TÉCNICO LISBOA

Quantum Dynamic Logic

João Miguel Neves Coelho

Thesis to obtain the Master of Science Degree in

Matemática e Aplicações

Supervisor: Prof. Maria Cristina De Sales Viana Serôdio Sernadas

Examination Committee

Chairman: Prof. Paulo Alexandre Carreira Mateus
Supervisor: Prof. Maria Cristina De Sales Viana Serôdio Sernadas
Members of the Commitee: Prof. Jaime Arsénio de Brito Ramos
Prof. Maria Cristina De Sales Viana Serôdio Sernadas

October 2021

Acknowledgments

I would like to express my special tanks to my family and friends for the support and encouragement they gave me, to my supervisor who always available to help me, to my friend Marisa for the study sessions that help me to get motivation to write, and to my dogs for keeping me sane during the pandemic.

Resumo

A primeira menção a uma lógica baseada em Mecânica Quântica foi feita no artigo de Birkhoff e Neumann em 1936 (ver [3]). Aí, os conectivos da lógica quântica ($\sim$, $\wedge$, $\sqcup$) refletem as operações do reticulado de todos os subespaços fechados de um espaço de Hilbert. Como consequência, essa lógica não é uma extensão da lógica clássica. Nomeadamente, algumas propriedades da lógica clássica como a distributividade de $\wedge$ e $\sqcup$ já não são válidas. Atualmente existem muitas variantes da lógica quântica, algumas delas seguindo o paradigma de Birkhoff e von Neumann e outras onde as características quânticas são adicionadas à lógica clássica (para mais detalhes ver [4],[5],[6]). Nesta tese, iremos nos focar na lógica dinâmica quântica (ver [1],[2]) para programas quânticos, que é da segunda variante.
Lógica dinâmica quântica tem o mesmo papel para programas quânticos que a lógica dinâmica tem para programas clássicos. O papel desta última foi muito importante para a criação de técnicas de verificação para programação. Espera-se que a lógica quântica dinâmica faça o mesmo para programas quânticos, isto é, lidando com medições quânticas ,evoluções unitárias e entrelaçamento em sistemas quânticos compostos.

Palavras Chave

Lógica Quântica, Lógica Dinâmica, Mecânica Quântica, Computação Quântica

Abstract

The first logical account of quantum mechanics was presented by Birkhoff and Neumann's 1936 paper (see [3]). Therein, the connectives ($\sim$, $\wedge$, $\sqcup$) of quantum logic reflect the operations in the lattice of all closed subspaces of a Hilbert space. As a consequence this logic is not an extension of classical logic. Namely, some properties of classical logic like distributivity of $\wedge$ and $\sqcup$ are no longer valid. Nowadays there are many variants of quantum logic some of them following the paradigm of Birkhoff and von Neumann and others where quantum features are added to classical logic (for more details see [4],[5],[6]). In this thesis, we concentrate on quantum dynamic logic (see [1],[2]) for quantum programs which is from the latter variant.

Quantum dynamic logic has the same role for quantum programs as dynamic logic for classic programs. The role of the latter was very important for defining verification techniques for programming. It is expected that dynamic quantum logic would do the same to quantum programs, namely dealing with quantum measurements, unitary evolutions and entanglements in compound quantum systems.

Keywords

Quantum Logic, Dynamic Logic, Quantum Mechanics, Quantum Computation

List of Figures

Glossary

PQL Propositional Quantum Logic

PDL Propositional Dynamic Logic

QDF Quantum Dynamic Frame

LQP Logic of Quantum Programs

QDA Quantum Dynamic Algebra

Contents

Chapter 1

Introduction

1.1 Motivation

There have been many news related with quantum computers, with titles such as “Game-Changing”, “Quantum Computing Race”, and “Quantum Supremacy”.
Quantum supremacy is just a scientific goal of having a quantum computer solve a problem that no classical computer is capable of solving in a feasible amount of time. This goal, however, does not specify the type of problem, it could be one that has no utility at all (solving a useful problem is still a long term goal).
Despite quantum supremacy not having intimidate application, many big companies (such as IBM, Google, Intel, Microsoft, and others) have spent millions of dollars into research on this area, as building a quantum computer is expensive and having one running are has great costs.
Since having a quantum computer working is expensive, it is vital that when a quantum program is run we have a guarantee that it works as intended. This is where Quantum Dynamic Logic fits in - it provides a way to show that a quantum algorithm is *sound* (*i.e.*, after running, it yields a result that is correct), just like Propositional Dynamic Logic does for classical algorithms.

1.2 Objective

Given the utility of Quantum Dynamic Logic, the goal of this thesis was to create a work that would be self-contained and a stepping-stone that would make Quantum Dynamic Logic easier to learn.

1.3 Challenges

When learning about Quantum Dynamic Logic there was four main challenges faced that this thesis tries to overcome.
Quantum Mechanics by its very nature is a hard[1] subject to learn therefore any area related to it will share this inherent difficulty. Besides Quantum Mechanics, Quantum Dynamic Logic requires or greatly benefits from knowledge about other areas (Quantum Logic, Propositional Dynamic Logic, Quantum

[1] There was a famous conference, the fifth Solvay conference where the most notorious physicists of the time gathered to discuss Quantum Mechanics, and seventeen were or ended being Nobel Prize winners.

Computation).
Thirdly, there was very little information regarding Quantum Dynamic Logic, searches yielded mostly the two main papers we already read for this thesis ([1],[2]). Lastly, said papers were time consuming to follow as they provide very few proofs of theirs statements.

1.4 What was Done

In order to reach the goal and overcome the challenges faced, introductory chapters were written about the required topics, as they were needed, proofs were done for the results that were not proven in the papers ([1],[2]), and, when needed, supplementary results and their proofs were added in order to ease the following of this work.

1.5 Topic Overview

To better help understand Quantum Dynamic Logic we can look at each of those three words individual. Logic is concerned with propositions and the laws to use such propositions that create a valid argument. Dynamic is related to change, so when we allow a system to change, as in a computer program, we need Dynamic Logic to reason about its properties. Finally, joining Quantum to Dynamic Logic, we have the same idea, we can reason about computer programs, but in this case we have quantum computers.

1.6 Chapter Overview

This thesis aims to be a self-contained work, therefore we compiled all relevant topics and results in order to provide a easy following for the reader.
Chapter 2 introduces concepts that are required thorough the rest of the text. *Hilbert Spaces* on Section 2.1 and *Lattices* on Section 2.2 are the concepts that form the base of *Propositional Quantum Logic*, summarized on Section 2.3, and whose logics present on other sections are expanding upon. Finally, on Section 2.4 we introduce concepts about relations, as it is a core concept for dynamic logic.
The path of expanding quantum logic followed by A. Baltag and S. Smets deals with the inclusion of time evolutions, that are seen as *quantum programs*, that is, they take a dynamic approach, so Chapter 3 will introduce the concepts of *Propositional Dynamic Logic* to help the reader familiarize themselves with the concepts.
In Chapter 4 we will see the first structure capable of handling quantum programs. Section 4.1 gives the general definition of the structure, a *dynamic frame*, Section 4.2 gives the properties the structure needs to satisfy in order to be a *Quantum Dynamic Frame* and from those properties we prove some results. Finally Section 4.3 we combine the programs using composition and non-deterministic choice into a more general family of programs, *quantum actions* or *quantum programs*, and prove results for these general programs.
In Chapter 5 the *Logic of Quantum Programs* is finally introduced - the syntax, semantics, and axioms and rules.

Chapter 6 introduces *Quantum Dynamic Algebras* and proves that they are equivalent to a Quantum Dynamic Frame and that both of them can always be induced by some Hilbert space.
In Chapter 7 we do a detour into quantum computation to both explain concepts that will be used for the enrichment of LQP in the final chapter, as well a explaining the teleportation protocol, which will be used as an example in the last chapter.
Finally the last Chapter builds upon LQP with concepts from the previous Chapter to create a logic of compound-system quantum frames, and on the last section there is a sketch, of the proof done in [2], of the correctness of the teleportation protocol, done using this logic.

Chapter 2

Preliminaries

The goal of this Chapter is to introduce concepts that are the stepping stones for a Quantum Dynamic Logic. *Hilbert spaces* (Section 2.1) and *lattices* (Section 2.2) are key concepts of Quantum Mechanics and thus necessary to understand *Propositional Quantum Logic* (Section 2.3), and *relations* (Section 2.4) are necessary for any dynamic logic.

2.1 Hilbert Spaces

Hilbert spaces play a key role in Quantum Logic as we shall see, so this Section will introduce its definition.
The first characteristic of a Hilbert space is that it must be a vector space over $\mathbb{C}$, *i.e.*, it must be a complex vector space. Secondly, a Hilbert space is a *inner product space*, that is, it has a *(complex) inner product*.

Def. 2.1.1 (Complex Inner Product Space):
Let V be a complex vector space. A COMPLEX INNER PRODUCT is a map

$$\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C} \tag{2.1}$$

satisfying the following properties for all $x, y \in V$ and $\alpha \in \mathbb{C}$:

1. Linearity in the first argument:
   - $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$
   - $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$
2. Conjugate Symmetry: $\langle y, x \rangle = \overline{\langle x, y \rangle}$
3. Positive Definiteness: $\langle x, x \rangle \geqslant 0$ with equality only if $x = 0$

Then, we say that the pair $(V, \langle \cdot, \cdot \rangle)$ is a INNER PRODUCT SPACE.

An example of a complex inner product space is $\mathbb{C}^n$ with the canonical inner product.

Example 2.1.2 ($\mathbb{C}^n$):

Considering the complex vector space $\mathbb{C}^n$, let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n \in \mathbb{C}^n$.

The canonical inner product is then given by

$$\langle x, y \rangle := x_1\overline{y_1} + \cdots + x_n\overline{y_n} \tag{2.2}$$

Another concept that we shall use is *metric* and, consequently, *metric space*.

Def. 2.1.3 (Metric Space):

Let X be a set. A METRIC is a map

$$d \colon X \times X \to \mathbb{R} \tag{2.3}$$

that satisfies for all $x, y, z \in X$:

1. Symmetry: $d(x, y) = d(y, x)$
2. Triangle inequality: $d(x, y) \leqslant d(x, z) + d(z, y)$
3. Positive: $d(x, y) \geqslant 0$ with equality iff $x = y$

Moreover, the pair (X, d) is said to be a METRIC SPACE.

It turns out that from any inner product it is possible to induce a metric, that is, every inner product space can be a metric space. This induced metric will be used in Hilbert spaces.

Def. 2.1.4 (Metric of a Inner Product):

Let V be a complex inner product space, with inner product $\langle \cdot, \cdot \rangle$.

First we define the norm of a vector

$$\|x\| := \sqrt{\langle x, x \rangle} \tag{2.4}$$

Let

$$d(x, y) := \|x - y\| \tag{2.5}$$

It is easy to see that d is a metric.

Going back to the example of the inner product space of $\mathbb{C}^n$, lets us see the definition in action.

Example 2.1.5 ($\mathbb{C}^n$):

Lets consider the Example 2.1.2, and $x, y \in \mathbb{C}^n$ with the coordinates given as before.

Following the first step of the definition above, we have that

$$\|x\| = \sqrt{|x_1|^2 + \cdots + |x_n|^2} \tag{2.6}$$

Therefore, the metric, d, is given by

$$d(x, y) = \sqrt{|x_1 - y_1|^2 + \cdots + |x_n - y_n|^2} \tag{2.7}$$

The next concept we have to present is *complete metric space*. In order to do that we need the notion of a *Cauchy sequence*.

Def. 2.1.6 (Cauchy Sequence):

Let (X, d) be a metric space. The sequence (x_k) in X is said to be a CAUCHY SEQUENCE if for every $\varepsilon > 0$ there exists a positive integer N such that for every integers $n, m > N$ (x_k) satisfies

$$d(x_n, x_m) < \varepsilon \tag{2.8}$$

Intuitively, the terms of a Cauchy are getting closer and closer together. This seems to imply that the sequence has a limit. However that needs not be the case, and this is what motivates the definition of a complete metric space.

Def. 2.1.7 (Complete Metric Space):

A metric space (X, d) is said to be COMPLETE if every Cauchy sequence converges in X.

Now we have all we need to define a *Hilbert space*.

Def. 2.1.8 (Hilbert Space):

A complex inner product space $(V, \langle \cdot, \cdot \rangle)$ is said to be a HILBERT SPACE if the metric space induced by the inner product is also a complete metric space.

It is common to use $\mathcal{H}$ to denote a general Hilbert space over $\mathbb{C}$, so this convention will be used thorough the rest of the text.

Example 2.1.9 ($\mathbb{C}^2$):

The vector space $\mathbb{C}^2$ over the complex field with the canonical inner product $\langle \cdot, \cdot \rangle$ from Example 2.1.2 is a Hilbert space.

In Quantum Mechanics it is usual to use the notation

$$|0\rangle := (1, 0) \qquad\qquad |1\rangle := (0, 1) \tag{2.9}$$

to represent the vectors of the canonical basis of $\mathbb{C}^2$.

For this thesis, really, only requires understanding of the $\mathbb{C}^2$ Hilbert space, but for more examples we recommend the reader to see [8].

The second concept needed to understand Quantum Logic is the notion of a *closed linear subspaces*.In Quantum Mechanics (and therefore in Quantum Logic), they represent the possible states of the system. Closed sets are common to all topological spaces, but herein we only define them in the context of Hilbert space.

Def. 2.1.10 (Open and Closed Sets):

Let $\mathcal{H}$ be a Hilbert space. A set $A \subset \mathcal{H}$ is said to be OPEN if it can be written as an (arbitrary) union of open balls of the form $B_r(x) := \{y \in \mathcal{H} \colon d(x, y) < r\}$. A set $F \subset \mathcal{H}$ is CLOSED if its complement $\mathcal{H} \backslash F$ is open.[1]

To understand the next result, we need first the definition of *dimension*.

[1] The notation $A \subset B$ means that A is strictly a subset of B or $A = B$, when meaning only strictly subset it will be denoted by $A \subsetneq B$.

Def. 2.1.11 (Basis and Dimension):

Let $\mathcal{H}$ be a Hilbert space, and $B \subset \mathcal{H}$ a subset. We say that B is a BASIS of $\mathcal{H}$ (over the complex numbers) if:

• For every finite subset $\{v_1, \ldots, v_n\} \subset B$, if $\exists_{\alpha_1,\ldots,\alpha_n \in \mathbb{C}}\ \alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ then $\alpha_1 = \cdots = \alpha_n = 0$

• For every $v \in \mathcal{H}\ \exists_{n \in \mathbb{N}}\ \exists_{\alpha_1,\ldots,\alpha_n \in \mathbb{C}}\ \exists_{v_1,\ldots,v_n \in B}$ such that $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$

The cardinality of B is called the DIMENSION of $\mathcal{H}$.

There is a very useful result that relates finite-dimensional subspaces and closed sets:

Prop. 2.1.12:

Every subspace with finite dimension of a Hilbert space is a closed set.

Using this Proposition, we can identify all closed linear subspaces of a finite-dimensional Hilbert space. Looking at the simple case of the 2-dimensional $\mathbb{C}^2$ we have:

Example 2.1.13 (Closed Linear Subspaces of $\mathbb{C}^2$):

The closed linear subspaces of the Hilbert space $\mathbb{C}^2$ from Example 2.1.9 are: the 0-dimensional subspace $\{0\}$, the 1-dimensional $\mathrm{span}(z)$ (for $z \neq 0$), and $\mathbb{C}^2$ itself.

Related with closed linear subspaces are the concepts of *closure* of a set and the *orthogonal complement*.

Def. 2.1.14 (Closure of a Set):

Given a set $S \subset \mathcal{H}$ the CLOSURE of S, denoted by $\overline{S}$, is the smallest closed set containing S. That is

$$\overline{S} := \bigcap_{S \subset F, F \text{ closed}} F. \tag{2.10}$$

If S is a singleton $\{s\}$ we write $\overline{s}$ instead of $\overline{\{s\}}$.

For a simple example, lets use $\mathbb{C}^2$.

Example 2.1.15:

From last Example, given $z \in \mathbb{C}^2$, we have that $\overline{z} = \mathrm{span}(z)$.

The orthogonal complement is pivotal for quantum logic, as it constitutes the foundation for *quantum negation*.

Def. 2.1.16 (Orthogonal Complement):

Given a subset $S \subset \mathcal{H}$, the ORTHOGONAL COMPLEMENT of S is

$$S^{\perp} := \{x \in \mathcal{H} \colon \forall_{s \in S}\ \langle x, s \rangle = 0\} \tag{2.11}$$

Example 2.1.17:

Considering $|0\rangle \in \mathbb{C}^2$ we have that $|0\rangle^{\perp} = \overline{|0\rangle}^{\perp} = \overline{|1\rangle}$.

Before continuing with a last important concept, we will enumerate some results that will be needed further on.

Prop. 2.1.18:

The orthogonal complement of $S \subset \mathcal{H}$, $S^{\perp}$, is a closed subspace.

Prop. 2.1.19:

Let $S \subset \mathcal{H}$ be a subset. Then $S \subset (S^{\perp})^{\perp}$, with equality if and only if S is a closed linear subspace.

Corollary 2.1.20:

The closure of a subset $S \subset \mathcal{H}$ is equal to the double orthogonal complement, that is, $\overline{S} = (S^{\perp})^{\perp}$.

Prop. 2.1.21:

Let $S, T \subset \mathcal{H}$ be subsets. Then $\overline{S \cup T} = (S^{\perp} \cap T^{\perp})^{\perp}$

***Proof*:**

From corollary 2.1.20 we have that $\overline{S \cup T} = (S \cup T)^{\perp\perp}$

Then, it suffices to show that $(S \cup T)^{\perp} = S^{\perp} \cap T^{\perp}$

$x \in (S \cup T)^{\perp} \Leftrightarrow \forall_{y \in (S \cup T)}\, x \perp y \Leftrightarrow \forall_{s \in S}\, x \perp s \text{ and } \forall_{t \in T}\, x \perp t \Leftrightarrow x \in S^{\perp} \text{ and } x \in T^{\perp} \Leftrightarrow x \in (S^{\perp} \cap T^{\perp})$

Thus $(S \cup T)^{\perp} = S^{\perp} \cap T^{\perp}$ ■

Prop. 2.1.22:

Let $S \subset \mathcal{H}$ be a closed linear subspace. Then $\mathcal{H} = S \oplus S^{\perp}$.

The final concept needed is *orthogonal projections*. They have a important role in quantum mechanics, representing measurements.

Def. 2.1.23 (Projection and Orthogonal Projection):

A linear operator on a linear space V, $P \colon V \to V$, is said to be a PROJECTION if $P \circ P = P$.

On a Hilbert space $\mathcal{H}$, a projection operator $P : \mathcal{H} \to \mathcal{H}$ is said to be a ORTHOGONAL PROJECTION if $\forall_{x,y \in \mathcal{H}}\ \langle Px, y \rangle = \langle x, Py \rangle$, that is, P is *self-adjoint*.

Example 2.1.24:

Given $z \in \mathbb{C}^2$, the orthogonal projection over $\overline{z}$, $proj_z \colon \mathbb{C}^2 \to \mathbb{C}^2$, is given by $proj_z(w) := \dfrac{\langle w, z \rangle}{\|z\|} z$.

The next Proposition relates the concepts of measurements and states together.

Prop. 2.1.25:

There is a bijection between closed linear subspaces and orthogonal projections.

2.2 Lattices

The postulates of quantum mechanics say that the state space of a system is composed of the closed linear subspaces of a Hilbert space and, furthermore, it forms a *orthomodular lattice*.

This section presents the definition of orthomodular lattices in steps, starting from the definition of lattice.

Def. 2.2.1 (Lattice):

A LATTICE is a tuple $(L, \leq, \sqcap, \sqcup)$ where $(L, \leq)$ is a partially ordered set such that for every $a, b, c \in L$.

• There exists a SUPREMUM or JOIN $a \sqcup b \in L$, that is, $a \leq a \sqcup b$, $b \leq a \sqcup b$, and if $a \leq c$ and $b \leq c$ then $a \sqcup b \leq c$

• There exists a INFIMUM or MEET $a \sqcap b \in L$, that is, $a \sqcap b \leq a$, $a \sqcap b \leq b$, and if $c \leq a$ and $c \leq b$ then $c \leq a \sqcap b$

Let us look at two examples, the first using natural numbers, and it is assumed that 0 is not a natural number.

Example 2.2.2:

Let us consider the ordered set $(\mathbb{N}, |\,)$, where $n|m$ means that n divides m, *i.e.*, $m = qn$ for some $q \in \mathbb{N}$. We can define a lattice by choosing the meet as the greatest common divider and the join as the least common multiple, that is, for $n, m \in \mathbb{N}$:

- $n \sqcap m := \gcd(n, m)$
- $n \sqcup m := \mathrm{lcm}(n, m)$

The second Example uses as basis any set X. This Example gives insight on the use of the notation $\sqcap$ and $\sqcup$ for the meet and join.

Example 2.2.3:

Let X be a set, and consider $(\mathcal{P}(X), \subset)$ as the power set of X ordered by inclusion. We can form a lattice by defining, for any $A, B \in \mathcal{P}(X)$, the meet and join as:

- $A \sqcap B := A \cap B$
- $A \sqcup B := A \cup B$

From the examples we can see a difference, while both have a minimum element (in Example 2.2.2 is 1 and in Example 2.2.3 is $\varnothing$) only the second has a maximum element (the set X itself). This motivates the definition of *bounded lattice*.

Def. 2.2.4 (Bounded Lattice):

A BOUNDED LATTICE is a tuple $(L, \leq, \sqcap, \sqcup, 0, 1)$ where $(L, \leq, \sqcap, \sqcup)$ is a lattice and such that $0 \in L$ is the MINIMUM or BOTTOM, and $1 \in L$ is the MAXIMUM or TOP. That is, for all $a \in L$, $0 \leq a$ and $a \leq 1$.

As mentioned above, the lattice from Example 2.2.3 has both a maximum (being the element X) and a minimum (the element $\varnothing$), thus it is a bounded lattice.

The next concept to be defined is *complemented lattices*, and they expand upon bounded lattices.

Def. 2.2.5 (Complemented Lattice):

A COMPLEMENTED LATTICE is a bounded lattice such that for for every $a \in L$ exists $b \in L$ such that $a \sqcap b = 0$ and $a \sqcup b = 1$. The element b is said to be a COMPLEMENT of a (not necessarily unique).

The example that we have been using is still relevant as it is a *complemented lattice*:

Example 2.2.6:

Given the lattice from Example 2.2.3 and a set $A \subset X$ we have that $A \cap (X \setminus A) = \varnothing$ and $A \cup (X \setminus A) = X$.

Note that in the Example above, not only every element has a complement, its complement is also unique. This motivates the next definition.

Def. 2.2.7 (Orthocomplemented Lattice):

A ORTHOCOMPLEMENTED LATTICE is a tuple $(L, \leq, \sqcap, \sqcup, 0, 1, \cdot^{\perp})$, where $(L, \leq, \sqcap, \sqcup, 0, 1)$ is a complemented lattice and $\cdot^{\perp} : L \to L$ is a map satisfying for all $a, b \in L$

- $a \sqcap a^{\perp} = 0$ and $a \sqcup a^{\perp} = 1$ (complement law)
- $(a^{\perp})^{\perp} = a$ (involution law)
- if $a \leq b$ then $b^{\perp} \leq a^{\perp}$ (order-reversing)

The Example above is clearly a orthocomplemented lattice, with the $\cdot^{\perp}$ map being given by the set complement. However, by the notation and the name, one should suspect that the orthogonal complement of a inner product space would fit into this definition.

Example 2.2.8 (Lattice of Hilbert Space):

Lets consider a Hilbert space $\mathcal{H}$. The orthocomplemented lattice based on $\mathcal{H}$ is

$$(L, \subset, \cap, \sqcup, \{0\}, \mathcal{H}, \cdot^{\perp}) \tag{2.12}$$

Where:

- L be the family of closed linear subspaces of $\mathcal{H}$;
- $\subset$ is set inclusion;
- $\cap$ is set intersection;
- $\{0\}$ is the 0-dimensional linear subspace of $\mathcal{H}$;
- $\cdot^{\perp}$ is the orthogonal complement in $\mathcal{H}$;
- $\sqcup$ is the closure of the union, that is, for $F, F' \in \mathcal{L}$ $F \sqcup F' := \overline{F \cup F'}$.

One may note that this Example is of a orthocomplemented lattice, but in the beginning of this section we mentioned that the lattices needed were *orthomodular lattices*. There is no problem since the lattice of the Example is also a orthomodular lattice as it satisfies the requirement defined below.

Moreover, the Example above is the lattice we will use thorough this thesis whenever we refer to a lattice based on a given Hilbert space.

Def. 2.2.9 (Orthomodular Lattice):

A ORTHOMODULAR LATTICE is a orthocomplemented lattice such that for all $a, b, c \in L$ if $a \leq c$ then $a \sqcup (a^{\perp} \sqcap c) = c$.[2]

On the previous section we used largely the example of $\mathbb{C}^2$, so, for the sake of completeness, we present the detailed lattice based on $\mathbb{C}^2$.

