THE UNIVERSITY OF
WARWICK

Original citation:
Papanikolaou, N. K. (2005) Reasoning formally about quantum systems : an overview. University of Warwick. Department of Computer Science. (Department of Computer Science Research Report). CS-RR-416

Permanent WRAP url:
http://wrap.warwick.ac.uk/61398

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

A note on versions:
The version presented in WRAP is the published version or, version of record, and may be cited as it appears here.For more information, please contact the WRAP Team at: publications@warwick.ac.uk

http://wrap.warwick.ac.uk/

Reasoning Formally about Quantum Systems: An Overview

Nick Papanikolaou
Department of Computer Science
University of Warwick
http://www.warwick.ac.uk/go/nikos

July 13, 2005

Abstract

This article is intended as an introduction to the subject of quantum logic, and as a brief survey of the relevant literature. Also discussed here are logics for specification and analysis of quantum information systems, in particular, recent work by P. Mateus and A. Sernadas, and also by R. van der Meyden and M. Patra. Overall, our objective is to provide a high-level presentation of the logical aspects of quantum theory. Mateus' and Sernadas' EQPL logic is illustrated with a small example, namely the state of an entangled pair of qubits. The "KT" logic of van der Meyden and Patra is demonstrated briefly in the context of the B92 protocol for quantum key distribution.

1 Introduction

Quantum theory is widely accepted as the most successful theory of natural science. Its precepts challenge our fundamental understanding of the universe, and are often in direct conflict with what our intuition leads us to believe. The implications of quantum theory for information processing are very hard to ignore; indeed, to harness the potential of the quantum world is to enable extremely powerful computational techniques, as well as novel means of data communication.

With the emergence of practical quantum cryptographic systems and related products, there is already a growing need for means of designing and analysing systems involving quantum–mechanical components. For instance, quantum cryptographic protocols involve a sequence of steps for manipulating given quantum states, and their implementation presupposes the existence of usable quantum channels, with properties not found in conventional transmission media; how is one to model protocols such as these and the properties they exploit? How is one to demonstrate that a quantum–mechanical component operates in accordance with its specification, or that it guarantees (where applicable) a particular level of security?

Computer scientists have already developed a number of formalisms allowing one to reason about quantum–mechanical behaviour in general as well as about systems consisting of both conventional and quantum–mechanical elements. This includes quantum programming

languages (intended primarily for the description of quantum algorithms; see the recent survey [15] by S. Gay), quantum process algebras (capable of describing quantum computational processes in general, as well as quantum communication schemes), and logics for quantum information systems.

The subject of 'quantum logic' is an interesting line of work, reserved till now for physicists and mathematicians who are interested in the algebraic structures which arise in the mathematics of quantum theory. While it is a very specialised subject, quantum logic can provide insights into the workings of nature, and it has already been put to use by S. Abramsky and B. Coecke to analyse problems in quantum information [1].

This inquiry will be centred around the logical aspects of quantum theory. The discussion will remain at a high level, focusing on philosophical problems and the syntax of certain logics. First we will describe the principles of quantum theory; we will pay attention particularly to the issue of quantum measurement, which lies at the heart of Birkhoff's and von Neumann's 'quantum logic,' to which we will then turn our attention. This will be followed by a summary of recent work by R. van der Meyden and M. Patra [36, 37, 28, 27], and by P. Mateus and A. Sernadas [20, 19], on logics for quantum information systems.

We have chosen to distinguish clearly between quantum logic and 'logics for quantum information systems;' the former is more of a semantic approach to logic, with an emphasis on mathematical structures, while the latter refers to logical calculi specifically targeted at applications in quantum computing and quantum information theory. Quantum logic is usually studied at a very abstract level, and applications or examples of it are quite superficial; our presentation of quantum logic here is also abstract, and focuses on its semantic connection with classical propositional logic. For the two other logics, specific examples have been included.

Acknowledgements. I wish to thank my supervisor, R. Nagarajan, for his guidance and particularly for his patience with my independent writing efforts. I also thank much–respected collaborator, S. Gay, and also my advisor, M. Jurdziński, for their counsel and encouragement.

Disclaimer. I have received input on the material presented here from a number of people, but any errors or omissions are entirely my own. I welcome any feedback; do feel free to contact me at `nikos@dcs.warwick.ac.uk`.

2 Fundamentals of Quantum Theory

A fundamental tenet of quantum theory is the belief that, at the lowest level, the physical world is discrete, or *quantised.* This claim is corroborated by several experiments, described in all the standard texts on the subject (see e.g. the books by Bohm [9], Cohen–Tannoudji *et al.* [13], Peres [29] and Shankar [34]). More interestingly, quantum theory stipulates that there is a limit to the amount of knowledge we can gain about a particular quantum system; this is known as the *uncertainty principle.* But the greatest departure of quantum theory from the notions of classical physics is its use of probability laws and, hence, the abandonment of causality. Quantum theory thus presents us with several philosophical problems, and this directly affects any attempt to arrive at its formulation in the language of logic. We shall soon enter into a discussion of the details, but first a brief introduction to the key aspects the theory is in order.

By the term *physical system* is understood an identifiable, isolated portion of the physical universe; such a system is characterised by its *state,* which is the result of experimental procedures used to isolate and prepare it. An *observable* is a quantity associated with the state of a system, which can be directly measured. These are our basic terms of reference.

2.1 The Hilbert Space Formalism

Quantum theory finds mathematical expression in the so–called Hilbert space formalism, which coordinates to a physical system a *state space,* namely, a complex–valued vector space $\mathcal{H}_n$ equipped with an inner product. The quantum state of a system is described by a vector in this space; such a vector is normally written in the form $|v\rangle$. Any physical system will have several degrees of freedom, this being one of its intrinsic properties. The dimension, n, of the state space associated with the system reflects the number of degrees of freedom of the system in question. Furthermore, every vector in this space is realisable as an actual physical state.

