiro**
Fragments of Fixpoint Logics: Automata and Expressiveness

ILLC DS-2016-01: **Ivano A. Ciardelli**
Questions in Logic

ILLC DS-2016-02: **Zoé Christoff**
Dynamic Logics of Networks: Information Flow and the Spread of Opinion

ILLC DS-2016-03: **Fleur Leonie Bouwer**
What do we need to hear a beat? The influence of attention, musical abilities, and accents on the perception of metrical rhythm

ILLC DS-2016-04: **Johannes Marti**
Interpreting Linguistic Behavior with Possible World Models

ILLC DS-2016-05: **Phong Lê**
Learning Vector Representations for Sentences - The Recursive Deep Learning Approach

ILLC DS-2016-06: **Gideon Maillette de Buy Wenniger**
Aligning the Foundations of Hierarchical Statistical Machine Translation

ILLC DS-2016-07: **Andreas van Cranenburgh**
Rich Statistical Parsing and Literary Language

ILLC DS-2016-08: **Florian Speelman**
Position-based Quantum Cryptography and Catalytic Computation

ILLC DS-2016-09: **Teresa Piovesan**
Quantum entanglement: insights via graph parameters and conic optimization

ILLC DS-2016-10: **Paula Henk**
Nonstandard Provability for Peano Arithmetic. A Modal Perspective

ILLC DS-2017-01: **Paolo Galeazzi**
Play Without Regret

ILLC DS-2017-02: **Riccardo Pinosio**
The Logic of Kant's Temporal Continuum

ILLC DS-2017-03: **Matthijs Westera**
Exhaustivity and intonation: a unified theory

ILLC DS-2017-04: **Giovanni Cinà**
Categories for the working modal logician

ILLC DS-2017-05: **Shane Noah Steinert-Threlkeld**
Communication and Computation: New Questions About Compositionality

ILLC DS-2017-06: **Peter Hawke**
The Problem of Epistemic Relevance

ILLC DS-2017-07: **Aybüke Özgün**
Evidence in Epistemic Logic: A Topological Perspective

ILLC DS-2017-08: **Raquel Garrido Alhama**
Computational Modelling of Artificial Language Learning: Retention, Recognition & Recurrence

ILLC DS-2017-09: **Miloš Stanojević**
Permutation Forests for Modeling Word Order in Machine Translation

ILLC DS-2018-01: **Berit Janssen**
Retained or Lost in Transmission? Analyzing and Predicting Stability in Dutch Folk Songs

ILLC DS-2018-02: **Hugo Huurdeman**
Supporting the Complex Dynamics of the Information Seeking Process

ILLC DS-2018-03: **Corina Koolen**
Reading beyond the female: The relationship between perception of author gender and literary quality

ILLC DS-2018-04: **Jelle Bruineberg**
Anticipating Affordances: Intentionality in self-organizing brain-body-environment systems

ILLC DS-2018-05: **Joachim Daiber**
Typologically Robust Statistical Machine Translation: Understanding and Exploiting Differences and Similarities Between Languages in Machine Translation

ILLC DS-2018-06: **Thomas Brochhagen**
Signaling under Uncertainty

ILLC DS-2018-07: **Julian Schlöder**
Assertion and Rejection

ILLC DS-2018-08: **Srinivasan Arunachalam**
Quantum Algorithms and Learning Theory

ILLC DS-2018-09: **Hugo de Holanda Cunha Nobrega**
Games for functions: Baire classes, Weihrauch degrees, transfinite computations, and ranks

ILLC DS-2018-10: **Chenwei Shi**
Reason to Believe

ILLC DS-2018-11: **Malvin Gattinger**
New Directions in Model Checking Dynamic Epistemic Logic

ILLC DS-2018-12: **Julia Ilin**
Filtration Revisited: Lattices of Stable Non-Classical Logics

ILLC DS-2018-13: **Jeroen Zuiddam**
Algebraic complexity, asymptotic spectra and entanglement polytopes