Example 2.2.10 ($\mathbb{C}^2$ Lattice):

Considering the Hilbert space of Example 2.1.9, $\mathbb{C}^2$. The corresponding lattice of closed linear subspaces has $L = L_0 \cup L_1 \cup L_2$ where L_i contains the closed i-dimensional subspaces of $\mathbb{C}^2$, and as seen on Example 2.1.13 they are given by $L_0 = \{\{0\}\}$, $L_1 = \{\overline{z}\}_{z \in \mathbb{C}^2 \setminus \{0\}}$, and $L_2 = \{\mathbb{C}^2\}$.

2.3 Propositional Quantum Logic

With the concepts from the last sections it is possible to introduce PROPOSITIONAL QUANTUM LOGIC. As mentioned before, this logic is based on lattices built from a complex Hilbert space, as in Example 2.2.8.

Subsection 2.3.1 introduces the syntax and semantics of PQL and in Subsection 2.3.2 we give examples where this logic differs from positional logic.

[2] It is true in any orthocomplemented lattice that $c = (a \sqcup a^{\perp}) \sqcap c$

2.3.1 Syntax and Semantics

Let $P = \{p, q, \ldots\}$ be a set of propositional variables. The set of *propositional quantum formulas* L_P) is such that

$$\varphi ::= \bot \,|\, p \,|\sim \varphi \,|\, \varphi \wedge \varphi \tag{2.13}$$

The notation above is called *Backus-Naur form* or *Backus normal form*. Its meaning is that a propositional formula is either $\bot$, a propositional variable, a negation of other formula, or the conjunction of two formulas.

We define top and disjunction using the usual abbreviations $\top := \sim \bot$, $\varphi \sqcup \psi := \sim (\sim \varphi \wedge \sim \psi)$.
Note that implication was not mentioned, because implication in Quantum Logic is not the usual one. It is given by $\varphi \xrightarrow{S} \psi := \sim \varphi \sqcup (\varphi \wedge \psi)$, this is also called the "Sasaki hook".

This logic is based on the orthomodular lattice of a Hilbert space, so we should use such structure in the semantics.
That is, a formula should correspond to a closed linear subspace of $\mathcal{H}$, and the logical relations as operations on the lattice.

Def. 2.3.1 (Semantic Structure of PQL):
A SEMANTIC STRUCTURE or MODEL for PQL is a pair $\mathcal{M} = (\mathcal{L}, V)$ where $\mathcal{L}$ is a orthomodular lattice based on a Hilbert space $\mathcal{H}$ and $V : P \to L$ is a *valuation function*, where L is the carrier set of $\mathcal{L}$.
The *interpretation* of a formula, $\| \cdot \|^{\mathcal{M}} : L_P \to L$, satisfies:

1. $\|\bot\|^{\mathcal{M}} = \{0\}$
2. $\|p\|^{\mathcal{M}} = V(p)$
3. $\| \sim \varphi\|^{\mathcal{M}} = (\|\varphi\|^{\mathcal{M}})^{\perp}$
4. $\|\varphi \wedge \psi\|^{\mathcal{M}} = \|\varphi\|^{\mathcal{M}} \cap \|\psi\|^{\mathcal{M}}$

For the sake of not overwhelm the reader with too much symbols, when the context is clear, we will omit the superscript $\mathcal{M}$. Note also that $\|\cdot\|$ is the same notation used for the norm of a vector, but from the context it should be clear which is being used, since the majority of this text uses it with the meaning of interpretation.

We say that a formula φ is true under $(\mathcal{L}, V)$, written $(\mathcal{L}, V) \vDash \varphi$, if $\|\varphi\| = \mathcal{H}$.
We say that a formula φ is *valid*, denoted by $\vDash \varphi$, if it is true under every semantic structure $(\mathcal{L}, V)$.

It is easy to find the interpretation for top and disjunction:
Prop. 2.3.2:
$\|\top\| = \mathcal{H}$
$\|\varphi \sqcup \psi\| = \|\varphi\| \sqcup \|\psi\|$

***Proof*:**

$\|\top\| = \| \sim \bot\| = \{0\}^{\bot} = \mathcal{H}$

$\|\varphi \sqcup \psi\| = \| \sim (\sim \varphi \wedge \sim \psi)\| = (\|\varphi\|^{\bot} \cap \|\psi\|^{\bot})^{\bot} \overset{(*)}{=} \overline{\|\varphi\| \cup \|\psi\|} = \|\varphi\| \sqcup \|\psi\|$

where on equality $(*)$ we are using Proposition 2.1.21. ■

2.3.2 Diferences between Classical and Quantum Logic

Using a orthomodular lattice of closed subspaces of a Hilbert space as the semantical foundation for this logic leads to differences from *classical* propositional logic, mainly, the quantum negation is stronger than classical negation and quantum disjunction is weaker than the classical counterpart.

Among the differences between this logic and classical propositional logic is that the quantum conjunction does not distribute with quantum disjunction, and *vice versa*, as we shall see in the next result.

Prop. 2.3.3:

Quantum logic does not have the distributive property with respect to $\wedge$ *and* $\sqcup$*. That is, given a model* $(\mathcal{L}, V)$ *is not necessarily true that the following holds:*

- $(\mathcal{L}, V) \vDash \varphi \wedge (\phi \sqcup \psi)$ *iff* $(\mathcal{L}, V) \vDash (\varphi \wedge \phi) \sqcup (\varphi \wedge \psi)$
- $(\mathcal{L}, V) \vDash \varphi \sqcup (\phi \wedge \psi)$ *iff* $(\mathcal{L}, V) \vDash (\varphi \sqcup \phi) \wedge (\varphi \sqcup \psi)$

***Proof*:**

Lets consider the 2-dimensional Hilbert space $\mathbb{C}^2$. Considering $\|\cdot\|$ such that $\|\varphi\| = \overline{|0\rangle} = \overline{(1,0)}$, $\|\phi\| = \overline{|1\rangle} = \overline{(0,1)}$, and $\|\psi\| = \overline{|0\rangle + |1\rangle} = \overline{(1,1)}$, we have:

$\|\varphi \wedge (\phi \sqcup \psi)\| = \overline{(1,0)} \cap \left(\overline{(0,1)} \sqcup \overline{(1,1)}\right) = \overline{(1,0)} \cap \mathbb{C}^2 = \overline{(1,0)}$

$\|(\varphi \wedge \phi) \sqcup (\varphi \wedge \psi)\| = \left(\overline{(1,0)} \cap \overline{(0,1)}\right) \sqcup \left(\overline{(1,0)} \cap \overline{(1,1)}\right) = \{0\} \sqcup \{0\} = \{0\}$

$\|\varphi \sqcup (\phi \wedge \psi)\| = \overline{(1,0)} \sqcup \left(\overline{(0,1)} \cap \overline{(1,1)}\right) = \overline{(1,0)} \sqcup \{0\} = \overline{(1,0)}$

$\|(\varphi \sqcup \phi) \wedge (\varphi \sqcup \psi)\| = \left(\overline{(1,0)} \sqcup \overline{(0,1)}\right) \cap \left(\overline{(1,0)} \sqcup \overline{(1,1)}\right) = \mathbb{C}^2 \cap \mathbb{C}^2 = \mathbb{C}^2$ ■

Continuing the comparison with propositional logic, as was mentioned, the quantum implication (Sasaki hook) is not the same as the classical counterpart, in particular. In particular, it has a different abbreviation from the classical case ($\neg\varphi \vee \psi$). Nonetheless, the abbreviation of the Sasaki hook, $\sim \varphi \sqcup (\varphi \wedge \psi)$, captures the inclusion relation of the lattice.

Prop. 2.3.4:

Let $(\mathcal{L}, V)$ *be a semantic structure. Then,*

$$(\mathcal{L}, V) \vDash \sim \varphi \sqcup (\varphi \wedge \psi) \quad \text{iff} \quad \|\varphi\| \subset \|\psi\| \tag{2.14}$$

***Proof*:**

Let U, W be defined as $U := \|\varphi\|$ and $W := \|\psi\|$. Note that U and W are closed linear subspaces.

We have that $\| \sim \varphi \sqcup (\varphi \wedge \psi)\| = U^{\bot} \sqcup (U \cap W)$

$\leftarrow)$

If $U \subset W$ then $U \cap W = U$, therefore $U^{\bot} \sqcup (U \cap W) = U^{\bot} \sqcup U$ and $U^{\bot} \sqcup U = \mathcal{H}$ by complement law of

orthocomplemented lattices.

$\rightarrow$)
If $U^{\perp} \sqcup (U \cap W) = \mathcal{H}$, then, by definition of $\sqcup$ in Hilbert lattices, we have that

$$U^{\perp} \sqcup (U \cap W) = (U^{\perp\perp} \cap (U \cap W)^{\perp})^{\perp} \tag{2.15}$$

Since U is a closed linear subspace, $U^{\perp\perp} = U$, thus $(U^{\perp\perp} \cap (U \cap W)^{\perp})^{\perp} = (U \cap (U \cap W)^{\perp})^{\perp}$.
Substituting on the hypothesis leads to

$$(U \cap (U \cap W)^{\perp})^{\perp} = \mathcal{H} \tag{2.16}$$

No we just need to take the orthogonal complement on both sides to arrive at

$$U \cap (U \cap W)^{\perp} = \{0\} \tag{2.17}$$

This is true if and only if $U \subset ((U \cap W)^{\perp})^{\perp} = U \cap W$, that is, if and only if $U \subset W$ ■

2.4 Relations

In this section we introduce the notion of *relation* and some useful properties in order to prepare the framework for dynamic logic.

Def. 2.4.1 (Relation):
Let X and Y be two sets, then R is said to be a (binary) RELATION from X to Y if $R \subset X \times Y$. If $R \subset X \times X$ we say R is a relation on X.
If $(x, y) \in R$ we say that x stands in the relation R to y, and we can denote it by xRy.

Some times it might be useful to refer to the elements of X that are in the relation, or the elements of Y, those are the *domain* and *range* of the relation.

Def. 2.4.2 (Domain and Range of a Relation):
Let $R \subset X \times Y$ be a relation, then the DOMAIN and RANGE of R, denoted by dom and ran, are:

$$\operatorname{dom} R := \{x \in X : \exists_{y \in Y}\, xRy\} \tag{2.18}$$

$$\operatorname{ran} R := \{y \in Y : \exists_{x \in X}\, xRy\} \tag{2.19}$$

Given one or two relations, it is possible to perform operations with them. Some important operations on relations that can be made are *composition*, *union* and *Kleene star*.

Def. 2.4.3 (Composition of Relations):
Let X, Y, Z be sets and $R \subset X \times Y$, $S \subset Y \times Z$ be two relations. Then the COMPOSITION of R and S is the relation

$$R \cdot S := \{(x, z) \in X \times Z : \exists_{y \in Y}\, xRy \wedge ySz\} \tag{2.20}$$

If R is a relation on X and $n \in \mathbb{N}$ then R^n is the composition of R with itself n times, with

$$R^0 := \{(x, x) \in X \times X : x \in X\} \tag{2.21}$$

Def. 2.4.4 (Union of Relation):

Let X, Y be sets and $R, S \subset X \times Y$ be two relations. Then the UNION of R and S is the relation

$$R \cup S := \{(x, y) \in X \times Y : xRy \vee xSy\} \tag{2.22}$$

In other words, the unions of relations corresponds with the set union of R and S.

Def. 2.4.5 (Kleene Star of a Relation):

Let X be a set and R a relation on X. The KLEEN STAR of R is the relation

$$R^* := \bigcup_{n \geqslant 0} R^n = R^0 \cup R^1 \cup R^2 \cup \cdots \tag{2.23}$$

The final two concepts, that are important to mention, are the ones of *image* of A by R and of *weakest precondition* of R with respect to A.

Def. 2.4.6 (Image of A by R):

Let $R \subset X \times Y$ be a relation and $A \subset X$ be a set. We denote the IMAGE of A by R as

$$R(A) := \{y \in X : \exists_{x \in A}\, xRy\} \tag{2.24}$$

Def. 2.4.7 (Weakest precondition of R with respect to A):

Let $R \subset X \times Y$ be a relation and $A \subset Y$ be a set. The WEAKEST PRECONDITION of R with respect to (postcondition) A is given by

$$[R]A := \{x \in X : \forall_{y \in X}\, (xRy \Rightarrow y \in A)\} \tag{2.25}$$

The next result sums up, very elegantly, how these two concepts are related:

Prop. 2.4.8:

Let R be a relation on X and $A, B \subset X$. Then

$$A \subset [R]B \Leftrightarrow R(A) \subset B$$

***Proof*:**

$A \subset [R]B \Leftrightarrow \forall_{a \in A}\, a \in [R]B \Leftrightarrow \forall_{a \in A} \forall_{y \in X}\, (a\ R\ y \Rightarrow y \in B)$

$\Leftrightarrow \forall_{a \in A} \forall_{y \in X}\, (y \in R(a) \Rightarrow y \in B) \Leftrightarrow \forall_{a \in A} \forall_{y \in R(a)}\, y \in B$

$\Leftrightarrow \forall_{a \in A}\, R(a) \subset B \Leftrightarrow R(A) \subset B$ ■

Now that we have the concept of weakest precondition, one can ask what is the result of the weakest precondition of the operations of composition and union. The last two results answer this question.

Prop. 2.4.9:

Let R, S be two relations on X and $A \subset X$. Then

$$[R \cdot S]A = [R][S]A$$

***Proof*:**

$\subset$)

Let $x \in [R \cdot S]A$, then given $z \in X$

$$x(R \cdot S)z \Rightarrow z \in A \quad (\dagger)$$

We want to show that given any $y \in X$ we have that $x\ R\ y \Rightarrow y \in [S]A$

Let $y \in X$ be such that $x\ R\ y$.
Then $y \in [S]A$ iff $\forall_{z \in X}\ y\ S\ z \Rightarrow z \in A$.

Let $z \in X$ be such that $y\ S\ z$.
Since $x\ R\ y$ we have that $x\ (R \cdot S)\ z$, thus, by $(\dagger)$, we have that $z \in A$.

$\supset)$
Let $x \in [R][S]A$.
We need to show that $\forall_{z \in X}\ x\ (R \cdot S)\ z \Rightarrow z \in A$

Let $z \in X$ such that $x\ (R \cdot S)\ z$.
That is, $\exists_{y \in X}$ such that $x\ R\ y$ and $y\ S\ z$.
Since $x \in [R][S]A$ and $x\ R\ y$ we have that $y \in [S]A$, and then, because $y\ S\ z$ we get that $z \in A$. ■

Prop. 2.4.10:
Let R_{ii} be a family of relations on X and $A \subset X$. Then

$$[\cup_i R_i]\ A = \cap_i [R_i]A$$

***Proof*:**
$\subset)$
Let $x \in [\cup_i R_i]A$, that is, $\forall_{y \in X}\ x\ (\cup_i R_i)\ y \Rightarrow y \in A \quad (\dagger)$
We want to show that $\forall_i \forall_{y \in X}\ x\ R_i\ y \Rightarrow y \in A$.

Let i be an index. Let also $y \in X$ be such that $x\ R_i\ y$.
Since $x\ R_i\ y$ then $x\ (\cup_i R_i)\ y$, therefore, by $(\dagger)$, we have that $y \in A$.

$\supset)$
Let $x \in \cap_i [R_i]A$, that is, $x \in [R_i]A$ for all i.
We need to show that $\forall_{y \in X}\ x\ (\cup_i R_i)\ y \Rightarrow y \in A$

Let $y \in X$ be such that $x\ (\cup_i R_i)\ y$.
Therefore $\exists_i$ such that $x\ R_i\ y$. Since $x \in [R_i]A$ we must have that $y \in A$. ■

Chapter 3

Propositional Dynamic Logic

Many of the ideas needed for Quantum Dynamic Logic come from Propositional Dynamic Logic (PDL) so this chapter aims to familiarize the reader with such concepts. The *syntax* (Section 3.1) and *semantics* (Section 3.2) of PDL will be used as a basis for constructing a quantum version, therefore many axioms and rules from the *Hilbert calculus* (Section 3.3) of PDL will be used too.

3.1 Syntax of PDL

In PDL, as indicated in the name, we have *propositions* $\varphi, \phi, \psi, \ldots$ (Propositional part) and *programs* or *actions* $\alpha, \beta, \gamma, \ldots$ (Dynamic part), therefore, PDL has propositional operators, program operators, and mixed operators:

- **Propositional Operators:** $\bot$ false, $\neg$ negation, $\wedge$ conjunction.
- **Program Operators:** $\cdot$ composition, $\cup$ (non-deterministic) choice, $*$ iteration.
- **Mixed Operators:** $[\,]$ necessity, $?$ test.

Given a set P of *propositional variables* $p, q, \ldots$ and a set Π of atomic programs $a, b, \ldots$, the set of *well-formed propositions* L_P and the set of *well-formed programs* L_Π are defined by mutually induction the following way:

$$\begin{aligned} \varphi &::= p \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\alpha]\varphi \\ \alpha &::= a \mid \alpha \cdot \alpha \mid \alpha \cup \alpha \mid \alpha^* \mid \varphi? \end{aligned} \tag{3.1}$$

With respect to $\bot$, $\neg$ and $\wedge$ they have the normal meanings, and the standard logical operators $\top, \vee, \Rightarrow$, and $\Leftrightarrow$ are defined by their usual abbreviations.
For the rest of operators, it is helpful to give the intuitive meaning before the semantics. For the program operators:

- $\alpha \cdot \beta$ "first execute program α and then β".
- $\alpha \cup \beta$ "chose non-deterministically α or β and execute it".
- α^* "execute α a finite number of times chosen non-deterministically".

For the mixed operators:

- $[\alpha]\varphi$ "it is necessary that φ is true after executing α".
- $\varphi?$ "test φ, if *true* proceed, if *false* fail".

Observe that $[\alpha]$ is a modal operator, and there is one for each program α - we are in the presence of a multi-modal logic.
Similar to modal logic, for the modality $[\alpha]$ we can define its dual modality, $\langle\alpha\rangle$, in the usual way:

$$\langle\alpha\rangle\varphi := \neg[\alpha]\neg\varphi \tag{3.2}$$

This operator is the *possibility* modality, and it expresses that there is a execution of α that terminates in a state satisfying φ.

Two programs worth mentioning as an example are $\mathbf{skip}$ and $\mathbf{fail}$, defined by abbreviation as $\mathbf{skip} := \top?$ and $\mathbf{fail} := \bot?$.
There are other expressions that can be defined, but since they would not be used on the rest of the text, they will be omitted, but can be found on [10].

3.2 Semantics of PDL

As we saw, PDL contains several modalities, so the semantic structure will be the similar to modal logic - a *Kripke Frame*.

Def. 3.2.1 (Propositional Dynamic Logic Model):

A MULTI-MODAL KRIPKE FRAME is a pair $\mathcal{K} = (\Sigma, \{R_\alpha\}_{\alpha\in\Pi})$ where Σ is a set of *states* $u, v, w, \ldots$, Π is a countable set, and $\{R_\alpha\}_{\alpha\in\Pi}$ is a family of relations in Σ.
A PROPOSITIONAL DYNAMIC LOGIC MODEL is a tuple $\mathcal{M} = (\Sigma, \{R_a\}_{a\in\Pi}, V)$ where $(\Sigma, \{R_a\}_{a\in\Pi})$ is a multi-modal Kripke frame and $V\colon P \to \mathcal{P}(\Sigma)$ is a VALUATION FUNCTION assigning a subset of Σ to each propositional variable in P, intuitively, $V(p)$ is the set of states where p is true.

Given a PDL model, $\mathcal{M}$, we can define the interpretation of formulas and programs, $\|\cdot\|^{\mathcal{M}}$, that assigns the set of states where a formula is true and assigns each program a relation in Σ.

Def. 3.2.2 (Interpretation of Formulas):

- $\|p\|^{\mathcal{M}} = V(p) \subset \Sigma$
- $\|\bot\|^{\mathcal{M}} = \varnothing$
- $\|\neg\varphi\|^{\mathcal{M}} = \Sigma \setminus \|\varphi\|^{\mathcal{M}}$
- $\|\varphi \wedge \psi\|^{\mathcal{M}} = \|\varphi\|^{\mathcal{M}} \cap \|\psi\|^{\mathcal{M}}$
- $\|[\alpha]\varphi\|^{\mathcal{M}} = [\|\alpha\|^{\mathcal{M}}]\, \|\varphi\|^{\mathcal{M}}$

Def. 3.2.3 (Interpretation of Programs):

- $\|a\|^{\mathcal{M}} = R_a \in \Sigma \times \Sigma$
- $\|\alpha \cdot \beta\|^{\mathcal{M}} = \|\alpha\|^{\mathcal{M}} \cdot \|\beta\|^{\mathcal{M}}$
- $\|\alpha \cup \beta\|^{\mathcal{M}} = \|\alpha\|^{\mathcal{M}} \cup \|\beta\|^{\mathcal{M}}$
- $\|\alpha^*\|^{\mathcal{M}} = (\|\alpha\|^{\mathcal{M}})^*$
- $\|\varphi?\|^{\mathcal{M}} = \{(u, u) \in \Sigma \times \Sigma\colon u \in \|\varphi\|^{\mathcal{M}}\}$

The interpretation of a program is a relation and so the operations $\cdot$, $\cup$, $*$ and $[\ ]$ are the operations on relations described in Section 2.4.

Just like we did in PQL, when the model is clear from context, we will drop the superscript.

Prop. 3.2.4:

Let $(\Sigma, \{R_a\}_{a\in\Pi}, V)$ *be a model, then:*

- $\|\top\| = \Sigma$
- $\|\varphi \vee \psi\| = \|\varphi\| \cup \|\psi\|$
- $\|\langle\alpha\rangle\varphi\| = \Sigma\backslash[\|\alpha\|](\Sigma\backslash\|\varphi\|)$
- $\|\text{skip}\| = \{(u,u) \in \Sigma \times \Sigma \colon u \in \Sigma\} = id_\Sigma$
- $\|\text{fail}\| = \varnothing$

With the interpretation it is possible now to talk about *satisfiability* and *validity*.

Def. 3.2.5 (Satisfiability and Validity):

Given a model $\mathcal{M} = (\Sigma, \{R_a\}_{a\in\Pi}, V)$, a state $s \in \Sigma$, and a proposition φ we say that:

- State u *satisfies* φ in $\mathcal{M}$, written $\mathcal{M}, s \vDash \varphi$ if $s \in \|\varphi\|$.
- φ is *valid* in $\mathcal{M}$, written $\mathcal{M} \vDash \varphi$ if $\mathcal{M}, s \vDash \varphi$ for all states $s \in \Sigma$.
- Proposition φ is *valid*, written $\vDash \varphi$ if $\mathcal{M} \vDash \varphi$ for all models $\mathcal{M}$.

Let $\Gamma \subset L_P$ be a set of propositions. We say that:

- $\mathcal{M} \vDash \Gamma$ if $\mathcal{M} \vDash \psi$ for all $\psi \in \Gamma$.
- φ is a *semantical consequence* of Γ, written $\Gamma \vDash \varphi$ if for every model $\mathcal{M}$ we have $\mathcal{M} \vDash \varphi$ whenever $\mathcal{M} \vDash \Gamma$.

Given a model $\mathcal{M}$ we have an immediate result for the validity of a proposition φ in model $\mathcal{M}$.

Prop. 3.2.6:

Let $\mathcal{M} = (\Sigma, \{R_a\}_{a\in\Pi}, V)$ *be a model and* φ *a formula. Then*

$$\mathcal{M} \vDash \varphi \text{ iff } \|\varphi\| = \Sigma \tag{3.3}$$

***Proof*:**

Let $\mathcal{M}$ be such that $\mathcal{M} \vDash \varphi$

iff for all $s \in \Sigma$ $\mathcal{M}, s \vDash \varphi$

iff for all $s \in \Sigma$ $s \in \|\varphi\|$

iff $\|\varphi\| = \Sigma$ ■

We will use this equivalence in the example below.

Example 3.2.7:

The formula $[\alpha]\top$ is valid for any α.

***Proof*:**

$[\alpha]\top$ is valid, that is $\vDash [\alpha]\top$ iff $\mathcal{M} \vDash [\alpha]\top$ for all models $\mathcal{M}$ iff for all models $\mathcal{M}$ we have $\|[\alpha]\top\| = \Sigma$.

Let $\mathcal{M} = (\Sigma, \{R_a\}_{a\in\Pi}, V)$ be a model.

$\|[\alpha]\top\| = \{u \in \Sigma \colon \forall_{s\in\Sigma}\,((u \,\|\alpha\|\, s) \Rightarrow s \in \|\top\|)\} = \{u \in \Sigma \colon \forall_{s\in\Sigma}\,((u \,\|\alpha\|\, s) \Rightarrow s \in \Sigma)\}$

We have that $s \in \Sigma$, therefore the right hand-side of the implication is true and therefore the implication is true, thus $\|[\alpha]\top\| = \Sigma$. ■

3.3 Hilbert Calculus for PDL

Propositional Dynamic Logic has the following axioms and rules.

