Quantum Computation and Logic

How Quantum Computers Have Inspired Logical Investigations
Trends in Logic

Volume 48
SCOPE OF THE SERIES

The book series Trends in Logic covers essentially the same areas as the journal Studia Logica, that is, contemporary formal logic and its applications and relations to other disciplines. The series aims at publishing monographs and thematically coherent volumes dealing with important developments in logic and presenting significant contributions to logical research.

The series is open to contributions devoted to topics ranging from algebraic logic, model theory, proof theory, philosophical logic, non-classical logic, and logic in computer science to mathematical linguistics and formal epistemology. However, this list is not exhaustive, moreover, the range of applications, comparisons and sources of inspiration is open and evolves over time.

More information about this series at http://www.springer.com/series/6645
Quantum Computation and Logic

How Quantum Computers Have Inspired Logical Investigations
Dedicated to the memory of David Foulis, Peter Mittelstaedt and Giuliano Toraldo di Francia
After the publication of Richard Feynman’s pioneering contributions (in the 80s of the last century), investigations in the field of quantum computation theory have become more and more intense. In spite of some initial skepticism, important achievements have recently been obtained in the technological realizations of quantum computers, which nowadays cannot be any longer regarded as mere “thought experiments”. These researches have naturally inspired new theoretical ideas, stimulating also a new interest for foundational and philosophical debates about quantum theory.

As is well known, classical computers have a perfect abstract model represented by the concept of Turing machine. Due to the intuitive strength of this concept and the high stability of the notion of Turing computability (which has turned out to be equivalent to many alternative definitions of computability) for a long time the Church-Turing thesis (according to which a number-theoretic function \( f \) is computable from an intuitive point of view iff \( f \) is Turing-computable) has been regarded as a deeply reasonable conjecture. This hypothesis seems to be also confirmed by a number of studies about alternative concepts of computing machine that at first sight may appear “more liberal”. A significant example is represented by the notion of non-deterministic (or probabilistic) Turing machine. Interestingly enough, one has proved that non-deterministic Turing-machines do not go beyond the “limits and the power” of deterministic Turing machines; for, any probabilistic Turing machine can be simulated by a deterministic one.

To what extent have quantum computers “perturbed” such clear and well established approaches to computation-problems? After Feynman’s contributions, the abstract mathematical model for quantum computers has often been represented in terms of the notion of quantum Turing machine, the quantum counterpart of the classical notion of Turing machine. But what exactly are quantum Turing machines? So far, the literature has not provided a rigorous “institutional” concept of quantum Turing machine. Some definitions seem to be based on a kind of “imitation” of the classical definition of Turing machine, by referring to a tape (where the symbols are written) and to a moving head (which changes its position on the tape). These concepts, however, seem to be hardly applicable to physical quantum
computers. We need only think of the intriguing situations determined by quantum uncertainties that, in principle, should also concern the behavior of moving heads. In this book, we will consider a more general concept, represented by the notion of abstract quantum computing machine, which neglects both tapes and moving heads. Do abstract quantum computing machines go beyond the computational limits of classical Turing machines? In other words, does quantum computation theory lead us to a refutation of the Church-Turing thesis? In spite of some interesting examples discussed in the literature, this hard problem seems to be still undecided.

Quantum computation theories have naturally inspired new ideas in the field of logic, bringing about some important conceptual changes in the quantum-logical investigations. The interaction between quantum theory and logic has a long history that started in 1936 with the publication of Birkhoff and von Neumann’s celebrated article “The logic of quantum mechanics”. At the very beginning, this article did not raise any great interest either in the physical or in the logical community. Strangely enough, logicians did not immediately recognize the most “revolutionary logical idea” of quantum logic: the possible divergence between the concepts of maximal information and logically complete information.

As is well known, the pure states of a classical physical system $S$ (a gas-molecule, a table, a planet, etc.) represent pieces of information that are at the same time maximal and logically complete. The information provided by a pure state of $S$ cannot be consistently extended to a richer knowledge; at the same time, such information decides all possible events that may occur to $S$. For this reason, the notion of pure state of a classical physical object seems to be very close to the idea of complete concept, investigated by Leibniz: although many properties of an individual object (say, the Moon) may be unknown to human minds, God knows the complete concept of any object (living either in the actual or in some possible world), and this concept represents a maximal and logically complete information about the object in question.

