An Algebra of Quantum Programs with the Kleene Star Operator

Tsubasa Takagi[1,2]

[1] *Japan Advanced Institute of Science and Technology, Nomi, Japan*
[2] *Research Fellow of Japan Society for the Promotion of Science*

Abstract

Dynamic Algebra is an algebra that extends the expressive power of Hoare logic and has been used in formal verification of programs. However, quantum programs (programs executed by a quantum computer) behave differently from classical programs. Therefore, it is natural to extend dynamic algebra based on classical logic (Boolean lattice) to quantum dynamic algebra based on quantum logic (complete orthomodular lattice). Nevertheless, quantum dynamical algebra has not been formulated to date because of the difficulty in dealing with repeated execution of quantum programs, which the Kleene star operator represents. In this paper, we formulate an algebra of quantum programs with the Kleene star operator by using an algebraic specification that directly represents the iteration of quantum programs. In addition, we discuss how to construct the algebra from a transition system representing program execution.

Keywords

Quantum Program, Dynamic Algebra, Orthomodular Lattice, Kripke Frame

1. Introduction

Dynamic Quantum Logic (DQL) [1] is a logic for formal verification of quantum programs. Specifically, some quantum protocols, such as Quantum Teleportation [2], Quantum Secret Sharing [2], Quantum Search Algorithm [3], the quantum leader election protocol [3, 4], and the BB84 quantum key distribution protocol [4] have been verified by using DQL (see also [5]). DQL is a dynamical extension of the traditional quantum logic [6], and is based on the idea of propositional dynamic logic (PDL) [7]. 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.

However, the previous studies of DQL have not discussed the Kleene star operator (iteration) of a quantum program. This is because it was not necessary to use the Kleene star 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 [2]. It does not mean that it is not worth adding the Kleene star operator to DQL. Using the Kleene star operator is necessary to deal with quantum while loops. For example, quantum while loops are used

International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols 2022
tsubasa@jaist.ac.jp (T. Takagi)
0000-0001-9890-1015 (T. Takagi)

in the quantum walk algorithm [8] for repeatedly choosing quantum programs corresponding to “Left” or “Right.” 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 (see [9] for example).

In this paper, we define an algebra of regular quantum programs with the Kleene star operator and call it quantum dynamic algebra (QD-algebra). The algebra is constructed by combining the algebra of quantum mechanics (called complete orthomodular lattice) with dynamic algebra [10].

QD-algebra is used for giving algebraic semantics to DQL. However, algebraic semantics is not suited to express a state transition system (in that transitions represent program execution) in general because algebra merely defines various conditions, and the notion of states does not appear explicitly. To overcome this problem, we propose a specific QD-algebra that is associated with a state transition system called a QD-frame (Definition 4.3) and call it a characteristic algebra (Definition 5.5). Characteristic algebra gives relational semantics (namely, Kripke semantics) to DQL.

2. Preliminaries

Various algebras for quantum mechanics have already been well studied since 1936 [6]. The starting point for the study of algebra for quantum mechanics is a complete orthomodular lattice that characterizes the lattice of all closed subspaces of a Hilbert space (Theorem 2.3). For more details, see [11].

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 complete ortholattice 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) $\neg\neg p = p$, and
(3) $p \preceq q$ implies $q \preceq p$,

for any $p, q \in P$. A complete orthomodular is a complete ortholattice satisfying the orthomodular law

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

Many equivalent definitions of the orthomodular law are known [12, Lemma 19]. One of them is that $p \preceq q$ implies $q = p \vee (\neg p \wedge q)$.

Example 2.1 (Powerset Lattice). Let $\wp(S)$ be the powerset of a set S. Then, $(\wp(S), \subseteq, {}^c)$ is a complete orthomodular lattice and is called the powerset lattice of S, where ^{c} denotes the set complementation 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 $\Gamma \subseteq \wp(S)$. 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 $\mathscr{H}$ be a Hilbert space, and $\mathbf{C}(\mathscr{H})$ be the set of all closed subspaces of $\mathscr{H}$. Then, $(\mathbf{C}(\mathscr{H}), \subseteq, {}^\perp)$ is a complete orthomodular lattice [11, Proposition 4.5] and is called a Hilbert lattice. Here, for each $V \in \mathbf{C}(\mathscr{H})$, $V^\perp$ is defined as the orthogonal complement

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

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

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

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

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

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

The following theorem states that the orthomodularity characterizes Hilbert spaces among inner product spaces.

