Doctoral Dissertation

Quantum Dynamic Algebra: From Orthomodular Lattice to Algebra of Quantum Programs

Tsubasa Takagi

Supervisor: Kazuhiro Ogata

Graduate School of Advanced Science and Technology
Japan Advanced Institute of Science and Technology

(Information Science)

September, 2023

Abstract

Quantum Logic is the logic of quantum mechanics, originated by von Neumann and Birkhoff in 1936. Half a century later, computation based on quantum mechanics, namely quantum computation, was invented and has developed dramatically up to the present day. Therefore, it is expected to incorporate the viewpoint of quantum computation to reformulate Quantum Logic into a modern logic.

In this dissertation, we study algebraic structures. The algebraic structure of Quantum Logic is known as orthomodular lattices, which are abstractions of the sets of all closed subspaces of Hilbert spaces. Orthomodular lattices are challenging to deal with because the distributive law does not hold. Besides that, orthomodularity is not determined by any first-order properties of the accessibility relation of Kripke frames for Quantum Logic. These features are not found in other well-known algebraic structures of logics, such as Boolean lattices (Classical Logic), Heyting lattices (Intuitionistic Logic), or Modal algebras (Modal Logic).

Interestingly, orthomodular lattices, with these hard-to-handle properties, can be made easier to deal with by adding the notion of quantum programs. This is another motivation for extending orthomodular lattices to algebra of quantum programs. Incorporating a quantum computation perspective into orthomodular lattices is not only beneficial for its reformulating as modern algebras, but also from a technical point of view.

We name the algebra of quantum programs Quantum Dynamic Algebra (QDA). QDA is constructed by combing the algebra of quantum mechanics (orthomodular lattices), Regular Program Algebra, and Modal Algebra. The quantum programs that QDA can express are limited to regular programs. However, regular programs are expressive enough to describe various programs, such as conditional programs, guarded commands, while programs, and until programs. The interpretation of tests in QDA differs from that in Dynamic Algebra (the algebra of classical programs): tests are interpreted as the execution of projective measurement in quantum mechanics. Because the execution of projective measurement may change the current state, there is no corresponding notion in Dynamic Algebra.

QDA provides the algebraic foundation for quantum program verification. We show that the inference rules in Hoare Logic are valid in QDA if the usual conjunc-

tion is replaced by the Sasaki conjunction. The validity of the Hoare-like inference rules means that the inference rules in Hoare Logic also work in the quantum setting as long as the appropriate logical connective(s) are chosen. Behind this is the fact that the more fundamental law called the law of residuation holds if the usual conjunction is replaced by the Sasaki conjunction in Quantum Logic. The law of residuation is significant because the law corresponds to one of the most significant theorems called the deduction theorem in logics, such as Classical Logic, Intuitionistic Logic, Modal Logic. More generally, algebras that satisfy the law of residuation give algebraic semantics for various substructural logics. There has been no discussion of this kind of relevance to the field of logic (not only Hoare Logic) in existing studies.

Another achievement of this study is to show the Stone-type representation theorem for QDA at the cost of simplifying QDA to star-free (iteration-free) QDA. It is traditionally known that the iteration operator is challenging to deal with. For example, the Stone-type representation theorem has been proved only for star-free (Classical) Dynamic Algebra. The difficulty arises because the iterative operator allows the existence of non-standard Kripke models. Even for star-free QDAs, the proof of the Stone-type representation theorem is not straightforward. (Star-free) QDA is made up of a complex combination of multiple algebras, namely an orthomodular lattice, a regular program algebra, and a modal algebra. It is not apparent to prove the Stone-type representation theorem consistent with all these algebras.

Proving Stone-type representation theorems is significant because it reveals the relation between algebraic semantics and Kripke semantics. The most well-known Stone-type representation theorem is Stone's representation theorem for Boolean lattices. The theorem is extended to Jónsson–Tarski theorem, also known as the Stone-type representation theorem for modal algebras. However, although the algebraic structure of DQL is an extension of the modal algebra, its Stone-type representation theorem has not been known so far.

In summary, we formulate QDA for reformulating the algebraic structure of quantum mechanics into a modern algebra from the perspective of quantum computation. We also show the Stone-type representation theorem for its star-free fragment, which ensures the theoretical adequacy of QDA. Furthermore, it is expected to apply QDA to quantum program verification because Hoare-like inference rules are valid in QDA.

Key Words: Orthomodular Lattice, Dynamic Algebra, Sasaki Conjunction, Quantum Program Verification, Stone-type Representation Theorem

Acknowledgments

First and foremost, I am extremely grateful to my supervisor, Professor Kazuhiro Ogata, for his invaluable guidance from the perspective of computer science to improve my work. Moreover, he gave me many opportunities to present my studies. He financially supported me in making my paper open-access. Besides that, he encouraged me to present my papers at international conferences.

Also, I would like to express my sincere gratitude to the people who helped me to conduct my research. Dr. Canh Minh Do collaborated with me by implementing my ideas. Mr. Minoru Koga made many suggestions for improving this dissertation. Dr. Tomoaki Kawano and Mr. Yosuke Watanabe gave me feedback on my research on numerous occasions in Tokyo Institute of Technology and Nagoya University, respectively.

Furthermore, I am deeply indebted to many researchers in JAIST, especially Professor Emeritus Satoshi Tojo and Hiroakira Ono, who gave me a lot of advice during my master's program. I have been greatly assisted by them in maturing as a scholar. I also thank the dissertation committee members, Professor Kazuhiro Ogata, Kunihiko Hiraishi, Nao Hirokawa, Takashi Tomita, Satoshi Tojo, and Ryo Kashima, for their helpful comments on a draft of this dissertation.

I welcome this opportunity to thank those who were not directly involved in my research. Mr. Takumi Ueda, Xinyu Wang, and Yudai Kubono spent much time with me, teaching each other to learn basic notions in mathematical logic. They also gave me so much help in my school life. I got friends I will never forget.

This work was supported by Grant-in-Aid for JSPS Research Fellow Grant Number 22J23575. I could not have accomplished this work without this research grant.

Nomi, Japan

Tsubasa Takagi

Contents

Chapter 1

Introduction

1.1 Background

Quantum computing has the potential to transform various computing applications by offering the ability to solve problems that are currently infeasible for classical computing, such as Shore's fast algorithm for integer factoring and Grover's algorithm for unstructured search. However, quantum computing is counter-intuitive and distinct from classical computing, which makes it challenging to design and implement quantum protocols, algorithms, and programs accurately. Therefore, it is crucial to ensure their correctness through verification. While existing logics/algebras can be used to verify that classical systems enjoy some desired properties, they cannot be directly applied to quantum systems due to the distinct principles used in quantum computing. Therefore, new formal verification techniques are necessary for quantum systems.

The purpose of this study is to extend orthomodular lattices known as the algebraic structure of Quantum Logic into a modern algebraic structure by reconsidering it from the viewpoint of quantum computation. First of all, we explain the background of the logics relevant to this study.

Quantum Logic

Quantum Logic is the logic of quantum mechanics, originated by von Neumann and Birkhoff in 1936 [10]. Although the mathematical structure of quantum mechanics was clarified by von Neumann in his book "Mathematische Grundlagen der Quantenmechanik" in 1932, the axioms of quantum mechanics were not experimentally testable in comparison with the axioms of classical mechanics (Newton's law of motion). Therefore, von Neumann tried to reconstruct quantum mechanics by constructing a logic from only experimentally testable propositions (observable

propositions). Von Neumann discovered that Quantum Logic has a lattice structure by collaborating with Birkhoff, a researcher who had made great achievements in lattice theory: Quantum Logic is a lattice consisting of closed subspaces of a Hilbert space. [33] is the standard textbook in this field.

Dynamic Logic

Dynamic Logic is a logic of programs originated by Pratt in 1976 [32]. Dynamic Logic describes the execution of regular programs, namely, programs described by regular expressions and tests, using modal operators. Dynamic Logic is a kind of modal logics with different modal operators for each regular program. It is also an extension of Hoare Logic in that it can deal with more complex programs than those dealt with by Hoare Logic. In particular, because the weakest preconditions can be described using the modal operators of Dynamic Logic, the inference rules of Hoare Logic can be verified from a more fundamental level in Dynamic Logic. [20] is the standard textbook in this field.

Dynamic Quantum Logic

Dynamic Quantum Logic (DQL) [4] is a logic of *quantum* programs originated by Baltag and Smets in [2]. As Dynamic Logic is utilized for classical program verification, DQL is utilized for *quantum* program verification. Specifically, some quantum protocols (written as quantum programs), such as Quantum Teleportation [3], Quantum Secret Sharing [3], the quantum search algorithm [1], Quantum Leader Election Protocol [1, 9], and the BB84 quantum key distribution protocol [9] have been verified using DQL. [5] provides a comprehensive overview of this field.

DQL is a variant of (Propositional) Dynamic Logic. The key idea of DQL is that tests used in guard clauses called tests are not interpreted as formulas in Classical Logic. It reflects the feature of tests in quantum programs: quantum tests represent projective measurement and are interpreted as formulas in Quantum Logic. Different from classical tests, quantum tests may change a current state after executing them. More interestingly, [2] found that the weakest precondition $[p?]q$ of such a quantum test $p?$ with respect to a postcondition q is identical to the implication $p \rightsquigarrow q$ in Quantum Logic called the Sasaki hook [21]. Thus, we see that quantum tests are implications in Quantum Logic. This fact makes a strong connection between quantum programs and Quantum Logic.

1.2 Motivation

The previous studies of DQL lacked two things. One is the iteration (Kleene star) operator of quantum programs, and the other is a representation theorem.

The reason why the previous studies of DQL lacked the iteration operator is that it was not necessary to use the iteration operator to construct a prototype of DQL in the earlier stage. Baltag and Smets, the initiators of DQL, stated that "Notice that we did not include *iteration* (Kleene star) among our program constructs: this is only because we do not need it for any of the applications in this paper" in [3]. It does not mean that it is not worth adding the iteration operator to DQL. Using the iteration operator is necessary to deal with quantum while loops. For example, quantum while loops are used in the quantum walk algorithms for repeatedly choosing quantum programs corresponding to "Left" or "Right." Moreover, it is significant to discuss the iteration operator of quantum programs for connecting DQL to a considerable amount of previous research on finite quantum automata.

Representation theorems give an alternative characterization of a mathematical structure. Among the many representation theorems, this dissertation focuses on Stone-type representation theorems. The most well-known Stone-type representation theorem is Stone's representation theorem for Boolean lattices. The theorem states that every Boolean lattice is embeddable into its canonical extension. Because the canonical extension of a Boolean lattice is an algebra of sets, the theorem also states that every Boolean lattice is "represented" by an algebra of sets. The theorem is extended to Jónsson–Tarski theorem [24], which is also known as the Stone-type representation theorem for modal algebras. However, although the algebraic structure of DQL is an extension of the modal algebra, its Stone-type representation theorem has not been known so far. To prove the Stone-type representation theorem is significant because it reveals the relation between algebraic semantics and Kripke semantics of DQL.

1.3 Method

To tackle the two problems in the previous section, we choose an algebraic formulation of DQL. One of the advantages of the algebraic approach is that infinite conjunction/disjunction can be easily dealt with as infimum/supremum (or meet/join). On the other hand, almost all logics cannot deal with it (one exception is Infinitary Logic, but it is less well-known and studied). The iteration operator is straightforwardly defined using infinite conjunction (infimum). Besides that, the algebraic approach brings new developments by reviewing logic from the algebraic perspective. For example, Stone-type representation theorems for various

logics were obtained from the algebraic perspective, and these logics were related to topology. Furthermore, the algebraic approach allows us to avoid discussions about inference rules specific to each logic and concentrate on the study of semantics. The usual Hilbert-style proof system for DQL is tough to deal with in that it is challenging to automate proofs in the proof system.

1.4 Results

We define an algebra of regular quantum programs with the iteration operator. We name it Quantum Dynamic Algebra (QDA). QDA is constructed by combining the algebra of quantum mechanics (orthomodular lattices), Regular Program Algebra, and Modal Algebra.

Furthermore, to make QDA a more practical tool for the purpose of formal verification, we discuss the relation to Hoare Logic. We clarify that the inference rules in Hoare Logic are sound if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\barwedge$. Besides that, apply the Hoare-like inference rules to verify the partial correctness of simple quantum programs.

Note that this study focuses on an abstraction of the concrete quantum structure. For example, we discuss orthomodular lattices, which are abstractions of Hilbert lattices (the lattice that consists of all closed subspaces of a Hilbert space) in that orthomodular lattices have some essentially significant properties of Hilbert lattices. This is because the concrete quantum structure is much more difficult to deal with than its abstraction. This strategy has usually been adopted in studies of Quantum Logic. What an abstraction satisfies is also satisfied in its concrete example, thus it is meaningful to focus on the abstraction.

Finally, we prove the Stone-type representation theorem for QDA at the cost of simplifying QDA to star-free (iteration-free) QDA. It is traditionally known that the iteration operator is difficult to deal with. For example, the Stone-type representation theorem has been proved only for star-free (Classical) Dynamic Algebra [26]. The difficulty arises because the iterative operator allows the existence of non-standard Kripke models [15]. Even for star-free QDAs, the proof of the Stone-type representation theorem is not straightforward. QDA is made up of a complex combination of multiple algebras, namely an orthomodular lattice, a regular program algebra, and a modal algebra. It is not obvious to prove the Stone-type representation theorem consistent with all these algebras.

The most significant implication of this study is a new development from orthomodular lattice to algebra of quantum programs. That is, QDA bridges the gap between the algebraic structure of Quantum Logic and quantum computation. QDA is expected to be used to verify the weakest preconditions for specific quantum computation algorithms, quantum communication protocols, or quantum

cryptography protocols.

1.5 Related Work

Some different approaches share similar ideas. Here we compare these approaches to QDA.

Quantum Hoare Logic (QHL) by [37] was designed to be a quantum counterpart of Hoare Logic. Among the various variants of QHL, Applied Quantum Hoare Logic (AQHL) by [40] is particularly relevant to QDA. AQHL is a restriction of QHL in that preconditions and postconditions are projections. Similarly, preconditions and postconditions represented by QDA are also intended to be projections (more precisely, closed subspaces that correspond one-to-one to closed subspaces).

Compared to (A)QHL, QDA can express more fundamental components of quantum programs: if-then programs and while-do programs are atomic programs in (A)QHL. However, these programs are further divided into more basic programs in QDA. For example, the **if** $\cdots$ **fi** statement that represents a non-deterministic measurement cannot be divided anymore in (A)QHL. On the other hand, QDA can express its non-deterministic feature explicitly using the non-deterministic choice operator $\cup$. Also, QDA can express (projective) measurements by tests. However, the test operators are not included in the syntax of (A)QHL. Tests can be converted into implications in Classical/Quantum Dynamic Logic/Algebra. Thus, tests can be replaced by simpler expressions under certain conditions. This is the reason for focusing on tests.

Non-idempotent Kleene Algebra with Tests (NKAT) was employed for quantum compiler optimization by [31]. Both QDA and NKAT can express regular expressions and tests (namely, regular programs), unlike (A)QHL. Also, both can be used for verifying the partial correctness of regular programs.

Compared to NKAT, QDA can convert $\Box(p?, q)$ with a test $p?$ to simpler form, the implication $p \rightsquigarrow q$ in Quantum Logic called the Sasaki hook [21]. Recall that the implication $p \to q$ in Classical Logic is equivalent to $\neg p \vee q$. Similarly, $p \rightsquigarrow q$ is equivalent to $\neg p \vee (p \wedge q)$ (but note that the meaning of logical connectives in Classical Logic and Quantum Logic are different). The static formula $\neg p \vee (p \wedge q)$ is simpler than the dynamic (or modal) formula $\Box(p?, q)$ because state transitions are needed to evaluate $\Box(p?, q)$ from the perspective of semantics due to its dynamic operator $p?$. This advantage of QDA is inherited from DQL. Besides that, the difference between (classical) Dynamic Algebra and (idempotent) Kleene Algebra with Tests (KAT) is also the difference between QDA and NKAT.

1.6 Contributions

In the previous section, we pointed out that QDA can analyze the most fundamental components of quantum programs defined by the syntax of QHL furthermore. Owing to this feature of QDA, quantum analogs of the inference rules in Hoare Logic can be verified from a more fundamental starting point. That is, these inference rules are verified based on quantum counterparts of the law of residuation and the loop invariance rule. Focusing on the law of residuation is meaningful from the perspective of logic because the law corresponds to one of the most significant theorems called the deduction theorem in logics, such as Classical Logic, Intuitionistic Logic, Modal Logic. More generally, algebras that satisfy the law of residuation give algebraic semantics for various substructural logics (see [29]). There has been no discussion of this kind of relevance to the field of logic (not only Hoare Logic) in existing studies.

Note that the Hoare-like inference rules (Theorem 4.2.4) differ from that of (A)QHL in that the Sasaki conjunction $\Cap$ is used. The Hoare-like inference rules in this dissertation are more similar to the original inference rules in Hoare Logic because the usual conjunction $\wedge$ is just replaced by $\Cap$. The validity of the Hoare-like inference rules in this dissertation means that the inference rules in Hoare Logic also work in the quantum setting as long as the appropriate logical connective(s) are chosen.

Another contribution of this study is to establish a new method to prove a Stone-type representation theorem. It is known that orthomodularity is not elementary [14], which means that orthomodularity is not determined by any first-order properties of the accessibility relation of Kripke frames for Quantum Logic. Due to this fact, it is challenging to show Stone-type representation theorems for orthomodular lattices. Because QDA is an orthomodular lattice, we need some new ideas to overcome this difficulty. For this, we use the Kripke frames for QDA with two kinds of accessibility relations. One accessibility relation is an abstraction of the orthogonality relation, and the other accessibility relations are abstractions of the graphs of unitary operators (quantum gates).

From a more general standpoint, we also contribute to formulating a new quantum counterpart of the existing algebra of programs (namely, Dynamic Algebra) with its potential for application. Because the verification of quantum programs is in its early stage, there is still no established theory. Therefore, it is significant to accumulate candidate theories for quantum program verification by proposing various possibilities. Such accumulation will assist in developing a new appropriate theory by combining these candidates.

1.7 Organisation of the Dissertation

The rest of the dissertation is organized as follows. In Chapter 2, we review some basic notions related to the subsequent parts of this dissertation. In Chapter 3, we review some Stone-type representation theorems, namely the Stone-type representation theorems for Boolean lattices (Theorem 3.3.3), for ortholattices (Theorem 3.4.16), and for modal algebras (Theorem 3.5.6). In Chapter 4, we formulate QDA, and show that the inference rules of Hoare Logic are satisfied in QDA if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\Cap$ (Theorem 4.2.4). Moreover, we formulate a transition system called a Quantum Dynamic Frame (QDF) and how to construct a QDA from a given QDF (Theorem 4.4.5). We use the constructed QDA called the complex algebra of a QDF for verifying the correctness of two simple quantum programs as running examples. In Chapter 5, we show how to construct a star-free QDA from a given star-free QDF (Theorem 5.3.4) and how to construct a star-free QDF from a given star-free QDA (Theorem 5.4.4). We apply these construction methods to prove our main theorem, the Stone-type representation theorem for star-free QDAs (Theorem 5.5.3). Finally, in Chapter 6, we summarize and discuss the significant results drawn in this dissertation. Also, we suggest some future work.

Chapter 2

Basic Notions

This chapter contains:

In this chapter, we review some basic notions related to the subsequent parts of this dissertation.

2.1 Order

Definition 2.1.1. Let L be a non-empty set. A relation $\leq$ on L is said to be

- **reflexive** if $p \leq p$ for any $p \in L$.
- **transitive** if $p \leq q$ and $q \leq r$ jointly imply $p \leq r$ for any $p, q, r \in L$.
- **antisymmetric** if $p \leq q$ and $q \leq p$ jointly imply $p = q$ for any $p, q \in L$.
- **strongly connected** if $p \leq q$ or $q \leq p$ for any $p, q \in L$.

A relation $\leq$ on L is called

- a **preorder** (also called a **quasi-order**) if $\leq$ is reflexive and transitive.
- a **partial order** if $\leq$ is an antisymmetric preorder.

- a **total order** (also called a **linear order**) if $\leq$ is a strongly connected partial order.

A non-empty set L with a preorder $\leq$ on L, denoted $(L, \leq)$, is called a **preordered set**. Similarly, a **partially ordered set** (also called a **poset**) and **totally ordered set** are defined. A **chain** in L is a non-empty totally ordered subset of L. We write $p < q$ to mean the condition that $p \leq q$ and $p \neq q$.

Example 2.1.2.

(1) The set $\mathbb{R}$ of real numbers is a totally ordered set with its usual order $\leq$.

(2) The powerset $\wp(S)$ of a set S is a partially ordered set with the inclusion relation $\subseteq$. However, $\wp(S)$ is not a totally ordered set with $\subseteq$ if S has two or more elements because a singleton (a set with exactly one element) is incomparable to another singleton. That is, neither $\{p\} \subseteq \{q\}$ nor $\{q\} \subseteq \{p\}$ if $p \neq q$.

(3) Denote a finite set by S and the number of elements in $P \subseteq S$ by $|P|$. Then $\wp(S)$ is a preordered set with $\preceq$ such that $P \preceq Q$ is defined by $|P| \leq |Q|$, where $\leq$ stands for the usual order on natural numbers. The set $\wp(S)$ is not a partially ordered set with $\preceq$ because $\{p\} \leq \{q\}$ and $\{q\} \leq \{p\}$ but $\{p\} \neq \{q\}$ for any distinct elements p and q.

(4) A set may be ordered by different orders. The set $\mathbb{N}$ of natural numbers without 0 is a totally ordered set with the usual order $\leq$ and is a partially ordered set with the relation $|$ of divisibility ($n|m$ if and only if n divides m). The relation $|$ is not a total order because 3 is incomparable to 5 by $|$, for example.

Remark 2.1.3. In some cases, L is allowed to be empty in the definition of ordered sets. Because $\emptyset$ is the only subset of $\emptyset \times \emptyset$, a relation on $\emptyset$ must be $\emptyset$ itself. In this sense, $\emptyset$ is the only total order on $\emptyset$.

The following theorem gives a general procedure for constructing the partially ordered set $L/\!\sim$ with $\leq_\sim$ from a preordered set L with $\leq$.

Theorem 2.1.4. Let $(L, \leq)$ be a preordered set and $\sim$ be a relation on L such that $p \sim q$ is defined by the condition that $p \leq q$ and $q \leq p$. Then $\sim$ is an equivalence relation. Furthermore, the quotient set $L/\!\sim$ is a partially ordered set with $\preceq$ such that $[p] \preceq [q]$ defined by $p \leq q$, where $[p]$ denotes the equivalence class of p.

Proof. Straightforward. □

Definition 2.1.5. Let L be a partially ordered set with $\leq$ and Γ be a subset of L. An element $p \in L$ is called

- the **least element** (also called the **minimum**) of L, denoted $\curlywedge$, if $p \leq q$ for any $q \in L$.
- the **greatest element** (also called the **maximum**) of L, denoted $\curlyvee$, if $q \leq p$ for any $q \in L$.
- a **minimal element** of L if $q \leq p$ implies $q = p$ for any $q \in L$.
- a **maximal element** of L if $p \leq q$ implies $p = q$ for any $q \in L$.

Example 2.1.6.

(1) The totally ordered set $\mathbb{R}$ with the usual order $\leq$ has neither the least element nor the greatest element.

(2) The partially ordered set $\wp(S)$ with the inclusion relation $\subseteq$ has the least element $\emptyset$ and the greatest element $\wp(S)$.

Remark 2.1.7. Do not confuse the least elements (greatest elements) with minimal elements (maximal elements). Although the least elements and greatest elements are unique when they exist, minimal elements and maximal elements may not. The least elements (greatest elements) are global notions, but minimal elements (maximal elements) are local notions.

Definition 2.1.8. Let L be a partially ordered set with $\leq$ and Γ be a subset of L. An element $p \in L$ is called

- a **lower bound** of Γ if $p \leq q$ for any $q \in \Gamma$.
- the **infimum** (also called **meet**) of Γ, denoted $\bigwedge \Gamma$, if p is the greatest lower bound of Γ:
  (1) p is a lower bound of Γ, and
  (2) $q \leq p$ for any lower bound q of Γ.
- an **upper bound** of Γ if $q \leq p$ for any $q \in \Gamma$.
- the **supremum** (also called **join**) of Γ, denoted $\bigvee \Gamma$, if p is the least upper bound of Γ:
  (1) p is a upper bound of Γ, and
  (2) $p \leq q$ for any upper bound q of Γ.

Example 2.1.9.

(1) Consider the totally ordered set $\mathbb{R}$ with the usual order $\leq$. The property known as the least upper bound property of $\mathbb{R}$ is as follows: every non-empty set of $\mathbb{R}$ that has an upper bound have the supremum. For example, $\{x \in \mathbb{R} : x^2 < 2\}$ has the supremum $\sqrt{2} \in \mathbb{R}$. As is seen from this example, the supremum (infimum) of Γ may not exist in Γ.

(2) For each $\Gamma \subseteq \wp(S)$, define $\bigcap \Gamma$ and $\bigcup \Gamma$ by

$$\bigcap \Gamma = \bigcap_{P \in \Gamma} P = \{p : p \in P \text{ for any } P \in \Gamma\},$$
$$\bigcup \Gamma = \bigcup_{P \in \Gamma} P = \{p : p \in P \text{ for some } P \in \Gamma\}.$$

In the partially ordered set $\wp(S)$ with the inclusion relation $\subseteq$, the infimum of Γ is $\bigcap \Gamma$, and the supremum of Γ is $\bigcup \Gamma$. For the proof, see Theorem 2.1.10.

(3) Let L be a partially ordered set with $\curlywedge$ and $\curlyvee$. Then because any $p \in L$ is a lower (upper) bound of $\emptyset$, we have $\bigwedge \emptyset = \curlyvee$ (dually, $\bigvee \emptyset = \curlywedge$).

Theorem 2.1.10. For each $\Gamma \in \wp(S)$, $\bigwedge \Gamma = \bigcap \Gamma$ and $\bigvee \Gamma = \bigcup \Gamma$ in the partially ordered set $\wp(S)$ with the inclusion relation $\subseteq$.

Proof. We only prove the case of $\bigwedge$. For any $P \in \Gamma$, we have $\bigcap \Gamma \subseteq P$. Thus, $\bigcap \Gamma$ is a lower bound of Γ. It remains to show that if $Q \subseteq P$ for any $P \in \Gamma$, then $Q \subseteq \bigcap \Gamma$. Take any element p in Q. Then $p \in P$ for any $P \in \Gamma$, and thus $p \in \bigcap P$. Therefore, $Q \subseteq \bigcap \Gamma$. □

Lemma 2.1.11 (Zorn's Lemma)**.** Let L be a partially ordered set with $\leq$. If any chain in L has an upper bound in L, then L has a maximal element with respect to $\leq$.

Proof. Because some knowledge (not relevant to the main topic of this paper) is required to prove Zorn's lemma, it is omitted here. □

2.2 Lattice

Definition 2.2.1. A **lattice** $(L, \leq)$ is a partially ordered set that $\bigwedge\{p, q\}$ and $\bigvee\{p, q\}$ exist in L for any $p, q \in L$. Hereafter, we write $p \wedge q$ and $p \vee q$ instead of $\bigwedge\{p, q\}$ and $\bigvee\{p, q\}$, respectively. A lattice $(L, \leq)$ is said to be

- **finite** if L is a finite set.

- **bounded** if $\curlywedge$ and $\curlyvee$ exist (in L).
- **complete** if $\bigwedge \Gamma$ and $\bigvee \Gamma$ exist (in L) for each $\Gamma \subseteq L$.

A bounded lattice $(L, \leq)$ is said to be **trivial** if $\curlywedge = \curlyvee$.

Hereinafter, we only consider non-trivial lattices. If trivial lattices are allowed, $S^{\mathcal{L}}$ in Definition 3.4.12 can be the empty set, and then Theorem 3.4.13 does not hold. For example, [35, p.8] supposes non-triviality in the definition of bounded lattices. Excluding trivial lattices does not affect the essence of the discussion that follows.

Example 2.2.2.

(1) The set $\mathbb{R}$ of real numbers with the usual order $\leq$ forms a lattice $(\mathbb{R}, \leq)$. However, $(\mathbb{R}, \leq)$ is neither bounded nor complete because $\bigvee \mathbb{R}$ does not exist in $\mathbb{R}$. Whereas $\mathbb{R}$ has the least upper bound property (recall Example 2.1.9 (1)).

(2) The closed interval

$$[-2, 2] = \{x \in \mathbb{R} : -2 \leq x \leq 2\}$$

with the usual order $\leq$ forms a lattice $([-2, 2], \leq)$. In fact, $([-2, 2], \leq)$ is bounded and complete (distinguish from bounded completeness). In general, $([a, b], \leq)$ is a bounded and complete lattice, provided that $a \leq b$.

(3) Let $\mathbb{Q}$ be rational numbers. The set

$$[\![-2, 2]\!] = \{x \in \mathbb{Q} : -2 \leq x \leq 2\}$$

with the usual order $\leq$ forms a lattice $([\![-2, 2]\!], \leq)$ and is bounded. However, $([\![-2, 2]\!], \leq)$ is not complete because $\bigvee\{x \in \mathbb{Q} : x^2 < 2\}$ does not exist in $[\![-2, 2]\!]$.

(4) There are no examples that are not bounded but complete. Every complete lattice $(L, \leq)$ is bounded because $\bigvee \emptyset = \bigwedge L = \curlywedge$ and $\bigwedge \emptyset = \bigvee L = \curlyvee$ exist.

(5) The powerset $\wp(S)$ of a set S with the inclusion relation $\subseteq$ forms a lattice $(\wp(S), \subseteq)$ and is called a **powerset lattice**. In fact, $(\wp(S), \subseteq)$ is complete because $\bigwedge \Gamma = \bigcap \Gamma \in \wp(S)$ and $\bigvee \Gamma = \bigcup \Gamma \in \wp(S)$ for each $\Gamma \subseteq \wp(S)$ (see Theorem 2.1.10).

Hereafter, we use the following three useful lemmas without mentioning these lemmas explicitly. Keep in mind these statements.

Lemma 2.2.3. The following conditions are equivalent:

(1) $p \leq q_1$ and $p \leq q_2$;

(2) $p \leq q_1 \wedge q_2$.

Dually, the following conditions are also equivalent:

(1) $q_1 \leq p$ and $q_2 \leq p$;

(2) $q_1 \vee q_2 \leq p$.

Proof. Assume that $p \leq q_1$ and $p \leq q_2$. Then p is a lower bound of $\{q_1, q_2\}$. Recall that $q_1 \wedge q_2$ is the greatest lower bound of $\{q_1, q_2\}$. Thus, $p \leq q_1 \wedge q_2$. Conversely, assume $p \leq q_1 \wedge q_2$. Then because $q_1 \wedge q_2 \leq q_1$ and $q_1 \wedge q_2 \leq q_2$, we have $p \leq q_1$ and $p \leq q_2$. The dual case follows in the same way. □

Lemma 2.2.4 is generalized to the following equivalence: $p \leq q$ for any $q \in \Gamma$ if and only if $p \leq \bigwedge \Gamma$, provided that $\bigwedge \Gamma$ exists in L. Dually, $q \leq p$ for any $q \in \Gamma$ if and only if $\bigvee \Gamma \leq p$, provided that $\bigvee \Gamma$ exists in L.

Lemma 2.2.4. The following conditions are equivalent:

(1) $p \leq q$;

(2) $p \wedge q = p$;

(3) $p \vee q = q$.

Proof. For (1) $\Rightarrow$ (2), assume $p \leq q$. Clearly, $p \wedge q \leq p$. Because $p \leq q$ and $p \leq p$, it follows from Lemma 2.2.3 that $p \leq p \wedge q$. For (2) $\Rightarrow$ (1), assume $p \wedge q = p$. Then $p = p \wedge q \leq q$. Similarly, (1) is equivalent to (3). □

Lemma 2.2.5. Every lattice satisfies the following conditions:

(1) $(p \wedge q) \wedge r = p \wedge (q \wedge r)$ and $(p \vee q) \vee r = p \vee (q \vee r)$ (the associative laws);

(2) $p \wedge q = q \wedge p$ and $p \vee q = q \vee p$ (the commutative laws);

(3) $p \wedge p = p$ and $p \vee p = p$ (the idempotent laws);

(4) $p \wedge (p \vee q) = p$ and $p \vee (p \wedge q) = p$ (the absorption laws).

Proof. (2) and (3) are immediate.

(1) We only prove the associative law for $\wedge$. It suffices to show that $x = (p \wedge q) \wedge r$ is the infimum of $\{p, q \wedge r\}$. Because x is the infimum of $\{p \wedge q, r\}$, we obtain $x \leq p \wedge q$ and $x \leq r$. Thus, $x \leq p$, $x \leq q$, and $x \leq r$. Hence, $x \leq p \wedge (q \wedge r)$. That is, x is a lower bound of $\{p, q \wedge r\}$. For any lower bound y of $\{p, q \wedge r\}$, $y \leq p$ and $y \leq q \wedge r$. Thus, $y \leq p$, $y \leq q$, and $y \leq r$. Hence, $y \leq (p \wedge q) \wedge r$. That is, y is a lower bound of $\{p \wedge q, r\}$. Recall that x is the infimum of $\{p \wedge q, r\}$. Therefore, $y \leq x$. Consequently, x is the infimum of $\{p, q \wedge r\}$.