Due to the celebrated uncertainty-principles (discovered by Heisenberg), complete concepts (in Leibniz’ sense) cannot exist for quantum objects. Consider a quantum system $S$ (say, an electron) in a pure state that assigns an exact value to its velocity in the $x$-direction. In such a case, the position of $S$ (with respect to the $x$-direction) will be completely indeterminate: the object $S$ turns out to be non-localized. Quantum objects, are in a sense, “poor”; and their “poverty” concerns the number of physical properties that can be satisfied at the same time. Furthermore, quantum properties seem to behave in a contextual way: properties that are completely indeterminate in a given context may become actual and determinate in a different context (for instance, after the performance of an appropriate measurement). Hence, the system of properties that are determinate for a given quantum object turns out to be context-dependent. Quantum pure states represent pieces of information that are at the same time maximal (since they cannot be consistently extended to a richer knowledge) and logically incomplete (since they cannot decide all the relevant properties of the objects under investigation). This divergence between the concepts of maximal knowledge and logically
complete knowledge represents a characteristic logical aspect of the quantum world that may appear prima facie strange, since it is in contrast with a basic theorem of classical logic (and of many alternative logics): Lindenbaum’s theorem, according to which any non-contradictory set of sentences $T$ can be extended to a set of sentences $T'$ that is at the same time non-contradictory (no contradiction can be derived from $T$), logically complete (for any sentence $x$ of the language either $x$ or its negation $\neg x$ belongs to $T'$), maximal (all proper extensions of $T'$, formalized in the same language of $T'$, are contradictory).

Apparently, quantum undecidabilities turn out to be much stronger than the syntactical undecidabilities discovered by Gödel’s incompleteness theorems. In the quantum world, undecidability is not only due to the limited proof-theoretic capacities of finite minds: against “Leibniz’ dream” even an infinite omniscient mind should be bound to quantum uncertainties.

Birkhoff and von Neumann’s quantum logic (as well as its further developments) represent, in a sense, static logics. The basic aim of these logics is the description of the abstract structure of all possible quantum events that may occur to a given quantum system and of the relationships between events and states. In this framework, the logical connectives are interpreted as (generally irreversible) operations, which do not reflect any time-evolution either of the physical system or of the observer.

Quantum computation theory has inspired a completely different approach to quantum logic, giving rise to new forms of logics that have been called quantum computational logics. The basic objects of these logics are pieces of quantum information: possible states of quantum systems that can store and transmit the information in question, evolving in time. Accordingly, any formula of a quantum computational language can be regarded as a synthetic logical description of a quantum logical circuit. In this way, linguistic expressions acquire a characteristic dynamic meaning, representing possible computational actions.

The most natural semantics for quantum computational logics is a form of holistic semantics, where some puzzling features of quantum entanglement (often described as mysterious and potentially paradoxical) are used as a positive semantic resource. Against the compositionality principle (a basic assumption of classical logic and of many other logics), the meaning of a compound expression of a quantum computational language cannot be generally represented as a function of the meanings of its well-formed parts. The procedure goes from the whole to the parts, and not the other way around. Furthermore, meanings are essentially context-dependent. In this way, quantum computational logics turn out to be a natural abstract tool that allows us to model semantic situations (even far from microphysics), where holism, contextuality, vagueness and ambiguity play an essential role, as happens in the case of natural languages and in the languages of arts (say, poetry or music).

The aim of this book is providing a general survey of the main concepts, questions and results that have been studied in the framework of the recent interactions between quantum information, quantum computation and logic.
Chapter 1 is an introduction to the basic concepts of the quantum-theoretic formalism used in quantum information. It is stressed how the characteristic uncertainties of the quantum world have brought about some deep logical innovations, due to the divergence between the concepts of maximal information and logically complete information. It is explained how Birkhoff and von Neumann’s quantum logic and the more recent forms of unsharp (or fuzzy) quantum logics have naturally emerged from the mathematical environment of quantum theory.

