UNIVERSITEIT VAN AMSTERDAM

Quantum Logics for Expressing and Proving the Correctness of Quantum Programs
J.M. Bergfeld

Abstract

In the first half of the twentieth century physicists discovered that elementary particles do not obey the classical Newtonian laws, instead obeying different laws. These laws are now known as the laws of quantum mechanics. Quantum mechanics has a tremendous influence on information theory and computer science. Incorporating quantum mechanics into information theory has led to new communication protocols that achieve goals deemed to be impossible by using classical computational techniques. Quantum mechanics also offers great opportunities for computer science: several alogrithms incorporating quantum mechanical techniques have been proven to be proven faster than any classical algorithm.

Similar as for classical computing, logic plays a fundamental role in the theory of quantum computing. The role of logic becomes central when we look at the design of quantum programs, especially when we look at their specification and verification. This thesis is positioned at the interface between quantum logic and quantum computation and contributes to the field in the following four themes.

Relating algebraic and spatial quantum structures. In Chapter **??** we study the duality of two different quantum structures, *Píron lattices* and *quantum dynamic frames*, which both are abstractions of Hilbert spaces, a standard tool for representing quantum systems. Both structures emphasize different properties of a quantum system and relating them shows how these different properties are connected.

Píron lattices provide an algebraic perspective on Hilbert spaces and focus on *testable properties* of a quantum physical system. A Píron lattice is such a lattice with the appropriate constraints for it to capture the abstract structure of a generalized Hilbert space, which is not exactly, but quite close to a normal Hilbert space. A Píron lattice that satisfies "Mayet's condition" captures the structure of an infinite dimensional Hilbert space over the complex numbers, reals, or quaternions. Quantum dynamic frames are a type of labelled transition

systems and provide a *dynamic* perspective on quantum systems.

To provide a full categorical structure for both Píron lattices and quantum dynamic frames, we consider two types of morphisms for each of the frames and the lattices. One type is that defined by Moore for two weaker structures that do not capture superposition, an important property of quantum theory: state spaces (symmetric anti-reflexive frames that separate points) and property lattices (complete atomistic orthocomplemented lattices). We also define stronger types of morphisms for both the Píron lattices and quantum dynamic frames. Both Píron lattice morphisms act directly on properties, while both quantum dynamic frame morphisms act directly on states.

Our duality result in Chapter **??** shows that quantum dynamic frames and Píron lattices form categories that are essentially the same (except for the direction of morphisms). We also show that this relation can be restricted to the objects satisfying Mayet's condition. As Píron lattices satisfying Mayet's condition have already been shown to be equivalent to Hilbert spaces, this result clarifies the close relationship that quantum dynamic frames have with Hilbert spaces. The structures of both quantum dynamic frames and Píron lattices are each a focal point of quantum logic, and hence our duality adds a new perspective to the formal relation between these different quantum structures.

Designing hybrid and probabilistic quantum logics (QHL and PLQP). We design two new logical systems: *Quantum Hybrid Logic (QHL)* and *Probabistic Logic for Quantum Programs (PLQP).*

In Chapter **??** we introduce a quantum hybrid logic (QHL), which means that next to the "standard modal operators" of negation ($\neg$), intersection ($\wedge$) and non-orthogonality ($\Box$), we add a special set of proposition letters called nominals, which refer to singleton states or atoms. The syntax of this logic is in fact equivalent to standard hybrid logic (with down arrow), but the standard deductive system is extended with four new axioms that are used to capture the properties of a quantum Kripke model which have been introduced by Zhong, with one new condition, which states the model has to have finite dimension. The axiom for this extra condition also shows QHL can express the concept of a basis.

We show the language can express standard quantum properties like orthocomplement and quantum join. As quantum Kripke models are equivalent to quantum dynamic frames, one could consider this logic to be an extension of the logic for quantum actions, introduced by Alexandru Baltag and Sonja Smets. Indeed, in Chapter **??** we show that all operators of the logic for quantum actions are in fact expressible in this quantum hybrid logic

The new logical system that we introduce for quantum reasoning in Chapter **??** and Chapter **??** is based on combining already existing formalisms of quantum logic, modal logic and probability logic. This gives us a Probabilistic Logic of Quantum Programs (PLQP), that extends a version of the older Logic

of Quantum Program (LQP). The language contains *dynamic modalities* $[\pi]$ (for quantum programs π) as well as "epistemic" modalities K_I (capturing the information that is 'known' to subsystem I, i.e. it is carried by the local state of subsystem I). In addition to the dynamic and epistemic modalities, the logic PLQP presented in Chapter **??** and Chapter **??** is endowed with a *probabilistic modality*, capturing the probability that a given test (of a quantum-testable property) will succeed. This is a novel feature, that greatly enhances the expressivity of the logic, allowing us to use it for the verification of probabilistic quantum algorithms.

In Chapter **??** we express the BB84 protocol and the quantum leader election protocol. In Chapter **??** we express the correctness of the Grover's search algorithm.

Axiomatising quantum logics (QHL and PLQP). In Chapter **??**, we provide a soundness and a completeness result for the quantum hybrid logic discussed above with respect to quantum Kripke frames of dimension at most n. As the language is very similar to standard hybrid logic, this result builds on a completeness result for a large class of hybrid logics. We show that part of our quantum hybrid logic falls inside this class for which the completeness result applies, while another part of our logic needs additional work to prove completeness. We show that three of the four new axioms define a frame property. That is, a frame has a certain property if and only if it validates the corresponding axiom.

Chapter **??** lays a foundation for an axiomatization of the probabilistic logic for quantum programs (PLQP) discussed above. The proof system introduced is shown to be sound. We also show a long list of basic and less basic properties of quantum theory concerning orthocomplement, quantum join and orthogonal bases. We use the deductive system and the list of basic properties to prove the properties of a Quantum Leader Election protocol and the BB84 quantum key distribution protocol. These two protocols are just examples of what our system can prove, and we are sure there are many others. But our logic also lays a foundation for the further development in axiomatizing logics for quantum systems, particularly those that involve probability.

Decidability for a class of Hilbert space based quantum logics. In the last part of this thesis we show that a class of Hilbert space based quantum logics, which includes the Probabilistic Logic for Quantum Programs, is *decidable*. To prove that a logical system is decidable essentially means that there exists an effective procedure to answer the question whether a formula is valid (or satisfiable) or not.

We give a general method for showing the decidability for a whole variety of quantum logics, including in particular the logic considered in Chapter **??**. The idea behind our method comes from the work of Dunn et. al. who translated stan-

dard quantum logic over finite-dimensional spaces into (the equational fragment of) the first-order theory of real numbers, which is known to be decidable due to Tarski's famous theorem. We extend this method to cover a wider range of quantum logics, by showing an inductive way to check if a language can be effectively translated. Basically, if each atomic sentence can be effectively translated to a defining first-order formula and each n-ary operator preserves this translatability, then the language is decidable. The method is applied to the language PLQP, which is therefore shown to be decidable.