The concept of quantum *state* is very subtle and controversial; the traditional view is that a quantum state represents all that can be known about a system. This view is known to lead to some contradictions, so many prefer to identify the concept of state not with an individual element of reality, but with a description of ensembles of systems. If this view is taken, then the most general form of quantum state is described by a statistical operator, known as the *density operator.* We will not adopt this view here; rather, we will deal only with *pure* quantum states, for which the former view is satisfactory. The interested reader is referred to advanced texts, such as [6, 3], for more details.

The state space $\mathcal{H}_n$ of a given physical system may or may not be finite–dimensional. It is only the former case with which we will be concerned here.

Vectors in $\mathcal{H}_n$ can be added together, producing so–called *superposition states*. It is a fundamental postulate of quantum mechanics that, if $|v\rangle$ and $|w\rangle$ represent valid physical states in $\mathcal{H}_n$, then so does their superposition, i.e. the state $\alpha \cdot |v\rangle + \beta \cdot |w\rangle$ with α, β being scalars. This principle is put to great advantage in quantum computing, where it is used to generate complex physical states with no classical analogue.

Example. Consider the two–dimensional Hilbert space $\mathcal{H}_2$. A pair of mutually orthogonal, normalised vectors, such as $|0\rangle$ and $|1\rangle$, forms a basis of $\mathcal{H}_2$. Another basis of $\mathcal{H}_2$ is the pair of vectors

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The space $\mathcal{H}_2$ represents the state space, say, of a spin-$\frac{1}{2}$ particle (where $|0\rangle$ could denote the particle's "spin–down" state, and $|1\rangle$ its "spin–up" state), or of a polarised photon (where $|0\rangle$ would stand for a polarisation angle of 0° and 1 for a polarisation angle of 90°). A more general, possible state of such a system is given by a linear combination of the basis vectors, i.e. $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$, for some $\alpha, \beta \in \mathbb{C}$. Quantum mechanics requires that $|\alpha|^2 + |\beta|^2 = 1$. There is an infinity of such combinations and thus, a quantum system with a state space even as simple as this has infinitely more realisable states than its classical analogue. A quantum system whose state space is specifically $\mathcal{H}_2$ is known as a quantum bit or *qubit.* Therefore, while a classical bit can only take on a single value $b \in \{0, 1\}$ at any given time, a qubit can be in the basis states $|0\rangle$, $|1\rangle$, or any superposition thereof.

The dual space $\mathcal{H}_n^*$ of $\mathcal{H}_n$, consists of linear functionals $\langle w| : \mathcal{H}_n \mapsto \mathbb{C}$, where $\mathbb{C}$ is the field

of complex numbers. The *inner product* $\langle w|v\rangle$ induces an isomorphism between $\mathcal{H}_n^*$ and $\mathcal{H}_n$; in particular, the image $\langle v'| \in \mathcal{H}_n^*$ of a vector $|v\rangle \in \mathcal{H}_n$ is defined as a function f such that $f(|v\rangle)$ is the inner product of $|v'\rangle$ and $|v\rangle$.

A quantum system composed of multiple subsystems, whose state spaces $\mathcal{H}_k^{(1)}, \ldots, \mathcal{H}_m^{(N)}$ are known, has a state belonging to the *tensor product space,* written $\mathcal{H}^{\otimes n} = \mathcal{H}_k^{(1)} \otimes \cdots \otimes \mathcal{H}_m^{(N)}$. The definition of the tensor product is detailed elsewhere, e.g. [3, 13, 23, 32].

The state of a quantum system evolves over time, this evolution being governed by a *unitary transformation;* such a transformation is described by a linear operator U with $U^{-1} = U^\dagger$. The symbol $U^\dagger$ denotes the *adjoint* of operator U, defined as its conjugate-transpose: $U^\dagger = (U^*)^T$.

In order to obtain any information about the quantum state of a system, a measurement, or *observation,* must be performed. An observable is usually associated with an Hermitian operator, and the only possible results of measurement are given by the eigenvalues of this operator. An operator U is said to be *Hermitian* in a finite–dimensional space if it is self–adjoint, i.e. if $U = U^\dagger$. We will have more to say about the issue of measurement in the following section.

2.2 Quantum Measurement

Quantum theory makes of the measurement, or observation, of a quantum system an issue of great importance; according to the theory, the actual state of a particular quantum system cannot be determined experimentally, for there is an interaction between the system and the means of observation. Indeed, this interaction manifests itself as an irreversible disturbance to the state of the system.

This result makes it difficult to reason about the actual quantum state of a given physical system. One can only *prepare* a system in a known state, but any attempt to measure the state will directly affect it. Therefore, there is a fundamental limit to the amount of information one can expect to obtain about a given system. The best we can do is to predict, with particular probability, the outcome of a specific measurement. Quantum mechanics provides rules for calculating the probability distributions associated with the measurement of system observables.

Interestingly, there are pairs of observables that are mutually dependent in such a way that an accurate measurement of one precludes any reasonable amount of accuracy in the measurement of the other, so that it is impossible to properly measure both at the same time. The most typical example of this arises when one tries to measure the position and momentum of a particle simultaneously. It is not our object to expound further on this matter; the reader should consult one of the several good texts on quantum theory.

For our purposes, it will suffice to say a few words about *projective measurements.* An observable described by an Hermitian operator, say M, describes a projective measurement. When such a measurement is made on a quantum system, the vector corresponding to its state is projected onto a subspace of the state space. Furthermore, according to Nielsen and Chuang [23]:

> *... the possible outcomes of the measurement are the eigenvalues of M. Upon making an observation with M of the system in state $|w\rangle$, the probability of getting an eigenvalue m is given by $\langle w|P_m|w\rangle$ where P_m is the projector onto the eigenspace of M with eigenvalue m. When the outcome m occurs, the quantum state evolves*

to the state given by

$$\frac{P_m |w\rangle}{\sqrt{\langle w| P_m |w\rangle}}$$

Having established all the necessary background material, we are now ready to start our journey into the logical aspects of quantum theory, and to enter into a discussion of some of the logics which have been designed specifically for reasoning about quantum systems.

