INTRODUCTION

JENNIFER CHUBB, ALI ESKANDARIAN, AND VALENTINA HARIZANOV

In the last two decades, the scientific community has witnessed a surge in activity, interesting results, and notable progress in our conceptual understanding of computing and information based on the laws of quantum theory. One of the significant aspects of these developments has been an integration of several fields of inquiry that not long ago appeared to be evolving, more or less, along narrow disciplinary paths without any major overlap with each other. In the resulting body of work, investigators have revealed a deeper connection among the ideas and techniques of (apparently) disparate fields. As is evident from the title of this volume, logic, mathematics, physics, computer science and information theory are intricately involved in this fascinating story. The inquisitive reader might focus, perhaps, on the marriage of the most unlikely and intriguing fields of quantum theory and logic and ask: *Why quantum logic?*

By many, "logic" is deemed to be panacea for faulty intuition. It is often associated with the rules of correct thinking and decision-making, but not necessarily in its most sublime role as a deep intellectual subject underlying the validity of mathematical structures and worthy of investigation and discovery in its own right. Indeed, within the realm of the classical theories of nature, one may encounter situations that defy comprehension, should one hold to the intuition developed through experiencing familiar macroscopic scenarios in our routine impressions of natural phenomena.

One such example is a statement within the special theory of relativity that the speed of light is the same in all inertial frames. It certainly defies the common intuition regarding the observation of velocities of familiar objects in relative motion. One might be tempted to dismiss it as contrary to observation. However, while analyzing natural phenomena for objects moving close to the speed of light and, therefore, unfamiliar in the range of velocities we are normally accustomed to, logical deductions based on the postulates of the special relativity theory lead to the correct predictions of experimental observations.

There exists an undeniable interconnection between the deepest theories of nature and mathematical reasoning, famously stated by Eugene Wigner as the unreasonable efficacy of mathematics in physical theories. The sciences,

Logic and Algebraic Structures in Quantum Computing
Edited by J. Chubb, A. Eskandarian and V. Harizanov
Lecture Notes in Logic, 45

and in particular physics, have relied on, and benefited from, the economy of mathematical expressions and the efficacy and rigor of mathematical reasoning with its underlying logical structure to make definite statements and predictions about nature. Mathematics has become the *de facto* language of the quantitative sciences, particularly scientific theories, and the major discoveries and predictive statements of these theories (whenever possible) are cast in the language of mathematics, as it affords them elegance as well as economy of expression. *What happens if the syntax and grammar of such a language become inadequate?*

This seems to have been the case when some of the more esoteric predictions of the then new theory of quantum mechanics began to challenge the scientific intuition of the times around the turn of the 20th century. This violation of intuition was so severe that even the most prominent of scientists were not able to reconcile the dictates of their intuition with the experimentally confirmed predictions of the theory. The discomfort with some of the features and predictions of quantum theory were, perhaps, most prominently brought out in the celebrated work of Einstein, Podolsky, and Rosen (EPR) in the mid 1930s. EPR fueled several decades of investigations on the foundations of quantum theory that continue to this day. The main assertion of the EPR work was that quantum theory had to be, by necessity, incomplete. Otherwise, long held understanding of what should be taken for granted as "elements of reality" had to be abandoned. Here, according to EPR, logical deductions based on primitives that were the very essence of reality and logical consistency forced the conclusion of the incompleteness of quantum theory; as if considering quantum theory as complete would question one's logical fitness and one's understanding of reality! Yet, in the decades since, with increasing sophistication in experimentation, and multiple ways of testing the theory, quantum theory has consistently outshined the alternatives. In particular, many predictions relying on the sensibilities of classical theories, where concepts such as separability, locality, and causality are the seemingly indispensable factors in our *understanding* of reality, are found to be entirely inconsistent with the *actual* reality around us. Quantum theory has not (as yet) suffered any such blow.

Confronted with the stark inability to reconcile the predictions of a theory, which are shown to be correct every time subjected to experimental verification, and a logical structure that seems to fall short in facilitating correct thinking and correct decision making (at least, in so far as the behavior of natural phenomena at the quantum level is concerned), one is forced to consider and question the validity of the premises on which that logical structure is built, or to discover alternative structures. Furthermore, the striking applications of quantum theory in the theory of computation, development of new algorithms, and the promising prospects for the building of a computing machine operating on the basis of the laws of quantum theory, necessitate a deeper investigation of alternative logical structures that encompass the elements of this new quantum reality. One must then give credence to the argument that, perhaps, the fault is not with the revolutionary quantum theory; rather, it is with the inadequacies of logical structures that were insufficient to be expanded and applied to a world that does not comply with the notions embodied in our understanding of the macroscopic classical physical theories of nature.