Theorem 2.3 (The Amemiya-Araki Theorem [13])**.** Let X be an inner product space. The triple $(\mathbf{C}(X), \subseteq, {}^\perp)$ is a complete orthomodular lattice if and only if X is a Hilbert space, where $\mathbf{C}(X)$ stands for the set of all subspaces of X satisfying $(X^\perp)^\perp = X$.

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 $\mathscr{H}$, and U be a one-dimensional subspace of $V + W$, then

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

but

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

Definition 2.5. A non-empty subset Q of P is called a sublattice of a lattice $(P, \preceq)$ if $p \wedge q, p \vee q \in Q$ for any $p, q \in Q$.

Let $\mathbf{Sub}(\mathscr{P})$ be the set of all sublattices of a lattice $\mathscr{P} = (P, \preceq)$, and $\langle X \rangle$ be the set

$$\bigcap\{Q \in \mathbf{Sub}(\mathscr{P}) \,:\, X \subseteq Q\}$$

for each non-empty set X. Then, $\langle X \rangle$ is the smallest sublattice of $\mathscr{P}$ containing X and is called the sublattice of $\mathscr{P}$ generated by X.

The next theorem tells us when the distributive law partially holds in a complete orthomodular lattice. p is said to commute with q, denoted pCq, if $p = (p \wedge q) \vee (p \wedge \neg q)$.

Theorem 2.6 (The Foulis-Holland Theorem [14, 15])**.** Let $(P, \preceq, \neg)$ be a (complete) orthomodular lattice. For any $p, q, r \in P$, pCq and pCr jointly imply that $(\langle\{p, q, r\}\rangle, \preceq)$ is distributive, where $\langle\{p, q, r\}\rangle$ is the sublattice of $(P, \preceq)$ generated by $\{p, q, r\}$.

3. Quantum Dynamic Algebra

In this section, we formulate a quantum dynamic algebra (QD-algebra), an algebra of DQL with the Kleene star operator. The QD-algebra specifies 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 infimum and supremum of an infinite set. Infinitary conjunction is used to characterize $\square(a^*, p)$ in Definition 3.2.

The most basic components (called atomic programs) of a quantum program are unitary operators on a given Hilbert space. In this paper, we do not specify unitary operators but instead, deal with them as mere symbols. Thus, no assumptions are imposed on atomic programs henceforth.

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 $\mathscr{L} = (P, \preceq, \neg)$, the set $\Pi_{\mathscr{L}}$ of all regular quantum programs is generated by the grammar

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

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

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. That is,

$$(p \wedge (q \vee r))? \neq ((p \wedge q) \vee (p \wedge r))?$$

in general.

$\Pi_{\mathscr{L}}$ includes various programs, but the if-then and while-do programs are particularly significant among them. These are defined by

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

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

which means that the right-hand side of $:=$ is abbreviated as the left-hand side of $:=$.

It is worth paying attention to a precondition and postcondition of programs to verify them, as Hoare Logic does. A regular quantum program $a \in \Pi_{\mathscr{L}}$ 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 partial correctness does not guarantee that the program halts, the correctness is called partial.

We introduce a function $\Box : \Pi_{\mathscr{L}} \times P \to P$ 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 $(P, \preceq, \neg, \Box)$ that consists of a complete orthomodular lattice $(P, \preceq, \neg)$ and function (scalar multiplication) $\Box$: $\Pi_{\mathscr{L}} \times P \to P$ satisfying the following conditions:

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

Note that $\Box(a^*, p)$ 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 $(\wp(S), \subseteq, {}^c, \Box)$ 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 $(\mathbf{C}(\mathscr{H}), \subseteq, {}^\perp, \Box)$ 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 [16], which is known as the implication in quantum logic. In fact, $\Box(V?, W)$ is the inverse image

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

of W under the projection $P_V : \mathscr{H} \to \mathscr{H}$ onto V [17]. Interpreting a quantum test as a projection is the key idea of DQL [1].