Chapter 2 gives a synthetic presentation of the main “mathematical characters” of the quantum computational game: qubits, quregisters, mixtures of quregisters, and quantum logical gates. The basic idea of quantum computer theory is that computations can be performed by some quantum systems that evolve in time. Accordingly, by applying Schrödinger’s equation, it is natural to assume that quantum information is processed by special examples of unitary operators (called quantum logical gates), which transform in a reversible way the pure states of the quantum systems that store the information in question. The last section of the chapter illustrates possible physical implementations of some quantum logical circuits by means of special variants of the Mach-Zehnder interferometer, an apparatus that has played an important role in the philosophical debates about quantum theory.

Chapter 3 investigates the puzzling entanglement-phenomena. The Einstein-Podolsky-Rosen paradox (EPR) is logically analyzed and it is shown how EPR-situations have later on been transformed into powerful resources, even from a technological point of view. As a significant example, teleportation-experiments are briefly illustrated.

Chapter 4 introduces the reader to quantum computational logics, new forms of quantum logic inspired by the theory of quantum circuits. The basic idea of these logics is that sentences denote pieces of quantum information, while logical connectives are interpreted as special examples of quantum logical gates. The most natural quantum computational semantics is a holistic and contextual theory of meanings, where quantum entanglement can be used as a logical resource. The concept of logical consequence, defined in this semantics, characterizes a weak form of quantum logic (called holistic quantum computational logic), where many important logical arguments (which are valid either in classical logic or in Birkhoff and von Neumann’s quantum logic) are possibly violated.

Chapter 5 develops a quantum computational semantics for a language that can express sentences like “Alice knows that everybody knows that she is pretty”. The basic question is: to what extent is it possible to interpret quantifiers and epistemic operators as special examples of Hilbert-space operations? It is shown how these logical operators have a similar logical behavior, giving rise to a “reversibility-breaking”. Unlike logical connectives, quantifiers and epistemic operators can be represented as particular quantum maps that are generally irreversible. An interesting feature of the epistemic quantum semantics is the failure of the unrealistic phenomenon of logical omniscience: Alice might know a given sentence without knowing all its logical consequences.
Chapter 6 is devoted to a “many-valued generalization” of the classical part of quantum computational logics, which only deals with bits, registers and gates that are reversible versions of Boolean functions (in the framework of a two-valued semantics). One can generalize this approach, by assuming a many-valued classical basis for quantum computation. In this way, qubits are replaced by qudits: quantum superpositions living in a Hilbert space whose dimension may be greater than two. The qudit-semantics gives rise to some interesting physical applications.

Chapter 7 introduces the concept of abstract quantum computing machine, which represents an adequate mathematical model for the description of concrete quantum computers. To what extent can abstract quantum computing machines be simulated by classical Turing machines? Does quantum computation give rise to possible violations of the Church-Turing thesis? These hard questions did not find, so far, a definite answer.

Chapter 8 describes some possible applications of the holistic quantum semantics to fields (far apart from microphysics), where ambiguity, vagueness, allusions and metaphors play an essential role. Some characteristic examples that arise in the framework of musical languages are illustrated.

Chapter 9 discusses some recent debates about foundational and philosophical questions of quantum theory, which have been stimulated by researches in the field of quantum information and quantum computation. “Information interpretations” according to which quantum theory should be mainly regarded as a “revolutionary information theory” have been opposed to more traditional “realistic views”, according to which the pure states of the quantum-theoretic formalism shall always “mirror” objective properties of physical systems that exist (or may exist) in the real world.

Chapter 10 contains a survey of the definitions of the main mathematical concepts used in the book.