Def. 3.3.1 (Axioms and Rules of PDL):

A1. $\varphi \Rightarrow (\psi \Rightarrow \varphi)$

A2. $(\varphi \Rightarrow (\psi \Rightarrow \phi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \phi))$

A3. $(\neg\varphi \Rightarrow \neg\psi) \Rightarrow (\psi \Rightarrow \varphi)$

A4. $[\alpha](\varphi \Rightarrow \psi) \Rightarrow ([\alpha]\varphi \Rightarrow [\alpha]\psi)$

A5. $[\alpha](\varphi \wedge \psi) \Leftrightarrow [\alpha]\varphi \wedge [\alpha]\psi$

A6. $[\alpha \cup \beta]\varphi \Leftrightarrow [\alpha]\varphi \wedge [\beta]\varphi$

A7. $[\alpha \cdot \beta]\varphi \Leftrightarrow [\alpha][\beta]\varphi$

A8. $[\psi?]\varphi \Leftrightarrow \psi \Rightarrow \varphi$

A9. $\varphi \wedge [\alpha][\alpha^*]\varphi \Leftrightarrow [\alpha^*]\varphi$

A10. $\varphi \wedge [\alpha^*](\varphi \Rightarrow [\alpha]\varphi) \Rightarrow [\alpha^*]\varphi$

MP. $\dfrac{\varphi, \quad \varphi \Rightarrow \psi}{\psi}$

Gen. $\dfrac{\varphi}{[\alpha]\varphi}$

The Rule MP is called *modus ponens* and rule Gen is called *(modal) generalization*. Axioms A1, A2, A3 and rule MP come from propositional logic, axioms A4, A5 and rule Gen come from modal logic. Axiom A10 is called the PDL *induction axiom*.

Def. 3.3.2 (Derivation Sequence and Theorem):

Let $\varphi_1, \ldots, \varphi_n$ be PDL formulas. Then we say that

$1.\ \varphi_1$
$\vdots\ \ \vdots$
$n.\ \varphi_n$

is a DERIVATION SEQUENCE for φ_n if for every k, $1 \leq k \leq n$, φ_k is an Axiom, or it comes from φ_i, φ_j using MP. and $i, j < k$, or comes from φ_i using Gen. and $i < k$.

Furthermore we say that φ_n is a THEOREM, written $\vdash \varphi_n$, if it has a derivation sequence.

Note that if we already know the derivation sequence for a theorem, we can, for simplicity, use it on another derivation sequence stating that it is a theorem (as we do for axioms), as was done in the proof of the next result.

Prop. 3.3.3:

$\neg\langle \text{fail} \rangle \varphi$ *is a theorem and it is valid, i.e.,* $\vdash \neg\langle \text{fail} \rangle \varphi$ *and* $\vDash \neg\langle \text{fail} \rangle \varphi$*, respectively.*

***Proof*:**

For $\vdash \neg\langle \text{fail} \rangle \varphi$ we just need to consider the following derivation sequence:

1. $\top$ ($\top$ is a theorem)
2. $\top \Rightarrow (\varphi \Rightarrow \top)$ (A1.)
3. $\varphi \Rightarrow \top$ (MP. 1., 2.)
4. $\varphi \Rightarrow \neg\bot$ (3., $\top = \neg\bot$)
5. $\neg\neg\varphi \Rightarrow \neg\bot$ (4., $\varphi \Leftrightarrow \neg\neg\varphi$ is a theorem)
6. $(\neg\neg\varphi \Rightarrow \neg\bot) \Rightarrow (\bot \Rightarrow \neg\varphi)$ (A3.)
7. $\bot \Rightarrow \neg\varphi$ (MP. 5., 6.)
8. $[\bot?]\neg\varphi$ (7. $[\bot?]\neg\varphi \Leftrightarrow \bot \Rightarrow \neg\varphi$ by A8.)
9. $\neg\langle \text{fail} \rangle \varphi$ (8. by definition $\neg\langle \text{fail} \rangle \varphi = [\bot?]\neg\varphi$)

For $\vDash \neg\langle \text{fail} \rangle \varphi$ lets consider a model $\mathcal{M} = (\Sigma, \{R_a\}_{a \in \Pi}, V)$.
$\mathcal{M} \vDash \neg\langle \text{fail} \rangle \varphi$ iff $\|\neg\langle \text{fail} \rangle \varphi\| = \Sigma$

$\|\neg\langle \text{fail} \rangle \varphi\| = \|[\bot?]\neg\varphi\| = [\varnothing]\,\|\neg\varphi\| = \{w \in \Sigma \colon \forall_{s \in \Sigma}((w,s) \in \varnothing \Rightarrow v \in \|\neg\varphi\|)\}$
Since is impossible for $(w,s) \in \varnothing$ the implication is true for all (w,s), thus $\|\neg\langle \text{fail} \rangle \varphi\| = \Sigma$. ■

We finalize this Chapter by mentioning that Propositional Dynamic Logic is *sound* and *complete*, that is, for every formula φ we have

$$(\text{Soundness}) \quad \text{If } \vdash \varphi \text{ then } \vDash \varphi \tag{3.4}$$

and

$$(\text{Completeness}) \quad \text{If } \vDash \varphi \text{ then } \vdash \varphi \tag{3.5}$$

Chapter 4

Quantum Transition Systems

Propositional Quantum Logic, as seen in Section 2.3, leaves out a large part of Quantum Mechanics - time evolutions (unitary operators). In order to enrich PQL with these operators one needs to switch to a dynamic logic.

This chapter presents a semantical structure capable of handling a quantum dynamic logic, Quantum Transitions Systems (see [1]), that is, it will be used to build a model for such logic. We start by introducing the skeleton of this structure, *dynamic frames* (Section 4.1), then by embedding these frames with properties that mimic Hilbert spaces we get a *quantum transition system* (Section 4.2), and finally we give some results about *quantum actions* (Section 4.3) that correspond to time evolutions.

4.1 Dynamic Frame

As we saw in Chapter 3, the first element of a PDL model is a Kripke frame and in this Section we shall capitalize on that to define dynamic frames.

Def. 4.1.1 (Labeled Transition System):

A LABELED TRANSITION SYSTEM is a multi-modal Kripke frame $(\Sigma, \{\xrightarrow{a}\}_{a\in\mathcal{A}})$ where Σ is a set of *states* and $\{\xrightarrow{a}\}_{a\in\mathcal{A}}$ is a family of binary relations on Σ called TRANSITION RELATIONS, labeled by BASIC ACTIONS in $\mathcal{A}$.

Def. 4.1.2 (Dynamic Frame):

A DYNAMIC FRAME is a labeled transition system $\mathcal{F} = (\Sigma, \{\xrightarrow{P?}\}_{P\in\mathcal{L}}, \{\xrightarrow{U}\}_{U\in\mathcal{U}})$, where:

• Σ is a set whose elements are called STATES;

• $\mathcal{L} \subset \mathcal{P}(\Sigma)$ is a family of subsets $P \subset \Sigma$ called TESTABLE PROPERTIES;

• $\{\xrightarrow{P?}\}_{P\in\mathcal{L}}$ is a family of binary transition relations on Σ, labeled by TEST ACTIONS $P?$;

• $\{\xrightarrow{U}\}_{U\in\mathcal{U}}$ is a family of binary transition relations on Σ, labeled by BASIC UNITARY EVOLUTIONS $U \in \mathcal{U}$.

Example 4.1.3 (Dynamic Frame of PDL):

From the last Chapter, it should be clear the similarities of a dynamic frame with propositional dynamic logic. Given a model of PDL, $\mathcal{M} = (\Sigma, \{R_a\}_{a\in\Pi}, V)$, the corresponding dynamic frame is such that $\mathcal{L} := \{\|\varphi\| : \varphi \in L_P\}$, $\xrightarrow{P?} := \{(u,u) \in \Sigma \times \Sigma : u \in P\}$, $\mathcal{U} := \Pi$, and $\xrightarrow{U} := \|U\|$.

Given a dynamic frame $\mathcal{F}$ we can define the binary relations $\rightarrow$ (measurement) and $\perp$ (orthogonality) in the following way:

Def. 4.1.4 (Measurement Relation):

Given states $s, t \in \Sigma$, t can be MEASURED from s,

$$s \to t \text{ iff } \exists_{P \in \mathcal{L}}\, s \xrightarrow{P?} t \tag{4.1}$$

Def. 4.1.5 (Orthogonality Relation):

Given states $s, t \in \Sigma$, s is ORTHOGONAL to t,

$$s \perp t \text{ iff } s \not\to t \tag{4.2}$$

Given a set of states $S \subset \Sigma$ we write

$$t \perp S \text{ iff } \forall_{s \in S}\, t \perp s \tag{4.3}$$

With this relations we can define the set of states that do not reach a given set S, that is the *orthogonal complement* of S.

Def. 4.1.6 (Orthocomplement):

Given a set of states $S \subset \Sigma$ the ORTHOCOMPLEMENT of S is the set $\sim S \equiv S^{\perp} := \{t \in \Sigma \colon t \perp S\}$

Prop. 4.1.7:

Let $S, P \subset \Sigma$. We have that

$$\text{If } S \subset P \text{ then } S^{\perp} \supset P^{\perp} \tag{4.4}$$

***Proof*:**

Let $t \in P^{\perp}$. Then $\forall_{s \in P}\, t \perp s$.

In particular, since $S \subset P$, $\forall_{s \in S}\, t \perp s$, that is $t \in S^{\perp}$. ■

If we take the orthocomplement twice, we have a special notation:

Def. 4.1.8 (Biorthogonal Closure):

The BIORTHOGONAL CLOSURE of S is the set $\overline{S} :=\sim (\sim S)$

One can ask if applying the orthocomplement twice we get back the original set. It is not always the case, but when it happens we say the set is *biorthogonally closed*.

Def. 4.1.9 (Biorthogonally Closed Set):

The set S is said to be BIORTHOGONALLY CLOSED if $\overline{S} = S$.

Although a set might not be biorthogonally closed, when the measurement relation $\to$ is symmetric we can say more about the biorthogonal closure of a set:

Prop. 4.1.10:

$S \subset \overline{S}$ for all $S \subset \Sigma$ iff $\to$ is a symmetric relation.

***Proof*:**

First we note that $\to$ is symmetric iff $\not\to$ is symmetric iff $\perp$ is symmetric

$\Rightarrow)$

Let $a, b \in \Sigma$ be such $a \perp b$, moreover, $a \perp \{b\}$

By hypothesis, $\{b\} \subset \overline{\{b\}}$, therefore, $b \in \overline{\{b\}}$, and we have:

$b \in \overline{\{b\}}$ iff $\forall_{t \in \{b\}^\perp}\, b \perp t$ iff $\forall_{t \perp b}\, b \perp t$, in particular, since $a \perp b$ we have that $b \perp a$
Thus, because a and b are arbitrary, we have that $\rightarrow$ is symmetric.

$\Leftarrow$)
Let $S \subset \Sigma$ and $w \in S$.
$w \in \overline{S}$ iff $\forall_{t \in S^\perp}\, w \perp t$ iff $\forall_{t \perp S}\, w \perp t$ $(\dagger)$
We have that $t \perp S$ iff $\forall_{s \in S}\, t \perp s$. Since $w \in S$ then $t \perp w$, and by hypothesis, $\rightarrow$ is symmetric, thus $\perp$ is symmetric and we get that $w \perp t$, therefore $(\dagger)$ is satisfied and we conclude that $S \subset \overline{S}$. ■

Example 4.1.11 (Dynamic Frame of PDL):
The Dynamic frame of PDL of Example 4.1.3 is such that $\sim S = \Sigma \backslash S$ and therefore $S = \overline{S}$, *i.e.*, all subsets $S \subset \Sigma$ are biorthogonally closed.

4.2 Quantum Transition System

As seen in the examples from previous Section, a dynamic frame can be used to capture the semantics of PDL. This section uses dynamic frames to create a semantics for a quantum logic with quantum actions/programs with base on propositional quantum logic. The straightforward way to do this is to try to capture the properties of a orthomodular lattice based on closed linear subspaces from a Hilbert space.
In PDL, $\mathcal{L}$ is the interpretation of formulas, so for the quantum version it is reasonable to have the condition that $\mathcal{L}$ will be the family of biorthogonal closed sets, since in PQL, the interpretation of a formula is a closed linear subspace.

Def. 4.2.1 (Quantum Transition System):
A QUANTUM TRANSITION SYSTEM or QUANTUM DYNAMIC FRAME is a dynamic frame

$$\mathcal{F} = (\Sigma, \{\xrightarrow{P?}\}_{P \in \mathcal{L}}, \{\xrightarrow{U}\}_{U \in \mathcal{U}}) \tag{4.5}$$

satisfying the properties below, where we consider $s, t, w \in \Sigma$, $P \in \mathcal{L}$, and $U \in \mathcal{U}$.

1. $\mathcal{L} = \{S \in \mathcal{P}(\Sigma) \colon \overline{S} = S\}$
2. Closure under arbitrary conjunctions: if $\mathcal{L}' \subset \mathcal{L}$ then $\bigcap_{L' \in \mathcal{L}'} L' \in \mathcal{L}$
3. Atomicity. $\{s\} \in \mathcal{L}$, *i.e.*, states are testable. (or equivalently, states can be distinguished by tests, if $s \neq t$ then $\exists_{P \in \mathcal{L}} \colon s \perp P, t \not\perp P$)
4. Adequacy. Testing a true property does not change the state: if $s \in P$ then $s \xrightarrow{P?} t$ iff $t = s$.
5. Repeatability. Any property holds after it has been successfully tested: if $s \xrightarrow{P?} t$ then $t \in P$
6. "Covering Law". If $s \xrightarrow{P?} w \neq t \in P$ then $\exists_{v \in P} \colon t \rightarrow v \not\rightarrow s$
7. Self-Adjointness Axiom. If $s \xrightarrow{P?} w \rightarrow t$ then $\exists_{v \in \Sigma} \colon t \xrightarrow{P?} v \rightarrow s$

8. Proper Superposition[1] Axiom. Every two states of a quantum system can be properly superposed into a new state: $\forall_{s,t\in\Sigma}\,\exists_{w\in\Sigma}\colon s\to w\to t$

9. Reversibility and Totality Axioms. Basic unitary evolutions are total bijective functions: $\forall_{t\in\Sigma}\,\exists^1_{s\in\Sigma}\colon s\xrightarrow{U}t$ and $\forall_{s\in\Sigma}\,\exists^1_{t\in\Sigma}\colon s\xrightarrow{U}t$

10. Orthogonality Preservation. Basic unitary evolutions preserve (non) orthogonality: If $s,t,s',t'\in\Sigma$ are such that $s\xrightarrow{U}s'$ and $t\xrightarrow{U}t'$, then $s\to t\Leftrightarrow s'\to t'$.

11. Mayet's Condition: Orthogonal Fixed Points. $\exists_{U\in\mathcal{U}}\,\exists_{P\in\mathcal{L}}: U(P)\subsetneq P$; and the set of fixed-point states of U has dimension $\geqslant 2$, *i.e.*: $\exists_{t,w\in\Sigma}\,\forall_{s\in\overline{\{t,w\}}}\colon t\perp w, U(s)=s$

With these we now discuss properties of the measurement relation $\to$.

Prop. 4.2.2 ($\to$ is Reflexive):

The measurement relation, $\to$, is reflexive, i.e., $\forall_{s\in\Sigma}\ s\to s$.

***Proof*:**

Let $s\in\Sigma$. By the atomicity property $\{s\}\in\mathcal{L}$, and, because $s\in\{s\}$, by adequacy we have $s\xrightarrow{\{s\}?}s$.
Thus by definition of $\to$ we have $s\to s$. ■

Prop. 4.2.3 ($\to$ is Symmetric):

The measurement relation, $\to$, is symmetric, i.e., $\forall_{s,t\in\Sigma}\ (s\to t\ \Rightarrow\ t\to s)$.

***Proof*:**

Let $s,t\in\Sigma$ be such that $s\to t$, then, by definition of $\to$, $\exists_{P\in\mathcal{L}}$ such that $s\xrightarrow{P?}t$.
Using the fact that $\to$ is reflexive we have that

$$s\xrightarrow{P?}t\to t \tag{4.6}$$

Then by the self-adjointness axiom we get

$$\exists_{v\in\Sigma}\ t\xrightarrow{P?}v\to s \tag{4.7}$$

Now we note that by repeatability if $s\xrightarrow{P?}t$ then $t\in P$, thus, by adequacy, $t\xrightarrow{P?}v$ iff $t=v$, therefore we can conclude that $t\to s$. ■

Prop. 4.2.4 ($\to$ is not Transitive):

Let $s,t,w\in\Sigma$. If $s\to w\to t$ it s not necessarily true that $s\to t$.

***Proof*:**

Let $s,t\in\Sigma$ be such that $s\perp t$, that is $s\not\to t$.
By the proper superposition we have that exists $w\in\Sigma$ such that $s\to w\to t$, however is not the case that $s\to t$. ■

The measurement relation is reflexive and symmetric, but not transitive. Moreover, since it is symmetric, we have the property that if $S\subset\Sigma$ then $S\subset\overline{S}$, as seen in Proposition 4.1.10. From this, we can prove a general property about complements and the family $\mathcal{L}$:

[1] In Quantum Mechanics, superposition of two states corresponds to linear combinations of those states.

Prop. 4.2.5:

Let $S \subset \Sigma$. Then $S^\perp \in \mathcal{L}$, that is $\overline{S^\perp} = S^\perp$. Moreover, $P \in \mathcal{L}$ iff $\exists_{S \subset \Sigma}\ P = S^\perp$.

***Proof*:**

From reflexivity of $\rightarrow$ we have $S^\perp \subset \overline{S^\perp}$, so we only need to show that $\overline{S^\perp} \subset S^\perp$.

$\overline{S^\perp} = S^{\perp\perp\perp} = \overline{S}^\perp$

Since $S \subset \overline{S}$ then $S^\perp \supset \overline{S}^\perp = \overline{S^\perp}$

This proves $\Leftarrow$ part of the iff, lets now see that if $P \in \mathcal{L}$ then $P = S^\perp$ for some S.

Let $P \in \mathcal{L}$, then by definition $P = \overline{P}$, that is $P = (P^\perp)^\perp$, so we only need to take $S = P^\perp$. ■

If we have in mind that this is trying to capture the properties of an orthomodular lattice based on Hilbert spaces, property 2 seen in this perspective is the topological property of a arbitrary intersection of closed sets is a closed set. Related with topology, we can also show that $\varnothing, \Sigma \in \mathcal{L}$.

Prop. 4.2.6:

In any quantum dynamic frame $\varnothing, \Sigma \in \mathcal{L}$. We also have that:

$\xrightarrow{\varnothing?} = \mathrm{fail}$*, i.e., the empty relation.*

$\xrightarrow{\Sigma?} = \mathrm{skip}$*, i.e., the identity relation in Σ.*

***Proof*:**

Since $\varnothing$ has no elements, then for any state t it is true that t is orthogonal to all elements of $\varnothing$, thus $t \perp \varnothing$.

Given a state s thanks to $\rightarrow$ being reflexive we have that $s \not\perp s$, thus $s \not\perp \Sigma$.

We have then:

$$\begin{aligned} \varnothing^\perp &= \{t \in \Sigma \colon t \perp \varnothing\} = \{t \in \Sigma \colon true\} = \Sigma \\ \Sigma^\perp &= \{t \in \Sigma \colon t \perp \Sigma\} = \{t \in \Sigma \colon false\} = \varnothing \end{aligned} \tag{4.8}$$

We conclude that $\overline{\varnothing} = \varnothing$ and $\overline{\Sigma} = \Sigma$.

Given $s, t \in \Sigma$ we have that:

If $s \xrightarrow{\varnothing?} t$ then $t \in \varnothing$ by the repeatability property, thus $\xrightarrow{\varnothing?}$ is the empty relation.

Since $s \in \Sigma$ then by adequacy $s \xrightarrow{\Sigma?} t$ iff $t = s$, therefore $\xrightarrow{\Sigma?}$ is the identity relation in Σ. ■

Property 9 states that given $U \in \mathcal{U}$ then $\xrightarrow{U}$ is a bijective function (which allows us to write, for simplicity, $U(s) = t$ instead of $s \xrightarrow{U} t$) and together with property 10 in the context of Hilbert spaces, it is stating that actions U are actually unitary operators.

A property not explored yet is property 6, that has as consequence that actions $\xrightarrow{P?}$ are partial function (which, just like unitary actions, allows for us to write $P?(s) = t$ instead of $s \xrightarrow{P?} t$), and together with other properties concerning tests, in a Hilbert space, tests correspond to orthogonal projections.

Prop. 4.2.7:

If $P \in \mathcal{L}$ then $\xrightarrow{P?}$ is a partial function.

***Proof*:**

Let $w \neq t \in P$ such that $s \xrightarrow{P?} w$ and $s \xrightarrow{P?} t$.

By covering law, $\exists_{v \in P}\, t \to v \not\to s \quad (\dagger)$.

We have then $s \xrightarrow{P?} t \to v$, therefore by self-adjointness $\exists_{u \in \Sigma}\, v \xrightarrow{P?} u \to s$.

However, using adequacy, since $v \in P$ then $u = v$ and we get $v \to s$ which contradicts $(\dagger)$. ■

Since $P?$ are partial functions we are interested in knowing what is the kernel of $P?$, that is $[P?]\varnothing$. It would be great, since we would like for $P?$ to correspond to projections in a Hilbert space, that the kernel would be $P^{\perp}$, and the next Proposition confirms this result:

Prop. 4.2.8:

Let $P \subset \Sigma$ and $P? := \overline{P}?$ if P is not testable. Then

$[P?]\varnothing = S^{\perp}$, and moreover $[P?]\varnothing$ is testable.

***Proof*:**

$\subset$)

Let $w \in [P?]\varnothing$, that is, $P?(w)\uparrow$ ($P?$ is not defined on w)

Assume by contradiction that there is $s \in P$ such that $w \not\perp s$, *i.e.*, $w \to s$.

Since $s \in P \subset \overline{P}$ then $P?(s) \in \overline{P}$. Thus we have

$$s \xrightarrow{P?} s \to w \tag{4.9}$$

And by self-adjointness $\exists_{v \in \Sigma}\, w \xrightarrow{P?} v \to s$, that is $P?(w)\downarrow$ ($P?$ is defined on w) which is a contradiction.

$\supset$)

Let $w \in P^{\perp}$, and assume, by contradiction, that $P?(w)\downarrow$.

Then by adequacy $P?(w) \in \overline{P}$. We have $w \to P?(w) \in \overline{P}$, that is, $w \not\perp P?(w) \in \overline{P}$, thus $w \notin \overline{P}^{\perp} = P^{\perp}$ which is a contradiction. ■

This properties mimic what happens in Hilbert spaces, so a obvious question would be to ask if a Hilbert space can be made into a quantum dynamic frame. As we will see, the answer is yes, but with a caveat.

Def. 4.2.9 (Concrete Quantum Dynamic Frame):

Given a Hilbert space $\mathcal{H}$, we can construct a dynamic frame $\mathcal{F}(\mathcal{H})$ in the following way:

- Σ is the family of 1-dimensional closed linear subspaces of $\mathcal{H}$
- $\mathcal{L} \subset \mathcal{P}(\Sigma)$ is such that if $P \in \mathcal{L}$ then $V_P := \bigcup_{s \in P} s$ is a closed linear subspace.
- $P?$ is the map induced on Σ by the orthogonal projector on V_P
- $\mathcal{U}$ is the family of maps induced on Σ by the unitary operators on $\mathcal{H}$

This is called a CONCRETE DYNAMIC FRAME

If $F : \mathcal{H} \longrightarrow \mathcal{H}$ is a linear map, $x \in \mathcal{H}$, and $s = \overline{x} := \overline{\{x\}}$ a state, then the induced map on Σ, $F_{\Sigma} : \Sigma \longrightarrow \Sigma$ is given by

$$F_{\Sigma}(s) = F_{\Sigma}(\overline{x}) := \begin{cases} \overline{F(x)}, & \text{if } F(x) \neq 0 \\ \text{undefined}, & \text{otherwise} \end{cases} \tag{4.10}$$

F_{Σ} is well-defined since $\overline{y} = \overline{x}$ iff $y = \lambda x$, therefore $F(y) = \lambda F(x)$, thus $\overline{F(y)} = \overline{F(x)}$.

Prop. 4.2.10:

Definition 4.2.9 satisfies properties 1-10. If it satisfies property 11 then $\mathcal{H}$ has infinite dimension.

***Proof*:**

1.

By definition, if $P \in \mathcal{L}$ then V_P is a closed linear subspace, therefore $\overline{V_P} = V_P$.

2.

Let $\mathcal{L}' \subset \mathcal{L}$ and $P := \bigcap \mathcal{L}'$.