(4) We only prove one of the absorption laws. For, we show that p is the infimum of $\{p, p \vee q\}$. Because $p \leq p$ and $p \leq p \vee q$, it follows that p is a lower bound of $\{p, p \vee q\}$. For any lower bound x of $\{p, p \vee q\}$, $x \leq p$. Thus, p is the infimum of $\{p, p \vee q\}$.

□

Theorem 2.2.6. Let L be a non-empty set and $\overline{\wedge}, \veebar : L \times L \to L$ be functions satisfying the associative law, commutative law, idempotent law, and absorption law. The relation $\preceq$ on L defined by $\preceq = \{(p, q) : p \mathbin{\overline{\wedge}} q = p\}$ is a partial order. Furthermore, $(L, \preceq)$ is a lattice with the infimum $p \mathbin{\overline{\wedge}} q$ and supremum $p \veebar q$ of $\{p, q\}$ with respect to $\preceq$.

Proof. By the idempotent law, $p \mathbin{\overline{\wedge}} p = p$. Thus, $\preceq$ is reflexive. Suppose that $p \preceq q$ and $q \preceq r$. Then $p \mathbin{\overline{\wedge}} q = p$ and $q \mathbin{\overline{\wedge}} r = q$. By the associative law,

$$p \mathbin{\overline{\wedge}} r = (p \mathbin{\overline{\wedge}} q) \mathbin{\overline{\wedge}} r = p \mathbin{\overline{\wedge}} (q \mathbin{\overline{\wedge}} r) = p \mathbin{\overline{\wedge}} q = p,$$

and we have $p \preceq r$. Thus, $\preceq$ is transitive. Finally, suppose that $p \preceq q$ and $q \preceq p$. Then $p \mathbin{\overline{\wedge}} q = p$ and $q \mathbin{\overline{\wedge}} p = q$. By the commutative law, $p = p \mathbin{\overline{\wedge}} q = q \mathbin{\overline{\wedge}} p = q$. Thus, $\preceq$ is antisymmetric. Consequently, $\preceq$ is a partial order. Now we show that $p \mathbin{\overline{\wedge}} q$ is the infimum of $\{p, q\}$. Observe that

$$\begin{aligned}
(p \mathbin{\overline{\wedge}} q) \mathbin{\overline{\wedge}} p &= (q \mathbin{\overline{\wedge}} p) \mathbin{\overline{\wedge}} p && \text{(By the commutative law)} \\
&= q \mathbin{\overline{\wedge}} (p \mathbin{\overline{\wedge}} p) && \text{(By the associative law)} \\
&= q \mathbin{\overline{\wedge}} p && \text{(By the idempotent law)} \\
&= p \mathbin{\overline{\wedge}} q. && \text{(By the commutative law)}
\end{aligned}$$

Hence, $p \mathbin{\overline{\wedge}} q \leq p$. Similarly, $p \mathbin{\overline{\wedge}} q \leq q$. It means that $p \mathbin{\overline{\wedge}} q$ is a lower bound of $\{p, q\}$. For any r satisfying $r \preceq p$ and $r \preceq q$, we obtain $r \mathbin{\overline{\wedge}} p = r$ and $r \mathbin{\overline{\wedge}} q = r$. Thus,

$$r = r \mathbin{\overline{\wedge}} q = (r \mathbin{\overline{\wedge}} p) \mathbin{\overline{\wedge}} q = r \mathbin{\overline{\wedge}} (p \mathbin{\overline{\wedge}} q)$$

by the associative law. It means that $r \preceq p \mathbin{\overline{\wedge}} q$. Therefore, $p \mathbin{\overline{\wedge}} q$ is the greatest lower bound of $\{p, q\}$. It remains to show that $p \veebar q$ is the supremum of $\{p, q\}$. It

is shown in the same way as explained above. Note that $p \preceq q$ implies $p \veebar q = q$ because

$$\begin{aligned} q &= q \veebar (q \barwedge p) && \text{(By the absorption law)} \\ &= q \veebar (p \barwedge q) && \text{(By the commutative law)} \\ &= q \veebar p. && \text{(By } p \preceq q\text{)} \end{aligned}$$

□

Theorem 2.2.7 (Infinite Associative Laws)**.** Let $(L, \leq)$ be a complete lattice. Then the **infinite associative laws**

$$p \wedge \bigwedge \Gamma = \bigwedge \{p \wedge q : q \in \Gamma\}, \quad p \vee \bigvee \Gamma = \bigvee \{p \vee q : q \in \Gamma\}$$

hold for any $p \in L$ and $\Gamma \subseteq L$.

Proof. We only show one of the infinite associative laws. Because $\bigwedge \Gamma \leq q$ for any $q \in \Gamma$, we have $p \wedge \bigwedge \Gamma \leq p \wedge q$ for any $q \in \Gamma$. It means that $p \wedge \bigwedge \Gamma$ is a lower bound for $\{p \wedge q : q \in \Gamma\}$. Now we show that $p \wedge \bigwedge \Gamma$ is the greatest lower bound: $r \leq p \wedge \bigwedge \Gamma$ for any lower bound r for $\{p \wedge q : q \in \Gamma\}$. Because r is a lower bound for $\{p \wedge q : q \in \Gamma\}$, we obtain $r \leq p \wedge q \leq q$ for any $q \in \Gamma$. Thus, $r \leq \bigwedge \Gamma$. Also, we obtain $r \leq p \wedge q \leq p$. Combining them, we conclude $r \leq p \wedge \bigwedge \Gamma$, as desired. □

2.3 Closure System

In this section, we explain how to construct a complete lattice. The first theorem is a characterization of complete lattices.

Theorem 2.3.1. For any lattice $(L, \leq)$, the following conditions are equivalent:

(1) $(L, \leq)$ is complete;

(2) There exists the greatest element $\curlyvee$ of L and $\bigwedge \Gamma$ exists in L for any non-empty set $\Gamma \subseteq L$.

Proof. (1) $\Rightarrow$ (2) immediately follows from the definition of complete lattices. Conversely, assume (2). If $\Gamma \neq \emptyset$, then $\bigwedge \Gamma$ exists. If $\Gamma = \emptyset$, then $\bigwedge \Gamma = \curlyvee \in L$ because $\curlyvee$ exists. Consequently, $\bigwedge \Gamma$ exists for each $\Gamma \subseteq L$. It remains to show that $\bigvee \Gamma$ exists for each $\Gamma \subseteq L$. Let Γ^u be the set of all upper bounds of Γ. Then $\curlyvee \in \Gamma^u$, and thus $\Gamma^u \neq \emptyset$. Hence, $\bigwedge \Gamma^u$ exists by (2). It suffices to show that $\bigwedge \Gamma^u$ is the least upper bound of Γ (if so, $\bigvee \Gamma = \bigwedge \Gamma^u$ exists). By the definition of upper bounds, for any $p \in \Gamma$ and $q \in \Gamma^u$, $p \leq q$. Hence, $p \leq \bigwedge \Gamma^u$ (note: $\bigvee \Gamma \leq q$ is not derivable because $\bigvee \Gamma$ may not exist). Thus, $\bigwedge \Gamma^u$ is an upper bound of Γ. Moreover, $\bigwedge \Gamma^u \leq q$ for any $q \in \Gamma^u$ by the definition of infimums. Consequently, $\bigwedge \Gamma^u = \bigvee \Gamma$. □

Let L_S be a subset of $\wp(S)$. Although any powerset lattice $(\wp(S), \subseteq)$ is a complete lattice, $(L_S, \subseteq)$ may not complete (it may not even be a lattice). By applying Theorem 2.3.1, the condition for making $(L_S, \subseteq)$ be a complete lattice is obtained.

Definition 2.3.2. A **closure system** (also called a **topped intersection structure**) on S is a subset L_S of $\wp(S)$ such that

(1) $\bigcap \Gamma \in L_S$ for each non-empty set $\Gamma \subseteq L_S$,

(2) $S \in L_S$.

The elements of a closure system are called **closures**.

Theorem 2.3.3. Let L_S be a closure system on S. Then $(L_S, \subseteq)$ is a complete lattice by $\bigwedge \Gamma = \bigcap \Gamma$ and

$$\bigvee \Gamma = \bigcap \{P \in L_S : \bigcup \Gamma \subseteq P\}.$$

Proof. It follows from Theorem 2.3.1 that $(L_S, \subseteq)$ is a complete lattice by $\bigwedge \Gamma = \bigcap \Gamma$. In the proof of Theorem 2.3.1, we obtained $\bigvee \Gamma = \bigwedge \Gamma^u$. Thus,

$$\begin{aligned} \bigvee \Gamma = \bigwedge \Gamma^u &= \bigcap \{P \in L_S : Q \subseteq P \text{ for any } Q \in \Gamma\} \\ &= \bigcap \{P \in L_S : \bigcup \Gamma \subseteq P\}. \end{aligned}$$

□

According to Theorem 2.3.3, it suffices to find a closure system to construct a complete lattice. In fact, closure systems are obtained from closure operators defined below.

Definition 2.3.4. A **closure operator** on a set S is a function $C : \wp(S) \to \wp(S)$ such that for any $P, Q \in \wp(S)$,

(1) C is **extensive**: $P \subseteq C(P)$,

(2) C is **monotonic**: $P \subseteq Q$ implies $C(P) \subseteq C(Q)$,

(3) C is **idempotent**: $C(P) = C(C(P))$.

Example 2.3.5.

(1) Let L be a partially ordered set with $\leq$. Then the **downward closure** $d(p)$ of $p \in L$ is defined by $d(p) = \{q : q \leq p\}$. More generally, the downward closure $\hat{d}(\Gamma)$ of $\Gamma \subseteq L$ is defined by $\bigcup\{d(p) : p \in \Gamma\}$. In fact,

$$\hat{d}(\Gamma) = \{q : q \leq p \text{ for some } p \in \Gamma\}.$$

The function $\hat{d} : \wp(L) \to \wp(L)$ that assigns $\hat{d}(\Gamma)$ to each $\Gamma \in \wp(L)$ is a closure operator on L.

(2) Let Γ^l (Γ^u) be the set of all lower (upper) bounds of Γ. Then the function $f^{ul} : \wp(L) \to \wp(L)$ that assigns $f^{ul}(\Gamma) = (\Gamma^u)^l$ to each $\Gamma \in \wp(L)$ is a closure operator on L.

(3) Let R be a relation on a non-empty set S. The functions $\Box_R : \wp(S) \to \wp(S)$ and $\Diamond_R : \wp(S) \to \wp(S)$ (called a **necessity operator** and **possibility operator**, respectively) are defined by

$$\Box_R(P) = \{s \in S : sRt \text{ implies } t \in P \text{ for any } t \in S\},$$
$$\Diamond_R(P) = \{s \in S : sRt \text{ and } t \in P \text{ for some } t \in S\}.$$

The necessity operator and possibility operator are first defined as the operators in modal logic.

(a) The function composition $\Box_R\Diamond_{R^{-1}}$ is a closure operator, where R^{-1} denotes the converse relation of R. As a corollary, $\Box_R\Diamond_R$ is also a closure operator if R is symmetric.

(b) Substitute a partial order $\leq$ for R. Then observe that $\Diamond_\leq(P) = \hat{d}(P)$ for each $P \in \wp(S)$. It follows from Example 2.3.5 (1) that $\Diamond_\leq$ is a closure operator.

Theorem 2.3.6. Let C be a closure operator on S. Then,

$$L_S^C = \{P \in \wp(S) : C(P) = P\}$$

is a closure system on S. Furthermore, $(L_S^C, \subseteq)$ is a complete lattice by $\bigwedge \Gamma = \bigcap \Gamma$ and

$$\bigvee \Gamma = C(\bigcup \Gamma).$$

Proof. We first confirm that L_S^C is a closure system.

(1) Let Γ be a non-empty subset of L_S^C. Then $C(P) = P$ and $\bigcap \Gamma \subseteq P$ for any $P \in \Gamma$. Hence, by the monotonicity of C, we have

$$C(\bigcap \Gamma) \subseteq C(P) = P$$

for any $P \in \Gamma$. Thus, $C(\bigcap \Gamma) \subseteq \bigcap \Gamma$. On the other hand, $\bigcap \Gamma \subseteq C(\bigcap \Gamma)$ by the extensivity of C. Consequently, $C(\bigcap \Gamma) = \bigcap \Gamma$, which is equivalent to $\bigcap \Gamma \in L_S^C$.

(2) Because C is a function from $\wp(S)$ to $\wp(S)$, we obtain $C(P) \in \wp(S)$ for any $P \in \wp(S)$. In particular, $C(S) \in \wp(S)$. Equivalently, $C(S) \subseteq S$. On the other hand, $S \subseteq C(S)$ by the extensivity of C. Consequently, $C(S) = S$, which is equivalent to $S \in L_S^C$.

Therefore, it follows from Theorem 2.3.3 that $(L_S^C, \subseteq)$ is a complete lattice. Finally, we prove that $\bigvee \Gamma = C(\bigcup \Gamma)$. By Theorem 2.3.3, it suffices to show that

$$C(\bigcup \Gamma) = \bigcap \{P \in L_S^C : \bigcup \Gamma \subseteq P\}.$$

Let Γ' be the set $\{P \in L_S^C : \bigcup \Gamma \subseteq P\}$. For any $P \in \Gamma'$,

$$C(\bigcup \Gamma) \subseteq C(P) = P$$

by the monotonicity of C. It means that $C(\bigcup \Gamma)$ is a lower bound of Γ'. Our goal is to show that $C(\bigcup \Gamma)$ is the greatest lower bound of Γ'. For this purpose, it is enough to see $C(\bigcup \Gamma) \in \Gamma'$ because we saw that $C(\bigcup \Gamma)$ is a lower bound of Γ'. By the idempotence and extensivity of C, we have $C(\bigcup \Gamma) \in L_S^C$ and $\bigcup \Gamma \subseteq C(\bigcup \Gamma)$. Therefore, $C(\bigcup \Gamma) \in \Gamma'$. □

Example 2.3.7. By applying Theorem 2.3.6 to the closure operators in Example 2.3.5, we have the following complete lattices.

(1) $(\{P \in \wp(S) : \hat{d}(P) = P\}, \subseteq)$ is a complete lattice.

(2) $(\{P \in \wp(S) : \Box_R \Diamond_{R^{-1}} P = P\}, \subseteq)$ is a complete lattice.

Theorem 2.3.6 states that a closure system is obtained from a closure operator. Conversely, a closure operator is obtained from a closure system.

Theorem 2.3.8. Let L_S be a closure system on S. Then a function $C_{L_S} : \wp(S) \to \wp(S)$ defined by

$$C_{L_S}(P) = \bigcap \{Q \in L_S : P \subseteq Q\}$$

is a closure operator on S. That is, $C_{L_S}(P)$ is the smallest set containing P among all elements of L_S.

Proof. We show each of the conditions of closure operators.

(1) Take any $p \in P$. Then $p \in Q$ for each $Q \supseteq P$. Thus, $p \in C_{L_S}(P)$. It means that C_{L_S} is extensive.

(2) Assume $p \in C_{L_S}(P)$. Then $p \in Q$ for each $Q \supseteq P$. Thus, $p \in Q$. Because $p \in Q'$ for each $Q \supseteq Q'$, we obtain $p \in C_{L_S}(Q)$. Hence, $C_{L_S}(P) \subseteq C_{L_S}(Q)$ for each $Q \supseteq P$. Consequently, C_{L_S} is monotonic.

(3) Observe that

$$\begin{aligned} C_{L_S}(C_{L_S}(P)) &= \bigcap\{Q \in L_S : C_{L_S}(P) \subseteq Q\} \\ &= \bigcap\{Q \in L_S : \bigcap\{Q' \in L_S : P \subseteq Q'\} \subseteq Q\}. \end{aligned}$$

Thus, for the idempotence of C_{L_S}, it suffices to show

$$\{Q \in L_S : P \subseteq Q\} = \{Q \in L_S : \bigcap\{Q' \in L_S : P \subseteq Q'\} \subseteq Q\}.$$

Assume that Q is an element of the left-hand side of the above equation. That is, $P \subseteq Q$ and $Q \in L_S$. Then $Q \in \{Q' \in L_S : P \subseteq Q'\}$. Hence, $\bigcap\{Q' \in L_S : P \subseteq Q'\} \subseteq Q$. In other words, Q is an element of the right-hand side of the above equation. The converse follows from the extensivity of C_{L_S} that has already been proved in (1). That is,

$$\begin{aligned} \{Q \in L_S : P \subseteq Q\} &\supseteq \{Q \in L_S : C_{L_S}(P) \subseteq Q\} \\ &= \{Q \in L_S : \bigcap\{Q' \in L_S : P \subseteq Q'\} \subseteq Q\} \end{aligned}$$

because $P \subseteq C_{L_S}(P)$.

□

2.4 Dedekind–MacNeille Completion

Definition 2.4.1. Let L_1 be a partially ordered set with $\leq_1$ and L_2 be a partially ordered set with $\leq_2$. A function $f : L_1 \to L_2$ is called

- an **order homomorphism** (also called **order preserving**) if $p \leq_1 q$ implies $f(p) \leq_2 f(q)$ for any $p, q \in L_1$.
- an **order embedding** if $p \leq_1 q$ is equivalent to $f(p) \leq_2 f(q)$ for any $p, q \in L_1$.
- an **order isomorphism** if f is a surjective order embedding.

A partially ordered set L_1 with $\leq_1$ is said to be **isomorphic** to a partially ordered set L_2 with $\leq_2$ if there exists an order isomorphism from L_1 to L_2.

Remark 2.4.2. Evidently, every order embedding is injective.

Definition 2.4.3. Let $(L_1, \leq_1)$ and $(L_2, \leq_2)$ be lattices. A function $f : L_1 \to L_2$ is called

- a **lattice homomorphism** if the following conditions are satisfied:

  (1) $f(p \wedge_1 q) = f(p) \wedge_2 f(q)$,
  (2) $f(p \vee_1 q) = f(p) \vee_2 f(q)$,

  for any $p, q \in L_1$, where $\wedge_i$ and $\vee_i$ stand for an infimum and a supremum in L_i, respectively.

- a **(lattice) embedding** if f is an injective lattice homomorphism.

- a **lattice isomorphism** if f is a bijective homomorphism.

A lattice $(L_1, \leq_1)$ is said to be **isomorphic** to a lattice $(L_2, \leq_2)$ if there exists a lattice isomorphism from L_1 to L_2.

Hereafter, we omit subscripts in $\leq_i$, $\wedge_i$, and $\vee_i$, which should be clear from the context.

Theorem 2.4.4. Let $(L_1, \leq)$ and $(L_2, \leq)$ be lattices. A function $f : L_1 \to L_2$ is an order isomorphism if and only if f is a lattice isomorphism.

Proof. ($\Rightarrow$) We only show the condition for $\wedge$. The goal is to show that $f(p \wedge q)$ is the greatest lower bound of $\{f(p), f(q)\}$. Clearly, $p \wedge q \leq p$. Because f is an order embedding, we have $f(p \wedge q) \leq f(p)$. Similarly, $f(p \wedge q) \leq f(q)$. Hence, $f(p \wedge q)$ is a lower bound of $\{f(p), f(q)\}$. Next, let r be a lower bound of $\{f(p), f(q)\}$. That is, $r \leq f(p)$ and $r \leq f(q)$. Recall that f is surjective. Thus, there exists r' such that $r = f(r')$. Hence, $f(r') \leq f(p)$ and $f(r') \leq f(q)$. Because f is an order embedding, we have $r' \leq p$ and $r' \leq q$, which implies $r' \leq p \wedge q$. That is, $r = f(r') \leq f(p \wedge q)$, as desired.

($\Leftarrow$) If $p \leq q$, then

$$f(p) = f(p \wedge q) = f(p) \wedge f(q).$$

Thus, $f(p) \leq f(q)$. Conversely, assume $f(p) \leq f(q)$. Then,

$$f(p) = f(p) \wedge f(q) = f(p \wedge q).$$

Because f is injective, we have $p = p \wedge q$. Equivalently, $p \leq q$. □

Corollary 2.4.5. Every lattice homomorphism is an order homomorphism, but the converse does not hold. Similarly, every lattice embedding is an order embedding, but the converse does not hold.

Proof. The first half part of each statement immediately follows from Theorem 2.4.4. The second half part of each statement is shown by a counterexample (left as an exercise for the reader). □

Theorem 2.4.6. For any complete lattice $(L, \leq)$, there exists a closure system L_S such that $(L, \leq)$ is isomorphic to $(L_S, \subseteq)$.

Proof. Let $(L, \leq)$ be a complete lattice and $d : L \to \wp(L)$ be a function that assigns $d(p) = \{q : q \leq p\}$ to each $p \in L$. Then $d : L \to \wp(L)$ is an order embedding. Thus, $\tilde{d} : L \to d(L)$ is an order isomorphism, where $d(L) = \{d(p) : p \in L\}$. By Theorem 2.4.4, $\tilde{d}$ is a lattice isomorphism. It remains to show that $(d(L), \subseteq)$ is a closure system.

(1) Let Γ be a non-empty subset of $d(L)$. Then every Γ is of the form $\{d(p) : p \in \Delta\}$ for some non-empty set $\Delta \subseteq L$. Thus,

$$\bigcap \Gamma = \bigcap \{d(p) : p \in \Delta \subseteq L\} \in d(L).$$

(2) Because $\bigvee L \in L$, we obtain $L = d(\bigvee L) \in d(L)$.

□

Definition 2.4.7. A complete lattice $(L_2, \leq)$ is called a **completion** of a partially ordered set $(L_1, \leq)$ via $f : L_1 \to L_2$ if f is an order embedding.

Example 2.4.8. A completion can be found if a closure operator C is given. That is, $(L_S^C, \subseteq)$ is a completion of a lattice $(L, \leq)$ via $f : L \to L_S^C$ (recall Theorem 2.3.6). More concretely, we enumerate completions of $(L, \leq)$ below.

(1) Let $\hat{d}$ be the closure operator $\hat{d} : \wp(L) \to \wp(L)$ defined in Example 2.3.5. Then $(L_S^{\hat{d}}, \subseteq)$ is a completion of a partially ordered set $(L, \leq)$ via the function $d : L \to L_S^{\hat{d}}$ that assigns $d(p) = \{q : q \leq p\}$ to each $p \in L$. In other words, d is an order embedding. Note that $d : L \to L_S^{\hat{d}}$ is well-defined because $d(p) \in L_S^{\hat{d}}$ (equivalently, $\hat{d}(d(p)) = d(p)$).

(2) $(L_S^{f^{ul}}, \subseteq)$ is a completion of a partially ordered set $(L, \leq)$ via the function $d : L \to L_S^{f^{ul}}$ that assigns $d(p) = \{q : q \leq p\}$ to each $p \in L$. Note that $d : L \to L_S^{f^{ul}}$ is well-defined because $d(p) \in L_S^{f^{ul}}$ (equivalently, $f^{ul}(d(p)) = d(p)$). This completion $(L_S^{f^{ul}}, \subseteq)$ is called the **Dedekind–MacNeille completion** of $(L, \leq)$.

The Dedekind–MacNeille completion is smaller than the completion in Example 2.4.8 (1). That is, $L_S^{f^{ul}} \subseteq L_S^{\hat{d}}$. Take any $\Gamma \in L_S^{f^{ul}}$. Then $f^{ul}(\Gamma) = \Gamma$. Our goal is to show $\Gamma \in L_S^{\hat{d}}$, or equivalently $\hat{d}(\Gamma) = \Gamma$. Because $\hat{d}$ is extensive, it suffices to show $\hat{d}(\Gamma) \subseteq \Gamma$. Take any $q \in \hat{d}(\Gamma)$. Then there exists $p \in \Gamma$ satisfying $q \leq p$. Because $p \in \Gamma = f^{ul}(\Gamma) = (\Gamma^u)^l$, we obtain $p \leq r$ for each $r \in \Gamma^u$. Thus, $q \leq r$ for each $r \in \Gamma^u$ by $q \leq p$. Hence, $q \in (\Gamma^u)^l = \Gamma$, which completes the proof.

Here we give an alternative expression of the Dedekind–MacNeille completion using cuts.

Definition 2.4.9. A **cut** in a partially ordered set $(L, \leq)$ is a pair (Γ, Δ) of $\Gamma, \Delta \subseteq L$ such that $\Gamma^u = \Delta$ and $\Gamma = \Delta^l$.

Example 2.4.10. $(\{p : p \leq q\}, \{p : q \leq p\})$ is a cut. That is, $\{p : p \leq q\} \cup \{p : q \leq p\}$ is "cut" by the point q.

Theorem 2.4.11. (Γ, Γ^u) is a cut if and only if $(\Gamma^u)^l = \Gamma$.

Proof. Straightforward. □

Corollary 2.4.12. $(L^{\mathrm{DM}}, \subseteq)$ is isomorphic to the Dedekind–MacNeille completion $(L_S^{f^{ul}}, \subseteq)$ of $(L, \leq)$, where

$$L^{\mathrm{DM}} = \{\Gamma : (\Gamma, \Gamma^u) \text{ is a cut in } (L, \leq)\}.$$

Proof. It immediately follows from Theorem 2.4.11. □

Lemma 2.4.13. (1) If $\bigvee \Gamma$ exists, then $(\Gamma^u)^l = d(\bigvee \Gamma)$.

(2) $\Gamma \subseteq \Delta$ implies $(\Gamma^u)^l \subseteq (\Delta^u)^l$.

Proof.

(1) Let $u(p)$ be the **upward closure** of $p \in L$ defined by $u(p) = \{q : p \leq q\}$. If $\Gamma^u = u(\bigvee \Gamma)$ and $\Gamma^l = d(\bigwedge \Gamma)$, then

$$(\Gamma^u)^l = d(\bigwedge u(\bigvee \Gamma)) = d(\bigvee \Gamma).$$

Thus, it remains to show $\Gamma^u = u(\bigvee \Gamma)$. The other equation $\Gamma^l = d(\bigwedge \Gamma)$ is proved similarly. Recall that $p \in \Gamma^u$ if and only if, $q \leq p$ for any $q \in \Gamma$. Thus, it is also equivalent to $\bigvee \Gamma \leq p$. That is, $p \in u(\bigvee \Gamma)$, as desired.

(2) If $\Gamma \subseteq \Delta$, then $\bigvee \Gamma \leq \bigvee \Delta$. Thus, $d(\bigvee \Gamma) \subseteq d(\bigvee \Delta)$. It follows from Lemma 2.4.13 (1) that $(\Gamma^u)^l \subseteq (\Delta^u)^l$.

□

Theorem 2.4.14. The function $d : L \to L_S^{f^{ul}}$ defined in Example 2.4.8 (2) satisfies $d(\bigwedge \Gamma) = \bigwedge\{d(p) : p \in \Gamma\}$ if $\bigwedge \Gamma$ exists in L, for any $\Gamma \subseteq L$. Similarly, $d(\bigvee \Gamma) = \bigvee\{d(p) : p \in \Gamma\}$ if $\bigvee \Gamma$ exists in L.

Proof. We first prove that $d : L \to L_S^{f^{ul}}$ preserves infimums. Because f^{ul} is a closure operator, it follows from Theorem 2.3.6 that $(L_S^{f^{ul}}, \subseteq)$ is a complete lattice by $\bigwedge \Gamma = \bigcap \Gamma$. Thus,

$$\begin{aligned}\bigwedge\{d(p) : p \in \Gamma\} &= \bigcap\{d(p) : p \in \Gamma\} = \{q \in d(p) : p \in \Gamma\} \\ &= \{q : q \leq p \text{ for any } p \in \Gamma\} = \{q : q \leq \bigwedge \Gamma\} \\ &= d(\bigwedge \Gamma).\end{aligned}$$

Next, we show that $d : L \to L_S^{f^{ul}}$ preserves supremums. The goal is to show that $d(\bigvee \Gamma)$ is the least upper bound of $\{d(p) : p \in \Gamma\}$. Observe that $p \leq \bigvee \Gamma$ for any $p \in \Gamma$. Thus, $d(p) \subseteq d(\bigvee \Gamma)$, which implies that $d(\bigvee \Gamma)$ is an upper bound of $\{d(p) : p \in \Gamma\}$. Let P be an upper bound of $\{d(p) : p \in \Gamma\}$. Then $p \in d(p) \subseteq P$ for any $p \in \Gamma$. Hence, $\Gamma \subseteq P$. Because f^{ul} is a closure operator, it is monotonic. It follows from Lemma 2.4.13 that

$$d(\bigvee \Gamma) = f^{ul}(\Gamma) \subseteq f^{ul}(P) = P,$$

as desired. □

2.5 Various Lattices

Definition 2.5.1. An **ortholattice** is a triple

$$\mathcal{L} = (L, \leq, \neg)$$

that consists of a bounded lattice $(L, \leq)$ and function $\neg : L \to L$ (called **orthocomplementation**) such that

(1) $p \wedge \neg p = \curlywedge$, $p \vee \neg p = \curlyvee$,

(2) $\neg\neg p = p$,

(3) $p \leq q$ implies $\neg q \leq \neg p$.

An **orthomodular lattice** is an ortholattice satisfying the orthomodular law

(4) $p \wedge (\neg p \vee (p \wedge q)) \leq q$.

An ortholattice $(L, \leq, \neg)$ is said to be **complete** if $(L, \leq)$ is a complete lattice.

Example 2.5.2 (Hilbert Lattice)**.** Let $\mathcal{H}$ be a Hilbert space and $\mathcal{S}(\mathcal{H})$ be the set of all closed subspaces of $\mathcal{H}$. Then $(\mathcal{S}(\mathcal{H}), \subseteq, {}^{\perp})$ is a complete orthomodular lattice [33, Proposition 4.5] and is called a **Hilbert lattice**. Here, for each $V \in \mathcal{S}(\mathcal{H})$, $V^{\perp}$ is defined as the orthogonal complement

$$\{w \in \mathcal{H} : w \perp v \text{ for any } v \in V\}$$

of V, where $\perp$ denotes the orthogonality relation on $\mathcal{H}$. An orthogonal complement of a closed subspace is always a closed subspace. A Hilbert lattice is complete because $\bigwedge \Gamma = \bigcap \Gamma$ and

$$\bigvee \Gamma = \bigcap \{V \in \mathcal{S}(\mathcal{H}) : \bigcup \Gamma \subseteq V\}$$

exist for each $\Gamma \subseteq \mathcal{S}(\mathcal{H})$.

Theorem 2.5.3 (De Morgan's Laws)**.** The condition (3) in Definition 2.5.1 can be replaced by **De Morgan's laws**:

$$\neg(p \wedge q) = \neg p \vee \neg q, \quad \neg(p \vee q) = \neg p \wedge \neg q.$$

Proof. We only show one of De Morgan's laws (the other one is proved similarly). Because $p \wedge q \leq p$, we obtain $\neg p \leq \neg(p \wedge q)$. Similarly, $\neg q \leq \neg(p \wedge q)$. Thus, $\neg p \vee \neg q \leq \neg(p \wedge q)$. It remains to show the other inequality. Because $\neg p \leq \neg p \vee \neg q$, we have

$$\neg(\neg p \vee \neg q) \leq \neg\neg p = p.$$

Similarly, $\neg(\neg p \vee \neg q) \leq q$. Hence, $\neg(\neg p \vee \neg q) \leq p \wedge q$. Therefore,

$$\neg(p \wedge q) \leq \neg\neg(\neg p \vee \neg q) = \neg p \vee \neg q.$$

Conversely, we show the condition (3) in Definition 2.5.1 using De Morgan's laws. Assume $p \leq q$. Then $q = p \vee q$. Thus,

$$\neg q = \neg(p \vee q) = \neg p \wedge \neg q$$

by one of De Morgan's laws. Consequently, $\neg q \leq \neg p$. □

De Morgan's laws are extended to that for infinite (even uncountable) sets.

Theorem 2.5.4 (Infinite De Morgan's Laws)**.** Let $(L, \leq, \neg)$ be a complete ortholattice. Then the **infinite De Morgan's laws** hold:

$$\neg \bigwedge \Gamma = \bigvee \{\neg p : p \in \Gamma\} \text{ and } \neg \bigvee \Gamma = \bigwedge \{\neg p : p \in \Gamma\}$$

for each $\Gamma \subseteq L$.

Proof. The proof is similar to that of Theorem 2.5.3 (of the first part). □

Remark 2.5.5. The distributive laws do not hold in ortholattices and orthomodular lattices in general. However, partial distributive laws hold (in any lattices). That is, the inequalities

$$p \vee (q \wedge r) \leq (p \vee q) \wedge (p \vee r) \text{ and } (p \wedge q) \vee (p \wedge r) \leq p \wedge (q \vee r)$$

hold in any lattices [13, Lemma 4.1].

Definition 2.5.6. A **Boolean lattice** (also called a **Boolean algebra**) is an ortholattice with the distributive law

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r).$$

Example 2.5.7.