Another significant example of QD-algebra is a characteristic algebra. We define the algebra and prove that a characteristic algebra is a QD-algebra in Section 5.

Definition 3.3. Two regular quantum programs $a, b \in \Pi_{\mathscr{L}}$ are said to be inseparable, denoted $a \approx b$, if $\Box(a, p) = \Box(b, p)$ for any $p \in P$. A QD-algebra is said to be separable if $\approx$ is the identity relation. That is, $a \approx b$ implies $a = b$.

The separability of a QD-algebra $(P, \preceq, \neg, \Box)$ is required for $\Box(a, -) : P \to P$ to satisfy function extensionality. If not separable, it is possible that $\Box(a, p) = \Box(b, p)$ for any $p \in P$ but $\Box(a, -) \neq \Box(b, -)$.

Theorem 3.4. The following inseparability equations hold.

(1) $a; (b; c) \approx (a; b); c$.
(2) $a \cup (b \cup c) \approx (a \cup b) \cup c$.
(3) $a; \mathbf{skip} \approx \mathbf{skip}; a \approx a$.
(4) $a \cup \mathbf{abort} \approx \mathbf{abort} \cup a \approx a$.
(5) $a; (b \cup c) \approx (a; b) \cup (a; c)$.
(6) $(a \cup b); c \approx (a; c) \cup (b; c)$.
(7) $a \cup b \approx b \cup a$.
(8) $a; \mathbf{abort} \approx \mathbf{abort}; a \approx \mathbf{abort}$.
(9) $a \cup a \approx a$.
(10) $\mathbf{skip} \approx \vee?$.
(11) $\mathbf{abort} \approx \wedge?$.
(12) $p? \approx \mathbf{if}\ p\ \mathbf{then\ skip\ else\ abort}$.

Proof. Straightforward. □

It follows from the conditions (1)–(9) that $(\Pi_{\mathscr{L}}, \cup, ;)$ is an idempotent semiring with addition $\cup : \Pi_{\mathscr{L}} \to \Pi_{\mathscr{L}}$ and multiplication $; : \Pi_{\mathscr{L}} \to \Pi_{\mathscr{L}}$ if $(P, \preceq, \neg, \Box)$ is separable. Evidently, **abort** is the additive identity, and **skip** is the multiplicative identity of this semiring.

4. Quantum Dynamic Frame

So far, we have not mentioned the notion of states and the 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 (also called an orthogonality space [18]) is used for giving Kripke (or relational) semantics to orthologic (the smallest quantum logic) [19]. 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 $\mathscr{H}$ be a Hilbert space, $\mathbf{Pure}(\mathscr{H})$ be the set of all pure states (unit vectors) in $\mathscr{H}$, and $\perp$ be the orthogonality relation on $\mathscr{H}$. Then, $(\mathbf{Pure}(\mathscr{H}), \perp)$ is an orthoframe, and is called a Hilbert frame. Note that $(\mathscr{H}, \perp)$ 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 $\mathscr{H}$.

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 definition.

The notion of a closed subspace is also generalized by using the above generalization of an orthogonal complement. Recall that $V \subseteq \mathscr{H}$ 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 $a \in \Pi_{\mathscr{L}}$ 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. For this reason, we extend an orthoframe by adding relations for programs.

Definition 4.3. A quantum dynamic frame (QD-frame) is a triple $(S, R, \mathscr{R})$ that consists of an orthoframe (S, R) and family $\mathscr{R} := \{R_a\}_{a \in \Pi_{\mathscr{L}}}$ 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 $s \in q$.

The above condition of $R_{p?}$ is borrowed from [20].

Example 4.2 (Hilbert QD-frame). Let $\{U_\pi\}_{\pi \in \Pi_0}$ be a family of unitary operators (quantum gates) on $\mathscr{H}$. The graph $G(U_\pi)$ of U_π is defined by

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

Then, for any Hilbert frame $(\mathbf{Pure}(\mathscr{H}), \perp)$, the QD-frame $(\mathbf{Pure}(\mathscr{H}), \perp, \mathscr{R})$, 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 $(S, R, \mathscr{R})$ 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 $t\cancel{R}u$ jointly imply that $uR_{p?}v$ and $s\cancel{R}v$ for some $v \in S$.
- A QD-frame $(S, R, \mathscr{R})$ 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 $s\cancel{R}u$ and for any $v \in S$, $u\cancel{R}v$ implies $vR_\pi t$.