First we show that $V_P = \bigcap_{L \in \mathcal{L}} V_L$, that is

$$\bigcup_{s \in P} s = \bigcap_{L \in \mathcal{L}'} \bigcup_{t \in L} t \tag{4.11}$$

$\subset)$

$x \in V_P \Rightarrow \exists_{s \in P}\, x \in s$

Since $s \in L$ for all $L \in \mathcal{L}'$ then $s \subset \bigcup_{t \in L} t$ for all $L \in \mathcal{L}'$

Thus, we have $x \in \bigcup_{t \in L} t$ for all $L \in \mathcal{L}'$, *i.e.*, $x \in \bigcap_{L \in \mathcal{L}'} \bigcup_{t \in L} t$

$\supset)$

$x \in \bigcap_{L \in \mathcal{L}'} \bigcup_{t \in L} t$ iff $\forall_{L \in \mathcal{L}'} \exists_{t_L \in L}\, x \in t_L$

Since t_L's are 1-dimensional subspaces we have that for all $L \in \mathcal{L}'$ $t_L = \operatorname{span}\{x\} =: s$

Therefore, exists $s \in P$ such that $x \in s$, *i.e.*, $x \in \bigcup_{s \in P} s$

Finally, $\bigcap_{L \in \mathcal{L}} V_L$ is a closed linear subspace because the intersection of linear subspaces is a linear subspace, and the intersection of closed sets is a closed set.

3.

$\{s\} \in \mathcal{L}$ if $V_{\{s\}} = s$ is a closed linear subspace, which is trivially true since Σ is the set of 1-dimensional closed linear subspaces and $s \in \Sigma$.

4.

Let $P \subset \Sigma$, $s \in P$, and $0 \neq x \in s$.

Let $proj_P$ be the orthogonal projection on V_P.

$x \in V_P$ since $s \subset V_P$. Therefore, $P?(s) = P?(\overline{x}) = \overline{proj_P(x)} = \overline{x} = s$.

5.

Let $P \subset \Sigma$ and $s, t \in \Sigma$, such that $s \xrightarrow{P?} t$, that is, $P?(s) = t$.

Let $x \in s$, then $t = P?(s) = P?(\overline{x}) = \overline{proj_P(x)}$.

We have that $proj_P(x) \in V_P$, thus, $t = \overline{proj_P(x)} \in P$.

6.

Let $P \subset \Sigma$, $s \in \Sigma$, and $w, t \in P$ such that $w \neq t$ (this implies $\dim \mathcal{H} > 1$) and $P?(s) = w$.

Let $S = \{s\}$, then $\mathcal{H} = V_S \oplus {V_S}^\perp = s \oplus s^\perp$. We note that $s^\perp$ is non-trivial since it must have dimension at least 1.

We have two cases: $s \in P$ or $s \notin P$

- $s \in P$:

In this case we have that $s = w$. Let $0 \neq x \in s$, $0 \neq y \in s^\perp$, we know that $\langle x, y\rangle = 0$

By the properties of projections, $\langle proj_P(x), y\rangle = \langle x, proj_P(y)\rangle$

Since $proj_P(x) = x$ we have $\langle x, proj_P(y)\rangle = \langle x, y\rangle = 0$. We just need to chose $v := \overline{y}$

Since $t \neq w$ any non-zero vector of t is not in s therefore $t \not\perp v$, thus $t \to v \not\to s$.

- $s \notin P$

In this case we have that $\dim \mathcal{H} \geq 3$, let $W := s \oplus w \oplus t$ ($\dim W = 3$)

Since $\mathcal{H} = s \oplus s^\perp$ then there exists non linear non zero vectors $y_1, y_2 \in s^\perp$ such that $W = s \oplus \overline{y_1} \oplus \overline{y_2}$.

Now we have that[2] $\dim((\overline{y_1} \oplus \overline{y_2}) + (w \oplus t)) = \dim W = 3$ therefore $\dim((\overline{y_1} \oplus \overline{y_2}) \cap (w \oplus t)) = 1$

let $y \in (\overline{y_1} \oplus \overline{y_2}) \cap (w \oplus t)$, thus $y \in V_P \cap s^\perp$, moreover, $proj_P(y) = y$ and $\langle y, x\rangle = 0$.

We conclude that $\langle y, proj_P(x)\rangle = \langle proj_P(y), x\rangle = \langle y, x\rangle = 0$, we can take $v := \overline{y}$ and have $t \to v \not\to s$.

7.

Comes directly from orthogonal projections being self-adjoint.

Let $s, t, w \in \Sigma$ such that $s \xrightarrow{P?} w = P?(s) \to t$, then let $0 \neq x \in s$ and $0 \neq y \in t$, such that $\exists_{P' \in \mathcal{L}} \langle proj_P(x), y\rangle \neq 0$.

By self-adjointness of orthogonal projections $\langle x, proj_P(y)\rangle \neq 0$.

Thus, choosing $v := \overline{proj_P(y)}$ we have $t \xrightarrow{P?} v \to s$.

8.

Let $s, t \in \Sigma$, $0 \neq x \in s$, and $0 \neq y \in t$. Let $z = \alpha x + \beta y$ such that $proj_s(\beta y) \neq -\alpha x$ and $proj_t(\alpha x) \neq -\beta y$.

Then $proj_s(z) = \alpha x + proj_s(\beta y) \neq 0$ and $proj_t(z) = proj_t(\alpha x) + \beta y \neq 0$.

Thus $\exists_{v \in \Sigma}\, s \to v \to t$, with $v := \overline{z}$.

9. and 10.

Unitary operators are bijective and satisfy $\langle x, y\rangle = \langle U(x), U(y)\rangle$.

Lets now see that in order to satisfy property 11 it must have infinite dimension:

Let P be such that V_P as a finite orthogonal basis $v_1, \ldots, v_n$, and $U(V_P) = V_P$. Since U is unitary, $U(v_1), \ldots, U(v_n)$ is still a orthogonal basis for $U(V_P)$, therefore $\dim V_P = \dim U(V_P)$. Since $U(V_P) \subset V_P$ and they have the same dimension (and its finite) we must have $U(V_P) = V_P$.

Thus, for $U(V_P) \subsetneq V_P$ it must be that V_P has infinite dimension, and therefore $\mathcal{H}$ must have infinite dimension. ■

[2] $s \to w$ therefore $w \not\subset (\overline{y_1} \oplus \overline{y_2})$

4.3 Quantum Actions

We have seen some properties of quantum dynamic frames involving tests and unitary actions, now we are going to show more results about actions that can be made from composition and union of tests and unitary actions.

Def. 4.3.1 (Quantum Action):

The class of QUANTUM ACTIONS or QUANTUM PROGRAMS, $\mathcal{Q}(\mathcal{F})$ over a quantum dynamic frame $\mathcal{F}$ is the smallest family of binary relations which contain all tests $\xrightarrow{P?}$, all basic unitary actions $\xrightarrow{U}$ and their inverses $\xrightarrow{U^{-1}} := (\xrightarrow{U})^{-1}$, is closed under relational composition $R \cdot R'$, and is closed under arbitrary union of relations $\cup_{i\in I} R_i$.

Def. 4.3.2 (Deterministic Action):

A action that can expressed without using union is called a DETERMINISTIC ACTION. The set of deterministic action is denoted by $\mathcal{D}$.

Is important to note that deterministic action are partial functions.

Prop. 4.3.3:

Every quantum actions is either a deterministic action or can be written as a union (choice) of deterministic actions.

***Proof*:**

We just need to notice that given a family of actions $\{\alpha_i\}_{i\in I}$ and $\{\beta_j\}_{j\in J}$ we have

$$\bigcup_{i\in I} \alpha_i \cdot \bigcup_{j\in J} \beta_j = \bigcup_{(i,j)\in I\times J} \alpha_i \cdot \beta_j \tag{4.12}$$

Indeed,

$(s,t) \in \bigcup_{i\in I} \alpha_i \cdot \bigcup_{j\in J} \beta_j$
iff $\exists_{w\in\Sigma}\, (s,w) \in \bigcup_{i\in I} \alpha_i \wedge (w,t) \in \bigcup_{j\in J} \beta_j$
iff $\exists_{w\in\Sigma}\, (\exists_{i\in I}(s,w) \in \alpha_i \wedge \exists_{j\in J}(w,t) \in \beta_j)$
iff $\exists_{w\in\Sigma}\, \exists_{(i,j)\in I\times J}((s,w) \in \alpha_i \wedge (w,t) \in \beta_j)$
iff $\exists_{(i,j)\in I\times J}((s,t) \in \alpha_i \cdot \beta_j)$
iff $(s,t) \in \bigcup_{(i,j)\in I\times J} \alpha_i \cdot \beta_j$ ■

Prop. 4.3.4 (Adjointness for Deterministic Actions):

There is a unique map $\cdot^\dagger : \mathcal{D} \longrightarrow \mathcal{D}$ satisfying:

- $(P?)^\dagger = P?$
- $U^\dagger = U^{-1}$, $(U^{-1})^\dagger = U$
- $(\pi \cdot \sigma)^\dagger = \sigma^\dagger \cdot \pi^\dagger$.

Prop. 4.3.5:

Let $s, w, t \in \Sigma$ and $\pi \in \mathcal{D}$. Then:
If $s \xrightarrow{\pi} w \to t$ then $\exists_{v\in\Sigma}\, t \xrightarrow{\pi^\dagger} v \to s$.

***Proof*:**

Lets prove by induction on the structure of π.

First we note that π is a partial function, therefore $w = \pi(s)$ and $v = \pi^\dagger(t)$ are uniquely defined.

Base:

The case $\pi = P?$ is true by self-adjointness, since $(P?)^\dagger = P?$.

For the case $\pi = U$, we note that we want to prove:

If $U(s) \to t$ then $s \to U^{-1}(t)$

We know that $s \xrightarrow{U} U(s)$ and $U^{-1}(t) \xrightarrow{U} t$, since by hypothesis $U(s) \to t$, using orthogonality preservation we get the desired result $s \to U^{-1}(t)$.

$$\begin{array}{ccc} s & \xrightarrow{U} & U(s) \\ \downarrow & & \downarrow \\ U^{-1}(t) & \xrightarrow{U} & t \end{array} \tag{4.13}$$

Step:

Again, we want to prove that if $\pi(s) \to t$ then $s \to \pi^\dagger(t)$

Let $\pi = \pi_1 \cdot \ldots \cdot \pi_{n+1} = \pi_1 \cdot \pi', \quad \pi_i$ of the form $P?$ or U.

Induction Hypotesis: If $\pi'(w') \to t$ them $w' \to \pi'^\dagger(t)$

We have that $s \xrightarrow{\pi_1} \pi_1(s) =: w' \xrightarrow{\pi'} \pi'(w') \to t$

Applying the Induction Hypothesis we get $w' \to \pi'^\dagger(t)$

We have then $\pi_1(s) \to \pi'^\dagger(t)$

Since π_1 is either $P?$ or U, cases covered in the Base, we get

$$s \to \pi_1^\dagger(\pi'^\dagger(t)) = (\pi'^\dagger \cdot \pi_1^\dagger)(t) = (\pi_1 \cdot \pi')^\dagger(t) = \pi^\dagger(t) \tag{4.14}$$

That is the desired result, $s \to \pi^\dagger(t)$. ■

Note that, since $(\pi^\dagger)^\dagger = \pi$, what this result is saying is

$$\pi(s)\downarrow \wedge \pi(s) \to t \quad \Leftrightarrow \quad \pi^\dagger(t)\downarrow \wedge \pi^\dagger(t) \to s \tag{4.15}$$

And negating both sides we get

$$\pi(s)\uparrow \vee \pi(s) \perp t \quad \Leftrightarrow \quad \pi^\dagger(t)\uparrow \vee \pi^\dagger(t) \perp s \tag{4.16}$$

For a deterministic action π, we can identify $\pi(s)$ and $\pi(\{s\})$, since $\pi(\{s\})$ is a singleton or the empty set[3]. Then we can simply write

$$\pi(s) \perp t \quad \Leftrightarrow \quad \pi^\dagger(t) \perp s \tag{4.17}$$

Corollary 4.3.6:

Let $s \in \Sigma$ be a state and $\pi \in \mathcal{D}$ be a deterministic action. Then

$$\pi(s) = ([\pi^\dagger]s^\perp)^\perp \quad \text{and} \quad \pi^\dagger(s) = ([\pi]s^\perp)^\perp \tag{4.18}$$

[3]Note that given $S \subset \Sigma$ it is always true that $S \perp \varnothing$.

***Proof*:**

Given $s, t \in \Sigma$ we have that $\pi(s) \perp t \Leftrightarrow s \perp \pi^\dagger(t)$, *i.e.*, $t \in (\pi(s))^\perp \Leftrightarrow \pi^\dagger(t) \subset s^\perp$.

Therefore $(\pi(s))^\perp = \{t \in \Sigma \colon \pi^\dagger(t)\uparrow \vee \pi^\dagger(t) \in s^\perp\} = [\pi^\dagger]s^\perp$.

Since π is deterministic, $\pi(s)$ is the empty set or is a state, either way we have $\pi(s) \in \mathcal{L}$ so

$\pi(s) = (\pi(s))^{\perp\perp} = ([\pi^\dagger]s^\perp)^\perp$.

Similarly we have that $\pi^\dagger(s) \perp t \Leftrightarrow s \perp \pi(t)$, that is, $t \in (\pi^\dagger(s))^\perp \Leftrightarrow \pi(t) \subset s^\perp$.

Thus $(\pi^\dagger(s))^\perp = \{t \in \Sigma \colon \pi(t)\uparrow \vee \pi(t) \in s^\perp\} = [\pi]s^\perp$.

Since π is deterministic, so is $\pi^\perp$ and therefore $\pi^\dagger(s)$ is empty or is a state, either way we have $\pi^\dagger(s) \in \mathcal{L}$ so

$\pi^\dagger(s) = (\pi^\dagger(s))^{\perp\perp} = ([\pi]s^\perp)^\perp$. ■

From the above result, it is possible to define the ajoint of a general quantum action $R \in \mathcal{Q}$.

Def. 4.3.7 (Adjoint for Quantum Actions):

Given a quantum action $R \in \mathcal{Q}$ we can define the quantum action $R^\dagger$ such that

$$sR^\dagger t \text{ iff } t \perp [R]s^\perp \tag{4.19}$$

Which can be written similarly to the previous result:

$$R^\dagger(s) = ([R]s^\perp)^\perp \tag{4.20}$$

We now know that given an action R and state s that $R(s) = ([R]s^\perp)^\perp$, but what happens when we have $S \subset \Sigma$? It turns out that we get something similar $\overline{R(S)} = ([R^\dagger]S^\perp)^\perp$, and it happens that $\overline{R(S)}$ is the strongest testable postcondition ensured by applying action R on a state satisfying S.

Def. 4.3.8 (Strongest Testable Postcondition):

Let $R \in \mathcal{Q}$ be a quantum action and $S \subset \Sigma$, we defined the STRONGEST TESTABLE POSTCONDITION as the biorthogonal closure of the image of S by R, and we denoted it by $R[S] := \overline{R(S)}$

Prop. 4.3.9:

$R[S]$ is the strongest testable postcondition ensured by executing R on any state satisfying S.

***Proof*:**

It is testable since it is the biorthogonal closure of a set.

It is the strongest testable postcondition, *i.e.*, $\forall_{Q \in \mathcal{L}} (R[S] \subset Q \Leftrightarrow R(S) \subset Q)$

$\Rightarrow$)

We just need to note that $R(S) \subset \overline{R(S)} = R[S]$

$\Leftarrow$)

$R(S) \subset Q \Rightarrow (R(S))^\perp \supset Q^\perp \Rightarrow \overline{R(S)} \subset \overline{Q}$

Since Q is testable we have that $\overline{Q} = Q$ and therefore $R[S] \subset Q$. ■

Prop. 4.3.10:

Let R, Z be two quantum actions, $s, t \in \Sigma$ two states, and $S \subset \Sigma$. Then

1. $R(s) \perp t \Leftrightarrow s \perp R^\dagger(t)$

2. $(R \cdot Z)^\dagger = Z^\dagger \cdot R^\dagger$

3. $(R \cup Z)^\dagger = R^\dagger \sqcup Z^\dagger$

4. $R[S] = ([R^\dagger]S^\perp)^\perp$

Where we define the relation $R \sqcup Z$ as

$$s \; R \sqcup Z \; t \quad \text{iff} \quad t \in R(s) \sqcup Z(s) \tag{4.21}$$

***Proof*:**

It will be shown later in this subsection that given $R \in \mathcal{Q}$ and $T \in \mathcal{L}$ that $[R]T \in \mathcal{L}$, *i.e.*,

$$[R]T = \overline{[R]T} \quad (*) \tag{4.22}$$

1. $R(s) \perp t \;\Leftrightarrow\; s \perp R^\dagger(t)$

$R(s) \perp t \Leftrightarrow R(s) \subset t^\perp \Leftrightarrow \{s\} \subset [R]t^\perp \overset{*}{=} \overline{[R]t^\perp} \Leftrightarrow s \perp ([R]t^\perp)^\perp = R^\dagger(t)$

2. $(R \cdot Z)^\dagger = Z^\dagger \cdot R^\dagger$

$(R{\cdot}Z)^\dagger(s) = ([R{\cdot}Z]s^\perp)^\perp = ([R][Z]s^\perp)^\perp \overset{*}{=} ([R]([Z]s^\perp)^{\perp\perp})^\perp = ([R](Z^\dagger(s))^\perp)^\perp = R^\dagger(Z^\dagger(s)) = (Z^\dagger{\cdot}R^\dagger)(s)$

3. $(R \cup Z)^\dagger = R^\dagger \sqcup Z^\dagger$

$(R \cup Z)^\dagger(s) = ([R \cup Z]s^\perp)^\perp = ([R]s^\perp \cap [Z]s^\perp)^\perp = [R]s^\perp \sqcup [Z]s^\perp = R^\dagger(s) \sqcup Z^\dagger(s)$

4. $R[S] = ([R^\dagger]S^\perp)^\perp$

$\subset)$

Lets start by seeing that given a action Z and $s \in S$ we have $([Z]s^\perp)^\perp \subset ([Z]S^\perp)^\perp$:

$\{s\} \subset S \Rightarrow s^\perp \supset S^\perp \Rightarrow [Z]s^\perp \supset [Z]S^\perp \Rightarrow ([Z]s^\perp)^\perp \subset ([Z]S^\perp)^\perp$

Now we have:

$R(S) = \cup_{s \in S}\{R(s)\} = \cup_{s \in S}([R^\dagger]s^\perp)^\perp \subset ([R^\dagger]S^\perp)^\perp$

Thus we get $R[S] = \overline{R(S)} \subset \overline{([R^\dagger]S^\perp)^\perp}$. Since the orthogonal complement of a set is always testable we get $R[S] \subset \overline{([R^\dagger]S^\perp)^\perp} = ([R^\dagger]S^\perp)^\perp$

$\supset)$

First, we notice that $R(S)^\perp \subset [R^\dagger]S^\perp \;\Rightarrow\; R[S] \supset ([R^\dagger]S^\perp)^\perp$, so we will prove that $(R(S))^\perp \subset [R^\dagger]S^\perp$.

We have that $R(S)^\perp \subset [R^\dagger]S^\perp \;\Leftrightarrow\; R^\dagger(R(S)^\perp) \subset S^\perp$

The only thing left is to show that given $w \in R(S)^\perp$ we have $R^\dagger(w) \subset S^\perp$.

$$w \in R(S)^\perp$$

iff

$$w \perp R(S)$$

iff

$$\forall_{s \in S} \; w \perp R(s)$$

iff

$$\forall_{s\in S}\ R^\dagger(w) \perp s$$

iff

$$R^\dagger(w) \perp S$$

iff

$$R^\dagger(w) \subset S^\perp$$

■

In this proof we used a result not proven yet, so we are left to show that indeed $[R]T \in \mathcal{L}$ for any quantum relation R and testable property T. For that, we need the following two results.

Prop. 4.3.11:

Let $S \subset \Sigma$ and $P \in \mathcal{L}$. Then

$$P?(\overline{S}) \subset \overline{P?(S)} \tag{4.23}$$

***Proof*:**

Let $x \in \overline{S}$, that is, $x \perp S^\perp$, which is equivalent to

$$\forall_{t\in S^\perp}\ x \perp t \quad (\dagger) \tag{4.24}$$

We want to show that $P?(x) \in \overline{P?(S)}$ that is

$$\forall_{y\in (P?(S))^\perp}\ P?(x) \perp y \tag{4.25}$$

Let $y \in (P?(S))^\perp$, that is, $y \perp P?(s)$ for all $s \in S$ (note that if it is not defined $P?(s) = \varnothing$).
Using self-adjointness we get for all $s \in S$ $P?(y) \perp s$, *i.e.*, $P?(y) \in S^\perp$.

From $(\dagger)$ we immediately get that $x \perp P?(y)$ and, applying self-adjointness, it is equivalent to

$$P?(x) \perp y \tag{4.26}$$

Therefore we conclude that $P?(x) \in \overline{P?(S)}$ ■

Prop. 4.3.12:

Let $S \subset \Sigma$ and $U \in \mathcal{U}$. Then $U(S^\perp) = U(S)^\perp$. Moreover $U(\overline{S}) = \overline{U(S)}$

***Proof*:**

$\subset$)

Let $t \in S^\perp$, that is $t \perp S$. Then

$$U(t) \in U(S)^\perp$$

iff

$$\forall_{s\in S}\ U(t) \perp U(s)$$

iff

$$\forall_{s\in S}\ t \perp U^\dagger(U(s)) = U^{-1}(U(s)) = s$$

iff

$$t \perp S$$

iff

True

$\supset$)

Let $w \in U(S)^\perp$, *i.e.*

$$\forall_{s \in S}\ w \perp U(s)$$
iff
$$\forall_{s \in S}\ U^\dagger(w) = U^{-1}(w) \perp s$$
iff
$$U^{-1}(w) \in S^\perp$$

Let $t := U^{-1}(w)$. Then $t \in S^\perp$ and $w = U(t)$, thus $w \in U(S^\perp)$.

The second part of the Proposition then follows easily:
$U(\overline{S}) = U((S^\perp)^\perp) = U(S^\perp)^\perp = (U(S)^\perp)^\perp = \overline{U(S)}$. ■

Finally we have the everything needed to show that the weakest precondition of a testable property is testable. We will show it first for the base cases of tests $P?$ and unitary programs U, and then we will show for a general quantum action using the fact that a every quantum action can be written as a choice of deterministic action, which are composition of tests and unitary actions.

Corollary 4.3.13:

Let $S \subset \Sigma$, $T \in \mathcal{L}$, and $U \in \mathcal{U}$ (and $S? := \overline{S}?$ if S is not testable).Then

$[S?]T \in \mathcal{L}$*, that is, it is testable.*

$[U]T \in \mathcal{L}$.

***Proof*:**

Let π be either $P?$ or U. We need to prove that $\overline{[\pi]T} \subset [\pi]T$.

First we notice that given a relation R and sets S, T we have:

$$R(S) \subset T \quad \Leftrightarrow \quad S \subset [R]T \tag{4.27}$$

In particular, by switching the sides, we have that

$$\overline{[\pi]T} \subset [\pi]T \quad \Leftrightarrow \quad \pi(\overline{[\pi]T}) \subset T \tag{4.28}$$

From the two above propositions, since π is either $P?$ or U we have that $\pi(\overline{[\pi]T}) \subset \overline{\pi([\pi]T)}$.

It is easy to see that $\pi([\pi]T) = T$, therefore $\overline{\pi([\pi]T)} = \overline{T}$.

Since $T \in \mathcal{L}$ we have that $\overline{T} = T$, thus $\pi(\overline{[\pi]T}) \subset T$, and we conclude that $\overline{[\pi]T} \subset [\pi]T$. ■

Corollary 4.3.14:

Let $R \in \mathcal{Q}$ be a quantum action and $T \in \mathcal{L}$ a testable property. Then $[R]T \in \mathcal{L}$.

***Proof*:**

We notice that every quantum action is either deterministic or a union of deterministic actions, and that every deterministic action is a composition of tests and unitary actions.

Let $\pi \in \mathcal{D}$, that is $\pi = \alpha_1 \cdot \ldots \cdot \alpha_n$, with α_i either $P?$ or U.
We know that given two relations R and Z on Σ and a set $S \subset \Sigma$ that $[R \cdot Z]S = [R][Z]S$. Thus

$$[\pi]T = [\alpha_1] \cdots [\alpha_n]T \tag{4.29}$$

Since α_n is either $P?$ or U and $T \in \mathcal{L}$ then $[\alpha_n]T \in \mathcal{L}$. Again, α_{n-1} is either $P?$ or U, and $[\alpha_n]T \in \mathcal{L}$, therefore $[\alpha_{n-1}][\alpha_n]T \in \mathcal{L}$.
Proceeding with this, we get that $[\pi]T = [\alpha_1] \cdots [\alpha_n]T \in \mathcal{L}$.

Let $R = \bigcup_i \pi_i$ with $\pi_i \in \mathcal{D}$.
We know that $[\bigcup_i \pi_i]\, T = \bigcap_i [\pi_i]T$.
Since every $[\pi_i]T \in \mathcal{L}$, using the fact that $\mathcal{L}$ is closed for intersections we conclude that
$[R]T = \bigcap_i [\pi_i]T \in \mathcal{L}$. ■

Chapter 5

Logic of Quantum Programs

On last section we saw that quantum dynamic frames are a structure that capture the properties of orthomodular lattices based on Hilbert spaces. Furthermore its structure also allows for the use of unitary actions and, moreover, of quantum programs.
The goal was to have a logic that could express quantum propositions like PQL, that would support time evolutions, *i.e.* unitary operators, and that would not contradict propositional logic.
This section will introduce such a logic, the *Logic of Quantum Programs* (LQP), starting with its *syntax* (Subsection 5.1.1), that is based on PDL, and its *semantics* (Subsection 5.1.2), that it is based on QDF. After we take a look at what *new properties* (Section 5.2) of this logic. We proceed with presenting *axioms and rules* (Section 5.3) for LQP and end the Chapter with a summary of *the differences* between PDL and LQP.

5.1 Syntax and Semantics of LQP

An interesting observation one can make is that the dynamic frame orthocomplement in QDF corresponds to the orthogonal complement on a Hilbert space, and in a frame based on PDL it is the set complement. In the former case it gives the quantum negation of PQL and in the latter, the usual negation of PDL.
However, it is possible to use set complement in quantum dynamic frames as it is defined for any set and does not depend on the structure that those sets have. This will allow for LQP to have both types of negation, thus we can express both classical and quantum propositions and LQP will have the traditional rules of PQL without giving up on all basic properties that we are accustomed from classical logic, while being able have programs like PDL.

5.1.1 Syntax

As in PDL, we have a set P of *propositional variables* and a set Π of *basic programs*. The sets of *well-formed formulas*, L_P, and *well-formed programs*, L_Π, are given by:

$$\begin{aligned} \varphi &::= p \mid \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\pi]\varphi \\ \pi &::= U \mid \pi^\dagger \mid \pi \cdot \pi \mid \pi \cup \pi \mid \varphi? \end{aligned} \tag{5.1}$$

where $p \in P$ and $U \in \Pi$.
The usual logical operators are defined in the regular way: $\bot := \neg\top$, $\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi)$,

$\varphi \Rightarrow \psi := \neg\varphi \vee \psi$, $\varphi \Leftrightarrow \psi := (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$, and $\langle\pi\rangle\varphi := \neg[\pi]\neg\varphi$.

Note that there are two differences in the syntax of programs in relation with PDL: LQP does not have iteration and has the adjoint.
Iteration is not included because there are no *while* cycles used in quantum computation (since quantum operator consist only of tests and unitary operators), and the adjoint operator is needed because it is used in Quantum Mechanics.

5.1.2 Semantics

A LQP-model is a tuple $\mathcal{M} = (\Sigma(\mathcal{H}), V)$ where $\Sigma(\mathcal{H})$ is a concrete quantum frame of a Hilbert space $\mathcal{H}$ and V a valuation mapping a propositional variable to a set of states $V(p) \subset \Sigma$ and basic actions to relations $V(U) \in \mathcal{U}$.
The interpretation $\|\cdot\|^{\mathcal{M}}$ of formulas and programs in a model $\mathcal{M}$ is given (and we will again drop the superscript) in the following way:
Def. 5.1.1 (Interpretation of Programs):

$$\begin{aligned} \|U\| &:= V(U) & \left\|\pi^\dagger\right\| &:= \|\pi\|^\dagger \\ \|\pi_1 \cup \pi_2\| &:= \|\pi_1\| \cup \|\pi_2\| & \|\pi_1 \cdot \pi_2\| &:= \|\pi_1\| \cdot \|\pi_2\| \\ \|\varphi?\| &:= \|\varphi\|? \end{aligned} \tag{5.2}$$

Def. 5.1.2 (Interpretation of Formulas):

$$\begin{aligned} \|p\| &:= V(p) & \|\top\| &:= \Sigma \\ \|\neg\varphi\| &:= \Sigma \backslash \|\varphi\| & \|\varphi \wedge \psi\| &:= \|\varphi\| \cap \|\psi\| \\ \|[\pi]\varphi\| &:= [\|\pi\|]\,\|\varphi\| \end{aligned} \tag{5.3}$$

The definitions of satisfiability and validity will be exaclty the same as in PDL:
Def. 5.1.3 (Satisfiability and Validity):
Given a model $\mathcal{M}$ and φ a formula, we say that:

- state $s \in \Sigma$ *satisfies* φ in $\mathcal{M}$, written $\mathcal{M}, s \vDash \varphi$ if $s \in \|\varphi\|$.
- φ is *valid* in $\mathcal{M}$, written $\vDash_\Sigma \varphi$ if $\mathcal{M}, s \vDash_\Sigma \varphi$ for all $s \in \Sigma$, *i.e.*, $\|\varphi\| = \Sigma$.
- φ is *valid*, written $\vDash \varphi$ if $\mathcal{M} \vDash \varphi$ for all models $\mathcal{M}$.

Let $\Gamma \subset L_P$ be a set of propositions. We say that:

- $\mathcal{M} \vDash \Gamma$ if $\mathcal{M} \vDash \psi$ for all $\psi \in \Gamma$.
- φ is a *logical consequence* of Γ, written $\Gamma \vDash \varphi$ if $\mathcal{M} \vDash \varphi$ whenever $\mathcal{M} \vDash \Gamma$.

5.2 What is New?

So far, with a few exceptions, the kind of formulas is the same as in PDL, so a pertinent question is how quantum fits into this?

The first difference, already stated, is LQP formulas do not use iteration and may use the adjoint operator, which will mean that the axioms of LQP do not include the iteration axioms of PDL and have some new axioms for the adjoint operator.
The second difference, although very similar, is in the interpretation of basic programs, U. In PDL the valuation of a basic program is a general relation in Σ, but in LQP will be relations that correspond to a unitary operator in the Hilbert space.
Another difference is on the tests $S?$. In PDL $S?$ is the identity in S and in QDF it is the projection onto $\overline{S}$. This difference is made clear in the fact that the PDL axiom $[\varphi?]\psi \Leftrightarrow \varphi \Rightarrow \psi$ is not valid in LQP.

Prop. 5.2.1:
Let $\mathcal{M}$ be a LQP-model. Then it is not necessarily true that

$$\mathcal{M} \vDash [\varphi?]\psi \Leftrightarrow \varphi \Rightarrow \psi \tag{5.4}$$

***Proof*:**
Let p be a propositional variable, $\mathcal{M}$ a LQP-model, and $P := V(p)$.
Lets consider φ to be p and ψ to be $[p?]\bot$, we get the formula

$$[p?]([p?]\bot) \Leftrightarrow p \Rightarrow [p?]\bot \tag{5.5}$$

Then $\mathcal{M} \vDash [p?][p?]\bot \Leftrightarrow p \Rightarrow [p?]\bot$ if and only if

$$\|[p?][p?]\bot\| = \|p \Rightarrow [p?]\bot\| \tag{5.6}$$

Using Proposition 4.2.8, we know that $\|[p?]\bot\| = [P?]\varnothing = P^{\bot}$. We have then:
$\|p \Rightarrow [p?]\bot\| = \Sigma\backslash P \cup P^{\bot} = \Sigma\backslash P$ (if $w \in P^{\bot}$ them $w \notin P$)
$\|[p?][p?]\bot\| = [P?]P^{\bot} = [P?]\varnothing = P^{\bot}$ (if $P?(w)\downarrow$ then $P?(w) \in \overline{P}$ thus $P?(w) \notin P^{\bot}$)
Thus $\|[p] \sim p\| \neq \|p \Rightarrow \sim p\|$ ■

The fact that tests correspond to orthogonal projections in a a Hilbert space leads to $[S?]\varnothing = S^{\bot}$, as seen in Proposition 4.2.8. Therefore the quantum negation of PQL can be defined by

$$\sim \varphi := [\varphi?]\bot \tag{5.7}$$

Thus the formula $\sim \varphi$ intuitively means the impossibility of performing test $\varphi?$, that is, test $\varphi?$ fails.

Prop. 5.2.2:
Let $\varphi \in L_P$ and $\mathcal{M}$ be a model. Then $\|\sim \varphi\| = \|\varphi\|^{\bot}$. Moreover $\|\sim \varphi\| \in \mathcal{L}$.

***Proof*:**
$\|\sim \varphi\| = \|[\varphi?]\bot\| = [\|\varphi\|?]\,\|\bot\| = [\|\varphi\|?]\varnothing = \|\varphi\|^{\bot}$ ■

With quantum negation, it is possible to express the quantum disjunction as defined in PQL

$$\varphi \sqcup \psi := \sim (\sim \varphi \wedge \sim \psi) \tag{5.8}$$

expressing superposition of φ and ψ.

Prop. 5.2.3:

Let $\varphi \in L_P$ and $(\Sigma(\mathcal{H}), V)$ be a model. Then $\|\varphi \sqcup \psi\| = \|\varphi\| \sqcup \|\psi\|$. Moreover $\|\varphi \sqcup \psi\| \in \mathcal{L}$.

We can also define the $\Diamond$ and $\Box$ modalities, with $\Diamond\varphi$ meaning that after some measurement it is possible to reach a state satisfying φ, and $\Box\varphi$ that after any measurement we will reach a state satisfying φ.
The diamond modality is defined by

$$\Diamond\varphi := \langle\varphi?\rangle\top \tag{5.9}$$

and the box modality is given by its dual

$$\Box\varphi := \neg\Diamond\neg\varphi \tag{5.10}$$

Def. 5.2.4:

Let $\Sigma(\mathcal{H})$ be a quantum frame, and $S \subset \Sigma$. Then the sets $\Box S$ and $\Diamond S$ are given by:
$\Box S := \{w \in \Sigma \colon \forall_{t\in\Sigma}\,(w \to t \Rightarrow t \in S)\}$.
$\Diamond S := \Sigma\backslash\Box(\Sigma\backslash S) = \{w \in \Sigma \colon \exists_{t\in\Sigma}\,(w \to t \ \wedge\ t \in S)\}$

The definition of box and diamond of a set of states is what the desired meaning of the respective modalities is, as the next result shows.

Prop. 5.2.5:

Let $S \subset \Sigma$, then $[S?]\varnothing = \Sigma\backslash\Diamond S = \Box(\Sigma\backslash S)$.

***Proof*:**

$\Sigma\backslash\Diamond S = \Sigma\backslash(\Sigma\backslash\Box(\Sigma\backslash S)) = \Box(\Sigma\backslash S) = \{w \in \Sigma \colon \forall_{t\in\Sigma}\,(w \to t \Rightarrow t \in \Sigma\backslash S)\} = \{w \in \Sigma \colon \forall_{t\in\Sigma}\,(w \not\perp t \Rightarrow t \notin S)\}$

$\subset$) Clearly $S^\perp \subset \Sigma\backslash\Diamond S$

$\supset$) Let $s \in S$, if $w \in \Sigma\backslash\Diamond S$ then $w \perp s \vee s \notin S$, therefore $w \perp s$ and $w \in S^\perp$ ■

Corollary 5.2.6:

Let $\varphi \in L_P$ and $(\Sigma(\mathcal{H}), V)$ be a model. Then
$\|\Diamond\varphi\| = \Diamond\|\varphi\|$
$\|\Box\varphi\| = \Box\|\varphi\|$
Moreover, $\|\Box\varphi\| \in \mathcal{L}$.

***Proof*:**

$\|\Diamond\varphi\| = \|\langle\varphi?\rangle\top\| = \langle\|\varphi\|?\rangle\Sigma = \Sigma\backslash[\|\varphi\|?](\Sigma\backslash\Sigma) = \Sigma\backslash[\|\varphi\|?]\varnothing = \Sigma\backslash(\Sigma\backslash\Diamond\|\varphi\|) = \Diamond\|\varphi\|$
$\|\Box\varphi\| = \|\neg\Diamond\neg\varphi\| = \Sigma\backslash(\Diamond\Sigma\backslash\|\varphi\|) = \Box\|\varphi\|$
$= [(\Sigma\backslash\|\varphi\|)?]\varnothing = (\Sigma\backslash\|\varphi\|)^\perp \in \mathcal{L}$ ■

We saw that given any set $S \subset \Sigma$ that $S^\perp$ is always testable, and since $\Box S = (\Sigma\backslash S)^\perp$, $\Box S$ is also always testable. This leads to the following result about the testable properties:

Prop. 5.2.7:

Let $S \subset \Sigma$. The following are equivalent:

$S = \overline{S}$ *(i.e. $S \in \mathcal{L}$)* $\Leftrightarrow \exists_{T \subset \Sigma} S = T^{\perp} \Leftrightarrow \exists_{T \subset \Sigma} S = \Box T$

Another formula of interest is the double box of a formula, $\Box\Box\varphi$, which the next results explains why it is called UNIVERSAL MODALITY.

Prop. 5.2.8 (Universal Modality):

Let $S \subset \Sigma$. Then $\Box\Box S \neq \varnothing \Leftrightarrow S = \Sigma$

***Proof*:**

$\Box\Box S = \{w \in \Sigma \colon \forall_{t \in \Sigma} (w \to t \Rightarrow t \in \Box S)\} =$

$= \{w \in \Sigma \colon \forall_{t \in \Sigma} (w \to t \Rightarrow \forall_{s \in \Sigma} (t \to s \Rightarrow s \in S))\}$

$\Leftarrow)$

If $S = \Sigma$ then $s \in S$ is true and therefore the inner implication is true, and the outer implication is also true, thus $\Box\Box S = \Sigma \neq \varnothing$.

$\Rightarrow)$

If $\Box\Box S \neq \varnothing$ let $w \in \Box\Box S$. Also, let $s \in \Sigma$.

By proper superposition (axiom of QDF) $\exists_{t \in \Sigma} w \to t \to s$, furthermore, since $w \in \Box\Box S$, $w \to t$ and $t \to s$ we must have $s \in S$. Since s is an arbitrary state of Σ then $S = \Sigma$.

We should note that since $S = \Sigma \;\Rightarrow\; \Box\Box S = \Sigma$, we also have that $\Box\Box S \neq \varnothing \;\Leftrightarrow\; \Box\Box S = \Sigma$. ■

The importance of the universal modality is that if a state satisfies $\Box\Box\varphi$ then all states satisfy property φ, hence it is called *universal modality*.

Corollary 5.2.9:

Let $\mathcal{M}$ be a model and $s \in \Sigma$ a state. Then

$$\mathcal{M}, s \vDash \Box\Box\varphi \quad \Leftrightarrow \quad \mathcal{M} \vDash \varphi \tag{5.11}$$

With the universal modality we can define being *logically weaker*

$$\varphi \leqslant \psi := \Box\Box(\varphi \Rightarrow \psi) \tag{5.12}$$

and logically equivalent

$$\varphi = \psi := \Box\Box(\varphi \Leftrightarrow \psi) \tag{5.13}$$

The $\leqslant$ will correspond to the order relation in the lattice, and in this case, the order relation is the inclusion, as the next results show.

Prop. 5.2.10:

Let Let $\mathcal{M}$ be a model. Then

$$\mathcal{M} \vDash \varphi \Rightarrow \psi \quad \text{iff} \quad \|\varphi\| \subset \|\psi\| \tag{5.14}$$

Moreover, we have

$$\mathcal{M} \vDash \varphi \Leftrightarrow \psi \quad \text{iff} \quad \|\varphi\| = \|\psi\| \tag{5.15}$$

Therefore, if we use the universal modality, from being satisfied by one state we can infer a more general information about the interpretation:

Corollary 5.2.11:

Let $\mathcal{M}$ be a model and $s \in \Sigma$ a state. Then

$$\mathcal{M}, s \vDash \varphi \leqslant \psi \quad \text{iff} \quad \|\varphi\| \subset \|\psi\| \tag{5.16}$$

$$\mathcal{M}, s \vDash \varphi = \psi \quad \text{iff} \quad \|\varphi\| = \|\psi\| \tag{5.17}$$

We can see that the logical operator $\leqslant$ captures the order relation of the orthomodular lattice, and with $\leqslant$ (inclusion) and $\sim$ (complement), it is possible to capture the orthogonality relation:

$$\varphi \perp \psi := \varphi \leqslant \sim \psi \tag{5.18}$$

Prop. 5.2.12:

Let $\mathcal{M}$ be a model and $s \in \Sigma$ a state. Then

$$\mathcal{M}, s \vDash \varphi \perp \psi \quad \text{iff} \quad \|\varphi\| \perp \|\psi\| \tag{5.19}$$

***Proof*:**

$\mathcal{M}, s \vDash \varphi \perp \psi$ iff $\mathcal{M}, s \vDash \varphi \leqslant \sim \psi$ iff $\|\varphi\| \subset \|\psi\|^{\perp}$ iff $\forall_{s \in \|\varphi\|}\, s \perp \|\psi\|$ iff $\|\varphi\| \perp \|\psi\|$ ■

From last Proposition it immediately follows that the logical operator $\perp$ is symmetric, as it is shown in the next Corollary.

Corollary 5.2.13:

Let $\mathcal{M}$ be a model and $s \in \Sigma$ a state. Then

$$\mathcal{M}, s \vDash \varphi \perp \psi \quad \text{iff} \quad \mathcal{M}, s \vDash \psi \perp \varphi \tag{5.20}$$

***Proof*:**

$\mathcal{M}, s \vDash \varphi \perp \psi$ iff $\|\varphi\| \perp \|\psi\|$

Since the orthogonality relation $\perp$ of the frame is symmetric we immediately get

$\|\varphi\| \perp \|\psi\|$ iff $\|\psi\| \perp \|\varphi\|$ iff $\mathcal{M}, s \vDash \psi \perp \varphi$ ■

After the orthogonal relation, another property from the quantum dynamic frame we can capture is the one of testable property

$$T(\varphi) := \sim\sim \varphi \leqslant \varphi \tag{5.21}$$

Prop. 5.2.14:

Let $\mathcal{M}$ be a model and $s \in \Sigma$ a state. Then

$$\mathcal{M}, s \vDash T(\varphi) \quad \text{iff} \quad \|\varphi\| \in \mathcal{L} \tag{5.22}$$

***Proof*:**

$\mathcal{M}, s \vDash T(\varphi)$ iff $(\|\varphi\|^{\perp})^{\perp} \subset \|\varphi\|$ iff $\overline{\|\varphi\|} \subset \|\varphi\|$ iff $\|\varphi\|$ is biorthogonaly closed iff $\|\varphi\| \in \mathcal{L}$ ■

We can also express the strongest post-condition easily by looking at $4.$ of Proposition 4.3.10:

$$\pi[\varphi] :=\sim [\pi^{\dagger}] \sim \varphi \tag{5.23}$$

The next results follows from Proposition 4.3.10

Prop. 5.2.15:

Let $\mathcal{M}$ be a model, then

$$\|\pi[\varphi]\| = \|\pi\| [\|\varphi\|] \tag{5.24}$$

5.3 Axioms and Rules of LQP

We already know the syntax and semantics of LQP, so we are ready to define the deductive system. As LQP is based on PDL, it is clear that we must have the axioms and rules of PDL, except the ones concerning tests $?$ (axiom A8. of PDL) and Kleene star $*$ (axioms A9. and A10. of PDL):

A1. $\varphi \Rightarrow (\psi \Rightarrow \varphi)$

A2. $(\varphi \Rightarrow (\psi \Rightarrow \phi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \phi))$

A3. $(\neg\varphi \Rightarrow \neg\psi) \Rightarrow (\psi \Rightarrow \varphi)$

A4. $[\alpha](\varphi \Rightarrow \psi) \Rightarrow ([\alpha]\varphi \Rightarrow [\alpha]\psi)$

A5. $[\alpha](\varphi \wedge \psi) \Leftrightarrow [\alpha]\varphi \wedge [\alpha]\psi$

A6. $[\alpha \cup \beta]\varphi \Leftrightarrow [\alpha]\varphi \wedge [\beta]\varphi$

A7. $[\alpha \cdot \beta]\varphi \Leftrightarrow [\alpha][\beta]\varphi$

MP. $\dfrac{\varphi, \quad \varphi \Rightarrow \psi}{\psi}$

Gen. $\dfrac{\varphi}{[\alpha]\varphi}$

To these axioms and rules, the following are added:

A8. $\Box\varphi \Rightarrow [\psi?]\varphi$ (Testability)

A9. $\neg[\varphi?]\psi \Rightarrow [\varphi?]\neg\psi$ (Partial Functionality)

A10. $\varphi \wedge \psi \Rightarrow \langle\varphi?\rangle\psi$ (Adequacy)

A11. $T(\varphi) \Rightarrow [\varphi?]\varphi$ (Repeatability)

A12. $\langle\pi\rangle\Box\Box\varphi \Rightarrow [\pi]\varphi$ (Proper Superpositions)

A13. $\neg[U]\varphi \Leftrightarrow [U]\neg\varphi$ (Unitary Functionality)

A14. $\varphi \Leftrightarrow [U \cdot U^{\dagger}]\varphi$ (Unitary Bijectivity 1)

A15. $\varphi \Leftrightarrow [U^\dagger \cdot U]\varphi$ (Unitary Bijectivity 2)

A16. $\varphi \Rightarrow [\pi]\Box\langle\pi^\dagger\rangle\Diamond\varphi$ (Adjointness)

Test Gen. $\dfrac{\varphi \Rightarrow [p?]\psi}{\varphi \Rightarrow \Box\psi}$ provided p does not occur in φ or ψ.

Theorem 5.3.1 (Soundness and Completeness):

The deductive system is (weakly) sound with respect to semantics. Moreover, Quantum Dynamic Frames are a (weakly) complete proof system that includes the axioms of LQP[1] *.*

As an example, lets prove the soundness of A16.

Prop. 5.3.2:

Axiom A16. is sound. That is $\vDash \varphi \Rightarrow [\pi]\Box\langle\pi^\dagger\rangle\Diamond\varphi$

***Proof*:**

First we notice that given a model $\mathcal{M}$

$$\mathcal{M} \vDash \varphi \Rightarrow \psi \quad \text{iff} \quad \|\varphi\| \subset \|\psi\| \tag{5.25}$$

Let $\mathcal{M}$ be a model, let $S := \|\varphi\|$, and $R := \|\pi\|$.

We need to show that

$$S \subset [R]\Box\langle R^\dagger\rangle\Diamond S \tag{5.26}$$

Let $s \in S$. Then

$s \in [R]\Box\langle R^\dagger\rangle\Diamond S$

iff $R(s) \subset \Box\langle R^\dagger\rangle\Diamond S$

iff $\forall_{w\in R(s)}\ \forall_{t\in\Sigma}(w \to t \Rightarrow t \in \langle R^\dagger\rangle\Diamond S)$

iff $\forall_{w\in R(s)}\ \forall_{t\in\Sigma}(w \to t \Rightarrow \exists_{v\in R^\dagger(t)}\ v \in \Diamond S)$

iff $\forall_{w\in R(s)}\ \forall_{t\in\Sigma}(w \to t \Rightarrow \exists_{v\in R^\dagger(t)}\ \exists_{z\in S}\ v \to z)$

Looking at item 1. of Proposition 4.3.10, given a quantum action R and two states s, t we have

$$R(s) \perp t \quad \text{iff} \quad s \perp R^\dagger(t) \tag{5.27}$$

That is

$$\forall_{w\in R(s)}\ w \perp t \quad \text{iff} \quad \forall_{v\in R^\dagger(t)} v \perp s \tag{5.28}$$

Taking the negation on both sides we get

$$\exists_{w\in R(s)}\ w \to t \quad \text{iff} \quad \exists_{v\in R^\dagger(t)} v \to s \tag{5.29}$$

We have two cases:

If $s \notin \mathrm{dom}R$ then we have that $s \in [R]A$ for any $A \subset \Sigma$, in particular $s \in [R]\Box\langle R^\dagger\rangle\Diamond S$.

If $s \in \mathrm{dom}R$

Let $w \in R(s)$ and let $t \in \Sigma$ be such that $w \to t$.

[1] QDF includes two more axioms that are of technical nature: Covering Law and Mayet's Condition.

By the above result, we have that $\exists_{v \in R^\dagger(t)}\ v \to s$.
Since $s \in S$ we have that $s \to s$, so choosing $z := s$ we have that

$$w \to t \Rightarrow \exists_{v \in R^\dagger(t)}\ \exists_{z \in S}\ v \to z \tag{5.30}$$

Thus $s \in [R]\Box\langle R^\dagger\rangle\Diamond S$ ■

5.4 Comparison of LQP with PQL and PDL

Logic of Quantum Programs combines the properties of Hilbert spaces used in Propositional Quamtum Logic with the capacity of reasoning about programs of Propositional Dynamic Logic.

Hence LQP acomodates the *negations* of both logics, the usual negation $\neg$ of PDL and the orthogonal complement $\sim$ of PQL, with leads to two disjunction operators, the classical $\vee$ and the quantum $\sqcup$. Each of these operators carries the same *meaning* as in the original logic, so we can recover Propositional Logic from LQP (note also that the three first axioms of LQP and the MP. rule are from propositional logic) which was not possible in PQL.

Another objective for this logic was to be able to handle unitary operators, called quantum programs or quantum actions, which is possible by the use of Quantum Dynamic Frames and the concepts from PDL.
Logic of Quantum programs has two disjunctions $\wedge$ and $\sqcup$ and two negations $\neg$ and $\sim$, from the definitions, one can see that they correspond to the classical ($\wedge$ and $\neg$) ones used in Propositional Dynamic Logic and the quantum ($\sqcup$ and $\sim$) ones used in Propositional Quantum Logic, Quantum Dynamic Frames, and Quantum Actions.