The utility of logical rules is most pronounced when applied to the building and operation of computing machines. With the advent of computing that takes advantage of the laws of quantum theory, i.e., quantum computing, it is only natural to search for those logical and algebraic structures that underlie the scaffolding of the quantum rules in computations. As obvious as it is that Boolean logic underlies classical computing and much of classical reasoning, it is equally obvious that it is not sufficient to express the logic underlying quantum mechanics or quantum computing. Birkhoff and von Neumann were among the first to propose a generalization of Boolean logic in which propositions about quantum systems could be formulated. While their endeavor was revolutionary, the Birkhoff-von Neumann quantum logic was not to be the final word on the subject of a logic for quantum mechanics, and indeed the investigation continues with increasing urgency.

In this volume, we present the work of a select group of scholars with an abiding interest in tackling some of the fundamental issues facing quantum computing and information theory, as investigated from the perspective of logical and algebraic structures. This selection, no doubt, reflects the intellectual proclivities and curiosities of the editors, within the reasonable limitations of space and coverage of topics for a volume of this size, and for the purpose of generating ideas that would fuel further investigation and research in these and related fields.

The first two articles, by Stairs and Parke, address philosophical and historical issues. Brandenburger and Keisler use ideas from continuous model theory to explore determinism and locality in quantum mechanical systems. Abramsky and Heunen, and Jacobs and Mandemaker describe the relationship between the category-theoretic and operator-theoretic approaches to the foundations of quantum physics. Döring gives a topos-based distributive form of quantum logic as an alternative to the quantum logic of Birkhoff and von Neumann. The papers by Coecke and Kartsaklis et al. use a diagrammatic calculus in analyzing quantum mechanical systems and, very recently, in computational linguistics. Kauffman's article presents an extensive treatment of the prominent role of algebraic structures arising from topological considerations in quantum information and computing; the pictorial approach used in knot theory is closely related to the quantum categorical logic presented in other articles in this volume.

Could logic be empirical? The Putnam-Kripke debate, by Allen Stairs. In his article in the present volume, Stairs outlines Hilary Putnam's position that quantum mechanics provides an empirical basis for a re-evaluation of our idea of logic and Saul Kripke's response, in which he takes issue with the very idea of a logic that is based on anything empirical. Stairs carefully interprets their positions, and in the end offers the beginnings of a compromise, which includes "disjunctive facts," which can be true even if their disjuncts are not, and the notion of "l-complementarity," to describe the relationship between statements having non-commuting associated projectors. The article wrestles with the idea of whether and how quantum mechanics should inform our logic and reasoning processes.

The essence of quantum theory for computers, by William C. Parke. In this article, Parke provides a thorough yet succinct introduction to the elements of physical theories, classical and quantum, which are relevant to a deeper understanding of the mathematical and logical structures underlying (or derived) from such theories, and important in the appreciation of the more subtle quandaries of quantum theory, leading to its utilization in computation. The emphasis has been placed on the physical content of information and elements of computation from a physicist's point of view. This includes a treatment of the role of space-time in the development of physical theories from an advanced point of view, and the limitations that our current understanding of space-time imposes on building and utilizing computing machines based on the rules of quantum theory. The treatment of the principles of quantum theory is also developed from an advanced point of view, without too much focus on unnecessary details, but covering the essential conceptual ingredients, in order to set the stage properly and provide motivation for the work of the others on logical and algebraic structures.

Fiber products of measures and quantum foundations, by Adam Brandenburger and H. Jerome Keisler. In this model-theoretic article, the authors use fiber products of (probability) measures within a framework they construct for empirical and hidden-variable models to prove determinization theorems. These objects (fiber products) were conceived by Rae Shortt in a 1984 paper, and were used recently by Itaï Ben Yaacov and Jerome Keisler in their work on continuous model theory (2009). Techniques in continuous model theory are relevant to the notion of models of quantum structures as in that context the "truth value" of a statement may take on a continuum of values, and can be thought of as probabilistic. In this case, a technique employed in continuous model theory is used in the construction of models in proofs of theorems that assert that every empirical model can be realized by an extension that is a deterministic hidden-variable model, and for every hidden-variable model satisfying locality and λ-independence, there is a realization-equivalent (both models extend a common empirical submodel) hidden-variable model satisfying determinism and λ-independence. The latter statement, together with Bell's theorem, precludes the existence of a hidden-variable model in which both determinism and λ-independence hold. The notion of λ-independence was first formulated by W. Michael Dickson (2005). It says that the choices made by an entity as to which observable to measure in a system are not influenced by the process of the determination of the value of a relevant hidden-variable.