3 Quantum Logic

The term *quantum logic* is reserved for the study of the algebraic structures which arise in the mathematical formalism of quantum mechanics. It was G. Birkhoff and J. von Neumann who first pointed out that quantum–mechanical *propositions,* which are the simplest type of observable associated with a given system, altogether constitute an *orthocomplemented, quasi–modular lattice* [8, 6, 21]. This algebraic structure has formal similarities with Boolean algebra, which provides the semantics of classical propositional logic. In light of these similarities, Birkhoff and von Neumann suggested that the lattice of all propositions associated with a quantum system must provide the semantic foundation for a quantum–mechanical, propositional calculus of logic; it is this particular calculus which was christened 'quantum logic.' In the words of Beltrametti *et al.* [6]:

> *Roughly, the starting question is whether the propositions of a quantum system can be associated with, or can be interpreted as, sentences of a language (or propositional calculus) and which rules this language inherits from the ordered structure of propositions. In raising this question one has in mind the fact that when the physical system is classical its propositions form a Boolean algebra, and Boolean algebras are the algebraic models of the calculus of classical logic. Thus, the question above can also be phrased as follows: when a Boolean algebra is relaxed into an orthomodular nondistributive lattice, which logic is it the model of? "Quantum logic" is the name that designates the answer, but there are several views about the content of this name.*

The precise syntax and applicability of quantum logic has been debated for a very long time and is still an active area of research. The fact that there is currently no commonly agreed syntax for quantum propositions limits the applicability of quantum logic to specific problems. But one should remember that the emphasis in quantum logic is placed not on syntax, not on applications, but on semantics.

Let it be made clear at the outset that the subject of quantum logic is more usually treated as part of a programme to understand quantum theory in depth. We have the occasion to present this topic here, since it is likely to be of some wider interest.

3.1 Motivation for Quantum Logic

As we have seen in Section 2.2, the formalism of quantum mechanics provides us with a means of predicting the possible outcomes of a measurement on a quantum system. These predictions have an associated probability of materialising; if an actual measurement is made, only one of these predictions will turn out to be correct. A quantum–mechanical *proposition* is just such

a prediction; quantum logic is the logic of these propositions. Birkhoff and von Neumann [8] explain this as follows:

> *It is clear that an "observation" of a physical system $\mathcal{S}$ can be described generally as a writing down of the readings from various compatible measurements. Thus if the measurements are denoted by the symbols $\mu_1,\ldots,\mu_n$, then an observation of $\mathcal{S}$ amounts to specifying numbers $x_1,\ldots,x_n$ corresponding to the different μ_k.*
>
> *It follows that the most general form of a prediction concerning $\mathcal{S}$ is that the point $(x_1,\ldots,x_n)$ determined by actually measuring $\mu_1,\ldots,\mu_n$, will lie in a subset S of $(x_1,\ldots,x_n)$–space. Hence if we call the $(x_1,\ldots,x_n)$–spaces associated with $\mathcal{S}$, its "observation–spaces," we may call the subsets of the observation–spaces associated with any physical system $\mathcal{S}$, the "experimental propositions" concerning $\mathcal{S}$.*

Quantum logic allows us to reason about measurements by defining logical connectives for quantum–mechanical propositions. In terms of the Hilbert–space formalism, a quantum–mechanical proposition is simply an observable which admits two possible values (0 and 1).

The literature on the subject is generally concerned with the semantics of quantum logic (see e.g. [6, 8, 11, 21, 30, 35, 38, 12]). We will proceed to discuss the semantics of quantum logic after explaining the connection between propositional logic and the theory of lattices. Our treatment is basic, and we provide no proofs; mathematical rigour is not our priority in this article.

3.2 Boolean Algebra

In formal logic, a proposition is an assertion which has a definite truth value (either "true" or "false"). The calculus of propositional logic allows to relate propositions using connectives such as 'and', 'or' and 'not'. Each connective expresses a *logical operation;* for the connectives just mentioned, the operations are, respectively, *conjunction, disjunction* and *negation.* It was George Boole who realised that logical operations are amenable to an algebraic treatment, and that they obey similar laws to set–theoretic operations [17]. He extracted the algebraic laws for these operations and came up with what is now known as 'Boolean algebra.' Boolean algebra is thus the mathematical structure common to the algebra of sets and the algebra of propositions. The formal definition of a Boolean algebra is given below.

Definition 1 (from [17]) *A **Boolean algebra** $(B;\wedge,\vee,\neg,0,1)$ is a set B, together with operations on the set which satisfy certain laws. We will denote the operations by '$\wedge$', '$\vee$', and '$\neg$' and they will be called 'meet', 'join' and 'complement' respectively. There are two distinguished and distinct elements of B, denoted by 0 and 1 that are subject to the following laws.*

1. *Idempotence: $a\wedge a = a$, and $a\vee a = a$.*
2. *Complement laws: $a\vee\neg a = 1$, $a\wedge\neg a = 0$, and $\neg\neg a = a$.*
3. *Commutativity: $a\wedge b = b\wedge a$, and $a\vee b = b\vee a$.*
4. *Associativity: $a\wedge(b\wedge c) = (a\wedge b)\wedge c$, and $a\vee(b\vee c) = (a\vee b)\vee c$.*
5. *Distributivity: $a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c)$, and $a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c)$.*

6. *Property of 1:* $a \wedge 1 = a$.
7. *Property of 0:* $a \vee 0 = a$.
8. *De Morgan's laws:* $\neg(a \wedge b) = \neg a \vee \neg b$, *and* $\neg(a \vee b) = \neg a \wedge \neg b$.