The self-adjointness of a frame is also defined in [21] and [20] for different kinds of frames. The self-adjointness of a quantum transition frame is defined in [21], and that of a DO-frame is defined in [20].

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 $C(\mathscr{F})$ of an orthoframe $\mathscr{F} = (S, R)$ is a triple $(P_{\mathscr{F}}, \subseteq, \neg_R)$ that consists of the set $P_{\mathscr{F}}$ of all orthoclosed sets in $\mathscr{F}$, set inclusion relation $\subseteq$ on $P_{\mathscr{F}}$, and function $\neg_R : P_{\mathscr{F}} \to P_{\mathscr{F}}$ 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 $p \in P_{\mathscr{F}}$. In other words, $\neg_R p \in P_{\mathscr{F}}$ if $p \in P_{\mathscr{F}}$. This guarantees that $\neg_R : P_{\mathscr{F}} \to P_{\mathscr{F}}$ is well-defined.

Lemma 5.2. $P_{\mathscr{F}}$ is a topped intersection structure on S:

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

Proof. (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 can assume $s \notin p$, and thus $s \notin \neg_R\neg_R p$. In other words, $s\not R t$ for some $t \in \neg_R p$. Hence, $s\not R t$ 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 say that $s\not R t$ and $t \in \neg_R(p \cap q)$. However, the supposition $s \in \neg_R\neg_R(p \cap q)$ means that sRu for any $u \in \neg_R(p \cap q)$, which leads to a contradiction.
The $\supseteq$-part is proved as follows:

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

(2) It suffices to show that $\neg_R\neg_R S = S$. It follows from (i) $S^\perp = \emptyset$ and (ii) $\emptyset^\perp = S$. (i) follows because no $s \in S$ satisfies that sRt for any $t \in S$. If there would be such s, then sRs but R is irreflexive by definition, a contradiction. (ii) is immediate.

$\square$

In general, a topped intersection structure ordered by inclusion is a complete lattice [22, Corollary 2.32]. Thus, the following corollary is obtained.

Corollary 5.3. $(P_{\mathscr{F}}, \subseteq)$ is a complete lattice, where the infimum and supremum of $\Gamma \subseteq P_{\mathscr{F}}$ in $(P_{\mathscr{F}}, \subseteq)$ are $\bigcap \Gamma$ and the smallest orthoclosed set $\biguplus \Gamma$ containing $\bigcup \Gamma$, respectively.

Symbolically,

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

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

Theorem 5.4. $C(\mathscr{F}) = (P_{\mathscr{F}}, \subseteq, \neg_R)$ is a complete ortholattice.

Proof. By Corollary 5.3, $(P_{\mathscr{F}}, \subseteq)$ is a complete lattice. The conditions (1)–(3) of an ortholattice lattice (Definition 2.2) 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 $p \in P_{\mathscr{F}}$.
(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 $\neg_R q \subseteq \neg_R p$.

$\square$

The notion of characteristic algebra of an orthoframe is extended to that of an orthostable self-adjoint QD-frame. Because $C(\mathscr{F})$ is a complete ortholattice by Theorem 5.4, $\Pi_{C(\mathscr{F})}$ is well-defined.

Definition 5.5. Let $\mathscr{F} = (S, R)$ be an orthoframe. A characteristic algebra $C(\mathscr{F}_{\mathscr{R}})$ of an orthostable self-adjoint QD-frame $\mathscr{F}_{\mathscr{R}} = (S, R, \mathscr{R})$ is a quadruple $(P_{\mathscr{F}}, \subseteq, \neg_R, \Box_{\mathscr{R}})$ that consists of the set $P_{\mathscr{F}}$ of all orthoclosed sets in $\mathscr{F}$, set inclusion relation $\subseteq$ on $P_{\mathscr{F}}$, and functions $\neg_R : P_{\mathscr{F}} \to P_{\mathscr{F}}$ and $\Box_{\mathscr{R}} : \Pi_{C(\mathscr{F})} \times P_{\mathscr{F}} \to P_{\mathscr{F}}$ 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) $\Box_{\mathscr{R}}(a, p) = \{s \in S : t \in p \text{ for any } t \in S \text{ satisfying } sR_a t\}$.

