氏　　　　　　　名	高木翼
学 位 の 種 類	博士（情報科学）
学 位 記 番 号	博情第 508 号
学位授与年月日	令和 5 年 9 月 22 日
論 文 題 目	Quantum Dynamic Algebra: From Orthomodular Lattice to Algebra of Quantum Programs
論 文 審 査 委 員	緒方　和博　北陸先端科学技術大学院大学　教授
	平石　邦彦　北陸先端科学技術大学院大学　教授
	廣川　　直　北陸先端科学技術大学院大学　准教授
	冨田　　尭　北陸先端科学技術大学院大学　准教授
	東条　　敏　亜細亜大学　教授
	鹿島　　亮　東京工業大学　准教授

論文の内容の要旨

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 conjunction 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 J¥'{o}nsson--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

論文審査の結果の要旨

量子力学の論理としてフォンノイマンとバーコフが 1936 年に量子論理を提唱した。その後半世紀の時を経て、量子力学の原理に基づく計算（量子計算）が発明され、現在に至るまで盛んに研究されている。特に、IBM や Google などの巨大 IT 企業は量子コンピュータの将来的な実用化（数十年後）を目指し、量子コンピュータのハードウェアの実現に向け切磋琢磨している。量子コンピュータが実用化されるとその上で動作する量子プログラムの正しさを担保するための形式検証も重要になる。量子コンピュータは従来のコンピュータと動作原理が異なり、その上で動作する量子プログラムも従来のプログラムとは動作原理が異なる。このため、意図どおりに動作する量子プログラムの設計・実装は従来のプログラム以上に困難になり、量子プログラムの形式検証はより重要になることが予想されている。量子プログラムの形式検証を可能にするには形式検証の基盤となる論理学が重要となる。本博士論文では、量子論理の代数的意味論であるオーソモジュラー束を量子計算の観点を取り入れた量子プログラムの代数（量子動的代数）に拡張することで、量子論理を現代的な論理として生まれ変わらせた。さらに、本博士論文で初めて提案された量子動的代数は量子プログラムの形式検証の基盤として有効であることが具体的な量子プログラム検証への応用によって確かめられた。

量子動的代数はオーソモジュラー束、正規プログラム代数、そして様相代数から構成される。古典的な動的代数と量子動的代数は原子プログラムとテストの解釈において異なる。前者では原子プログラムの解釈に制限はないが、後者では原子プログラムは必ず量子ゲート（ユニタリ作用素）として解釈される。また、前者のテスト前後で状態は変化しないが、後者ではテストが射影作用素で表現される量子測定として解釈されるため、テストの前後で状態が変化しうる。量子動的代数は量子プログラム検証の代数的基盤を与える。本研究では、ホーア論理の推論規則に現れる全ての連言を新たな連言（佐々木連言）に置き換えることで、それらの推論規則が量子動的代数上で妥当であることを証明している。これは、適切な論理結合子を選びさえすればホーア論理の手法は量子プログラムの文脈でも同様に機能することを意味している。また、本研究では実際にホーア論理と同様の戦略で具体的な量子プログラムの形式検証を行っている。本研究でのもう一つの主要な成果はスター自由な量子動的代数に対するストーン型表現定理を証明した点である。ストーン型表現定理はブール代数、ハイティング代数、様相代数などの主要な代数に対して証明されており、それらの代数が望ましい性質を満たしていることを示している。本研究により、スター自由な量子動的代数も望ましい性質を満たすことが示されている。ここで「望ましい性質」とは代数と状態遷移系間の双対性のことを指し、この双対性により代数と状態遷移系が強力に結び付けられる。

本研究では、数十年後の実用化が期待される量子コンピュータ上で動作する量子プログラムの形式検証の基礎研究の重要な一歩が達成された。学術的に有用なだけでなく量子プログラムの形式検証という実用化にも道を開く研究である。十二分に博士（情報科学）に値する研究成果である。