Operational theories and categorical quantum mechanics, by Samson Abramsky and Chris Heunen. There are two complementary research programs in the foundations of quantum mechanics, one based on operational theories (also called general probabilistic theories) and the other on category-theoretic foundation of quantum theory. Samson Abramsky and Chris Heunen establish strong and important connections between these two formalisms. Operational theories focus on empirical and observational content, and quantum mechanics occupies one point in a space of possible theories. The authors define a symmetric monoidal categorical structure of an operational theory, which they call process category, and exploit the ideas of categorical quantum mechanics to obtain an operational theory as a certain representation of this process category. They lift the notion of non-locality to the general level of operational category. They further propose to apply a similar analysis to contextuality, which can be viewed as a broader phenomenon than non-locality.

Relating operator spaces via adjunctions, by Bart Jacobs and Jorik Mandemaker. By exploiting techniques of category theory, Jacobs and Mandemaker clarify and present in a unified framework various, seemingly different results in the foundation of quantum theory found in the literature. They use category-theoretic tools to describe relations between various spaces of operators on a finite-dimensional Hilbert space, which arise in quantum theory, including bounded, self-adjoint, positive, effect, projection, and density operators. They describe the algebraic structure of these sets of operators in terms of modules over various semirings, such as the complex numbers, the real numbers, the non-negative real numbers. The authors give a uniform description of such modules via the notion of an algebra of the multiset monad. They show how some spaces of operators are related by free constructions between categories of modules, while the other spaces of operators are related by a dual adjunction between convex sets (conveniently described via a monad) and effect modules.

Topos-based logic for quantum systems and bi-Heyting algebras, by Andreas Döring. Döring replaces the standard quantum logic, introduced by Birkhoff and von Neumann, which comes with a host of conceptual and interpretational problems, by the topos-based distributive form of quantum logic. Instead of having a non-distributive orthomodular lattice of projections, he considers a complete bi-Heyting algebra of propositions. More specifically, Döring considers clopen subobjects of the presheaf attaching the Gelfand spectrum to each abelian von Neumann algebra, and shows that these clopen subojects form a bi-Heyting algebra. He gives various physical interpretations of the objects in this algebra and of the operations on them. For example, he introduces two kinds of negation associated with the Heyting and co-Heyting algebras, and gives physical interpretation of the two kinds of negation. Döring considers the map called outer daseinisation of projections, which provides a link between the usual Hilbert space formalism and his topos-based quantum logic.

The logic of quantum mechanics – Take II, by Bob Coecke. Schrödinger maintained that composition of systems is the heart of quantum computing, and Coecke agrees. He suggests that the Birkhoff-von Neumann formulation of quantum logic fails to adequately and elegantly capture composition of quantum systems. The author puts forth a model of quantum logic that is based on composition rather superposition. He axiomatizes composition without reference to underlying systems using strict monoidal categories as the basic structures and explains a graphical language that exactly captures these structures. Imposing minimal additional structure on these categories (to obtain dagger compact categories) allows for the almost trivial derivation of a number of quantum phenomena, including quantum teleportation and entanglement swapping. This (now widely adopted) formalism has been used not only to solve open problems in quantum information theory, but has also provided new insight into non-locality.

Coecke's framework has been applied both to logic concerned with natural language interpretations, and to more formal automated reasoning processes. In this article, the focus is on the former. Coecke applies the graphical language of dagger compact categories to natural language processing—"from word meaning to sentence meaning"—implementing Lambek's theory of grammar and the notion of words as "meaning vectors." He argues that sentence meaning amounts to more than the meanings of the constituent words, but also the way in which they *compose*.

In the end, Coecke confesses that dagger compact categories do not capture all we might want them to, in particular, measurement, observables, and complementarity are left by the wayside. The model can be expanded (using spiders!) in such a way that all these are captured. Coecke closes with speculation about an important question: Where is the traditional logic hiding in all this?