It is not obvious that there exist $\Box_{\mathscr{R}}(a, p)$ in $P_{\mathscr{F}}$ for any $p \in P_{\mathscr{F}}$ and $a \in \Pi_{\mathscr{L}}$. Before proving this, we show some lemmas.

Lemma 5.6.

(1) $\Box_{\mathscr{R}}(\mathbf{skip}, p) = p$.

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

Proof. (1) Proof of $\Box_{\mathscr{R}}(\mathbf{skip}, p) = p$.

$$\begin{aligned}\Box_{\mathscr{R}}(\mathbf{skip}, p) &= \{s \in S : t \in p \text{ for any } t \in S \text{ satisfying } sR_{\mathbf{skip}}t\}\\ &= \{s \in S : s \in p \text{ for any } s \in S\} = p.\end{aligned}$$

(2) Proof of $\Box_{\mathscr{R}}(\mathbf{abort}, p) = S$.

$$\begin{aligned}\Box_{\mathscr{R}}(\mathbf{abort}, p) &= \{s \in S : t \in p \text{ for any } t \in S \text{ satisfying } sR_{\mathbf{abort}}t\}\\ &= S.\end{aligned}$$

(3) Proof of $\Box_{\mathscr{R}}(a;b,p) = \Box_{\mathscr{R}}(a, \Box_{\mathscr{R}}(b,p))$.

$$\begin{aligned}\Box_{\mathscr{R}}(a;b,p) &= \{s \in S : \forall t \in S(\exists u \in S(sR_a u \text{ and } uR_b t) \Rightarrow t \in p)\}\\ &= \{s \in S : \forall t \in S(\forall u \in S \text{ not } (sR_a u \text{ and } uR_b t) \text{ or } t \in p)\}\\ &= \{s \in S : \forall t \in S, \forall u \in S(\text{not } (sR_a u \text{ and } uR_b t) \text{ or } t \in p)\}\\ &= \{s \in S : \forall u \in S, \forall t \in S(\text{not } (sR_a u \text{ and } uR_b t) \text{ or } t \in p)\}\\ &= \{s \in S : \forall u \in S, \forall t \in S(\text{not } sR_a u \text{ or not } uR_b t \text{ or } t \in p)\}\\ &= \{s \in S : \forall u \in S(\text{not } sR_a u \text{ or } \forall t \in S(\text{not } uR_b t \text{ or } t \in p))\}\\ &= \{s \in S : \forall u \in S(sR_a u \Rightarrow \forall t \in S(uR_b t \Rightarrow t \in p))\}\\ &= \{s \in S : \forall u \in S(sR_a u \Rightarrow u \in \Box_{\mathscr{R}}(b,p))\}\\ &= \Box_{\mathscr{R}}(a, \Box_{\mathscr{R}}(b,p)).\end{aligned}$$

(4) Proof of $\Box_{\mathscr{R}}(a \cup b, p) = \Box_{\mathscr{R}}(a,p) \cap \Box_{\mathscr{R}}(b,p)$.

$$\begin{aligned}\Box_{\mathscr{R}}(a \cup b, p) &= \{s \in S : \forall t \in S(s(R_a \cup R_b)t \Rightarrow t \in p)\}\\ &= \{s \in S : \forall t \in S(sR_a t \text{ or } sR_b t \Rightarrow t \in p)\}\\ &= \{s \in S : \forall t \in S((sR_a t \Rightarrow t \in p) \text{ and } (sR_b t \Rightarrow t \in p))\}\\ &= \{s \in S : \forall t \in S(sR_a t \Rightarrow t \in p) \text{ and } \forall t \in S(sR_b t \Rightarrow t \in p)\}\\ &= \Box_{\mathscr{R}}(a,p) \cap \Box_{\mathscr{R}}(b,p).\end{aligned}$$

(5) Proof of $\Box_{\mathscr{R}}(a^*, p) = \bigcap\{\Box_{\mathscr{R}}(a^i, p) : i \geq 0\}$.

$$\begin{aligned}\Box_{\mathscr{R}}(a^*, p) &= \{s \in S : \forall t \in S(s(\textstyle\bigcup_{i\geq 0} R_a^i)t \Rightarrow t \in p)\}\\ &= \bigcap\{\Box_{\mathscr{R}}(a^i, p) : i \geq 0\}\end{aligned}$$

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

$\square$

The following proof of Lemma 5.7 is attributed to the work of [20] by changing the notations.