(1) Let $\wp(S)$ be the powerset of a set S. Then $(\wp(S), \subseteq, {}^{-})$ is a complete Boolean lattice called the **powerset Boolean lattice** of S, where ${}^{-}$ denotes the set complementation in S.

(2) The **two-element Boolean lattice** is the tuple $(\{\bot, \top\}, \leq, \neg)$ such that

$$\bot \leq \bot, \quad \bot \leq \top, \quad \top \leq \top,$$

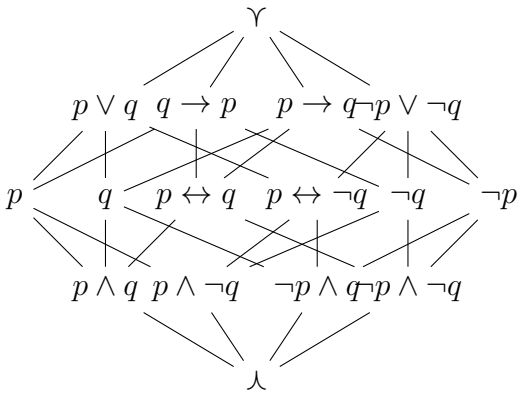
and

$$\neg\bot = \top, \quad \neg\top = \bot.$$

(3) Let L_S be a subset of $\wp(S)$. Then $(L_S, \subseteq, {}^{-})$ is a complete Boolean lattice called an **algebra of sets** if L_S is closed under $\cap$, $\cup$, and ${}^{-}$. For example, the **finite–cofinite field** $(L_S^{\mathrm{fin}} \cup L_S^{\mathrm{cofin}}, \subseteq, {}^{-})$ on S is a complete Boolean lattice, where L_S^{fin} (L_S^{cofin}) stands for the set of all finite (cofinite) subsets of S. Here, $P \subseteq S$ is said to be **cofinite** if its complement $\overline{P}$ is finite. Observe that $P \cap Q, P \cup Q, \overline{P} \in L_S^{\mathrm{fin}} \cup L_S^{\mathrm{cofin}}$ if $P, Q \in L_S^{\mathrm{fin}} \cup L_S^{\mathrm{cofin}}$.

(4) The lattice depicted in the following Hasse diagram is a Boolean lattice, where $p \to q$ and $p \leftrightarrow q$ are abbreviations for $\neg p \vee q$ and $(p \wedge q) \vee (\neg p \wedge \neg q)$, respectively. This lattice is called the **four-dimensional hypercube** and

is denoted by $\mathbf{2}^4$.



The following theorem states that the distributive law in Definition 2.5.6 can be replaced by its dual form

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r).$$

Theorem 2.5.8. Let $(L, \leq)$ be a lattice. Then the following conditions are equivalent:

(1) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ for any $p, q, r \in L$;

(2) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ for any $p, q, r \in L$.

Proof. We only show the implication from (1) to (2) (the converse direction follows in the same way):

$$\begin{aligned}
p \vee (q \wedge r) &= (p \vee (p \wedge q)) \vee (q \wedge r) && \text{(By the absorption law)} \\
&= p \vee ((p \wedge q) \vee (q \wedge r)) && \text{(By the associative law)} \\
&= p \vee ((q \wedge p) \vee (q \wedge r)) && \text{(By the commutative law)} \\
&= p \vee (q \wedge (p \vee r)) && \text{(By (1))} \\
&= (p \wedge (p \vee r)) \vee (q \wedge (p \vee r)) && \text{(By the absorption law)} \\
&= ((p \vee r) \wedge p) \vee ((p \vee r) \wedge q) && \text{(By the commutative law)} \\
&= (p \vee r) \wedge (p \vee q) && \text{(By (1))} \\
&= (p \vee q) \wedge (p \vee r). && \text{(By the commutative law)}
\end{aligned}$$

□

Theorem 2.5.9 (Infinite Distributive Laws)**.** Let $(L, \leq, \neg)$ be a complete Boolean lattice. Then the **infinite distributive laws**

$$p \wedge \bigvee \Gamma = \bigvee \{p \wedge q : q \in \Gamma\}$$

and

$$p \vee \bigwedge \Gamma = \bigwedge \{p \wedge q : q \in \Gamma\}$$

hold for any $\Gamma \subseteq L$.

Proof. We only show the first equation. The goal is to show that $p \wedge \bigvee \Gamma$ is the least upper bound of $\{p \wedge q : q \in \Gamma\}$. Because $q \leq \bigvee \Gamma$ for any $q \in \Gamma$, we obtain $p \wedge q \leq p \wedge \bigvee \Gamma$ for any $q \in \Gamma$. Thus, $p \wedge \bigvee \Gamma$ is an upper bound of $\{p \wedge q : q \in \Gamma\}$. Next, let r be an upper bound of $\{p \wedge q : q \in \Gamma\}$. Because $p \wedge q \leq r$ and $\neg p \wedge q \leq \neg p$ for any $q \in \Gamma$,

$$q = (p \vee \neg p) \wedge q = (p \wedge q) \vee (\neg p \wedge q) \leq r \vee \neg p$$

for any $q \in \Gamma$. Hence, $\bigvee \Gamma \leq r \vee \neg p$, which implies

$$p \wedge \bigvee \Gamma \leq p \wedge (r \vee \neg p) = (p \wedge r) \vee (p \wedge \neg p) = p \wedge r \leq r,$$

as desired. □

Definition 2.5.10. A **modal algebra** is a tuple

$$(L, \leq, \neg, \Box)$$

that consists of a Boolean lattice $(L, \leq, \neg)$ and a function $\Box : L \to L$ satisfying the following conditions:

(1) $\Box \Upsilon = \Upsilon$;

(2) $\Box(p \wedge q) = \Box p \wedge \Box q$.

Theorem 2.5.11. $\Box$ is monotonic: $p \leq q$ implies $\Box p \leq \Box q$.

Proof. If $p \leq q$, then $p = p \wedge q$. Thus,

$$\Box p = \Box(p \wedge q) = \Box p \wedge \Box q \leq \Box q$$

by Definition 2.5.10 (2). □

2.6 Quantum Computation

Here we briefly review quantum computation and fix our notation. We assume the readers have basic knowledge of linear algebra.

Generally speaking, quantum systems are formulated as complex Hilbert spaces. However, for quantum computation, it is enough to consider specific Hilbert spaces

called qubit systems. An n-qubit system is the complex 2^n-space $\mathbb{C}^{2^n}$, where $\mathbb{C}$ stands for the complex plane. **Pure states** in the n-qubit system $\mathbb{C}^{2^n}$ are unit vectors in $\mathbb{C}^{2^n}$. The orthogonal basis called computational basis in the one-qubit system $\mathbb{C}^2$ is a set $\{|0\rangle, |1\rangle\}$ that consists of the column vectors $|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$, where ^{T} denotes the transpose operator. The linear combinations $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ of $|0\rangle$ and $|1\rangle$ are also pure states. In general, $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$ represents a pure state in the one-qubit system $\mathbb{C}^2$ provided that $|c_0|^2 + |c_1|^2 = 1$. This notation of vectors is called **bra-ket notation** (also called **Dirac notation**). $|\psi\rangle$ is called a **ket vector**. The **bra vector** $\langle\psi|$ is defined as a row vector whose elements are complex conjugates of the elements of the corresponding ket vector $|\psi\rangle$. In the two-qubit system $\mathbb{C}^4$, there are pure states that cannot be represented in the form $|\psi_1\rangle \otimes |\psi_2\rangle$ and are called **entangled states**, where $\otimes$ denotes the tensor product (more precisely, the Kronecker product). For example, the **EPR state** (Einstein-Podolsky-Rosen state)

$$|\mathrm{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

is an entangled state, where $|00\rangle = |0\rangle \otimes |0\rangle$ and $|11\rangle = |1\rangle \otimes |1\rangle$. Entangled states also exist in the three-qubit system $\mathbb{C}^8$. For example, the **GHZ state** (Greenberger–Horne–Zeilinger state)

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

and the **W state**

$$|\mathrm{W}\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

are entangled states, where $|ijk\rangle = |i\rangle \otimes |j\rangle \otimes |k\rangle$. These states $|\mathrm{GHZ}\rangle$ and $|\mathrm{W}\rangle$ cannot be represented in the form $|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$.

Quantum computation is represented by unitary operators (also called **quantum gates**). There are various quantum gates. For example, the **Hadamard gate** H and **Pauli gates** X, Y, and Z are typical quantum gates on the one-qubit system $\mathbb{C}^2$ and are defined as follows:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Two typical quantum gates on the two-qubit system $\mathbb{C}^4$ are the controlled-X gate (also called the controlled NOT gate) CX and the swap gate SWAP are defined by

$$\mathrm{CX} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$

$$\mathrm{SWAP} = \mathrm{CX}(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)\mathrm{CX},$$

where I denotes the identity matrix of size 2×2. Measurement is a completely different process from applying quantum gates. Here we roughly explain specific projective measurements. For the general definition of projective measurement, see [27]. Observe that $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ are projections, respectively. After executing the measurement $\{P_0, P_1\}$, a current state $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$ is transitioned into $P_0 |\psi\rangle / |c_0| = c_0 |0\rangle / |c_0|$ with probability $|c_0|^2$ and into $P_1 |\psi\rangle / |c_1| = c_1 |1\rangle / |c_1|$ with probability $|c_1|^2$. There is no other possibility because $|c_0|^2 + |c_1|^2 = 1$.

Chapter 3

Stone-type Representation Theorems

This chapter contains:

In this chapter, we review some Stone-type representation theorems, namely the Stone-type representation theorems for Boolean lattices (Theorem 3.3.3), for ortholattices (Theorem 3.4.16), and for modal algebras (Theorem 3.5.6). The Stone-type representation theorems for Boolean lattices is known as Stone's representation theorem, that for ortholattices is known as Goldblatt's representation theorem [17], that for modal algebras is known as Jónsson–Tarski theorem [24].

Because one of the main results of this dissertation is to prove the Stone-type representation theorem for QDAs, the proofs of the existing Stone-type representation theorems are detailed for comparison in this chapter.

3.1 Atom

Definition 3.1.1. Let $(L, \leq)$ be a lattice with $\curlywedge$. An element $a \in L$ is called an **atom** in $(L, \leq)$ with $\curlywedge$ if

(1) $a \neq \curlywedge$ and

(2) $p < a$ implies $p = \curlywedge$.

A lattice $(L, \leq)$ with $\curlywedge$ is said to be

- **atomic** if, for any $p \in L$ satisfying $p \neq \curlywedge$, there exists an atom a in $(L, \leq)$ such that $a \leq p$.
- **atomistic** if, for any $p \in L$,

$$p = \bigvee \{a \in A : a \leq p\},$$

where A denotes the set of all atoms in $(L, \leq)$.

Furthermore, an ortholattice $(L, \leq, \neg)$ is said to be **atomic** (**atomistic**) if $(L, \leq)$ is.

Example 3.1.2. Every finite lattice is atomic. Boolean powerset lattices are atomic. Atoms in Boolean powerset lattices are singletons.

Example 3.1.3. Every Hilbert lattice $(\mathcal{S}(\mathcal{H}), \subseteq, ^\perp)$ is atomic. This is because, for any closed subspace V with the dimension 1 or more, V includes at least one one-dimensional subspace.

Theorem 3.1.4. Let $(L, \leq, \neg)$ be a Boolean lattice. Then $(L, \leq, \neg)$ is atomic if and only if $(L, \leq, \neg)$ is atomistic.

Proof. ($\Rightarrow$) Let A be the set of all atoms in $(L, \leq)$, and $\tilde{\theta} : L \to \wp(A)$ be a function defined by

$$\tilde{\theta}(p) = \{a \in A : a \leq p\}.$$

Then it suffices to show that $p = \bigvee \tilde{\theta}(p)$. It immediately follows that $\bigvee \tilde{\theta}(p) \leq p$. Thus, we only show the other inequality. Put $p' = \bigvee \tilde{\theta}(p)$. Our goal is to prove $p \leq p'$, which is equivalent to $p' = p' \vee p$. Because

$$p' \vee (\neg p' \wedge p) = (p' \vee \neg p') \wedge (p' \vee p) = p' \vee p,$$

it suffices to show that $\neg p' \wedge p = \curlywedge$. Suppose for the sake of contradiction that $\neg p' \wedge p \neq \curlywedge$. Then because $(L, \leq, \neg)$ is atomic, there exists an atom a such that $a \leq \neg p' \wedge p \leq p$. Hence, $a \in \tilde{\theta}(p)$, which implies $a \leq \bigvee \tilde{\theta}(p) = p'$. Equivalently, $a \wedge p' = a$. Thus, because $a \wedge p' \leq (\neg p' \wedge p) \wedge p'$ by $a \leq \neg p' \wedge p$, we see that

$$a = a \wedge p' \leq (\neg p' \wedge p) \wedge p' = \curlywedge.$$

However, it contradicts the assumption that a is an atom.

($\Leftarrow$) It suffices to show that $\tilde{\theta}(p) \neq \emptyset$ if $p \neq \curlywedge$. Suppose that $\tilde{\theta}(p)$ is the empty set. Then it follows from the atomisticity that

$$\curlywedge \neq p = \bigvee \tilde{\theta}(p) = \bigvee \emptyset = \curlywedge,$$

a contradiction. □

Theorem 3.1.5. If $(L, \leq, \neg)$ is an atomistic Boolean lattice, then $\tilde{\theta}$ is bijective.

Proof. For the surjectivity of $\tilde{\theta}$, it suffices to show that for any $A' \in \wp(A)$, there exists $p \in L$ such that $A' = \tilde{\theta}(p)$. Here we prove that $p = \bigvee A'$ is a witness for $A' = \tilde{\theta}(p)$. Proof of $A' \subseteq \tilde{\theta}(\bigvee A')$ is straightforward: $a \in A'$ implies $a \leq \bigvee A'$, which means $a \in \tilde{\theta}(\bigvee A')$. Thus, it remains to prove $\tilde{\theta}(\bigvee A') \subseteq A'$. Suppose for the sake of contradiction that there exists $a \in A$ such that $a \in \tilde{\theta}(\bigvee A')$ but $a \notin A'$. Because $a \in \tilde{\theta}(\bigvee A')$, we obtain $a \leq \bigvee A'$. Hence, it follows from Theorem 2.5.9 that

$$a = a \wedge \bigvee A' = \bigvee_{q \in A'} (a \wedge q).$$

By the assumption $a \notin A'$, every $q \in A'$ satisfies $q \neq a$. Therefore, $a \wedge q < q$, and thus $a \wedge q = \curlywedge$ because a is an atom. However, it follows from the above equation that

$$a = \bigvee_{q \in A'} (a \wedge q) = \bigvee_{q \in A'} \curlywedge = \curlywedge,$$

which contradicts the assumption that a is an atom. □

3.2 Filter

Definition 3.2.1. A **filter** of a lattice $(L, \leq)$ is a set $F \subseteq L$ such that

(1) $F \neq \emptyset$,

(2) F is upward closed: $p \in F$ and $p \leq q$ jointly imply $q \in F$,

(3) F is closed under $\wedge$: if $p, q \in F$, then $p \wedge q \in F$.

A filter F is said to be **proper** if F is a proper subset of L.

Example 3.2.2.

(1) The smallest filter containing $p \in L$ is the upward closure $p{\uparrow} = \{q : p \leq q\}$ of p and is called the **principal filter** generated by p. More generally,

$$\langle \Gamma \rangle = \{q \in L : \bigwedge \Gamma^{\mathrm{fin}} \leq q \text{ for some finite set } \Gamma^{\mathrm{fin}} \subseteq \Gamma\}.$$

is the smallest filter containing a non-empty set $\Gamma \subseteq L$. For the proof, see Theorem 3.2.3. In particular, the smallest filter containing a non-empty finite set $\{p_1, \ldots, p_n\}$ is identical to the principal filter generated by $\bigwedge\{p_1, \ldots, p_n\}$. Hence, every filter of a finite lattice is principal.

In addition, the smallest filter $\emptyset{\uparrow}$ containing $\emptyset$ exists, provided that $(L, \leq)$ is a lattice with $\curlyvee$. That is, if $(L, \leq)$ has $\curlyvee$, then $\emptyset{\uparrow} = \{\curlyvee\}$. In fact, $\{\curlyvee\}$ is the smallest filter among all filters of $(L, \leq)$.

(2) Let S be an infinite set and L_S^{cofin} be the set of all cofinite subsets of S. Then L_S^{cofin} is a filter of $(\wp(S), \subseteq, {}^-)$ and is called the **Fréchet filter** on S. The set S must be infinite so that L_S^{cofin} is a proper filter; otherwise, $\emptyset \in L_S^{\text{cofin}}$, and thus L_S^{cofin} is not proper. In finite–cofinite fields on an infinite set S, every non-principal filter is the Fréchet filter on S.

Theorem 3.2.3. The smallest filter containing a non-empty set $\Gamma \subseteq L$ is $\langle \Gamma \rangle$.

Proof. It follows from the reflexivity of $\leq$ that $\bigwedge\{p\} = p \leq p$ for any $p \in \Gamma$. Thus, $p \in \langle \Gamma \rangle$, which implies $\Gamma \subseteq \langle \Gamma \rangle$. Furthermore, $\langle \Gamma \rangle$ is a filter, as is shown below.

(1) Because Γ is non-empty, $p \in \Gamma$ for some $p \in L$. Hence, $\langle \Gamma \rangle \neq \emptyset$.

(2) Assume $p \in \langle \Gamma \rangle$. Equivalently, $\bigwedge \Gamma^{\text{fin}} \leq p$ for some finite set $\Gamma^{\text{fin}} \subseteq \Gamma$. If $p \leq q$, then $\bigwedge \Gamma^{\text{fin}} \leq q$ by the transitivity of $\leq$. Thus, $q \in \langle \Gamma \rangle$. Consequently, $\langle \Gamma \rangle$ is upward closed.

(3) Assume $p, q \in \langle \Gamma \rangle$. Then there exist finite sets $\Gamma_1^{\text{fin}}, \Gamma_2^{\text{fin}} \subseteq \Gamma$ such that $\bigwedge \Gamma_1^{\text{fin}} \leq p$ and $\bigwedge \Gamma_2^{\text{fin}} \leq q$. Thus,

$$\bigwedge(\Gamma_1^{\text{fin}} \cup \Gamma_2^{\text{fin}}) = \bigwedge \Gamma_1^{\text{fin}} \wedge \bigwedge \Gamma_2^{\text{fin}} \leq p \wedge q,$$

which implies $p \wedge q \in \langle \Gamma \rangle$. Consequently, $\langle \Gamma \rangle$ is closed under $\wedge$.

It follows immediately that $\langle \Gamma \rangle$ is the smallest. □

Theorem 3.2.4. The condition (2) in Definition 3.2.1 can be replaced by

(2′) $p \wedge q \in F$ implies $p, q \in F$.

Proof. Assume $p \wedge q \in F$. Because $p \wedge q \leq p$ and $p \wedge q \leq q$, we have $p, q \in F$. Conversely, we show the condition (2) in Definition 3.2.1 by using (2′). Assume $p \in F$ and $p \leq q$. Then $p \wedge q = p \in F$. Thus, it follows from (2′) that $q \in F$. □

Theorem 3.2.5. Let $(L, \leq)$ be a lattice with $\curlywedge$. Then a filter F of $(L, \leq)$ is proper if and only if $\curlywedge \notin F$.

Proof. If F is not proper, then $F = L$. Thus, $\curlywedge \in F$. Conversely, if $\curlywedge \in F$, then $\curlywedge \leq p$ for any $p \in F$ by the upward closedness of F. It means that $F = L$. □

The next property is a significant property that deserves attention.

Definition 3.2.6. Let $(L, \leq)$ be a lattice. A subset Γ of L is said to have the **finite meet property** if there is no finite subset Γ^{fin} of Γ such that $\bigwedge \Gamma^{\text{fin}} = \curlywedge$.

Notice that the finite meet property is well-defined because $\bigwedge \Gamma^{\text{fin}}$ exists for each finite set Γ^{fin} by the definition of lattices (but $\bigwedge \Gamma$ may not exist if Γ is an infinite set).

Theorem 3.2.7. If Γ satisfies the finite meet property, then $\langle \Gamma \rangle$ is a proper filter.

Proof. By Theorem 3.2.5, it suffices to show that $\curlywedge \notin \langle \Gamma \rangle$. If $\curlywedge \in \langle \Gamma \rangle$, then $\bigwedge \Gamma^{\text{fin}} = \curlywedge$ for some finite set $\Gamma^{\text{fin}} \subseteq \Gamma$ by Theorem 3.2.3. However, such Γ^{fin} must not exist by the finite meet property. □

Definition 3.2.8. A proper filter F of a lattice $(L, \leq)$ is called an **ultrafilter** (also called a **maximal filter**) if F is maximal: for any proper filter F', $F \subseteq F'$ implies $F = F'$.

Remark 3.2.9. To define ultrafilters, the condition that ultrafilters must be proper filters is necessary. If an ultrafilter F were defined as the maximal filter, the only ultrafilter would be L because $F \subseteq L$ for any filter F.

Example 3.2.10.

(1) The principal filter $a{\uparrow}$ generated by an atom in $(L, \leq)$ is an ultrafilter of $(L, \leq)$. In fact, every principal ultrafilter is of the form $a{\uparrow}$. For the proof, see Theorem 3.2.11. In finite lattices, every ultrafilter is principal.

(2) Are there any non-principal ultrafilters? The answer is yes. Let S be an infinite set and F be an ultrafilter of $(\wp(S), \subseteq)$. In fact, if F is a Fréchet filter of S, then F is a non-principal ultrafilter. Contrapositively, if F is a principal ultrafilter of $(\wp(S), \subseteq)$, then F is not a Fréchet filter. For, recall that atoms in $(\wp(S), \subseteq)$ are singletons $\{p\}$. Thus, any principal ultrafilter of $(\wp(S), \subseteq)$ is of the form $\{p\}{\uparrow}$ by Theorem 3.2.11. However, $\{p\} \in \{p\}{\uparrow}$, but $\{p\}$ is not cofinite, which implies that any principal ultrafilter of $(\wp(S), \subseteq)$ is not a Fréchet filter.

(3) Note that a Fréchet filter may not be an ultrafilter. For example, consider the Fréchet filter $L_{\mathbb{N}}^{\text{cofin}}$ on natural numbers $\mathbb{N}$. Then the set of all even numbers and its complement (the set of all odd numbers) are not elements of $L_{\mathbb{N}}^{\text{cofin}}$. However, it contradicts one of the characterizations of ultrafilters (see Theorem 3.2.13).

Theorem 3.2.11. F is a principal ultrafilter of $(L, \leq)$ if and only if $F = a{\uparrow}$ for some atom a in $(L, \leq)$.

Proof. ($\Rightarrow$) Because F is a principal filter, $F = p{\uparrow}$ for some $p \in L$. If p were not an atom, then there would be $q \in L$ such that $\curlywedge < q < p$. By this inequality,

$p\uparrow$ must be a proper subset of $q\uparrow$. However, it leads to a contradiction because $F = p\uparrow$ is an ultrafilter.

($\Leftarrow$) We show that $F = a\uparrow$ is maximal. Suppose for the sake of contradiction that there exists a proper filter F' properly contains F. Then $q \notin F$ but $q \in F'$ for some $q \in L$. Because $q \notin F$, we obtain $a \not\leq q$. Hence, $a \wedge q \neq a$. Because $q \in F'$, it follows from the definition of filters that $a \wedge q \in F'$. Thus, $a \wedge q$ must not be $\curlywedge$ (recall Theorem 3.2.5). Therefore, $\curlywedge < a \wedge q < a$, which leads to a contradiction with the assumption that a is an atom. □

Definition 3.2.12. A proper filter F of a lattice $(L, \leq)$ is called a **prime filter** if $p \vee q \in F$ implies either $p \in F$ or $q \in F$.

Theorem 3.2.13. Let $(L, \leq, \neg)$ be a Boolean lattice. For any proper filter F of $(L, \leq)$, the following conditions are equivalent:

(1) F is an ultrafilter;

(2) F is a prime filter;

(3) For each $p \in L$, either $p \in F$ or $\neg p \in F$.

Proof. For (1) $\Rightarrow$ (2), assume that F is an ultrafilter. Now we show that $p \vee q \in F$ and $p \notin F$ jointly imply $q \in F$. Let F' be the set $\{r : p \vee r \in F\}$. In fact, F' is a proper filter.

(i) By the assumption $p \vee q \in F$, we have $q \in F'$. Thus, $F' \neq \emptyset$.

(ii) If $r_1 \in F$ and $r_1 \leq r_2$, then $p \vee r_1 \in F$ and $p \vee r_1 \leq p \vee r_2$. Thus, $p \vee r_2 \in F$ because F is a filter. Hence, $r_2 \in F'$. It means that F' is upward closed.

(iii) If $r_1, r_2 \in F'$, then $p \vee r_1, p \vee r_2 \in F$. Because F is a filter,

$$(p \vee r_1) \wedge (p \vee r_2) \in F.$$

By the distributive law, $p \vee (r_1 \wedge r_2) \in F$. Therefore, $r_1 \wedge r_2 \in F$. Consequently, F' is closed under $\wedge$.

(iv) By the assumption $p \notin F$, we obtain $p \vee \curlywedge = p \notin F$. It implies that $\curlywedge \notin F'$. Hence, $F' \neq L$.

Because F is an ultrafilter and F' is a proper filter, $F \subseteq F'$ implies $F = F'$. It follows from the assumption $p \vee q \in F$ that $q \in F' = F$, as desired. That is, it remains to show $F \subseteq F'$. It is proved as follows: if $r \in F$, then $p \vee r \in F$ by $r \leq p \vee r$, and thus $r \in F'$.

For (2) $\Rightarrow$ (3), assume F is a prime filter. Then because $p \vee \neg p = \curlyvee \in F$, either $p \in F$ or $\neg p \in F$.

For (3) $\Rightarrow$ (1), it suffices to show that $F \subseteq F'$ and $F \neq F'$ jointly imply a contradiction for some proper filter F'. By the assumptions, there exists $p \in L$ such that $p \in F'$ but $p \notin F$. Because $p \notin F$, it follows from (3) that $\neg p \in F \subseteq F'$. Therefore, $\curlywedge = p \wedge \neg p \in F'$, but it leads to a contradiction with the assumption that F' is proper. □

Every proper filter can be extended to an ultrafilter.

Theorem 3.2.14 (Ultrafilter Theorem)**.** For any proper filter F of $(L, \leq)$, there exists an ultrafilter $\widehat{F}$ satisfying $F \subseteq \widehat{F}$.

Proof. Let L' be the set

$$\{F' \subseteq L : F \subseteq F' \text{ and } F' \text{ is a proper filter of } (L, \leq)\}.$$

Then $(L', \subseteq)$ is a partially ordered set. By Zorn's lemma (Lemma 2.1.11), it suffices to show that there exists an upper bound of any non-empty totally ordered set

$$\{F'_1, F'_2, F'_3, \dots\} \subseteq L'$$

in L' (observe that a maximal element of L' with respect to $\subseteq$ is a maximal proper filter containing F). In fact, $\widehat{F} = \bigcup_{i \geq 0} F'_i$ is a witness for the statement. $\widehat{F}$ is an upper bound because $F'_i \subseteq \widehat{F}$. Thus, it remains to show that $\widehat{F} \in L'$: $F \subseteq \widehat{F}$ and $\widehat{F}$ is a proper filter. Because $F \subseteq F'_i \subseteq \widehat{F}$, we obtain $F \subseteq \widehat{F}$. Furthermore, it is to be proved that $\widehat{F}$ is a proper filter.

(i) Because each F_i is a filter, $F_i \neq \emptyset$. Hence, $\widehat{F} \neq \emptyset$;

(ii) Assume $p \in \widehat{F}$. Then there exists F'_i such that $p \in F'_i$. Because F'_i is a filter, $p \leq q$ implies $q \in F'_i \subseteq \widehat{F}$. Consequently, $\widehat{F}$ is upward closed.

(iii) Assume $p, q \in \widehat{F}$. Then there exist F'_i and F'_j such that $p \in F'_i$ and $q \in F'_j$. Because F'_i and F'_j are totally ordered by $\subseteq$, we assume that $F'_i \subseteq F'_j$ without loss of generality. Then $p, q \in F'_j$, and thus $p \wedge q \in F'_j \subseteq \widehat{F}$. Consequently, $\widehat{F}$ is closed under $\wedge$.

(iv) Because each F'_i is proper, $\curlywedge \notin F'_i$. Hence, $\curlywedge \notin \widehat{F}$ (equivalently, $\widehat{F} \neq L$).

□

Corollary 3.2.15. If Γ satisfies the finite meet property, then there exists an ultrafilter $\widehat{F}$ satisfying $\langle \Gamma \rangle \subseteq \widehat{F}$.

Proof. It follows from Theorem 3.2.7 and 3.2.14. □

3.3 Representation Theorem for Boolean lattices

We have already defined lattice homomorphisms in Definition 2.4.3. This definition can be extended to that for ortholattices (Boolean lattices).

Definition 3.3.1. Let $(L_1, \leq_1, \neg_1)$ and $(L_2, \leq_2, \neg_2)$ be ortholattices (Boolean lattices). A function $f : L_1 \to L_2$ is called

- a **homomorphism** between ortholattices (Boolean lattices) if the following conditions are satisfied:

  (1) f is a lattice homomorphism,

  (2) $f(\neg_1 p) = \neg_2 f(p)$.

- an **embedding** between ortholattices (Boolean lattices) if f is an injective homomorphism between ortholattices (Boolean lattices).

- an **isomorphism** if f is a bijective homomorphism between ortholattices (Boolean lattices).

An ortholattice (Boolean lattice) $(L_1, \leq_1)$ is said to be **isomorphic** to an ortholattice (Boolean lattice) $(L_2, \leq_2)$ if there exists an isomorphism from L_1 to L_2.

Similar to the case of lattice homomorphism, we omit subscripts in $\leq_i$, $\wedge_i$, and $\vee_i$, which should be clear from the context.

Definition 3.3.2. Let U be the set of all ultrafilters of a lattice $(L, \leq)$. The **Stone embedding** for Boolean lattices $(L, \leq, \neg)$ is the function $\theta : L \to \wp(U)$ defined by

$$\theta(p) = \{F \in U : p \in F\}.$$

The **canonical extension** of a Boolean lattice $(L, \leq, \neg)$ is a tuple

$$(\wp(U), \subseteq, ^{-}).$$

Theorem 3.3.3 (Stone's Representation Theorem)**.** Every Boolean lattice is embeddable into its canonical extension via the Stone embedding for Boolean lattices.

Proof. We show that the Stone embedding $\theta : L \to \wp(U)$ for Boolean lattices is an embedding of a Boolean lattice $\mathcal{L} = (L, \leq, \neg)$ into the canonical extension $(\wp(U), \subseteq, ^{-})$ of $\mathcal{L}$.

- Proof of $\theta(p \wedge q) = \theta(p) \wedge \theta(q)$.

$$\begin{aligned} F \in \theta(p \wedge q) &\Leftrightarrow p \wedge q \in F \Leftrightarrow p \in F \text{ and } q \in F \\ &\Leftrightarrow F \in \theta(p) \text{ and } F \in \theta(q) \Leftrightarrow F \in \theta(p) \cap \theta(q). \end{aligned}$$

- Proof of $\theta(p \vee q) = \theta(p) \cup \theta(q)$. Recall that F is a prime filter (Theorem 3.2.13).

  ($\Rightarrow$)

  $$\begin{aligned} F \in \theta(p \vee q) &\Leftrightarrow p \vee q \in F \Rightarrow p \in F \text{ or } q \in F \\ &\Leftrightarrow F \in \theta(p) \text{ or } F \in \theta(q) \Leftrightarrow F \in \theta(p) \cup \theta(q). \end{aligned}$$

  ($\Leftarrow$) follows from the fact $p \leq p \vee q$.

- Proof of $\theta(\neg p) = \overline{\theta(p)}$. Because either $p \in F$ or $\neg p \in F$ (Theorem 3.2.13),

  $$F \in \theta(\neg p) \Leftrightarrow \neg p \in F \Leftrightarrow p \notin F \Leftrightarrow F \notin \theta(p).$$

To show that θ is injective, suppose $p \neq q$. Then $p \not\leq q$ or $q \not\leq p$ by the contraposition of the antisymmetry of $\leq$. Without loss of generality, we assume $p \not\leq q$. Then $p \wedge \neg q \neq \curlywedge$. For, suppose that $p \wedge \neg q = \curlywedge$. Then $p \wedge \neg q \leq p \wedge q$. Hence, $(p \wedge \neg q) \vee (p \wedge q) = p \wedge q$, and thus

$$p = p \wedge (\neg q \vee q) = (p \wedge \neg q) \vee (p \wedge q) = p \wedge q.$$

It is equivalent to $p \leq q$, which completes the proof of the implication from $p \not\leq q$ to $p \wedge \neg q \neq \curlywedge$. Therefore, we see that $\{p, \neg q\}$ has the finite meet property. It follows from Corollary 3.2.15 that there exists an ultrafilter $\widehat{F}$ satisfying $\langle \{p, \neg q\} \rangle \subseteq \widehat{F}$. It implies $p, \neg q \in \widehat{F}$. Equivalently, $\widehat{F} \in \theta(p)$ and $\widehat{F} \in \theta(\neg q) = \overline{\theta(q)}$. That is, $\widehat{F} \in \theta(p)$ but $\widehat{F} \notin \theta(q)$. Consequently, $\theta(p) \neq \theta(q)$, as desired. □

Corollary 3.3.4. Every Boolean lattice is isomorphic to an algebra of sets via the Stone embedding for Boolean lattices.