Reasoning about meaning in natural language with compact closed categories and Frobenius algebras, by Dimitri Kartsaklis, Mehrnoosh Sadrzadeh, Stephen Pulman, and Bob Coecke. The authors apply category-theoretic methods to computational lingustics by mapping the derivations of the grammar logic to the distributional interpretation *via* a strongly monoidal functor. Such functors are structure preserving morphims. Grammatical structure is modeled through the derivations of pregroup grammars. A pregroup is a partially ordered monoid with left and right adjoints for every element in the partial order. The authors build tensors for linguistic constructs with complex types by using a Frobenius algebra. The Frobenius operations allow them to assign and compare the meanings of different language constructs such as words, phrases, and sentences in a single space. The authors present their experimental results for the evaluation of their model in a number of natural languages.

Knot logic and topological quantum computing with Majorana fermions, by Louis H. Kauffman. Kauffman presents several topics exploring the relationship between low-dimensional topology and quantum computing. These topics have been introduced and developed by Kauffman and Samuel J. Lomonaco over the last ten years. Kauffman uses the diagrammatic approach, and is particularly interested in models based upon the Temperley-Lieb categories. He discusses from several different perspectives the Fibonacci model related to the Temperley-Lieb algebra at fifth roots of unity. Kauffman shows how knots are related to braiding and quantum operators, as well as to quantum set-theoretic foundations. For example, the negation can generate the fusion algebra for a Majorana fermion, which is a particle that interacts with itself and can even annihilate itself. Thus, Kauffman calls the negation the mark.

He investigates the relationship between knot-theoretic recoupling theory and topological quantum field theory. Kauffman works with braid groups and their representations, and produces unitary representations of the braid groups that are dense in the unitary groups. He describes the Jones polynomial in terms of his bracket polynomial and applies his approach to design a quantum algorithm for computing the colored Jones polynomials for knots and links. Kauffman also gives a quantum algorithm for computing the Witten-Reshetikhin-Turaev invariant of three manifolds.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SAN FRANCISCO
SAN FRANCISCO, CA 94117
E-mail: jcchubb@usfca.edu

DEPARTMENT OF PHYSICS
VIRGINIA SCIENCE & TECHNOLOGY CAMPUS
GEORGE WASHINGTON UNIVERSITY
ASHBURN, VIRGINIA 20147
E-mail: ea1102@gwu.edu

DEPARTMENT OF MATHEMATICS
GEORGE WASHINGTON UNIVERSITY
WASHINGTON, D.C. 20052
E-mail: harizanv@gwu.edu

A (VERY) BRIEF TOUR OF QUANTUM MECHANICS, COMPUTATION, AND CATEGORY THEORY

JENNIFER CHUBB AND VALENTINA HARIZANOV

This chapter is intended to be a brief treatment of the basic mechanics, framework, and concepts relevant to the study of quantum computing and information for review and reference. Part 1 (sections 1–4) surveys quantum mechanics and computation, with sections organized according to the commonly known postulates of quantum theory. The second part (sections 5–7) provides a survey of category theory. Additional references to works in this volume are included throughout, and general references appear at the end.

Part 1: Quantum mechanics & computation

§1. Qubits & quantum states.

Postulate of quantum mechanics: Representing states of systems. The state of a quantum system is represented by a unit-length vector in a complex Hilbert space[1], $\mathcal{H}$, that corresponds to that system. The state space of a composite system is the tensor product of the state spaces of the subsystems.

The Dirac bra-ket notation for states of quantum systems is ubiquitous in the literature, and we adopt it here. A vector in a complex Hilbert space representing a quantum state is written as a *ket*, $|\psi\rangle$, and its conjugate-transpose (adjoint, or sometimes Hermitian conjugate) is written as a *bra*, $\langle\psi|$. In this notation, a bra-ket denotes an inner product, $\langle\varphi|\psi\rangle$, and a ket-bra denotes an outer product, $|\varphi\rangle\langle\psi|$.

Each one-dimensional subspace of $\mathcal{H}$ corresponds to a possible state of the system, and a state is usually described as a linear combination in a relevant orthonormal basis. The basis elements are often thought of as *basic states*. Quantum systems can exist in a *superposition* of more than one basic state: If a quantum system has access to two basic states, say $|\alpha\rangle$ and $|\beta\rangle$, then, in general, the system's "current state" can be represented by a linear combination of these states in complex Hilbert space:

$$|\psi\rangle = c_1|\alpha\rangle + c_2|\beta\rangle, \text{ where } ||\psi\rangle| = 1.$$

[1] A Hilbert space is a complete, normed metric space, where the norm and distance function are induced by an inner product defined on the space.