Florence, Italy
Cagliari, Italy
Bergamo, Italy
Cagliari, Italy

Maria Luisa Dalla Chiara
Roberto Giuntini
Roberto Leporini
Giuseppe Sergioli

Preface xi
Acknowledgements

Many ideas discussed in this book have been inspired by long collaborations with other scholars. Some of them have been co-authors of previous contributions of ours. We are especially grateful to Enrico Beltrametti, Gianpiero Cattaneo, Anatolij Dvurečenskij, Hector Freytes, Richard Greechie, Stanley Gudder, Antonio Ledda, Eleonora Negri, Francesco Paoli, Sylvia Pulmannová and Miklos Rédei. Our work has also been greatly stimulated by interactions with scientists and philosophers who have represented for us an important scientific and human point of reference: Dirk Aerts, Alexandru Baltag, Sergio Bernini, Jeremy Butterfield, Michele Camerota, Andrea Cantini, Roberto Casalbuoni, Ettore Casari, Gianni Cassinelli, Elena Castellani, Domenico Costantini, Marcello D’Agostino, Francesco De Martini, Christian de Ronde, Antonio Di Nola, Dov Gabbay, Claudio Garola, Amit Hagar, Décio Krause, Pekka Lahti, Federico Laudisa, Pierluigi Minari, Mioara Mugur Schächter, Daniele Mundici, Mirko Navara, Giulio Peruzzi, Pavel Pták, Jaroslaw Pykacz, Zdenka Riečanová, Giovanni Sambin, Frank Schroeck, Sonja Smets, Sandro Sozzo, Karl Svozil, Silvano Tagliagambe, Bas van Fraassen and Paola Verrucchi. We would like to mention also the periodical meetings of the International Quantum Structures Association (IQSA), splendid occasions for scientific collaboration.

Some great scholars and friends are no longer with us. We fondly remember Sławomir Bugajski, Paul Busch, Roberto Cignoli, David Finkelstein, David Foulis, GianCarlo Ghirardi, Peter Mittelstaedt, Franco Montagna, Belo Riečan, Charles Randall, Alberto Rimini, Gottfried Rüttimann, Patrick Suppes and Giuliano Toraldo di Francia.

Finally, we warmly thank Heinrich Wansing (editor-in-chief of Trends in Logic), who has encouraged our work and patiently waited for the final version of this book. We are also deeply grateful to the anonymous referee who has proposed to us many interesting and useful suggestions.

This work has been partially supported by Regione Autonoma della Sardegna in the framework of the project “Time-logical evolution of correlated microscopic systems” (CRP 55, L.R. 7/2007, 2015).
# Contents

1  **The Mathematical Environment of Quantum Information**  
   1.1 Physics and Logic in Classical Information Theory  
   1.2 From the Classical to the Quantum-Theoretic Formalism  
   1.3 The Mathematics of Quantum Theory  
   1.4 Composite Systems  
   1.5 Time Evolution and Quantum Measurements  
   1.6 The Unsharp Approaches to Quantum Theory  
   1.7 Quantum Logics  
   References  

2  **Pieces of Quantum Information and Quantum Logical Gates**  
   2.1 Qubits, Quregisters and Mixtures of Quregisters  
   2.2 Quantum Logical Gates  
   2.3 Quantum Logical Circuits  
   2.4 Physical Implementations by Optical Devices  
   References  

3  **Entanglement: Mystery and Resource**  
   3.1 Entangled Pure States  
   3.2 The Einstein-Podolsky-Rosen Paradox  
   3.3 Quantum Teleportation  
   References  

4  **From Quantum Circuits to Quantum Computational Logics**  
   4.1 A New Approach to Quantum Logic: Quantum Computational Logics  
   4.2 A Sentential Quantum Computational Language  
   4.3 A Holistic Computational Semantics  
   4.4 Quantum Computational Logical Arguments  
   References  

References
5 Individuals, Quantifiers and Epistemic Operators ........................................ 85
  5.1 Introduction .................................................................................. 85
  5.2 Truth-Perspectives ......................................................................... 86
  5.3 A First-Order Epistemic Quantum Computational Language .......... 88
  5.4 A Holistic Quantum Computational Semantics for
      a Fragment of the Language $\mathcal{L}_1$ ........................................ 91
  5.5 An Epistemic Quantum Computational Semantics ......................... 95
  5.6 Physical Examples and Relativistic-Like Epistemic Effects ............. 105
  5.7 Quantifiers as Quantum Maps .................................................... 112
  References ..................................................................................... 116

6 From Qubits to Qudits ........................................................................ 117
  6.1 Introduction .................................................................................. 117
  6.2 Qudit-Spaces ................................................................................ 118
  6.3 Quantum Logical Gates in Qudit-Spaces ...................................... 120
  6.4 Łukasiewicz-Quantum Computational Logics ............................... 124
  References ..................................................................................... 126

7 What Exactly Are Quantum Computations? Classical
   and Quantum Turing Machines ....................................................... 127
  7.1 Introduction .................................................................................. 127
  7.2 Classical Deterministic and Probabilistic Machines ....................... 128
  7.3 Quantum State Machines ............................................................ 131
  7.4 Abstract Quantum Computing Machines .................................... 135
  References ..................................................................................... 138