Proof. Because θ is injective, every Boolean lattice $(L, \leq, \neg)$ is isomorphic to $(\theta(L), \subseteq, ^-)$, where $\theta(L)$ denotes the image of L under θ. In addition, because θ is a homomorphism, $\theta(L)$ is closed under $\cap$, $\cup$, and $^-$. Clearly, $\theta(L) \subseteq \wp(U)$. Thus, $(\theta(L), \subseteq, ^-)$ is a filed of sets. □

Theorem 3.3.5. Let $\widetilde{U}$ be the set of all principal ultrafilters in an atomic complete Boolean lattice $(L, \leq, \neg)$. Then $(L, \leq, \neg)$ is isomorphic to $(\wp(\widetilde{U}), \subseteq, ^-)$ via the function $\tilde{\theta} : L \to \wp(\widetilde{U})$ defined by

$$\tilde{\theta}(p) = \{F \in \widetilde{U} : p \in F\}.$$

Proof. Let A be the set of all atoms in $(L, \leq, \neg)$. Then,

$$\tilde{\theta}(p) = \{a\uparrow : p \in \langle a \rangle \text{ and } a \in A\} \qquad \text{(By Theorem 3.2.11)}$$

$$= \{a\uparrow : a \leq p \text{ and } a \in A\}.$$

For the injectivity of $\tilde{\theta}$, suppose $p \neq q$. If either $p = \curlywedge$ or $q = \curlywedge$, we can suppose $p = \curlywedge$ without loss of generality. Then $\tilde{\theta}(p) = \emptyset$, but $\tilde{\theta}(q) \neq \emptyset$ by atomicity. Thus, $\tilde{\theta}(p) \neq \tilde{\theta}(q)$, which completes the proof. For this reason, we only consider the case that $p \neq \curlywedge$ and $q \neq \curlywedge$. Recall that atomicity and atomisticity are equivalent for Boolean lattices (Theorem 3.1.4). It follows from atomisticity and the assumption $p \neq q$ that

$$\bigvee\{a \in A : a \leq p\} = p \neq q = \bigvee\{a \in A : a \leq q\}.$$

Observe that $\bigvee \Gamma \neq \bigvee \Delta$ implies $\Gamma \neq \Delta$. Hence,

$$\{a \in A : a \leq p\} \neq \{a \in A : a \leq q\},$$

which implies that $a \leq p$ but $a \not\leq q$ for some $a \in A$. Therefore, $a\uparrow \in \tilde{\theta}(p)$ but $a\uparrow \notin \tilde{\theta}(q)$. Consequently, $\tilde{\theta}(p) \neq \tilde{\theta}(q)$.

For the surjectivity of $\tilde{\theta}$, it suffices to show that for any $M \in \wp(\widetilde{U})$, there exists $p \in L$ such that $M = \tilde{\theta}(p)$. Because M is a set of principal ultrafilters, it follows from Theorem 3.2.11 that

$$M = \{a\uparrow : a \in A'\}$$

for some $A' \subseteq A$. Thus, our goal is to show that $A' = \{a \in A : a \leq p\}$. Let $p = \bigvee A'$. Then $a' \leq p$ for any $a' \in A'$. Therefore, $A' \subseteq \{a \in A : a \leq p\}$. For the other inclusion, suppose by way of contradiction that $a^\circ \in \{a \in A : a \leq p\}$ for some $a^\circ \notin A'$. Then $a^\circ \leq p$, which implies

$$a^\circ = a^\circ \wedge p = a^\circ \wedge \bigvee A' = \bigvee\{a^\circ \wedge a' : a' \in A'\}$$

by Theorem 2.5.9. Because $a^\circ \notin A'$, we have $a^\circ \neq a'$ for any $a' \in A'$. It implies that $a^\circ \wedge a' < a'$. Because a' is an atom, $a^\circ \wedge a' = \curlywedge$. It follows from the above equation that $a^\circ = \curlywedge$. This is a contradiction with $a^\circ \in A$. □

3.4 Representation Theorem for Ortholattices

By regarding the orthogonality relation as a relation on a Hilbert space, we obtain a state transition system called an orthoframe [16]. Henceforth, we shall write $s \not R t$ for the condition that not sRt (namely, $(s,t) \notin R$).

Definition 3.4.1. An **orthoframe** $\mathcal{F} = (S, R)$ is a pair of a non-empty set S of states and relation R on S that is irreflexive ($s \not R s$ for any $s \in S$) and symmetric (sRt implies tRs for any $s, t \in S$).

Example 3.4.2 (Hilbert Frame)**.** Let $\mathcal{H}$ be a Hilbert space, $\mathsf{Pure}(\mathcal{H})$ be the set of all pure states (unit vectors) in $\mathcal{H}$, and $\perp$ be the orthogonality relation on $\mathcal{H}$. Then $(\mathsf{Pure}(\mathcal{H}), \perp)$ is an orthoframe, and is called a **Hilbert frame**. Note that $(\mathcal{H}, \perp)$ is not an orthoframe because $\perp$ is not irreflexive. A counter-example is that $\mathbf{0} \perp \mathbf{0}$, where $\mathbf{0}$ denotes the zero vector (origin of $\mathcal{H}$).

Usually, closed subspaces and the orthogonal complements of them are defined for Hilbert spaces. These notions are adapted for an orthoframe as follows. Recall that $V \subseteq \mathcal{H}$ is a closed subspace if and only if $(V^{\perp})^{\perp} = V$.

Definition 3.4.3. Let $\mathcal{F} = (S, R)$ be an orthoframe, and P be a (possibly empty) subset of S.

- The **orthogonal complement** $\neg_R P$ of P is defined by

$$\neg_R P = \{s \in S : sRt \text{ for any } t \in P\}.$$

- P is said to be **orthoclosed** in $\mathcal{F}$ if $\neg_R \neg_R P = P$.

Remark 3.4.4. $\emptyset^{\perp}$ is not defined because $\emptyset$ is not a vector space. On the other hand, $\neg_R \emptyset$ is defined and is equal to S by the definition of $\neg_R$. In addition, $\neg_R S = \emptyset$. If there would be $s \in S$ satisfying sRt for any $t \in S$, then sRs. However, R is irreflexive by the definition of R, a contradiction. Therefore, $\neg_R S = \emptyset$.

In the sequel, we shall denote by $L_{\mathcal{F}}$ the set of all orthoclosed sets in $\mathcal{F}$. That is,

$$L_{\mathcal{F}} = \{P \subseteq S : \neg_R \neg_R P = P\}.$$

The relation between ortholattices and orthoframes defined so far is intriguing. On the one hand, an ortholattice called a complex algebra is obtained from an orthoframe. On the other hand, an orthoframe called a canonical frame is obtained from an ortholattice. In fact, every complex algebra of an orthoframe is an ortholattice (Theorem 3.4.9), and every canonical frame of an ortholattice is an orthoframe (Theorem 3.4.13).

Definition 3.4.5. The **complex algebra** of an orthoframe $\mathcal{F} = (S, R)$ is the triple

$$\mathcal{C}(\mathcal{F}) = (L_{\mathcal{F}}, \subseteq, \neg_R),$$

where $\neg_R : L_{\mathcal{F}} \to L_{\mathcal{F}}$ is a function that returns the orthogonal complement of an input.

Remark 3.4.6. $\mathcal{C}(\mathcal{F})$ is well-defined in the sense that $\neg_R P \in L_{\mathcal{F}}$ for each $P \in L_{\mathcal{F}}$: because $P \in L_{\mathcal{F}}$,

$$\neg_R P = \neg_R(\neg_R \neg_R P) = (\neg_R \neg_R)\neg_R P.$$

The name "complex algebra" is derived from [11, Definition 5.21]. The same notion is also called "dual" (of an original frame) in [12], for example. However, because the word "dual" is also frequently used in different senses, we prefer to call it complex algebra to avoid ambiguity.

Hereafter, we shall denote by $\biguplus \Gamma$ the smallest orthoclosed set containing $\bigcup \Gamma$. Symbolically,

$$\biguplus \Gamma = \bigcap \{P \in L_{\mathcal{F}} : \bigcup \Gamma \subseteq P\}.$$

In particular, we shall write $P \uplus Q$ for $\biguplus\{P, Q\}$.

Theorem 3.4.7. Every complex algebra $\mathcal{C}(\mathcal{F})$ of an orthoframe $\mathcal{F} = (S, R)$ is a complete lattice by $\bigwedge \Gamma = \bigcap \Gamma$ and $\bigvee \Gamma = \biguplus \Gamma$.

Proof. Theorem 2.3.3 states that a closure system ordered by inclusion is a complete lattice. Thus, it suffices to show that $L_{\mathcal{F}}$ is a closure system on S. For this, see Lemma 3.4.8. □

Lemma 3.4.8. $L_{\mathcal{F}}$ is a closure system on S. That is,

(1) $\bigcap \Gamma \in L_{\mathcal{F}}$ for any non-empty set $\Gamma \subseteq L_{\mathcal{F}}$,

(2) $S \in L_{\mathcal{F}}$.

Proof. We show each of the conditions of closure systems.

(1) We only prove the case that the number of elements in Γ is 2. The general case is obtained by a similar argument.

Suppose that $\neg_R\neg_R P = P$ and $\neg_R\neg_R Q = Q$. Then it suffices to show that

$$\neg_R\neg_R(P \cap Q) = P \cap Q.$$

For the $\subseteq$-part, suppose by contradiction that $s \in \neg_R\neg_R(P \cap Q)$ but $s \notin P \cap Q$. Then either $s \notin P$ or $s \notin Q$. Without loss of generality, we assume $s \notin P$, and thus $s \notin \neg_R\neg_R P$. In other words, $s \not R t$ for some $t \in \neg_R P$. Fix $t \in \neg_R P$ such that $s \not R t$. Then sRt and tRu for any $u \in P$. By strengthening the condition of u, we can state that $s \not R t$ and tRu for any $u \in P \cap Q$. It is equivalent to saying that $s \not R t$ and $t \in \neg_R(P \cap Q)$. However, the assumption $s \in \neg_R\neg_R(P \cap Q)$ means that sRu for any $u \in \neg_R(P \cap Q)$, which leads to a contradiction.

The $\supseteq$-part is proved as follows:

$$\begin{aligned} s \in P \cap Q &\Leftrightarrow s \in \neg_R\neg_R P \cap \neg_R\neg_R Q \\ &\Leftrightarrow \forall t \in S\,(t \in \neg_R P \Rightarrow sRt) \text{ and } \forall t \in S\,(t \in \neg_R Q \Rightarrow sRt) \end{aligned}$$

$$
\begin{aligned}
&\Leftrightarrow \forall t \in S\,((t \in \neg_R P \Rightarrow sRt) \text{ and } (t \in \neg_R Q \Rightarrow sRt))\\
&\Leftrightarrow \forall t \in S\,((t \in \neg_R P \text{ or } t \in \neg_R Q) \Rightarrow sRt)\\
&\Leftrightarrow \forall t \in S\,((\forall u \in S\,(u \in P \Rightarrow tRu) \text{ or } \forall u \in S\,(u \in Q \Rightarrow tRu)) \Rightarrow sRt)\\
&\Rightarrow \forall t \in S\,((\forall u \in S\,(u \in P \Rightarrow tRu, \text{ or } u \in Q \Rightarrow tRu)) \Rightarrow sRt)\\
&\Leftrightarrow \forall t \in S\,((\forall u \in S,\, u \in P \text{ and } u \in Q \Rightarrow tRu) \Rightarrow sRt)\\
&\Leftrightarrow \forall t \in S\,((\forall u \in P \cap Q,\, tRu) \Rightarrow sRt)\\
&\Leftrightarrow s \in \neg_R\neg_R(P \cap Q).
\end{aligned}
$$

(2) By Remark 3.4.4,

$$\neg_R\neg_R S = \neg_R\emptyset = S.$$

□

Theorem 3.4.9. Every complex algebra $\mathcal{C}(\mathcal{F})$ of an orthoframe $\mathcal{F} = (S, R)$ is a complete ortholattice.

Proof. By Theorem 3.4.7, $\mathcal{C}(\mathcal{F})$ is a complete lattice. Thus, we only show that $\mathcal{C}(\mathcal{F})$ is an ortholattice. We first prove the conditions (2) and (3) in the definition of ortholattices (Definition 2.5.1).

(2) Proof of $\neg_R\neg_R P = P$. It immediately follows from $P \in L_{\mathcal{F}}$.

(3) Proof of the condition that $P \subseteq Q$ implies $\neg_R Q \subseteq \neg_R P$. Suppose that $P \subseteq Q$ and $s \in \neg_R Q$. Then $t \in P$ implies $t \in Q$, and $t \in Q$ implies sRt. Thus, $t \in P$ implies sRt, which is equivalent to $s \in \neg_R P$. Consequently, $P \subseteq Q$ implies $\neg_R Q \subseteq \neg_R P$.

Now we show that the remaining conditions $P \cap \neg_R P = \emptyset$ and $P \uplus \neg_R P = S$. Suppose for the sake of contradiction that $s \in P \cap \neg_R P$ for some $s \in S$. Then $s \in P$ and $s \in \neg_R P$, and thus sRs. However, it contradicts the condition that R is irreflexive. Hence, $P \cap \neg_R P = \emptyset$. Therefore, it follows from the above (2) and De Morgan's laws that

$$P \uplus \neg_R P = \neg_R(\neg_R P \cap \neg_R\neg_R P) = \neg_R(\neg_R P \cap P) = \neg_R\emptyset = S.$$

Note that De Morgan's laws are derivable from the above (2) and (3) using the same idea as in [33, Proposition 3.4]. □

Lemma 3.4.10 ([36, Proposition 2])**.** Let $(L, \leq, ^\perp)$ be a complete atomistic ortholattice, and let $\mathcal{A}(L)$ be the set of all atoms in $(L, \leq, ^\perp)$. Then the complex algebra $(L_{\mathcal{F}}, \subseteq, \neg_\perp)$ of the orthoframe $\mathcal{F}_L = (\mathcal{A}(L), \perp)$, where the relation $\perp$ is the same as in $(L, \leq, ^\perp)$, is isomorphic to the original ortholattice $(L, \leq, ^\perp)$.

Proof. We claim that the following mapping

$$\omega(p) = \{a \in \mathcal{A}(L) \ : \ a \leq p\} \quad (p \in L)$$

is an isomorphism of ortholattices between $(L, \leq, {}^{\perp})$ and $(L_{\mathcal{F}}, \subseteq, \neg_{\perp})$. First, we show that ω preserves the orthocomplementation: $\neg_{\perp}\omega(p) = \omega(p^{\perp})$ for any $p \in L$. Let $p \in L$. Because L is a complete atomistic ortholattice, we have

$$p = \bigvee_{a \in \omega(p)} a, \quad p^{\perp} = \bigwedge_{a \in \omega(p)} a^{\perp}.$$

Note that the orthogonality relation in the orthoframe $(\mathcal{A}(L), \perp)$ is the same as in $(L, \leq, {}^{\perp})$.

$$\begin{aligned}
\neg_{\perp}\omega(p) &= \{b \in \mathcal{A}(L) \ : \ b \perp a \text{ for any } a \in \omega(p)\} \\
&= \left\{b \in \mathcal{A}(L) \ : \ b \leq a^{\perp} \text{ for any } a \in \omega(p)\right\} \\
&= \left\{ b \in \mathcal{A}(L) \ : \ b \leq \bigwedge_{a \in \omega(p)} a^{\perp} \right\} \\
&= \left\{b \in \mathcal{A}(L) \ : \ b \leq p^{\perp}\right\} \\
&= \omega(p^{\perp}).
\end{aligned}$$

Hence, we have

$$\neg_{\perp}\neg_{\perp}\omega(p) = \omega((p^{\perp})^{\perp}) = \omega(p).$$

This implies that $\omega(p)$ is orthoclosed in $\mathcal{F}_L$, that is $\omega(p) \in L_{\mathcal{F}}$. Therefore, ω is a mapping from L to $L_{\mathcal{F}_L}$.

Next, we show that ω preserves infima and suprema.

- $\omega(p \wedge q) = \omega(p) \cap \omega(q)$: Let $a \in \omega(p \wedge q)$. Then we have $a \leq p \wedge q \leq p, q$. Hence,

  $$a \in \omega(p) \text{ and } a \in \omega(q).$$

  Therefore, we obtain $a \in \omega(p) \cap \omega(q)$. On the other hand, let $a \in \omega(p) \cap \omega(q)$. Then because $a \leq p, q$, we have $a \leq p \wedge q$; hence, $a \in \omega(p \wedge q)$.

- $\omega(p \vee q) = \omega(p) \uplus \omega(q)$: By De Morgan's laws, we obtain

  $$\begin{aligned}
  \omega(p \vee q) &= \omega((p^{\perp} \wedge q^{\perp})^{\perp}) = \neg_{\perp}\omega\left(p^{\perp} \wedge q^{\perp}\right) \\
  &= \neg_{\perp}\left(\omega(p^{\perp}) \cap \omega(q^{\perp})\right) = \neg_{\perp}\left(\neg_{\perp}\omega(p) \cap \neg_{\perp}\omega(q)\right) \\
  &= \omega(p) \uplus \omega(q).
  \end{aligned}$$

Finally, we show that ω is bijective. Let $\omega(p) = \omega(q)$ for some $p, q \in L$. Because L is atomistic, we have

$$p = \bigvee_{a \in \omega(p)} a = \bigvee_{a \in \omega(q)} a = q.$$

Therefore, ω is injective. To show that ω is surjective, take an arbitrary $A \in L_{\mathcal{F}}$. Put

$$p := \bigvee_{a \in A} a.$$

Here, we took the supremum in $(L, \leq, {}^{\perp})$ (Note that $A \subseteq \mathcal{A}(L) \subseteq L$). We show that this p is a witness of the surjectivity of ω: $\omega(p) = A$. Let $b \in A$. Then because $b \leq \bigvee_{a \in A} a = p$, we have $b \in \omega(p)$. Conversely, let $b \in \omega(p)$. Then we have $b \leq p$, and by the (infinite) De Morgan's law,

$$p = \left(\bigwedge_{a \in A} a^{\perp} \right)^{\perp}.$$

Hence, $b \leq p$ is equivalent to the condition

$$b \leq \left(\bigwedge_{a \in A} a^{\perp} \right)^{\perp}.$$

In the following, we show that assuming that $b \notin A$ leads to a contradiction. Now, because A is orthoclosed in $\mathcal{F}_L$, that is, $\neg_{\perp}\neg_{\perp} A = A$, we have

$$\begin{aligned} A = \neg_{\perp}\neg_{\perp} A &= \neg_{\perp}(\neg_{\perp} A) \\ &= \{ d \in \mathcal{A}(L) \ : \ d \perp c \ \text{ for any } c \in \neg_{\perp} A \}. \end{aligned}$$

By the assumption $b \notin A$, there exists $c \in \neg_{\perp} A$ such that $b \not\perp c$. Note that the condition $b \not\perp c$ is equivalent to the condition

$$b \not\leq c^{\perp}.$$

On the other hand, observe that

$$\begin{aligned} c \in \neg_{\perp} A &\Leftrightarrow c \perp a \ \text{ for all } a \in A \\ &\Leftrightarrow c \leq a^{\perp} \ \text{ for all } a \in A \\ &\Leftrightarrow c \leq \bigwedge_{a \in A} a^{\perp} \\ &\Leftrightarrow \left(\bigwedge_{a \in A} a^{\perp} \right)^{\perp} \leq c^{\perp}. \end{aligned}$$

By $b \leq p$, we have

$$b \leq \left(\bigwedge_{a \in A} a^{\perp} \right)^{\perp} \leq c^{\perp}.$$

This contradicts the condition that $b \not\leq c^{\perp}$. Therefore, we have $b \in A$. Consequently, we obtain $\omega(p) = A$; ω is surjective. □

Corollary 3.4.11. Every Hilbert lattice $(\mathcal{S}(\mathcal{H}), \subseteq, ^{\perp})$ is isomorphic to the complex algebra $(L_{\mathcal{F}_{\mathcal{H}}}, \subseteq, \neg_{\perp})$ of the Hilbert frame $\mathcal{F}_{\mathcal{H}} = (\Sigma(\mathcal{H}), \perp)$.

Definition 3.4.12. The **canonical frame** of an ortholattice $\mathcal{L} = (L, \leq, \neg)$ is the pair

$$\mathcal{C}(\mathcal{L}) = (S^{\mathcal{L}}, R^{\mathcal{L}})$$

of the set $S^{\mathcal{L}}$ of all proper filters of $(L, \leq)$ and the relation $R^{\mathcal{L}}$ on $S^{\mathcal{L}}$ defined by

$$R^{\mathcal{L}} = \{(F, G) : p \in F \text{ and } \neg p \in G \text{ for some } p \in L\}.$$

Theorem 3.4.13. Every canonical frame $\mathcal{C}(\mathcal{L})$ of an ortholattice $\mathcal{L} = (L, \leq, \neg)$ is an orthoframe.

Proof. $S^{\mathcal{L}}$ is non-empty because $\{\curlyvee\}$ is a proper filter.

$R^{\mathcal{L}}$ is irreflexive. Suppose for the sake of contradiction that $FR^{\mathcal{L}}F$ for some $F \in S^{\mathcal{L}}$. To lead a contradiction, we show that F is not proper. Equivalently, we show that $\curlywedge \in F$ (recall Theorem 3.2.5). By the assumption $FR^{\mathcal{L}}F$, there exists $p \in L$ such that $p, \neg p \in F$, and thus $p \wedge \neg p \in F$ by the definition of filters. It is equivalent to $\curlywedge \in F$ by the definition of ortholattices.

$R^{\mathcal{L}}$ is symmetric. $FR^{\mathcal{L}}G$ implies that $p \in F$ and $\neg p \in G$ for some $p \in L$. Put $q = \neg p$. Then $\neg q = \neg\neg p = p \in F$ and $q = \neg p \in G$. Thus, $GR^{\mathcal{L}}F$. □

The Stone-type representation theorem for ortholattices was first shown by [17]. It states that an ortholattice is embeddable into the canonical extension of the ortholattice.

Definition 3.4.14. The **Stone embedding** for ortholattices $\mathcal{L} = (L, \leq, \neg)$ is the function $\theta : L \to L_{\mathcal{C}(\mathcal{L})}$ defined by

$$\theta(p) = \{F \in S^{\mathcal{L}} : p \in F\}.$$

The **canonical extension** of an ortholattice $\mathcal{L} = (L, \leq, \neg)$ is the complex algebra $\mathcal{C}(\mathcal{C}(\mathcal{L}))$ of the canonical frame $\mathcal{C}(\mathcal{L})$ of $\mathcal{L}$.

Remark 3.4.15. θ is well-defined in the sense that $\theta(p) \in L_{\mathcal{C}(\mathcal{L})}$ for each $p \in L$. For, it suffices to show $\neg_{R^{\mathcal{L}}}\theta(p) = \theta(\neg p)$ because it implies

$$\neg_{R^{\mathcal{L}}}\neg_{R^{\mathcal{L}}}\theta(p) = \theta(\neg\neg p) = \theta(p).$$

For the $\subseteq$-part of $\neg_{R^{\mathcal{L}}}\theta(p) = \theta(\neg p)$, suppose $F \in \neg_{R^{\mathcal{L}}}\theta(p)$. Then $FR^{\mathcal{L}}G$ for $G = \{q : p \leq q\}$ satisfying $p \neq \curlywedge$ because $G \in \theta(p)$. Thus, there exists $r \in L$ such that $r \in F$ and $\neg r \in G$. Hence, $p \leq \neg r$ by $\neg r \in G$. It implies that $r \leq \neg p$. Recall $r \in F$. By the definition of filters, $\neg p \in F$. Consequently, $F \in \theta(\neg p)$.

For the $\supseteq$-part of $\neg_{R^{\mathcal{L}}}\theta(p) = \theta(\neg p)$, suppose $F \in \theta(\neg p)$ (equivalently, $\neg p \in F$). It suffices to show that $G \in \theta(p)$ (equivalently, $p \in G$) implies $FR^{\mathcal{L}}G$ for any $G \in L_{\mathcal{C}(\mathcal{L})}$. It follows from $\neg p \in F$ and $p \in G$ that $GR^{\mathcal{L}}F$, and thus $FR^{\mathcal{L}}G$, as desired.

Theorem 3.4.16 (Stone-type Representation Theorem for Ortholattices)**.** Every ortholattice is embeddable into its canonical extension via the Stone embedding for ortholattices.

Proof. We show that the Stone embedding $\theta : L \to L_{\mathcal{C}(\mathcal{L})}$ for ortholattices is an embedding of an ortholattice $\mathcal{L}$ into $\mathcal{C}(\mathcal{C}(\mathcal{L}))$.

(1) Proof of $\theta(p \wedge q) = \theta(p) \cap \theta(q)$.

$$\begin{aligned} F \in \theta(p \wedge q) &\Leftrightarrow p \wedge q \in F \Leftrightarrow p \in F \text{ and } q \in F \\ &\Leftrightarrow F \in \theta(p) \text{ and } F \in \theta(q) \Leftrightarrow F \in \theta(p) \cap \theta(q). \end{aligned}$$

(2) Proof of $\theta(p \vee q) = \theta(p) \uplus \theta(q)$. Because $\theta(p \wedge q) = \theta(p) \cap \theta(q)$ and $\theta(\neg p) = \neg_{R^{\mathcal{L}}}\theta(p)$ (for the proof, see below),

$$\theta(p \vee q) = \theta(\neg(\neg p \wedge \neg q)) = \neg_{R^{\mathcal{L}}}(\neg_{R^{\mathcal{L}}}\theta(p) \cap \neg_{R^{\mathcal{L}}}\theta(q)) = \theta(p) \cup \theta(q).$$

(3) Proof of $\theta(\neg p) = \neg_{R^{\mathcal{L}}}\theta(p)$. See Remark 3.4.15.

To show that θ is injective, suppose $p \neq q$. Then $p \not\leq q$ or $q \not\leq p$ by the contraposition of the antisymmetry of $\leq$. Without loss of generality, we assume $p \not\leq q$. Then $p \neq \curlywedge$; otherwise, $p \leq q$. Thus, it follows from Theorem 3.2.5 that the principal filter $p{\uparrow}$ is proper, and we have $q \notin p{\uparrow}$ by the assumption $p \not\leq q$. However, $p \in p{\uparrow}$ by the reflexivity of $\leq$. Therefore, $p{\uparrow} \in \theta(p)$ but $p{\uparrow} \notin \theta(q)$, which implies $\theta(p) \neq \theta(q)$, as desired. □

3.5 Representation Theorem for Modal Algebras

Orthoframes are state transition systems corresponding to ortholattices. Similarly, frames are state transition systems corresponding to modal algebras.

Definition 3.5.1. A (Kripke) **frame** is a pair (S, R) of a non-empty set S of states and relation R on S.

Observe that orthoframes are irreflexive and symmetric frames. Thus, frames are a more general notion than orthoframes.

Definition 3.5.2. The **complex algebra** of a frame $\mathcal{F} = (S, R)$ is the tuple

$$\mathcal{C}(\mathcal{F}) = (\wp(S), \subseteq, ^{-}, \Box_R),$$

where $(\wp(S), \subseteq, ^{-})$ is a powerset Boolean lattice, and $\Box_R$ is a function on $\wp(S)$ such that

$$\Box_R P = \{s \in S : sRt \text{ implies } t \in P \text{ for any } t \in S\}.$$

Definition 3.5.3. The **canonical frame** of a modal algebra $\mathcal{L} = (L, \leq, \neg, \Box)$ is the pair

$$\mathcal{C}(\mathcal{L}) = (S^{\mathcal{L}}, R^{\mathcal{L}})$$

of the set $S^{\mathcal{L}}$ of all ultrafilters of $(L, \leq)$ and the relation $R^{\mathcal{L}}$ on $S^{\mathcal{L}}$ defined by

$$R^{\mathcal{L}} = \{(F, G) : \Box p \in F \text{ implies } p \in G\}.$$

We have already defined homomorphisms for ortholattices/Boolean lattices in Definition 3.3.1. Here we define homomorphisms for modal algebras.

Definition 3.5.4. Let $(L_1, \leq_1, \neg_1, \Box_1)$ and $(L_2, \leq_2, \neg_2, \Box_2)$ be modal algebras. A function $f : L_1 \to L_2$ is called

- a **homomorphism** between modal algebras if the following conditions are satisfied:
  (1) f is a homomorphism between Boolean lattices,
  (2) $f(\Box_1 p) = \Box_2 f(p)$.
- an **embedding** between modal algebras if f is an injective homomorphism between modal algebras.
- an **isomorphism** between modal algebras if f is a bijective homomorphism between modal algebras.

A modal algebra $(L_1, \leq_1, \neg_1, \Box_1)$ is said to be **isomorphic** to a modal algebra $(L_2, \leq_2, \neg_2, \Box_2)$ if there exists an isomorphism from L_1 to L_2.

Definition 3.5.5. The **Stone embedding** for modal algebras $\mathcal{L} = (L, \leq, \neg, \Box)$ is the function $\theta : L \to \wp(S^{\mathcal{L}})$ defined by

$$\theta(p) = \{F \in S^{\mathcal{L}} : p \in F\}.$$

The **canonical extension** of a modal algebra $\mathcal{L} = (L, \leq, \neg, \Box)$ is the complex algebra $\mathcal{C}(\mathcal{C}(\mathcal{L}))$ of the canonical frame $\mathcal{C}(\mathcal{L})$ of $\mathcal{L}$.

Theorem 3.5.6 (Stone-type Representation Theorem for Modal Algebras)**.** Every modal algebra is embeddable into its canonical extension via the Stone embedding for modal algebras.

Proof. We show that the Stone embedding $\theta : L \to \wp(S^{\mathcal{L}})$ for modal algebras is an embedding of a modal algebra $\mathcal{L}$ into the canonical extension $\mathcal{C}(\mathcal{C}(\mathcal{L}))$ of $\mathcal{L}$.

Most part of the proof is reduced to the proof of Stone's representation theorem. It remains to show

$$\theta(\Box p) = \Box_{R^{\mathcal{L}}}\theta(p).$$

For the $\subseteq$-part, suppose $F \in \theta(\Box p)$ (equivalently, $\Box p \in F$). If $FR^{\mathcal{L}}G$, then $p \in G$ (recall that is, $G \in \theta(p)$) by the definition of $R^{\mathcal{L}}$. Hence, $F \in \Box_{R^{\mathcal{L}}}\theta(p)$.

For the $\supseteq$-part, suppose $F \in \Box_{R^{\mathcal{L}}}\theta(p)$. Let Γ be the set $\{q \in L : \Box q \in F\}$, which is non-empty because $\top \in \Gamma$ by $\Box\top = \top \in F$. Thus, there exists the smallest filter G containing Γ, which in fact is

$$\{q \in L : \bigwedge\{p_1, \ldots, p_n\} \leq q \text{ for some } p_1, \ldots, p_n \in \Gamma\}$$

by Theorem 3.2.3. Now we show $FR^{\mathcal{L}}G$, that is, $\Box q \in F$ implies $q \in G$ for any $q \in L$. If $\Box q \in F$, then $q \in \Gamma$, which implies $q \in G$. Consequently, $FR^{\mathcal{L}}G$. Hence, $G \in \theta(p)$ by the assumption $F \in \Box_{\mathcal{R}^{\mathcal{L}}}\theta(p)$, and is equivalent to $p \in G$. It implies that there exist $p_1, \ldots, p_n \in \Gamma$ such that $\bigwedge\{p_1, \ldots, p_n\} \leq p$. Thus, by Definition 2.5.10 (2) and the monotonicity of $\Box$ (Theorem 2.5.11),

$$\bigwedge\{\Box p_1, \ldots, \Box p_n\} = \Box(\bigwedge\{p_1, \ldots, p_n\}) \leq \Box p.$$

Because $p_1, \ldots, p_n \in \Gamma$, we have $\Box p_i \in F$. It follows from the definition of filters that $\Box p \in F$. Therefore, $F \in \theta(\Box p)$, as desired. $\Box$

Chapter 4

Quantum Dynamic Algebra

This chapter contains:

In this chapter, we formulate QDA, and show that the inference rules of Hoare Logic are satisfied in QDA if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\Cap$ (Theorem 4.2.4). Moreover, we formulate a transition system called a Quantum Dynamic Frame (QDF), and how to construct a QDA from a given QDF (Theorem 4.4.5). We use the constructed QDA called the complex algebra of a QDF for verifying the correctness of two simple quantum programs as running examples.