If we were to identify the Boolean operations, meet, join and complement with the set–theoretic operations intersection '$\cap$', union '$\cap$' and complement '^{c}', we would find that the above definition just gives the laws of set theory, assuming B is the set of all subsets of a given set U. But the above definition also embodies the laws of propositional logic, which is evident if we identify B with the set of all equivalence classes of propositions [17].

A Boolean algebra is actually a special case of a more general algebraic structure, known as a *lattice*. In particular, a Boolean algebra is a *complemented distributive lattice,* defined as follows:

Definition 2 (from [17]) *A* ***complemented distributive lattice*** *is a partially ordered set* $(P, \leqslant)$ *that satisfies the following conditions:*

1. *Each pair of elements of P has a least upper bound, denoted* $a \vee b$, *and a greatest lower bound, denoted* $a \wedge b$.
2. $(P, \leqslant)$ *has a* top *value, denoted* 1, *and a* bottom *value, denoted* 0. *The top value is defined as the element* $c \in P$ *which satisfies* $c \geqslant a$ *for all* $a \in P$. *Similarly, the bottom value is the element* $b \in P$ *for which* $b \leqslant a$ *for all* $a \in P$.
3. *Distributivity holds in P, i.e. for any* $a, b, c \in P$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, *and* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
4. *Every element in P has a complement.*

Theorem 1 (from [17]) *Every complemented distributive lattice is a Boolean algebra under the operations of meet, join and complement and with the distinguished elements 0 and 1. Conversely, every Boolean algebra is a complemented distributive lattice under the partial order that is defined by*

$$a \leqslant b \text{ if and only if } a = a \wedge b.$$

The purpose of presenting these mathematical facts here is to demonstrate the connection between logic and set theory. In order to understand Birkhoff and von Neumann's work on quantum logic, one must be aware of the algebraic structure of classical propositional logic.

3.3 The Structure of Quantum–Mechanical Propositions

Birkhoff and von Neumann describe their motivation and main result as follows [8]:

> *The object of the present paper is to discover what logical structure one may hope to find in physical theories which, like quantum mechanics, do not conform to classical logic. Our main conclusion, based on admittedly heuristic arguments, is that one can reasonably expect to find a calculus of propositions which is formally indistinguishable from the calculus of linear subspaces with respect to set products, linear sums, and orthogonal complements—and resembles the usual calculus of propositions with respect to and, or and not.*

As mentioned earlier, a quantum–mechanical proposition corresponds to an observable with two possible values. As discussed in Section 2.1, an observable is described by a projection operator[1], or *projector*. Therefore, every proposition about a given quantum system with state space $\mathcal{H}$ has an associated projector. What is interesting is that the set of all projectors $\mathcal{P}(\mathcal{H})$ on $\mathcal{H}$ is actually a lattice. We will briefly list the characteristics of this structure here (see Beltrametti *et al.* [6] for details). First, the following definitions are in order.

Definition 3 (from [30]) *A lattice L is said to be **orthocomplemented** if it is provided with an orthocomplementation, that is to say, a mapping of L onto L which to each element $b \in L$ brings into correspondence an element denoted as $b' \in L$, such that:*

1. $\forall b \in L : (b')' = b$
2. $\forall b \in L : b \wedge b' = 0$, *and* $b \vee b' = 1$
3. $b < c \Rightarrow c' < b'$

Definition 4 (from [6]) *A lattice L is called σ–orthocomplete when it is orthocomplemented and there exists in L the join of every countable orthogonal subset of L. Furthermore, L is called **orthomodular** if, in addition to being σ–orthocomplete, it satisfies the condition: $\forall a, b \in B : a \leqslant b \Rightarrow b = a + (b - a)$.*

Definition 5 (from [6]) *A lattice L is **complete** if the meet and join of any subset of L exist.*

Definition 6 (from [6]) *Let L be a lattice. The elements $a, b, c \in L$ form a **distributive triple** if*

1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

with the other four equalities being obtained by cyclical permutation of a, b and c.

Definition 7 (from [6]) *A lattice L is **distributive** if every triple of elements in L is distributive.*

Theorem 2 (from [6]) *Any distributive lattice is orthomodular.*

As mentioned in [6], distributivity is a natural framework for describing classical mechanics, while orthomodularity is the corresponding framework for quantum mechanics.

The lattice $\mathcal{P}(\mathcal{H})$ of projectors on a state space $\mathcal{H}$ has the following characteristics:

- A projection operator corresponds to a closed subspace of $\mathcal{H}$, and $\mathcal{P}(\mathcal{H})$ is the set of all closed subspaces of $\mathcal{H}$.
- $\mathcal{P}(\mathcal{H})$ is partially ordered by set–theoretic inclusion (denoted $\subseteq$).
- $\mathcal{P}(\mathcal{H})$ is a complete lattice with a meet and a join.
- The greatest element of $\mathcal{P}(\mathcal{H})$ is the whole space $\mathcal{H}$, and the least element of $\mathcal{P}(\mathcal{H})$ is the set consisting only of the zero vector.
- $\mathcal{P}(\mathcal{H})$ is an orthocomplemented lattice.
- $\mathcal{P}(\mathcal{H})$ is orthomodular.

[1] Not *all* observables in quantum mechanics are represented by projection operators, but we have restricted our discussion to those which are (see Section 2.2).

- $\mathcal{P}(\mathcal{H})$ is nondistributive.
- $\mathcal{P}(\mathcal{H})$ is *atomic* and has the so–called *covering property.* It is also *separable.* For an explanation of these terms, see [6].
- $\mathcal{P}(\mathcal{H})$ is *modular* only if $\mathcal{H}$ is finite–dimensional. That is why $\mathcal{P}(\mathcal{H})$ is more generally referred to as *quasi–modular*. Note that there is a subtle difference between modularity and orthomodularity.

The discovery of the structure of $\mathcal{P}(\mathcal{H})$ is an important result, as one can reconstruct all the ingredients of the Hilbert–space formalism (states, transformations and observables) using only the properties of quantum–mechanical propositions. In [38], Wilce observes that:

> *From the single premise that the "experimental propositions" associated with a physical system are encoded by projections in the way indicated above, one can reconstruct the rest of the formal apparatus of quantum mechanics. The first step, of course, is Gleason's theorem, which tells us that probability measures on $\mathcal{P}(\mathcal{H})$ correspond to density operators. There remains to recover, e.g., the representation of "observables" by self-adjoint operators, and the dynamics (unitary evolution). The former can be recovered with the help of the Spectral theorem and the latter with the aid of a deep theorem of E. Wigner on the projective representation of groups. [...] The point to bear in mind is that, once the quantum-logical skeleton $\mathcal{P}(\mathcal{H})$ is in place, the remaining statistical and dynamical apparatus of quantum mechanics is essentially fixed. In this sense, then, quantum mechanics – or, at any rate, its mathematical framework – reduces to quantum logic and its attendant probability theory.*

In other words, quantum logic allows us to define the mathematical framework of quantum mechanics on a more abstract footing.

It is always interesting to find an underlying mathematical relationship between seemingly unrelated things; in the case of quantum logic, an investigation into the mathematical structure of quantum mechanics has revealed the possibility of greatly generalizing propositional logic. We have only attempted to scratch the surface of this vast and complicated subject here; however, we have included numerous references for the more advanced reader.

Bibliographic Notes. There are several good textbooks on quantum logic; of these we have selected and recommend the books by Piron [30], Beltrametti and Cassinelli [6], and Mittelstaedt [21]. Piron's book attempts to unify the mathematical framework of quantum mechanics with that of classical mechanics, and it uses the hidden–variables interpretation of quantum theory. In their book, Beltrametti and Cassinelli provide a comprehensive presentation of the subject, introducing first the Hilbert–space formalism and then dealing with the relevant algebraic stuctures in depth; they also describe how the whole formalism may be reconstructed using only the results of quantum logic. Mittelstaedt's book is quite readable, and is comparable to Piron's in terms of coverage. Survey articles of quantum logic include [11], by Dalla Chiara and Giuntini, also [35], by Svozil, and [38], by Wilce. The book [12] is a collection of articles on a particular variant, known as *operational* quantum logic. The philosopher Hans Reichenbach designed a simple, three–valued quantum logic which appeals to one's intuition about measurement [31]; his exposition of the philosophical aspects of quantum theory is very readable and informative.

4 Logics for Quantum Information Systems

The increased interest in quantum computation and quantum information in recent years has made quantum logic very relevant today. Ever since research in quantum logic was initiated by Birkhoff and von Neumann, physicists were constantly at odds over what its precise form should be. As we saw in the previous section, the emphasis was mostly put on the *semantics* of quantum logic — in particular, on the mathematical structures that underlie quantum theory. What is needed today is a means of reasoning formally about systems with quantum–mechanical components and procedures, namely, a specialized logic with a formal syntax for describing quantum algorithms, quantum protocols, and their properties. In order to fulfil this need, one must design a suitable logic using the top–down approach, rather than starting from low–level algebraic structures and their properties. In the words of [19]:

> *It is to be expected that the lattice approach to quantum logic will play a similar role to the one played by modal algebras in modal logic, by Heyting algebras in intuitionistic logic, by Boolean algebras in classical logic, etc. But, as in those cases, the algebraic approach is not the right source of inspiration for discovering the linguistic ingredients of the envisaged logic. For instance, modal algebras appeared much later than Kripke structures, well after the modal language was widely accepted.*

P. Mateus and A. Sernadas [20, 19], and also R. van der Meyden and M. Patra [36, 37, 28, 27], are among those who have taken up this challenge. Their approaches are fundamentally different to the one of Birkhoff and von Neumann; both pairs of authors have designed quantum logics which are extensions of probabilistic logic.

Mateus and Sernadas have used the *exogenous* approach to design a logic for reasoning about quantum systems. This means that they have kept intact the classical model of propositional logic as the basis for their logic and simply augmented it to account for the probabilism inherent in quantum mechanics; in particular, the semantics of their logic is such that the meaning of a quantum proposition is given by *a superposition of the meanings of classical propositions*. So, instead of building their logic atop the algebraic structures of quantum mechanics, Mateus and Sernadas have used models of propositional logic as their starting point. Their work is particularly inspired by the semantics of probabilistic logic, as given in [14, 24]. The name of the logic they have proposed is "Exogenous Quantum Propositional Logic" (EQPL). A more powerful version of the logic, which allows one to describe the dynamics of quantum systems, is "Dynamic Exogenous Quantum Propositional Logic" (DEQPL).

Van der Meyden and Patra have focused on adapting the probabilistic logic in [14] to quantum systems, and they have come up with a logic for knowledge and time in quantum systems [36], and a logic for probability in quantum systems [37]. We will only consider the former of the two logics [36] here.

4.1 Exogenous Quantum Propositional Logic (EQPL)

EQPL [20, 19] is designed to allow one to write assertions about quantum systems consisting of a finite number of qubits. The constructs of the logic allow one to reason about a wide range of systems, ranging from entangled pairs of qubits to whole quantum cryptographic protocols. EQPL only allows one to reason about quantum states and measurements; the extended version of the logic, DEQPL, can be used to write formulae which include quantum operators.

A quantum system is described in EQPL by a finite set of propositional constants, $P = \{\mathbf{p}_k \mid k \in \mathbb{N}\}$. Each propositional constant $\mathbf{p}_k$ corresponds to a single qubit in the system under consideration. We define a set V of so–called *classical valuations* on P. A classical valuation is just a function which attaches a truth value to a propositional constant, so $V = \{v \mid v : P \mapsto \{0,1\}\}$. Classical valuations give meaning to "classical formulae" which are used in EQPL. The formal syntax of classical formulae is given in BNF below.

$$\varphi ::= \mathbf{p}_k \mid (\neg\varphi) \mid (\varphi \Rightarrow \varphi) \qquad \text{(Classical formulae)}$$

In practice, of course, classical formulae in EQPL will also include other Boolean connectives, such as 'and' ($\wedge$), and 'or' ($\vee$). Classical formulae have their usual meaning from propositional logic.

The full language of EQPL includes general formulae, classical formulae, real terms and complex terms. The syntax of the full language is defined as follows:

$$\gamma ::= \varphi \mid (t \leqslant t) \mid ([S] \Diamond \overrightarrow{\psi : u}) \mid (\boxminus\gamma) \mid (\gamma \sqsupset \gamma) \qquad \text{(Formulae)}$$
$$t ::= r \mid (\textstyle\int \varphi) \mid (\int \varphi_2 \,|\, \varphi_1) \mid (t+t) \mid (t\,t) \mid \mathrm{Re}(u) \mid \mathrm{Im}(u) \mid \arg(u) \mid \|u\| \qquad \text{(Real terms)}$$
$$u ::= (t + \mathbf{i}t) \mid t\exp(\mathbf{i}t) \mid u \mid (u+u) \mid (u\,u) \qquad \text{(Complex terms)}$$

In the above, r denotes a real number, and $\mathbf{i} = \sqrt{-1}$.

The most important ingredients of the logic are (see [20, 19] for the formal definitions):

$([S] \Diamond \overrightarrow{\psi : u})$ Quantum modality; this is for making assertions about qubits.

$(\boxminus\gamma)$ Quantum "negation."

$(\gamma \sqsupset \gamma)$ Quantum "implication."

$(\int \varphi)$ gives the probability of getting an outcome for which φ holds, when a measurement is made.

$(\int \varphi_2 \,|\, \varphi_1)$ gives the probability of getting an outcome for which φ_2 holds, given that φ_1 holds, when we observe the quantum system.

A very simple example of the use of the logic is the following EQPL specification, which describes the state of a two–qubit system in the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

$$\left([\mathbf{p}_0, \mathbf{p}_1] \Diamond (\mathbf{p}_0 \wedge \mathbf{p}_1) : \frac{1}{\sqrt{2}},\ ((\neg\mathbf{p}_0) \wedge (\neg\mathbf{p}_1)) : \frac{1}{\sqrt{2}}\right)$$

In this specification, $\mathbf{p}_0$ and $\mathbf{p}_1$ are the propositional constants corresponding to the two qubits in the system in question. Obviously, this particular system is uninteresting, but it serves to illustrate EQPL's syntax. The specification entails the following formulae:

$(\int \mathbf{p}_0) = \frac{1}{2}$ i.e. "the probability that, *the outcome of measuring the first qubit is the truth value 1,* is $\frac{1}{2}$."

$(\int \mathbf{p}_1 | \mathbf{p}_0) = 1$ i.e. "the probability that, *the outcome of measuring the second qubit is the truth value 1, given that the outcome of measuring the first qubit was the truth value 1,* is 1."

Dynamic EQPL (or DEQPL) introduces means of reasoning about state transitions of a quantum system. It adds to the language of EQPL a number of unitary quantum operators, as well as notation for projectors. Dynamic EQPL has enough expressive power to describe quantum protocols, as demonstrated in [20] for the BB84 quantum cryptographic protocol [26, 23].

4.2 A Logic for Knowledge and Time in Quantum Systems

R. van der Meyden and M. Patra have proposed a modal logic for knowledge and time in quantum protocols [36]. They recognise the fact that, in the literature on quantum computation and information, epistemic locutions of the form

" Alice knows x. "

are frequently encountered; the logical framework which they propose is essentially an attempt to make such informal language precise. Their ultimate objective is to lay the foundations for "epistemic analysis" of quantum cryptographic protocols, and related schemes, using logical methods. Here, we will state the syntax of this "KT" quantum logic and show how it has been used to specify certain properties of the B92 protocol for quantum key distribution.

The KT quantum logic involves formulas over a set of uninterpreted propositions, `Prop`. A formula in the logic may be a proposition, a conjunction or negation of formulae, or one of the following:

- the form $\Box\phi_1$, which retains the usual temporal meaning ("always, formula ϕ_1 holds");
- the form $init(\phi_1)$, which is true if ϕ_1 holds in the initial state of a protocol;
- the form $K_i^c(\phi_1)$, which means "agent i knows, given her classical bits and observations, that ϕ_1 holds in the current state;
- the form $K_i^q(\phi_1)$, which means "agent i knows, given a set of qubits in her possession, that ϕ_1 holds in the current state.

So, the syntax of formulae, Φ, in the quantum logic is given by the following grammar:

$$\Phi ::= p \mid \phi_1 \mid \phi_2 \mid \phi_1 \wedge \phi_2 \mid \neg\phi_1 \mid \Box\phi_1 \mid init(\phi_1) \mid K_i^c(\phi_1) \mid K_i^q(\phi_1)$$

where $p \in$`Prop`. The concept of "knowledge" has two variations in the logic, since it depends on what information is used by a particular agent to decide her actions. There is a concept of "classical knowledge," which is obtained from only classical bits, and a concept of "quantum knowledge," which represents information which can be inferred from a finite set of given quantum states.

In order to define a property using this logic, a model of the protocol under consideration must be built. The logic assumes that protocols are described as *qubit message passing environments,* which are defined as follows (we have modified the original definition slightly):

Definition 8 *A **qubit message passing environment** is an abstract model of the computational setting in a quantum protocol, involving agents and channels for synchronous communication. It is defined as a tuple*

$$\langle n, S, I, Act \rangle$$

where n is the number of agents involved in the system, $S = S^q \times S^c$ is the set of all states that occur in the system, I is the initial state and Act is the set of actions performed by the various agents.

The global state S is partitioned into a set of classical states, S^c, and a set of quantum states, S^q. Clearly S^q is a subset of the Hilbert space $\mathcal{H}$ of dimension 2^N, the vector space inhabited by N qubits. The set of classical states consists of elements of the form $s^q = \langle var, loc, chan, res \rangle$, which include

- classical bit assignments, $var(i) : Var_i \longmapsto \{0,1\}$ (here, Var_i is the set of variable names belonging to agent i).
- qubit location assignments, $loc : [0,N] \mapsto [0,n]$. The value of $loc(x)$ is the name of the agent to which x is attached.
- channel value assignments, $chan : [1..n]^2 \mapsto \texttt{Msg}$, where Msg is a set of classical messages. If $chan(i,j) = m$ in a particular state, this means that message $m \in \texttt{Msg}$ has just been transmitted from agent i to agent j.
- measurement result assignments. If $res(i) = (M^i, m_i)$ in a particular state, it means that the measurement operator M^i has been applied to the quantum states in S^q, producing as a classical outcome, the value m_i.

It is instructive to show how the logic can be used to describe certain properties of the B92 protocol for quantum key distribution [7] formally. The B92 protocol is listed in Figure 1, but the reader should consult one of the many references on quantum cryptography if he or she is unfamiliar with the technique.

Van der Meyden and Patra generally treat *protocols* as functions **P** pertaining to a particular environment.

Definition 9 *A **run** $r : \mathbb{N} \mapsto S$ describes a potential evolution of the system, with $r(m)$ representing the global state of the system at time m.*

Definition 10 *A **protocol** is a system comprised of specific sets of runs, which are generated by various agents engaging in a particular pattern of behaviour. For agent i, a protocol is defined as a function $\mathbf{P} : O_i^+ \mapsto Act_i$, where O_i^+ is the set of all observations the agent has made, and Act_i is the set of actions performed by the agent.*

The B92 protocol satisfies the following formulae of KT quantum logic:

$\Box(b = 1 \Rightarrow k_A^c(a) \wedge k_B^c(a))$ i.e. "In successful runs, Alice and Bob come to 'classically know' bit a."

$\Box(b = 1 \Rightarrow \neg k_E^c(a))$ i.e. "Eve never comes to know bit a based on 'classical observations' alone."

$\Box(b = 1 \Rightarrow k_E^q(a))$ i.e. "If Eve could perform repeatable measurements on the qubit intercepted, she could come to learn the value of a."

5 Concluding Remarks

Our goal in this brief survey has been primarily to stimulate interest and provoke thought; we have only attempted to introduce the reader to the interesting issues at the intersection, so to speak, of logic and quantum theory. We have introduced the subject of quantum logic and given a brief account of the literature. We have also given a summary of recent work on developing logics for quantum information systems.

It is hoped that an understanding of quantum logic will be useful in the quest to understand and model the structure of Nature's laws, and that computer scientists will be able, in their own way, to contribute to this adventure.

The B92 protocol [7] allows two users, Alice and Bob, to establish a common secret key, using a single quantum channel and a classical communication medium, such as a telephone connection. The idea is to prevent an eavesdropper ("Eve") from obtaining the value of the key, which is a random binary sequence encoded using qubits; these qubits are transmitted over the quantum channel, and Bob measures each in order to recover the encoded bit values. According to quantum theory, only a compatible measurement is guaranteed to recover the correct bit value. If an incompatible measurement is made (i.e. a measurement with respect to a different basis of the qubit's state space), then the correct bit will only be obtained with probability 0.5. The first part of the protocol, which involves Alice sending to Bob a sequence of qubits over the quantum channel, is as follows:

1. **Initial State:** Alice has a single qubit, and a classical bit, a. Bob has two classical bits, a' and b. The bases for the set of quantum states S^q in the system are $\boxplus = \{|0\rangle, |1\rangle\}$ and $\boxtimes = \{|+\rangle, |-\rangle\}$.
2. **Alice flips her bit, a.**
   - If $a = 0$, she prepares her qubit in state $|0\rangle$.
   - If $a = 1$, she prepares her qubit in state $|+\rangle$.
3. **Alice transmits her qubit to Bob.**
4. **Bob flips his bit a'.**
   - If $a' = 0$, he measures the qubit with basis $\boxplus$.
   - If $a' = 1$, he measures the qubit with basis $\boxtimes$.
5. **If the result of the measurement is either $|0\rangle$ or $|+\rangle$, Bob sets $b = 0$.** Otherwise, he sets $b = 1$.
6. **Bob sends a classical message to Alice stating the value of b.**
7. **The run of the protocol is deemed successful only if $b = 1$.**

We write **P** for the eavesdropping version of B92, in environment $\mathcal{E}$, if it prescribes the above behaviour for Alice and Bob, and an eavesdropper, Eve, receives the qubit transmitted as well as Bob's classical message. For details, consult [36]. We use the notation $k_i^x(a) \equiv K_i^x(a = 0) \vee K_i^x(a = 1)$, where $x \in \{c, q\}$, to define the properties of **P**.

Figure 1: A simplified model of the B92 protocol, as used by Van der Meyden and Patra to define the protocol's properties in the quantum logic.

References

[1] ABRAMSKY, S., AND COECKE, B. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science: LICS 2004* (2004), pp. 415—425.

[2] ANDERSON, E. E. *Modern Physics and Quantum Mechanics*. W.B. Saunders Company, 1971.

[3] BALLENTINE, L. E. *Quantum Mechanics: A Modern Development*. World Scientific, 1998.

[4] BALTAG, A., AND SMETS, S. The logic of quantum programs. In Selinger [33].

[5] BALTAG, A., AND SMETS, S. What can logic learn from quantum mechanics? To appear, 2005.

[6] BELTRAMETTI, E., AND CASSINELLI, G. *The Logic of Quantum Mechanics*, vol. 15 of *Encyclopedia of Mathematics and its Applications*. Addison–Wesley, 1981.

[7] BENNETT, C. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters 68*, 21 (1992), 3121—3124.

[8] BIRKHOFF, G., AND VON NEUMANN, J. The logic of quantum mechanics. *The Annals of Mathematics 37*, 4 (October 1936), 823—843.

[9] BOHM, D. *Quantum Theory*. Dover, 1979.

[10] BUTLER, M., AND HARTEL, P. Reasoning about Grover's quantum search algorithm using probabilistic **wp**. *ACM Trans. Program. Lang. Syst. 21*, 3 (1999), 417–429.

[11] CHIARA, M. L. D., AND GIUNTINI, R. *Quantum Logics*, second ed., vol. 6 of *Handbook of Philosophical Logic*. Kluwer Academic Publishers, Dordrecht, 2002, pp. 129—228.

[12] COECKE, B., MOORE, D., AND WILCE, A., Eds. *Current Research in Operational Quantum Logic: Algebras, Categories, Languages*. Kluwer Academic Publishers, 2000.

[13] COHEN-TANNOUDJI, C., DIU, B., AND LALOË, F. *Quantum Mechanics*, vol. I and II. John Wiley, 1977.

[14] FAGIN, R., HALPERN, J. Y., AND MEGIDDO, N. A logic for reasoning about probabilities. *Information and Computation 87* (1990), 78—128.

[15] GAY, S. Quantum programming languages: Survey and bibliography. *Bulletin of the EATCS 86* (2005), 176—196.

[16] GAY, S., NAGARAJAN, R., AND PAPANIKOLAOU, N. Probabilistic model–checking of quantum protocols. Quantum Physics Repository Preprint quant-ph/0504007, available at `www.arxiv.org`.

[17] HUMPHREYS, J., AND PREST, M. *Numbers, groups and codes*. Cambridge University Press, 1989.

[18] HUTH, M. R., AND RYAN, M. D. *Logic in Computer Science: Modelling and reasoning about systems*, 1st ed. Cambridge University Press, 2000.

[19] MATEUS, P., AND SERNADAS, A. Exogenous quantum logic. In *Proceedings of CombLog'04 - Workshop on Combination of Logics: Theory and Applications* (Lisbon, 2004), W. A. Carnielli, F. M. Dionísio, and P. Mateus, Eds., IST Press, pp. 141—150.

[20] MATEUS, P., AND SERNADAS, A. Reasoning about quantum systems. In *Proceedings of Ninth European Conference on Logics in Artificial Intelligence* (2004), Springer–Verlag, pp. 239—251.

[21] MITTELSTAEDT, P. *Quantum Logic*, vol. 126 of *Synthese Library: Studies in Epistemology, Logic, Methodology, and Philosophy of Science*. D. Reidel Publishing Company, 1978.

[22] NAGARAJAN, R., PAPANIKOLAOU, N., BOWEN, G., AND GAY, S. An automated analysis of the security of quantum key distribution. CoRR Preprint cs.CR/0502048, available at `www.arxiv.org`.

[23] NIELSEN, M. A., AND CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[24] NILSSON, N. J. Probabilistic logic. *Artificial Intelligence 28*, 1 (1986), 71—87.

[25] PAPANIKOLAOU, N. Techniques for design and validation of quantum protocols. Master's thesis, Department of Computer Science, University of Warwick, 2005. Also available as Research Report CS-RR-413.

[26] PAPANIKOLAOU, N. Introduction to quantum cryptography. *ACM Crossroads Magazine 11.3* (Spring 2005 Issue).

[27] PATRA, M. A logic for quantum circuits and protocols. Submitted for publication, 2005.

[28] PATRA, M. A logic for quantum computation and information. Submitted for publication, 2005.

[29] PERES, A. *Quantum Theory: Concepts and Methods*. Kluwer, 1995.

[30] PIRON, C. *Foundations of Quantum Physics*. W.A. Benjamin, Inc., 1976.

[31] REICHENBACH, H. *Philosophic Foundations of Quantum Mechanics*. Dover, 1998.

[32] RIEFFEL, E., AND POLAK, W. An introduction to quantum computing for non–physicists. ACM *Computing Surveys 32*, 3 (2000), 300—335.

[33] SELINGER, P., Ed. *Proceedings of the 2nd International Workshop on Quantum Programming Languages* (2004), Turku Centre for Computer Science.

[34] SHANKAR, R. *Principles of Quantum Mechanics*. Plenum, 1980.

[35] SVOZIL, K. Quantum logic: A brief outline. In *Mathematical and Quantum Logic. Proceedings of the 4th Summer School on Analysis, Geometry and Mathematical Physics* (Karlovassi, Samos, 1998), K. Keremedis, Ed.

[36] VAN DER MEYDEN, R., AND PATRA, M. Knowledge in quantum systems. In *Proceedings of the 9th conference on Theoretical Aspects of Rationality and Knowledge* (New York, USA, 2003), ACM Press, pp. 104–117.

[37] VAN DER MEYDEN, R., AND PATRA, M. A logic for probability in quantum systems. In *Proceedings of Computer Science Logic and 8th Kurt Gödel Colloquium* (Vienna, Austria, 2003), Lecture Notes in Computer Science, Springer–Verlag.

[38] WILCE, A. Quantum logic and probability theory. In *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. Spring 2003.