Lemma 5.7. If $(S, R, \mathscr{R})$ is self-adjoint, then

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

Proof. (1) If $s \in q$, then $s \in \neg_R p \cup q \subseteq \neg_R p \uplus q$. Thus, $s \in p$ and $s \in q$ jointly imply that $s \in p \cap (\neg_R p \uplus q)$. That is, $sR_{p?}s$.

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

$(\star)$ $t \in p \cap \neg_R(p \cap q)$

but $s\not{R}t$. Thus, $tR_{p?}t$ by $t \in p$ (Lemma 5.7 (1)). Because $tR_{p?}t$ 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 $sR_{p?}u$ and $t\not{R}u$ for some $u \in S$.

$$\begin{tikzcd} t \arrow[r, "R_{p?}"] \arrow[d, "\not{R}"'] & t \arrow[d, "\not{R}"] \\ \exists u & s \arrow[l, "R_{p?}"'] \end{tikzcd}$$

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 $sR_{p?}u$. Therefore, $u \notin q$ is obtained. It means that $sR_{p?}u$ and $u \notin q$ for some $u \in S$. Equivalently, $s \notin \Box_{\mathscr{R}}(p?, q)$.

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

$$\begin{tikzcd} s \arrow[r, "R_{p?}"] \arrow[d, "\not{R}"'] & t \arrow[d, "\not{R}"] \\ \exists v & u \arrow[l, "R_{p?}"'] \end{tikzcd}$$

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

$$s \notin \neg_R(p \cap (\neg_R p \uplus \neg_R q)) = \neg_R p \uplus (\neg_R\neg_R p \cap \neg_R\neg_R q) = \neg_R p \uplus (p \cap q).$$

$\Box$

Theorem 5.8. If $(S, R, \mathscr{R})$ is an orthostable self-adjoint QD-frame, then $P_{\mathscr{F}}$ is closed under $\Box_{\mathscr{R}}$: $p \in P_{\mathscr{F}}$ implies $\Box_{\mathscr{R}}(a, p) \in P_{\mathscr{F}}$ for each $a \in \Pi_{\mathscr{L}}$.

Proof. We prove by structural induction on $a \in \Pi_{\mathscr{L}}$.

(1) The base cases, namely $a = \textbf{skip}$, $a = \textbf{abort}$, or $a = \pi \in \Pi_0$. For $a = \textbf{skip}$, $\Box_{\mathscr{R}}(\textbf{skip}, p) = p \in P_{\mathscr{F}}$ by Lemma 5.6 (1). For $a = \textbf{abort}$, $\Box_{\mathscr{R}}(\textbf{abort}, p) = S \in P_{\mathscr{F}}$ by Lemma 5.6 (2) and Lemma 5.2 (2). For $a = \pi \in \Pi_0$, it suffices to show that

$$\neg_R\neg_R\Box_{\mathscr{R}}(\pi, p) = \Box_{\mathscr{R}}(\pi, p).$$

For the $\subseteq$-part, suppose that $s \in \neg_R\neg_R\Box_{\mathscr{R}}(\pi, p)$. Then,

$$\begin{aligned} s \in \neg_R\neg_R\Box_{\mathscr{R}}(\pi, p) &\Leftrightarrow \forall t \in S((\forall u \in \Box_{\mathscr{R}}(\pi, p),\ tRu) \Rightarrow sRt) \\ &\Leftrightarrow \forall t \in S((\forall u \in S((\forall v \in S(uR_\pi v \Rightarrow v \in p)) \Rightarrow tRu)) \Rightarrow sRt) \\ &\Leftrightarrow \forall t \in S(s\not R t \Rightarrow \exists u \in S(\forall v \in S(uR_\pi v \Rightarrow v \in p) \text{ and } t\not R u)) \qquad \text{(I)} \end{aligned}$$

Assume that $sR_\pi t$, and then we prove $t \in p$ to show $s \in \Box_{\mathscr{R}}(\pi, p)$. Because $(S, R, \mathscr{R})$ is orthostable, there exists $u' \in S$ such that

(II) $s\not R u'$ and

(III) $\forall v \in S(u'\not R v \Rightarrow vR_\pi t)$.

By (I) and (II), there exists $u \in S$ such that

(IV) $\forall v \in S(uR_\pi v \Rightarrow v \in p)$ and

(V) $u'\not R u$.

By (III) and (V), $uR_\pi t$. Therefore, $t \in p$ by (IV). We then prove the $\supseteq$-part. Because R is symmetric, $\not R$ is also symmetric. Thus, it suffices to show that

$$\forall t \in S(s\not R t \Rightarrow \exists u \in S(u \in \Box_{\mathscr{R}}(\pi, p) \text{ and } u\not R t)).$$

It is satisfied by choosing s as u if $s \in \Box_{\mathscr{R}}(\pi, p)$.

(2) The case of $a = b; c$. $\Box_{\mathscr{R}}(a; b, p) = \Box_{\mathscr{R}}(a, \Box_{\mathscr{R}}(b, p)) \in P_{\mathscr{F}}$ by Lemma 5.6 (3) and the induction hypothesis.

(3) The case of $a = b \cup c$. $\Box_{\mathscr{R}}(a \cup b, p) = \Box_{\mathscr{R}}(a, p) \cap \Box_{\mathscr{R}}(b, p) \in P_{\mathscr{F}}$ by Lemma 5.6 (4), Lemma 5.2 (1), and the induction hypothesis.

(4) The case of $a = b^*$. $\Box_{\mathscr{R}}(a^*, p) = \bigcap\{\Box_{\mathscr{R}}(a^i, p) : i \geq 0\} \in P_{\mathscr{F}}$ by Lemma 5.6 (5), Lemma 5.2 (1), and the induction hypothesis.

(5) The case of $a = p?$. $\Box_{\mathscr{R}}(p?, q) = \neg_R p \uplus (p \cap q) \in P_{\mathscr{F}}$ by Lemma 5.7 (2) and the definition of $\uplus$.

$\Box$

Theorem 5.9. The characteristic algebra $C(\mathscr{F}_{\mathscr{R}})$ of an orthostable self-adjoint QD-frame $\mathscr{F}_{\mathscr{R}} = (S, R, \mathscr{R})$ is a QD-algebra.

Proof. $(P_{\mathscr{F}}, \subseteq)$ is a complete ortholattice with the infimum $\bigcap\Gamma$ and supremum $\biguplus\Gamma$ for each $\Gamma \subseteq P_{\mathscr{F}}$ by Theorem 5.4.

Moreover, $(P_{\mathscr{F}}, \subseteq)$ is an orthomodular lattice. To show the orthomodular law, it suffices to show that $s \in p \cap \Box_{\mathscr{R}}(p?, q)$ implies $s \in q$. Because $s \in p$, it follows from Lemma 5.7 (1) that $sR_{p?}s$. Therefore, $s \in \Box_{\mathscr{R}}(p?, q)$ implies $s \in q$.

Finally, we prove that $C(\mathscr{F}_{\mathscr{R}})$ 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) $\Box_{\mathscr{R}}(a, S) = S$ and (4) $\Box_{\mathscr{R}}(a, p \cap q) = \Box_{\mathscr{R}}(a, p) \cap \Box_{\mathscr{R}}(a, q)$ have already been shown in Lemma 5.6.