Thanks to this, any valid formula in PQL is valid in LQP and any valid formula in PDL is valid in LQP provided that it does not use tests ot iteration. Also, noticing that LQP has axioms from PDL, any derivation in PDL that does not use the axioms for tests or iteration is also a derivation in LQP.

Chapter 6

Quantum Dynamic Algebra

This section will describe an alternative quantum structure (see [1]), the *Quantum Dynamic Algebra* (Section 6.1), which is a algebraic semantics for quantum actions. Then we will see that a Quantum Dynamic Frame can be made into a quantum dynamic algebra (Section 6.2), and we shall see that every quantum dynamic algebra is isomorphic to one made from a concrete quantum dynamic frame.

6.1 Definition

Def. 6.1.1 (Quantum Dynamic Algebra):
A QUANTUM DYNAMIC ALGEBRA is a tuple $(\mathcal{Q}, \cup, \cdot, \sim)$ satifying the axioms on definition 6.1.3, where the elements of $\mathcal{Q}$ are called QUANTUM ACTIONS or QUANTUM PROGRAMS and are denoted by variables $x, y, \ldots$, and the operations on quantum actions are: *union* or *choice* $\cup : \mathcal{Q} \times \mathcal{Q} \to \mathcal{Q}$, (*sequential*) *composition* $\cdot : \mathcal{Q} \times \mathcal{Q} \to \mathcal{Q}$, and *test for failure* $\sim : \mathcal{Q} \to \mathcal{Q}$.

We need some auxiliary notions:

Def. 6.1.2:

- $\mathcal{L} := \{\sim x : x \in \mathcal{Q}\}$ is the set of tests, and the variables $p, q, \ldots$ will be used to abbreviate then.
- $0 := \cup\varnothing$ is the action that is undefined for all input.
- $1 :=\sim 0$ represents the failure of action 0, that is, 1 is the action that always succeeds.
- $[x]p :=\sim (x \cdot \sim p)$, $[x]p$ is true if x cannot be applied or, if it can, we reach a state satisfying p, which is the definition of the weakest precondition.
- $\bigwedge_i p_i :=\sim \bigcup_i \sim p_i$, $\bigwedge_i p_i$ is true if none of the failures tests $\sim p_i$ can be executed.
- $p \leqslant q$ iff $p \wedge q = p$, that is p is logicaly weaker that q.
- $p \perp q$ iff $p \leqslant \sim q$
- $\bigvee_i p_i :=\sim\sim \bigcup_i p_i$ corresponds to the biorthogonal closure, that is, the superposition of the p_i
- $\mathsf{At}(\mathcal{L}) := \{p \in \mathcal{L} : \forall_{q \in \mathcal{L}} (0 \neq q \leqslant p \Rightarrow q = p)\}$ are the *atoms* of $\mathcal{L}$.
- $\mathcal{U} := \{x \in \mathcal{Q} : \exists_y x \cdot y = y \cdot x = 1 \text{ and } \forall_{p \in \mathcal{L}} x \cdot \sim p =\sim (x \cdot p)\}$ is the set of *unitary evolutions*.

- $\mathcal{D} := \{x \in \mathcal{Q} \colon \forall_{a \in \mathrm{At}(\mathcal{L})} \exists_{b \in \mathrm{At}(\mathcal{L})}\, a \leqslant [x]b\}$
- The *image-set of* p *via* x is defined by:
  $x(p) := \{b \in \mathrm{At}(\mathcal{L}) \colon \exists_{a \in \mathrm{At}(\mathcal{L})} \exists_{y \in \mathcal{D}}\, a \leqslant p, y \leqslant x, a \leqslant [y]b, a \not\leqslant \sim y\}$
- $x[p] := \bigvee x(p)$

In order to have a better understanding, it is useful to compare this definitions with the ones already discussed in Section 4. First we note that on quantum dynamic frames we have both sets of states in Σ and quantum actions, however, here we only have actions.

Knowing that given a set $S \in \mathcal{L}$ we can easily identify S with the test $S?$ since there is a bijection between closed linear subsets and orthogonal projections, so we can drop the $?$.
Second, noticing that for $S \subset \Sigma$ we have $S^{\perp} = [S?]\varnothing$, $\sim$ has the meaning of *test for failure* if given a quantum action R we use $\sim R$ as $([R]\varnothing)?$.

With this in mind, the above definitions became the usual ones already used before, $\mathcal{L}$ are the testable properties, 0 is **fail**, 1 is **skip**, $[x]p$ is the weakest precondition, $\wedge$ is set intersection, $\leq$ is inclusion, $\perp$ is the orthogonal relation, $\vee$ the quantum union, $\mathrm{At}(\mathcal{L})$ has the properties that are a single state $\{s\}$, $\mathcal{U}$ the unitary actions, $\mathcal{D}$ the deterministic actions, $x(p)$ the image of p by action x, and $x[p]$ the strongest post-condition.

Def. 6.1.3 (Axioms for Quantum Dynamic Algebra):

1. $0 \in \mathcal{L}$; (or $\sim 1 = 0$)
2. $(\mathcal{Q}, \bigcup, \cdot, 1)$ is a quantale[1] generated by the set $\mathcal{L} \cup \mathcal{U}$ of tests and unitary evolutions
3. Choice: $[\bigcup_i x_i]p = \bigwedge_i [x_i]p$ (or $\sim \bigcup_i x_i = \bigwedge_i \sim x_i$)
4. Composition: $[\pi \cdot \sigma]p = [\pi][\sigma]p$ (or $\sim (x \cdot y) = [x] \sim y$)
5. Adequacy: $p \wedge q \leqslant [q]p$ and also $p \wedge [p]q \leqslant q$
6. Proper Superposition: if $p, q \neq 0$ then $\exists_{r \in \mathcal{L}}$ such that $r \not\perp p, r \not\perp q$
7. Self-Adjointness Axiom: $\forall_{p,q \in \mathcal{L}}\, p \leqslant [q] \sim [q] \sim p$
8. Covering Law: if $q \in \mathrm{At}(\mathcal{L})$ and $p \not\perp q$, then $p \wedge (\sim p \vee q) \in \mathcal{L}$
9. Atomicity: $\mathcal{L}$ is atomistic, that is, $p \leqslant \bigvee \{q \in \mathcal{L} \colon q \leqslant p\}$
10. Mayet's Condition. $\exists_{p,q,r \in \mathcal{L}} \exists_{u \in \mathcal{U}}$ such that $\forall_{s \leqslant q \vee r} \colon p \leqslant [u]p, p \neq [u]p, q \neq 0, r \neq 0, q \perp r, s = [u]s$
11. Actions are determined by their behavior on atoms: If $\forall_{a \in \mathrm{At}(cL)}\, x(a) = y(a)$, then $x = y$
12. Image commutes with unions: $(\bigcup_{i \in I} x_i)(p) = \bigcup_{i \in I} x_i(p)$ (on the left $\cup$ is the quantale *sup* and on the right the set-theoretical union)

[1] $(\mathcal{Q}, \bigcup, \cdot, 1)$ is a quantale if $(\mathcal{Q}, \cup)$ is a complete lattice, $(\mathcal{Q}, \cdot, 1)$ is a monoid, and $\cdot$ distributes over $\cup$.

One can easily see that most of these have the same name of the ones for Quantum Dynamic Frames. Furthermore, we will show that a QDA made from a QDF satisfies this axioms, and moreover, they correspond to the ones of the same name.

Axiom 1 is a familiar property that we know QDF have, as well as axioms 3 and 4 with the rules for union and composition of actions. Axiom 2 deals with the structure of $\mathcal{Q}$ and some rules for actions, all that we are already familiar. Proper superposition can be stated exactly as the axiom of the same name in QDF noticing that $\not\perp$ is just the measurement relation, $\rightarrow$. Another axiom that is stated very similarly to its QDF counterpart is the Mayet's Condition.

The first part of Adequacy is saying that given a state s in p and q that if we test for q either q is not defined on s or we will still be in a state that satisfies p, in particular, if p is atomic and q is defined on p, then $q(p) = p$. The second part is saying that the states of p that are in q after testing for p must be states that were already satisfying q, again, in particular, if s is atomic state of p and $p(s) = q$, then $s = q$. In summary, we have the same property as in the adequacy axiom of QDF.

Axioms 7 and 8 are stated in a diferent manner that in QDF, but we will see that when we make a QDA from a QDF they will be related to their homonyms in QDF.

Axiom 9, although having the same same as an axiom in QDF, they do not refer to the same properties, this one is stating that a property p is contained in the superposition of all its states, and the atomicity axiom in QDF states that states are testable properties.

Finally, axioms 11. and 12. are more technical properties that actions and for the last one, the union operator, must satisfy. they required since in the definition of Quantum Dynamic Algebras there is no mention of what actions are, but in Quantum Dynamic Frames, they are required *a priori* to be relations on he set of states.

6.2 Concrete Quantum Dynamic Algebra

With the definition of Quantum Dynamic Algebra, we now discuss how to define a QDA from a QDF, and with particular interest in Concrete Quantum Dynamic Frames. We end the Section by stating that every QDA is isomorphic to a concrete one, which has as a consequence that every QDF is isomorphic to a concrete one, *i.e.*, to a QDF based on a Hilbert space.

Def. 6.2.1 (Quantum Dynamic Algebra from Quantum Dynamic Frame):
Given a Quantum Dynamic Frame, $\mathcal{F}$, we can define a Quantum Dynamic Algebra in the following way:

1. $\mathcal{Q}$ are the quantum actions of $\mathcal{F}$ (in the context of QDA the test symbol, $?$, is dropped when referring to tests),

2. $\cup$ is the non-deterministic choice of actions,

3. $\cdot$ is the composition of actions,

4. $\sim$ is the kernel of a action, *i.e*, $\sim x := [x]\varnothing$.

Furthermore, we say a QDA made from a QDF is a CONCRETE QUANTUM DYNAMIC ALGEBRA if it is made from a *Concrete Quantum Dynamic Frame*.

As seen from the definition above, the operations of a concrete QDA $(\cup, \cdot, \sim)$ correspond to the ones using the same symbols in a QDF. One could ask if the symbols used in Definition 6.1.2 also have the same meaning, thus justifying the use of the same notation.

Prop. 6.2.2 (Definitions in QDA vs. definitions in QDF):
Given a concrete Quantum Dynamic Algebra based on $\mathcal{F}$, the symbols used in Definition 6.1.2 have the same meaning as the correspondent ones in the Quantum Dynamic Frame $\mathcal{F}$.

***Proof*:**
Since quantum dynamic algebras and quantum dynamic frames use the same symbols, when needed, for clarification, the quantum dynamic algebra symbols will have a QDA in superscript.

$\mathcal{L}^{\mathrm{QDA}} = \mathcal{L}$:
Given $x \in \mathcal{Q}$, $\sim x \in \mathcal{L}$ since $\sim x = [x]\varnothing$ is testable, therefore $\mathcal{L}^{\mathrm{QDA}} \subset \mathcal{L}$
Given $p \in \mathcal{L}$, p can be written as $\sim\sim p = \sim p^{\perp}$ and $p^{\perp}?$ is a quantum action, therefore $\mathcal{L} \subset \mathcal{L}^{\mathrm{QDA}}$.

0 and 1 are just the tests $\varnothing?$ and $\Sigma?$.

$[x]p^{\mathrm{QDA}} := \sim (x\cdot \sim p) = [x\cdot \sim p]\varnothing = \{w \in \Sigma :\ w \notin \mathrm{dom}(x\cdot \sim p)\}$
$= \{w \in \Sigma :\ w \notin \mathrm{dom}(x) \vee \forall_{t \in x(\{w\})}\, t \notin \mathrm{dom}(\sim p)\} = \{w \in \Sigma :\ w \notin \mathrm{dom}(x) \vee \forall_{t \in x(\{w\})}\, t \notin \mathrm{dom}(p^{\perp})\} =$
$\{w \in \Sigma :\ w \notin \mathrm{dom}(x) \vee \forall_{t \in x(\{w\})}\, t \in p\} = \{w \in \Sigma :\ \forall_{t \in \Sigma}\, ((w,t) \in x \Rightarrow t \in p)\} = [x]p$

$\bigwedge_i p_i := \sim \bigcup_i \sim p_i = [\bigcup_i \sim p_i]\,\varnothing = (\bigcup_i \sim p_i)^{\perp} = \left(\bigcup_i p_i^{\perp}\right)^{\perp} = \bigcap_i p_i$, so the conjunction works in the usual way.

$p \leqslant q$ iff $p \wedge q = p$ iff $p \cap q = p$ iff $p \subset q$

$p \perp^{\mathrm{QDA}} q$ iff $p \leqslant \sim q$ iff $p \subset q^{\perp}$
Noticing also that, if $p \subset q^{\perp}$ then $p^{\perp} \supset \overline{q} = q$ iff $p \perp^{\mathrm{QDA}} q$, *i.e.*, is symmetric.
Thus $\perp^{\mathrm{QDA}}$ is $\perp$.

$\bigvee_i p_i := \sim\sim \bigcup p_i = \sim\sim \bigcup \sim\sim p_i = \sim \bigcap_i \sim p_i = (\bigcap_i p_i^{\perp})^{\perp} = \overline{\bigcup_i p_i}$ is the superposition of p_i.

Let $p = \{s\}$, with $s \in \Sigma$, then the only non-empty subset of p is p, therefore $p \in \mathrm{At}(\mathcal{L})$.
Let $p \in \mathrm{At}(\mathcal{L})$ be non-empty, then there exists $s \in p$. Since $\{s\} \subset p$, that is, $\{s\} \leqslant p$, we must have that $\{s\} = p$.

$\mathrm{At}(\mathcal{L})$ contains 0 and tests of atomic properties(*i.e.*, properties whose set only has one state of Σ).

The first condition says that $x \in \mathcal{U}$ is a total bijective function.
If $x\cdot \sim p = \sim (x \cdot p)$ then $\mathrm{dom}(x\cdot \sim p) = \mathrm{dom}(\sim (x \cdot p))$
$\mathrm{dom}(x\cdot \sim p) = \{w \in \Sigma :\ x(w) \in \mathrm{dom}(\sim p)\} = \{w \in \Sigma :\ x(w) \in \Sigma\backslash p\} = x^{-1}(\Sigma\backslash p) = \Sigma\backslash x^{-1}(p)$, the last equality is justifiable by x being bijective in Σ.
$\mathrm{dom}(\sim (x \cdot p)) = \mathrm{dom}(\sim (x\cdot \sim\sim p)) = \mathrm{dom}(([x]p^{\perp})?) = \Sigma\backslash([x]p^{\perp})^{\perp}$
Thus we conclude that $x^{-1}(p) = ([x]p^{\perp})^{\perp}$)

The condition for $\mathcal{D}^{\mathrm{QDA}}$ says that for a atom $a = \{s\}$ there is a atom $b = \{t\}$ such that $a \leqslant [x]b$, that is, $x(s)$ is not defined or $x(s) \in \{t\}$ iff $x(s) = t$, *i.e.*, x is a (partial) function, which corresponds to the deterministic actions.

For the image-set of p by x, we notice that any action x can be written as $x = \cup_i y_i$ with $y_i \in \mathcal{D}$, and that an atom $b = \{t\}$ be part of it, we must have an atom $a = \{s\}$ and a deterministic action y_i such that $s \in p$ ($a \leqslant p$) and y is defined on a ($a \leqslant \sim y$), and $y(s) = t$ ($a \leqslant [y]b$).
Its important to note that this is a set of atoms of At and not a set of states of Σ, but there is a obvious bijection between them.

Finally, $x[p]_{\mathrm{QDA}} = \bigvee x(p)_{\mathrm{QDA}} = \overline{\bigcup x(p)_{\mathrm{QDA}}} = \overline{x(p)} = x[p]$ ■

We just saw that the used of the same notation is justified so we just need to see that it is indeed a Quantum Dynamic Algebra.

Prop. 6.2.3:

The construction in Definition 6.2.1 satisfies the axioms for QDA.

***Proof*:**

Some axioms are intuitive, but some look different from the ones with the same name in the definition of quantum dynamic frame.

$1.\ 0 \in \mathcal{L}$

Easy to see, 0 is the test $\varnothing?$ and $\varnothing \in \mathcal{L}$.

$2.$

- $(\mathcal{Q}, \cup)$ is a complete lattice, *i.e.*, every subset of $\mathcal{Q}$ as a supremum and a infimum: they correspond to the union and the intersection of relations, respectively.
- We have that $1 = \Sigma?$ which is the identity, so $(\mathcal{Q}, \cdot, 1)$ is a monoid.
- As seen before in Proposition 4.3.3, the composition, $\cdot$, commutes with the choice, $\cup$.
- The construction of $\mathcal{Q}$ in a QDF is made from $\mathcal{L} \cup \mathcal{U}$.

3. and 4. Choice and Composition

Axioms 3 and 4 are satisfied as seen in Propositions 2.4.9 and 2.4.10.

5. Adequacy

(H): We know that given p and $s \in p$ then $s \xrightarrow{p} t$ iff $s = t$. (QDF *Adequacy*)

Given $s \in p \cap q$ we have $s \in p$ and $s \in q$, therefore, by (H), $q(s) = s$. We have then that $q(s)\downarrow$ and $q(s) \in p$, thus $s \in [q]p$.

Given $s \in p \cap [p]q$ we have that $s \in [p]q$ and $s \in p$, so by (H), $p(s) = s$. Since p is defined on s and $p(s) = s$ then $s = p(s) \in q$.

6. Proper Superposition

Given $p, q \in \mathcal{L}$ let $s \in p$ and $t \in q$ be two states. From QDF *superposition* axiom we know that $\exists_{w \in \Sigma}\ s \to w \to t$, that is $w \not\perp s$ and $w \not\perp t$, thus $w \not\perp p$ and $w \not\perp q$. We just need to chose $r = \{w\}$ to conclude.

7. Self-adjointness Axiom

Let $s \in p$ such that $q(s)$ is defined. We want to show that $q(s) \in \sim [q] \sim p = ([q]p^{\perp})^{\perp}$, using Corollary 4.3.6, $([q]p^{\perp})^{\perp} = q^{\dagger}(p)$ and since tests are self-adjoint, *i.e.*, $q^{\dagger} = q$, we need to show that $q(s) \in q(p)$, which is true since $s \in p$.

8. Covering Law

Let $q \in \mathrm{At}(\mathcal{L})$,*i.e*, $q = \{s\}$ for some state $s \in \Sigma$, and $p \in \mathcal{L}$. We want to show that $p \cap (p^{\perp} \sqcup q) \in \mathrm{At}(\mathcal{L})$.

We have that $p \cap (p^{\perp} \sqcup s) = p \cap (p \cap s^{\perp})^{\perp}$.

∘ First, lets see that it is not empty by checking that it contains the state $p(s)$:

Clearly, $p(s) \in p$, so we need to show that $p(s) \perp (p \cap q^{\perp})$.

Let $t \in p \cap s^{\perp}$. We have that $t \in p$, therefore $p(t) = t$.

We also have that $t \in s^{\perp} \Leftrightarrow t \perp s \Leftrightarrow p(t) \perp s \Leftrightarrow t \perp p(s)$.

Thus $p(s) \perp (p \cap q^{\perp})$, that is, $p(s) \in p \cap (p^{\perp} \sqcup s)$.

∘ Finally, we will see that $p(s)$ is the only element of $p \cap (p^{\perp} \sqcup s)$.

Lets assume, by contradiction, that exists $t \in p \cap (p \cap s^{\perp})^{\perp}$ such that $t \neq p(s)$.

We have then $s \xrightarrow{p} p(s) \neq t \in p$. By the covering law axiom of QDF we know that $\exists_{v \in p}\ t \to v \not\to s$.

First we note that $v \in p \cap s^{\perp}$. Then, since $t \in (p \cap s^{\perp})^{\perp}$, we have that $t \perp w$ for every $w \in p \cap s^{\perp}$, and in particular, $t \perp v$.

However, we just saw that $t \to v$, which is a contradiction. Thus $p \cap (p^{\perp} \sqcup s) = \{p(s)\}$.

9. Atomicity

Let $p \in \mathcal{L}$. We need to show that $p \subset \bigsqcup_{s \in p} s$.

We have that $\bigsqcup_{s \in p} s = (\bigcap_{s \in p} s^{\perp})^{\perp} = (p^{\perp})^{\perp} = \overline{p}$ and we already know that $p \subset \overline{p}$.

10. Mayet's Condition

In QDF, Mayet's Condition says that $\exists_{U\in\mathcal{U}}\exists_{P\in\mathcal{L}}\, U(P)\subsetneq P$ and $\exists_{t,w\in\Sigma}\forall_{s\in\overline{\{t,w\}}}\, t\perp w, U(s)=s$.

This is extremely similar to the Mayet's Condition stated in QDA: we just need to chose $p:=P$, $u:=U$, $q:=\{t\}$, $r:=\{w\}$, and note that $q\vee r$ is $\overline{\{t,w\}}$ and that $p\subset[u]p$ iff $u(p)\subset p$.

11. Actions are determined by their behavior on atoms

Its obviously true since actions x unions of (possible partial) functions on Σ.

12. Image commutes with unions

Given $p\in\mathcal{L}$ and a family $\{x_i\}_{i\in I}$ of actions in $\mathcal{Q}$ we have:

$(\bigcup_{i\in I}x_i)(p)=\{t\in\Sigma:\ \exists_{s\in p}\, t\in(\bigcup_{i\in I}x_i)(s)\}=\{t\in\Sigma:\ \exists_{s\in p}\exists_{i\in I}\, t\in x_i(s)\}=\{t\in\Sigma:\ \exists_{i\in I}\exists_{s\in p}\, t\in x_i(s)\}$

$=\bigcup_{i\in I}\{t\in\Sigma:\ \exists_{s\in p}\, t\in x_i(s)\}=\bigcup_{i\in I}x_i(p)$ ■

Theorem 6.2.4:

Every quantum dynamic algebra is isomorphic to a concrete quantum dynamic algebra.

The sketch of the proof can be found in [1]. Since a quantum dynamic frame can be made into a quantum dynamic algebra, we have the following consequence.

Corollary 6.2.5:

Every quantum dynamic frame is isomorphic to a concrete quantum dynamic frame.

This is an important result. Thorough this work, every time we tried to make the meaning of something clear, we resorted to examples using Hilbert spaces, because, ultimately, the properties of Hilbert spaces were the ones that we were trying to replicate. This result validates this approach because not only those properties were replicated but no new ones were gained when considering a general Quantum Dynamic Frame.

Chapter 7

Quantum Computation

So far we have a quantum logic that does not contradict classical logic and that has quantum programs in its language. Considering that Propositional Dynamic Logic is used to argue about computer programs, the next step is to try to understand the relation between Logic of Quantum Programs and Quantum Computation.
In order to understand this relation, it is helpful to recall the basis of Quantum Computation: *quantum bits* (Section 7.1) and *quantum gates* (Section 7.2). Finally we see the example of *quantum teleportation* (Section 7.3) as we will use it on the last Chapter.

7.1 Quantum Bits

In classical computation the *bit* is the most important concept, as it is the basic unit of information. A *bit* has a state, it can be either 0 or 1. A *Quantum Bit*, or *Qubit* for short, also has a state. Two possible states, corresponding to the classical states 1 and 0, are $|1\rangle$ and $|0\rangle$. Unfortunately, similarities of classical and quantum *bits* stop here.
Qubits are well explained by Schrödinger's cat: if we put a cat inside a opaque box with poison and close the box, then the cat is neither dead or alive, but in a *superposition* of those two states, and only after we open the box the cat will be in one of two states.
Just like this poor cat, we can have a superposition of the *qubits* $|0\rangle$ and $|1\rangle$, such that a general *qubit* $|\psi\rangle$ is in the form:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{7.1}$$

It is usual to assume that $|\alpha|^2 + |\beta|^2 = 1$ so that $|\alpha|^2$ corresponds to the probability of measuring $|0\rangle$ and $|\beta|^2$ to the probability of measuring $|1\rangle$.
Mathematically, this can be achieved easily using a Hilbert space:

Def. 7.1.1 (*Qubit*):
Considering the complex Hilbert space $\mathbb{C}^2$ we define

$$|0\rangle := \begin{pmatrix}1\\0\end{pmatrix} \qquad\qquad |1\rangle := \begin{pmatrix}0\\1\end{pmatrix} \tag{7.2}$$

A QUBIT, $|\psi\rangle$, is a vector

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{7.3}$$

Where $\alpha, \beta \in \mathbb{C}^2$ are such that $|\alpha|^2 + |\beta|^2 = 1$.

There are two *qubits* that will be important later on:

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad\qquad |-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{7.4}$$

These *qubits* have 50% of probability of measuring either $|0\rangle$ or $|1\rangle$.

Bits have a physical interpretation of *on*/*off*, which can be accomplished with high and low voltage. A *qubit* can represent, for example, the spin of an electron, with $|0\rangle$ corresponding to spin *up* ($\uparrow$), and $|1\rangle$ representing spin *down* ($\downarrow$) - which explains the other notation of $|\uparrow\rangle/|\downarrow\rangle$ for $|0\rangle/|1\rangle$.