8 Ambiguity in Natural and Artistic Languages: A Quantum
   Semantic Analysis ........................................................................... 139
  8.1 Introduction .................................................................................. 139
  8.2 Vague Possible Worlds and Metaphors ........................................ 140
  8.3 A Quantum Semantics for Musical Languages .............................. 142
  References ..................................................................................... 149

9 Quantum Information in the Foundational and Philosophical
   Debates About Quantum Theory .................................................... 151
  9.1 Information Interpretations of Quantum Theory ............................ 151
  9.2 The Collapse-Problems .................................................................. 152
  9.3 Determinism, Indeterminism, Realism ......................................... 153
  9.4 A “Quantum Logical Thinking” in Different Fields ....................... 159
  References ..................................................................................... 161

10 Mathematical Survey ........................................................................ 163
  10.1 Introduction .................................................................................. 163
  10.2 Algebraic Concepts ...................................................................... 163
  10.3 Hilbert-Space Concepts ............................................................... 167

Index .................................................................................................. 175
Chapter 1
The Mathematical Environment of Quantum Information

1.1 Physics and Logic in Classical Information Theory

The general idea that inspires all approaches to quantum information is that information can be stored and transmitted by quantum physical systems. Accordingly, any piece of quantum information is identified with a possible state of an appropriate quantum system that is storing the information in question. In this way, the quantum-theoretic formalism for the description of quantum systems becomes the natural mathematical environment for the theories of quantum information and quantum computation.

As is well known, classical information is measured in terms of bits. Consider a single (atomic) question: \( \alpha \) ?, where \( \alpha \) is a sentence expressed in a given language (say, “2 is a prime number”). One assumes that any question of this kind admits two possible answers: “Yes” or “No”. Such answers naturally correspond to the classical truth-values Truth and Falsity. When the answer to the question \( \alpha \) ? is “Yes”, then the sentence \( \alpha \) is supposed to be true; \( \alpha \) is instead false, when the answer is “No”. Intermediate truth-values are not taken into consideration: classical information theory is essentially based on a two-valued semantics (where Truth and Falsity are usually denoted by the natural numbers 1 and 0, respectively). Bits represent the natural “informational counterpart” of classical truth-values. By definition, one bit measures the information-quantity that is determined by the choice of one element from a set \( B \) consisting of two distinct elements. Like in the case of truth-values, it is customary to represent the two bits as the natural numbers 0 and 1 (assuming that \( B = \{0, 1\} \)).

From a physical point of view, bits can be implemented in a number of different ways. For instance, a canonical implementation uses electrical wires with switches. Any switch of a wire can assume two different (concrete) states: either ON or OFF. One can conventionally assume that ON corresponds to the bit 1, while OFF corresponds to the bit 0. In this way, the two bits 1 and 0 can be dealt with as two abstract states that mathematically represent the two concrete states ON and OFF, respectively.

In classical physics dichotomic state-spaces (like \( \{0, 1\} \)) represent special cases that are very simple. Generally, a classical physical system may assume many (possibly infinite) abstract states. An important example is represented by the abstract...
states of a single classical particle $S$ (say, a gas-molecule). In order to have a **complete information** about $S$ (at a given time-instant), six real numbers $r_1, \ldots, r_6$ are necessary and sufficient: $r_1, r_2, r_3$ represent the three position-coordinates, while $r_4, r_5, r_6$ are the three momentum-components. The set $\mathbb{R}^6$ of all sextuplets of real numbers is called the **phase space** of $S$, indicated by $\mathcal{P}h_S$. Any point $s$ of $\mathcal{P}h_S$ represents a possible **pure state**: a complete and maximal information about $S$. When an observer is able to associate to $S$ a pure state $s$, his (her) knowledge about $S$ corresponds to the knowledge that in this connection would have a hypothetical omniscient mind.

How to represent the pure states of a composite system $S$ (say, a gas consisting of $n$ particles)? In such a case it is natural to assume that the phase space $\mathcal{P}h_S$ of $S$ is the cartesian product

$$\mathbb{R}^6 \times \ldots \times \mathbb{R}^6 = \mathbb{R}^{6n}.$$ Accordingly, any point $s$ of $\mathcal{P}h_S = \mathbb{R}^{6n}$ turns out to represent a possible pure state of $S$.

Consider now a classical physical system $S$. The physical properties of $S$ (say, “the velocity of $S$ in the $x$-direction is less than the light’s velocity in vacuum”) correspond to possible **physical events** that can be mathematically represented as subsets $X$ of the phase space $\mathcal{P}h_S$. On this basis, in perfect harmony with classical semantics, the power set of $\mathcal{P}h_S$ can be identified with the set of all possible physical events that may hold for pure states $s$ of $S$. It is natural to assume that:

the system $S$ in the pure state $s$ **verifies** the event $X$ iff $s \in X$.

What about the algebraic structure of physical events? As is well known, the power set of any set gives rise to a **Boolean algebra**. And also the set $\mathcal{M}(\mathcal{P}h_S)$ of all measurable subsets of $\mathcal{P}h_S$ (which is more tractable than the full power set of $\mathcal{P}h_S$ from a measure-theoretic point of view) turns out to have a Boolean structure. Accordingly, one can assume that the “natural” algebraic structure of the physical events that may occur to a classical system $S$ is the following $\sigma$-complete Boolean algebra

$$\mathcal{M}_S = (\mathcal{M}(\mathcal{P}h_S), \cap, \cup, ', \emptyset, \mathcal{P}h_S)$$

(where $'$, $\cap$, $\cup$ are the set-theoretic complement, intersection and union).

As a consequence, one immediately obtains that any pure state $s$ of a system $S$ **semantically decides** any physical event $X$ that belongs to $\mathcal{P}h_S$. We have:

either $s \in X$ or $s \in X'$.

In this sense, classical particle-mechanics is strongly **deterministic**.

---

1. $\mathcal{M}(\mathcal{P}h_S)$ is the smallest subset of the power set of $\mathcal{P}h_S$ that contains all singletons, the total set, the empty set and is closed under the set-theoretic complement, countable intersections, countable unions. For the concepts of **Boolean algebra**, **complete Boolean algebra** and $\sigma$-**complete Boolean algebra** see Definitions 10.8 and 10.4 (in the **Mathematical Survey** of Chap. 10).
The abstract concept of observable (or physical quantity) that can be measured on a system $S$ can be now defined in terms of the notion of physical event.

**Definition 1.1 (Classical observable)** Consider the set $\mathcal{M}(\mathcal{P}h_S)$ of all events that may hold for a system $S$ and let $\mathcal{B}(\mathbb{R})$ be the set of all Borel-sets of real numbers. An observable of $S$ is a map $O$ that satisfies the following conditions:

1. $O : \mathcal{B}(\mathbb{R}) \rightarrow \mathcal{M}(\mathcal{P}h_S)$. For any $\Delta \in \mathcal{B}(\mathbb{R})$, the event $O(\Delta)$ is physically interpreted as follows: the observable $O$ of system $S$ has a value included in the Borel-set $\Delta$.
2. $O(\emptyset) = \emptyset$; $O(\mathbb{R}) = \mathcal{M}(\mathcal{P}h_S)$. Thus, for all pure states the event “having no value for the observable $O$” is impossible, while the event “the value for the observable $O$ is included in $\mathbb{R}$” is certain.
3. $O$ is a $\sigma$-homomorphism from the $\sigma$-complete Boolean algebra based on $\mathcal{B}(\mathbb{R})$ into the $\sigma$-complete Boolean algebra based on $\mathcal{M}(\mathcal{P}h_S)$. Hence:
   - $O(\Delta') = O(\Delta)'$.
   - $O(\bigcap \{\Delta_i\}_{i \in I}) = \bigcap \{O(\Delta_i)\}_{i \in I}$; $O(\bigcup \{\Delta_i\}_{i \in I}) = \bigcup \{O(\Delta_i)\}_{i \in I}$, for any countable set $\{\Delta_i\}_{i \in I}$ of elements of $\mathcal{B}(\mathbb{R})$.

As we have seen, any pure state of a classical system $S$ semantically decides all physical events that may occur to $S$. Of course the information that a human observer has about the system under investigation cannot always correspond to a pure state. In such cases it is useful to refer to special examples of non-maximal pieces of information that are called mixtures (or mixed states). Mathematically, a mixture can be represented as a convex combination of pure states:

$$W = \sum_i w_i s_i,$$

where $w_i$ are positive real numbers (called weights) such that $\sum_i w_i = 1$.

When an observer has associated to a system $S$ the mixture $W = \sum_i w_i s_i$, the intuitive physical interpretation is the following: $S$ might be in the pure state $s_i$ with probability-value $w_i$. In classical physics, a mixture can be regarded as a kind of ignorance of the observer, who does not know which is the “real” pure state of the system. But a hypothetical omniscient mind would always deal with pure states only.

### 1.2 From the Classical to the Quantum-Theoretic Formalism

The transition from classical physics to quantum theory has brought about some deep logical innovations that have not immediately been understood either by the...
logical or by the physical community. As is well known, the basic feature that strongly
distinguishes classical mechanics from quantum theory is the essential indeterminism
that characterizes the quantum world.

We have seen how the pure states of classical physical objects decide all the
relevant properties that may hold for them. If $s$ is a pure state of a classical system $S$
and $X$ is a physical event that may occur to $S$, we have:

$$
either s \in X \text{ or } s \in X'.
$$

Hence $s$ verifies either the event $X$ or its negation $X'$, according to the semantic
excluded-middle principle. The logic of classical physical objects is naturally based
on a two-valued semantics. Such a dichotomic situation breaks down in quantum
theory. The celebrated uncertainty-principles have shown that the pure states of
quantum objects cannot decide all the relevant properties that may hold for them.
Consider a quantum object $S$ (say, an electron) in a pure state that assigns an exact
value to its velocity in the $x$-direction. In such a case, the position of $S$ (with respect
to the $x$-direction) will be completely indeterminate: the object $S$ turns out to be
non-localized. Quantum objects are, in a sense, “poor”; and their “poverty” concerns
the number of physical properties that can be satisfied at the same time. Furthermore,
quantum properties seem to behave in a contextual way: properties that are completely
indeterminate in a given context may become actual and determinate in a different
context (for instance, after the performance of an appropriate measurement). Hence,
the system of properties that are determinate for a given quantum object turns out to
be context-dependent.

As we have seen, the pure states of a classical physical object $S$ represent pieces of
information that are at the same time maximal and logically complete. The information
provided by a pure state cannot be consistently extended to a richer knowledge;
at the same time such information decides all possible events that may occur to $S$.
For this reason the notion of pure state of a classical physical object seems to be
very close to the idea of complete concept, investigated by Leibniz: although many
properties of an individual object (say, the Moon) may be unknown to human minds,
God knows the complete concept of any object (living either in the actual or in
some possible world), and this concept represents a maximal and logically complete
information about the object in question.

Due to the uncertainty-principles complete concepts (in Leibniz’ sense) cannot
exist for quantum objects. Quantum pure states represent pieces of information that
are at the same time maximal (since they cannot be consistently extended to a richer
knowledge) and logically incomplete (since they cannot decide all the relevant prop-
erties of the objects under investigation). This divergence between the concepts of
maximal knowledge and logically complete knowledge represents a characteristic
logical aspect of the quantum world that may appear prima facie strange, since it
is in contrast with a basic theorem of classical logic and of many alternative logics.
As is well known, according to Lindenbaum’s theorem any non-contradictory set of
sentences $T$ can be extended to a set of sentences $T'$ that is at the same time
• non-contradictory (no contradiction can be derived from $T'$);
• logically complete (for any sentence $\alpha$ of the language either $\alpha$ or its negation $\neg\alpha$ belongs to $T'$);
• maximal (all proper extensions of $T'$, formalized in the same language of $T'$, are contradictory).

Apparently, quantum undecidabilities turn out to be much stronger than the syntactical undecidabilities discovered by Gödel’s incompleteness theorems.

### 1.3 The Mathematics of Quantum Theory

The emergence of quantum uncertainties has determined some radical changes in the mathematical representation of physical concepts: quantum pure states and quantum events shall behave differently from their classical counterparts. In quantum theory the role of phase spaces has been replaced by the more sophisticated class of Hilbert spaces, which represent a generalization of the Cartesian plane and of Euclidean spaces. According to the standard axiomatization of quantum theory any quantum physical system $S$ (say, an electron or an atom) is associated to a particular Hilbert space $\mathcal{H}_S$, which represents the mathematical environment for $S$. As happens in the case of classical phase spaces, the possible pure states of $S$ can be mathematically represented as particular points of $\mathcal{H}_S$ that correspond to unit vectors. As is customary, following a happy notation introduced by Paul Dirac, we will indicate the vectors of $\mathcal{H}_S$ by $|\psi\rangle$, $|\varphi\rangle$, $|\chi\rangle$, ... .

The basic properties of a Hilbert space $\mathcal{H}$ can be synthetically sketched as follows$^3$:

1. The set $V_\mathcal{H}$ of the vectors of $\mathcal{H}$ is associated to a division ring that is based either on the set $\mathbb{R}$ of all real numbers or on the set $\mathbb{C}$ of all complex numbers or on the set $\mathbb{Q}$ of all quaternions. The elements of the division ring are called scalars.
2. $\mathcal{H}$ is equipped with an inner product: a map that associates to any pair of vectors $|\psi\rangle$ and $|\varphi\rangle$ a scalar $\langle\psi|\varphi\rangle$.
3. The inner product induces a norm and a metric in $\mathcal{H}$:
   - for any vector $|\psi\rangle$, the norm (or length) of $|\psi\rangle$ is the (real) number $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$;
   - for any vectors $|\psi\rangle$ and $|\varphi\rangle$, the distance $d(|\psi\rangle, |\varphi\rangle)$ is the (real) number $\||\psi\rangle - |\varphi\rangle\|$ (where $-$ is the vector-difference);
   - $\mathcal{H}$ is metrically complete (with respect to the metric determined by $d$): any Cauchy sequence of $\mathcal{H}$ converges to a vector of $\mathcal{H}$.

$^3$For a detailed definition of Hilbert space see Definition 10.20 (in the Mathematical Survey of Chap. 10).
A canonical example of a Hilbert space is represented by the plane $\mathbb{R}^2$, whose vectors are all possible pairs of real numbers and whose division ring is the real field (based on $\mathbb{R}$). Quantum theory normally uses complex Hilbert spaces, whose division ring is the complex field $\mathbb{C}$. The simplest example of a complex Hilbert space (which plays an important role in quantum information) is the space $\mathbb{C}^2$, whose vectors are all possible pairs of complex numbers.

An interesting relation that may hold between two vectors of a Hilbert space is the orthogonality-relation, which is defined in terms of the notion of inner product.

**Definition 1.2 (Orthogonality)** Two vectors $|\psi\rangle$ and $|\varphi\rangle$ of a Hilbert space $H$ are called orthogonal ($|\psi\rangle \perp |\varphi\rangle$) iff the inner product $\langle \psi | \varphi \rangle$ is 0.

From an intuitive point of view the relation $\perp$ can be regarded as a kind of opposition that is generally stronger than the simple inequality-relation. One can prove that in the case of non-null vectors the orthogonality-relation is:

- irreflexive ($|\psi\rangle \not\perp |\psi\rangle$);
- symmetric ($|\psi\rangle \perp |\varphi\rangle \implies |\varphi\rangle \perp |\psi\rangle$);
- generally non-transitive.

All vectors $|\psi\rangle$ of a Hilbert space $H$ can be represented in infinitely many ways as linear combinations of other vectors:

$$|\psi\rangle = \sum_i c_i |\psi_i\rangle,$$

where each $c_i$ is a scalar, while $\sum_i$ represents a (finite or infinite) vector-sum.

Any Hilbert space $H$ has infinitely many orthonormal bases: special sets of vectors that allow us to represent as convenient linear combinations all possible vectors of the space.

**Definition 1.3 (Orthonormal basis)** A set $B$ of vectors of $H$ is called an orthonormal basis for $H$ iff $B$ satisfies the following conditions:

- the elements of $B$ are pairwise orthogonal unit vectors (whose length is 1);
- any vector $|\psi\rangle$ of $H$ can be represented as a linear combination

$$|\psi\rangle = \sum_i c_i |\varphi_i\rangle,$$

where $|\varphi_i\rangle \in B$.

From an intuitive point of view the elements of $B$ can be thought of as a kind of “bricks” that allow us to “construct” all elements of the space by means of scalars and of vector-operations.