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

(4) Proof of $\Box_{\mathscr{R}}(a, p \cap q) = \Box_{\mathscr{R}}(a, p) \cap \Box_{\mathscr{R}}(a, q)$.

$$\begin{aligned}\Box_{\mathscr{R}}(a, p \cap q) &= \{s \in S : \forall t \in S(sR_a t \Rightarrow t \in p \cap q)\}\\ &= \{s \in S : \forall t \in S(sR_a t \Rightarrow t \in p \text{ and } t \in q)\}\\ &= \{s \in S : \forall t \in S((sR_a t \Rightarrow t \in p) \text{ and } (sR_a t \Rightarrow t \in q))\}\\ &= \{s \in S : \forall t \in S(sR_a t \Rightarrow t \in p) \text{ and } \forall t \in S(sR_a t \Rightarrow t \in q)\}\\ &= \Box_{\mathscr{R}}(a, p) \cap \Box_{\mathscr{R}}(a, q).\end{aligned}$$

□

6. Conclusion

In this paper, 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 (Theorem 5.9).

The contribution of this paper is to give the 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.

Acknowledgments

The author would like to thank Prof. Kazuhiro Ogata for helpful feedback on this manuscript. This work was supported by Grant-in-Aid for JSPS Research Fellow Grant Number 22J23575.

References

[1] A. Baltag, S. Smets, Quantum logic as a dynamic logic, Synthese 179 (2011) 285–306.

[2] A. Baltag, S. Smets, LQP: the dynamic logic of quantum information, Mathematical structures in computer science 16 (2006) 491–525.

[3] A. Baltag, J. Bergfeld, K. Kishida, J. Sack, S. Smets, S. Zhong, PLQP & company: decidable logics for quantum algorithms, International Journal of Theoretical Physics 53 (2014) 3628–3647.

[4] J. M. Bergfeld, J. Sack, Deriving the correctness of quantum protocols in the probabilistic logic for quantum programs, Soft Computing 21 (2017) 1421–1441.

[5] A. Baltag, S. Smets, Reasoning about quantum information: An overview of quantum dynamic logic, Applied Sciences 12 (2022) 4458.

[6] G. Birkhoff, J. von Neumann, The logic of quantum mechanics, Annals of mathematics 57 (1936) 823–843.

[7] D. Harel, D. Kozen, J. Tiuryn, Dynamic Logic, MIT Press, 2000.
[8] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, J. Watrous, One-dimensional quantum walks, in: Proceedings of the thirty-third annual ACM symposium on Theory of computing, 2001, pp. 37–49.
[9] M. Hirvensalo, Quantum automata theory–a review, Algebraic Foundations in Computer Science (2011) 146–167.
[10] V. Pratt, Dynamic algebras: Examples, constructions, applications, Studia Logica 50 (1991) 571–605.
[11] M. Rédei, Quantum logic in algebraic approach, volume 91 of *Fundamental Theories of Physics*, Springer, 1998.
[12] M. L. D. Chiara, R. Giuntini, Quantum logics, in: Handbook of Philosophical Logic, volume 6, 2nd ed., Kluwer Academic Publishers, 2002, pp. 129–228.
[13] I. Amemiya, H. Araki, A remark on piron's paper, Publications of the Research Institute for Mathematical Sciences 2 (1966) 423–427.
[14] D. J. Foulis, A note on orthomodular lattices, Portugaliae mathematica 21 (1962) 65–72.
[15] S. S. Holland, A radon-nikodym theorem in dimension lattices, Transactions of the American Mathematical Society 108 (1963) 66–87.
[16] L. Herman, E. L. Marsden, R. Piziak, Implication connectives in orthomodular lattices, Notre Dame Journal of Formal Logic 16 (1975) 305–328.
[17] G. M. Hardegree, The conditional in quantum logic, Synthese 29 (1974) 63–80.
[18] D. J. Foulis, C. H. Randall, Lexicographic orthogonality, Journal of Combinatorial Theory, Series A 11 (1971) 157–162.
[19] R. I. Goldblatt, Semantic analysis of orthologic, Journal of Philosophical Logic 3 (1974) 19–35.
[20] T. Kawano, Advanced Kripke frame for quantum logic, in: International Workshop on Logic, Language, Information, and Computation, 2018, pp. 237–249.
[21] A. Baltag, S. Smets, Complete axiomatizations for quantum actions, International Journal of Theoretical Physics 44 (2005) 2267–2282.
[22] B. A. Davey, H. A. Priestley, Introduction to lattices and order, 2nd ed., Cambridge university press, 2002.