Considering the example of electron spin, how do we represent the system of two electrons?
After measuring the spin of both electrons, each can be in 2 possible states, *up* or *down*, that is, the two electron system can be in one of $2 \times 2 = 4$ possible states. These states, represented using *tensor product*, are:

$$|00\rangle := |0\rangle \otimes |0\rangle \qquad |01\rangle := |0\rangle \otimes |1\rangle \qquad |10\rangle := |1\rangle \otimes |0\rangle \qquad |11\rangle := |1\rangle \otimes |1\rangle \tag{7.5}$$

Note that given vectors (a, b) and (c, d) the tensor product of them is:

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \tag{7.6}$$

This allow us to write the above states as vector in $\mathbb{C}^4$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{7.7}$$

This construction can be generalized for any finite number of *qubits*.

Def. 7.1.2 (n *Qubit* System):
A system with n *qubits* is supported in the Hilbert space $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ of $\mathbb{C}^2$ tensored with itself n times. The basis of this space is composed of vectors of the form

$$|x_1 \dots x_n\rangle := |x_1\rangle \otimes \cdots \otimes |x_n\rangle, \qquad x_i \in \{0, 1\} \tag{7.8}$$

It is important to note that for n *qubits*, there are 2^n vectors in the basis therefore to specify a state $|\psi\rangle$ of n *qubits* it is necessary to know the value of the 2^n coefficients. In contrast, in classical computation, to specify a state with n *bits* we need only n numbers.
From this perspective, *qubits* hold exponentially more information than *bits* and it would seen that we can improve any classical algorithm to be better. However, the problem comes from when we measure a *qubit*, it will collapse in either $|0\rangle$ or $|1\rangle$ and we cannot recuperate the coefficients α and β.

In quantum computation, despite not being possible to access all the information in a *qubit*, it is possible to have some non-classic capabilities because of quantum properties. One of them, already mentioned,

is *superposition* of states, and another important one is *entanglement*. To understand entanglement lets look at the following (apparently) simple state:

$$|\beta_{00}\rangle := \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{7.9}$$

When measured, it has 50% chance to be in state $|00\rangle$ and 50% of being in state $|11\rangle$.
Suppose we measure the first *qubit*: we either measure $|0\rangle$ or $|1\rangle$. If we measure $|0\rangle$ (respectively, $|1\rangle$) it can only be the case that the second *qubit* is also $|0\rangle$ (resp. $|1\rangle$), and *vice-versa* if the second *qubit* is the first to be measured.
It is this *correlation* between *qubits* that we call *entanglement*. More specifically:

Def. 7.1.3 (Entanglement):
A *qubit* $|\psi\rangle$ is said to be SEPARABLE if we can write it as a tensor of two states $|\psi'\rangle$ and $|\psi''\rangle$, *i.e.*, if

$$|\psi\rangle = |\psi'\rangle \otimes |\psi''\rangle \tag{7.10}$$

Otherwise, $|\psi\rangle$ is said to be ENTANGLED.

Example 7.1.4 (Separable Vector):
Let us consider vector $|\psi\rangle = |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$.
It is easy to check that $|\psi\rangle = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$, thus vector $|\psi\rangle$ is separable.

Example 7.1.5 (Entangled State):
Now lets consider the vector $|\beta_{00}\rangle = |00\rangle + |11\rangle$.
Let $|\psi'\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi''\rangle = \gamma|0\rangle + \delta|1\rangle$, we have that

$$|\psi'\rangle \otimes |\psi''\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \tag{7.11}$$

Then to be true that $|\beta_{00}\rangle = |\psi'\rangle \otimes |\psi''\rangle$ we must have $\alpha\delta = 0$, that is, $\alpha = 0 \ \vee \ \delta = 0$.
If $\alpha = 0$ the coefficient of $|00\rangle$ is 0 and not 1, and if $\delta = 0$ the coefficient of $|11\rangle$ is 0 and not 1.
We can conclude that the state $\overline{|\psi\rangle}$ is not separated.

7.2 Quantum Gates

Every classical program can be seen as a *circuit* of *logical gates* that operate on an input of *bits*. However, most people are more used to see a program as a code in their favorite language, or for the most theoretical, as a Turing Machine.
Unlike the classical case, quantum computation is done using QUANTUM GATES. These are just unitary operations and because the workings of some of them do not have intuitive classical description, as is the case in most of Quantum Mechanics, there is no analogous for most of them in the classical world.

In classical computation, the only interesting single *bit* gate is the NOT gate, changing the truth value of the *bit*. On the other hand, since the only requisite for a quantum gate is being a unitary transformation, there is an infinite number of them.

The most common quantum gates are the X, Y, Z and *Hadamard* gates. The first three act on $|0\rangle$ and $|1\rangle$ in the following way:

$$\begin{array}{lll} X|0\rangle = |1\rangle & Y|0\rangle = i|1\rangle & Z|0\rangle = |0\rangle \\ X|1\rangle = |0\rangle & Y|1\rangle = -i|0\rangle & Z|1\rangle = -|1\rangle \end{array} \tag{7.12}$$

The X-gate corresponds to the quantum NOT, but the other two have no analogous, with the Y-gate doing almost the same that X but changing the coefficients, and Z is almost the identity but flips the sign of the $|1\rangle$ *qubit*.

In matrix form they are given by:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7.13}$$

The other single bit gate important to mention is the *Hadamard*-gate. Its function is to given a state $|0\rangle$ or $|1\rangle$ it transforms it into a state that is a superposition of both with equal probability of measuring $|0\rangle$ or $|1\rangle$.

$$\begin{array}{l} H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle \\ H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle \end{array} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{7.14}$$

All four gates have a circuit representation as follows:

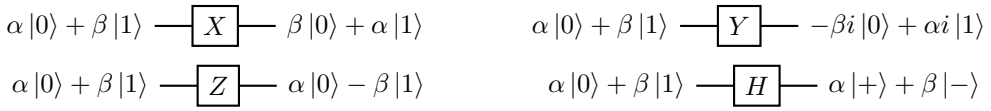

Figure 7.1: Circuits that represent the X, Y, Z, and *Hadamard* gates and their operation on a general *qubit* $\alpha|0\rangle + \beta|1\rangle$.

For a two *qubit* system, the most important gate is the *controled*-NOT gate, also called CNOT. The first input is called the *control qubit* and the second is the *target qubit*.

If the control *qubit* is $|0\rangle$ the target is left unchanged, but if it is $|1\rangle$ the target is flipped.

$$\begin{array}{ll} CNOT|00\rangle = |00\rangle & CNOT|10\rangle = |11\rangle \\ CNOT|01\rangle = |01\rangle & CNOT|11\rangle = |10\rangle \end{array} \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{7.15}$$

The circuit form of CNOT is given in Figure 7.2 on the left, where the top wire corresponds to the control and the bottom to the target.

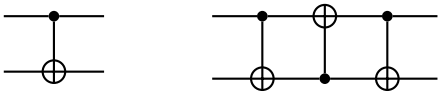

Figure 7.2: CNOT circuit (left) and swap circuit (right)

An interesting circuit made with CNOT gates is one combining three of them as shown in Figure 7.2. This circuit swaps the *qubits* of a two *qubit* state. On the first and third gate, the control is the top wire but on the second gate it is the bottom wire instead.

Representing the first and third gates by $CNOT_{12}$ and the second with $CNOT_{21}$, the evolution of the *qubits* is then:

$$\begin{aligned}
|00\rangle &\xrightarrow{CNOT_{12}} |00\rangle \xrightarrow{CNOT_{21}} |00\rangle \xrightarrow{CNOT_{12}} |00\rangle \\
|01\rangle &\xrightarrow{CNOT_{12}} |01\rangle \xrightarrow{CNOT_{21}} |11\rangle \xrightarrow{CNOT_{12}} |10\rangle \\
|10\rangle &\xrightarrow{CNOT_{12}} |11\rangle \xrightarrow{CNOT_{21}} |01\rangle \xrightarrow{CNOT_{01}} |01\rangle \\
|11\rangle &\xrightarrow{CNOT_{12}} |10\rangle \xrightarrow{CNOT_{21}} |10\rangle \xrightarrow{CNOT_{11}} |00\rangle
\end{aligned} \tag{7.16}$$

Note that *CNOT* can be seen as: if the control is $|1\rangle$ apply X to the target otherwise do nothing.
This idea of a controlled gate can be extended to any arbitrary gate U in a similar way and with a similar circuit: if the control is $|1\rangle$ apply U to the target otherwise do nothing.

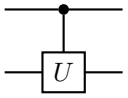

Figure 7.3: Circuit for a controlled-U gate

The last important operation on *qubits* we will describe the circuit is the measurement. As said before, a *qubit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ when measured must yield $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.

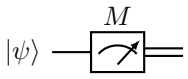

Figure 7.4: Measurement circuit representation.

The double wire represents that now since we have either $|0\rangle$ or $|1\rangle$ is the same as having the classical *bits* 0 or 1.

7.3 Quantum Teleportation

Lets suppose that Alice has a *qubit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ that she wishes to give to Bob, but Bob is far away to give it personally and all she can do is send him classical *bits*.
However, before they departed, they entangled two *qubits* in state $|\beta_{00}\rangle$ and Alice kept the first *qubit* while Bob kept the second.

With this and the gates discussed in the previous section we have all we need for quantum teleportation. The *Teleportation Protocol* circuit is shown in the figure below.

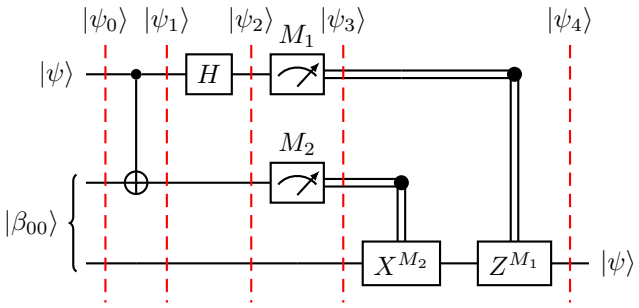

Figure 7.5: Circuit for the teleportation protocol.

On the final section of the next chapter, we will use LQP to show the teleportation protocol is sound, but now lets use the gate properties to show that it works.

The 3-*qubit* system is in state

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\right] \tag{7.17}$$

Alice then sends $|\psi\rangle$ and her part of $|\beta_{00}\rangle$ through a CNOT-gate, changing the state of the system to

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\right] \tag{7.18}$$

Next,the first *qubit* goes through a Hadamard gate obtaining

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right] \tag{7.19}$$

Reorganizing the terms, we get

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}\big[&|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle)\\ &+ |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |00\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\big]\end{aligned} \tag{7.20}$$

Looking at this equation, after Alice measures her *qubits* we know in which state Bob's *qubit* will be. Noting that it will be $|\psi\rangle$ in the case of $|00\rangle$ and very similar on the other cases.
We have that if $M_1 = 0$ the signs are correct and that if $M_2 = 0$ the coefficients are in the correct place. So if $M_2 = 1$ the controlled-X will place the coefficients in the correct places, and on the cases that one sign is incorrect, the sign will be on the $|1\rangle$ part, thus, the controlled-Z gate will flip it to $+$. In the end Bob's *qubit* will end up as $|\psi\rangle$. This evolution is detailed below.

$$\begin{aligned}
M = 00:&\ |\psi_3\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle\\
M = 01:&\ |\psi_3\rangle = \alpha\,|1\rangle + \beta\,|0\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle\\
M = 10:&\ |\psi_3\rangle = \alpha\,|0\rangle - \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle - \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle\\
M = 11:&\ |\psi_3\rangle = \alpha\,|1\rangle - \beta\,|0\rangle \longrightarrow \alpha\,|0\rangle - \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle = |\psi\rangle
\end{aligned} \tag{7.21}$$

Chapter 8

Compound-System Quantum Frame

As we saw, every Quantum Dynamic Frame is isomorphic to a concrete one, that is, one based on a Hilbert space. For this reason, we can consider the semantics of LQP just based in Hilbert spaces. In doing so, using tensor product, we will be able to talk about systems with several *qubits*, which allows us to express properties such as quantum entanglement and properties related to quantum computation.
This Chapter then starts by providing *definitions* (Section 8.1) of Compound-System Quantum Frame, followed by the *syntax, semantics* (Section 8.2), and *axioms and rules* (Section 8.3) for this extension of LQP - Compound-System Quantum Logic. Finally, we put this in practice by showing some *results* (Section 8.4) with inclusion of the example of *correctness of the teleportation protocol* (Subsection 8.4.1) capitalizing on the work in [2].

8.1 Definitions

Since we want to consider *qubits*, we take as the foundation for construction a 2-dimensional Hilbert space, H, with orthonormal basis $\{|0\rangle, |1\rangle\}$.

Def. 8.1.1 (Compound-System Quantum Frame):
Let $n \geqslant 2$ be a natural number and $N := \{1, \ldots, n\}$. A COMPOUND-SYSTEM QUANTUM FRAME is the quantum frame $\Sigma(\mathcal{H}_n)$ based on the Hilbert space $\mathcal{H}_n := H^{\otimes n} = H \otimes \cdots \otimes H$ (n times), with the caveat that it does not satisfy Mayet's condition.
Moreover, the n copies of H are considered distinct but isomorphic. The i-th component of $H^{\otimes n}$ is denoted by $H^{(i)}$ and given $I \subset N$ we denote $\mathcal{H}_I := H^{\otimes I} = \bigotimes_{i \in I} H^{(i)}$, with $\mathcal{H}_N = \mathcal{H}_n =: \mathcal{H}$. Also, when clarification is needed, will denote an element $|x\rangle \in H^{(i)}$ by $|x\rangle_i$, using the subscript i to indicate that it belongs to $H^{(i)}$.

Furthermore, we denote the canonical isomorphism between H and $H^{(i)}$ by $\epsilon_i \colon H \to H^{(i)}$, and similarly, by extending this notation to $I \subset N$ with $|I| = k$, the canonical isomorphism between $H^{\otimes k}$ and $\mathcal{H}_I$ is denoted by $\epsilon_I \colon H^{\otimes k} \to \mathcal{H}_I$. We will also denote by $\mu_I \colon \mathcal{H}_I \otimes \mathcal{H}_{N \setminus I} \to \mathcal{H}$ the isomorphism between these two spaces.

Def. 8.1.2 (I-separation):
A state $s \in \Sigma(\mathcal{H})$ is said to have its I-*qubits* in state $s' \in \Sigma(\mathcal{H}_I)$, written as $s_I = s'$, if

$$\exists_{|\psi\rangle \in s} \exists_{|\psi'\rangle \in \mathcal{H}_i} \exists_{|\psi''\rangle \in \mathcal{H}_{N \setminus I}} \text{ such that } |\psi\rangle = \mu_I(|\psi'\rangle \otimes |\psi''\rangle). \tag{8.1}$$

We say that a state s is I-SEPARATED if s_I exists, and s_I is called the I-*local component* (or *local state*) of s. In particular, for $I = \{i\}$, we denote $s_{\{i\}}$ by s_i and call it the i-*th coordinate* of state s.

Note that if a state is I-separated it is also $N \backslash I$-separated.

Example 8.1.3 (Separated State):

Consider the vector $|\psi\rangle = |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$.

It is easy to check that $|\psi\rangle = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$, thus the state $\overline{|\psi\rangle}$ is 1-separated and 2-separated.

Example 8.1.4 (Entangled State):

Now consider vector $|\beta_{00}\rangle = |00\rangle + |11\rangle$.

Let $|\psi'\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\psi''\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$, we have that

$$|\psi'\rangle \otimes |\psi''\rangle = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle \tag{8.2}$$

Then to be true that $|\beta_{00}\rangle = |\psi'\rangle \otimes |\psi''\rangle$ we must have $\alpha\delta = 0$, that is, $\alpha = 0 \ \vee \ \delta = 0$.

If $\alpha = 0$ the coefficient of $|00\rangle$ is 0 and not 1, and if $\delta = 0$ the coefficient of $|11\rangle$ is 0 and not 1.

We can conclude that the state $\overline{|\psi\rangle}$ is not separated.

Def. 8.1.5 (I-Local Property):

Given $I \subset N$, we say that a property $S \subset \Sigma$ is I-LOCAL if it corresponds to a property of the subsystem formed by the qubits in I, *i.e.*, if $\exists_{S' \subset \Sigma(\mathcal{H}_I)}$ such that

$$S = \{s \in \Sigma \colon s_I \in S'\} = \{\overline{\mu_I(\psi \otimes \psi')} \colon \overline{\psi} \in S', \psi \in \mathcal{H}_{N \backslash I}\} \tag{8.3}$$

The family of local properties with inclusion forms lattice. The join is the union $S \cup T$, the atoms are properties that correspond to a state in $\mathcal{H}_I$, we call the atoms LOCAL STATES, and the greatest element is the property

$$\top_I^\Sigma := \{s \in \Sigma \colon s \text{ is } I\text{−separated}\} = \bigcup \{S \subset \Sigma \colon S \text{ is } I\text{−local}\} \tag{8.4}$$

The family of I-local properties is closed for the union and intersection, but not for complementation.

Def. 8.1.6 (Local Map):

Given $I \subset N$, we say that a linear map $F \colon \mathcal{H} \to \mathcal{H}$ is I-LOCAL if it affects only the qubits in I, that is, there exists a map $G \colon \mathcal{H}_I \to \mathcal{H}_I$ shuch that $F \circ \mu_I(\psi \otimes \psi') = \mu_I(G(\psi) \otimes \psi')$

A map $F \colon \Sigma \to \Sigma$ is I-local, if the it is induced by a I-local map on $\mathcal{H}$.

Def. 8.1.7 (Local Action):

A LOCAL ACTION is a quantum action $R \in \mathcal{Q}$ that can be written as an arbitrary union of deterministic actions that are local maps.

The family of local actions forms a lattice, the join is the union (the choice) $R \cup R'$ and the greatest element is the action

$$\top_I^{\Sigma \times \Sigma} := \bigcup \{\pi \in \mathcal{D} \colon \pi \text{ is an } I\text{−local map}\} \tag{8.5}$$

Prop. 8.1.8:

If $S_I \subset \Sigma$ is a I-local property, then $S_I?$ is a I-local map.

An interesting question about liner maps $F : \Sigma \to \Sigma$ is how many states are needed to uniquely determine F?

For a linear map $F : H \to H$ we only need to know the image of a basis of H for F to be uniquely determined, that is, we only need to know the values $F(|0\rangle)$ and $F(|1\rangle)$.

Example 8.1.9:

Let us consider the linear functions id and Z. We have that:

$\circ\ id(|0\rangle) = |0\rangle$ and $id(|1\rangle) = |1\rangle$

$\circ\ Z(|0\rangle) = |0\rangle$ and $Z(|1\rangle) = -|1\rangle$

For the induced maps on Σ we have for states $\overline{|0\rangle}$ and $\overline{|1\rangle}$:

$\circ\ id(\overline{|0\rangle}) = \overline{id(|0\rangle)} = \overline{|0\rangle} = \overline{Z(|0\rangle)} = Z(\overline{|0\rangle})$

$\circ\ id(\overline{|1\rangle}) = \overline{id(|1\rangle)} = \overline{|1\rangle} = \overline{-|1\rangle} = \overline{Z(|1\rangle)} = Z(\overline{|1\rangle})$

However we have for state $\overline{|+\rangle}$ that $id(\overline{|+\rangle}) \neq Z(\overline{|+\rangle})$.Furthermore,

$\circ\ id(\overline{|+\rangle}) = \overline{id(|+\rangle)} = \overline{|+\rangle}$

$\circ\ Z(\overline{|+\rangle}) = \overline{Z(|+\rangle)} = \overline{|-\rangle}$

As we can see from this Example, with two states we cannot uniquely define a linear map on Σ. However, we only need a finite number of states:

Prop. 8.1.10:

A linear function on $\Sigma(\mathcal{H}_1)$ is uniquely defined by its image on states $\overline{|0\rangle}$, $\overline{|1\rangle}$ and $\overline{|+\rangle}$.

Corollary 8.1.11:

A linear function on $\Sigma(\mathcal{H}_n)$ is uniquely defined by its image on states

$$\{\overline{|x\rangle_1 \otimes \cdots \otimes |x\rangle_n} : |x\rangle_i \in \{|0\rangle_i, |1\rangle_i, |+\rangle_i\}\} \tag{8.6}$$

We already discussed separation and locality, however, it is also important to be able to express entanglement between the states of two *qubits* i and j in a n*-qubit* system (as the teleportation protocol needs it).

This is done by using linear functions, which may seem odd, but the next result helps to give an idea how they are related.

Prop. 8.1.12:

Let $F : H^{(i)} \to H^{(j)}$ be a linear function such that in the canonical basis we have:

$$F|\psi\rangle = \begin{pmatrix} m_{00} & m_{10} \\ m_{01} & m_{11} \end{pmatrix} |\psi\rangle \tag{8.7}$$

That is, $F|0\rangle_i = m_{00}|0\rangle_j + m_{01}|1\rangle_j$ and $F|1\rangle_i = m_{10}|0\rangle_j + m_{11}|1\rangle_j$. Then there exists a bijective correspondence σ between linear functions $F : H^{(i)} \to H^{(j)}$ and the elements of $H^{(i)} \otimes H^{(j)}$ given by:

$$\sigma(F) = m_{00}|00\rangle_{ij} + m_{01}|01\rangle_{ij} + m_{10}|10\rangle_{ij} + m_{11}|11\rangle_{ij} \tag{8.8}$$

Example 8.1.13 (Entangled State β_{00}):

Lets consider the function $id_{ij} : H^{(i)} \to H^{(j)}$ given by $id_{ij} := \epsilon_j \circ id \circ \epsilon_i^{-1}$, where id is the identity in H. Clearly we have:

$$id_{ij}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |\psi\rangle \tag{8.9}$$

Therefore the corresponding state in $\Sigma(H^{(i)} \otimes H^{(i)})$ is

$$\overline{\sigma(id_{ij})} = \overline{|00\rangle_{ij} + |11\rangle_{ij}} = \overline{\frac{1}{\sqrt{2}}(|00\rangle_{ij} + |11\rangle_{ij})} = \overline{|\beta_{00}\rangle_{ij}} \tag{8.10}$$

Note that this is not enough, since we will need a state in a n-*qubit* system, which also means that we will need a linear function $F\colon \mathcal{H}_N \to \mathcal{H}_N$.

The next result deals with the function part.

Prop. 8.1.14:

Considering $\mathcal{H}_N$, let $W = \{|x\rangle \otimes |0\rangle^{\otimes(n-1)} : |x\rangle \in H\}$. Then any linear map $F : \mathcal{H}_N \to \mathcal{H}_N$ induces a linear map $F_{(1)} : H \to H$ given by

$$F_{(1)} |x\rangle := (P_1 \circ P_W \circ F)(|x\rangle \otimes |0\rangle^{\otimes(n-1)}) \tag{8.11}$$

Where P_W is the projection onto W and P_1 gives the 1-qubit.

Also, a linear map $G\colon H \to H$ can be written as $G = F_{(1)}$ for some $F\colon \mathcal{H}_N \to \mathcal{H}_N$.

Now, given a linear map F in $\mathcal{H}_N$ we define a function $F^{(ij)}_{(1)} : H^{(i)} \to H^{(j)}$ similarly as in the Example above

$$F^{(ij)}_{(1)} := \epsilon_j \circ F_{(1)} \circ \epsilon_i^{-1} \tag{8.12}$$

And the state in $H^{(i)} \otimes H^{(j)}$ is

$$\overline{F}_{(ij)} := \overline{\sigma(F^{(ij)}_{(1)})} \tag{8.13}$$

The next result shows the connection between these states and entanglement (acording to F).

Prop. 8.1.15:

Let $F : \mathcal{H}_N \to \mathcal{H}_N$ be a linear map. We have that state $\overline{F}_{(ij)}$ is 'entangled according to F', that is, if $F_{(1)} |x\rangle = |y\rangle$ and the state of a 2-qubit system is $\overline{F}_{(ij)} \in H^{(i)} \otimes H^{(j)}$, then we have that any measurement of the qubit i resulting in state $|x\rangle$ will collapse the qubit j to state $|y\rangle$.

Moreover, $\overline{F}_{(ij)}$ is entangled iff $F_{(1)}$ is invertible.

***Proof*:**

Let $\{|x\rangle, |z\rangle\}$ be a basis for H, then we know that

$$\sigma(F_{(1)}) = m_{xx} |xx\rangle + m_{xz} |xz\rangle + m_{zx} |zx\rangle + m_{zz} |zz\rangle \tag{8.14}$$

where the coefficients are taken from the matrix of F written in the given basis.

Reorganizing the terms, we get:

$$\sigma(F_{(1)}) = |x\rangle \otimes (m_{xx} |x\rangle + m_{xz} |z\rangle) + |z\rangle \otimes (m_{zx} |x\rangle + m_z |zz\rangle) \tag{8.15}$$

Now we just need to notice that $(m_{xx} |x\rangle + m_{xz} |z\rangle = F_{(1)} |x\rangle$ and $m_{zx} |x\rangle + m_z |zz\rangle = F_{(1)} |z\rangle$. That is, the equation becomes

$$\sigma(F_{(1)}) = |x\rangle \otimes F_{(1)} |x\rangle + |z\rangle \otimes F_{(1)} |z\rangle \tag{8.16}$$

Thus if the measurement of the i *qubit* is $|x\rangle$ then the j *qubit* will be in state $F_{(1)} |x\rangle = |y\rangle$.

