An Algebra of Quantum Programs with the Kleene Star Operator

Tsubasa Takagi

JAIST

Contents

1 Introduction

2 Preliminaries

3 Quantum Dynamic Algebra

4 Quantum Dynamic Frame

5 Characteristic Algebra

What is DQL?

- Dynamic Quantum Logic (DQL) is a logic for formal verification of quantum programs.
- Specifically, some quantum protocols, such as Quantum Teleportation, Quantum Secret Sharing, Quantum Search Algorithm, the quantum leader election protocol, and the BB84 quantum key distribution protocol have been verified by using DQL.
- DQL is a dynamical extension of the traditional quantum logic, and is based on the idea of propositional dynamic logic (PDL).
- By incorporating program constructs $a; b$ (composition), $a \cup b$ (non-deterministic choice), $p?$ (quantum test) into quantum logic as a modal logic, DQL makes it possible to deal with quantum programs.

Problem

- However, the previous studies of DQL have not discussed the Kleene star operator (iteration) of a quantum program.
- Baltag and Smets, the initiators of DQL, stated that[1] "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."

[1] LQP: the dynamic logic of quantum information, Mathematical structures in computer science, 491–525, 2006.

It does not mean that it is not worth adding the Kleene star operator to DQL.

1. Using the Kleene star operator is necessary to deal with quantum while loops.
2. Moreover, it is significant to discuss the Kleene star operator of quantum programs for connecting DQL to a considerable amount of previous research on finite quantum automata.

Contents

1. Introduction

2. **Preliminaries**

3. Quantum Dynamic Algebra

4. Quantum Dynamic Frame

5. Characteristic Algebra

Definition 2.1

A lattice $(P, \preceq)$ is a poset that a two-element set $\{p, q\}$ has the infimum (greatest lower bound) $p \wedge q$ and supremum (least upper bound) $p \vee q$ for any $p, q \in P$. A lattice $(P, \preceq)$ is said to be complete if each subset Γ of P has the infimum $\bigwedge \Gamma$ and supremum $\bigvee \Gamma$.

In the sequel, the least element $\bigwedge P$ and greatest element $\bigvee P$ in a complete lattice $(P, \preceq)$ are denoted as $\curlywedge$ and $\curlyvee$ respectively.

Definition 2.2

A lattice $(Q, \preceq)$ is called a sublattice of a lattice $(P, \preceq)$ if Q is a non-empty subset of P satisfying $p \wedge q, p \vee q \in Q$ for any $p, q \in Q$.

Definition 2.3

A complete orthomodular lattice is a triple $(P, \preceq, \neg)$ that consists of a complete lattice $(P, \preceq)$ and function $\neg : P \to P$ such that

1. $p \wedge \neg p = \curlywedge$, $p \vee \neg p = \curlyvee$,
2. $\neg\neg p = p$,
3. $p \preceq q$ implies $\neg q \preceq \neg p$, and
4. the orthomodular law $p \wedge (\neg p \vee (p \wedge q)) \preceq q$ holds,

for any $p, q \in P$. A complete ortholattice is a complete orthomodular lattice without the orthomodular law.

- In quantum logic, implication $p \to q$ called Sasaki implication is defined as $\neg p \vee (p \wedge q)$.
- The orthomodular law corresponds to a rule of inference, Modus Ponens in quantum logic: q is deducible from p and $p \to q$.

Example 2.1 (Powerset Lattice)

Let $\mathcal{P}(S)$ be the powerset of a set S. Then, $(\mathcal{P}(S), \subseteq, {}^c)$ is a complete orthomodular lattice and is called a powerset lattice for the set complement ^{c} in S. A powerset lattice is complete because $\bigwedge \Gamma = \bigcap_{p \in \Gamma} p$ and $\bigvee \Gamma = \bigcup_{p \in \Gamma} p$ exist for each $\Gamma \subseteq \mathcal{P}(S)$. Hereafter, we shall use the symbols $\bigcap \Gamma$ and $\bigcup \Gamma$ for the infimum and supremum of a set Γ in a powerset lattice respectively.

Example 2.2 (Hilbert Lattice)

Let $\mathcal{H}$ be a Hilbert space, and $\mathcal{C}(\mathcal{H})$ be the set of all closed subspaces of $\mathcal{H}$. Then, $(\mathcal{C}(\mathcal{H}), \subseteq, ^{\perp})$ is a complete orthomodular lattice and is called a Hilbert lattice. Here, for each $V \in \mathcal{C}(\mathcal{H})$, $V^{\perp}$ 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

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

exist for each $\Gamma \subseteq \mathcal{C}(\mathcal{H})$. It is known that $\bigvee \Gamma = ((\bigcup \Gamma)^{\perp})^{\perp}$.

Note that the least element $\bigwedge \mathcal{C}(\mathcal{H})$ is the singleton $\{\mathbf{0}\}$ of the zero vector (origin) $\mathbf{0}$, and the greatest element $\bigvee \mathcal{C}(\mathcal{H})$ is $\mathcal{H}$. The supremum $V \vee W$ of $\{V, W\} \subseteq \mathcal{C}(\mathcal{H})$ is the closed subspace $\overline{V + W}$ generated by

$$V + W := \{v + w : v \in V, w \in W\}.$$

Definition 2.4

A complete orthomodular lattice $(P, \preceq, \neg)$ is called a complete Boolean lattice if $(P, \preceq)$ is distributive. That is, the distributive law

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

holds for any $p, q, r \in P$.

For example, a powerset lattice is a complete Boolean lattice, but a Hilbert lattice is not. In fact, a counter-example to the distributive law in a Hilbert lattice is as follows: let V, W be one-dimensional subspaces of $\mathcal{H}$, and U be a one-dimensional subspace of $V + W$, then

$$U \cap (V + W) = U \neq \{\mathbf{0}\}$$

but

$$(U \cap V) + (U \cap W) = \{\mathbf{0}\} + \{\mathbf{0}\} = \{\mathbf{0}\}.$$

Contents

1 Introduction

2 Preliminaries

3 Quantum Dynamic Algebra

4 Quantum Dynamic Frame

5 Characteristic Algebra

Regular quantum programs are formed from the atomic programs and elements in the domain of a complete orthomodular lattice by using the program constructs

- ; (sequential composition),
- $\cup$ (non-deterministic choice),
- * (iteration), and
- ? (test).

These notations are used in Propositional Dynamic Logic (PDL).

Definition 3.1

Let Π_0 be a set of atomic programs. For any complete ortholattice $\mathcal{L} = (P, \preceq, \neg)$, the set $\Pi_{\mathcal{L}}$ of all regular quantum programs is generated by the grammar

$$\Pi_{\mathcal{L}} \ni a ::= \textbf{skip} \mid \textbf{abort} \mid \pi \mid a; a \mid a \cup a \mid a^* \mid p?,$$

where $\pi \in \Pi_0$ and $p \in P$.

$\Pi_{\mathcal{L}}$ includes various programs, but the if-then and while-do programs are of particular significance. These are defined by

$$\textbf{if}\ p\ \textbf{then}\ a\ \textbf{else}\ b := (p?; a) \cup (\neg p?; b),$$
$$\textbf{while}\ p\ \textbf{do}\ a := (p?; a)^{*}; \neg p?,$$

Unlike classical programs, the guard clause $p?$ in the quantum if-then-else program (while-do program) is evaluated in a complete orthomodular lattice that may not be a complete Boolean lattice.

- It is worth paying attention to a precondition and postcondition of programs to verify them, as Hoare Logic does.
- A regular quantum program $a \in \Pi_{\mathcal{L}}$ is said to be partially correct with respect to a precondition $p \in P$ and postcondition $q \in P$ (denoted $\{p\}\, a\, \{q\}$) 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.
- Because the partial correctness does not guarantee that the program halts, the correctness is called partial.
- We introduce a function $\Box : \Pi_{\mathcal{L}} \times P \to P$ to express the partial correctness: $\Box(a, p)$ represents the weakest precondition ensuring that p will hold after executing a.
- Then, $\{p\}\, a\, \{q\}$ is expressed as $p \preceq \Box(a, q)$. This function $\Box$ is subject to some conditions described in the following.

Definition 3.2

A quantum dynamic algebra (QD-algebra) is a quadruple $(P, \preceq, \neg, \square)$ that consists of a complete orthomodular lattice $(P, \preceq, \neg)$ and function (scalar multiplication) $\square : \Pi_{\mathcal{L}} \times P \to P$ satisfying the following conditions:

1. $\square(\textbf{skip}, p) = p$;
2. $\square(\textbf{abort}, p) = \curlyvee$;
3. $\square(a, \curlyvee) = \curlyvee$;
4. $\square(a, p \wedge q) = \square(a, p) \wedge \square(a, q)$;
5. $\square(a; b, p) = \square(a, \square(b, p))$;
6. $\square(a \cup b, p) = \square(a, p) \wedge \square(b, p)$;
7. $\square(a^*, p) = \bigwedge\{\square(a^i, p) : i \geq 0\}$, where a^i is defined recursively by $a^0 = \textbf{skip}$ and $a^{i+1} = a^i; a$ for each $i \geq 0$;
8. $\square(p?, q) = \neg p \vee (p \wedge q)$.

Note that $\square(a^*, p)$ exists owing to the completeness of $(P, \preceq, \neg)$. The condition (7) of Definition 3.2 is called $*$-continuity.

Example 3.1 (Powerset Dynamic Algebra)

A powerset lattice $(\mathcal{P}(S), \subseteq, {}^{c}, \Box)$ with a function $\Box$ satisfying the conditions of Definition 3.2 is a QD-algebra and is called a powerset QD-algebra. Because a power lattice is a complete Boolean lattice, $\Box(p?, q) = p^{c} \cup q$ holds by the distributive law. Thus, $\Box(p, q)$ is regarded as the (material) implication in classical logic.

Example 3.2 (Hilbert Dynamic Algebra)

A Hilbert lattice $(\mathcal{C}(\mathcal{H}), \subseteq, {}^{\perp}, \Box)$ with a function $\Box$ satisfying the conditions of Definition 3.2 is a QD-algebra and is called a Hilbert Dynamic algebra. In a Hilbert Dynamic algebra, $\Box(V?, W)$ is called the Sasaki hook, which is known as the implication in quantum logic. 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. Interpreting a quantum test as a projection is the key idea of DQL.

Contents

1 Introduction

2 Preliminaries

3 Quantum Dynamic Algebra

4 Quantum Dynamic Frame

5 Characteristic Algebra

- So far, we have not mentioned the notion of states and relations between them at all.
- However, it is helpful to intuitively understand the properties of regular quantum programs by representing their execution by relations.
- An orthoframe is used for giving Kripke (or relational) semantics to orthologic.
- Henceforth, we write $s \not R t$ for the condition $(s, t) \notin R$.

Definition 4.1

An orthoframe (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 4.1 (Hilbert Frame)

Let $\mathcal{H}$ be a Hilbert space, $\mathbf{Pure}(\mathcal{H})$ be the set of all pure states (unit vectors) in $\mathcal{H}$, and $\perp$ be the orthogonality relation on $\mathcal{H}$. Then, $(\mathbf{Pure}(\mathcal{H}), \perp)$ 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 $\mathcal{H}$.

- The notion of the orthogonal complement of a closed subspace is generalized as follows: the orthogonal complement $T^\perp$ of $T \subseteq S$ is defined as
$$\{s \in S : sRt \text{ for any } t \in T\}.$$
- Here, T may be empty, and $\emptyset^\perp = S$ by the definition.
- The notion of a closed subspace is also generalized by using the above generalization of an orthogonal complement.
- Recall that $V \subseteq \mathcal{H}$ is a closed subspace if and only if $(V^\perp)^\perp = V$.

Definition 4.2

$T \subseteq S$ is said to be orthoclosed in an orthoframe (S, R) if $(T^\perp)^\perp = T$.

- A relation R_a on S can be defined for each $a \in \Pi_{\mathcal{L}}$ by interpreting R_a as the execution process of a program a.
- That is, sR_at is intended that t is accessible from s by executing a.

Definition 4.3

A quantum dynamic frame (QD-frame) is a triple $(S, R, \mathcal{R})$ that consists of an orthoframe (S, R) and family $\mathcal{R} := \{R_a\}_{a \in \Pi_{\mathcal{L}}}$ 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. $sR_{a;b}t$ if and only if sR_au and uR_bt for some $u \in S$;
4. $sR_{a \cup b}t$ if and only if $s(R_a \cup R_b)t$;
5. $sR_{a^*}t$ if and only if $s(\bigcup_{i \geq 0} R^i)t$, where $R^0 := R_{\mathbf{skip}}$ and $R^{i+1} := R^i; R$ for each $i \geq 0$;
6. $sR_{p?}t$ if and only if $t \in p \wedge (\neg p \vee q)$ for any q satisfying $s \in q$.

Example 4.2 (Hilbert QD-frame)

Let $\{U_\pi\}_{\pi \in \Pi_0}$ be a family of unitary operators (quantum gates) on $\mathcal{H}$. The graph $G(U_\pi)$ of U_π is defined by

$$G(U_\pi) = \{(s, U_\pi(s)) : s \in \mathbf{Pure}(\mathcal{H})\}.$$

Then, for any Hilbert frame $(\mathbf{Pure}(\mathcal{H}), \perp)$, the QD-frame $(\mathbf{Pure}(\mathcal{H}), \perp, \mathcal{R})$, called a Hilbert QD-frame, is uniquely constructed from $\{R_\pi\}_{\pi \in \Pi_0} = \{G(U_\pi)\}_{\pi \in \Pi_0}$.

Among various QD-frames, those satisfying the following properties are of particular significance.

Definition 4.4

- A QD-frame $(S, R, \mathcal{R})$ is said to be self-adjoint if $R_{p?}$ is self-adjoint for each $p \in P$: for any $s, t, u \in S$, $sR_{p?}t$ and $t \not\mathcal{R} u$ jointly imply that $uR_{p?}v$ and $s \not\mathcal{R} v$ for some $v \in S$.
- A QD-frame $(S, R, \mathcal{R})$ is said to be orthostable if for any $s, t \in S$ and $\pi \in \Pi_0$, $sR_\pi t$ implies that there exists $u \in S$ such that $s \not\mathcal{R} u$ and for any $v \in S$, $u \not\mathcal{R} v$ implies $vR_\pi t$.

Contents

1. Introduction

2. Preliminaries

3. Quantum Dynamic Algebra

4. Quantum Dynamic Frame

5. Characteristic Algebra

- Now we construct a characteristic algebra from a QD-frame (orthoframe).
- Moreover, we prove that a characteristic algebra of an orthostable self-adjoint QD-frame is a QD-algebra.
- Before embarking on this proof, we show that a characteristic algebra of an orthoframe is an ortholattice.

Definition 5.1

A characteristic algebra $C(\mathcal{F})$ of an orthoframe $\mathcal{F} = (S, R)$ is a triple $(P_{\mathcal{F}}, \subseteq, \neg_R)$ that consists of the set $P_{\mathcal{F}}$ of all orthoclosed sets in $\mathcal{F}$, set inclusion relation $\subseteq$ on $P_{\mathcal{F}}$, and function $\neg_R : P_{\mathcal{F}} \to P_{\mathcal{F}}$ such that

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

Note that $\neg_R p = p^{\perp}$ by the definition of $^{\perp}$. Hence,

$$\neg_R \neg_R(\neg_R p) = \neg_R(\neg_R \neg_R p) = \neg_R p$$

if $p \in P_{\mathcal{F}}$. In other words, $\neg_R p \in P_{\mathcal{F}}$ if $p \in P_{\mathcal{F}}$. This guarantees that $\neg_R : P_{\mathcal{F}} \to P_{\mathcal{F}}$ is well-defined.

Lemma 5.2

$P_{\mathcal{F}}$ is a topped intersection structure on S:

1. $\bigcap \Gamma \in P_{\mathcal{F}}$ for any $\Gamma \subseteq P_{\mathcal{F}}$, and
2. $S \in P_{\mathcal{F}}$.

In general, a topped intersection structure ordered by inclusion is a complete lattice. Thus, the following corollary is obtained.

Corollary 5.3

$(P_{\mathcal{F}}, \subseteq)$ is a complete lattice, where the infimum and supremum of $\Gamma \subseteq P_{\mathcal{F}}$ in $(P_{\mathcal{F}}, \subseteq)$ are $\bigcap \Gamma$ and the smallest orthoclosed set $\biguplus \Gamma$ containing $\bigcup \Gamma$ respectively.

Symbolically,

$$\biguplus \Gamma := \bigcap \{p \in P_{\mathcal{F}} : \bigcup \Gamma \subseteq p\}.$$

We shall denote by $p \uplus q$ the supremum of $\{p, q\}$.

Theorem 5.4

$C(\mathcal{F}) = (P_{\mathcal{F}}, \subseteq, \neg_R)$ is a complete ortholattice.

Proof: By Corollary 5.3, $(P_{\mathcal{F}}, \subseteq)$ is a complete lattice. The conditions (1)–(3) of an ortholattice lattice (Definition 2.3) are proved as follows.

1. Proof of $p \cap \neg_R p = \emptyset$ and $p \uplus \neg_R p$. Suppose for the sake of contradiction that $s \in p \cap \neg_R p$. Then, $s \in p$ and $s \in \neg_R p$, and thus sRs but it contradicts to the condition that R is irreflexive. Hence, $p \cap \neg_R p = \emptyset$.
2. Proof of $\neg_R \neg_R p = p$. It immediately follows from $p \in P_{\mathcal{F}}$.
3. Proof of $p \subseteq q$ 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 $\neg_R q \subseteq \neg_R p$.

The notion of characteristic algebra of an orthoframe is extended to that of an orthostable self-adjoint QD-frame.

Definition 5.5

Let $\mathcal{F} = (S, R)$ be an orthoframe. A characteristic algebra $C(\mathcal{F}_{\mathcal{R}})$ of an orthostable self-adjoint QD-frame $\mathcal{F}_{\mathcal{R}} = (S, R, \mathcal{R})$ is a quadruple $(P_{\mathcal{F}}, \subseteq, \neg_R, \square_{\mathcal{R}})$ that consists of the set $P_{\mathcal{F}}$ of all orthoclosed sets in $\mathcal{F}$, set inclusion relation $\subseteq$ on $P_{\mathcal{F}}$, and functions $\neg_R : P_{\mathcal{F}} \to P_{\mathcal{F}}$ and $\square_{\mathcal{R}} : \Pi_{C(\mathcal{F})} \times P_{\mathcal{F}} \to P_{\mathcal{F}}$ such that

1. $\neg_R p = p^{\perp}$, which means $\neg_R p = \{s \in S : sRt \text{ for any } t \in p\}$, and
2. $\square_{\mathcal{R}}(a, p) = \{s \in S : t \in p \text{ for any } t \in S \text{ satisfying } sR_a t\}$.

It is not obvious that there exist $\square_{\mathcal{R}}(a, p)$ in $P_{\mathcal{F}}$ for any $p \in P_{\mathcal{F}}$ and $a \in \Pi_{\mathcal{L}}$.

Lemma 5.6

1. $\Box_{\mathcal{R}}(\mathbf{skip}, p) = p$.
2. $\Box_{\mathcal{R}}(\mathbf{abort}, p) = S$.
3. $\Box_{\mathcal{R}}(a; b, p) = \Box_{\mathcal{R}}(a, \Box_{\mathcal{R}}(b, p))$.
4. $\Box_{\mathcal{R}}(a \cup b, p) = \Box_{\mathcal{R}}(a, p) \cap \Box_{\mathcal{R}}(b, p)$.
5. $\Box_{\mathcal{R}}(a^*, p) = \bigcap\{\Box_{\mathcal{R}}(a^i, p) : i \geq 0\}$.

Lemma 5.7

If $(S, R, \mathcal{R})$ is self-adjoint, then

1. $s \in p$ implies that $sR_{p?}s$, and
2. $\Box_{\mathcal{R}}(p?, q) = \neg_R p \uplus (p \cap q)$.

Theorem 5.8

If $(S, R, \mathcal{R})$ is an orthostable self-adjoint QD-frame, then $P_{\mathcal{F}}$ is closed under $\Box_{\mathcal{R}}$: $p \in P_{\mathcal{F}}$ implies $\Box_{\mathcal{R}}(a, p) \in P_{\mathcal{F}}$ for each $a \in \Pi_{\mathcal{L}}$.

Theorem 5.9

The characteristic algebra $C(\mathcal{F}_\mathcal{R})$ of an orthostable self-adjoint QD-frame $\mathcal{F}_\mathcal{R} = (S, R, \mathcal{R})$ is a QD-algebra.

Proof:

- $(P_\mathcal{F}, \subseteq)$ is a complete ortholattice with the infimum $\bigcap \Gamma$ and supremum $\biguplus \Gamma$ for each $\Gamma \subseteq P_\mathcal{F}$ by Theorem 5.4.
- Moreover, $(P_\mathcal{F}, \subseteq)$ is an orthomodular lattice. To show the orthomodular law, it suffices to show that $s \in p \cap \Box_\mathcal{R}(p?, q)$ implies $s \in q$. Because $s \in p$, it follows from Lemma 5.7 (1) that $sR_{p?}s$. Therefore, $s \in \Box_\mathcal{R}(p?, q)$ implies $s \in q$.
- Finally, we prove that $C(\mathcal{F}_\mathcal{R})$ is a QD-algebra. The only remaining thing to be shown is the conditions (1)–(8) of Definition 3.2 but all of them except for (3) $\Box_\mathcal{R}(a, S) = S$ and (4) $\Box_\mathcal{R}(a, p \cap q) = \Box_\mathcal{R}(a, p) \cap \Box_\mathcal{R}(a, q)$ have already been shown in Lemma 5.6.
  (3) Proof of $\Box_\mathcal{R}(a, S) = S$. Immediate.
  (4) Proof of $\Box_\mathcal{R}(a, p \cap q) = \Box_\mathcal{R}(a, p) \cap \Box_\mathcal{R}(a, q)$. By straightforward calculation.

Conclusion

- In this talk, we formulated an algebra of regular quantum programs with the Kleene star operator called QD-algebra by combining complete orthomodular lattice and dynamic algebra.
- Moreover, to relate a QD-algebra to a state transition system induced by transitions of programs, we defined a specific QD-algebra associated with relations called characteristic algebra.
- Our main result is that a characteristic algebra of an orthostable self-adjoint QD-frame is a QD-algebra.

Conclusion

- The contribution of this paper is to give semantics of the full-fledged DQL.
- The semantics proposed so far are those of DQL lacking the Kleene star operator.
- However, the Kleene star operator is indispensable to express practical quantum programs, especially quantum while programs.
- Therefore, the semantics proposed in this paper is useful for the formal verification of meaningful quantum programs.

Thank you for listening.