4.1 Quantum Dynamic Algebra

In this section, we formulate Quantum Dynamic Algebra (QDA). QDA specify all properties (namely, axioms) that DQL is supposed to satisfy. The advantage of using algebra rather than logic is that algebra can naturally express infinitary conjunction and disjunction as the infimum and the supremum of infinite sets, respectively. Infinitary conjunction is used to characterize $\Box(a^*, p)$ in Definition 4.1.2.

Definition 4.1.1. Let L be a non-empty set. A **regular program algebra** (RPA) is a tuple

$$\mathcal{P}[L] = (\mathsf{Prog}[L], ;, \cup, ^*, ?)$$

that consists of a non-empty set $\mathsf{Prog}[L]$ depending on L and functions

$$; : \mathsf{Prog}[L] \times \mathsf{Prog}[L] \to \mathsf{Prog}[L], \quad \cup : \mathsf{Prog}[L] \times \mathsf{Prog}[L] \to \mathsf{Prog}[L],$$
$$^* : \mathsf{Prog}[L] \to \mathsf{Prog}[L], \quad ? : L \to \mathsf{Prog}[L].$$

Let **skip** and **abort** be specific symbols (called **program constants**), and Π_0 be a set of symbols (called **atomic programs**). The RPA generated by $\Pi = \{\mathbf{skip}, \mathbf{abort}\} \cup \Pi_0$ is defined as the smallest RPA

$$\mathcal{P}[\Pi, L] = (\mathsf{Prog}[\Pi, L], ;, \cup, ^*, ?)$$

satisfying $\Pi \subseteq \mathsf{Prog}[\Pi, L]$, where $\mathsf{Prog}[\Pi, L]$ stands for a non-empty set depending on Π and L.

For the meaning of regular programs, see Table 4.1. Regular programs are formed from program constants **skip**, **abort**, atomic programs, and elements of a non-empty set by using the program constructs ; (sequential composition), $\cup$ (non-deterministic choice), * (iteration), and ? (test). These notations are used in Propositional Dynamic Logic (PDL). The most typical atomic programs are substitutions. The notion of variables is needed to define substitutions as is done in First-order Dynamic Logic. However, substitutions and variables are outside the scope of PDL. The reason why we do not deal with substitutions and variables in this paper is that our purpose is just to simplify the discussion. A drawback of First-order Dynamic Logic is that it is not decidable.

Table 4.1: Meaning of Regular Programs

Program	**Name**	**Meaning**
skip	Skip	Do nothing.
abort	Abort	Forcing to halt.
$a\ ;\ b$	Composition	Execute a, and then execute b.
$a \cup b$	Non-deterministic Choice	Execute either a or b non-deterministically.
a^*	Iteration	Repeat a some finite number of times.
$p?$	Test	Confirm that p is whether true or false.

Regular programs are expressive enough to describe various programs, such as conditional programs, guarded commands, while programs, and until programs.

- **Conditional Program**: the regular program

$$\textbf{if } p \textbf{ then } a \textbf{ else } b \textbf{ fi} = (p? \,;\, a) \cup (\neg p? \,;\, b)$$

  means that "if p is true, then execute a, otherwise execute b."

- **Guarded Command**: the regular program

$$p_1 \to a_1 \mid \cdots \mid p_n \to a_n = (p_1? \,;\, a_1) \cup \cdots \cup (p_n? \,;\, a_n)$$

  is the guarded command used in Dijkstra's Guarded Command Language. The guarded command is adopted in Promela, which is used by the SPIN model checker.

- **While Program**: the regular program

$$\textbf{while } p \textbf{ do } a \textbf{ od} = (p? \,;\, a)^* \,;\, \neg p?$$

  means that "repeat a while p is true."

- **Until Program**: the regular program

$$\textbf{repeat } a \textbf{ until } p = a \,;\, (\neg p? \,;\, a)^* \,;\, p?$$

  means that "repeat a until p is true."

As Hoare Logic does, it is worth paying attention to a precondition and postcondition of programs to verify them. A regular program $a \in \mathsf{Prog}[\Pi, L]$ is said to be **partially correct** with respect to a precondition $p \in L$ and postcondition $q \in L$ (denoted $\{p\}\, a\, \{q\}$, and is called a **Hoare triple**) if, whenever a is executed in a state satisfying p, and it halts in states s, then q is satisfied in any such states s. The correctness is called partial because it does not guarantee that the program halts.

We introduce a function $\Box : \mathsf{Prog}[\Pi, L] \times L \to L$ to express partial correctness: $\Box(a, p)$ represents the weakest precondition ensuring p will hold after executing a. Then $\{p\}\, a\, \{q\}$ is expressed as $p \leq \Box(a, q)$. That is, $\Box(a, q)$ is the weakest precondition among preconditions that make the program a partially correct with respect to the postcondition q. This function $\Box$ is subject to some conditions described in Definition 4.1.2.

Definition 4.1.2. A **quantum dynamic algebra** (QDA) is a tuple

$$\mathcal{L}_{\mathrm{QD}} = (L, \leq, \neg, \Box)$$

that consists of a complete orthomodular lattice $(L, \leq, \neg)$ and a function (scalar multiplication) $\Box : \mathsf{Prog}[\Pi, L] \times L \to L$ satisfying the following conditions: for any $\pi \in \Pi_0$, $a, b \in \mathsf{Prog}[\Pi, L]$, and $p, q \in L$,

(1) $\neg\Box(\pi, p) = \Box(\pi, \neg p)$;

(2) $\Box(\mathbf{skip}, p) = p$;

(3) $\Box(\mathbf{abort}, p) = \Upsilon$;

(4) $\Box(a, \Upsilon) = \Upsilon$;

(5) $\Box(a, p \wedge q) = \Box(a, p) \wedge \Box(a, q)$;

(6) $\Box(a; b, p) = \Box(a, \Box(b, p))$;

(7) $\Box(a \cup b, p) = \Box(a, p) \wedge \Box(b, p)$;

(8) $\Box(a^*, p) = \bigwedge\{\Box(a^i, p) : i \geq 0\}$, where a^i is defined recursively by $a^0 = \mathbf{skip}$ and $a^{i+1} = a^i \,;\, a$;

(9) $\Box(p?, q) = \neg p \vee (p \wedge q)$.

Note that DQL is not the only algebra that interprets tests as elements of a weak Boolean lattice. For example, tests in Constructive Dynamic Logic (CDL) [28] are interpreted as elements of a Heyting lattice, which is the algebraic semantics of Intuitionistic Logic. Orthomodular lattices lack the distributive law but satisfy the law of double negation. On the other hand, Heyting lattices lack the law of double negation but satisfy the distributive law.

Here we note the meaning of the above conditions from (1) to (9).

(1) Negation $\neg$ preserves the dynamic operator $\Box$.

(2) p will hold after executing **skip** (do nothing) if and only if p holds now.

(3) p will hold after executing **abort** (forcing to halt) if and only if Υ holds now.

(4) Υ will hold after executing a if and only if Υ holds now.

(5) $p \wedge q$ will hold after executing a if and only if p and q will hold after executing a.

(6) p will hold after executing $a \,;\, b$ if and only if p will hold after executing a and b consecutively in this order.

(7) p will hold after executing $a \cup b$ if and only if p will hold regardless of whether a or b is executed.

(8) p will hold after executing a^* if and only if p will hold no matter how many times a is repeatedly executed. $\Box(a^*, p)$ exists owing to the completeness of $(L, \leq, \neg)$. The condition (8) of Definition 4.1.2 is called $*$-continuity.

(9) q will hold after executing $p?$ if and only if $\neg p \vee (p \wedge q)$. Here, $\neg p \vee (p \wedge q)$ is the equivalent form of the implication (that is, p implies q) in Quantum Logic just as $\neg p \vee q$ is that in Classical Logic. In particular, $\neg p \vee (p \wedge q)$ is called the **Sasaki hook** if the underlying lattice is a Hilbert lattice (see Example 4.1.4). It means that quantum tests are regarded as the implications in Quantum Logic. This identification is similar to that in (Classical) Dynamic Algebra: classical tests are regarded as the implication in Classical Logic.

Unlike (classical) Dynamic Algebra, the condition regarding atomic programs is added, and tests are evaluated in a complete orthomodular lattice (not a complete Boolean lattice). As we noted above, tests in QDA are the implications in Quantum Logic. Thus, these tests should be called quantum tests.

Example 4.1.3 (Powerset Dynamic Algebra)**.** A powerset Boolean lattice $(\wp(S), \subseteq, {}^{-}, \Box)$ with a function $\Box$ satisfying the conditions of Definition 4.1.2 is a QDA, and is called a **powerset dynamic algebra**.

Example 4.1.4 (Hilbert Dynamic Algebra)**.** A Hilbert lattice $(\mathcal{S}(\mathcal{H}), \subseteq, {}^{\perp}, \Box)$ with a function $\Box$ satisfying the conditions of Definition 4.1.2 is a QDA and is called a **Hilbert dynamic algebra**. In fact, $\Box(V?, W)$ is the inverse image

$$P_V^{-1}(W) := \{v \in \mathcal{H} : P_V(v) \in W\}$$

of W under the self-adjoint projection $P_V : \mathcal{H} \to \mathcal{H}$ onto V [19].

Another significant example of QDA is a complex algebra. We define the algebra and prove that every complex algebra is a QDA in Theorem 4.4.5.

4.2 Inference Rules for Quantum Programs

The **law of residuation**

$$p \wedge q \leq r \iff q \leq p \to r$$

holds in Boolean lattices, where $p \to r$ denotes the (material) implication $\neg p \vee r$ in Classical Logic. This law amounts to the algebraic deduction theorem: r is derivable from the assumptions p and q if and only if $p \to r$ is derivable from the assumption q. However, the Sasaki hook $p \rightsquigarrow r := \neg p \vee (p \wedge r)$ does not satisfy the counterpart

$$p \wedge q \leq r \iff q \leq p \rightsquigarrow r$$

in orthomodular lattices. In fact, the law of residuation implies the distributive law [19]. Contrapositively, non-distributive lattices (such as orthomodular lattices) cannot satisfy the law of residuation.

On the other hand, orthomodular lattices satisfy the law of residuation by changing the definition of conjunction. New conjunction $\Cap$ defined by

$$p \Cap q := p \wedge (\neg p \vee q)$$

is called the Sasaki conjunction, named after the Sasaki projection

$$\phi_p(q) = p \wedge (\neg p \vee q)$$

in [34]. The Sasaki projection ϕ_p is a projection onto p in Hilbert lattices. The Sasaki conjunction is equal to the usual conjunction in Boolean lattices because of the distributive law:

$$p \Cap q = p \wedge (\neg p \vee q) = (p \wedge \neg p) \vee (p \wedge q) = p \wedge q.$$

As the next theorem states, the law of residuation is satisfied if $\wedge$ is replaced by $\Cap$.

Theorem 4.2.1. $p \Cap q \leq r$ if and only if $q \leq p \rightsquigarrow r$.

Proof. ($\Rightarrow$) Assume $p \Cap q \leq r$. Then,

$$\neg p \vee (p \wedge (p \Cap q)) \leq \neg p \vee (p \wedge r) = p \rightsquigarrow r.$$

Thus, it suffices to show that

$$q \leq \neg p \vee (p \wedge (p \Cap q)).$$

It is proved as follows:

$$\begin{aligned}
& p \wedge (\neg p \vee (p \wedge \neg q)) \leq \neg q && \text{(By the orthomodular law)} \\
\Leftrightarrow\ & \neg\neg q \leq \neg(p \wedge (\neg p \vee (p \wedge \neg q))) && \text{(By Definition 2.5.1 (2) and (3))} \\
\Leftrightarrow\ & q \leq \neg p \vee (p \wedge (\neg p \vee q)) && \text{(By Definition 2.5.1 (2) and Theorem 2.5.3)} \\
\Leftrightarrow\ & q \leq \neg p \vee (p \wedge (p \wedge (\neg p \vee q))) \\
\Leftrightarrow\ & q \leq \neg p \vee (p \wedge (p \Cap q)).
\end{aligned}$$

($\Leftarrow$) Assume $q \leq p \rightsquigarrow r$. Then,

$$p \wedge (\neg p \vee q) \leq p \wedge (\neg p \vee (p \rightsquigarrow r)).$$

Thus,

$$\begin{aligned}
p \Cap q = p \wedge (\neg p \vee q) &\leq p \wedge (\neg p \vee (p \rightsquigarrow r)) \\
&= p \wedge (\neg p \vee (\neg p \vee (p \wedge r))) \\
&= p \wedge (\neg p \vee (p \wedge r)) \\
&= p \wedge r && \text{(By Theorem **??**)} \\
&\leq r.
\end{aligned}$$

□

By replacing $\wedge$ with $\Cap$, some rules in Hoare Logic hold owing to the law of residuation. To show this, we prepare two lemmas, Lemma 4.2.2 and 4.2.3.

Lemma 4.2.2. $\Box(a, -)$ is monotonic: $p \leq q$ implies $\Box(a, p) \leq \Box(a, q)$ for each $a \in \mathsf{Prog}[\Pi, L]$.

Proof. Similar to Theorem 2.5.11. □

Lemma 4.2.3. The loop invariance rule

$$\frac{\{p\}\, a\, \{p\}}{\{p\}\, a^*\, \{p\}}$$

holds: $p \leq \Box(a, p)$ implies $p \leq \Box(a^*, p)$.

Proof. Assume $p \leq \Box(a, p)$. Then,

$$\Box(a, p) \leq \Box(a, \Box(a, p)) = \Box(a^2, p)$$

is obtained by Lemma 4.2.2. Thus, $p \leq \Box(a^2, q)$. Repeating this discussion yields $p \leq \Box(a^i, q)$ for each natural number $i \geq 0$ (the case of $i = 0$ follows from Definition 4.1.2 (2) and the reflexivity of $\leq$). Hence, $p \leq \Box(a^*, p)$ is obtained by Definition 4.1.2 (8). □

Here we prove that the inference rules in Hoare Logic are sound if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\Cap$. The proof is based on quantum counterparts of the law of residuation (Theorem 4.2.1), the monotonicity of $\Box$ (Lemma 4.2.2), and the loop invariance rule (Lemma 4.2.3).

Theorem 4.2.4. The following rules of Hoare Logic (where $\wedge$ is replaced by $\Cap$) are satisfied in QDA. More precisely, the following rules are sound with respect to the algebraic semantics given by QDA.

(1) The **skip** rule (axiom):

$$\frac{}{\{p\}\, \mathbf{skip}\, \{p\}}$$

That is, $p \leq \Box(\mathbf{skip}, p)$.

(2) The composition rule:

$$\frac{\{p\}\, a\, \{q\} \qquad \{q\}\, b\, \{r\}}{\{p\}\, a\, ;\, b\, \{r\}}$$

That is, $p \leq \Box(a, q)$ and $q \leq \Box(b, r)$ jointly imply that $p \leq \Box(a \,;\, b, r)$.

(3) The conditional rule:

$$\frac{\{p \Cap q\}\, a\, \{r\} \qquad \{\neg p \Cap q\}\, b\, \{r\}}{\{q\}\ \textbf{if}\ p\ \textbf{then}\ a\ \textbf{else}\ b\ \textbf{fi}\ \{r\}}$$

That is, $p \Cap q \leq \Box(a, r)$ and $\neg p \Cap q \leq \Box(b, r)$ jointly imply that $q \leq \Box((p? \,;\, a) \cup (\neg p? \,;\, b), r)$.

(4) The **while** rule:

$$\frac{\{p \Cap q\}\, a\, \{q\}}{\{q\}\ \textbf{while}\ p\ \textbf{do}\ a\ \textbf{od}\ \{\neg p \Cap q\}}$$

That is, $p \Cap q \leq \Box(a, q)$ implies $q \leq \Box((p? \,;\, a)^* \,;\, \neg p?, \neg p \Cap q)$.

(5) The weakening rule:

$$\frac{p \leq p' \qquad \{p'\}\, a\, \{q'\} \qquad q' \leq q}{\{p\}\, a\, \{q\}}$$

That is, if $p \leq p'$, $p' \leq \Box(a, q')$, and $q' \leq q$, then $p \leq \Box(a, q)$.

Proof.

(1)

$$\begin{aligned} p &\leq p && \text{(By the reflexivity of } \leq) \\ &= \Box(\textbf{skip}, p). && \text{(By Definition 4.1.2 (2))} \end{aligned}$$

(2)

$$\begin{aligned} p \leq \Box(a, q) \text{ and } q \leq \Box(b, r) &\Rightarrow p \leq \Box(a, q) \text{ and } \Box(a, q) \leq \Box(a, \Box(b, r)) \\ &\qquad \text{(By Lemma 4.2.2)} \\ &\Rightarrow p \leq \Box(a, \Box(b, r)) \quad \text{(By the transitivity of } \leq) \\ &\Leftrightarrow p \leq \Box(a \,;\, b, r). \qquad \text{(By Definition 4.1.2 (6))} \end{aligned}$$

(3)

$$\begin{aligned} p \Cap q \leq \Box(a,r) &\Leftrightarrow q \leq p \rightsquigarrow \Box(a,r) && \text{(By Theorem 4.2.1)} \\ &\Leftrightarrow q \leq \neg p \vee (p \wedge \Box(a,r)) \\ &\Leftrightarrow q \leq \Box(p?, \Box(a,r)) && \text{(By Definition 4.1.2 (9))} \\ &\Leftrightarrow q \leq \Box(p? \,;\, a, r). && \text{(By Definition 4.1.2 (6))} \end{aligned}$$

Similarly,

$$\neg p \Cap q \leq \Box(b,r) \Leftrightarrow q \leq \Box(\neg p? \,;\, b, r)$$

is obtained. Thus,

$$\begin{aligned} p \Cap q \leq \Box(a,r) \text{ and } \neg p \Cap q \leq \Box(b,r) &\Leftrightarrow q \leq \Box(p? \,;\, a, r) \wedge \Box(\neg p? \,;\, b, r) \\ &\Leftrightarrow q \leq \Box((p? \,;\, a) \cup (\neg p? \,;\, b), r). \\ & \qquad \text{(By Definition 4.1.2 (7))} \end{aligned}$$

(4)

$$\begin{aligned} p \Cap q \leq \Box(a,q) &\Leftrightarrow q \leq p \rightsquigarrow \Box(a,q) && \text{(By Theorem 4.2.1)} \\ &\Leftrightarrow q \leq \neg p \vee (p \wedge \Box(a,q)) \\ &\Leftrightarrow q \leq \Box(p?, \Box(a,q)) && \text{(By Definition 4.1.2 (9))} \\ &\Leftrightarrow q \leq \Box(p? \,;\, a, q) && \text{(By Definition 4.1.2 (6))} \\ &\Rightarrow q \leq \Box((p? \,;\, a)^*, q) && \text{(By Lemma 4.2.3)} \end{aligned}$$

Thus, the proof is completed if

$$\Box((p? \,;\, a)^*, q) \leq \Box((p? \,;\, a)^* \,;\, \neg p?, \neg p \Cap q)$$

is proved. It is shown as follows:

$$\begin{aligned} q \leq p \vee q &\Leftrightarrow q \leq p \vee (\neg p \wedge (p \vee q)) && \text{(By Theorem \textbf{??})} \\ &\Leftrightarrow q \leq \neg\neg p \vee (\neg p \wedge (\neg p \wedge (\neg\neg p \vee q))) && \text{(By Definition 2.5.1 (2))} \\ &\Leftrightarrow q \leq \neg\neg p \vee (\neg p \wedge (\neg p \Cap q)) \\ &\Leftrightarrow q \leq \Box(\neg p?, \neg p \Cap q) && \text{(By Definition 4.1.2 (9))} \\ &\Rightarrow \Box((p? \,;\, a)^*, q) \leq \Box((p? \,;\, a)^*, \Box(\neg p?, \neg p \Cap q)) \\ & \qquad \text{(By Lemma 4.2.2)} \\ &\Leftrightarrow \Box((p? \,;\, a)^*, q) \leq \Box((p? \,;\, a)^* \,;\, \neg p?, \neg p \Cap q). \\ & \qquad \text{(By Definition 4.1.2 (6))} \end{aligned}$$

(5) $p \leq p'$ and $p' \leq \Box(a, q')$ jointly imply $p \leq \Box(a, q')$ by the transitivity of $\leq$. On the other hand, $q' \leq q$ implies $\Box(a, q') \leq \Box(a, q)$ by Lemma 4.2.2. Thus, $p \leq \Box(a, q)$ by the transitivity of $\leq$.

□

Owing to Theorem 4.2.4, it is expected to apply QDA to quantum program verification. The validity of the Hoare-like inference rules means that the inference rules in Hoare Logic also work in the quantum setting as long as the appropriate logical connective(s) are chosen.

4.3 Quantum Dynamic Frame

So far, we have not mentioned the notion of states at all. However, it is helpful to intuitively understand the properties of quantum programs by representing their execution by relations.

A relation R_a on S is defined for each $a \in \mathsf{Prog}[\Pi, L]$. That is, sR_at is intended that t is reachable from s by executing a. For this reason, we extend orthoframes by adding relations for programs.

Definition 4.3.1. A **quantum dynamic frame** (QDF) is a triple

$$\mathcal{F}_{\mathrm{QD}} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$$

that consists of an orthoframe $\mathcal{F} = (S, R)$, family $\mathcal{U} = \{\mathfrak{u}_\pi : \pi \in \Pi_0\}$ of functions on S, and family $\mathcal{R} = \{R_a : a \in \mathsf{Prog}[\Pi, L_\mathcal{F}]\}$ of relations on S satisfying the following conditions: for any $\pi \in \Pi_0$, $a, b \in \mathsf{Prog}[\Pi, L_\mathcal{F}]$, and $P \in L_\mathcal{F}$,

(1) $sR_{\mathbf{skip}}t$ if and only if $s = t$;

(2) $R_{\mathbf{abort}} = \emptyset$;

(3) $sR_\pi t$ if and only if $\mathfrak{u}_\pi(s) = t$;

(4) $sR_{a;b}t$ if and only if sR_au and uR_bt for some $u \in S$;

(5) $sR_{a\cup b}t$ if and only if $s(R_a \cup R_b)t$;

(6) $sR_{a^*}t$ if and only if $s(\bigcup_{i\geq 0} R_{a^i})t$;

(7) $sR_{P?}t$ if and only if $t \in P \Cap Q$ for any $Q \in L_\mathcal{F}$ satisfying $s \in Q$;

(8) $\mathfrak{u}_\pi$ is bijective: for any $t \in S$, there exists exactly one $s \in S$ such that $t = \mathfrak{u}_\pi(s)$;

(9) $\mathfrak{u}_\pi$ preserves R: sRt if and only if $\mathfrak{u}_\pi(s)R\mathfrak{u}_\pi(t)$;

(10) $R_{P?}$ is self-adjoint: for any $s, t, u \in S$, if $sR_{P?}t$ and $t \not R u$, then $uR_{P?}v$ and $s \not R v$ for some $v \in S$.

Example 4.3.2 (Hilbert Dynamic Frame)**.** Let $\{U_\pi : \pi \in \Pi_0\}$ be a family of unitary operators (quantum gates) on $\mathcal{H}$. Then for any Hilbert frame $(\mathcal{H}\setminus\{\mathbf{0}\}, \perp)$, the QDF $(\mathcal{H} \setminus \{\mathbf{0}\}, \perp, \mathcal{R})$, called a **Hilbert dynamic frame**, is uniquely constructed from $\{\mathfrak{u}_\pi : \pi \in \Pi_0\}$. It is not difficult to show that $(\mathcal{H} \setminus \{\mathbf{0}\}, \perp, \mathcal{R})$ is a QDF.

The self-adjointness of frames is also defined in [2, 8, 25] for different kinds of frames. The self-adjointness of quantum transition frames is defined in [2], that of quantum dynamic frames is defined in [8], and that of DO-frames is defined in [25]. The self-adjointness of frames is an abstraction of the self-adjointness of operators.

Example 4.3.3. Let $\mathcal{F}_\mathcal{H}$ be a Hilbert frame $(\Sigma(\mathcal{H}), \perp)$ (recall Example 3.4.2). Then by Corollalry 3.4.11, the complex algebra $(L_{\mathcal{F}_\mathcal{H}}, \subseteq, \neg_\perp)$ of the Hilbert frame $(\Sigma(\mathcal{H}), \perp)$ is isomorphic to the Hilbert lattice $(\mathcal{S}(\mathcal{H}), \subseteq, ^\perp)$ as ortholattices. Henceforth, we identify an element $V \in L_\mathcal{H}$ with the corresponding closed subspace of $\mathcal{H}$. Put $\mathcal{U} = \{U_\pi : \pi \in \Pi_0\}$, where each U_π denotes a unitary operator (quantum gate) on $\mathcal{H}$. By the condition in Definition 4.3.1, $\mathcal{R} = \{R_a : a \in \mathsf{Prog}[\Pi, L_{\mathcal{F}_\mathcal{H}}]\}$ is uniquely constructed from $\mathcal{U}$. Here, we show that $(\Sigma(\mathcal{H}), \perp, \mathcal{U}, \mathcal{R})$ is a star-free QDF. By the definition of unitary operators, U_π is bijective and preserves $\perp$ for each $\pi \in \Pi_0$. To show that $R_{V?}$ is self-adjoint, first observe that

$$\begin{aligned} R_{V?} &= \{(s,t) : s \in W \text{ implies } t \in V \cap (V^\perp \uplus W) \text{ for each } W \in L_{\mathcal{F}_\mathcal{H}}\} \\ &= \{(s,t) : s \in W \text{ implies } t \in P_V[W] \text{ for each } W \in L_{\mathcal{F}_\mathcal{H}}\} \qquad \text{(see [34])} \\ &= \{(s,t) : P_V[s] = t\}, \end{aligned}$$

where $P_V : \mathcal{H} \to \mathcal{H}$ denotes the self-adjoint projection onto V, and $P_V[\,]$ denotes the image under P_V. For the self-adjointness of $R_{V?}$, it suffices to show that $P_V[s] \not\perp u$ implies $s \not\perp P_V[u]$. Recall that P_V is said to be self-adjoint (as an operator on $\mathcal{H}$) if

$$\langle P_V(x), y | P_V(x), y\rangle = \langle x, P_V(y) | x, P_V(y)\rangle$$

for any $x, y \in \mathcal{H}$, where $\langle\cdot,\cdot|\cdot,\cdot\rangle$ stands for the inner product on $\mathcal{H}$. Note that for any $w, u \in \Sigma(\mathcal{H})$, $w \not\perp u$ if and only if $\langle \bar{w}, \bar{u} | \bar{w}, \bar{u}\rangle \neq 0$, where $\bar{w}$ and $\bar{u}$ stand for unit vectors in one-dimensional subspaces w and u, respectively. This shows that the self-adjointness of P_V implies that of $R_{V?}$.

Remark 4.3.4. Although the definition of $R_{P?}$ in this paper is different from that in [2, 8], the properties called the

- **adequacy** ($s \in P$ implies $sR_{P?}s$) of $R_{P?}$ and
- **repeatability** ($sR_{P?}t$ implies $t \in P$) of $R_{P?}$

are also satisfied. For the adequacy of $R_{P?}$, assume $s \in P$ and $s \in Q$. Then,

$$s \in \neg_R P \cup Q \subseteq \neg_R P \uplus Q$$

by $s \in Q$, and thus $s \in P \cap (\neg_R P \uplus Q)$ by $s \in P$. That is, $s \in P$ implies $sR_{P?}s$. For the repeatability of $R_{P?}$, assume $sR_{P?}t$. Because $S \in L_{\mathcal{F}}$ (Theorem 3.4.8 (2)), we have

$$t \in P \cap (\neg_R P \uplus S) = P.$$

4.4 Complex Algebra of QDF

Complex algebras are employed to verify systems. Suppose a state transition system modeling the actual system to be verified is given. The property to be verified can be confirmed by searching for states that can be transitioned from the initial state in that system. This kind of verification is called reachability analysis and is one of the prominent techniques for model checking. However, some properties can be proved without actually searching for possible transition states. For example, "if a property p holds in the current state, then p also holds after executing **skip**" is always true regardless of an underlying state transition system. Thus, extra calculations can be omitted in reachability analysis if the properties that always hold (let us say "valid") are known in advance. Algebras provide the answer to what properties are valid. For example, $\Box(\mathbf{skip}, p) = p$ corresponds to the above property. Not only the equations that appear in the definition of algebras but also any equations obtained in the algebras correspond to properties that are valid. In this way, algebraic computation is useful in the reachability analysis of state transition systems, and complex algebras relate state transition systems to algebras.

The notion of the complex algebras of an orthoframe (Definition 3.4.5) is now extended to that of a QDF.

Definition 4.4.1. The **complex algebra** of a QDF $\mathcal{F}_{\mathrm{QD}} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$ is a tuple

$$\mathcal{C}(\mathcal{F}_{\mathrm{QD}}) = (L_{\mathcal{F}}, \subseteq, \neg_R, \Box_{\mathcal{R}})$$

that consists of the set $L_{\mathcal{F}}$ of all orthoclosed sets in $\mathcal{F}$, set inclusion relation $\subseteq$ on $L_{\mathcal{F}}$, and functions $\neg_R : L_{\mathcal{F}} \to L_{\mathcal{F}}$ and $\Box_{\mathcal{R}} : \mathsf{Prog}[\Pi, L_{\mathcal{F}}] \times L_{\mathcal{F}} \to L_{\mathcal{F}}$ such that

(1) $\neg_R P = \{s \in S : sRt \text{ for any } t \in P\}$ (recall Definition 3.4.3),

(2) $\Box_{\mathcal{R}}(a, P) = \{s \in S : t \in P \text{ for any } t \in S \text{ satisfying } sR_a t\}$.

Remark 4.4.2. $\mathcal{C}(\mathcal{F}_{\mathrm{QD}})$ is well-defined in the sense that $\neg_R P \in L_{\mathcal{F}}$ and $\Box_{\mathcal{R}}(a, P) \in L_{\mathcal{F}}$ for each $P \in L_{\mathcal{F}}$. For the proof of $\neg_R P \in L_{\mathcal{F}}$, see Remark 3.4.6. Before embarking on the proof of $\Box_{\mathcal{R}}(a, P) \in L_{\mathcal{F}}$, we prepare the following lemma.

Lemma 4.4.3.

(1) $\neg_R \Box_{\mathcal{R}}(\pi, P) = \Box_{\mathcal{R}}(\pi, \neg_R P)$.

(2) $\Box_{\mathcal{R}}(\mathbf{skip}, P) = P$.

(3) $\Box_{\mathcal{R}}(\mathbf{abort}, P) = S$.

(4) $\Box_{\mathcal{R}}(a, S) = S$.

(5) $\Box_{\mathcal{R}}(a, P \cap Q) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(a, Q)$.

(6) $\Box_{\mathcal{R}}(a \,;\, b, P) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P))$.

(7) $\Box_{\mathcal{R}}(a \cup b, P) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P)$.

(8) $\Box_{\mathcal{R}}(a^*, P) = \bigcap\{\Box_{\mathcal{R}}(a^i, P) : i \geq 0\}$.

(9) $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q)$.

Proof.

(1) Proof of $\neg_R \Box_{\mathcal{R}}(\pi, P) = \Box_{\mathcal{R}}(\pi, \neg_R P)$. Observe that

$$\begin{aligned}\Box_{\mathcal{R}}(\pi, P) &= \{s \in S : \forall t \in S\,(sR_\pi t \Rightarrow t \in P)\} \\ &= \{s \in S : \forall t \in S\,(\mathfrak{u}_\pi(s) = t \Rightarrow t \in P)\} \\ &= \{s \in S : \mathfrak{u}_\pi(s) \in P\}.\end{aligned}$$

In other words, $\Box_{\mathcal{R}}(\pi, P)$ is the inverse image of P under $\mathfrak{u}_\pi$. Thus,

$$\begin{aligned}\neg_R \Box_{\mathcal{R}}(\pi, P) &= \{s \in S : \forall u \in S\,(u \in \Box_{\mathcal{R}}(\pi, P) \Rightarrow sRu)\} \\ &\qquad\qquad \text{(By Definition 4.3.1 (9))} \\ &= \{s \in S : \forall u \in S\,(\mathfrak{u}_\pi(u) \in P \Rightarrow \mathfrak{u}_\pi(s) R \mathfrak{u}_\pi(u))\} \\ &\qquad\qquad \text{(By Definition 4.3.1 (8))} \\ &= \{s \in S : \forall t \in S\,(t \in P \Rightarrow \mathfrak{u}_\pi(s) R t)\} \\ &= \{s \in S : \mathfrak{u}_\pi(s) \in \neg_R P\} = \Box_{\mathcal{R}}(\pi, \neg_R P).\end{aligned}$$

(2) Proof of $\Box_{\mathcal{R}}(\mathbf{skip}, P) = P$. Immediate.

(3) Proof of $\Box_{\mathcal{R}}(\mathbf{abort}, P) = S$. Immediate.

(4) Proof of $\Box_{\mathcal{R}}(a, S) = S$. Immediate.

(5) Proof of $\Box_{\mathcal{R}}(a, P \cap Q) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(a, Q)$.

$$\begin{aligned}
\Box_{\mathcal{R}}(a, P \cap Q) &= \{s \in S : \forall t \in S\,(sR_at \Rightarrow t \in P \cap Q)\} \\
&= \{s \in S : \forall t \in S\,(sR_at \Rightarrow t \in P \text{ and } t \in Q)\} \\
&= \{s \in S : \forall t \in S\,((sR_at \Rightarrow t \in P) \text{ and } (sR_at \Rightarrow t \in Q))\} \\
&= \{s \in S : \forall t \in S\,(sR_at \Rightarrow t \in P) \text{ and } \forall t \in S\,(sR_at \Rightarrow t \in Q)\} \\
&= \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(a, Q).
\end{aligned}$$

(6) Proof of $\Box_{\mathcal{R}}(a\,;b, P) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P))$.

$$\begin{aligned}
\Box_{\mathcal{R}}(a\,;b, P) &= \{s \in S : \forall t \in S\,(\exists u \in S\,(sR_au \text{ and } uR_bt) \Rightarrow t \in P)\} \\
&= \{s \in S : \forall t \in S\,(\forall u \in S \text{ not } (sR_au \text{ and } uR_bt) \text{ or } t \in P)\} \\
&= \{s \in S : \forall t \in S,\, \forall u \in S\,(\text{not } (sR_au \text{ and } uR_bt) \text{ or } t \in P)\} \\
&= \{s \in S : \forall u \in S,\, \forall t \in S\,(\text{not } (sR_au \text{ and } uR_bt) \text{ or } t \in P)\} \\
&= \{s \in S : \forall u \in S,\, \forall t \in S\,(s\not{R}_au \text{ or } u\not{R}_bt \text{ or } t \in P)\} \\
&= \{s \in S : \forall u \in S\,(s\not{R}_au \text{ or } \forall t \in S\,(u\not{R}_bt \text{ or } t \in P))\} \\
&= \{s \in S : \forall u \in S\,(sR_au \Rightarrow \forall t \in S\,(uR_bt \Rightarrow t \in P))\} \\
&= \{s \in S : \forall u \in S\,(sR_au \Rightarrow u \in \Box_{\mathcal{R}}(b, P))\} \\
&= \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P)).
\end{aligned}$$

(7) Proof of $\Box_{\mathcal{R}}(a \cup b, P) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P)$.

$$\begin{aligned}
\Box_{\mathcal{R}}(a \cup b, P) &= \{s \in S : \forall t \in S\,(s(R_a \cup R_b)t \Rightarrow t \in P)\} \\
&= \{s \in S : \forall t \in S\,(sR_at \text{ or } sR_bt \Rightarrow t \in P)\} \\
&= \{s \in S : \forall t \in S\,((sR_at \Rightarrow t \in P) \text{ and } (sR_bt \Rightarrow t \in P))\} \\
&= \{s \in S : \forall t \in S\,(sR_at \Rightarrow t \in P) \text{ and } \forall t \in S\,(sR_bt \Rightarrow t \in P)\} \\
&= \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P).
\end{aligned}$$

(8) Proof of $\Box_{\mathcal{R}}(a^*, P) = \bigcap\{\Box_{\mathcal{R}}(a^i, P) : i \geq 0\}$.

$$\begin{aligned}
\Box_{\mathcal{R}}(a^*, P) &= \{s \in S : \forall t \in S\,(s(\bigcup\nolimits_{i\geq 0} R_{a^i})t \Rightarrow t \in P)\} \\
&= \bigcap\{\Box_{\mathcal{R}}(a^i, P) : i \geq 0\}
\end{aligned}$$

is obtained in a similar way as in the case of $a \cup b$.

(9) Proof of $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q)$.

For the $\subseteq$-part, suppose $s \notin \neg_R(P \cap \neg_R(P \cap Q))$. Then there exists $t \in S$ such that

$(\star)$ $t \in P \cap \neg_R(P \cap Q)$

but $s \not R t$. Thus, $t R_{P?} t$ by the adequacy of $R_{P?}$ (Remark 4.3.4). Because $t R_{P?} t$ and $t \not R s$ (the symmetry of $\not R$ follows from that of R), it follows from the self-adjointness of $R_{P?}$ that $s R_{P?} u$ and $t \not R u$ for some $u \in S$.

$$\begin{array}{ccc} t & \xrightarrow{R_{P?}} & t \\ {\scriptstyle \not R}\downarrow & & \downarrow{\scriptstyle \not R} \\ \exists u & \xleftarrow{R_{P?}} & s \end{array}$$

By $(\star)$, $t \in \neg_R(P \cap Q)$. That is, $t \not R v$ implies $v \notin P \cap Q$ for any $v \in S$. Hence, $u \notin P \cap Q$ by $t \not R u$. It implies that $u \notin P$ or $u \notin Q$, but the former must be false by $s R_{P?} u$. Therefore, $u \notin Q$ is obtained. It means that $s R_{P?} u$ and $u \notin Q$ for some $u \in S$. Equivalently, $s \notin \Box_{\mathcal{R}}(P?, Q)$.

For the $\supseteq$-part, suppose $s \notin \Box_{\mathcal{R}}(P?, Q)$. Then there exists $t \in S$ such that $s R_{P?} t$ but $t \notin Q$. Thus, $t \notin \neg_R \neg_R Q$ by $Q \in L_{\mathcal{F}}$. Hence, $u \in \neg_R Q$ but $t \not R u$ for some $u \in S$. Because $s R_{P?} t$ and $t \not R u$, it follows from the self-adjointness of $R_{P?}$ that $u R_{P?} v$ and $s \not R v$ for some $v \in S$.

$$\begin{array}{ccc} s & \xrightarrow{R_{P?}} & t \\ {\scriptstyle \not R}\downarrow & & \downarrow{\scriptstyle \not R} \\ \exists v & \xleftarrow{R_{P?}} & u \end{array}$$

Therefore, $v \in P \cap (\neg_R P \uplus \neg_R Q)$ by $u R_{P?} v$ and $u \in \neg_R Q$. Consequently, it follows from $s \not R v$ that

$$s \notin \neg_R(P \cap (\neg_R P \uplus \neg_R Q)) = \neg_R P \uplus (\neg_R \neg_R P \cap \neg_R \neg_R Q) = \neg_R P \uplus (P \cap Q).$$

□

Theorem 4.4.4. $L_{\mathcal{F}}$ is closed under $\Box_{\mathcal{R}}$: $\Box_{\mathcal{R}}(a, P) \in L_{\mathcal{F}}$ for each $P \in L_{\mathcal{F}}$.

Proof. We prove by structural induction on $a \in \mathsf{Prog}[\Pi, L]$.

(1) The base cases, namely $a = \mathbf{skip}$, $a = \mathbf{abort}$, or $a = \pi \in \Pi_0$. If $a = \mathbf{skip}$, then $\Box_{\mathcal{R}}(a, P) = P \in L_{\mathcal{F}}$ by Lemma 4.4.3 (2). If $a = \mathbf{abort}$, then $\Box_{\mathcal{R}}(a, P) = S \in L_{\mathcal{F}}$ by Lemma 4.4.3 (3) and Lemma 3.4.8 (2). If $a = \pi \in \Pi_0$, then it follows from Lemma 4.4.3 (1) and Definition 2.5.1 (2) that

$$\neg_R \neg_R \Box_{\mathcal{R}}(\pi, P) = \neg_R \Box_{\mathcal{R}}(\pi, \neg_R P) = \Box_{\mathcal{R}}(\pi, P).$$

(2) For the case $a = b\,;\,c$, $\Box_{\mathcal{R}}(a\,;\,b, P) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P)) \in L_{\mathcal{F}}$ by Lemma 4.4.3 (6) and the induction hypothesis.

(3) For the case $a = b \cup c$, $\Box_{\mathcal{R}}(a \cup b, P) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P) \in L_{\mathcal{F}}$ by Lemma 4.4.3 (7), Lemma 3.4.8 (1), and the induction hypothesis.

(4) For the case $a = b^*$, $\Box_{\mathcal{R}}(b^*, P) = \bigcap\{\Box_{\mathcal{R}}(b^i, P) : i \geq 0\} \in L_{\mathcal{F}}$ by Lemma 4.4.3 (8), Lemma 3.4.8 (1), and the induction hypothesis.

(5) For the case $a = P?$, $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q) \in L_{\mathcal{F}}$ by Lemma 4.4.3 (9) and the definition of $\uplus$.

□

Theorem 4.4.5. Every complex algebra $\mathcal{C}(\mathcal{F}_{\mathrm{QD}})$ of QDFs $\mathcal{F}_{\mathrm{QD}} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$ is a QDA.

Proof. We need to show that $(L_{\mathcal{F}}, \subseteq, \neg_R)$ is a complete orthomodular lattice, and $\mathcal{C}(\mathcal{F}_{\mathrm{QD}})$ satisfies the conditions from (1) to (11) in Definition 5.1.2.

It follows from Theorem 3.4.9 that $(L_{\mathcal{F}}, \subseteq, \neg_R)$ is a complete ortholattice. It follows from Lemma **??** that $\mathcal{C}(\mathcal{F}_{\mathrm{QD}})$ satisfies the conditions from (1) to (11) in Definition 5.1.2.

It remains to show that $(L_{\mathcal{F}}, \subseteq, \neg_R)$ satisfies the orthomodular law

$$P \cap (\neg_R P \uplus (P \cap Q)) \subseteq Q.$$

The condition (11) in Definition 5.1.2 states that $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q)$. Thus, it suffices to show $P \cap \Box_{\mathcal{R}}(P?, Q) \subseteq Q$. Take an arbitrary $s \in P$. Then because $s \in P$, it follows from the adequacy of $R_{P?}$ (Remark 4.3.4) that $sR_{P?}s$. Therefore, because $s \in \Box_{\mathcal{R}}(P?, Q)$, we obtain $s \in Q$. Consequently, $P \cap \Box_{\mathcal{R}}(P?, Q) \subseteq Q$. □

4.5 Running Examples

Finally, we apply Theorem 4.4.5 to verification of the partial correctness of quantum programs. The verification procedure is as follows.

Step 1 Prepare a quantum program (quantum protocol or quantum algorithm) and a precondition and postcondition of the quantum program.

Step 2 Construct a QDF (quantum state transition system) from the quantum gates used in the quantum program.

Step 3 Construct the complex algebra from the QDF by following Definition 4.4.1.

Step 4 Describe the weakest precondition of the quantum program as an element of the complex algebra and rewrite it by following the rules from (1) to (9) in Definition 4.1.2. (The theoretical background of this step is based on Theorem 4.4.5.)

As an example, we verify the partial correctness of simple while-do/if-then-else programs according to the above procedure.

While-do Program

For the discussion below, we introduce some notations. Let $\langle |\psi_1\rangle, \ldots, |\psi_n\rangle\rangle$ be the smallest closed subspace that contains a set $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ of ket vectors and $\langle |\psi_1\rangle, \ldots, |\psi_n\rangle\rangle_{\mathbf{0}}$ be $\langle |\psi_1\rangle, \ldots, |\psi_n\rangle\rangle$ without the origin (zero vector) $\mathbf{0}$. That is,

$$\langle |\psi_1\rangle, \ldots, |\psi_n\rangle\rangle_{\mathbf{0}} = \langle |\psi_1\rangle, \ldots, |\psi_n\rangle\rangle \setminus \{\mathbf{0}\}.$$

In addition, let H be the Hadamard gate and $\mathtt{H}$ be the atomic program corresponding to H. The quantum program **qwhile** defined below is borrowed from [39, Example 3.1].

Step 1. We verify the partial correctness of the quantum program

$$\textbf{qwhile} := \textbf{while } \langle |1\rangle\rangle_{\mathbf{0}} \textbf{ do } \mathtt{H} \textbf{ od}$$

with respect to the precondition $\langle |-\rangle\rangle_{\mathbf{0}}$ and postcondition $\langle |0\rangle\rangle_{\mathbf{0}}$, where $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$. The program **qwhile** means that while $\langle |1\rangle\rangle_{\mathbf{0}}$ holds (while it is confirmed that the current state is in $\langle |1\rangle\rangle_{\mathbf{0}}$), execute H.

Step 2. For the purpose of verification of the partial correctness of **qwhile**, it suffices to fix S, R, and $\mathfrak{u}_{\mathtt{H}}$ as follows:

$$S = \mathbb{C}^2 \setminus \{\mathbf{0}\}, \quad R = \perp, \quad \mathfrak{u}_{\mathtt{H}} = H,$$

where $\mathbb{C}^2$ denotes the complex 2-space, and $\perp$ denotes the orthogonality relation. Formally, this is not the full description of the QDF $\mathcal{F}$. The other components of $\mathcal{F}$ irrelevant to the following discussion are omitted.

Step 3. Then we can calculate the components $L_{\mathcal{F}}$, $\subseteq$, $\neg_R$, and $\Box_{\mathcal{R}}$ of the complex algebra $\mathcal{C}(\mathcal{F}_{\mathrm{QD}})$ by following Definition 4.4.1.

Step 4. Now we deduce the Hoare triple $\{\langle|-\rangle\rangle_{\mathbf{0}}\}$ **while** $\langle|1\rangle\rangle_{\mathbf{0}}$ **do** H **od** $\{\langle|0\rangle\rangle_{\mathbf{0}}\}$ by using the established rules in Theorem 4.2.4. Observe that $\{\langle|1\rangle\rangle_{\mathbf{0}}\}$ H $\{\langle|-\rangle\rangle_{\mathbf{0}}\}$. Because

$$\langle|1\rangle\rangle_{\mathbf{0}} \Cap \langle|-\rangle\rangle_{\mathbf{0}} = \langle|1\rangle\rangle_{\mathbf{0}} \cap (\neg_R\langle|1\rangle\rangle_{\mathbf{0}} \uplus \langle|-\rangle\rangle_{\mathbf{0}}) = \langle|1\rangle\rangle_{\mathbf{0}},$$

we have $\{\langle|1\rangle\rangle_{\mathbf{0}} \Cap \langle|-\rangle\rangle_{\mathbf{0}}\}$ H $\{\langle|-\rangle\rangle_{\mathbf{0}}\}$. Thus, by the **while** rule, we obtain $\{\langle|-\rangle\rangle_{\mathbf{0}}\}$ **while** $\langle|1\rangle\rangle_{\mathbf{0}}$ **do** H **od** $\{\neg_R\langle|1\rangle\rangle_{\mathbf{0}} \Cap \langle|-\rangle\rangle_{\mathbf{0}}\}$. Because

$$\neg_R\langle|1\rangle\rangle_{\mathbf{0}} \Cap \langle|-\rangle\rangle_{\mathbf{0}} = \neg_R\langle|1\rangle\rangle_{\mathbf{0}} \cap (\neg_R\neg_R\langle|1\rangle\rangle_{\mathbf{0}} \uplus \langle|-\rangle\rangle_{\mathbf{0}}) = \langle|0\rangle\rangle_{\mathbf{0}},$$

we have $\{\langle|-\rangle\rangle_{\mathbf{0}}\}$ **while** $\langle|1\rangle\rangle_{\mathbf{0}}$ **do** H **od** $\{\langle|0\rangle\rangle_{\mathbf{0}}\}$.

If-then-else Program

Consider the situation in that Alice wants to send a quantum state to Bob. However, because the state is fragile, she should not send the state itself. Instead, she transmits sufficient classical information for Bob to regenerate the state. It is achieved by quantum teleportation protocol [6]. This protocol is depicted in Figure 4.1, where $|\psi\rangle$ stands for any ket vector.

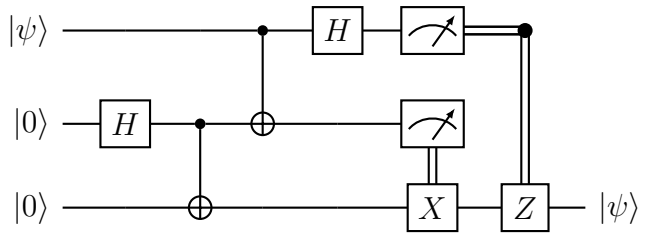


Figure 4.1: Quantum Teleportation

We use the following abbreviations to verify quantum teleportation. Because it is clear from the context, we use the same symbol $\mathbf{0}$ for the origins in different Hilbert spaces $\mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$.

$$|\varphi\rangle := |00\rangle \otimes |\psi\rangle + |01\rangle \otimes X|\psi\rangle + |10\rangle \otimes Z|\psi\rangle + |11\rangle \otimes XZ|\psi\rangle,$$

$$P' := \langle |00\rangle \otimes |\psi\rangle, |01\rangle \otimes X|\psi\rangle, |10\rangle \otimes Z|\psi\rangle, |11\rangle \otimes XZ|\psi\rangle\rangle_{\mathbf{0}},$$
$$P'' := \langle |00\rangle \otimes |\psi\rangle, |01\rangle \otimes |\psi\rangle, |10\rangle \otimes Z|\psi\rangle, |11\rangle \otimes Z|\psi\rangle\rangle_{\mathbf{0}},$$
$$P(0, |0\rangle) := \langle|0\rangle\rangle_{\mathbf{0}} \otimes \mathbb{C}^2 \otimes \mathbb{C}^2,$$
$$P(1, |0\rangle) := \mathbb{C}^2 \otimes \langle|0\rangle\rangle_{\mathbf{0}} \otimes \mathbb{C}^2$$

Furthermore, let $\mathtt{H}[1]$, $\mathtt{CNOT}[1,2]$, $\mathtt{CNOT}[0,1]$, $\mathtt{H}[0]$ be the atomic programs that correspond to the unitary operators $I \otimes H \otimes I$, $I \otimes CNOT$, $CNOT \otimes I$, and $H \otimes I \otimes I$, respectively, where I denotes the identity operator, and $CNOT$ denotes the controlled NOT gate.

We verify the partial correctness of the quantum program

$$\begin{aligned} \textbf{teleport} &= \mathtt{H}[1] \,;\, \mathtt{CNOT}[1,2] \,;\, \mathtt{CNOT}[0,1] \,;\, \mathtt{H}[0] \,;\, \textbf{qtmeasure}, \\ \textbf{qtmeasure} &= \textbf{if } p(1,|0\rangle) \textbf{ then skip else } \mathtt{X}[2] \textbf{ fi} \\ &\quad ; \textbf{if } p(0,|0\rangle) \textbf{ then skip else } \mathtt{Z}[2] \textbf{ fi}. \end{aligned}$$

with respect to the precondition $\langle |\psi\rangle \otimes |00\rangle \rangle_{\mathbf{0}}$ and postcondition $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}$. That is, we verify the statement "$|\psi\rangle$ is correctly teleported." Recall that **if** p **then** a **else** b **fi** is an abbreviation for $(p? \,;\, a) \cup (\neg p? \,;\, b)$.

Because the procedure for verifying **teleport** is similar to that for verifying **qwhile** in Section 4.5, we only show the crucial part. The Hoare triple $\{\langle |\psi\rangle \otimes |00\rangle \rangle_{\mathbf{0}}\}$ **teleport** $\{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}\}$ is derived by using the established rules in Theorem 4.2.4.

$\{\langle |\psi\rangle \otimes |00\rangle \rangle_{\mathbf{0}}\}\ \mathtt{H}[1] \,;\, \mathtt{CNOT}[1,2] \,;\, \mathtt{CNOT}[0,1] \,;\, \mathtt{H}[0]\ \{\langle |\varphi\rangle \rangle_{\mathbf{0}}\}$ (1)

$\langle |\varphi\rangle \rangle_{\mathbf{0}} \subseteq P'$ (2)

$\{\langle |\psi\rangle \otimes |00\rangle \rangle_{\mathbf{0}}\}\ \mathtt{H}[1] \,;\, \mathtt{CNOT}[1,2] \,;\, \mathtt{CNOT}[0,1] \,;\, \mathtt{H}[0]\ \{P'\}$ (3: weakning 1,2)

$\{P(1,|0\rangle) \Cap P'\}$ **skip** $\{P(1,|0\rangle) \Cap P'\}$ (4: skip)

$P(1,|0\rangle) \Cap P' \subseteq P''$ (5)

$\{P(1,|0\rangle) \Cap P'\}$ **skip** $\{P''\}$ (6: weakning 4,5)

$\{\langle |01\rangle \otimes X|\psi\rangle, |11\rangle \otimes XZ|\psi\rangle \rangle_{\mathbf{0}}\}\ \mathtt{X}[2]\ \{\langle |01\rangle \otimes |\psi\rangle, |11\rangle \otimes Z|\psi\rangle \rangle_{\mathbf{0}}\}$ (7)

$\langle |01\rangle \otimes |\psi\rangle, |11\rangle \otimes Z|\psi\rangle \rangle_{\mathbf{0}} \subseteq P''$ (8)

$\langle |01\rangle \otimes X|\psi\rangle, |11\rangle \otimes XZ|\psi\rangle \rangle_{\mathbf{0}} = \neg_R P(1,|0\rangle) \Cap P'$ (9)

$\{\neg_R P(1,|0\rangle) \Cap P'\}\ \mathtt{X}[2]\ \{P''\}$ (10: weakning 7,8,9)

$\{P'\}$ **if** $P(1,|0\rangle)$ **then skip else** $\mathtt{X}[2]$ **fi** $\{P''\}$ (11: conditional 6,10)

$\{P(0,|0\rangle) \Cap P''\}$ **skip** $\{P(0,|0\rangle) \Cap P''\}$ (12: skip)

$P(0,|0\rangle) \Cap P'' \subseteq \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle$ (13)

$\{P(0,|0\rangle) \Cap P''\}$ **skip** $\{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}\}$ (14: weakning 12,13)

$\{\langle |10\rangle \otimes Z|\psi\rangle, |11\rangle \otimes Z|\psi\rangle \rangle_{\mathbf{0}}\}\ \mathtt{Z}[2]\ \{\langle |10\rangle \otimes |\psi\rangle, |11\rangle \otimes |\psi\rangle \rangle_{\mathbf{0}}\}$ (15)

$\langle |10\rangle \otimes |\psi\rangle, |11\rangle \otimes |\psi\rangle \rangle_{\mathbf{0}} \subseteq \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}$ (16)

$\langle |10\rangle \otimes Z|\psi\rangle, |11\rangle \otimes Z|\psi\rangle \rangle_{\mathbf{0}} = \neg_R P(0,|0\rangle) \Cap P''$ (17)

$\{\neg_R P(0,|0\rangle) \Cap P''\}\ \mathtt{Z}[2]\ \{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}\}$ (18: weakning 15,16,17)

$\{P''\}$ **if** $P(0,|0\rangle)$ **then skip else** $\mathtt{Z}[2]$ **fi** $\{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle |\psi\rangle \rangle_{\mathbf{0}}\}$ (19: conditional 14,18)

$\{P'\}$ **if** $P(1,|0\rangle)$ **then skip else** $\mathtt{X}[2]$ **fi** ; **if** $P(0,|0\rangle)$ **then skip else** $\mathtt{Z}[2]$ **fi**
$\{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle|\psi\rangle\rangle_{\mathbf{0}}\}$ (20: composition 11,19)
$\{\langle|\psi\rangle \otimes |00\rangle\rangle_{\mathbf{0}}\}$ **teleport** $\{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \langle|\psi\rangle\rangle_{\mathbf{0}}\}$ (21: composition 3,20)

Chapter 5

The Stone-type Representation Theorem for Star-free QDA

This chapter contains:

In this chapter, we focus on the star-free fragment: We show how to construct a star-free QDA from a given star-free QDF (Theorem 5.3.4) and how to construct a star-free QDF from a given star-free QDA (Theorem 5.4.4). We apply these construction methods to prove our main theorem, the Stone-type representation theorem for star-free QDAs (Theorem 5.5.3).

5.1 Star-free Quantum Dynamic Algebra

First of all, we define the star-free fragments of RPA and QDA, respectively. Note that QDA is not just QDA without the iteration operator: a star-free QDA is a QDA equipped with an auxiliary operator $\blacksquare$ for proving the Stone-type representation theorem.

Definition 5.1.1. Let L be a non-empty set. A **star-free regular program algebra** (star-free RPA) is a tuple

$$\mathcal{P}^{-}[L] = (\mathsf{Prog}^{-}[L], ;, \cup, ?)$$

that consists of a non-empty set $\mathsf{Prog}^-[L]$ depending on L and functions

$$\begin{aligned} ; &: \mathsf{Prog}^-[L] \times \mathsf{Prog}^-[L] \to \mathsf{Prog}^-[L], \\ \cup &: \mathsf{Prog}^-[L] \times \mathsf{Prog}^-[L] \to \mathsf{Prog}^-[L], \\ ? &: L \to \mathsf{Prog}^-[L]. \end{aligned}$$

Let **skip** and **abort** be specific symbols (called **program constants**), and Π_0 be a set of symbols (called **atomic programs**). The star-free RPA generated by $\Pi = \{\mathbf{skip}, \mathbf{abort}\} \cup \Pi_0$ is defined as the smallest star-free RPA

$$\mathcal{P}^-[\Pi, L] = (\mathsf{Prog}^-[\Pi, L], ;, \cup, ?)$$

satisfying $\Pi \subseteq \mathsf{Prog}^-[\Pi, L]$, where $\mathsf{Prog}[\Pi, L]$ stands for a non-empty set depending on Π and L.

Star-free QDA is not just QDA without the iteration operator: a star-free QDA is an algebra equipped with an auxiliary operator $\blacksquare$ for proving the Stone-type representation theorem (Theorem 5.5.3).

Definition 5.1.2. A **star-free quantum dynamic algebra** (star-free QDA) is a tuple

$$\mathcal{L}^-_{\mathrm{QD}} = (L, \leq, \neg, \Box, \blacksquare)$$

that consists of an orthomodular lattice $(L, \leq, \neg)$ and functions (scalar multiplication)

$$\Box : \mathsf{Prog}^-[\Pi, L] \times L \to L, \quad \blacksquare : \Pi_0 \times L \to L$$

satisfying the following conditions: for any $\pi \in \Pi_0$, $a, b \in \mathsf{Prog}^-[\Pi, L]$, and $p, q \in L$,

(1) $\neg\Box(\pi, p) = \Box(\pi, \neg p)$;

(2) $\blacksquare(\pi, \Box(\pi, p)) = \Box(\pi, \blacksquare(\pi, p)) = p$;

(3) $\blacksquare(\pi, \Upsilon) = \Upsilon$;

(4) $\blacksquare(\pi, p \wedge q) = \blacksquare(\pi, p) \wedge \blacksquare(\pi, q)$;

(5) $\Box(\mathbf{skip}, p) = p$;

(6) $\Box(\mathbf{abort}, p) = \Upsilon$;

(7) $\Box(a, \Upsilon) = \Upsilon$;

(8) $\Box(a, p \wedge q) = \Box(a, p) \wedge \Box(a, q)$;

(9) $\Box(a \,;\, b, p) = \Box(a, \Box(b, p))$;

(10) $\Box(a \cup b, p) = \Box(a, p) \wedge \Box(b, p)$;

(11) $\Box(p?, q) = \neg p \vee (p \wedge q)$.

One concern is whether the addition of the conditions with respect to $\blacksquare$ for convenience causes problems when applying star-free QDFs to quantum program verification. In fact, these conditions are satisfied in star-free Hilbert Dynamic Algebra (see below).

Example 5.1.3 (Star-free Hilbert Dynamic Algebra)**.** A Hilbert lattice $(\mathcal{S}(\mathcal{H}), \subseteq, ^{\perp}, \Box, \blacksquare)$ with $\Box$ and $\blacksquare$ satisfying the conditions of Definition 5.1.2 is a star-free QDA, and is called **star-free Hilbert synamic algebra**. In fact, $\Box(V?, W)$ is the inverse image

$$P_V^{-1}(W) = \{v \in \mathcal{H} : P_V(v) \in W\}$$

of W under the projection $P_V : \mathcal{H} \to \mathcal{H}$ onto V [19]

5.2 Star-free Quantum Dynamic Frame

Star-free quantum dynamic frames are just star-free fragments of quantum dynamic frames. We restate the conditions for convenience.

Definition 5.2.1. A **star-free quantum dynamic frame** (star-free QDF) is a tuple

$$\mathcal{F}_{\mathrm{QD}}^{-} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$$

that consists of an orthoframe $\mathcal{F} = (S, R)$, family $\mathcal{U} = \{\mathfrak{u}_\pi : \pi \in \Pi_0\}$ of functions on S, and family $\mathcal{R} = \{R_a : a \in \mathsf{Prog}^{-}[\Pi, L_{\mathcal{F}}]\}$ of relations on S satisfying the following conditions:

(1) $sR_{\mathbf{skip}}t$ if and only if $s = t$;

(2) $R_{\mathbf{abort}} = \emptyset$;

(3) $sR_\pi t$ if and only if $\mathfrak{u}_\pi(s) = t$;

(4) $sR_{a;b}t$ if and only if $sR_a u$ and $uR_b t$ for some $u \in S$;

(5) $sR_{a \cup b}t$ if and only if $s(R_a \cup R_b)t$;

(6) $sR_{P?}t$ if and only if $t \in P \Rrightarrow Q$ for any $Q \in L_{\mathcal{F}}$ satisfying $s \in Q$;

(7) $\mathfrak{u}_\pi$ is bijective: for any $t \in S$, there exists exactly one $s \in S$ such that $t = \mathfrak{u}_\pi(s)$;

(8) $\mathfrak{u}_\pi$ preserves R: sRt if and only if $\mathfrak{u}_\pi(s)R\mathfrak{u}_\pi(t)$;

(9) $R_{P?}$ is self-adjoint: for any $s,t,u \in S$, if $sR_{P?}t$ and $t\not R u$, then $uR_{P?}v$ and $s\not R v$ for some $v \in S$.

Example 5.2.2. Let $\mathcal{F}_\mathcal{H}$ be a Hilbert frame $(\mathsf{Pure}(\mathcal{H}), \perp)$ (recall Example 3.4.2). Then each $V \in L_{\mathcal{F}_\mathcal{H}}$ is a closed subspace of $\mathcal{H}$. Put $\mathcal{U} = \{U_\pi : \pi \in \Pi_0\}$, where each U_π denotes a unitary operator (quantum gate) on $\mathcal{H}$. By the condition in Definition 5.2.1, $\mathcal{R} = \{R_a : a \in \mathsf{Prog}^-[\Pi, L_{\mathcal{F}_\mathcal{H}}]\}$ is uniquely constructed from $\mathcal{U}$. Here, we show that $(\mathsf{Pure}(\mathcal{H}), \perp, \mathcal{U}, \mathcal{R})$ is a star-free QDF. By the definition of unitary operators, U_π is bijective and preserves $\perp$. To show that $R_{V?}$ is self-adjoint, first observe that

$$\begin{aligned} R_{V?} &= \{(s,t) : s \in W \text{ implies } t \in V \cap (V^\perp \uplus W) \text{ for each } W \in L_{\mathcal{F}_\mathcal{H}}\} \\ &= \{(s,t) : s \in W \text{ implies } t \in P_V(W) \text{ for each } W \in L_{\mathcal{F}_\mathcal{H}}\} \qquad \text{(see [34])} \\ &= \{(s,t) : P_V(s) = t\}, \end{aligned}$$

where $P_V : \mathcal{H} \to \mathcal{H}$ denotes the self-adjoint projection onto V. Thus, for the self-adjointness of $R_{V?}$, it suffices to show that $P_V(s)\not\perp u$ implies $s\not\perp P_V(u)$. Recall that P_V is said to be self-adjoint (as an operator on $\mathcal{H}$) if

$$\langle P_V(s), t | P_V(s), t\rangle = \langle s, P_V(t) | s, P_V(t)\rangle\,,$$

where $\langle \cdot, \cdot | \cdot, \cdot \rangle$ stands for the inner product on $\mathcal{H}$. Because $s\not\perp t$ if and only if $\langle s, t | s, t\rangle \neq 0$, the self-adjointness of P_V implies that of $R_{V?}$.

5.3 Complex Algebra of Star-free QDF

There is a remarkable relation between star-free QDAs and star-free QDFs: a star-free QDA is constructed from a star-free QDF, and vice versa. The star-free QDA constructed from a star-free QDF is called the complex algebra (Definition 5.3.1), and the star-free QDF constructed from a star-free QDA is called the canonical frame (Definition 5.4.1). We show that every complex algebra of a star-free QDF is a star-free QDA in Section 5.3 (Theorem 5.3.4), and also every canonical frame of a star-free QDA is a star-free QDF in Section 5.4 (Theorem 5.4.4).

Definition 5.3.1. The **complex algebra** of a star-free QDF $\mathcal{F}^-_{\mathrm{QD}} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$ is a tuple

$$\mathcal{C}(\mathcal{F}^-_{\mathrm{QD}}) = (L_\mathcal{F}, \subseteq, \neg_R, \Box_\mathcal{R}, \blacksquare_\mathcal{U}),$$

where $\neg_R : L_\mathcal{F} \to L_\mathcal{F}$, $\Box_\mathcal{R} : \mathsf{Prog}^-[\Pi, L_\mathcal{F}] \times L_\mathcal{F} \to L_\mathcal{F}$, and $\blacksquare_\mathcal{U} : \Pi_0 \times L_\mathcal{F} \to L_\mathcal{F}$ are functions such that

(1) $\neg_R P = \{s \in S : sRt \text{ for any } t \in P\}$ (recall Definition 3.4.3),

(2) $\Box_{\mathcal{R}}(a, P) = \{s \in S : t \in P \text{ for any } t \in S \text{ satisfying } sR_a t\}$,

(3) $\blacksquare_{\mathcal{U}}(\pi, P) = \{\mathfrak{u}_\pi(s) : s \in P\}$ (that is, $\blacksquare_{\mathcal{U}}(\pi, P)$ is the image of P under $\mathfrak{u}_\pi$).

Remark 5.3.2. $\mathcal{C}(\mathcal{F}^-_{\mathrm{QD}})$ is well-defined in the sense that $\neg_R P \in L_{\mathcal{F}}$, $\Box_{\mathcal{R}}(a, P) \in L_{\mathcal{F}}$, and $\blacksquare_{\mathcal{U}}(\pi, P) \in L_{\mathcal{F}}$ for each $P \in L_{\mathcal{F}}$. For the proof of $\neg_R P \in L_{\mathcal{F}}$, see Remark 3.4.6. Before embarking on the proof of $\Box_{\mathcal{R}}(a, P) \in L_{\mathcal{F}}$ and $\blacksquare_{\mathcal{U}}(\pi, P) \in L_{\mathcal{F}}$, we prepare the next lemma.

Lemma 5.3.3.

(1) $\neg_R \Box_{\mathcal{R}}(\pi, P) = \Box_{\mathcal{R}}(\pi, \neg_R P)$.

(2) $\blacksquare_{\mathcal{U}}(\pi, \Box_{\mathcal{R}}(\pi, P)) = \Box_{\mathcal{R}}(\pi, \blacksquare_{\mathcal{U}}(\pi, P)) = P$.

(3) $\blacksquare_{\mathcal{U}}(\pi, S) = S$.

(4) $\blacksquare_{\mathcal{U}}(\pi, P \cap Q) = \blacksquare_{\mathcal{U}}(\pi, P) \cap \blacksquare_{\mathcal{U}}(\pi, Q)$.

(5) $\Box_{\mathcal{R}}(\mathbf{skip}, P) = P$.

(6) $\Box_{\mathcal{R}}(\mathbf{abort}, P) = S$.

(7) $\Box_{\mathcal{R}}(a, S) = S$.

(8) $\Box_{\mathcal{R}}(a, P \cap Q) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(a, Q)$.

(9) $\Box_{\mathcal{R}}(a \,;\, b, P) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P))$.

(10) $\Box_{\mathcal{R}}(a \cup b, P) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P)$.

(11) $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q)$.

Proof.

(1) Proof of $\Box_{\mathcal{R}}(\pi, \neg_R P) = \neg_R \Box_{\mathcal{R}}(\pi, P)$. See Lemma 4.4.3 (1).

(2) Proof of $\blacksquare_{\mathcal{U}}(\pi, \Box_{\mathcal{R}}(\pi, P)) = \Box_{\mathcal{R}}(\pi, \blacksquare_{\mathcal{U}}(\pi, P)) = P$. It follows from the fact that the image of the inverse image of a function f and the inverse image of the image of f are identical if f is a bijection (in this case, $f = \mathfrak{u}_\pi$).

(3) Proof of $\blacksquare_{\mathcal{U}}(\pi, S) = S$. Immediate.

(4) Proof of $\blacksquare_{\mathcal{U}}(\pi, P \cap Q) = \blacksquare_{\mathcal{U}}(\pi, P) \cap \blacksquare_{\mathcal{U}}(\pi, Q)$. The proof follows from the fact that every bijection preserves intersection.

(5) Proof of $\Box_{\mathcal{R}}(\mathbf{skip}, P) = P$. See Lemma 4.4.3 (2)

(6) Proof of $\Box_{\mathcal{R}}(\mathbf{abort}, P) = S$. See Lemma 4.4.3 (3).

(7) Proof of $\Box_{\mathcal{R}}(a, S) = S$. See Lemma 4.4.3 (4).

(8) Proof of $\Box_{\mathcal{R}}(a, P \cap Q) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(a, Q)$. See Lemma 4.4.3 (5).

(9) Proof of $\Box_{\mathcal{R}}(a \,;\, b, P) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, P))$. See Lemma 4.4.3 (6).

(10) Proof of $\Box_{\mathcal{R}}(a \cup b, P) = \Box_{\mathcal{R}}(a, P) \cap \Box_{\mathcal{R}}(b, P)$. See Lemma 4.4.3 (7).

(11) Proof of $\Box_{\mathcal{R}}(P?, Q) = \neg_R P \uplus (P \cap Q)$. See Lemma 4.4.3 (9).

□

Theorem 5.3.4. Every complex algebra $\mathcal{C}(\mathcal{F}^-_{\mathrm{QD}})$ of star-free QDFs $\mathcal{F}^-_{\mathrm{QD}} = (\mathcal{F}, \mathcal{U}, \mathcal{R})$ is a star-free QDA.

Proof. Similar to the proof of Theorem 4.4.5 (but use Lemma 5.3.3 instead of Lemma 4.4.3). □

5.4 Canonical Frame of Star-free QDA

The canonical frame of star-free QDAs is constructed by extending that of ortholattices (Definition 3.4.12).

Definition 5.4.1. The **canonical frame** of a star-free QDA $\mathcal{L}^-_{\mathrm{QD}}$ is a tuple

$$\mathcal{C}(\mathcal{L}^-_{\mathrm{QD}}) = (S^{\mathcal{L}^-_{\mathrm{QD}}}, R^{\mathcal{L}^-_{\mathrm{QD}}}, \mathcal{U}^{\mathcal{L}^-_{\mathrm{QD}}}, \mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}})$$

that consists of

- the set $S^{\mathcal{L}^-_{\mathrm{QD}}}$ of all proper filters of $(L, \leq)$,
- a relation $R^{\mathcal{L}^-_{\mathrm{QD}}}$ on $S^{\mathcal{L}^-_{\mathrm{QD}}}$,
- family $\mathcal{U}^{\mathcal{L}^-_{\mathrm{QD}}} = \{\hat{\mathfrak{u}}_\pi : \pi \in \Pi_0\}$ of functions on $S^{\mathcal{L}^-_{\mathrm{QD}}}$, and
- family $\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}} = \{R_a^{\mathcal{L}^-_{\mathrm{QD}}} : a \in \mathsf{Prog}^-[\Pi, L]\}$ of relations on $S^{\mathcal{L}^-_{\mathrm{QD}}}$

satisfying the following conditions: for any $\pi \in \Pi_0$, $a, b \in \mathsf{Prog}^-[\Pi, L]$, and $p \in L$,

(1) $R^{\mathcal{L}^-_{\mathrm{QD}}} = \{(F, G) : p \in F \text{ and } \neg p \in G \text{ for some } p \in L\}$;

(2) $\hat{\mathfrak{u}}_\pi(F) = \{p : \Box(\pi, p) \in F\}$ for each $F \in S^{\mathcal{L}^-_{\mathrm{QD}}}$;

(3) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{\mathbf{skip}} = \{(F, F) : F \in S^{\mathcal{L}^-_{\mathrm{QD}}}\}$;

(4) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{\mathbf{abort}} = \emptyset$;

(5) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{\pi} = \{(F, G) : \hat{\mathfrak{u}}_\pi(F) = G\}$;

(6) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{a;b} = \{(F, G) : FR^{\mathcal{L}^-_{\mathrm{QD}}}_a H \text{ and } HR^{\mathcal{L}^-_{\mathrm{QD}}}_b G \text{ for some } H \in S^{\mathcal{L}^-_{\mathrm{QD}}}\}$;

(7) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{a\cup b} = R^{\mathcal{L}^-_{\mathrm{QD}}}_a \cup R^{\mathcal{L}^-_{\mathrm{QD}}}_b$;

(8) $R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?} = \{(F, G) : p \Cap q \in G \text{ for any } q \in L \text{ satisfying } q \in F\}$.

Remark 5.4.2. Note that $\hat{\mathfrak{u}}_\pi$ is well-defined in the sense that $\hat{\mathfrak{u}}_\pi(F) \in S^{\mathcal{L}^-_{\mathrm{QD}}}$ for each $F \in S^{\mathcal{L}^-_{\mathrm{QD}}}$. For, we confirm that $\hat{\mathfrak{u}}_\pi(F)$ satisfies all the conditions of proper filters.

- $\hat{\mathfrak{u}}_\pi(F) \neq \emptyset$: $\Upsilon \in \hat{\mathfrak{u}}_\pi(F)$ because $\Box(\pi, \Upsilon) = \Upsilon \in F$.
- To show that $\hat{\mathfrak{u}}_\pi(F)$ is upward closed, assume that $p \in \hat{\mathfrak{u}}_\pi(F)$ and $p \leq q$. Because $p = p \wedge q$ by the assumption $p \leq q$,

  $$p \in \hat{\mathfrak{u}}_\pi(F) \Leftrightarrow \Box(\pi, p) \in F \Leftrightarrow \Box(\pi, p \wedge q) \in F \Leftrightarrow \Box(\pi, p) \wedge \Box(\pi, q) \in F.$$

  Recall that $F \in S^{\mathcal{L}^-_{\mathrm{QD}}}$ and is upward closed. Thus, $\Box(\pi, q) \in F$ by

  $$\Box(\pi, p) \wedge \Box(\pi, q) \leq \Box(\pi, q).$$

- $\hat{\mathfrak{u}}_\pi(F)$ is closed under $\wedge$:

  $$\begin{aligned} p, q \in \hat{\mathfrak{u}}_\pi(F) &\Leftrightarrow \Box(\pi, p), \Box(\pi, q) \in F \Rightarrow \Box(\pi, p) \wedge \Box(\pi, q) \in F \\ &\Leftrightarrow \Box(\pi, p \wedge q) \in F \Leftrightarrow p \wedge q \in \hat{\mathfrak{u}}_\pi(F) \end{aligned}$$

- Finally, we show that $\hat{\mathfrak{u}}_\pi(F)$ is proper: $\hat{\mathfrak{u}}_\pi(F) \neq L$. Because F is proper, there exists $p \in L$ such that $p \notin F$. Therefore, $\Box(\pi, \blacksquare(\pi, p)) \notin F$ by Definition 5.1.2 (2). Hence, $\blacksquare(\pi, p) \notin \hat{\mathfrak{u}}_\pi(F)$, which means that $\hat{\mathfrak{u}}_\pi(F)$ is proper.

In Remark 4.3.4, we proved that the adequacy and repeatability of $R_{P?}$ are satisfied. The dual versions of them are also satisfied.

Theorem 5.4.3. $R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}$ satisfies dual adequacy and dual repeatability.

(1) The **dual adequacy** of $R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}$: $p \in F$ implies $FR_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}F$.

(2) The **dual repeatability** of $R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}$: $FR_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}G$ implies $p \in G$.

Proof.

(1) Assume that $p \in F$ and $q \in F$. Then $\neg p \vee q \in F$ because F is upward closed. Thus, $p \wedge (\neg p \vee q) \in F$ because F is closed under $\wedge$.

(2) Assume $FR_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}G$. Then $p \wedge (\neg p \vee q) \in G$ for any $q \in F$. Because F is a filter, $\Upsilon \in F$. Thus,
$$p = p \wedge (\neg p \vee \Upsilon) \in G.$$

□

In the next theorem, we prove that every canonical frame of star-free QDAs is a star-free QDF. ■ plays a role in this theorem. That is, the conditions with respect to ■ imposed on star-free QDAs are required to show that some conditions imposed on star-free QDFs: $\hat{\mathfrak{u}}_\pi$ is bijective, $\hat{\mathfrak{u}}_\pi$ preserves $R^{\mathcal{L}_{\mathrm{QD}}^-}$, and $R_{\theta(p)?}^{\mathcal{L}_{\mathrm{QD}}^-}$ is self-adjoint.

Theorem 5.4.4. Every canonical frame $\mathcal{C}(\mathcal{L}_{\mathrm{QD}}^-)$ of star-free QDAs $\mathcal{L}_{\mathrm{QD}}^- = (L, \leq, \neg, \Box, \blacksquare)$ is a star-free QDF.

Proof. It follows from Theorem 3.4.13 that $(S^{\mathcal{L}_{\mathrm{QD}}^-}, R^{\mathcal{L}_{\mathrm{QD}}^-})$ is an orthoframe. The conditions from (1) to (6) in Definition 4.3.1 are shown immediately. Thus, it remains to show the conditions (7), (8), and (9) in Definition 4.3.1.

(7): $\hat{\mathfrak{u}}_\pi$ is bijective. Suppose $\hat{\mathfrak{u}}_\pi(F) = \hat{\mathfrak{u}}_\pi(G)$ to show that $\hat{\mathfrak{u}}_\pi$ is injective. Then $\Box(\pi, p) \in F$ if and only if $\Box(\pi, p) \in G$ for each $p \in L$. Take an arbitrary $q \in L$. Then by substituting $\blacksquare(\pi, q)$ for p and by Definition 5.1.2 (2), $q = \Box(\pi, \blacksquare(\pi, q)) \in F$ if and only if $q = \Box(\pi, \blacksquare(\pi, q)) \in G$. Equivalently, $F = G$. For the surjectivity of $\hat{\mathfrak{u}}_\pi$, it suffices to show that for any $F \in S^{\mathcal{L}_{\mathrm{QD}}^-}$, there exists $G \in S^{\mathcal{L}_{\mathrm{QD}}^-}$ such that $F = \hat{\mathfrak{u}}_\pi(G)$. If we choose $\{p : \blacksquare(\pi, p) \in F\}$ as G, then $F = \hat{\mathfrak{u}}_\pi(G)$. This is because

$$\begin{aligned}\hat{\mathfrak{u}}_\pi(G) &= \{p : \Box(\pi, p) \in \{q : \blacksquare(\pi, q) \in F\}\} = \{p : \blacksquare(\pi, \Box(\pi, p)) \in F\} \\ &= \{p : p \in F\} = F\end{aligned}$$

by Definition 5.1.2 (2). It remains to show $G = \{p : \blacksquare(\pi, p) \in F\} \in S^{\mathcal{L}_{\mathrm{QD}}^-}$. It is shown in the same way as the proof of $\mathfrak{u}_\pi(F) \in S^{\mathcal{L}_{\mathrm{QD}}^-}$ explained in Remark 5.4.2.

(8): $\hat{\mathfrak{u}}_\pi$ preserves $R^{\mathcal{L}_{\mathrm{QD}}^-}$. Suppose $FR^{\mathcal{L}_{\mathrm{QD}}^-}G$ (equivalently, there exists $p \in L$ satisfying $p \in F$ and $\neg p \in G$). Then by Definition 5.1.2 (1) and (2),

$$\Box(\pi, \blacksquare(\pi, p)) = p \in F,$$

$$\Box(\pi, \neg\blacksquare(\pi, p)) = \neg\Box(\pi, \blacksquare(\pi, p)) = \neg p \in G.$$

Thus, $q = \blacksquare(\pi, p)$ satisfies $q \in \hat{\mathfrak{u}}_\pi(F)$ and $\neg q \in \hat{\mathfrak{u}}_\pi(G)$, which means that $(\hat{\mathfrak{u}}_\pi(F))R^{\mathcal{L}^-_{\mathrm{QD}}}(\hat{\mathfrak{u}}_\pi(G))$. Conversely, if $(\hat{\mathfrak{u}}_\pi(F))R^{\mathcal{L}^-_{\mathrm{QD}}}(\hat{\mathfrak{u}}_\pi(G))$, then there exists $p \in L$ satisfying $p \in \hat{\mathfrak{u}}_\pi(F)$ and $\neg p \in \hat{\mathfrak{u}}_\pi(G)$. Therefore, for some $p \in L$, $\Box(\pi, p) \in F$, and also $\neg\Box(\pi, p) = \Box(\pi, \neg p) \in G$ by Definition 5.1.2 (1). Thus, $q = \Box(\pi, p)$ satisfies $q \in F$ and $\neg q \in G$, which means that $FR^{\mathcal{L}^-_{\mathrm{QD}}}G$.

(9): $R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}$ is self-adjoint. Suppose that $FR^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}G$ and $G\not{R}^{\mathcal{L}^-_{\mathrm{QD}}}H$. It suffices to show that $HR^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}I$ and $F\not{R}^{\mathcal{L}^-_{\mathrm{QD}}}I$ for some $I \in S^{\mathcal{L}^-_{\mathrm{QD}}}$.

$$\begin{array}{ccc} F & \xrightarrow{R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}} & G \\ {\scriptstyle \not{R}^{\mathcal{L}^-_{\mathrm{QD}}}}\downarrow & & \downarrow{\scriptstyle \not{R}^{\mathcal{L}^-_{\mathrm{QD}}}} \\ \exists I & \xleftarrow{R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}} & H \end{array}$$

It follows from the assumption $FR^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}G$ that $p \in G$ by the dual repeatability of $R^{\mathcal{L}^-_{\mathrm{QD}}}_{p?}$ (Lemma 5.4.3 (2)). By the assumption $G\not{R}^{\mathcal{L}^-_{\mathrm{QD}}}H$, we obtain

(I) $\neg p \notin H$.

We can assume $p \neq \curlywedge$; otherwise, (I) implies that $\curlyvee = \neg p \notin H$, which contradicts the condition that H is a filter. Now we show that

$$\Delta = \{p \wedge (\neg p \vee q) : q \in H\}$$

has the finite meet property. Suppose for the sake of contradiction that there exists a finite subset Δ^{fin} of H such that

(II) $\bigwedge\{p \wedge (\neg p \vee q) : q \in \Delta^{\mathrm{fin}}\} = \curlywedge$.

Observe that

$$p \wedge (\neg p \vee (p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\})) \leq \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\}$$

by the orthomodular law. Equivalently,

(III) $\neg\bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\} \leq \neg(p \wedge (\neg p \vee (p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\})))$

by the definition of ortholattices. Furthermore,

$$\bigvee\{p \wedge \neg q : q \in \Delta^{\mathrm{fin}}\} \leq p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\}$$

by the part of the distributive law (Remark 2.5.5). Equivalently,

(IV) $\neg(p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\}) \leq \neg \bigvee\{p \wedge \neg q : q \in \Delta^{\mathrm{fin}}\}$

by the definition of ortholattices. Thus,

$$\begin{aligned}
\bigwedge \Delta^{\mathrm{fin}} &= \neg \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\} \\
&\leq \neg(p \wedge (\neg p \vee (p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\}))) && \text{(By (III))} \\
&= \neg p \vee (p \wedge \neg(p \wedge \bigvee\{\neg q : q \in \Delta^{\mathrm{fin}}\})) \\
&\leq \neg p \vee (p \wedge \neg(\bigvee\{p \wedge \neg q : q \in \Delta^{\mathrm{fin}}\})) && \text{(By (IV))} \\
&= \neg p \vee \bigwedge\{p \wedge (\neg p \vee q) : q \in \Delta^{\mathrm{fin}}\} \\
&= \neg p && \text{(By (II))}
\end{aligned}$$

Therefore, $\bigwedge \Delta^{\mathrm{fin}} \leq \neg p$. Recall that H is a filter. By the definition of filters, $\bigwedge \Delta^{\mathrm{fin}} \in H$, and it implies $\neg p \in H$. This leads to a contradiction to (I). Consequently, Δ has the finite meet property. It follows from Lemma 3.2.7 that $\langle \Delta \rangle$ is a proper filter. In fact, $\langle \Delta \rangle$ is a witness of the self-adjointness of $R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-}$, which is shown below. That is, it suffices to show that $F R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-} G$ and $G \not R^{\mathcal{L}_{\mathrm{QD}}^-} H$ jointly imply that $H R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-} \langle \Delta \rangle$ and $F \not R^{\mathcal{L}_{\mathrm{QD}}^-} \langle \Delta \rangle$. It follows the definition of Δ that $H R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-} \langle \Delta \rangle$. Hence, it remains to show $F \not R^{\mathcal{L}_{\mathrm{QD}}^-} \langle \Delta \rangle$. Suppose for the sake of contradiction that $F R^{\mathcal{L}_{\mathrm{QD}}^-} \langle \Delta \rangle$. Because $R^{\mathcal{L}_{\mathrm{QD}}^-}$ is symmetric, $r \in \langle \Delta \rangle$ and $\neg r \in F$ for some $r \in L$. Because $r \in \langle \Delta \rangle$, there exist $q_1, \ldots, q_n \in H$ such that

$$\bigwedge\{p \wedge (\neg p \vee q_i) : 1 \leq i \leq n\} \leq r.$$

Put

$$r' = \bigwedge\{\neg p \vee q_i : 1 \leq i \leq n\}.$$

Then $p \wedge r' \leq r$, which implies

$$\neg r \leq \neg(p \wedge r') = \neg p \vee \neg r'.$$

Because $\neg r \in F$ and F is a filter, $\neg p \vee \neg r' \in F$. Recall the assumption that $F R_{p?}^{\mathcal{L}_{\mathrm{QD}}^-} G$. Hence,

$$p \wedge (\neg p \vee (\neg p \vee \neg r')) \in G.$$

Therefore, we obtain

(V) $p \wedge (\neg p \vee \neg r') \in G$.

Observe that

$$\begin{aligned} p \wedge (\neg p \vee \neg r') &= p \wedge (\neg p \vee \neg \bigwedge \{\neg p \vee q_i : 1 \leq i \leq n\}) \\ &= p \wedge (\neg p \vee (\bigvee \{p \wedge \neg q_i : 1 \leq i \leq n\})) \\ &\leq p \wedge (\neg p \vee (p \wedge \bigvee \{\neg q_i : 1 \leq i \leq n\})) \\ &\qquad \text{(By the part of the distributive law (Remark 2.5.5))} \\ &\leq \bigvee \{\neg q_i : 1 \leq i \leq n\} \qquad \text{(By the orthomodular law)} \\ &= \neg \bigwedge \{q_i : 1 \leq i \leq n\}. \end{aligned}$$

Therefore,

$$p \wedge (\neg p \vee \neg r') \leq \neg \bigwedge \{q_i : 1 \leq i \leq n\}.$$

Because G is a filter, $\neg \bigwedge \{q_i : 1 \leq i \leq n\} \in G$ by (V). On the ther hand, because $q_1, \ldots, q_n \in H$ and H is a filter, $\bigwedge \{q_i : 1 \leq i \leq n\} \in H$. This leads a contradiction with the assumption $G \not\mathbb{R}^{\mathcal{L}^{-}_{\mathrm{QD}}} H$. Consequently, $F \not\mathbb{R}^{\mathcal{L}^{-}_{\mathrm{QD}}} \langle \Delta \rangle$ by proof by contradiction. □

5.5 Representation Theorem

Eventually, we prove our main theorem, the Stone-type representation theorem for star-free QDAs.

Definition 5.5.1. Let

$$(L_1, \leq_1, \neg_1, \Box_1, \blacksquare_1) \text{ and } (L_2, \leq_2, \neg_2, \Box_2, \blacksquare_2)$$

be star-free QDAs. A function $f : L_1 \to L_2$ is called

- a **homomorphism** between star-free QDAs if the following conditions are satisfied:
  - (1) f is a homomorphism between ortholattices $(L_1, \leq_1, \neg_1)$ and $(L_2, \leq_2, \neg_2)$ (see Definition 3.3.1),
  - (2) $f(\Box_1(a, p)) = \begin{cases} \Box_2(a, \theta(p)) & (a \neq q?), \\ \Box_2(\theta(q)?, \theta(p)) & (a = q?) \end{cases}$,
  - (3) $f(\blacksquare_1(\pi, p)) = \blacksquare_2(\pi, f(p))$.
- an **embedding** between star-free QDAs if f is an injective homomorphism between star-free QDAs.

- an **isomorphism** between star-free QDAs if f is a bijective homomorphism between star-free QDAs.

A star-free QDA $(L_1, \leq_1, \neg_1, \Box_1, \blacksquare_1)$ is said to be **isomorphic** to a star-free QDA $(L_2, \leq_2, \neg_2, \Box_2, \blacksquare_2)$ if there exists an isomorphism from L_1 to L_2.

Definition 5.5.2. The **Stone embedding** for star-free QDAs $\mathcal{L}^-_{\mathrm{QD}}$ is the function $\theta : L \to L_{\mathcal{C}(\mathcal{L}^-_{\mathrm{QD}})}$ defined by

$$\theta(p) = \{F \in S^{\mathcal{L}^-_{\mathrm{QD}}} : p \in F\}.$$

The **canonical extension** of a star-free QDA $\mathcal{L}^-_{\mathrm{QD}}$ is the complex algebra $\mathcal{C}(\mathcal{C}(\mathcal{L}^-_{\mathrm{DQ}}))$ of the canonical frame $\mathcal{C}(\mathcal{L}^-_{\mathrm{DQ}})$ of $\mathcal{L}^-_{\mathrm{QD}}$.

Now we prove the Stone-type representation theorem for star-free QDAs. This theorem is proved using Theorem 5.3.4 and Theorem 5.4.4.

Theorem 5.5.3 (Stone-type Representation Theorem for Star-free QDAs)**.** Every star-free QDA is embeddable into its canonical extension.

Proof. We show that the Stone embedding $\theta : L \to L_{\mathcal{C}(\mathcal{L}^-_{\mathrm{QD}})}$ for star-free QDAs is an embedding of a star-free QDA $\mathcal{L}^-_{\mathrm{QD}}$ into $\mathcal{C}(\mathcal{C}(\mathcal{L}^-_{\mathrm{DQ}}))$.

To show that θ is injective, suppose $p \neq q$. Then either $p \not\leq q$ or $q \not\leq p$ by the contraposition of the anti-symmetry of $\leq$. Assume that $p \not\leq q$ without loss of generality. Then $p \neq \curlywedge$; otherwise, $p \leq q$ for any $q \in L$. Because $p{\uparrow} = \{r : p \leq r\}$ is a proper principal filter if $p \neq \curlywedge$, we obtain ${\uparrow} p \in \theta(p)$. However, it follows from $p \not\leq q$ that $q \notin p{\uparrow}$ (that is, $p{\uparrow} \notin \theta(q)$). Consequently, $\theta(p) \neq \theta(q)$.

The only remaining thing to show is that θ is a homomorphism.

(1) Proof of $\theta(p \wedge q) = \theta(p) \cap \theta(q)$.

$$\begin{aligned} F \in \theta(p \wedge q) &\Leftrightarrow p \wedge q \in F \Leftrightarrow p \in F \text{ and } q \in F \\ &\Leftrightarrow F \in \theta(p) \text{ and } F \in \theta(q) \Leftrightarrow F \in \theta(p) \cap \theta(q). \end{aligned}$$

(2) Proof of $\theta(p \vee q) = \theta(p) \uplus \theta(q)$. Because $\theta(p \wedge q) = \theta(p) \cap \theta(q)$ and $\theta(\neg p) = \neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}} \theta(p)$ (for the proof, see below),

$$\theta(p \vee q) = \theta(\neg(\neg p \wedge \neg q)) = \neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}}(\neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}} \theta(p) \cap \neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}} \theta(q)) = \theta(p) \uplus \theta(q).$$

(3) Proof of $\theta(\neg p) = \neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}} \theta(p)$.

For the $\subseteq$-part, suppose $F \in \theta(\neg p)$ (equivalently, $\neg p \in F$). It suffices to show that $G \in \theta(p)$ (equivalently, $p \in G$) implies $F R^{\mathcal{L}^-_{\mathrm{QD}}} G$ for any $G \in L_{\mathcal{C}(\mathcal{L}^-_{\mathrm{QD}})}$.

It follows from $\neg p \in F$ and $p \in G$ that $GR^{\mathcal{L}^-_{\mathrm{QD}}}F$, and thus $FR^{\mathcal{L}^-_{\mathrm{QD}}}G$, as desired.

For the $\supseteq$-part, suppose $F \in \neg_{R^{\mathcal{L}^-_{\mathrm{QD}}}}\theta(p)$. Then $FR^{\mathcal{L}^-_{\mathrm{QD}}}G$ for $G = \{q : p \leq q\}$ satisfying $p \neq \curlywedge$ because $G \in \theta(p)$. Thus, there exists $r \in L$ such that $r \in F$ and $\neg r \in G$. Hence, $p \leq \neg r$ by $\neg r \in G$. It implies that $r \leq \neg p$. Recall $r \in F$. By the definition of filters, $\neg p \in F$. Consequently, $F \in \theta(\neg p)$.

(4) We prove that

$$\theta(\Box(a,p)) = \begin{cases} \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(a, \theta(p)) & (a \neq q?), \\ \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(\theta(q), \theta(p)) & (a = q?) \end{cases}$$

by structural induction on $a \in \mathsf{Prog}^-[\Pi, L]$.

(a) For the case $a = \mathbf{skip}$, by Definition 5.1.2 (5) and Lemma 5.3.3 (5),

$$\theta(\Box(\mathbf{skip}, p)) = \theta(p) = \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(\mathbf{skip}, \theta(p)).$$

(b) For the case $a = \mathbf{abort}$, by Definition 5.1.2 (6) and Lemma 5.3.3 (6),

$$\theta(\Box(\mathbf{abort}, p)) = \theta(\curlyvee) = S^{\mathcal{L}^-_{\mathrm{QD}}} = \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(\mathbf{abort}, \theta(p)).$$

(c) For the case $a = \pi \in \Pi_0$, observe that

$$\begin{aligned} FR_\pi^{\mathcal{L}^-_{\mathrm{QD}}}G &\Leftrightarrow \hat{\mathfrak{u}}_\pi(F) = G \Leftrightarrow \{p : \Box(\pi, p) \in F\} = G \\ &\Leftrightarrow (\Box(\pi, p) \in F \Leftrightarrow p \in G). \end{aligned}$$

For the $\subseteq$-part, suppose $F \in \theta(\Box(\pi, p))$ (equivalently, $\Box(\pi, p) \in F$). If $FR_\pi^{\mathcal{L}^-_{\mathrm{QD}}}G$, then $p \in G$ (that is, $G \in \theta(p)$) by the above equivalence. Hence, $F \in \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(\pi, \theta(p))$.

For the $\supseteq$-part, suppose $F \in \Box_{\mathcal{R}^{\mathcal{L}^-_{\mathrm{QD}}}}(\pi, \theta(p))$. Let X be the set $\{q \in L : \Box(\pi, q) \in F\}$, which is non-empty because $\curlyvee \in X$ by $\Box(\pi, \curlyvee) = \curlyvee \in F$. Thus, there exists the smallest filter G containing X, which in fact is

$$\{q \in L : \bigwedge\{p_1, \ldots, p_n\} \leq q \text{ for some } p_1, \ldots, p_n \in X\}.$$

by Theorem 3.2.3. Now we show $FR_\pi^{\mathcal{L}^-_{\mathrm{QD}}}G$, that is, $\Box(\pi, q) \in F$ if and only if $q \in G$. If $\Box(\pi, q) \in F$, then $q \in X$, which implies $q \in G$. Conversely, suppose $q \in G$. Then $\bigwedge\{p_1, \ldots, p_n\} \leq q$ for some

$p_1, \ldots, p_n \in X$. It follows from the monotonicity of $\Box(\pi, -)$ (the proof is similar to that of Lemma 4.2.2) that

$$\Box(\pi, \bigwedge\{p_1, \ldots, p_n\}) \leq \Box(\pi, q).$$

Because $\Box(\pi, p_i) \in F$ by $p_1, \ldots, p_n \in X$,

$$\Box(\pi, \bigwedge\{p_1, \ldots, p_n\}) = \bigwedge\{\Box(\pi, p_1), \ldots, \Box(\pi, p_n)\} \in F,$$

and thus $\Box(\pi, q) \in F$ by the definition of filters. Consequently, $F R_\pi^{\mathcal{L}_{\mathrm{QD}}^-} G$. Hence, $G \in \theta(p)$ by the assumption $F \in \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(\pi, \theta(p))$, and is equivalent to $p \in G$. It implies that there exist $p_1, \ldots, p_n \in X$ such that $\bigwedge\{p_1, \ldots, p_n\} \leq p$. Thus, by the monotonicity of $\Box(\pi, -)$,

$$\bigwedge\{\Box(\pi, p_1), \ldots, \Box(\pi, p_n)\} \leq \Box(\pi, p).$$

Because $\Box(\pi, p_i) \in F$ by $p_1, \ldots, p_n \in X$, we have $\Box(\pi, p) \in F$. Therefore, $F \in \theta(\Box(\pi, p))$, as desired.

(d) For the case $a = b \,;\, c$,

$$\begin{aligned}
\theta(\Box(b \,;\, c, p)) &= \theta(\Box(b, \Box(c, p))) && \text{(By Definition 5.1.2 (9))} \\
&= \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(b, \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(c, \theta(p))) \\
& && \text{(By the induction hypothesis)} \\
&= \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(b \,;\, c, \theta(p)). && \text{(By Lemma 5.3.3 (9))}
\end{aligned}$$

(e) For the case $a = b \cup c$,

$$\begin{aligned}
\theta(\Box(b \cup c, p)) &= \theta(\Box(b, p) \wedge \Box(c, p))) && \text{(By Definition 5.1.2 (10))} \\
&= \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(b, \theta(p)) \cap \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(c, \theta(p)) \\
& && \text{(By (1) in this proof (see above))} \\
&= \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(b \cup c, \theta(p)). && \text{(By Lemma 5.3.3 (10))}
\end{aligned}$$

(f) For the case $a = q?$,

$$\begin{aligned}
\theta(\Box(q?, p)) &= \theta(\neg q \vee (q \wedge p)) && \text{(By Definition 5.1.2 (11))} \\
&= \neg_{R^{\mathcal{L}_{\mathrm{QD}}^-}} \theta(q) \uplus (\theta(q) \cap \theta(p)) \\
& && \text{(By (1), (2), and (3) in this proof (see above))} \\
&= \Box_{\mathcal{R}^{\mathcal{L}_{\mathrm{QD}}^-}}(\theta(q)?, \theta(p)). && \text{(By Lemma 5.3.3 (11))}
\end{aligned}$$

(5) Finally, we prove that

$$\theta(\blacksquare(\pi, p)) = \blacksquare_{\mathcal{U}^{\mathcal{L}_{\mathrm{QD}}^-}}(\pi, \theta(p)).$$

Take an arbitrary $F \in \theta(\blacksquare(\pi, \theta))$. Then $\blacksquare(\pi, p) \in F$. Because $\hat{\mathfrak{u}}_\pi$ is bijective, there uniquely exists $G \in S^{\mathcal{L}_{\mathrm{QD}}^-}$ such that $\hat{\mathfrak{u}}_\pi(G) = F$. Thus, $\blacksquare(\pi, p) \in \hat{\mathfrak{u}}_\pi(G)$. It follows from Definition 5.4.1 (2) that $\square(\pi, \blacksquare(\pi, p)) \in G$. Hence, it follows from Definition 5.1.2 (2) that $p \in G$. Equivalently, $G \in \theta(p)$. Therefore,

$$F = \hat{\mathfrak{u}}_\pi(G) \in \{\hat{\mathfrak{u}}_\pi(G) : G \in \theta(p)\} = \blacksquare_{\mathcal{U}^{\mathcal{L}_{\mathrm{QD}}^-}}(\pi, \theta(p)).$$

Conversely, take an arbitrary $F \in \blacksquare_{\mathcal{U}^{\mathcal{L}_{\mathrm{QD}}^-}}(\pi, \theta(p))$. Then $F = \hat{\mathfrak{u}}_\pi(G)$ for some $G \in S_{\mathrm{QD}}^-$ satisfying $G \in \theta(p)$ (that is, $p \in G$). It follows from 5.1.2 (2) that $\square(\pi, \blacksquare(\pi, p)) = p \in G$. Thus, it follows from Definition 5.4.1 (2) that $\blacksquare(\pi, p) \in \hat{\mathfrak{u}}_\pi(G) = F$.

□

5.6 Examples from Quantum Computation

Although star-free QDA lacks the iteration operator, it is expressive enough to describe various quantum protocols in quantum computation. In this section, we describe some of them by star-free QDA. Based on the expressions in this section, we have developed a tool for assisting quantum program verification.

To describe the examples in this section, we fix

$$\Pi_0 = \{\mathtt{H}(i), \mathtt{X}(i), \mathtt{Y}(i), \mathtt{Z}(i), \mathtt{CX}(i,j) : i, j \in \mathbb{N}, i \neq j\},$$

where $\mathbb{N}$ stands for the set of all natural numbers (including 0).

Let I be the identity matrix of size 2×2. The family $\mathcal{U} = \{\mathfrak{u}_\pi : \pi \in \Pi_0\}$ of functions on $\mathbb{C}^{2^n}$ is defined as follows:

$$\mathfrak{u}_{\mathtt{H}(i)} = I^{\otimes i} \otimes H \otimes I^{\otimes n-i-1}, \quad \mathfrak{u}_{\mathtt{X}(i)} = I^{\otimes i} \otimes X \otimes I^{\otimes n-i-1},$$
$$\mathfrak{u}_{\mathtt{Y}(i)} = I^{\otimes i} \otimes Y \otimes I^{\otimes n-i-1}, \quad \mathfrak{u}_{\mathtt{Z}(i)} = I^{\otimes i} \otimes Z \otimes I^{\otimes n-i-1},$$

$$\mathfrak{u}_{\mathtt{CX}(i,j)} = I^{\otimes i} \otimes |0\rangle\langle 0| \otimes I^{\otimes n-i-1} + (I^{\otimes i} \otimes |1\rangle\langle 1| \otimes I^{\otimes n-i-1})(I^{\otimes j} \otimes X \otimes I^{\otimes n-j-1}),$$
$$\mathfrak{u}_{\mathtt{SWAP}(i,j)} = \mathfrak{u}_{\mathtt{CX}(i,j);\mathtt{CX}(j,i);\mathtt{CX}(i,j)},$$

where

$$I^{\otimes i} = \overbrace{I \otimes \cdots \otimes I}^{i}.$$

Because $\mathcal{R} = \{R_a : a \in \mathsf{Prog}[\Pi, L_{\mathcal{F}_{\mathbb{C}^{2^n}}}]\}$ is uniquely determined from $\mathfrak{u}$, the star-free QDF $\mathcal{F}_{\mathrm{QD}} = (\mathcal{F}_{\mathbb{C}^{2^n}}, \mathcal{U}, \mathcal{R})$ is also uniquely determined.

Henceforth, we use the symbols $P(i, |\psi\rangle)$ and $P(i, i{+}1, |\Psi\rangle)$ for specific elements in $L_{\mathbb{C}^{2^n}}$ defined as follow:

$$P(i, |\psi\rangle) = \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{i} \otimes \langle |\psi\rangle \rangle \otimes \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{n-i-1},$$

$$P(i, i+1, |\Psi\rangle) = \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{i} \otimes \langle |\Psi\rangle \rangle \otimes \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{n-i-2},$$

where $\langle |\psi\rangle \rangle$ (resp. $\langle |\Psi\rangle \rangle$) stands for $\{c\,|\psi\rangle : c \in \mathbb{C}\}$ (resp. $\{c\,|\Psi\rangle : c \in \mathbb{C}\}$).

Superdense Coding

Superdense Coding [7] allows us to transmit two classical bits using an entangled state. It consists of encoding and decoding the information. The encoding process of information 00, 01, 10, or 11 is described as follows:

$$\mathbf{encode}_{00} = \mathtt{H}(0)\ ;\ \mathtt{CX}(0,1), \quad \mathbf{encode}_{01} = \mathtt{H}(0)\ ;\ \mathtt{CX}(0,1)\ ;\ \mathtt{X}(0),$$

$$\mathbf{encode}_{10} = \mathtt{H}(0)\ ;\ \mathtt{CX}(0,1)\ ;\ \mathtt{Z}(0), \quad \mathbf{encode}_{11} = \mathtt{H}(0)\ ;\ \mathtt{CX}(0,1)\ ;\ \mathtt{X}(0)\ ;\ \mathtt{Z}(0).$$

The decoding process is described as $\mathbf{decode} = \mathtt{CX}(0,1)\ ;\ \mathtt{H}(0)$.

The desired property for Superdense Coding is that "the encoded information is correctly decoded." In BDQL, this property is expressed as follows:

$$|0\rangle \otimes |0\rangle \in \bigwedge_{i,j \in \{0,1\}} \Box(\mathbf{encode}_{ij}\ ;\ \mathbf{decode}, P(0, |i\rangle) \wedge P(1, |j\rangle)).$$

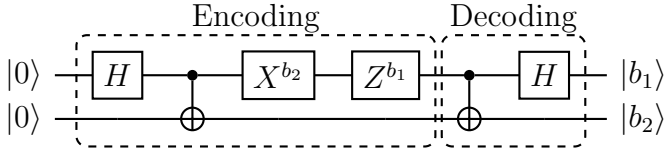


Figure 5.1: Superdense Coding

Quantum Teleportation

Quantum Teleportation [6] is a protocol for teleporting an arbitrary pure state by sending two bits of classical information. The program of Quantum Teleportation is described as follows:

$$\mathbf{teleport} = \mathtt{H}(1)\ ;\ \mathtt{CX}(1,2)\ ;\ \mathtt{CX}(0,1)\ ;\ \mathtt{H}(0)$$

$$
\begin{aligned}
&; \textbf{if } P(1, |0\rangle) \textbf{ then skip else } \mathtt{X}(2) \textbf{ fi} \\
&; \textbf{if } P(0, |0\rangle) \textbf{ then skip else } \mathtt{Z}(2) \textbf{ fi}.
\end{aligned}
$$

The desired property of Quantum Teleportation is that "a pure state $|\psi\rangle$ is correctly teleported." In BDQL, this property is expressed as follows:

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle \in \Box(\textbf{teleport}, P(2, |\psi\rangle)).$$

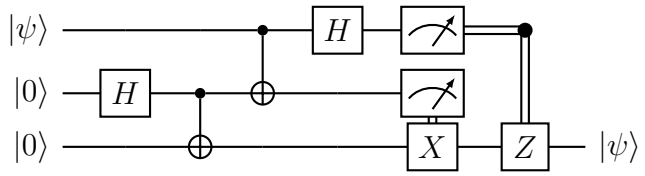


Figure 5.2: Quantum Teleportation

Quantum Secret Sharing

Quantum Secret Sharing (Quantum Information Splitting) [22] is a protocol for teleporting a pure state from a sender (Alice) to a receiver (Bob) with the help of a third party (Charlie). By this protocol, a secret pure state is shared between Alice and Bob, provided that Charlie permits it. The program of Quantum Secret Sharing is described as follows:

$$
\begin{aligned}
\textbf{share} = {} & \mathtt{H}(1) \,;\, \mathtt{CX}(1,2) \,;\, \mathtt{CX}(1,3) \,;\, \mathtt{CX}(0,1) \,;\, \mathtt{H}(0) \,;\, \mathtt{H}(2) \\
& ; \textbf{if } P(1, |0\rangle) \textbf{ then skip else } \mathtt{X}(3)) \textbf{ fi} \\
& ; \textbf{if } P(0, |0\rangle) \textbf{ then skip else } \mathtt{Z}(3) \textbf{ fi} \\
& ; \textbf{if } P(2, |0\rangle) \textbf{ then skip else } \mathtt{Z}(3) \textbf{ fi}.
\end{aligned}
$$

The desired property of secret sharing is similar to that of Quantum Teleportation. In BDQL, this property is expressed as follows:

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \in \Box(\textbf{share}, P(3, |\psi\rangle)).$$

Entanglement Swapping

Entanglement Swapping [23] is a protocol for creating a new entangled state. Suppose that Alice and Bob share two entangled qubits, and Bob and Charlie also

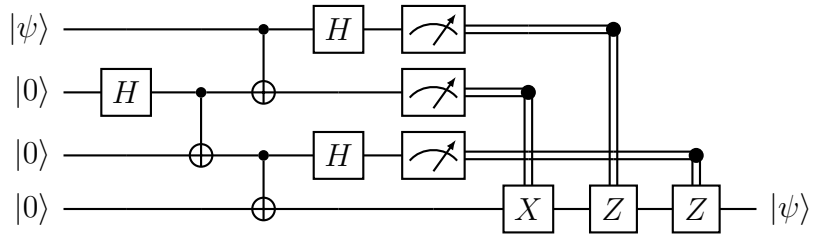


Figure 5.3: Quantum Secret Sharing

share two different entangled qubits. After executing Entanglement Swapping, Alice's qubit and Charlie's qubit become entangled. The program of Entanglement Swapping is described as follows:

$$\begin{aligned}\textbf{entangle} = {} & \texttt{H}(0)\ ;\ \texttt{CX}(0,1)\ ;\ \texttt{H}(2)\ ;\ \texttt{CX}(2,3)\ ;\ \texttt{CX}(1,2)\ ;\ \texttt{H}(1) \\ & ;\ \textbf{if}\ P(2,|0\rangle)\ \textbf{then skip else}\ \texttt{X}(3)\ \textbf{fi} \\ & ;\ \textbf{if}\ P(1,|0\rangle)\ \textbf{then skip else}\ \texttt{Z}(3)\ \textbf{fi} \\ & ;\ \texttt{SWAP}(1,3).\end{aligned}$$

The last $\texttt{SWAP}(1,3)$ is executed to adjoin the remaining qubits.

The desired property of Entanglement Swapping is that "an entangled state (in this case, $|\mathrm{EPR}\rangle$) is created." In BDQL, this property is expressed as follows:

$$|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \in \Box(\textbf{entangle}, P(0,1,|\mathrm{EPR}\rangle)).$$

Note that $\texttt{SWAP}(1,3)$ is needed because $P(i,i+1,|\Psi\rangle)$ is only defined for the consecutive numbers i and $i+1$. That is, the expression $P(0,3,|\mathrm{EPR}\rangle)$ is not defined.

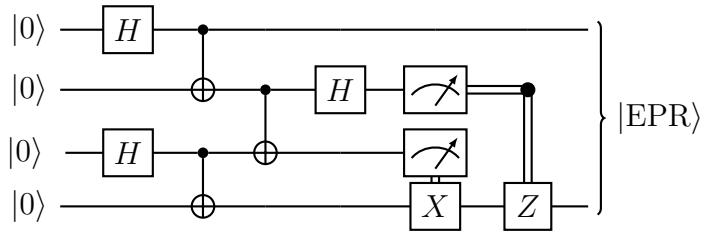


Figure 5.4: Entanglement Swapping

Quantum Gate Teleportation

Quantum Gate Teleportation [18] is a protocol for teleporting a quantum gate. The program of quantum gate teleportation is described as follows:

$$\textbf{gteleport} = \texttt{H}(1)\ ;\ \texttt{CX}(1,2)\ ;\ \texttt{H}(3)\ ;\ \texttt{CX}(3,4)\ ;\ \texttt{CX}(3,2)\ ;\ \texttt{CX}(0,1)\ ;\ \texttt{H}(0)\ ;\ \texttt{CX}(4,5)\ ;\ \texttt{H}(4)$$

; **if** $P(0, |0\rangle)$ **then skip else** $\mathtt{Z}(2)$; $\mathtt{Z}(3)$ **fi**
; **if** $P(1, |0\rangle)$ **then skip else** $\mathtt{X}(2)$ **fi**
; **if** $P(5, |0\rangle)$ **then skip else** $\mathtt{X}(2)$; $\mathtt{X}(3)$ **fi**
; **if** $P(4, |0\rangle)$ **then skip else** $\mathtt{Z}(3)$ **fi**.

The desired property of Quantum Gate Teleportation is that "a quantum gate (in this case, CX) is correctly teleported." In BDQL, this property is expressed as follows:

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |\psi'\rangle \in \Box(\mathbf{gteleport}, P(3, 4, \mathrm{CX}(|\psi'\rangle \otimes |\psi\rangle))).$$

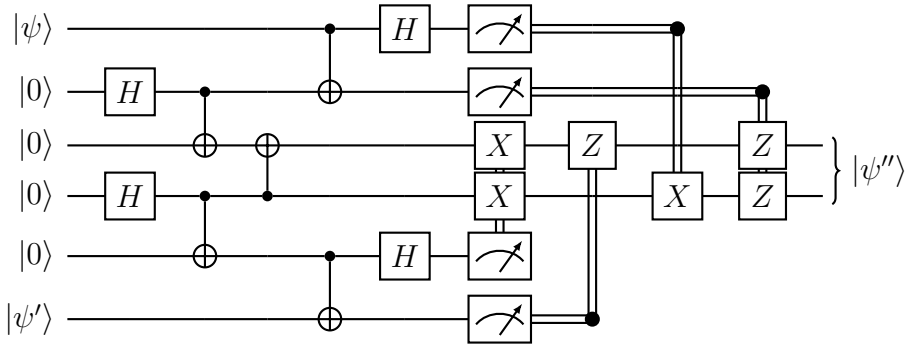


Figure 5.5: Quantum Gate Teleportation ($|\psi''\rangle = \mathrm{CX}(|\psi'\rangle \otimes |\psi\rangle)$)

Chapter 6

Conclusions and Future Work

In this section, we summarize the significant results drawn in this dissertation and discuss them. Also, we suggest some future work.

6.1 Conclusions

We formulated the algebra of quantum programs called Quantum Dynamic Algebra (QDA) for reformulating the algebraic structure of quantum mechanics into modern algebra from the perspective of quantum computation.

In Theorem 4.2.1, we proved that the law of residuation (the algebraic deduction theorem) holds if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\Cap$, which is defined by $p \Cap q = p \wedge (\neg p \vee q)$. This result is significant because algebras that satisfy the law of residuation give algebraic semantics for various substructural logics (see [29]) in general.

In Theorem 4.2.4, we proved that the inference rules in Hoare Logic are sound if the usual conjunction $\wedge$ is replaced by the Sasaki conjunction $\Cap$. The proof is based on quantum counterparts of the law of residuation (Theorem 4.2.1), the monotonicity of $\Box$ (Lemma 4.2.2), and the loop invariance rule (Lemma 4.2.3). Owing to Theorem 4.2.4, it is expected to apply QDA to quantum program verification. The validity of the Hoare-like inference rules means that the inference rules in Hoare Logic also work in the quantum setting as long as the appropriate logical connective(s) are chosen. We verified two simple quantum programs in Section 4.5 as running examples.

In Theorem 4.4.5, we proved that every complex algebra of QDFs is a QDA. Recall that a QDA is an orthomodular lattice. Orthomodular lattices are challenging to deal with because the distributive law does not hold. Besides that, orthomodularity is not determined by any first-order properties of the accessibility relation of Kripke frames for Quantum Logic [14]. These features are not

found in other well-known algebraic structures of logics, such as Boolean lattices (Classical Logic), Heyting lattices (Intuitionistic Logic), or Modal algebras (Modal Logic). Therefore, it is impossible to find a Kripke frame that satisfies its complex algebra, which is an orthomodular lattice. To overcome this difficulty, we extended the Kripke frames for Quantum Logic to QDFs. Unlike the usual Kripke frames, QDFs are equipped with two kinds of accessibility relations. One accessibility relation is an abstraction of the orthogonality relation, and the other accessibility relations are abstractions of the graphs of unitary operators (quantum gates). For this reason, the orthomdular law follows, and thus every complex algebra of QDFs is a QDA. This result implies that incorporating a quantum computation perspective into orthomodular lattices is not only beneficial for its reformulating as modern algebras but also from a technical point of view.

In Theorem 5.3.4, we proved that every complex algebra of star-free QDFs is a star-free QDA. The proof is almost the same as Theorem 4.4.5. Recall that star-free QDA is not just QDA without the iteration operator: a star-free QDA is a QDA equipped with an auxiliary operator $\blacksquare$ for proving the Stone-type representation theorem. Correspondingly, we must newly prove the conditions with respect to $\blacksquare$ imposed on the complex algebra of a star-free QDF: $\blacksquare_{\mathcal{U}}(a, \Box_{\mathcal{R}}(a, P)) = \Box_{\mathcal{R}}(a, \blacksquare_{\mathcal{U}}(a, P)) = P$, $\blacksquare_{\mathcal{U}}(a, S) = S$, and $\blacksquare_{\mathcal{U}}(a, P \cap Q) = \blacksquare_{\mathcal{U}}(a, P) \cap \blacksquare_{\mathcal{U}}(a, Q)$. This is the difference between Theorem 5.3.4 and Theorem 4.4.5.

In Theorem 5.4.4, we proved that every canonical frame of star-free QDAs is a star-free QDF. $\blacksquare$ plays a role in this theorem. That is, the conditions with respect to $\blacksquare$ imposed on star-free QDA are required to show that some conditions imposed on star-free QDF: $\hat{\mathfrak{u}}_\pi$ is bijective, $\hat{\mathfrak{u}}_\pi$ preserves $R^{\mathcal{L}^-_{\mathrm{QD}}}$, and $R^{\mathcal{L}^-_{\mathrm{QD}}}_{\theta(p)?}$ is self-adjoint. One concern is whether the addition of the conditions with respect to $\blacksquare$ for convenience causes problems when applying star-free QDF to quantum program verification. In fact, these conditions are satisfied in star-free Hilbert Dynamic Algebra (Example 5.1.3). Because the verification of the correctness of star-free quantum programs is done in some specific star-free Hilbert dynamic algebras (see Section 5.6), star-free QDA should satisfy the conditions with respect to $\blacksquare$. In fact, these conditions are satisfied in star-free Hilbert Dynamic Algebra (see Example 5.1.3).

In Theorem 5.5.3, we proved the Stone-type representation theorem for star-free QDAs, which states that every star-free QDA is embeddable into its canonical extension. This theorem is proved using Theorem 5.3.4 and Theorem 5.4.4. Even for star-free QDAs, the proof of the Stone-type representation theorem is not straightforward. A (star-free) QDA is made up of a complex combination of multiple algebras, namely an orthomodular lattice, a regular program algebra, and a modal algebra. It is not apparent to prove the Stone-type representation theorem consistent with all these algebras. In Table 6.1, we summarize a comparison with other known Stone-type representation theorems.

Table 6.1: Stone-type Representation Theorems

Algebra	**Complex Algebra**	**Canonical Frame**	**Representation Theorem**
Boolean Lattice	—	—	Theorem 3.3.3
Ortholattice	Definition 3.4.5	Definition 3.4.12	Theorem 3.4.16 [17]
Modal Algebra	Definition 3.5.2	Definition 3.5.3	Theorem 3.5.6 [24]
Star-free QDA	Definition 5.3.1	Definition 5.4.1	Theorem 5.5.3

Theorem 5.5.3 states that the Stone-type representation theorem for star-free QDAs holds. This theorem establishes half of the discrete duality [30] between star-free QDFs and star-free QDAs. That is, a representation theorem for star-free QDAs (as an example of [30, Theorem 2.2.3]) has been shown, but a representation theorem for star-free QDFs (as an example of [30, Theorem 2.2.4]) has not yet been shown. On the other hand, it is known that a categorical duality can be shown for an extension of an orthomodular lattice called a Piron lattice [8]. Because our star-free QDA is another extension of an orthomodular lattice, we expect that we can prove some kind of duality for star-free QDAs as well by combing this paper's result and of [8].

6.2 Future Work

At least two future works remain to be addressed.

On the Iteration Operator

The first future work is about the iteration operator. How to deal with the iteration operator is the major concern from the perspective of both theory and practice (formal verification).

From the theoretical point of view, we should find a full-fledged (namely, with the iteration operator) QDA that satisfies the Stone-type representation theorem.

To show the theorem, we may have to find an embedding that preserves infinite meet and join due to the condition of the iteration operator written by infinite meet (that is, $\Box(a^*, p) = \bigwedge\{\Box(a^i, p) : i \geq 0\}$ in Definition 4.1.2). For Boolean lattices, such an embedding has been found as a result of the Dedekind-MacNeille completion technique. It is also known that the Dedekind-MacNeille completion technique can be applied to ortholattices, but whether it is also applicable to Quantum Dynamic Algebras is an open question.

From the practical point of view, we should develop a general technique to verify the correctness of quantum programs with the iteration operator (which appears in loop programs, for example). In this dissertation, we proved the validity of the **while** rule for quantum programs (Theorem 4.2.4 (4)) and employed it to show the simple quantum while program **qwhile** in Section 4.5. However, it is challenging to find the loop invariance condition to apply the **while** automatically. The same difficulty is also known in (classical) Hoare Logic.

To make matters worse, a state space derived from a Hilbert space is infinite in general. For example, consider the quantum gate (unitary operator)

$$U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

This quantum gate represents rotation with the angle θ. If θ is an irrational multiple of π, then U_θ is aperiodic and generates infinite reachable states by executing U_θ.

One remedy is to allow only periodic rotations as quantum gates, the Pauli gates, for example. In [38], a quantum walk on a finite graph is introduced as an example of quantum while programs. It is expected to verify a desirable property of the quantum walk on a finite graph.

On Atomicity

The second future work is to study star-free QDA with atomicity. Recall that Stone's representation theorem states that every Boolean lattice is embeddable into a powerset lattice (called canonical extension). If the Boolean lattices are restricted to *atomic* and *complete* Boolean lattices, a stronger result is obtained: every atomic complete Boolean lattice is *isomorphic to* a powerset lattice (Theorem 3.3.5). A similar result is expected to obtain for QDA.

In fact, an atomic algebra that is similar to star-free QDA has been formulated. It is called a Piron lattice, which can be regarded as an algebra of quantum programs constructed from only the test operator. As pointed out by [8], there is a kind of dynamic frame (state transition system) with a test transition relation that reflects all the properties of a Piron lattice in the sense of duality in category theory. Such a dynamic frame is called a quantum dynamic frame in [8].

The apparent difference is that star-free QDFs are more like the dynamic frame corresponding to Dynamic Algebra. That is, star-free QDFs have various relations that represent programs constructed by the program constructs (including the test operator). However, quantum dynamic frames have only one kind of relation that represents tests.

The more significant difference is that star-free QDFs are more abstract than quantum dynamic frames. This difference is reflected in the algebras that each

frame corresponds to: a star-free QDF corresponds to an orthomodular lattice with some additional operators $\Box$ and $\blacksquare$ called a star-free QDA, and a quantum dynamic frame corresponds to the specific orthomodular lattice called a Piron lattice. In a Piron lattice, the relation $a \to b$ that represents non-orthogonality is characterized by the condition $a \not\leq b^{\perp}$ (see [8, (31)]). Stated differently, orthogonality is characterized by the condition $a \leq b^{\perp}$. On the other hand, the relation $FR^{\mathcal{L}^{-}_{\mathrm{QD}}}G$ that represents orthogonality in star-free QDAs is defined by the condition that $p \in F$ and $\neg p \in G$ for some $p \in L$ (see Definition 5.4.1). Although these two conditions are seemingly different, it can be shown that they correspond under the atomicity in fact.

Theorem 6.2.1. For any atomic ortholattice $(L, \leq, \neg)$, $F_a R^{\mathcal{L}^{-}_{\mathrm{QD}}} F_b$ if and only if $a \leq \neg b$, where F_a and F_b are the principal filters generated by atoms a and b, respectively.

Proof. ($\Rightarrow$) If $F_a R^{\mathcal{L}^{-}_{\mathrm{QD}}} F_b$, then $p \in F_a$ and $\neg p \in F_b$ for some $p \in L$. Thus, $a \leq p$ and $b \leq \neg p$. It follows from the definition of ortholattices that $p \leq \neg b$. Hence, $a \leq \neg b$ by the transitivity of $\leq$.

($\Leftarrow$) Suppose $a \leq \neg b$. It suffices to show that $a \leq p$ and $b \leq \neg p$ for some $p \in L$. It is satisfied by choosing a as p. Because $a \leq a$ holds by the reflexivity of $\leq$, we only show $b \leq \neg a$. It follows from the assumption $a \leq \neg b$ that $b = \neg\neg b \leq \neg a$, as desired. $\Box$

Because of this observation, it is expected to prove the extended Stone-type representation theorem for *atomic* star-free QDAs.

Bibliography

[1] A. Baltag, J. Bergfeld, K. Kishida, J. Sack, S. Smets, and S. Zhong. PLQP & company: decidable logics for quantum algorithms. *International Journal of Theoretical Physics*, 53(10):3628–3647, 2014.

[2] A. Baltag and S. Smets. Complete axiomatizations for quantum actions. *International Journal of Theoretical Physics*, 44(12):2267–2282, 2005.

[3] A. Baltag and S. Smets. LQP: the dynamic logic of quantum information. *Mathematical structures in computer science*, 16(3):491–525, 2006.

[4] A. Baltag and S. Smets. Quantum logic as a dynamic logic. *Synthese*, 179(2):285–306, 2011.

[5] A. Baltag and S. Smets. Reasoning about quantum information: An overview of quantum dynamic logic. *Applied Sciences*, 12(9), 2022.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[7] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[8] J. M. Bergfeld, K. Kishida, J. Sack, and S. Zhong. Duality for the logic of quantum actions. *Studia Logica*, 103:781–805, 2015.

[9] J. M. Bergfeld and J. Sack. Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs. *Soft Computing*, 21(6):1421–1441, 2017.

[10] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of mathematics*, 57(4):823–843, 1936.

[11] P. Blackburn, M. De. Rijke, and Y. Venema. *Modal Logic*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2001.

[12] A. Chagrov and M. Zakharyaschev. *Modal logic*, volume 35 of *Oxford Logic Guides*. Clarendon Press, 1997.

[13] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge university press, 2nd edition, 2002.

[14] R. Goldblatt. Orthomodularity is not elementary. *The Journal of Symbolic Logic*, 49(2):401–404, 1984.

[15] R. Goldblatt. *Logics of time and computation*. CSLI Lecture Notes ; 7. Center for the Study of Language and Information, second edition, 1987.

[16] R. I. Goldblatt. Semantic analysis of orthologic. *Journal of Philosophical Logic*, 3:19–35, 1974.

[17] R. I. Goldblatt. The Stone space of an ortholattice. *Bulletin of the London Mathematical Society*, 7:45–48, 1975.

[18] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[19] G. M. Hardegree. The conditional in quantum logic. In *Logic and Probability in Quantum Mechanics*, pages 55–72. Springer, 1976.

[20] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[21] L. Herman, E. L. Marsden, and R. Piziak. Implication connectives in orthomodular lattices. *Notre Dame Journal of Formal Logic*, 16(3):305–328, 1975.

[22] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, 1999.

[23] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, 1993.

[24] B. Jónsson and A. Tarski. Boolean algebras with operators. part I. *American journal of mathematics*, 73:891–939, 1951.

[25] T. Kawano. Advanced Kripke frame for quantum logic. In *International Workshop on Logic, Language, Information, and Computation*, pages 237–249, 2018.

[26] D. Kozen. A representation theorem for models of $*$-free PDL. In *International Colloquium on Automata, Languages, and Programming*, pages 351–362, 1980.

[27] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[28] H. Nishimura. Semantical analysis of constructive PDL. *Publications of the Research Institute for Mathematical Sciences*, 18(2):427–438, 1982.

[29] H. Ono. *Substructural logics and residuated lattices—an introduction*. Springer, 2003.

[30] Ewa Orłowska, Anna Maria Radzikowska, and Ingrid Rewitzky. *Dualities for structures of applied logics*, volume 56 of *Studies in Logic: Mathematical Logic and Foundations*. College Publications, 2015.

[31] Y. Peng, M. Ying, and X. Wu. Algebraic reasoning of quantum programs via non-idempotent Kleene algebra. In *Proceedings of the 43rd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, pages 657–670, 2022.

[32] V. R. Pratt. Semantical considerations on Floyd-Hoare logic. In *17th Annual Symposium on Foundations of Computer Science (sfcs 1976)*, pages 109–121. IEEE, 1976.

[33] M. Rédei. *Quantum logic in algebraic approach*, volume 91 of *Fundamental Theories of Physics*. Springer, 1998.

[34] U. Sasaki. Orthocomplemented lattices satisfying the exchange axiom. *Journal of Science Hiroshima Univertisty A*, 17:293–302, 1954.

[35] V. S. Varadarajan. *Geometry of Quantum Theory*. Springer, 2nd edition, 1985.

[36] T. Vetterlein. Transitivity and homogeneity of orthosets and inner-product spaces over subfield of $\mathbb{R}$. *Geometriae Dedicata*, 206(36), 2022.

[37] M. Ying. Floyd–Hoare logic for quantum programs. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 33(6):1–49, 2012.

[38] M. Ying and Y. Feng. Quantum loop programs. *Acta Informatica*, 47(4):221–250, 2010.

[39] N. Yu. Quantum temporal logic. *arXiv preprint arXiv:1908.00158*, 2019.

[40] L. Zhou, N. Yu, and M. Ying. An applied quantum Hoare logic. In *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 1149–1162, 2019.

List of Publications

Refereed Publications

1. **Tsubasa Takagi**, Canh Minh Do, Kazuhiro Ogata. Automated Quantum Program Verification in Dynamic Quantum Logic. In Proceedings of DaLí: Dynamic Logic – New trends and applications (DaLí 2023), *Lecture Notes in Computer Science (LNCS)*, forthcoming, 2023.

2. **Tsubasa Takagi**, Semantic Analysis of a Linear Temporal Extension of Quantum Logic and Its Dynamic Aspect. *ACM Transactions on Computational Logic*, 24(3): 1–21, 2023.

3. **Tsubasa Takagi**, An algebra of quantum programs with the Kleene star operator. In Proceedings of Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022 (FAVPQC 2022), *CEUR Workshop Proceedings*, 3280: 2–15, 2022.

4. **Tsubasa Takagi**, Translation from Three-Valued Quantum Logic to Modal Logic. *International Journal of Theoretical Physics*, 60(1): 366–377, Springer, 2021.

5. **Tsubasa Takagi**, Observable-Dependent Kripke Semantics for Quantum Logic (in Japanese). *Japanese Student Research Notes of Philosophy of Science*, 4: 1–8, 2021.

6. **Tsubasa Takagi**, Validity Checking by K4 Tableau and Filtration Method (in Japanese). *Journal of Science and Philosophy*, 2(1): 4–23, 2019.

Non-refereed Publications

1. **Tsubasa Takagi**, Quantum Program Verification and Its Implementation Based on Dynamic Quantum Logic (in Japanese). In the special interest group technical reports of Information Processing Society of Japan (9th Quantum Software Workshop at IPSJ), *IPSJ SIG Technical Report*, Vol.2023-QS-9 No.6, 2023.

Index