We also notice that it is entangled iff $F_{(1)} |x\rangle$ and $F_{(1)} |z\rangle$ are linearly independent, *i.e.*, F has rank 2, thus, is invertible. ■

Finally, from state $\overline{F}_{(ij)} \in H^{(i)} \otimes H^{(j)}$ we can define a property $\overline{F}_{ij} \in \mathcal{H}_N$ that corresponds to the states with $i, j -$ *qubits* in state $\overline{F}_{(ij)}$ in the following way:

$$\overline{F}_{ij} := \{s \in \Sigma \colon s_{\{i,j\}} = \overline{F}_{(ij)}\} \tag{8.17}$$

$$= \{\overline{\mu_{\{i,j\}}(|\psi\rangle \otimes |\psi'\rangle)} \colon |\psi\rangle \in \overline{F}_{(ij)},\ |\psi'\rangle \in \mathcal{H}_{N\setminus\{i,j\}}\} \tag{8.18}$$

Clearly, property $\overline{F}_{ij}$ is $\{i, j\}$-local, and is a atom of the lattice of $\{i, j\}$-local properties.

Example 8.1.16 (Bell States):
We can get similar examples of $|\beta_{00}\rangle$, that are denoted by $|\beta_{xy}\rangle$ with $x, y \in 0, 1$. These are called *Bell States*.
Considering X_1 and Z_1 the quantum gates in $\mathcal{H}_N$ affecting only the 1st *qubit*, we define, for distinct i, j:

$$\beta_{xy}^{ij} := \overline{(Z_1^x \cdot X_1^y)}_{ij} \tag{8.19}$$

Where $X_1^0 := id$, $Z_1^0 := id$, $X_1^1 := X_1$, and $Z_1^1 := Z_1$.
For $N = \{1, 2\}$ we have:

$$\beta_{00} = \overline{|00\rangle + |11\rangle} \quad \beta_{01} = \overline{|01\rangle + |10\rangle} \quad \beta_{10} = \overline{|00\rangle - |11\rangle} \quad \beta_{11} = \overline{|01\rangle - |10\rangle} \tag{8.20}$$

8.2 Syntax and Semantics

The syntax is build up from the syntax of LQP. The first addition is that we need to set n, the number of *qubits* of the system.
We still have the families $\mathcal{P}$, propositional variables, and $\mathcal{U}$, basic programs, but we add a family, $\mathcal{C}$, of *propositional constants* c, and for each basic action (to be interpreted as *quantum gates*) $U \in \mathcal{U}$ we add a index $I \subset N$ reflecting the set of *qubits* on which the quantum gate U is active. In particular, we require $\mathcal{C}$ to have constants 1 and $+$ (representing the states $\overline{|1\rangle^{\otimes n}}$ and $\overline{|+\rangle^{\otimes n}}$), and to have the usual quantum gates $X, Y, Z, H, CNOT, \ldots$ to be part of $\mathcal{U}$.
The well-formed formulas and programs are then given by:

$$\begin{aligned} \varphi &::= \top_I \,|\, p \,|\, c \,|\, \neg\varphi \,|\, \varphi \wedge \varphi \,|\, [\alpha]\varphi \\ \pi &::= \top_I \,|\, U \,|\, \pi^\dagger \,|\, \pi \cdot \pi \,|\, \pi \cup \pi \,|\, \varphi? \end{aligned} \tag{8.21}$$

The formula $\top_I$ expresses I-separation and we get the top defined by $\top := \top_N$, and the action $\top_I$ represents the trivial I-local program.

The interpretation of these new formulas and programs are then given by:
- Formulas: $\|\top_I\| := \top_I^\Sigma$, $\|1\| := \overline{|1\rangle^{\otimes n}}$, and $\|+\| := \overline{|+\rangle^{\otimes n}}$
- Programs: $\|\top_I\| := \top_I^{\Sigma\times\Sigma}$

The slight difference in the interpretation of only considering a finite-dimensional Hilbert space has the advantage of every linear subspace being a closed set, *i.e.*, every linear subspace is a testable

property. However, a QDF based on a finite-dimentional Hilbert space does not satisfy property 11 of QDF definition, as seen in 4.2.10.

The fact that every linear subspace of a finite-dimensional Hilbert space is closed is useful to express the image of a quantum actions. For a deterministic program π and a formula φ assumed to be testable, we define the image of φ by π as

$$\pi(\varphi) := \pi[\varphi] \tag{8.22}$$

And for a quantum action $R = \cup_i \pi_i$ we define as

$$R(\varphi) := \bigvee_i \pi_i(\varphi) \tag{8.23}$$

This is only possible because on a finite-dimensional Hilbert space, the image of a testable property by a deterministic action is testable, thus equal to its strongest testable post-condition.

Prop. 8.2.1:

If $\pi \in \mathcal{D}$ *and* $\|\varphi\| \in \mathcal{L}$ *then* $\|\pi\|(\|\varphi\|) \in \mathcal{L}$

***Proof*:**

Since $\|\varphi\|$ is a linear function and by hypothesis $\|\varphi\| \in \mathcal{L}$, thus a linear subspace, we will have that $\|\pi\|(\|\varphi\|)$ is also a linear subspace.

Because the Hilbert space has finite dimension, we have that $\|\pi\|(\|\varphi\|)$ is closed.

Therefore $\|\pi\|(\|\varphi\|) = \overline{\|\pi\|(\|\varphi\|)} = \|\pi\|[\|\varphi\|]$. ■

With the introduction of $\top_I$ both as a formula and program, it is possible to express formulas related with I-separability and I-locality.

Given a formula φ we can express its I-component in the following way:

$$\varphi_I := \top_I \wedge \langle \top_{N\backslash I} \rangle \varphi \tag{8.24}$$

In the special case that $I = \{i\}$ we define $\varphi_i := \varphi_{\{i\}}$ for convenience.

Noticing that the first $\top_I$ expresses I-separation and the second is the trivial $N\backslash I$-local program, we see that a state satisfies φ_I iff it is I-separated and if it is possible to reach a state in φ by non-deterministic applying a $N\backslash I$-local program, *i.e.*, only changing the $N\backslash I$ *qubits*.

If we consider a state s satisfying φ such that s is I-separated, then s also satisfies φ_I, since id is a J-local for any J. In the case that all states satisfying φ are the states satisfying φ_I we say that φ is I-local, written:

$$I(\varphi) := \varphi = \varphi_I \tag{8.25}$$

Prop. 8.2.2:

Let $s \in \Sigma(\mathcal{H})$*, then*

$$s \in \|I(\varphi)\| \quad \text{iff} \quad \|\varphi\| \text{ is } I\text{−local} \tag{8.26}$$

***Proof*:**
We know that $s \in \|I(\varphi)\|$, *i.e.*, $s \in \|\varphi = \varphi_I\|$ iff $\|\varphi\| = \|\varphi_I\|$

We also know that S is I-local if exist $S' \subset \Sigma(\mathcal{H}_I)$ such that

$$S = \{s \in \Sigma \colon s_I \in S'\} \tag{8.27}$$

Note that two I-separated states w, t that differ only on the *qubits* in $N \backslash I$ will have $w_I = t_I$. Thus, if $s \in S$ is such that $s_I \in S$ then all states w that only differ in the $N \backslash I$ *qubits* are also in S. That is, for all I-local maps F

$$s \in S \quad \text{iff} \quad F(s) \in S \tag{8.28}$$

$F(s) \in S$ being true for all local maps F is equivalent to

$$\text{If } s \xrightarrow{\top_I} t \text{ then} t \in S \tag{8.29}$$

$\Leftarrow$)
If $\|\varphi\|$ is I-local then all states of $\|\varphi\|$ are I-separated, and thus, as noted before, they will be in $\|\varphi_I\|$. So $\|\varphi\| \subset \|\varphi_I\|$.

If $s \in \|\varphi_I\|$ then there exists a local map F such that $F(s) \in \|\varphi\|$ therefore $s \in \|\varphi\|$.

$\Rightarrow$)
First we notice that $\|\varphi_I\| = \|\top_I\| \cap \|\langle \top_I \rangle \varphi\|$, so if $\|\varphi\| = \|\varphi_I\|$ then all states of $\|\varphi\|$ are in $\|\top_I\|$, that is, all states of φ are I-separated.

Lets see now that if $w \in \|\varphi_I\|$ and $t \in \Sigma$ is such that $t_I = w_I$ then $t \in \|\varphi_I\|$:
We have that $t_I = w_I$ iff they only differ in the *qubits* not in I, that is, exist a I-local map F such that $F(t) = w$. Since $w \in \|\varphi_I\|$ then exists a local map G such that $G(w) \in \|\varphi\|$. Combining those maps, $G \circ F$ is still a local map and $(G \circ F)(t) \in \|\varphi\|$, *i.e*, $t \in \|\varphi_I\|$.

In order to prove that $\|\varphi\|$ is I-local, we need to show that exists $S' \subset \Sigma(\mathcal{H}_I)$ such that

$$\|\varphi\| = \{s \in \Sigma \colon s_I \in S'\} \tag{8.30}$$

With the above result, it should be clear that we must take $S' := \{w_I \colon w \in \|\varphi_I\|\}$.
We have

$$\begin{gathered} w \in \{s \in \Sigma \colon s_I \in S'\} \\ \text{iff } w_I \in S' \\ \text{iff } w \in \|\varphi_I\| \\ \text{iff } w \in \|\varphi\| \end{gathered}$$

We conclude that $\|\varphi\| = \{s \in \Sigma \colon s_I \in S'\}$. ■

Just as we can say that two propositions are logically equivalent, $\varphi = \psi$, we can now also say that two propositions are I-equivalent, written $\varphi =_I \psi$, in a straightforward way:

$$\varphi =_I \psi := \varphi \leq \top_I \wedge \psi \leq \top_I \wedge \varphi_I = \psi_I \tag{8.31}$$

That is, both φ and ψ are I-equivalent iff all the states satisfying φ and ψ are I-separated and restricting to the *qubits* in I they form the same set.

We can express a property being a local property, and it is also possible to express when a programs is a local action. However, since, as we saw, a program in $\Sigma(\mathcal{H}_n)$ is defined by the image of 3^n states, we need first to be able to express the constants that represent those states.

We have the constants 1 and $+$ that represent the states $\overline{|1\rangle^{\otimes n}}$ and $\overline{|+\rangle^{\otimes n}}$. It is easy to see that 1_i and $+_i$ represent the single *qubit* states $\overline{|1\rangle}_i$ and $\overline{|+\rangle}_i$ of $\Sigma(H^{(i)})$. Furthermore,

$$0_i := \sim 1_i \qquad\qquad -_i := \sim +_i \tag{8.32}$$

represent the states $\overline{|0\rangle}_i$ and $\overline{|-\rangle}_i$ of $\Sigma(H^{(i)})$.

Prop. 8.2.3:

Given $n > 1$ we have:

$\circ\ \|1_i\| = \{\overline{\mu_i(|1\rangle \otimes |\psi\rangle)} \colon |\psi\rangle \in \mathcal{H}_{N\setminus\{i\}}\}$ $\qquad$ $\circ\ \|0_i\| = \{\overline{\mu_i(|0\rangle \otimes |\psi\rangle)} \colon |\psi\rangle \in \mathcal{H}_{N\setminus\{i\}}\}$

$\circ\ \|+_i\| = \{\overline{\mu_i(|+\rangle \otimes |\psi\rangle)} \colon |\psi\rangle \in \mathcal{H}_{N\setminus\{i\}}\}$ $\qquad$ $\circ\ \|-_i\| = \{\overline{\mu_i(|-\rangle \otimes |\psi\rangle)} \colon |\psi\rangle \in \mathcal{H}_{N\setminus\{i\}}\}$

Now we define constants 0 and $-$ that represent $\overline{|0\rangle^{\otimes n}}$ and $\overline{|-\rangle^{\otimes n}}$ in the following way:

$$0 := 0_1 \wedge \cdots \wedge 0_n \qquad\qquad - := -_1 \wedge \cdots \wedge -_n \tag{8.33}$$

With this constants, given a vetor $\vec{c} = (c_i)_{i\in I}$ with $c_i \in \{0_i, 1_i, +_i\}$ we define:

$$\vec{c_I} := \bigwedge_{i\in I} c_i \tag{8.34}$$

This represents the state $\overline{\bigotimes_{i\in I} |c_i\rangle}$ of $\Sigma(\mathcal{H}_I)$. And now we can express all the 3^n states required for a linear map in Σ to be uniquely defined.

We express a program π being I-local, written $I(\pi)$, in the following way:

$$I(\pi) := \bigwedge_{\vec{c},\vec{d},\vec{d'}} \left(\vec{d}_{N\setminus I} =_{N\setminus I} \pi(\vec{c}_I \wedge \vec{d}_{N\setminus I}) =_I \pi(\vec{c}_I \wedge \vec{d'}_{N\setminus I})\right) \tag{8.35}$$

Where $\vec{c}, \vec{d}, \vec{d'}$ are such that c_i, d_i, d'_i range over $\{0_i, 1_i, +_i\}$.

The $N\setminus I$-equivalence is saying that π leaves the *qubits* in $N\setminus I$ unchanged, and the I-equivalence says that π is defined only by the *qubits* in I.

8.3 Axioms and Rules

The axioms and rules for compound systems will consist of all from LQP plus some new ones dealing with the properties and formulas discussed in the previous sections.

Axioms for the trivial I-local program. The program $\top_I$ is the weakest I-local program, *i.e.*:

$$I(\pi) \Rightarrow \langle\pi\rangle\varphi \leqslant \langle\top_I\rangle\varphi \tag{8.36}$$

and

$$I(\top_I) \tag{8.37}$$

Local States Axiom. Testable local properties are "local states" (*i.e.* atomic local properties): If $I \neq N$ then

$$(T(\varphi) \wedge I(\varphi) \wedge I(\psi) \wedge \psi \neq \bot \wedge \psi \leqslant \varphi) \Rightarrow \psi = \varphi \tag{8.38}$$

Basic-State Testability Axiom. The basic local states c_i and $\overline{\pi_{ij}}$ are testable: If $i, j \in N$, $c \in \{0, 1, +, -\}$ and π is deterministic, then we have

$$T(c_i) \wedge T(\overline{\pi_{ij}}) \tag{8.39}$$

Local Atomicity Rule. Local properties are unions of testable local properties (*i.e.* local states): If $I \neq N$ and the variable p does not occur in φ, ψ or θ, then

$$\begin{array}{l}\text{from } (\psi \wedge T(p_I) \wedge p_I \leqslant \varphi) \Rightarrow p_I \leqslant \theta \\ \text{infer } (\psi \wedge I(\varphi)) \Rightarrow \varphi \leqslant \theta\end{array} \tag{8.40}$$

Separation Axiom. If a state is both I-separated and J-separated, then it is also $N\backslash I$-separated, $I \cup J$-separated, and $I \cap J$-separated.

$$\top_I \wedge \top_J \Rightarrow \top_{N\backslash I} \wedge \top_{I\cup J} \wedge \top_{I\cap J} \tag{8.41}$$

Proper Superposition Axiom. States $+_i$ and $-_i$ are proper superpositions of 0_i ans 1_i.

$$+_i \Rightarrow \Diamond 0_i \wedge \Diamond 1_i \qquad\qquad -_i \Rightarrow \Diamond 0_1 \wedge \Diamond 1_i \tag{8.42}$$

Determinacy Axiom of Deterministic Programs. For deterministic programs π and π':

$$T(\varphi_i) \wedge \bigwedge_{\vec{c}\in\{0,1,+\}^n} (\pi(\vec{c}_N) = \pi'(\vec{c}_N) \Rightarrow \pi(\varphi) = \pi'(\varphi)) \tag{8.43}$$

Entanglement Axiom. This axiom captures the entanglement according to π, for π deterministic and $i \neq j$.

$$T(\varphi_i) \Rightarrow \varphi_i?(\overline{\pi_{ij}}) =_j \pi_{ij}(\varphi_i) \tag{8.44}$$

Locality Axiom for Quantum Gates. The special quantum gates introduced are local affecting only the specified *qubits*:

$$\{i\}(X_i) \wedge \{i\}(Z_i) \wedge \{i\}(H_i) \wedge \{i, j\}(CNOT_{ij}) \tag{8.45}$$

Characteristic Axioms for Quantum Gates. As an example, we will show only the characteristic axioms for quantum gates X, Z and H, as they only say how the gate operates on the basis of states:

$$\begin{array}{lll} 0_i \Rightarrow [X_i]1_i & 1_i \Rightarrow [X_i]0_i & +_i \Rightarrow [X_i]+_i \\ 0_i \Rightarrow [Z_i]0_i & 1_i \Rightarrow [Z_i]1_i & +_i \Rightarrow [Z_i]-_i \\ 0_i \Rightarrow [H_i]+_i & 1_i \Rightarrow [H_i]-_i & +_i \Rightarrow [H_i]0_i \end{array} \tag{8.46}$$

Theorem 8.3.1 (Soundness):

The proof system for Compound-Systems is sound.

Compound-System is a sound logic. However, unlike LQP, there are no known completeness results for this logic.

8.4 Results and Applications

To finalize, the correctness of the teleportation protocol will be proven at the end of this section using compound-system logic.

To do so, this section follows more closely the paper [2], providing the results that allow for showing the correctness of the teleportation protocol, and their proofs can be found in the referred paper.

Prop. 8.4.1:

Let $I \subset N$, then

$$\vdash p_I \perp q \Leftrightarrow p_I \perp q_I \tag{8.47}$$

Using the above Proposition as well as the Local Atomicity Rule and the Local States Axiom, we are able to get:

Prop. 8.4.2 (Dual Local Atomicity Rule):

If $I \neq N$, φ and θ are I-separated, and p does not occur in φ, ψ or θ, then: from

$$\vdash \psi \wedge T(p_I) \wedge p_I \perp \varphi \Rightarrow p_I \perp \theta \tag{8.48}$$

infer

$$\vdash \psi \wedge T(\varphi_I) \wedge T(\theta_I) \Rightarrow \varphi =_I \theta \tag{8.49}$$

A very important result from Quantum Mechanics can be proven using this logic - a sufficient condition for two deterministic quantum programs commuting is that they should affect different *qubits*.

Theorem 8.4.3 (Compatibility of Programs Affecting Different Qubits):

If $I \cap J = \varnothing$ and π, π' are deterministic, then

$$\vdash I(\pi) \wedge J(\pi') \Rightarrow \pi \cdot \pi'(p) = \pi' \cdot \pi(p) \tag{8.50}$$

We can also prove some results about entanglement, in particular, the Dual Local Atomicity Rule and the above result on quantum programs we get:

Prop. 8.4.4 (Dual Entanglement):

If π is deterministic and $i \neq j$, then

$$\vdash T(q_j) \Rightarrow q_j?(\overline{\pi_{ij}}) =_i \pi_{ij}^{\dagger}(q_j) \tag{8.51}$$

On the other hand, using the Entanglement Axiom we can prove the following:

Prop. 8.4.5 (Entanglement preparation Lemma):

$$\pi_{ij}(p_i) \perp q_j \Rightarrow \overline{\pi_{ij}} \perp (p_i \wedge q_j) \tag{8.52}$$

Theorem 8.4.6 (Teleportation Property):

If i, j, k are distinct indices, then

$$\vdash (\overline{\sigma_{jk}}? \cdot \overline{\pi_{ij}}?)(p_i) =_k (\pi_{ij} \cdot \sigma_{jk})(p_i) \tag{8.53}$$

Corollary 8.4.7:

If i, j, k are distinct then

$$\vdash \overline{\pi_{ij}}?(p_i \wedge \overline{\sigma_{jk}}) =_k (\pi_{ij} \cdot \sigma_{jk})(p_i) \tag{8.54}$$

By defining the domain of a quantum action π as $dom(\pi) := \langle\pi\rangle\top$, we have a condition for when two I-local maps agree on *qubits* not in I.

Theorem 8.4.8 (Agreement Property):

If two I-local maps π, π' have the same domain and they separate the input-state, then their output states agree on all non-I qubits, i.e., for all deterministic π, π' we have:

$$\vdash (T(p) \wedge I(\pi) \wedge I(\pi') \wedge dom(\pi) = dom(\pi') \wedge \pi(p) \leqslant \top_I \wedge \pi'(p) \leqslant \top_I) \Rightarrow \pi(p) =_{N \setminus I} \pi'(p) \tag{8.55}$$

Finally, from the rules of quantum gates and with $\beta_{xy}^{ij} := \overline{(Z_1^x \cdot X_1^y)}_{ij}$ we have

Prop. 8.4.9:

For all $x, y \in \{0, 1\}$:

$$\vdash (H_i \cdot CNOT_{ij})(x_i \wedge y_j) = \beta_{xy}^{ij} \tag{8.56}$$

Corollary 8.4.10:

If i, j, k are all distinct

$$\vdash (CNOT_{ij} \cdot H_j \cdot (x_i \wedge y_j)?(p) =_k \beta_{xy}^{i,j}?(p)) \tag{8.57}$$

8.4.1 Correctness of the Teleportation Protocol

Now we these results we shall see the correctness of the teleportation protocol.

The teleportation protocol has the following quantum program:

$$\pi = \bigcup_{x,y \in \{0,1\}} CNOT_{12} \cdot H_1 \cdot (x_1 \wedge y_2)? \cdot X_3^y \cdot Z_3^x \tag{8.58}$$

And its correctness is expressed by

$$\vdash \pi(q_1 \wedge \beta_{00}^{23}) =_3 id_{13}(q_1) \tag{8.59}$$

Considering Alice has the first and second *qubits*, with the first being the one she wants Bob to have, then the state of the third *qubit* after performing the teleportation algorithm, that is π, is the same as changing the third *qubit* to have the value of the first, that is, performing id_{13}, which is what is required of the algorithm.

The sketch of the proof in [2] goes as follows:

Using Corollary 8.4.10 with $i = 1$, $j = 2$ and $k = 3$, we need to prove that

$$\vdash (\beta_{xy}^{12}? \cdot X_3^y \cdot Z_3^x)(q_1 \wedge \beta_{00}^{23}) =_3 id_{13}(q_1) \tag{8.60}$$

Using the definition of β_{xy}^{ij} we can rewrite it as

$$\vdash (\overline{(Z_1^x \cdot X_1^y)}_{12}? \cdot X_3^y \cdot Z_3^x)(q_1 \wedge \overline{id}_{23}) =_3 id_{13}(q_1) \tag{8.61}$$

From the corollary of the Teleportation Property we can write

$$\vdash \overline{(Z_1^x \cdot X_1^y)}_{12}?(q_1 \wedge \overline{id}_{23}) =_3 ((Z_1^x \cdot X_1^y)_{12} \cdot id_{23})(q_1) \tag{8.62}$$

Knowing that $X^{-1} = X$ and $Z^{-1} = Z$ we have that $Z^x \cdot X^y \cdot X^y \cdot Z^x = id$.

Together above result, we reach the desired result that teleportation protocol is correct.

Conclusion

The goal of this thesis was to introduce dynamic quantum logic for quantum programs in a self contained manner to make it easier to those who wish to learn about it.

There were two obstacles to tackle. The first being the lack material on the topic besides the original paper ([1] and [2]) which contained very few proofs. The second being that this logic is build upon several areas - Quantum Logic, Dynamic Logic and Quantum Computation. Both made learning the subject harder and time consuming.
For the first obstacle, detailed proofs were given to the results used in the papers cited above. To tackle the second problem it was necessary to include chapters with the basics of those areas required for the logic.

Bibliography

[1] A. Baltag and S. Smets. Complete Axiomatizations for Quantum Actions. *International Journal Theoretical Physics* 44 (2005).

[2] A. Baltag and S. Smets. LQP: The dynamic logic of quantum information. *Mathematical Structures in Computer Science* 16 (2006).

[3] G. Birkhoff and J. von Neumann. The logic of quantum mechanics, *Annals of Mathematics. Second Series* 37 (1936).

[4] M. Dalla Chiara, R. Giuntini, and R. Greechie. Reasoning in quantum theory, *Trends in Logic—Studia Logica Library* 22 (2004).

[5] K. Engesser, D. Gabbay, and D. Lehmann. *Handbook of Quantum Logic and Quantum Structures: Quantum Logic* (2009).

[6] K. Engesser, D. Gabbay, and D. Lehmann. *Handbook of Quantum Logic and Quantum Structures: Quantum Structures* (2007).

[7] P. Dirac. *The Principles of Quantum Mechanics*, fourth edition (1967).

[8] W. Rudin. Real and complex analysis, *McGraw-Hill Series in Higher Mathematics*, second edition (1974).

[9] G. Birkhoff. Lattice theory. *American Mathematical Society Colloquium Publications*, Vol. XXV (1967).

[10] D. Harel, J. Tiuryn and D. Kozen. *Dynamic Logic* (2000).

[11] P. Blackburn, M. de Rijke, and Y. Venema. Modal logic. *Cambridge Tracts in Theoretical Computer Science* 53 (2001).

[12] M. Nielsen and I. Chuang. Quantum computation and quantum information. *Cambridge University Press, Cambridge* (2000).