Logic and Algebraic Structures in Quantum Computing
Edited by J. Chubb, A. Eskandarian and V. Harizanov
Lecture Notes in Logic, 45

The complex coefficients, c_1 and c_2, of $|\alpha\rangle$ and $|\beta\rangle$ give classical probabilistic information about the state. For example, the value $|c_1|^2$ is the probability that the system would be found to be in state $|\alpha\rangle$ upon measurement. The coefficient itself, c_1, is called the *probability amplitude*. Two vectors in $\mathcal{H}$ represent the same state if they differ only by a global phase factor: If $|\psi\rangle = e^{i\theta}|\varphi\rangle$, then $|\psi\rangle$ and $|\varphi\rangle$ represent the same state, and the (real) probabilities described by the coefficients are the same.

The squared norm of the state vector $|\psi\rangle$ is the inner product of $|\psi\rangle$ with itself, i.e., the bra-ket $\langle\psi|\psi\rangle$. The quantity $|\langle\varphi|\psi\rangle|^2$ is the probability that upon measurement, $|\psi\rangle$ will be found to be in state $|\varphi\rangle$, and $\langle\varphi|\psi\rangle$ is the corresponding probability amplitude. (More about measurement of quantum systems can be found in Section 3 below.)

1.1. Qubits. A classical bit can be in only one of two states at a given time, $|0\rangle$ or $|1\rangle$. A quantum bit or *qubit* may exist in a *superposition* of these basic (orthogonal) states, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, where c_1 and c_2 are complex probability amplitudes. More precisely, a qubit is a 2-dimensional quantum system, the state of which is a unit-length vector in $\mathcal{H} = \mathbb{C}^2$. The basic states for this space are usually thought of as $|0\rangle$ and $|1\rangle$, but at times other bases are used (for example, $\{|+\rangle, |-\rangle\}$ or $\{|\uparrow\rangle, |\downarrow\rangle\}$). Basic states are typically the eigenstates (eigenvectors) of an observable of interest (see discussion of measurement below).

Any unit vector that is a (complex) linear combination of the basic states is a *pure* state and non-trivial linear combinations are *superpositions*. So-called *mixed* states are not proper state vectors, they are classical probabilistic combinations of pure states and are best represented by *density matrices*.

The state space of a qubit is often visualized as a point on the *Bloch sphere*. The norm of a state vector is always one, and states that differ only by a global phase factor are identified, so two real numbers, θ and ϕ, suffice to specify a distinct state via the decomposition

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle.$$

Respectively, the range of values taken on by θ and ϕ may be restricted to the intervals $[0,\pi]$ and $[0,2\pi)$ without any loss of generality, and so the corresponding distinct states may be mapped uniquely onto the unit sphere in $\mathbb{R}^3$. In this visualization, the basic vector $|0\rangle$ points up and $|1\rangle$ points down, θ describes the latitudinal angle, and φ the longitudinal angle. Orthogonal states are antipodal on the Bloch sphere. Note that states that differ by a global phase factor will (by design) coincide in this visualization.

1.2. Composite quantum systems. As described above, a single quantum system (for example, a single qubit) exists in a pure state that may be a superposition of basic states. A composition of systems may exist either in a *separable* or an *entangled* state. Separable states are states that can be written as tensor products of pure states of the constituent subsystems. Entangled states cannot be so written; they are non-trivial (complex) linear combinations of separable states. In the case of an entangled state, the subsystems cannot be thought of as existing in states independent of the composed system.

Example 1.1. Suppose we have a system of two qubits, the first in state $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and the second in state $|\varphi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. The state of the combined system is

$$|\psi\rangle \otimes |\varphi\rangle = |\psi\rangle|\varphi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

Such a state of the composite system that can be written as a tensor product of pure states is called *separable*.

Example 1.2. The *Bell states* of a 2-qubit system are not separable; they are important and canonical examples of *entangled* states:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Example 1.3. The GHZ *states* (for Greenberger-Horne-Zeilinger) are examples of entangled states in composite systems that have three or more subsystems. The GHZ state for a system with n subsystems is

$$\frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}.$$

For more on entangled states, see Parke's article in this volume, or Section 6 of Kauffman's article.

§2. Transformations and quantum gates.

Postulate of quantum mechanics: Evolution of systems. The time evolution of a closed quantum system is described by a unitary transformation.

A transformation is *unitary* if its inverse is equal to its adjoint. Such transformations preserve inner products and are reversible, deterministic, and continuous. In quantum computing, algorithms are often described as circuits in which information (and time) flows from left to right. Quantum gates represent unitary transformations applied to qubits in such a circuit.

Example 2.1. *The Hadamard gate*. The 1-qubit Hadamard gate has as input and output one qubit, as shown in the simple circuit diagram below: