Trends in Logic 48

Maria Luisa Dalla Chiara
Roberto Giuntini
Roberto Leporini
Giuseppe Sergioli

# Quantum Computation and Logic

## How Quantum Computers Have Inspired Logical Investigations

Springer

# Trends in Logic

Volume 48

# TRENDS IN LOGIC
*Studia Logica Library*

## 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

Maria Luisa Dalla Chiara
Roberto Giuntini · Roberto Leporini
Giuseppe Sergioli

# Quantum Computation and Logic

## How Quantum Computers Have Inspired Logical Investigations

Springer

Maria Luisa Dalla Chiara
Department of Philosophy
University of Florence
Florence, Italy

Roberto Giuntini
Department of Philosophy
University of Cagliari
Cagliari, Italy

Roberto Leporini
Department of Management, Information and Production Engineering
University of Bergamo
Dalmine, Bergamo, Italy

Giuseppe Sergioli
Department of Philosophy
University of Cagliari
Cagliari, Italy

ISSN 1572-6126 ISSN 2212-7313 (electronic)
Trends in Logic
ISBN 978-3-030-04470-1 ISBN 978-3-030-04471-8 (eBook)
https://doi.org/10.1007/978-3-030-04471-8

Library of Congress Control Number: 2018961691



This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*Dedicated to the memory of David Foulis, Peter Mittelstaedt and Giuliano Toraldo di Francia*

# Preface

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 $\alpha$ 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. 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 — Maria Luisa Dalla Chiara
Cagliari, Italy — Roberto Giuntini
Bergamo, Italy — Roberto Leporini
Cagliari, Italy — Giuseppe Sergioli

# 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

# 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 $\mathscr{B}$ 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 $\mathscr{B} = \{0, 1\}$).

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



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_1

states of a single classical particle $\mathbf{S}$ (say, a gas-molecule). In order to have a *complete information* about $\mathbf{S}$ (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 $\mathbf{S}$, indicated by $\mathscr{P}h_{\mathbf{S}}$. Any point $\mathbf{s}$ of $\mathscr{P}h_{\mathbf{S}}$ represents a possible *pure state*: a *complete and maximal information* about $\mathbf{S}$. When an observer is able to associate to $\mathbf{S}$ a pure state $\mathbf{s}$, his (her) knowledge about $\mathbf{S}$ corresponds to the knowledge that in this connection would have a hypothetical omniscient mind.

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

$$\underbrace{\mathbb{R}^6 \times \ldots \times \mathbb{R}^6}_{n-times} = \mathbb{R}^{6n}.$$

Accordingly, any point $\mathbf{s}$ of $\mathscr{P}h_{\mathbf{S}} = \mathbb{R}^{6n}$ turns out to represent a possible pure state of $\mathbf{S}$.

Consider now a classical physical system $\mathbf{S}$. The physical properties of $\mathbf{S}$ (say, "the velocity of $\mathbf{S}$ in the $\mathbf{x}$-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 $\mathscr{P}h_{\mathbf{S}}$. On this basis, in perfect harmony with classical semantics, the power set of $\mathscr{P}h_{\mathbf{S}}$ can be identified with the set of all possible physical events that may hold for pure states $\mathbf{s}$ of $\mathbf{S}$. It is natural to assume that:

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

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 $\mathscr{M}(\mathscr{P}h_{\mathbf{S}})$ of all *measurable* subsets of $\mathscr{P}h_{\mathbf{S}}$ (which is more tractable than the full power set of $\mathscr{P}h_{\mathbf{S}}$ from a measure-theoretic point of view) turns out to have a Boolean structure.[1] Accordingly, one can assume that the "natural" algebraic structure of the physical events that may occur to a classical system $\mathbf{S}$ is the following $\sigma$-complete Boolean algebra

$$\mathfrak{M}_{\mathbf{S}} = (\mathscr{M}(\mathscr{P}h_{\mathbf{S}}), \cap, \cup, {}', \emptyset, \mathscr{P}h_{\mathbf{S}})$$

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

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

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

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

[1] $\mathscr{M}(\mathscr{P}h_{\mathbf{S}})$ is the smallest subset of the power set of $\mathscr{P}h_{\mathbf{S}}$ 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 $\mathscr{M}(\mathscr{P}h_{\mathbf{S}})$ of all events that may hold for a system **S** and let $\mathscr{B}(\mathbb{R})$ be the set of all Borel-sets of real numbers.[2] An *observable* of **S** is a map $O$ that satisfies the following conditions:

(1) $O : \mathscr{B}(\mathbb{R}) \to \mathscr{M}(\mathscr{P}h_{\mathbf{S}})$. For any $\Delta \in \mathscr{B}(\mathbb{R})$, 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) $O(\emptyset) = \emptyset$; $O(\mathbb{R}) = \mathscr{M}(\mathscr{P}h_{\mathbf{S}})$. 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 $\mathscr{B}(\mathbb{R})$ into the $\sigma$-complete Boolean algebra based on $\mathscr{M}(\mathscr{P}h_{\mathbf{S}})$. 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 $\mathscr{B}(\mathbb{R})$.

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:

$$W = \sum_i w_i \mathbf{s}_i ,$$

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 $W = \sum_i w_i \mathbf{s}_i$, the intuitive physical interpretation is the following: **S** might be in the pure state $\mathbf{s}_i$ 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

[2] $\mathscr{B}(\mathbb{R})$ is the set of all measurable subsets of $\mathbb{R}$.

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:

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

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 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. 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 $\mathcal{H}_{\mathbf{S}}$, 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 $\mathcal{H}_{\mathbf{S}}$ that correspond to unit vectors. As is customary, following a happy notation introduced by Paul Dirac, we will indicate the vectors of $\mathcal{H}_{\mathbf{S}}$ by $|\psi\rangle, |\varphi\rangle, |\chi\rangle, \ldots$ .

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

1. The set $\mathbf{V}_{\mathcal{H}}$ 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 $\mathscr{H}$ 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 $\mathscr{H}$ 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 $\mathscr{H}$ 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 $\mathbf{B}$ of vectors of $\mathscr{H}$ is called an *orthonormal basis* for $\mathscr{H}$ iff $\mathbf{B}$ satisfies the following conditions:

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

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

where $|\varphi_i\rangle \in \mathbf{B}$.

From an intuitive point of view the elements of $\mathbf{B}$ 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.

One can prove that all orthonormal bases of a space $\mathscr{H}$ have the same cardinal number, which may be either finite or infinite. This number determines the *dimension* of $\mathscr{H}$. For instance, both the spaces $\mathbb{R}^2$ and $\mathbb{C}^2$ have dimension two. An important orthonormal basis of the space $\mathbb{C}^2$ is the *canonical basis*, which consists of the following two vectors:

$$|0\rangle = (1, 0), \ \ |1\rangle = (0, 1).$$

Although quantum theory cannot avoid the use of infinite dimensional Hilbert spaces, quantum information and quantum computation normally need finite dimensional spaces only. In such a case, for any choice of an orthonormal basis **B**, any vector $|\psi\rangle$ can be represented as a finite linear combination

$$|\psi\rangle = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle,$$

where $|\psi_1\rangle, \ldots, |\psi_n\rangle$ belong to **B**. Since this book is concerned with logical problems of quantum computation, for the sake of simplicity we will always refer to finite-dimensional Hilbert spaces.

Consider now a pure state $|\psi\rangle$ of a physical system **S** such that

$$|\psi\rangle = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle,$$

where $|\psi_1\rangle, \ldots, |\psi_n\rangle$ belong to a given orthonormal basis **B** of the space $\mathscr{H}_\mathbf{S}$ (associated with **S**). Since the length of all vectors $|\psi\rangle, |\psi_1\rangle, \ldots, |\psi_n\rangle$ is 1, the complex numbers $c_1, \ldots, c_n$ (also called *amplitudes*) shall satisfy the condition:

$$|c_1|^2 + \cdots + |c_n|^2 = 1.$$

In such a case it is customary to say that the pure state $|\psi\rangle$ is a *superposition* of the alternative pure states $|\psi_1\rangle, \ldots, |\psi_n\rangle$. We will see how the concept of superposition (which has no counterpart in classical physics) is responsible for some basic features of quantum theory that have for a long time been regarded as "strange", "mysterious" and "potentially paradoxical".

How to deal in this framework with *quantum events*? A "classical way of thinking" would suggest to identify the set of the quantum events that may occur to a system **S** with the set of all possible sets of pure states of **S**. Such a choice, however, could not adequately represent the peculiar uncertainties that characterize the behavior of quantum pure states: the very notion of *logical negation*, corresponding to the set-theoretic complement-operation $'$, should be transformed and possibly weakened. To this aim a good candidate seems to be the *orthocomplement* (or *orthogonal complement*), which is defined in terms of the orthogonality-relation.

**Definition 1.4** (*Orthocomplement*) For any set $X$ of vectors of a Hilbert space $\mathscr{H}$, the *orthocomplement* $X^\perp$ of $X$ is defined as follows:

$$X^{\perp} := \{|\psi\rangle \in \mathbf{V}_{\mathscr{H}} : \forall|\varphi\rangle \in X(|\psi\rangle \perp |\varphi\rangle)\}.$$

Thus, $X^{\perp}$ is the set of all vectors that are orthogonal to every vector in $X$.

If $X$ is a set of vectors of $\mathscr{H}$, the orthocomplement $X^{\perp}$ is generally a proper subset of the set-theoretic complement $X'$. Consequently, the excluded-middle principle turns out to be violated. For some vectors $|\psi\rangle$ and for some sets of vectors $X$ we may have:

$$|\psi\rangle \notin X \quad \text{and} \quad |\psi\rangle \notin X^{\perp}.$$

An important character of the Hilbert-space scenario is represented by the double orthocomplement of a given set of vectors. The following Lemma sums up some interesting properties of this operation.

**Lemma 1.1** *Let $X$ be a set of vectors of a Hilbert space $\mathscr{H}$.*

*(1)* $X \subseteq X^{\perp\perp}$.
*(2)* $X = X^{\perp\perp}$ *iff* $X$ *is a* closed subspace *of $\mathscr{H}$ (closed under linear combinations and metrically complete).*
*(3)* $X^{\perp\perp\perp} = X^{\perp}$.
*(4)* $|\psi\rangle \in X^{\perp\perp}$ *iff* $\forall|\varphi\rangle \not\perp |\psi\rangle \exists|\chi\rangle \not\perp |\varphi\rangle(|\chi\rangle \in X^{\perp\perp})$.

The nice properties of the sets $X^{\perp\perp}$ have suggested that the closed subspaces of a Hilbert space (which are richer than simple sets) can represent good mathematical representatives for the intuitive notion of *quantum event*.[4]

According to the *projection-theorem*, for any choice of a closed subspace $X$, any vector $|\psi\rangle$ of the space can be uniquely represented as a superposition

$$|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle,$$

where $|\psi_1\rangle \in X$ and $|\psi_2\rangle \in X^{\perp}$. The two vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ can be regarded as the two *components* of $|\psi\rangle$ that belong to the subspaces $X$ and $X^{\perp}$, respectively.

The set $\mathscr{C}(\mathscr{H})$ of all closed subspaces of a Hilbert space $\mathscr{H}$ gives rise to an algebraic structure that (unlike the case of classical physical events) is not a Boolean algebra. Consider the following algebraic structure

$$\mathfrak{C}_{\mathscr{H}} = (\mathscr{C}(\mathscr{H}), \sqcap, \sqcup, {}^{\perp}, \{\mathbf{0}\}, \mathbf{V}_{\mathscr{H}}),$$

where:

(1) $\sqcap$ (the *infimum*) coincides with the set-theoretic intersection $\cap$;
(2) $\sqcup$ (the *supremum*) is defined (in terms of $^{\perp}$ and $\sqcap$) via de Morgan-law:

$$X \sqcup Y := (X^{\perp} \sqcap Y^{\perp})^{\perp};$$

[4] See [3]. After Birkhoff and von Neumann's pioneering work, different abstract approaches to the foundations of quantum mechanics have been proposed. See, for instance, [5, 8, 10, 12, 14, 18, 19, 22, 23, 25].

(3) $^{\perp}$ is the orthocomplement;
(4) $\{\mathbf{0}\}$ is the singleton of the null vector $\mathbf{0}$, while $\mathbf{V}_{\mathscr{H}}$ represents the total closed subspace.

One can prove that $\mathfrak{C}_{\mathscr{H}}$ is a *complete orthomodular lattice*.[5] The subspaces $\{\mathbf{0}\}$ and $\mathbf{V}_{\mathscr{H}}$ represent, respectively, the *minimum* and the *maximum* element with respect to the lattice-partial order that is defined as follows:

$$X \sqsubseteq Y \quad \text{iff} \quad X \sqcap Y = X.$$

Orthomodular lattices $\mathfrak{C}_{\mathscr{H}}$ (based on some Hilbert space $\mathscr{H}$) are also called *Hilbert-space lattices* (briefly, *Hilbert-lattices*). An important Boolean property that is generally violated by Hilbert-lattices is *distributivity*. We may have:

$$X \sqcap (Y \sqcup Z) \not\sqsubseteq (X \sqcap Y) \sqcup (X \sqcap Z).$$

*Orthomodularity* (the characteristic property of orthomodular lattices) represents a special weakening of distributivity that can be formulated as follows:

$$X \sqsubseteq Y \implies Y = X \sqcup (Y \sqcap X^{\perp}).$$

*Example 1.1* Consider the orthomodular lattice based on the set $\mathscr{C}(\mathbb{R}^2)$ of all closed subspaces of the plane. The elements of $\mathscr{C}(\mathbb{R}^2)$ are:

- the singleton of the origin (represented by the null vector $\mathbf{0} = (0, 0)$);
- the total space $\mathbb{R}^2$;
- all straight lines through the origin.

In this case the orthocomplement $X^{\perp}$ of a closed subspace $X$ represented by a straight line $X$ is the straight line (through the origin) that is perpendicular to $X$. In order to "see" the failure of distributivity, take three pairwise non-orthogonal straight lines $X$, $Y$, $Z$ (Fig. 1.1). We have:

$$(X \sqcap Y) \sqcup (X \sqcap Z) = \{\mathbf{0}\}\,; \quad X \sqcap (Y \sqcup Z) = X.$$

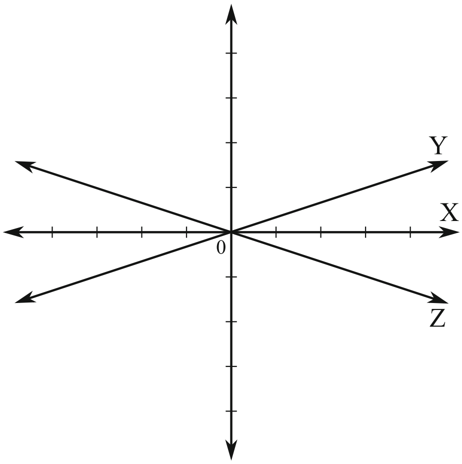
The orthomodular lattice based on the set $\mathscr{C}(\mathscr{H})$ of all closed subspaces of a Hilbert space $\mathscr{H}$ turns out to be isomorphic to a different structure whose support is the set $\mathscr{P}(\mathscr{H})$ of all *projection operators* (briefly, *projections*) $P$ of $\mathscr{H}$.

Let us recall the definition of *projection*, a concept that plays a fundamental role in the quantum-theoretic formalism.

**Definition 1.5** (*Projection*) A *projection* of $\mathscr{H}$ is an operator $P$ that transforms vectors of $\mathscr{H}$ into vectors of $\mathscr{H}$, satisfying the following conditions:

[5] See Definitions 10.7 and 10.4 (in the *Mathematical Survey* of Chap. 10).

**Fig. 1.1** A counterexample to distributivity




(1) $P$ is defined on the total space $\mathbf{V}_{\mathscr{H}}$;
(2) $P$ is *linear*. In other words, $P$ preserves all linear combinations:

$$P(c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle) = c_1 P|\psi_1\rangle + \cdots + c_n P|\psi_n\rangle;$$

(3) $P$ is *idempotent*:

$$PP|\psi\rangle = P|\psi\rangle;$$

(4) $P$ is *self-adjoint*. In other words:

$$P = P^\dagger,$$

where $P^\dagger$ is the *adjoint* of $P$.[6]

The set $\mathscr{P}(\mathscr{H})$ of all projections of a Hilbert space $\mathscr{H}$ is partially ordered by the following relation:

$$P \preccurlyeq Q \;\text{ iff }\; PQ = P.$$

By using the projection-theorem one can naturally define two maps

$$f : \mathscr{C}(\mathscr{H}) \;\to\; \mathscr{P}(\mathscr{H}); \quad g : \mathscr{P}(\mathscr{H}) \;\to\; \mathscr{C}(\mathscr{H})$$

that satisfy the following conditions:

- For any closed subspace $X$, $f(X)$ is the projection $P_X$ such that for any vector $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$ (with $|\psi_1\rangle \in X$ and $|\psi_2\rangle \in X^\perp$) we have:

[6] For the concepts of *adjoint operator* and *self-adjoint operator* see Definitions 10.29 and 10.30 (in the *Mathematical Survey* of Chap. 10).

$$P_X|\psi\rangle = |\psi_1\rangle.$$

Thus $P_X$ transforms $|\psi\rangle$ into its $X$-component.

- For any projection $P$, $g(P)$ is the smallest closed subspace $X_P$ that includes the *range* (the set of all possible values) of $P$.

One can prove that:

$$P_{(X_P)} = P \quad \text{and} \quad X_{(P_X)} = X.$$

Hence, the maps $f$ and $g$ determine a bijection from $\mathscr{C}(\mathscr{H})$ onto $\mathscr{P}(\mathscr{H})$. On this basis one can induce on $\mathscr{P}(\mathscr{H})$ an algebraic structure that turns out to be isomorphic to the orthomodular lattice $\mathfrak{C}_{\mathscr{H}}$. We will indicate this structure by $\mathfrak{P}_{\mathscr{H}}$. Accordingly, the mathematical representatives of quantum events can be equivalently thought of either as closed subspaces (living in the algebra $\mathfrak{C}_{\mathscr{H}}$) or as projections (living in the algebra $\mathfrak{P}_{\mathscr{H}}$).

As we have seen, the semantic excluded-middle principle fails for quantum events. Given a pure state $|\psi\rangle$ and a quantum event represented by the closed subspace $X$ (or by the corresponding projection $P_X$), three cases are possible:

1. $|\psi\rangle \in X$ and $P_X|\psi\rangle = |\psi\rangle$. In such a case one can say that the state $|\psi\rangle$ *certainly verifies* the event represented by $X$ and by $P_X$.
2. $|\psi\rangle \in X^{\perp}$ and $P_{X^{\perp}}|\psi\rangle = |\psi\rangle$. In such a case one can say that the state $|\psi\rangle$ *certainly falsifies* the event represented by $X$ and by $P_X$.
3. $|\psi\rangle \notin X$, $|\psi\rangle \notin X^{\perp}$ and $P_X|\psi\rangle \neq |\psi\rangle$, $P_{X^{\perp}}|\psi\rangle \neq |\psi\rangle$. In such a case one can say that the event represented by $X$ and by $P_X$ is *indeterminate* for the state $|\psi\rangle$.

In spite of a first appearance it would be wrong to conclude that the "natural logic" of quantum events is a three-valued logic. The relation between pure states and quantum events is highly more informative, since it essentially involves quantum probabilities. Given a quantum event represented by a closed subspace $X$ and by the corresponding projection $P_X$, any pure state $|\psi\rangle$ assigns to $X$ and to $P_X$ a probability-value (indicated by $\mathtt{p}_{|\psi\rangle}(X)$ and by $\mathtt{p}_{|\psi\rangle}(P_X)$), which is determined by the *Born-rule*:

$$\mathtt{p}_{|\psi\rangle}(X) = \mathtt{p}_{|\psi\rangle}(P_X) := \| P_X|\psi\rangle \|^2.$$

Thus, the probability that a quantum system in state $|\psi\rangle$ verifies the event represented by $X$ and by $P_X$ is the number $\| P_X|\psi\rangle \|^2$ (the squared length of the $X$-component of $|\psi\rangle$). One can easily show that

$$\mathtt{p}_{|\psi\rangle}(X) = \mathtt{p}_{|\psi\rangle}(P_X) \in [0, 1].$$

One can also show that:

$$\mathtt{p}_{|\psi\rangle}(X) = \mathtt{p}_{|\psi\rangle}(P_X) = \mathtt{tr}(P_{|\psi\rangle} P_X),$$

where:

- $P_{|\psi\rangle}$ is the projection determined by the one-dimensional closed subspace that contains the vector $|\psi\rangle$;
- $\mathtt{tr}$ is the trace-functional.[7]

For any closed subspaces $X$ and $Y$ of $\mathscr{H}$ we have:

$$X \sqsubseteq Y \quad \text{iff} \quad P_X \preccurlyeq P_Y \ \text{ iff for any pure state } \ |\psi\rangle : \mathtt{p}_{|\psi\rangle}(X) \leq \mathtt{p}_{|\psi\rangle}(Y).$$

Hence, the event-partial order turns out to have an interesting physical meaning. As a particular case consider a system **S** in a pure state

$$|\psi\rangle = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle,$$

where all amplitudes $c_i$ are different from 0. According to the Born-rule this system *might* satisfies with probability $|c_i|^2$ the properties that are *certain* for any system whose state is $|\psi_i\rangle$.

Quantum states seem to describe a kind of "cloud of potential properties" that are, in a sense, all co-existent. Interestingly enough, such a co-existence (which may appear *prima facie* strange and mysterious) can be used as a powerful resource for different aims. We will see in the next Chapters how the parallel computational paths of quantum computers are essentially based on superpositions, where alternative states of a quantum object *act* at the same time.

Since the algebraic structure of quantum events is not Boolean, the behavior of the quantum probabilities $\mathtt{p}_{|\psi\rangle}$, determined by the possible pure states of a quantum system, turns out to diverge from the behavior of classical probabilities. At the same time, quantum probabilities satisfy the following conditions (which are similar to some basic properties of classical probabilities):

1. $\mathtt{p}_{|\psi\rangle}(X) \in [0, 1]$ (for every event $X$).
2. $\mathtt{p}_{|\psi\rangle}(\{\mathbf{0}\}) = 0; \ \ \mathtt{p}_{|\psi\rangle}(\mathbf{V}_{\mathscr{H}}) = 1.$
3. $\mathtt{p}_{|\psi\rangle}(X^{\perp}) = 1 - \mathtt{p}_{|\psi\rangle}(X)$ (for every event $X$).
4. Let $\{X_i\}_{i\in I}$ be a countable set of quantum events that are pairwise orthogonal (i.e. $i \neq j \ \Rightarrow \ X_i \subseteq X_j^{\perp}$). We have:

$$\mathtt{p}_{|\psi\rangle}\left(\bigsqcup_i X_i\right) = \sum_i \mathtt{p}_{|\psi\rangle}(X_i).$$

Condition 4. clearly represents a quantum version of $\sigma$-additivity.

The concept of *quantum observable* (or *physical quantity* that can be measured on a quantum system **S**) can be now defined in terms of the notion of *event* (as happens in the case of classical mechanics).

---

[7]The concept of *trace-functional* is defined in Definition 10.34 (in the *Mathematical Survey* of Chap. 10).

**Definition 1.6** (*Quantum observable*) Consider the set $\mathscr{C}(\mathscr{H}_{\mathbf{S}})$ of all events that may hold for a quantum system **S** and let $\mathscr{B}(\mathbb{R})$ be the set of all Borel-sets of real numbers. An *observable* of **S** is a map $O$ that satisfies the following conditions:

(1) $O : \mathscr{B}(\mathbb{R}) \to \mathscr{C}(\mathscr{H}_{\mathbf{S}})$. For any $\Delta \in \mathscr{B}(\mathbb{R})$, the quantum event $O(\Delta) \in \mathscr{C}(\mathscr{H}_{\mathbf{S}})$ is physically interpreted as follows: the observable $O$ of system **S** has a value included in the Borel-set $\Delta$.
(2) $O(\emptyset) = \{\mathbf{0}\}$; $O(\mathbb{R}) = \mathbf{V}_{\mathscr{H}_{\mathbf{S}}}$. 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 $\mathscr{B}(\mathbb{R})$ into the complete orthomodular lattice based on $\mathscr{C}(\mathscr{H}_{\mathbf{S}})$. Hence:

- $O(\Delta') = O(\Delta)^{\perp}$.
- $O(\bigcap\{\Delta_i\}_{i\in I}) = \bigsqcap\{O(\Delta_i)\}_{i\in I}$; $O(\bigcup\{\Delta_i\}_{i\in I}) = \bigsqcup\{O(\Delta_i)\}_{i\in I}$, for any countable set $\{\Delta_i\}_{i\in I}$ of elements of $\mathscr{B}(\mathbb{R})$.

As expected, any observable $O$ can be equivalently defined by referring to the set $\mathscr{P}(\mathscr{H}_{\mathbf{S}})$ (instead of $\mathscr{C}(\mathscr{H}_{\mathbf{S}})$). For this reason, the observables $O$ of a space $\mathscr{H}_{\mathbf{S}}$ are often called *projection-valued measures* (or *spectral measures*).

One can prove that any observable $O$ of $\mathscr{H}_{\mathbf{S}}$ uniquely determines a self-adjoint operator $A_O$ of the space. Conversely, any self-adjoint operator $A$ of $\mathscr{H}_{\mathbf{S}}$ uniquely determines an observable $O_A$. We have:

$$A_{(O_A)} = A \quad \text{and} \quad O_{(A_O)} = O.$$

Hence, the physical quantities that can be measured on a quantum system can be mathematically represented either by projection-valued measures or by self-adjoint operators (as is more customary in many standard axiomatizations of quantum theory).

Consider a quantum system **S** in a state $|\psi\rangle$ and let $O$ be an observable of the space $\mathscr{H}_{\mathbf{S}}$. For any real number $a$, we have:

$$\mathrm{p}_{|\psi\rangle}(O(\{a\})) = 1 \text{ iff } A_O(|\psi\rangle) = a|\psi\rangle.$$

Thus, the event $O(\{a\})$ is *certain* for the system **S** in state $|\psi\rangle$ iff $|\psi\rangle$ is an eigenvector of the self-adjoint operator $A_O$ with corresponding eigenvalue $a$.[8]

So far we have been concerned with pure states, which represent *maximal* pieces of information about the physical systems under investigation. Like classical physics, quantum theory as well cannot avoid the use of *mixed states* (or *mixtures*) that correspond to a *non-maximal* knowledge of the observer.

Quantum mixtures can be represented in a form that is similar to classical mixtures. Let $\mathscr{H}_{\mathbf{S}}$ be the Hilbert space associated to a physical system **S**. Consider an operator of $\mathscr{H}_{\mathbf{S}}$ having the following form:

[8]For the concepts of *eigenvector* and *eigenvalue* see Definition 10.24 (in the *Mathematical Survey* of Chap. 10). Note that all eigenvalues of a self-adjoint operator are real numbers.

$$\rho = w_1 P_{|\psi_1\rangle} + \cdots + w_n P_{|\psi_n\rangle},$$

where $|\psi_1\rangle, \ldots, |\psi_n\rangle$ are possible pure states of **S**, while $w_1, \ldots, w_n$ are positive real numbers such that $w_1 + \cdots + w_n = 1$. Such an operator, which is expressed as a *convex combination* of pure states, represents a possible *mixed state* of **S**: a *mixture* of the pure states $|\psi_1\rangle, \ldots, |\psi_n\rangle$, with *weights* $w_1, \ldots, w_n$. When an observer has associated to **S** the mixed state $\rho$, the physical interpretation is the following: **S**, whose state is $\rho$, *might* be in the pure state $|\psi_i\rangle$ with probability $w_i$.

Any mixture represented as a convex combination $\rho = w_1 P_{|\psi_1\rangle} + \cdots + w_n P_{|\psi_n\rangle}$ (in a Hilbert space $\mathcal{H}$) belongs to a special class of operators called *density operators* of $\mathcal{H}$. This class is properly included in the wider class $\mathcal{B}(\mathcal{H})$ of all *bounded operators* of the space.

**Definition 1.7** (*Bounded operator*) A linear operator $A$ of a Hilbert space $\mathcal{H}$ is called *bounded* iff there exists a positive real number $a$ such that for every vector $|\psi\rangle$ of $\mathcal{H}$:

$$|| \, A|\psi\rangle \, || \leq || \, a|\psi\rangle \, || \, .$$

An important subclass of $\mathcal{B}(\mathcal{H})$ is represented by the class of all *positive operators* of $\mathcal{H}$.

**Definition 1.8** (*Positive operator*) A bounded operator $A$ of a Hilbert space $\mathcal{H}$ is called *positive* iff for every vector $|\psi\rangle$ of $\mathcal{H}$:

$$\langle \psi \mid A\psi \rangle \; \geq \; 0.$$

The concept of *density operator* of $\mathcal{H}$ can be now defined as follows.

**Definition 1.9** (*Density operator*) A *density operator* of a Hilbert space $\mathcal{H}$ is a positive, self-adjoint, trace-class operator $\rho$ such that $\mathtt{tr}(\rho) = 1$.[9]

The set of all density operators of $\mathcal{H}$ will be indicated by $\mathfrak{D}(\mathcal{H})$.

Using the concept of density operator a partial order relation can be defined on the set of all self-adjoint operators of $\mathcal{H}$ as follows:

$$A \preccurlyeq B \;\text{ iff }\; \forall \rho \in \mathfrak{D}(\mathcal{H})[\mathtt{tr}(\rho A) \leq \mathtt{tr}(\rho B)].$$

While any convex combination $w_1 P_{|\psi_1\rangle} + \cdots + w_n P_{|\psi_n\rangle}$ of pure states uniquely determines a density operator, the inverse relation does not hold: generally, a density operator $\rho$ can be represented in many different ways as a convex combination of pure states. Hence, it is convenient to identify the set of all possible *mixed states* of a quantum system **S** with the set $\mathfrak{D}(\mathcal{H}_\mathbf{S})$ of all density operators of the Hilbert

[9]For the concept of *trace-class operator* see Definition 10.33 (in the *Mathematical Survey* of Chap. 10).

space $\mathcal{H}_{\mathbf{S}}$. As expected, pure states correspond to special cases of mixtures that can be represented as projections $P_{|\psi\rangle}$ (where $|\psi\rangle$ is a unit vector of the space). Density operators that cannot be represented in this form are called *proper mixtures*.

The basic probabilistic rule of quantum theory, the *Born-rule*, can be now naturally extended to all states of a physical system **S** (which may be either pure or mixed). Let $\rho$ be a possible state of **S** and let the projection $P \in \mathcal{P}(\mathcal{H}_{\mathbf{S}})$ represent a quantum event. The probability that the system **S** in state $\rho$ verifies the event $P$ is defined as follows:

$$\mathtt{p}_\rho(P) := \mathtt{tr}(\rho P).$$

And we already know that in the case of pure states $|\psi\rangle$ we have:

$$\mathtt{p}_{|\psi\rangle}(P) = ||P|\psi\rangle||^2 = \mathtt{tr}(P_{|\psi\rangle}P).$$

In spite of a superficial formal appearance, mixtures (represented as particular convex combinations) should not be confused with superpositions, whose behavior is essentially different. Consider the following mixture (of the space $\mathbb{C}^2$):

$$\rho = \frac{1}{2}P_{|0\rangle} + \frac{1}{2}P_{|1\rangle} = \frac{1}{2}\mathtt{I}$$

(where $\mathtt{I}$ is the identity operator). Let us compare $\rho$ with the following superposition (which might appear *prima facie* similar):

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

Both states $\rho$ and $|\psi\rangle$ assign the same probability-value to the two events $P_{|0\rangle}$ and $P_{|1\rangle}$ (where $P_{|0\rangle}$ is certain for the state $|0\rangle$, while $P_{|1\rangle}$ is certain for the state $|1\rangle$). We have:

$$\mathtt{p}_{|\psi\rangle}(P_{|0\rangle}) = \mathtt{p}_{|\psi\rangle}(P_{|1\rangle}) = \mathtt{p}_\rho(P_{|0\rangle}) = \mathtt{p}_\rho(P_{|1\rangle}) = \frac{1}{2}.$$

At the same time, the pure state $|\psi\rangle$ certainly verifies its *characteristic* property represented by the event $P_{|\psi\rangle}$. We have:

$$\mathtt{p}_{|\psi\rangle}(P_{|\psi\rangle}) = \|P_{|\psi\rangle}|\psi\rangle\|^2 = \mathtt{tr}(P_{|\psi\rangle}P_{|\psi\rangle}) = 1.$$

The probability-value assigned to the event $P_{|\psi\rangle}$ by the mixture $\rho$ is, instead, $\frac{1}{2}$. For, we have:

$$\mathtt{p}_\rho(P_{|\psi\rangle}) = \mathtt{tr}(\rho P_{|\psi\rangle}) = \frac{1}{2}\mathtt{tr}(P_{|\psi\rangle}) = \frac{1}{2}.$$

Although a pure states $|\psi\rangle$ has many indeterminate properties, there is always at least one non-trivial event (different from the total event represented by the whole space) that is certainly verified by $|\psi\rangle$. Mixtures, instead, give rise to a higher degree of indeterminacy: there are proper mixtures (for instance, the state $\frac{1}{2}\mathtt{I}$ of $\mathbb{C}^2$) for which the total event only is certain.

To what extent is an "ignorance interpretation" of mixtures possible? This is a question that has often been discussed in the foundational debates about quantum theory. Is it reasonable to claim that any quantum system **S** is always in a well-determined pure state, which may be unknown to human observers, but would be perfectly known by a hypothetical omniscient mind? Such an interpretation of quantum mixtures can be hardly defended for many reasons. As we have seen, density operators can be generally represented as convex combinations of pure states in many different ways. How could we choose the "right" representation that determines the "real" pure state of a given system? Another serious difficulty arises in the framework of *entanglement-phenomena* (which will be investigated in Chap. 3). We will see that there are composite quantum systems **S** whose state is *pure and entangled*. This state determines the states of the *parts* of **S**, which are *indistinguishable* and cannot be represented as pure states. While in classical physics mixed states (which are useful for human observers) would never be used by a hypothetical omniscient mind, in quantum theory proper mixtures seem to be in principle unavoidable.

## 1.4 Composite Systems

Quantum physical systems (as well as classical systems) are often *composite systems* consisting of many *parts* (say, an $n$-electron system, a photon-beam, etc.). The mathematical formalism of the theory shall represent the special relations that hold between a possible state of a composite system and the states of its parts.

As we have seen, in classical mechanics the phase space $\mathscr{P}h_{\mathbf{S}}$ of a composite system **S** consisting of $n$ particles $\mathbf{S}_1, \ldots, \mathbf{S}_n$ is identified with the cartesian product of the phase spaces of its parts:

$$\mathscr{P}h_{\mathbf{S}} = \mathscr{P}h_{\mathbf{S}_1} \times \cdots \times \mathscr{P}h_{\mathbf{S}_n} = \underbrace{\mathbb{R}^6 \times \cdots \times \mathbb{R}^6}_{n-times} = \mathbb{R}^{6n}.$$

As a consequence, one can say that the pure states of the parts $(\mathbf{s}_1, \ldots, \mathbf{s}_n)$ determine the pure state

$$\mathbf{s} = \mathbf{s}_1 \times \cdots \times \mathbf{s}_n$$

of the global system **S**. Conversely, any pure state

$$\mathbf{s} = \mathbf{s}_1 \times \cdots \times \mathbf{s}_n$$

of **S** determines the *reduced state* $Red^i(\mathbf{s})$ of each part. We have:

$$Red^i(\mathbf{s}_1 \times \cdots \times \mathbf{s}_n) = \mathbf{s}_i = \Pi_i(\mathbf{s}),$$

where $\Pi_i(\mathbf{s})$ is the projection of $\mathbf{s}_1 \times \cdots \times \mathbf{s}_n$ on its $i$th component.

In quantum theory the essential role of superpositions and the possibility of *entangled* states give rise to a more complicated situation. Cartesian products, which cannot adequately represent the characteristic *holistic* features of quantum composite systems, have been replaced by the more sophisticated *tensor products*.

Let $\mathscr{H}_1$ and $\mathscr{H}_2$ be two Hilbert spaces. Roughly, the tensor product $\mathscr{H}_1 \otimes \mathscr{H}_2$ of $\mathscr{H}_1$ and $\mathscr{H}_2$ can be thought of as the smallest Hilbert space $\mathscr{H}$ (up to isomorphism) that satisfies the following conditions[10]:

- there is an injective map $\otimes$ that associates to every element $(|\psi^{(1)}\rangle, |\varphi^{(2)}\rangle)$ of the cartesian product $\mathbf{V}_{\mathscr{H}_1} \times \mathbf{V}_{\mathscr{H}_2}$ an element $|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle$ of $\mathbf{V}_{\mathscr{H}}$.
- $\mathbf{V}_{\mathscr{H}}$ is closed under all linear combinations of elements that belong to the range of the map $\otimes$.

One can show that $\otimes$ satisfies associativity:

$$\mathscr{H}_1 \otimes (\mathscr{H}_2 \otimes \mathscr{H}_3) = (\mathscr{H}_1 \otimes \mathscr{H}_2) \otimes \mathscr{H}_3.$$

Any vector

$$|\psi\rangle = |\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle$$

is called a *factorized* vector of the space $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$. Vectors of $\mathscr{H}$ that cannot be represented as factorized vectors are called *non-factorizable*. As an example, we can consider the case of a pure state that plays an important role in quantum theory and in quantum information. Let us refer to a composite system $\mathbf{S} = \mathbf{S}_1 + \mathbf{S}_2$, whose Hilbert space is:

$$\mathscr{H}_{\mathbf{S}} = \mathscr{H}_{\mathbf{S}_1} \otimes \mathscr{H}_{\mathbf{S}_2} = \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Consider the following superposition, which represents a possible pure state of $\mathbf{S}$:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle).$$

This state belongs to a class of pure states that are usually called *Bell-states*. According to the Born-rule the superposition $|\psi\rangle$ assigns probability $\frac{1}{2}$ to the two following possibilities:

- the subsystem $\mathbf{S}_1$ is in state $|1\rangle$, while the subsystem $\mathbf{S}_2$ is in state $|0\rangle$;
- the subsystem $\mathbf{S}_1$ is in state $|0\rangle$, while the subsystem $\mathbf{S}_2$ is in state $|1\rangle$.

The distinction between factorizable and non-factorizable states can be naturally extended to mixtures. Let $A$ and $B$ be two linear operators defined on the spaces $\mathscr{H}_1$ and $\mathscr{H}_2$, respectively. One can prove that the pair $(A, B)$ uniquely determines a linear operator $A \otimes B$ of the product-space $\mathscr{H}_1 \otimes \mathscr{H}_2$. As happens in the case of

[10] For a more detailed definition of *tensor product* see Definition 10.37 (in the *Mathematical Survey* of Chap. 10).

vectors, operators that have this form are called *factorized*. A mixed state $\rho$ of the space $\mathscr{H}_1 \otimes \mathscr{H}_2$ is called *factorizable* iff $\rho$ can be represented as a factorized operator $\rho_1 \otimes \rho_2$, where $\rho_1 \in \mathfrak{D}(\mathscr{H}_1)$ and $\rho_2 \in \mathfrak{D}(\mathscr{H}_2)$. Of course, there are density operators of $\mathscr{H}_1 \otimes \mathscr{H}_2$ that are not factorizable.

As happens in classical mechanics, any state of a composite quantum system determines the *reduced states* of all its parts. For the sake of simplicity, let us first consider a *bipartite* system consisting of two parts. In order to define the concept of *reduced state* we will first introduce the notion of *partial trace*. Consider two Hilbert spaces $\mathscr{H}_1$, $\mathscr{H}_2$ and their tensor product $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$. Let $\mathscr{T}(\mathscr{H})$, $\mathscr{T}(\mathscr{H}_1)$, $\mathscr{T}(\mathscr{H}_2)$ represent the sets of all trace-class operators of $\mathscr{H}$, $\mathscr{H}_1$, $\mathscr{H}_2$, respectively. One can prove that there exists a unique linear map

$$PTr_2 \, : \, \mathscr{T}(\mathscr{H}) \, \to \, \mathscr{T}(\mathscr{H}_1)$$

(called the *partial trace of the second component*) that satisfies the following condition for any $A \in \mathscr{T}(\mathscr{H}_1)$ and any $B \in \mathscr{T}(\mathscr{H}_2)$:

$$PTr_2(A \otimes B) = (\mathtt{tr} B)A.$$

In other words, $PTr_2(A \otimes B)$ is an operator of $\mathscr{H}_1$, where:

- $B$ (the component of $A \otimes B$ living in the space $\mathscr{H}_2$) has been "traced out";
- the "memory" of $B$ is preserved in $PTr_2(A \otimes B)$ by means of the number $\mathtt{tr} B$.

In a symmetric way one can determine the map $PTr_1$ (the *partial trace of the first component*).

The concept of partial trace can be now applied to define the two *reduced states* of a bipartite composite system.

**Definition 1.10** (*Reduced state*) Consider a composite system $\mathbf{S} = \mathbf{S}_1 + \mathbf{S}_2$ and its associated Hilbert space $\mathscr{H}_{\mathbf{S}} = \mathscr{H}_{\mathbf{S}_1} \otimes \mathscr{H}_{\mathbf{S}_2}$. Let $\rho$ be a state of $\mathscr{H}_{\mathbf{S}}$. The *reduced state* of $\rho$ with respect to the first subsystem ($Red^1(\rho)$) and the *reduced state* of $\rho$ with respect to the second subsystem ($Red^2(\rho)$) are defined as follows:

$$Red^1(\rho) := PTr_2(\rho); \quad Red^2(\rho) := PTr_1(\rho).$$

One can prove that $Red^1(\rho)$ is a density operator of $\mathscr{H}_1$, while $Red^2(\rho)$ is a density operator of $\mathscr{H}_2$. Moreover:

$$\rho = \rho_1 \otimes \rho_2 \implies Red^1(\rho) = \rho_1, \quad Red^2(\rho) = \rho_2$$

(but not the other way around).

The notion of *reduced state* can be naturally defined for multi-partite systems as well. Let $\mathbf{S} = \mathbf{S}_1 + \cdots + \mathbf{S}_n$ be a composite system whose Hilbert space is the tensor product

$$\mathscr{H}_{\mathbf{S}} = \mathscr{H}_{\mathbf{S}_1} \otimes \cdots \otimes \mathscr{H}_{\mathbf{S}_n}.$$

Any state $\rho$ of $\mathbf{S}$ determines the reduced state $Red^i(\rho)$ of each subsystem $\mathbf{S}_i$.[11]

As an example, consider again the Bell-state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle).$$

We have:

$$Red^1(P_{|\psi\rangle}) = Red^2(P_{|\psi\rangle}) = \frac{1}{2}\mathtt{I}.$$

While the state of the composite system is pure (a maximal piece of information) the reduced state of both subsystems is the proper mixture $\frac{1}{2}\mathtt{I}$, which represents a maximal degree of uncertainty. Hence, the information about the global system seems to be more precise than the information about its parts. Is it possible to "go back" from the information about the *parts* to the information about the *whole*, as happens in the case of classical pure states? The answer to this question is clearly negative. We have:

$$P_{|\psi\rangle} \neq Red^1(P_{|\psi\rangle}) \otimes Red^2(P_{|\psi\rangle}).$$

While $P_{|\psi\rangle}$ is a pure state, $Red^1(P_{|\psi\rangle}) \otimes Red^2(P_{|\psi\rangle})$ is a proper mixture.

In quantum theory the state of a composite system determines the states of its parts, but generally not the other way around. In Chap. 3 we will see how *holistic* situations of this kind play an important role in *entanglement-phenomena*.

## 1.5 Time Evolution and Quantum Measurements

As happens to all physical systems, quantum systems evolve in time. In quantum theory the time-evolution of *isolated* systems is governed by the celebrated Schrödinger's equation: the pure states of systems that evolve in a given time-interval, without any interaction with other systems, are determined by special examples of *unitary operators* that transform pure states into pure states in a reversible way.

**Definition 1.11** (*Unitary operator*) An operator $\mathtt{U}$ of a Hilbert space $\mathscr{H}$ is called *unitary* iff $\mathtt{U}$ satisfies the following conditions:

- $\mathtt{U}$ is defined on the whole space;
- $\mathtt{U}$ is linear;
- $\mathtt{U}\mathtt{U}^\dagger = \mathtt{U}^\dagger\mathtt{U} = \mathtt{I}$.

[11] A more general concept of *reduced state* will be considered in Sect. 2.1

One can show that any unitary operator $\mathtt{U}$ satisfies the following conditions:

(1) $\mathtt{U}$ preserves the inner product:

$$\forall |\psi\rangle, |\varphi\rangle \in \mathbf{V}_{\mathscr{H}} : \langle \mathtt{U}\psi | \, \mathtt{U}\varphi\rangle = \langle \psi | \varphi \rangle.$$

Consequently, $\mathtt{U}$ preserves the length of all vectors, transforming pure states into pure states.

(2) $\mathtt{U}$ is reversible:

$$\mathtt{U}^{-1}\mathtt{U} = \mathtt{U}\mathtt{U}^{-1} = \mathtt{I}.$$

Any unitary operator $\mathtt{U}$ of a space $\mathscr{H}$ can be canonically extended to a *unitary operation* ${}^{\mathfrak{D}}\mathtt{U}$ that transforms the density operators of $\mathscr{H}$ in a reversible way. The operation ${}^{\mathfrak{D}}\mathtt{U}$ is defined for any $\rho \in \mathfrak{D}(\mathscr{H})$ as follows:

$${}^{\mathfrak{D}}\mathtt{U}\rho := \mathtt{U}\rho\mathtt{U}^{\dagger}.$$

The general form of Schrödinger's axiom, based on Schrödinger's equation, can be now formulated as follows.

**Schrödinger's Axiom**

Consider a quantum system $\mathbf{S}$ and let $[t_0, t_1]$ be a time-interval (where either $t_0 \leq t_1$ or $t_1 \leq t_0$). There exists a unitary operator $\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}$ that maps the pure states of $\mathbf{S}$ into pure states of $\mathbf{S}$; for any pure state $|\psi\rangle$, $\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}|\psi\rangle$ represents the state of the system at time $t_1$, provided the system is in state $|\psi\rangle$ at time $t_0$. The map $\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}$ can be extended to mixed states by means of the corresponding unitary operation ${}^{\mathfrak{D}}\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}$.

Since unitary operators are linear, the time-evolution described by Schrödinger's equation generally preserves the uncertainties that characterize the initial state of the system. Suppose the state of $\mathbf{S}$ at time $t_0$ is the superposition

$$|\psi\rangle = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle, \quad \text{where} \;\; c_1 \neq 0, \ldots, c_n \neq 0.$$

At time $t_1$ the state of $\mathbf{S}$ will be:

$$\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}|\psi\rangle = c_1\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}|\psi_1\rangle + \cdots + c_n\mathtt{U}^{\mathbf{S}}_{[t_0,t_1]}|\psi_n\rangle.$$

Thus, events that are indeterminate at the initial time $t_0$ generally remain indeterminate at the final time $t_1$.

Schrödinger's axiom describes the spontaneous evolution of quantum systems that do not interact with an external environment. What happens when a measurement is performed, giving rise to a special kind of interaction between a system $\mathbf{S}$ and an apparatus $\mathbf{A}$, used in the measuring procedure? Consider a system $\mathbf{S}$ whose state is the density operator $\rho$ (in the Hilbert space $\mathscr{H}_{\mathbf{S}}$). Suppose the observer wants to measure on $\mathbf{S}$ an observable $O$ by means of a *non-destructive* measuring procedure.[12] Suppose the result of the measurement is the Borel-set $\Delta$ (possibly, a singleton $\{a\}$). In such a case, the observer has *tested* that the projection $O(\Delta)$ represents a *certain event* for the system **S**. In fact, after we do a measurement and see that the result is in the Borel-set $\Delta$, if we repeat the measurement immediately, we will always get the same result. Consequently, soon after the measurement, it is natural to transform the initial state $\rho$ (for which the event $O(\Delta)$ was possibly indeterminate) into a new state $\rho'$ such that:

$$\mathtt{p}_{\rho'}(O(\Delta)) = 1.$$

Such a state-transformation seems to be justified by a general rational principle according to which we should always take into account the results of experimental evidence. Technically, this idea is realized by another basic axiom of quantum theory, called *collapse* (or *reduction*) *of the wave function* (first proposed by von Neumann and generalized by Lüders).

**von Neumann–Lüders' Axiom**

Suppose the observer measures an observable $O$ on a system **S** during the time-interval $[t_0, t_1]$ by means of a non-destructive measurement procedure. Let $\rho$ represent the state of **S** at the initial time $t_0$. Suppose the result of the measurement is the Borel-set $\Delta$. Then, soon after the measurement, at time $t_1$, the observer will associate to the system the following state:

$$\rho' = \frac{O(\Delta)\rho O(\Delta)}{\mathtt{tr}(\rho O(\Delta))}.$$

One can show that $\rho'$ assigns probability 1 to the event $O(\Delta)$. Hence, the performance of a measurement induces a state-transformation that takes into account the information obtained by the measuring procedure. Synthetically we will also write:

$$\rho \;\mapsto_M\; \rho' = \frac{O(\Delta)\rho O(\Delta)}{\mathtt{tr}(\rho O(\Delta))}.$$

An interesting particular case that may arise when $\rho$ is a pure state is the following:

1. $\rho = P_{|\psi\rangle}$, where $|\psi\rangle = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle$, the vectors $|\psi_1\rangle, \ldots, |\psi_n\rangle$ are elements of a given orthonormal basis and all amplitudes $c_i$ are different from 0;
2. the result of the measurement of $O$ is $\Delta$ and the range of the projection $O(\Delta)$ is a one-dimensional closed subspace;

---

[12] For a long time non-destructive measurements have been considered a highly idealized concept. Interestingly enough, nowadays such "ideal" measurements can be experimentally realized by means of different technologies. For instance, one can manipulate some atoms by lasers and one can investigate their spectral features with high precision by means of optical clocks. In these experiments state-detection plays a crucial role: the fluorescence of an atom under laser-illumination reveals its internal quantum state.

3. $0 < \mathtt{p}_{|\psi\rangle}(O(\Delta)) < 1$ (the event $O(\Delta)$ is indeterminate for $|\psi\rangle$);
4. there is a component $|\psi_i\rangle$ of the superposition $|\psi\rangle$ such that:
   - $\mathtt{p}_{|\psi_i\rangle}(O(\Delta)) = 1$ (the event $O(\Delta)$ is certain for $|\psi_i\rangle$);
   - $\mathtt{p}_{|\psi_j\rangle}(O(\Delta)) < 1$, if $j \neq i$ (the event $O(\Delta)$ is not certain for all $|\psi_j\rangle$ different from $|\psi_i\rangle$).

In such a case, by *collapse of the wave function*, we obtain:

$$P_{|\psi\rangle} \quad \mapsto_M \quad P_{|\psi_i\rangle}.$$

State-transformations $M$ induced by measurements can be mathematically described by means of some special maps, called *quantum operations* (or *quantum channels*), which are defined on the set $\mathscr{B}(\mathscr{H})$ of all bounded operators of a Hilbert space $\mathscr{H}$. Unlike unitary operations, quantum operations are generally irreversible.

**Definition 1.12** (*Quantum operation*) A *quantum operation* (or *quantum channel*) of $\mathscr{H}$ is a linear map

$$\mathfrak{E} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})$$

such that for some set $J$ of indexes there exists a set $\{E_j\}_{j \in J}$ of elements of $\mathscr{B}(\mathscr{H})$ satisfying the following conditions:

(1) $\sum_j E_j^\dagger E_j = \mathtt{I}$;

(2) $\forall A \in \mathscr{B}(\mathscr{H}) : \mathfrak{E}(A) = \sum_j E_j A E_j^\dagger$.

The set $\{E_j\}_{j \in J}$ is also called a *system of Kraus-operators* for $\mathfrak{E}$.[13]

One can prove that quantum operations are trace-preserving; hence quantum states are transformed into quantum states. Of course, any unitary operation ${}^{\mathfrak{D}}\mathtt{U}$ corresponds to a special case of a quantum operation, but generally not the other way around. Furthermore, unlike unitary operations, quantum operations do not generally preserve pure states.

The conjunction between Schrödinger's axiom and von Neumann–Lüders' axiom gives rise to a conflictual situation and to potentially contradictory consequences, if the apparatus **A** (used in the measuring procedure) is dealt with as a quantum system that may belong to the *universe of discourse* of quantum theory. In such a case it is natural to investigate the behavior of the composite system **S** + **A**, whose states shall live in the product-space $\mathscr{H}_\mathbf{S} \otimes \mathscr{H}_\mathbf{A}$ (where $\mathscr{H}_\mathbf{S}$ is the space of the system **S**, while $\mathscr{H}_\mathbf{A}$ is the space of the apparatus **A**). The intriguing question that arises in this situation is the following: how do the states of such a composite system evolve in time? Shall

[13] This definition is based on the so-called *Kraus' first representation theorem* (See [20]). It is worthwhile recalling that in the literature one can also find a different definition of *quantum operation*, where condition (1) ($\sum_j E_j^\dagger E_j = \mathtt{I}$) is replaced by the weaker condition: $\mathtt{tr}(\rho \sum_j E_j^\dagger E_j) \leq 1$, for every $\rho \in \mathfrak{D}(\mathscr{H})$. In such a case, quantum operations are not trace-preserving. At the same time, *quantum channels* are defined as quantum operations that satisfy the stronger condition $\sum_j E_j^\dagger E_j = \mathtt{I}$.

we apply Schrödinger's equation or von Neumann–Lüders' collapse of the wave function? Actually, both choices seem to be reasonable from an intuitive point of view. The global system $\mathbf{S} + \mathbf{A}$ can be regarded as an isolated system that evolves in time according to Schrödinger's equation. At the same time, it is also reasonable to apply von Neumann–Lüders' axiom, since a measurement is performed on the system $\mathbf{S}$ by means of the apparatus $\mathbf{A}$ (during a given time-interval $[t_0, t_1]$). In such a situation it is natural to assume that the observable $O$ (measured on $\mathbf{S}$ by $\mathbf{A}$) is correlated with a corresponding observable $O^{\mathbf{A}}$ of the apparatus $\mathbf{A}$. The values of $O^{\mathbf{A}}$ can be represented by possible positions of a *pointer*.

Suppose now that at the initial time $t_0$ the system $\mathbf{S}$ is in the following pure state

$$|\psi\rangle^{\mathbf{S}}(t_0) = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle,$$

where $n > 1$ and all amplitudes $c_i$ are different from 0. Accordingly, the state of the global system $\mathbf{S} + \mathbf{A}$ can be represented as the following factorized state:

$$|\Psi\rangle^{\mathbf{S+A}}(t_0) = (c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle) \otimes |\varphi\rangle^{\mathbf{A}}(t_0),$$

where $|\varphi\rangle^{\mathbf{A}}(t_0)$ is a state of $\mathbf{A}$ that assigns probability 1 to the initial position of the pointer. Suppose the outcome of the measurement performed by $\mathbf{A}$ for the observable $O$ is the Borel-set $\Delta$. This means that at the final time $t_1$ (after the measurement-performance) the apparatus $\mathbf{A}$ shall be in a state $|\varphi\rangle^{\mathbf{A}}(t_1)$ that assigns probability 1 to the pointer-position corresponding to the value $\Delta$ for the observable $O$. Suppose that the event $O(\Delta)$ was indeterminate for the initial state of the system

$$|\psi\rangle^{\mathbf{S}}(t_0) = c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle,$$

while for some component $|\psi_i\rangle$ we have:

$$\mathtt{p}_{|\psi_i\rangle}(O(\Delta)) = 1 \quad \text{and} \quad \mathtt{p}_{|\psi_j\rangle}(O(\Delta)) < 1 \quad \text{for all} \quad |\psi_j\rangle \quad \text{different from} \quad |\psi_i\rangle.$$

By applying von Neumann–Lüders' axiom to the global system, we will obtain the following final factorized state:

$$|\Psi\rangle^{\mathbf{S+A}}(t_1) = |\psi_i\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_1).$$

Accordingly, we can write:

$$(c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle) \otimes |\varphi\rangle^{\mathbf{A}}(t_0) \quad \mapsto_M \quad |\psi_i\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_1).$$

The observer has "learnt" from the final state of the apparatus that the event $O(\Delta)$ is *certain* for system $\mathbf{S}$.

Does this result coincide with what is predicted by Schrödinger's equation? In other words, is it possible to describe the state-transformation

$$(c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle) \otimes |\varphi\rangle^{\mathbf{A}}(t_0) \quad \mapsto_M \quad |\psi_i\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_1)$$

by means of a unitary operator $\mathtt{U}^{\mathbf{S+A}}_{[t_0,t_1]}$? The answer to this question is generally negative. Since unitary operators are linear, we would obtain:

$$\mathtt{U}^{\mathbf{S+A}}_{[t_0,t_1]}[(c_1|\psi_1\rangle + \cdots + c_n|\psi_n\rangle) \otimes |\varphi\rangle^{\mathbf{A}}(t_0)] =$$

$$c_1\mathtt{U}^{\mathbf{S+A}}_{[t_0,t_1]}(|\psi_1\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_0)) + \cdots + c_n\mathtt{U}^{\mathbf{S+A}}_{[t_0,t_1]}(|\psi_n\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_0)).$$

And this state is generally different from the factorized state

$$|\psi_i\rangle \otimes |\varphi\rangle^{\mathbf{A}}(t_1).$$

The conflict between the predictions of Schrödinger's equation and of von Neumann–Lüder's axiom is usually called "the quantum-measurement problem", which represents the most serious logical difficulty of quantum mechanics.[14] After von Neumann's pioneering investigations, different foundational approaches to the theory have proposed different possible solutions.

In the next Chapters we will see how both Schrödinger's equation and von Neumann–Lüder's axiom play an important role for understanding the behavior of quantum computers.

## 1.6 The Unsharp Approaches to Quantum Theory

An important question that arises in the investigations about the quantum-theoretic formalism is the following: given a quantum system $\mathbf{S}$ (associated to a Hilbert space $\mathscr{H}_\mathbf{S}$), to what extent is the set $\mathscr{P}(\mathscr{H}_\mathbf{S})$ of all projections of $\mathscr{H}_\mathbf{S}$ the "best" mathematical representative for the intuitive concept of *event* that may occur to $\mathbf{S}$? Are there any other operators of $\mathscr{H}_\mathbf{S}$ for which a Born-probability could be reasonably defined? This question has a positive answer. Consider the set $\mathscr{E}(\mathscr{H}_\mathbf{S})$ of all self-adjoint operators $E$ of $\mathscr{H}_\mathbf{S}$ that satisfy the following condition:

$$\forall \rho \in \mathfrak{D}(\mathscr{H}_\mathbf{S}) : \ \mathtt{tr}(\rho E) \in [0, 1].$$

The elements of the set $\mathscr{E}(\mathscr{H}_\mathbf{S})$ are usually called *effects* of the space $\mathscr{H}_\mathbf{S}$.[15] Apparently, any state $\rho$ of $\mathscr{H}_\mathbf{S}$ assigns to any effect $E \in \mathscr{E}(\mathscr{H}_\mathbf{S})$ a probability-value according to the Born-rule. Hence, like in the projection-case, we can put:

$$\mathtt{p}_\rho(E) := \mathtt{tr}(\rho E).$$

---

[14] See [2, 4, 26, 27].

[15] See [1, 5–7, 9–11, 13, 15, 16, 21].

One can easily show that $\mathscr{P}(\mathscr{H}_{\mathbf{S}})$ is a proper subset of $\mathscr{E}(\mathscr{H}_{\mathbf{S}})$: any projection is an effect, but not the other way around. For instance, the operator $\frac{1}{2}\mathtt{I}$ (of the space $\mathbb{C}^2$) is an effect that is not a projection.

The following Lemma asserts a characteristic property of effects.

**Lemma 1.2** *A self-adjoint operator A of a Hilbert space $\mathscr{H}_{\mathbf{S}}$ is an effect iff A satisfies the following condition for any vector $|\psi\rangle$ of $\mathscr{H}_{\mathbf{S}}$:*

$$0 \leq \langle\psi|A\psi\rangle \leq \||\psi\rangle\|^2.$$

Since effects are self-adjoint operators, the set $\mathscr{E}(\mathscr{H}_{\mathbf{S}})$ turns out to be partially ordered by the relation $\preccurlyeq$:

$$E \preccurlyeq F \text{ iff } \forall\rho \in \mathfrak{D}(\mathscr{H}_{\mathbf{S}})(\mathtt{tr}(\rho E) \leq \mathtt{tr}(\rho F)).$$

Consequently, we obtain:

$$E \preccurlyeq F \text{ iff } \forall\rho \in \mathfrak{D}(\mathscr{H}_{\mathbf{S}})(\mathtt{p}_\rho(E) \leq \mathtt{p}_\rho(F)).$$

Thus, the partial order $\preccurlyeq$ has a natural physical meaning: an effect $E$ *precedes* an effect $F$ when all states assign to $E$ a probability-value that is less than or equal to the probability-value assigned to $F$.

One can prove that $\mathscr{E}(\mathscr{H}_{\mathbf{S}})$ coincides with the set of all self-adjoint operators $A$ of $\mathscr{H}_{\mathbf{S}}$ that satisfy the following condition:

$$\mathtt{O} \preccurlyeq A \preccurlyeq \mathtt{I},$$

where $\mathtt{O}$ and $\mathtt{I}$ are the null projection and the identity operator of $\mathscr{H}_{\mathbf{S}}$, respectively.

Unlike the case of projections, the partial order $\preccurlyeq$ does not determine a lattice-structure. Some pairs of effects have no *infimum*, as shown by the following example.

*Example 1.2* Consider the following effects of the Hilbert space $\mathbb{C}^2$:

$$E|0\rangle = \frac{1}{2}|0\rangle; \quad E|1\rangle = \frac{1}{2}|1\rangle;$$

$$F|0\rangle = \frac{3}{4}|0\rangle; \quad F|1\rangle = \frac{1}{4}|1\rangle;$$

$$G|0\rangle = \frac{1}{2}|0\rangle; \quad G|1\rangle = \frac{1}{4}|1\rangle.$$

It is not hard to see that $G \preccurlyeq E, F$. Suppose, by contradiction, that the infimum $L = E \sqcap F$ exists in $\mathscr{E}(\mathbb{C}^2)$. An easy computation shows that $L$ must be equal to $G$. Consider now the following effect:

$$M|0\rangle = \frac{7}{16}|0\rangle + \frac{1}{8}|1\rangle; \;\; M|1\rangle = \frac{1}{8}|0\rangle + \frac{3}{16}|1\rangle.$$

We have: $M \preccurlyeq E, F$; however $M \not\preccurlyeq L$, which is a contradiction.

An orthocomplement-like operation can be naturally defined on the set $\mathscr{E}(\mathscr{H}_S)$ in the following way:

$$\forall E \in \mathscr{E}(\mathscr{H}_S) : E^{\perp} := \mathtt{I} - E.$$

This operation turns out to correspond to the standard orthocomplement in the particular case of effects that are projections. For, any projection $P$ satisfies the property:

$$P^{\perp} = \mathtt{I} - P.$$

On this basis, the *orthogonality-relation* between effects can be defined as follows:

$$E \perp F \text{ iff } E \preccurlyeq F^{\perp}.$$

As expected, this relation turns out to coincide with the standard orthogonality-relation in the case of projections.

The structure $(\mathscr{E}(\mathscr{H}_S), \preccurlyeq)$ can be enriched in different ways giving rise to different kinds of algebraic structures, which have been investigated in a rich literature.[16] Effects and projections have a different behavior with respect to contradictions. The orthomodular lattice based on the set of all projections of a Hilbert space $\mathscr{H}_S$ satisfies the non-contradiction principle. The conjunction between an event $P$ and its negation $P^{\perp}$ is always the *impossible* event (the null projection $\mathtt{O}$):

$$P \sqcap P^{\perp} = \mathtt{O}.$$

At the same time, proper effects may violate this basic logical principle. We may have:

$$E \sqcap E^{\perp} \neq \mathtt{O}.$$

Hence, contradictions are not necessarily impossible. As an example consider the proper effect $\frac{1}{2}\mathtt{I}$ of the space $\mathbb{C}^2$. We have:

$$\frac{1}{2}\mathtt{I} \sqcap \frac{1}{2}\mathtt{I}^{\perp} = \frac{1}{2}\mathtt{I} \sqcap \frac{1}{2}\mathtt{I} = \frac{1}{2}\mathtt{I} \neq \mathtt{O}.$$

From an intuitive point of view projections can be regarded as mathematical representatives of *sharp* physical events, for which contradictions are always impossible. Effects, instead, can naturally represent *unsharp* or *fuzzy* events that are basically ambiguous. One obtains in this way two different forms of *uncertainty* for

[16]The simplest structures are represented by *effect algebras*, special examples of partial algebras (Definition 10.10 in the *Mathematical Survey* of Chap. 10). See, for instance, [9–11, 13, 15, 16].

quantum events. We can try to illustrate this difference by using a non-scientific example. Consider the following two sentences, which apparently have no definite truth-value:

1. Hamlet is 1.70 m tall;
2. Brutus is an honourable man.

The semantic uncertainty involved in the first example seems to depend on the logical incompleteness of the *individual concept* associated to the name "Hamlet": while the property "being 1.70 m tall" is a *sharp* property, our concept of Hamlet is not able to *decide* whether such a property is satisfied or not. Unlike real persons, literary characters have a number of indeterminate properties. On the contrary, the semantic uncertainty involved in the second example is mainly caused by the ambiguity of the concept "honourable". What does it mean "being honourable"? One need only recall how the ambiguity of the adjective "honourable" plays an important role in the famous Mark Antony's monologue in Shakespeare's *Julius Caesar*.

The mathematical and physical behavior of *unsharp quantum events* has been deeply investigated by the *unsharp approaches to quantum theory*.[17] In this framework the concept of *quantum observable* can be defined as an *effect-valued measure*:

$$O : \mathscr{B}(\mathbb{R}) \ \rightarrow \ \mathscr{E}(\mathscr{H}_{\mathbf{S}}),$$

which maps Borel-sets of real numbers into effects (instead of projections). An interesting advantage of this approach is the possibility of representing as a "genuine" observable the *joint observable* of two *incompatible* physical quantities (like *position* and *momentum*), which is generally forbidden in standard quantum theory.

## 1.7 Quantum Logics

The mathematical structures that arise in the quantum theoretic formalism have inspired the development of different forms of non-classical logics, termed *quantum logics*. The prototypical example of quantum logic is Birkhoff and von Neumann's quantum logic (first proposed in their celebrated article "The logic of quantum mechanics"). This logic (which will be indicated by $\mathbf{QL^{BN}}$) represents a natural logical abstraction from the class of all Hilbert-lattices:

$$\mathfrak{C}_{\mathscr{H}} = (\mathscr{C}(\mathscr{H}),\, \sqcap,\, \sqcup,\, ^{\perp},\, \{\mathbf{0}\}\,,\, \mathbf{V}_{\mathscr{H}}).$$

Consider a sentential language $\mathscr{L}$ with atomic sentences and the following logical connectives: $\neg$ (negation), $\wedge$ (conjunction), $\vee$ (disjunction). A *model* of $\mathscr{L}$ (in the Birkhoff and von Neumann's semantics) can be defined as a pair

[17] See, for instance, [1, 4, 10, 11, 24].

$$(\mathfrak{C}_{\mathscr{H}}, val),$$

where $\mathfrak{C}_{\mathscr{H}}$ is a Hilbert-lattice, while *val* is an interpretation-function that assigns to any sentence a *meaning* represented by a quantum event $X$ in $\mathfrak{C}_{\mathscr{H}}$. The map *val* shall preserve the logical form of all sentences, satisfying the following conditions (for any sentences $\alpha$, $\beta$ of $\mathscr{L}$):

$$val(\neg\alpha) = val(\alpha)^{\perp};\;\; val(\alpha \wedge \beta) = val(\alpha) \sqcap val(\beta);\;\; val(\alpha \vee \beta) = val(\alpha) \sqcup val(\beta).$$

On this basis one can define the concepts of *truth*, *logical truth* and *logical consequence* (for the Birkhoff and von Neumann's semantics).

**Definition 1.13** *Truth* Let $\mathscr{M} = (\mathfrak{C}_{\mathscr{H}}, val)$ be a model of $\mathscr{L}$.

(1) A sentence $\alpha$ is called *true* for a state $\rho$ of $\mathscr{H}$ (abbreviated as $\vDash_\rho \alpha$) iff $\mathtt{p}_\rho(val(\alpha)) = 1$.
(2) A sentence $\alpha$ is called *true* in the model $\mathscr{M}$ (abbreviated as $\vDash_{\mathscr{M}} \alpha$) iff $val(\alpha)$ is the whole space $\mathbf{V}_{\mathscr{H}}$ (hence, for all states $\rho$ of $\mathscr{H}$: $\mathtt{p}_\rho(val(\alpha)) = 1$).

**Definition 1.14** (*Logical truth and logical consequence*)

(1) A sentence $\alpha$ is called a *logical truth* of the logic $\mathbf{QL^{BN}}$ (abbreviated as $\vDash_{\mathbf{QL^{BN}}} \alpha$) iff $\alpha$ is true in any model $\mathscr{M}$.
(2) $\beta$ is called a *logical consequence* of $\alpha$ in the logic $\mathbf{QL^{BN}}$ (abbreviated as $\alpha \vDash_{\mathbf{QL^{BN}}} \beta$) iff for any model $\mathscr{M} = (\mathfrak{C}_{\mathscr{H}}, val)$, $val(\alpha) \sqsubseteq val(\beta)$ (hence, for all states $\rho$ of $\mathscr{H}$: $\mathtt{p}_\rho(val(\alpha)) \le \mathtt{p}_\rho(val(\beta))$).

It is interesting to recall some important logical truths and logical arguments that hold in the logic $\mathbf{QL^{BN}}$:

1. $\alpha \vDash_{\mathbf{QL^{BN}}} \neg\neg\alpha$; $\neg\neg\alpha \vDash_{\mathbf{QL^{BN}}} \alpha$ (the double-negation principle).
2. $\vDash_{\mathbf{QL^{BN}}} \neg(\alpha \wedge \neg\alpha)$ (the non-contradiction principle).
3. $\vDash_{\mathbf{QL^{BN}}} \alpha \vee \neg\alpha$ (the excluded-middle principle).
4. $\alpha \wedge \neg\alpha \vDash_{\mathbf{QL^{BN}}} \beta$ (Duns Scotus' law: *ex absurdo sequitur quodlibet*).
5. $\alpha \vDash_{\mathbf{QL^{BN}}} \beta$ iff $\neg\beta \vDash_{\mathbf{QL^{BN}}} \neg\alpha$ (contraposition).
6. $(\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \vDash_{\mathbf{QL^{BN}}} \alpha \wedge (\beta \vee \gamma)$ (weak distributivity).

As expected, a characteristic classical argument that is generally violated in Birkhoff and von Neumann's quantum logic is the strong distributivity principle. We have:

$$\alpha \wedge (\beta \vee \gamma) \nvDash_{\mathbf{QL^{BN}}} (\alpha \wedge \beta) \vee (\alpha \wedge \gamma).$$

Interestingly enough, the validity of the logical excluded-middle principle does not imply the semantic *tertium non datur* (for any sentence $\alpha$, either $\alpha$ or its negation $\neg\alpha$ is true in any model $\mathscr{M}$). While any sentence whose form is $\alpha \vee \neg\alpha$ is true in any model, there are sentences $\gamma$ that are semantically indeterminate in some models $\mathscr{M}$, where (unlike classical models) we may have:

$$\nvDash_{\mathscr{M}} \gamma \quad \text{and} \quad \nvDash_{\mathscr{M}} \neg\gamma.$$

The divergence between the *logical excluded-middle principle* ($\vDash_\rho \alpha \vee \neg\alpha$, for any state $\rho$) and the *semantic excluded-middle* (either $\vDash_\rho \alpha$ or $\vDash_\rho \neg\alpha$, for any state $\rho$) is a peculiar feature of quantum logic.

The models of Birkhoff and von Neumann's quantum logic have a direct physical meaning, since they are based on Hilbert lattices. From a logical point of view it is interesting to consider a convenient abstract generalization of Hilbert lattices, by referring to the variety of all orthomodular lattices (which includes Hilbert lattices as particular cases). In this way, one can semantically characterize a different form of quantum logic (also called *abstract quantum logic*), whose models are based on orthomodular lattices.[18] This logic (indicated by **QL**) does not represent a "faithful" generalization of Birkhoff and von Neumann's quantum logic, because some equations that hold in all Hilbert lattices are possibly violated in the variety of all orthomodular lattices.[19] While **QL** is an axiomatizable logic, the axiomatizability of Birkhoff and von Neumann's quantum logic is still an open problem.

New forms of quantum logics have been suggested by the unsharp approaches to quantum theory. As expected, these logics (called *unsharp quantum logics*) represent fuzzy versions of quantum logic, where the non-contradiction principle, the logical excluded-middle and Duns Scotus' law are possibly violated.

Both sharp and unsharp quantum logics seem to be characterized by some "static" features. Their basic aim 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 operations that are generally irreversible and do not reflect any time-evolution either of the physical system under investigation or of the observer.

Quantum information and quantum computation have inspired a completely different approach to quantum logic, giving rise to new forms of logics that have been termed *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.

The next Chapter will be devoted to a synthetic description of the main abstract characters of the quantum computational game.

## References

1. Beltrametti, E., Bugajski, S.: Effect algebras and statistical physical theories. J. Math. Phys. **53**(38), 3020–3030 (1997)
2. Beltrametti, E., Cassinelli, G.: The Logic of Quantum Mechanics. Encyclopedia of Mathematics and its Applications, vol. 15. Addison-Wesley, Cambridge (1981)

[18] See, for instance, [10].

[19] An example is represented by the *orthoarguesian law*. See [10, 17].

3. Birkhoff, G., von Neumann, J.: The logic of quantum mechanics. Ann. Math. **37**(4), 823–843 (1936)
4. Busch, P., Lahti, P., Mittelstaedt, P.: The Quantum Theory of Measurement. Springer, Heidelberg (1996)
5. Cattaneo, G.: A unified framework for the algebra of unsharp quantum mechanics. Int. J. Theor. Phys. **36**, 3085–3117 (1997)
6. Cattaneo, G., Gudder, S.P.: Algebraic structures arising in axiomatic unsharp quantum physics. Found. Phys. **29**(10), 1607–1637 (1999)
7. Cattaneo, G., Laudisa, F.: Axiomatic unsharp quantum theory (from Mackey to Ludwig). Found. Phys. **24**(5), 631–683 (1994)
8. Chiribella, G., D'Ariano, G.M., Perinotti, P.: Quantum Theory from First Principles: An Informational Approach. Cambridge University Press, Cambridge (2017)
9. Dalla Chiara, M.L., Giuntini, R.: Unsharp quantum logics. Found. Phys. **24**, 1161–1177 (1994)
10. Dalla Chiara, M.L., Giuntini, R., Greechie, R.: Reasoning in Quantum Theory: Sharp and Unsharp Quantum Logics. Kluwer, Dordrecht (2004)
11. Dvurečenskij, A., Pulmannová, S.: New Trends in Quantum Structures. Kluwer, Dordrecht (2000)
12. Foulis, D.J.: A half-century of quantum logic, what have we learned? In: Aerts, D., Pykacz, J. (eds.) Quantum Structures and the Nature of Reality, vol. 7, pp. 1–36. Kluwer, Dordrecht (1999)
13. Foulis, D.J., Bennett, M.K.: Effect algebras and unsharp quantum logics. Found. Phys. **24**(10), 1325–1346 (1994)
14. Foulis, D.J., Greechie, R., Dalla Chiara, M.L., Giuntini, R.: Quantum Logic. In: Trigg, G. (ed.) Encyclopedia of Applied Physics, vol. 15, pp. 229–255. VCH Publishers, Weinheim (1996)
15. Giuntini, R.: Quantum MV algebras. Studia Logica **56**(3), 393–417 (1996)
16. Giuntini, R., Greuling, H.: Toward an unsharp language for unsharp properties. Found. Phys. **19**(7), 931–945 (1989)
17. Greechie, R.: A non-standard quantum logic with a strong set of states. In: Beltrametti, E., van Fraassen, B.C. (eds.) Current Issues in Quantum Logic. Plenum, New York (1981)
18. Gudder, S.P.: A survey of axiomatic quantum mechanics. In: Hooker, C.A. (ed.) The Logico-Algebraic Approach to Quantum Mechanics, vol. II, pp. 323–363. Reidel, Dordrecht (1979)
19. Jauch, J.M.: Foundations of Quantum Mechanics. Addison-Wesley, London (1968)
20. Kraus, K.: States, Effects and Operations. Springer, Berlin (1983)
21. Ludwig, G.: Foundations of Quantum Mechanics. Springer, Berlin (1983)
22. Mackey, G.: The Mathematical Foundations of Quantum Mechanics. Benjamin, New York (1957)
23. Mittelstaedt, P.: Quantum Logic. Reidel, Dordrecht (1978)
24. Mittelstaedt, P.: Rational Reconstruction of Modern Physics. Springer, Heidelberg (2011)
25. Piron, C.: Foundations of Quantum Physics. W.A. Benjamin, Reading (1976)
26. von Neumann, J.: Mathematische Grundlagen der Quantenmechanik. Springer, Berlin (1932)
27. von Neumann, J.: Mathematical Foundations of Quantum Theory. Princeton University Press, Princeton (1996)

# Chapter 2
# Pieces of Quantum Information and Quantum Logical Gates

## 2.1 Qubits, Quregisters and Mixtures of Quregisters

The "mathematical stages" where pieces of quantum information are usually supposed to live are special examples of finite-dimensional Hilbert spaces whose general form is:

$$\mathscr{H}^{(n)} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n-times} \ \text{(where } \ n \geq 1).$$

The dimension of $\mathscr{H}^{(n)}$ is, obviously, $2^n$.

Any space $\mathscr{H}^{(n)}$ can be decomposed in different ways as

$$\mathscr{H}^{(n)} = \mathscr{H}_1^{(m_1)} \otimes \cdots \otimes \mathscr{H}_r^{(m_r)},$$

where $m_1 + \cdots + m_r = n$. Accordingly, any density operator $\rho$ of $\mathscr{H}^{(n)}$ can be regarded as a possible state of a composite system

$$\mathbf{S} = \mathbf{S}_1 + \cdots + \mathbf{S}_r$$

(where $\mathscr{H}^{(m_i)}$ is the Hilbert space associated to the subsystem $\mathbf{S}_i$).

Consider now a particular subsystem of $\mathbf{S}$:

$$\mathbf{S}_{i_1} + \cdots + \mathbf{S}_{i_k} \ \text{(with } \ 1 \leq i_1, \ldots, i_k \leq r).$$

We will indicate by

$$Red^{(i_1,\ldots,i_k)}_{[m_1,\ldots,m_r]}(\rho)$$

the reduced state of $\rho$ with respect to the subsystem $\mathbf{S}_{i_1} + \cdots + \mathbf{S}_{i_k}$ and with respect to the decomposition $\mathscr{H}^{(n)} = \mathscr{H}_1^{(m_1)} \otimes \cdots \otimes \mathscr{H}_r^{(m_r)}$. By simplicity we will omit the subscript $[m_1, \ldots, m_r]$ in the cases where the decomposition of $\mathscr{H}^{(n)}$ is obvious.


M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_2

In the simplest situations a piece of quantum information can be stored by the pure state of a single quantum system, associated to the Hilbert space $\mathscr{H}^{(1)} = \mathbb{C}^2$. Such a state is called a *qubit-state* (briefly, a *qubit*).[1] Accordingly, any qubit $|\psi\rangle$ can be represented as a superposition of the two elements of the canonical basis of $\mathbb{C}^2$:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle.$$

From an intuitive point of view, the concept of *qubit* can be regarded as a quantum variant of the classical concept of *bit*: any pure state $c_0|0\rangle + c_1|1\rangle$ represents a *probabilistic information* that might be *false* with probability-value $|c_0|^2$ and might be *true* with probability-value $|c_1|^2$ (according to the Born-rule). The two vectors $|0\rangle$ and $|1\rangle$ play, in this framework, the role of the two classical bits.

In more complex situations pieces of quantum information are represented by *quregisters*: pure states of composite systems (consisting of $n$ parts), whose associated Hilbert space is $\mathscr{H}^{(n)}$. Accordingly, any quregister $|\psi\rangle$ can be represented as a superposition:

$$|\psi\rangle = \sum_i c_i |x_{i_1}, \ldots, x_{i_n}\rangle,$$

where $x_{i_1}, \ldots, x_{i_n} \in \{0, 1\}$ and $|x_{i_1}, \ldots, x_{i_n}\rangle$ (an abbreviation for $|x_{i_1}\rangle \otimes \cdots \otimes |x_{i_n}\rangle$) is an element of the canonical basis of $\mathscr{H}^{(n)}$, representing, in this framework, a classical *register*.

More generally, pieces of quantum information (which may correspond to a *non-maximal knowledge*) can be represented as *mixtures of quregisters*: density operators $\rho$ of a Hilbert space $\mathscr{H}^{(n)}$.

One can usefully generalize to registers the distinction that holds between a *true bit* ($|1\rangle$) and a *false bit* ($|0\rangle$). The basic idea is that for any register $|\psi\rangle = |x_1, \ldots, x_n\rangle$, the last bit $|x_n\rangle$ determines the truth-value of $|\psi\rangle$.[2]

**Definition 2.1** (*True and false registers*) Let $|x_1, \ldots, x_n\rangle$ be a register of $\mathscr{H}^{(n)}$.

- $|x_1, \ldots, x_n\rangle$ is called *true* iff $x_n = 1$;
- $|x_1, \ldots, x_n\rangle$ is called *false* iff $x_n = 0$.

On this basis one can identify in any space $\mathscr{H}^{(n)}$ two special projections that represent the *Truth-property* and the *Falsity-property* (respectively) for all pieces of quantum information living in $\mathscr{H}^{(n)}$.

---

[1] In the literature the term "qubit" is sometimes used in an ambiguous sense. Usually "qubit" means "pure state of a single particle" (say, an electron or a photon): a mathematical object living in the space $\mathbb{C}^2$. In some cases the term "qubit" is also used as an expression that refers to the particle itself. One says, for instance: "take a qubit in the pure state $|\psi\rangle$".

[2] In the next Section we will see how this convention plays an important role in the definitions of some basic logical gates, where the last bit of an input-register represents the *target* that is transformed by the gate in question into the final truth-value of the output.

**Definition 2.2** (*Truth and Falsity*) Consider a Hilbert space $\mathcal{H}^{(n)}$.

- The *Truth-property* of $\mathcal{H}^{(n)}$ is the projection $P_1^{(n)}$ whose range is the smallest closed subspace that contains all true registers of $\mathcal{H}^{(n)}$.
- The *Falsity-property* of $\mathcal{H}^{(n)}$ is the projection $P_0^{(n)}$ whose range is the smallest closed subspace that contains all false registers of $\mathcal{H}^{(n)}$.

In this way *Truth* and *Falsity* are dealt with as two special examples of *quantum events* to which any (pure or mixed) state $\rho$ of the space assigns a probability-value according to the Born-rule. For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$ we have:

$$\mathtt{p}_\rho(P_1^{(n)}) = \mathtt{tr}(\rho P_1^{(n)}); \;\; \mathtt{p}_\rho(P_0^{(n)}) = \mathtt{tr}(\rho P_0^{(n)}).$$

Apparently, $\mathtt{p}_\rho(P_1^{(n)})$ represents the probability that the information stored by a quantum system in state $\rho$ is true. In the following we will briefly write: $\mathtt{p}_1(\rho)$, instead of $\mathtt{p}_\rho(P_1^{(n)})$. In the case of pure states we will also write: $\mathtt{p}_1(|\psi\rangle)$, instead of $\mathtt{p}_1(P_{|\psi\rangle})$.

The probability-function $\mathtt{p}_1$ allows us to define a natural pre-order relation $\preceq$ on the set $\mathfrak{D} = \bigcup_n \mathfrak{D}(\mathcal{H}^{(n)})$ of all possible pieces of quantum information.[3]

**Definition 2.3** (*The pre-order relation*) Consider two density operators $\rho, \sigma \in \mathfrak{D}$.

$$\rho \preceq \sigma \quad \text{iff} \quad \mathtt{p}_1(\rho) \leq \mathtt{p}_1(\sigma).$$

Thus, the information $\rho$ *precedes* the information $\sigma$ iff the probability of $\rho$ is less than or equal to the probability of $\sigma$. In the case of pure states we will also write: $|\psi\rangle \preceq |\varphi\rangle$, instead of $P_{|\psi\rangle} \preceq P_{|\varphi\rangle}$. One can easily check that the relation $\preceq$ is reflexive and transitive, but generally non-antisymmetric. We have, for instance:

$$|0,1\rangle \preceq |1,1\rangle; \;\; |1,1\rangle \preceq |0,1\rangle; \;\; |0,1\rangle \neq |1,1\rangle.$$

A *probabilistic equivalence-relation* $\cong$ between two pieces of quantum information can be then defined in the expected way.

**Definition 2.4** (*The probabilistic equivalence*) Consider two density operators $\rho, \sigma \in \mathfrak{D}$.

$$\rho \cong \sigma \quad \text{iff} \quad \rho \preceq \sigma \;\text{ and }\; \sigma \preceq \rho.$$

In the case of pure states we will also write: $|\psi\rangle \cong |\varphi\rangle$, instead of $P_{|\psi\rangle} \cong P_{|\varphi\rangle}$.

In the next Chapters we will see how the relations $\preceq$ and $\cong$ will play an important role in the development of the quantum computational semantics.

[3]Of course, the pre-order relation $\preceq$ (defined on the set of all density operators) should not be confused with the partial order $\preccurlyeq$ (defined on the set of all self-adjoint operators).

## 2.2 Quantum Logical Gates

The basic idea of the theory of quantum computers is that computations can be performed by some quantum objects that evolve in time. As we have seen in Chap. 1, according to Schrödinger's equation the time-evolution of quantum systems is described by unitary operators. Thus, it is natural to assume that quantum information is processed by *quantum logical gates* (briefly, *gates*): special examples of unitary operators that transform (in a reversible way) the pure states of the quantum systems that store the information in question.[4] As expected, any gate $\mathtt{G}^{(n)}$ (defined on the space $\mathscr{H}^{(n)}$) can be extended to a unitary operation ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ (defined on the set $\mathfrak{D}(\mathscr{H}^{(n)})$ of all density operators of $\mathscr{H}^{(n)}$) according to the rule:

$$\forall \rho \in \mathfrak{D}(\mathscr{H}^{(n)}) : \ {}^{\mathfrak{D}}\mathtt{G}^{(n)}\rho = \mathtt{G}^{(n)}\rho\,\mathtt{G}^{(n)\dagger}.$$

For the sake of simplicity, we will call *gate* either a unitary operator $\mathtt{G}^{(n)}$ or the corresponding unitary operation ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$.

We will now give the definitions of some basic gates that play an important role both from the computational and from the logical point of view. We will first consider some gates, called "semiclassical", that cannot "create" superpositions from register-inputs. The simplest example is the *trivial* gate, represented by the identity operator $\mathtt{I}^{(n)}$ that transforms every vector of a space $\mathscr{H}^{(n)}$ into itself. Other gates that are computationally important (for instance, in the network-design for quantum computers) are the *swap-gates*.

**Definition 2.5** (*The swap-gates on the space* $\mathscr{H}^{(n)}$) For any $n \geq 1$ and any $j, k$ such that $1 \leq j \leq k \leq n$, the *swap-gate* $\mathtt{Swap}^{(n)}_{j,k}$ on $\mathscr{H}^{(n)}$ is the linear operator that satisfies the following condition for every element $|x_1, \ldots, x_n\rangle$ of the canonical basis:

$$\mathtt{Swap}^{(n)}_{j,k}|x_1, \ldots, x_j, \ldots, x_k, \ldots, x_n\rangle := |x_1, \ldots, x_k, \ldots, x_j, \ldots, x_n\rangle.$$

Thus, $\mathtt{Swap}^{(n)}_{j,k}$ permutes the $j$th bit with the $k$th bit of the input-register. Of course, we have: $\mathtt{Swap}^{(n)}_{j,k} = \mathtt{I}^{(n)}$, when $j = k$. One can prove that $\mathtt{Swap}^{(n)}_{j,k}$ is a unitary operator.

We will now introduce three gates that have a special logical interest: the *negation-gate*, the $\mathtt{XOR}$-*gate* and the *Toffoli-gate*.

**Definition 2.6** (*The negation-gate on the space* $\mathscr{H}^{(1)}$) The *negation-gate* on $\mathscr{H}^{(1)}$ is the linear operator $\mathtt{NOT}^{(1)}$ that satisfies the following condition for every element $|x\rangle$ of the canonical basis:

$$\mathtt{NOT}^{(1)}|x\rangle := |1 - x\rangle.$$

[4] See [2, 3, 5–9, 11].

One can prove that $\mathtt{NOT}^{(1)}$ is a unitary operator.

The gate $\mathtt{NOT}^{(1)}$ represents a natural quantum generalization of the classical negation. We have:

$$\mathtt{NOT}^{(1)}|0\rangle = |1\rangle; \;\; \mathtt{NOT}^{(1)}|1\rangle = |0\rangle.$$

When applied to "genuine" qubits, $\mathtt{NOT}^{(1)}$ behaves as follows:

$$\mathtt{NOT}^{(1)}(c_0|0\rangle + c_1|1\rangle) = c_1|0\rangle + c_0|1\rangle,$$

inverting the amplitudes of the two bits that occur in the superposition.

The negation-gate can be naturally generalized to higher-dimensional spaces. For any $\mathscr{H}^{(n)}$ (with $n > 1$), the operator $\mathtt{NOT}^{(n)}$ is defined for every element $|x_1, \ldots, x_n\rangle$ of the canonical basis as follows:

$$\mathtt{NOT}^{(n)}|x_1, \ldots, x_n\rangle := (\mathtt{I}^{(n-1)} \otimes \mathtt{NOT}^{(1)})|x_1, \ldots, x_n\rangle.$$

Apparently, $\mathtt{NOT}^{(n)}$ always acts on the last bit of any register of $\mathscr{H}^{(n)}$.

**Definition 2.7** (*The* XOR-*gate on the space* $\mathscr{H}^{(2)}$) The XOR-*gate* on $\mathscr{H}^{(2)}$ is the linear operator $\mathtt{XOR}^{(1,1)}$ that satisfies the following condition for every element $|x, y\rangle$ of the canonical basis:

$$\mathtt{XOR}^{(1,1)}|x, y\rangle := |x, x\hat{+}y\rangle,$$

where $\hat{+}$ is the addition modulo 2.

One can prove that $\mathtt{XOR}^{(1,1)}$ is a unitary operator.

From a logical point of view it is natural to "read" the XOR-gate as a *reversible exclusive disjunction* ( "aut" in Latin). For, we have:

- $\mathtt{XOR}^{(1,1)}|x, y\rangle = |x, 1\rangle \iff (x = 1$ and $y = 0)$ or $(x = 0$ and $y = 1)$;
- $\mathtt{XOR}^{(1,1)}|x, y\rangle = |x, 0\rangle \iff (x = y = 1)$ or $(x = y = 0)$.

Thus, the second bit of the output corresponds to the truth-value of the exclusive disjunction.

At the same time, the XOR-gate can be also "read" as a "controlled negation". Consider a possible input $|x, y\rangle$ of the gate. The first bit $|x\rangle$ is called the *control-bit*, while the second bit $|y\rangle$ represents the *target-bit*. Consider the output: $\mathtt{XOR}^{(1,1)}|x, y\rangle = |x, x\hat{+}y\rangle$. The control-bit has remained unchanged, while the input-target has been transformed into the output-target $|x\hat{+}y\rangle$. We have:

- $\mathtt{XOR}^{(1,1)}|1, y\rangle = |1\rangle \otimes \mathtt{NOT}^{(1)}|y\rangle$;
- $\mathtt{XOR}^{(1,1)}|0, y\rangle = |0, y\rangle$.

When the control-bit is $|1\rangle$, the target-bit is transformed into its negation. Accordingly, one can say that $\mathtt{XOR}^{(1,1)}$ describes a *controlled negation* (also called "$\mathtt{C} - \mathtt{NOT}$ gate").

As happens in the case of the negation-gate, the XOR-gate can be naturally generalized to higher-dimensional spaces. In any space $\mathscr{H}^{(m+n)}$ such that $m > 1$ or $n > 1$, the operator $\mathtt{XOR}^{(m,n)}$ is defined for every element $|x_1, \ldots, x_m, y_1, \ldots, y_n\rangle$ of the canonical basis as follows:

$$\mathtt{XOR}^{(m,n)}|x_1, \ldots, x_m, y_1, \ldots, y_n\rangle :=$$

$$(\mathtt{I}^{(m+n-2)} \otimes \mathtt{XOR}^{(1,1)})\, \mathtt{Swap}^{(m+n)}_{m,\, m+n-1}\, |x_1, \ldots, x_m, y_1, \ldots, y_n\rangle.$$

Notice that $\mathtt{XOR}^{(m,n)}$ permutes the two bits $x_m$ and $y_{n-1}$ of the input-register. Consequently, $x_m$ and $y_n$ turn out to be *adjacent* before the application of the $\mathtt{XOR}^{(1,1)}$-gate. In the next Section we will see how the permutations determined by the Swap-gates are useful in the circuit-representation of gates. Defining all gates $\mathtt{XOR}^{(m,n)}$ in terms of $\mathtt{XOR}^{(1,1)}$ turns out to be natural and economical for physical implementations, where one and the same apparatus implementing $\mathtt{XOR}^{(1,1)}$ can be used for any choice of a pair $(m, n)$.[5]

As an example consider the gate $\mathtt{XOR}^{(2,2)}$ (defined on the space $\mathscr{H}^{(4)}$) and take the following input:

$$|x_1, x_2, y_1, y_2\rangle = |1, 1, 0, 0\rangle.$$

We have:

$$\mathtt{XOR}^{(2,2)}|1, 1, 0, 0\rangle = (\mathtt{I}^{(2)} \otimes \mathtt{XOR}^{(1,1)})\, \mathtt{Swap}^{(4)}_{2,3}\, |1, 1, 0, 0\rangle =$$

$$(\mathtt{I}^{(2)} \otimes \mathtt{XOR}^{(1,1)})\, |1, 0, 1, 0\rangle = |1, 0, 1, 1\rangle.$$

Of course, two different choices of a pair $(m, n)$ such that $m + n = t$ determine two different XOR-gates, both defined on the space $\mathscr{H}^{(t)}$.

**Definition 2.8** (*The Toffoli-gate on the space* $\mathscr{H}^{(3)}$) The *Toffoli-gate* on $\mathscr{H}^{(3)}$ is the linear operator $\mathtt{T}^{(1,1,1)}$ that satisfies the following condition for every element $|x, y, z\rangle$ of the canonical basis:

---

[5] It is worth-while recalling a standard definition (that can be found in the literature) of a generalized *controlled negation* in any space $\mathscr{H}^{(t)}$ (with $t > 2$). Let $i, j$ be two different indexes such that $1 \leq i, j \leq t$ and suppose that $x_i$ represents the control-bit, while $x_j$ is the target-bit. The gate $\mathtt{C-NOT}^{(t,i,j)}$ is defined for any register of $\mathscr{H}^{(t)}$ as follows:

$$\mathtt{C-NOT}^{(t,i,j)}|x_1, \ldots, x_t\rangle := |x_1, \ldots, x_{j-1}, x_i \hat{+} x_j, x_{j+1}, \ldots, x_t\rangle.$$

Consider now the gate $\mathtt{XOR}^{(m,n)}$, with $m + n = t$. We obtain:
$\mathtt{C-NOT}^{(t,m,m+n)}|x_1, \ldots, x_m, y_1, \ldots, y_n\rangle = \mathtt{Swap}^{(t)}_{(m,m+n-1)}\mathtt{XOR}^{(m,n)}|x_1, \ldots, x_m, y_1, \ldots, y_n\rangle =$ $|x_1, \ldots, x_m, y_1, \ldots, y_{n-1}, x_m \hat{+} y_n\rangle$. Notice that, for the sake of simplicity, in our definition of $\mathtt{XOR}^{(m,n)}$ we have avoided to apply twice the Swap-gate (in order to obtain the output $|x_1, \ldots, x_m, y_1, \ldots, y_{n-1}, x_m \hat{+} y_n\rangle$). As we will see in the next Chapters, the order of the control-bits in a XOR-output will not play any significant role in the logical applications.

$$\mathtt{T}^{(1,1,1)}|x, y, z\rangle := |x, y, ((x \cdot y) \hat{+} z)\rangle.$$

One can prove that $\mathtt{T}^{(1,1,1)}$ is a unitary operator.

We obtain:

$$\mathtt{T}^{(1,1,1)}|x, y, 0\rangle = |x, y, x \sqcap y\rangle; \quad \mathtt{T}^{(1,1,1)}|x, y, 1\rangle = |x, y, (x \sqcap y)'\rangle$$

(where $\sqcap$ and $'$ are the *infimum* and the *complement* of the two-valued Boolean algebra based on the set $\{0, 1\}$).

The gate $\mathtt{T}^{(1,1,1)}$ is also called *controlled controlled negation* ("$\mathtt{CC} - \mathtt{NOT}$ gate"). Given an input $|x, y, z\rangle$, the first two bits $|x\rangle$ and $|y\rangle$ are dealt with as the control-bits, while the third bit $|z\rangle$ represents the target. We have:

- $\mathtt{T}^{(1,1,1)}|x, y, z\rangle = |x, y\rangle \otimes \mathtt{NOT}^{(1)}|z\rangle$, if $x = y = 1$;
- $\mathtt{T}^{(1,1,1)}|x, y, z\rangle = |x, y, z\rangle$, if $x \neq 1$ or $y \neq 1$.

Thus, the target-bit $|z\rangle$ is transformed into its negation $\mathtt{NOT}^{(1)}|z\rangle$, when both the control-bits $|x\rangle$ and $|y\rangle$ are the bit $|1\rangle$.

The following Theorem determines a useful canonical representation for the gate $\mathtt{T}^{(1,1,1)}$.

**Theorem 2.1**

$$\mathtt{T}^{(1,1,1)} = [(\mathtt{I}^{(2)} - (P_1^{(1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)}] + [P_1^{(1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}].$$

*Proof* Consider a register $|x, y, z\rangle$ of $\mathscr{H}^{(3)}$.

1. Let $x = y = 1$. Then,

$$[(\mathtt{I}^{(2)} - (P_1^{(1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)}]|x, y, z\rangle = \mathbf{0} \text{ (where } \mathbf{0} \text{ is the null vector).}$$

Hence,

$$\left\{[(\mathtt{I}^{(2)} - (P_1^{(1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)}] + [P_1^{(1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}]\right\}|x, y, z\rangle =$$

$$[P_1^{(1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}]|x, y, z\rangle = |x, y\rangle \otimes \mathtt{NOT}^{(1)}|z\rangle = \mathtt{T}^{(1,1,1)}|x, y, z\rangle.$$

2. Let $x \neq 1$ or $y \neq 1$. Then,

$$[P_1^{(1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}]|x, y, z\rangle = \mathbf{0}.$$

Hence,

$$\left\{[(\mathtt{I}^{(2)} - (P_1^{(1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)}] + [P_1^{(1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}]\right\} |x, y, z\rangle =$$

$$[(\mathtt{I}^{(2)} - (P_1^{(1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)}]|x, y, z\rangle = |x, y, z\rangle = \mathtt{T}^{(1,1,1)}|x, y, z\rangle.$$

□

As happens in the case of the negation-gate and the XOR-gate, the Toffoli-gate can be generalized to higher-dimensional spaces. In any space $\mathscr{H}^{(m+n+1)}$ such that $m > 1$ or $n > 1$, the operator $\mathtt{T}^{(m,n,1)}$ is defined for every element $|x_1, \ldots, x_m, y_1, \ldots, y_n, z\rangle$ of the canonical basis of as follows:

$$\mathtt{T}^{(m,n,1)}|x_1, \ldots, x_m, y_1, \ldots, y_n, z\rangle :=$$

$$(\mathtt{I}^{(m+n-2)} \otimes \mathtt{T}^{(1,1,1)})\, \mathtt{Swap}^{(m+n+1)}_{m,m+n-1}\, |x_1, \ldots, x_m, y_1, \ldots, y_n,\ z\rangle.$$

Notice $\mathtt{T}^{(m,n,1)}$ permutes the two bits $x_m$ and $y_{n-1}$ (as happens in the definition of $\mathtt{XOR}^{(m,n)}$).[6]

As an example consider the case where $m = n = 2$ and take the following input (in the space $\mathscr{H}^{(5)}$):

$$|x_1, x_2, y_1, y_2,\ z\rangle = |1, 1, 0, 1, 0\rangle.$$

We have:

$$\mathtt{T}^{(2,2,1)}|1, 1, 0, 1, 0\rangle = (\mathtt{I}^{(2)} \otimes \mathtt{T}^{(1,1,1)})\, \mathtt{Swap}^{(5)}_{2,3}\, |1, 1, 0, 1, 0\rangle =$$

$$(\mathtt{I}^{(2)} \otimes \mathtt{T}^{(1,1,1)})\, |1, 0, 1, 1, 0\rangle = |1, 0, 1, 1, 1\rangle.$$

[6]Like in the case of the XOR-gate it may be useful to recall a standard definition of a generalized *controlled controlled negation* in any space $\mathscr{H}^{(t)}$ (with $t > 3$). Let $i, j, k$ be three different indexes such that $1 \le i, j, k \le t$ and suppose that $x_i$ and $x_j$ represent the control-bits, while $x_k$ is the target-bit. The gate $\mathtt{CC}-\mathtt{NOT}^{(t,i,j,k)}$ is defined for any register of $\mathscr{H}^{(t)}$ as follows:

$$\mathtt{CC}-\mathtt{NOT}^{(t,i,j,k)}|x_1, \ldots, x_t\rangle := |x_1, \ldots, x_{k-1}, (x_i \cdot x_j \hat{+} x_k), x_{k+1}, \ldots, x_t\rangle.$$

Consider now the gate $\mathtt{T}^{(m,n,1)}$, with $m + n + 1 = t$. We obtain:
$\mathtt{CC}-\mathtt{NOT}^{(t,m,m+n,m+n+1)}|x_1, \ldots, x_m, y_1, \ldots, y_n, z\rangle =$
$\mathtt{Swap}^{(t)}_{(m,m+n-1)}\mathtt{T}^{(m,n,1)}|x_1, \ldots, x_m, y_1, \ldots, y_n, z\rangle = |x_1, \ldots, x_m, y_1, \ldots, y_n, (x_m \cdot y_n \hat{+} z)\rangle.$
Notice that (like in the case of $\mathtt{XOR}^{(m,n)}$) in our definition of $\mathtt{T}^{(m,n,1)}$ we have avoided to apply twice the Swap-gate. The possibility of defining $\mathtt{XOR}^{(m,n)}$ in terms of $\mathtt{C}-\mathtt{NOT}^{(t,i,j)}$ and $\mathtt{T}^{(m,n,1)}$ in terms of $\mathtt{CC}-\mathtt{NOT}^{(t,i,j,k)}$ shows that an explicit reference to the swap-gate, although convenient, is not strictly necessary.

Of course, two different choices of a pair $(m, n)$ such that $m + n = t$ determine two different Toffoli-gates, both defined on the space $\mathcal{H}^{(t)}$.

The Toffoli-gate represents a very "powerful" gate that allows us to define *reversible* versions of all Boolean functions.[7] As is well known, in classical semantics the *logical negation* is interpreted as a reversible truth-function. At the same time, the operations that correspond to the basic binary connectives (*conjunction*, *disjunction*, *material implication*, etc.) are usually defined as irreversible operations, by means of appropriate *truth-tables* that refer to the two-valued Boolean algebra $(\{0, 1\}, \sqcap, \sqcup, {}', 0, 1)$. There is, however, an easy "trick" that allows us to transform any irreversible operation into a reversible one. To this aim it is sufficient to "preserve the memory" of the arguments that belong to the operation-inputs. Consider, for instance, a binary Boolean function $f$ (say, the *infimum* $\sqcap$):

$$f : \{0, 1\}^2 \rightarrow \{0, 1\}.$$

A reversible version of $f$ can be defined as a map

$$f^R : \{0, 1\}^3 \rightarrow \{0, 1\}^3$$

such that for every input $(x, y)$ of $f$:

$$f^R(x, y, a) = (x, y, f(x, y) \hat{+} a),$$

where $a$ is a particular element of the domain of $f$, which plays the conventional role of an *ancilla*. In particular, if $a = 0$ we obtain:

$$f(x, y) = \Pi_3(f^R(x, y, 0)) = \Pi_3(x, y, f(x, y))$$

(where $\Pi_3$ is the projection on the third component).

Such a "trick" is systematically used in quantum computation in order to represent as reversible operators some operations that are usually dealt with as irreversible either in classical semantics or in classical computation. Interesting examples are the definitions of a *reversible conjunction* and of a *reversible negative conjunction* in terms of the Toffoli-gate. For any choice of two natural numbers $m, n$ (such that $m, n \geq 1$) the reversible conjunction $\mathtt{AND}^{(m,n)}$ (the reversible negative conjunction $\mathtt{NAND}^{(m,n)}$) is dealt with as a *holistic* monadic operator that acts on *global* pieces of quantum information, represented by quregisters of the space $\mathcal{H}^{(m+n)}$. Accordingly, any quregister of $\mathcal{H}^{(m+n)}$ can be regarded as a *holistic description* of two possible members of the conjunction $\mathtt{AND}^{(m,n)}$ (of the negative conjunction $\mathtt{NAND}^{(m,n)}$), which live in the space $\mathcal{H}^{(m)}$ and $\mathcal{H}^{(n)}$, respectively.

**Definition 2.9** (*The conjunction on the space* $\mathcal{H}^{(m+n)}$) For any quregister $|\psi\rangle$ of $\mathcal{H}^{(m+n)}$,

---

[7]See [13].

$$\mathtt{AND}^{(m,n)}|\psi\rangle := \mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |0\rangle)$$

(where the bit $|0\rangle$ plays the role of an *ancilla*).

**Definition 2.10** (*The negative conjunction on the space $\mathscr{H}^{(m+n)}$*) For any quregister $|\psi\rangle$ of $\mathscr{H}^{(m+n)}$,

$$\mathtt{NAND}^{(m,n)}|\psi\rangle := \mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |1\rangle)$$

(where the bit $|1\rangle$ plays the role of an *ancilla*).

Notice that $\mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |0\rangle)$ and $\mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |1\rangle)$ are two quregisters of the space $\mathscr{H}^{(m+n+1)}$, while $|\psi\rangle$ is a quregister of $\mathscr{H}^{(m+n)}$. Accordingly, $\mathtt{AND}^{(m,n)}|\psi\rangle$ and $\mathtt{NAND}^{(m,n)}|\psi\rangle$ can be dealt with as two abbreviations for $\mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |0\rangle)$ and for $\mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |1\rangle)$, respectively.

In the case of mixed input-states $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$ we will write:

- ${}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)$ for ${}^{\mathfrak{D}}\mathtt{T}^{(m,n,1)}(\rho \otimes P_0^{(1)})$;
- ${}^{\mathfrak{D}}\mathtt{NAND}^{(m,n)}(\rho)$ for ${}^{\mathfrak{D}}\mathtt{T}^{(m,n,1)}(\rho \otimes P_1^{(1)})$,

where ${}^{\mathfrak{D}}\mathtt{T}^{(m,n,1)}$ is the unitary quantum operation that corresponds to the unitary operator $\mathtt{T}^{(m,n,1)}$.

As a particular case, consider a register $|x, y\rangle$ of the space $\mathscr{H}^{(2)}$.
We obtain:

- $\mathtt{AND}^{(1,1)}|x, y\rangle = \mathtt{T}^{(1,1,1)}|x, y, 0\rangle = |x, y, 1\rangle$ iff $x = y = 1$;
- $\mathtt{AND}^{(1,1)}|x, y\rangle = \mathtt{T}^{(1,1,1)}|x, y, 0\rangle = |x, y, 0\rangle$ iff $x = 0$ or $y = 0$.

Hence, $\mathtt{AND}^{(1,1)}$ represents a "good" quantum generalization of classical conjunction. At the same time, this particular form of quantum conjunction gives rise to a characteristic *holistic* behavior, which is deeply rooted in the holistic features of the quantum-theoretic formalism. Consider, for instance, the following quregister of the space $\mathscr{H}^{(2)}$ (which represents one of the possible examples of a *Bell-state*):

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0, 0\rangle + \frac{1}{\sqrt{2}}|1, 1\rangle.$$

We have:

$$\mathtt{AND}^{(1,1)}|\psi\rangle = \mathtt{T}^{(1,1,1)}(|\psi\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}|0, 0, 0\rangle + \frac{1}{\sqrt{2}}|1, 1, 1\rangle;$$

$${}^{\mathfrak{D}}\mathtt{AND}^{(1,1)}(P_{|\psi\rangle}) = {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(P_{|\psi\rangle} \otimes P_0^{(1)}) = P_{\frac{1}{\sqrt{2}}|0,0,0\rangle + \frac{1}{\sqrt{2}}|1,1,1\rangle}.$$

Hence, $\mathtt{AND}^{(1,1)}|\psi\rangle$ and ${}^{\mathfrak{D}}\mathtt{AND}^{(1,1)}(P_{|\psi\rangle})$ represent a pure state of the space $\mathscr{H}^{(3)}$. At the same time, the two reduced states of $P_{|\psi\rangle}$ turn out to be one and the same mixture (of the space $\mathscr{H}^{(1)}$):

$$Red^1(P_{|\psi\rangle}) = Red^2(P_{|\psi\rangle}) = \frac{1}{2}\mathtt{I}^{(1)}.$$

We have:

$$^{\mathfrak{D}}\mathtt{AND}^{(1,1)}(Red^1(P_{|\psi\rangle}) \otimes Red^2(P_{|\psi\rangle})) = {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(Red^1(P_{|\psi\rangle}) \otimes Red^2(P_{|\psi\rangle}) \otimes P_0^{(1)}),$$

which is a proper mixture. Hence,

$$^{\mathfrak{D}}\mathtt{AND}^{(1,1)}(P_{|\psi\rangle}) \neq {}^{\mathfrak{D}}\mathtt{AND}^{(1,1)}(Red^1(P_{|\psi\rangle}) \otimes Red^2(P_{|\psi\rangle})).$$

The conjunction over a *global* piece of information (consisting of two parts) does not generally coincide with the conjunction of the two separate parts. In the next Chapters we will see how the holistic features of the quantum conjunction $\mathtt{AND}^{(m,n)}$ allow us to formally describe some semantic situations that are strongly anti-classical.

The gates $\mathtt{NOT}^{(n)}$, $\mathtt{XOR}^{(m,n)}$, $\mathtt{T}^{(m,n,1)}$ have been called "semiclassical" because they are unable to "create" superpositions. Whenever the information-input is a register, the information-output will be a register. Quantum computation, however, cannot help referring also to "genuine quantum gates" that can transform classical inputs (represented by registers) into genuine superpositions. And it is needless to stress how superpositions play an essential role in quantum computation, being responsible for the characteristic parallel structures that determine the speed and the efficiency of quantum computers.

We will now give the definitions of two important genuine quantum gates: the *Hadamard-gate* (also called *square root of identity*) and the *square root of negation*.

**Definition 2.11** (*The Hadamard-gate on the space $\mathcal{H}^{(1)}$*) The *Hadamard-gate* on $\mathcal{H}^{(1)}$ is the linear operator $\sqrt{\mathtt{I}}^{(1)}$ that satisfies the following condition for every element $|x\rangle$ of the canonical basis:

$$\sqrt{\mathtt{I}}^{(1)}|x\rangle := \frac{1}{\sqrt{2}}((-1)^x|x\rangle + |1-x\rangle).$$

One can prove that $\sqrt{\mathtt{I}}^{(1)}$ is a unitary operator. We have:

$$\sqrt{\mathtt{I}}^{(1)}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad \sqrt{\mathtt{I}}^{(1)}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Accordingly, $\sqrt{\mathtt{I}}^{(1)}$ transforms both bits into two different genuine superpositions that might be either true or false with probability $\frac{1}{2}$.

The basic property of the Hadamard-gate is the property that has suggested its name ("square root of identity"):

$$\sqrt{\mathtt{I}}^{(1)}\sqrt{\mathtt{I}}^{(1)}|\psi\rangle = |\psi\rangle, \quad \text{for any qubit } |\psi\rangle.$$

In other words, applying twice the Hadamard-gate gives the identity.

**Definition 2.12** (*The square root of negation on the space* $\mathscr{H}^{(1)}$) The *square root of negation* on $\mathscr{H}^{(1)}$ is the linear operator $\sqrt{\mathtt{NOT}}^{(1)}$ that satisfies the following condition for every element $|x\rangle$ of the canonical basis:

$$\sqrt{\mathtt{NOT}}^{(1)}|x\rangle := \frac{1}{2}((1+\imath)|x\rangle + (1-\imath)|1-x\rangle)$$

(where $\imath$ is the imaginary unit).

One can prove that $\sqrt{\mathtt{NOT}}^{(1)}$ is a unitary operator, which transforms both bits into two different genuine superpositions that might be either true or false with probability $\frac{1}{2}$.

The basic property of the square root of negation is the property that has suggested its name:

$$\sqrt{\mathtt{NOT}}^{(1)}\sqrt{\mathtt{NOT}}^{(1)}|\psi\rangle = \mathtt{NOT}^{(1)}|\psi\rangle, \quad \text{for any qubit } |\psi\rangle.$$

In other words, applying twice the square root of negation means negating.

As expected, both $\sqrt{\mathtt{I}}^{(1)}$ and $\sqrt{\mathtt{NOT}}^{(1)}$ can be generalized to higher-dimensional spaces. In any space $\mathscr{H}^{(n)}$ (with $n > 1$), the operators $\sqrt{\mathtt{I}}^{(n)}$ and $\sqrt{\mathtt{NOT}}^{(n)}$ are defined for every element $|x_1, \ldots, x_n\rangle$ of the canonical basis as follows:

- $\sqrt{\mathtt{I}}^{(n)}|x_1, \ldots, x_n\rangle := (\mathtt{I}^{(n-1)} \otimes \sqrt{\mathtt{I}}^{(1)})|x_1, \ldots, x_n\rangle$;
- $\sqrt{\mathtt{NOT}}^{(n)}|x_1, \ldots, x_n\rangle := (\mathtt{I}^{(n-1)} \otimes \sqrt{\mathtt{NOT}}^{(1)})|x_1, \ldots, x_n\rangle$.

The two following Theorems sum up some important basic properties and some important probabilistic properties of the gates defined above.

**Theorem 2.2** *(1)* $\mathtt{NOT}^{(n)}\mathtt{NOT}^{(n)} = \mathtt{I}^{(n)}$
*(2)* $\sqrt{\mathtt{I}}^{(n)}\sqrt{\mathtt{I}}^{(n)} = \mathtt{I}^{(n)}$
*(3)* $\sqrt{\mathtt{NOT}}^{(n)}\sqrt{\mathtt{NOT}}^{(n)} = \mathtt{NOT}^{(n)}$
*(4)* $\mathtt{T}^{(m,n,1)} = [(\mathtt{I}^{(m+n)} - (P_1^{(m+n-1)} \otimes P_1^{(1)})) \otimes \mathtt{I}^{(1)} + P_1^{(m+n-1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}][\mathtt{Swap}_{m,m+n-1}^{(m+n-1)} \otimes \mathtt{I}^{(2)}]$.

*Proof* (1)–(3) By definition of the gates $\mathtt{NOT}^{(n)}$, $\sqrt{\mathtt{NOT}}^{(n)}$, $\sqrt{\mathtt{I}}^{(n)}$ it is sufficient to consider the case of $n = 1$. And by easy calculations one can show that for any bit $|x\rangle$:

$$\mathtt{NOT}^{(1)}\mathtt{NOT}^{(1)}|x\rangle = |x\rangle; \;\; \sqrt{\mathtt{I}}^{(1)}\sqrt{\mathtt{I}}^{(1)}|x\rangle = |x\rangle; \;\; \sqrt{\mathtt{NOT}}^{(1)}\sqrt{\mathtt{NOT}}^{(1)}|x\rangle = \mathtt{NOT}^{(1)}|x\rangle.$$

(4) Proof similar to the proof of Theorem 2.1. □

**Theorem 2.3** *(1)* $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) = \mathtt{tr}[(P_1^{(m)} \otimes P_1^{(n)})\,\rho]$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$.

*(2)* $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) \leq \mathtt{p}_1(Red^{(1)}_{[m,n]}(\rho))$; $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) \leq \mathtt{p}_1(Red^{(2)}_{[m,n]}(\rho))$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$.

*(3)* $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{NOT}^{(n)}(\rho)) = 1 - \mathtt{p}_1(\rho)$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$.

*(4)* $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma)) = \mathtt{p}_1(\rho) \cdot \mathtt{p}_1(\sigma)$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m)})$ *and any* $\sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$.

*(5)* ${}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma) \cong {}^{\mathfrak{D}}\mathtt{AND}^{(n,m)}(\sigma \otimes \rho)$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m)})$ *and any* $\sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$.[8]

*(6)* ${}^{\mathfrak{D}}\mathtt{AND}^{(m,n+p+1)}(\rho \otimes {}^{\mathfrak{D}}\mathtt{AND}^{(n,p)}(\sigma \otimes \tau)) \cong {}^{\mathfrak{D}}\mathtt{AND}^{(m+n+1,p)}({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma) \otimes \tau))$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m)})$, *any* $\sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$ *and any* $\tau \in \mathfrak{D}(\mathscr{H}^{(p)})$.

*(7)* ${}^{\mathfrak{D}}\mathtt{NOT}^{(n)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(n)}\rho \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(n)}\ {}^{\mathfrak{D}}\mathtt{NOT}^{(n)}\ \rho$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$.

*(8)* ${}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(n)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(n)}\rho \cong {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(n)}\rho$; ${}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(n)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(n)}\rho \cong {}^{\mathfrak{D}}\mathtt{NOT}^{(n)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(n)}\rho$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$.

*(9)* ${}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_0^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_1^{(1)}$.

*(10)* ${}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_0^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_1^{(1)}$.

*(11)* ${}^{\mathfrak{D}}\mathtt{NOT}^{(1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_0^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_0^{(1)}$; ${}^{\mathfrak{D}}\mathtt{NOT}^{(1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_1^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_1^{(1)}$.

*(12)* ${}^{\mathfrak{D}}\mathtt{NOT}^{(1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_0^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_0^{(1)}$; ${}^{\mathfrak{D}}\mathtt{NOT}^{(1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_1^{(1)} \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_1^{(1)}$.

*(13)* ${}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(m+n+1)}\ {}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho) \cong {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}P_0^{(1)}$; ${}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(m+n+1)}\ {}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho) \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_0^{(1)}$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$.

*(14)* ${}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(m+n+1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(m+n+1)}\ {}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho) \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}P_0^{(1)}$; ${}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(m+n+1)}\ {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(m+n+1)}\ {}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho) \cong {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(1)}\ P_0^{(1)}$, *for any* $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$.

*Proof* (1) By definition of $\mathtt{AND}^{(m,n)}$ and by Theorem 2.2(4) we have:

$$
\begin{aligned}
&{}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho) = \mathtt{T}^{(m,n,1)}(\rho \otimes P_0^{(1)})\mathtt{T}^{(m,n,1)} \\
&= [(\mathtt{I}^{(m+n)} - P_1^{(m+n-1)} \otimes P_1^{(1)}) \otimes \mathtt{I}^{(1)}](\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})(\rho \otimes P_0^{(1)}) \\
&(\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})[(\mathtt{I}^{(m+n)} - P_1^{(m+n-1)} \otimes P_1^{(1)}) \otimes \mathtt{I}^{(1)}] \\
&+ [P_1^{(m+n-1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}](\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})(\rho \otimes P_0^{(1)}) \\
&(\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})[P_1^{(m+n-1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}].
\end{aligned}
$$

One can easily see that

$$
\begin{aligned}
&P_1^{(m+n+1)}(\mathtt{I}^{(m+n)} - P_1^{(m+n-1)} \otimes P_1^{(1)}) \otimes \mathtt{I}^{(1)}(\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})(\rho \otimes P_0^{(1)}) \\
&(\mathtt{Swap}^{(m+n-1)}_{m,m+n-1} \otimes \mathtt{I}^{(2)})(\mathtt{I}^{(m+n)} - P_1^{(m+n-1)} \otimes P_1^{(1)}) \otimes \mathtt{I}^{(1)}
\end{aligned}
$$

[8] $\cong$ is the probabilistic equivalence relation (Definition 2.4).

is the null projection operator. Consequently:

$$\begin{aligned}
&\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) = \mathrm{tr}(P_1^{(m+n+1)}(P_1^{(m+n-1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)})\\
&(\mathtt{Swap}_{m,m+n-1}^{(m+n-1)} \otimes \mathtt{I}^{(2)})(\rho \otimes P_0^{(1)})\\
&(\mathtt{Swap}_{m,m+n-1}^{(m+n-1)} \otimes \mathtt{I}^{(2)})(P_1^{(m+n-1)} \otimes P_1^{(1)} \otimes \mathtt{NOT}^{(1)}))\\
&= \mathrm{tr}(P_1^{(m+n+1)}((P_1^{(m)} \otimes P_1^{(n)})\rho(P_1^{(m)} \otimes P_1^{(n)})) \otimes \mathtt{NOT}^{(1)} P_0^{(1)}\mathtt{NOT}^{(1)}))\\
&= \mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})\rho)\mathrm{tr}(P_1^{(1)} P_1^{(1)})\\
&= \mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})\rho).
\end{aligned}$$

(2) Let $\rho \in \mathfrak{D}(\mathscr{H}^{(m+n)})$. By (1), $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) = \mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})\rho)$. Since $(P_1^{(m)} \otimes P_1^{(n)})(P_1^{(m)} \otimes \mathtt{I}^{(n)}) = (P_1^{(m)} P_1^{(m)} \otimes P_1^{(n)} \mathtt{I}^{(n)}) = P_1^{(m)} \otimes P_1^{(n)}$, we have: $P_1^{(m)} \otimes P_1^{(n)} \preccurlyeq P_1^{(m)} \otimes \mathtt{I}^{(n)}$. Hence (by definition of reduced state): $\mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})\rho) \leq \mathrm{tr}((P_1^{(m)} \otimes \mathtt{I}^{(n)})\rho) = \mathrm{tr}(P_1^{(m)} Red_{[m,n]}^{(1)}(\rho))$.
Consequently: $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) \leq \mathtt{p}_1(Red_{[m,n]}^{(1)}(\rho))$.

In a similar way, one can prove: $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho)) \leq \mathtt{p}_1(Red_{[m,n]}^{(2)}(\rho))$.

(3) By definition of $\mathtt{NOT}^{(n)}$, we have for any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$: $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{NOT}^{(n)}(\rho)) = \mathrm{tr}(P_1^{(n)}\,\mathtt{NOT}^{(n)}\,\rho\,\mathtt{NOT}^{(n)}) = \mathrm{tr}(\mathtt{NOT}^{(n)}\,P_1^{(n)}\,\mathtt{NOT}^{(n)}\,\rho) = \mathrm{tr}(P_0^{(n)}\,\rho) = \mathrm{tr}((\mathtt{I}^{(n)} - P_1^{(n)})\,\rho) = \mathrm{tr}(\rho) - \mathrm{tr}(P_1^{(n)}\,\rho) = 1 - \mathtt{p}_1(\rho)$.

(4) By (1), $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma)) = \mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})(\rho \otimes \sigma))$, for any $\rho \in \mathfrak{D}(\mathscr{H}^{(m)})$ and any $\sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$. We have: $\mathrm{tr}((P_1^{(m)} \otimes P_1^{(n)})(\rho \otimes \sigma)) = \mathrm{tr}(P_1^{(m)}\rho) \cdot \mathrm{tr}(P_1^{(n)}\sigma)$.
Hence, $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma)) = \mathtt{p}_1(\rho) \cdot \mathtt{p}_1(\sigma)$.

(5) By (4), $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma)) = \mathtt{p}_1(\rho) \cdot \mathtt{p}_1(\sigma) = \mathtt{p}_1({}^{\mathfrak{D}}\mathtt{AND}^{(n,m)}(\sigma \otimes \rho))$, for any $\rho \in \mathfrak{D}(\mathscr{H}^{(m)})$ and any $\sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$. Hence, ${}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}(\rho \otimes \sigma) \cong {}^{\mathfrak{D}}\mathtt{AND}^{(n,m)}(\sigma \otimes \rho)$.

(6) Similar to (5).

(7) By Theorem 2.2(3).

(8)–(14) can be proved by similar arguments. □

Is it possible to define all possible gates of a space $\mathscr{H}^{(n)}$ by means of a finite set of gates? The answer to this question is clearly negative by trivial cardinality-reasons: while the set of all gates of $\mathscr{H}^{(n)}$ is non-denumerable, the set of all finite combinations of elements of any finite set of gates is denumerable.

Interestingly enough, one can prove that there exists a finite (and "small") system of gates that satisfies the following property: for any space $\mathscr{H}^{(n)}$, any gate $\mathtt{G}^{(n)}$ can be approximated with arbitrary precision by a convenient finite combination of elements of the system. This result can be obtained by using an important theorem proved by Shi and Aharonov.[9] Consider the following gate-system:

$$\mathfrak{G}^* = (\mathtt{I}^{(1)},\ \mathtt{NOT}^{(1)},\ \mathtt{T}^{(1,1,1)},\ \sqrt{\mathtt{I}}^{(1)}).$$

[9]See [1, 12].

For any space $\mathscr{H}^{(n)}$, consider the infinite (denumerable) family $\mathfrak{F}\mathfrak{G}^{*(n)}$ of *derived gates* $\mathtt{G}^{(n)}$ that can be defined as appropriate (finite) combinations of elements of $\mathfrak{G}^*$, by using gate-tensor products and gate-compositions.

**Theorem 2.4** *For any gate* $\mathtt{G}^{(n)}$ *of* $\mathscr{H}^{(n)}$ *and for any choice of a non-negative real number* $\varepsilon$ *there exists a finite sequence of gates* $(\mathtt{G}_1^{(n)}, \ldots, \mathtt{G}_u^{(n)})$ *such that:*

*(1)* $\mathtt{G}_1^{(n)}, \ldots, \mathtt{G}_u^{(n)} \in \mathfrak{F}\mathfrak{G}^{*(n)}$;
*(2) for any vector* $|\psi\rangle$ *of* $\mathscr{H}^{(n)}$, $\|\mathtt{G}^{(n)}|\psi\rangle - \mathtt{G}_1^{(n)} \ldots \mathtt{G}_u^{(n)}|\psi\rangle\| \leq \varepsilon$.

Thus, the family $\mathfrak{F}\mathfrak{G}^{*(n)}$ has the capacity of approximating with arbitrary accuracy all possible gates of $\mathscr{H}^{(n)}$. In this sense, the system $\mathfrak{G}^*$ can be described as an *approximately universal gate-system*.[10]

One could notice that $\mathfrak{G}^*$ is, in a sense, redundant. For, the negation-gate can be defined in terms of the Toffoli-gate, which represents a *controlled controlled negation*. Accordingly, $\mathtt{NOT}\,|x\rangle$ might be dealt with as an abbreviation for $\mathtt{T}^{(1,1,1)}|1, 1, x\rangle$. However, $\mathtt{T}^{(1,1,1)}|1, 1, x\rangle$ only exists in the space $\mathscr{H}^{(3)}$), while using an "autonomous" negation, defined on the smaller space $\mathscr{H}^{(1)}$, turns out to be more convenient both for computational and for logical applications.

## 2.3 Quantum Logical Circuits

Quantum computations are performed by appropriate combinations of gates that give rise to some special configurations called *quantum logical circuits* (briefly, *quantum circuits*). Roughly, a quantum circuit $\mathscr{C}$ can be described as a network consisting of *wires* that carry pieces of quantum information to gates whose actions transform the pieces of information in question. Wires are usually represented as horizontal lines, while gates are represented as *boxes* crossed by some of the wires. One conventionally assumes that pieces of quantum information *flow* from the left to the right (in a given circuit). Any quantum circuit $\mathscr{C}$ refers to a Hilbert space $\mathscr{H}^{(n)}$, where all possible inputs and outputs for $\mathscr{C}$ are supposed to live. Let us first consider the case of circuits where gates are unitary operators of a space $\mathscr{H}^{(n)}$, while all possible inputs and outputs are quregisters of the space. Of course each gate $\mathtt{G}^{(n)}$ of a circuit $\mathscr{C}$ may be the tensor product of other gates:

$$\mathtt{G}^{(n)} = \mathtt{G}_1^{(m_1)} \otimes \cdots \otimes \mathtt{G}_r^{(m_r)} \;\; (\text{where } \; m_1 + \cdots + m_r = n).$$

As an example, we will consider three characteristic instances of circuits. Figure 2.1 describes a three-wire circuit, where any possible input (living in the space $\mathscr{H}^{(3)}$) is submitted to the action of the gate $\mathtt{NOT}^{(3)} = \mathtt{I}^{(2)} \otimes \mathtt{NOT}^{(1)}$.[11]

[10]See [4].
[11]For the sake of simplicity one often avoids to represent identity-gates as particular boxes.

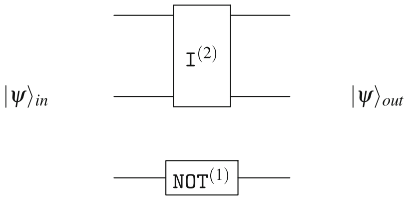



**Fig. 2.1** A quantum circuit for the gate $\mathtt{NOT}^{(3)}$

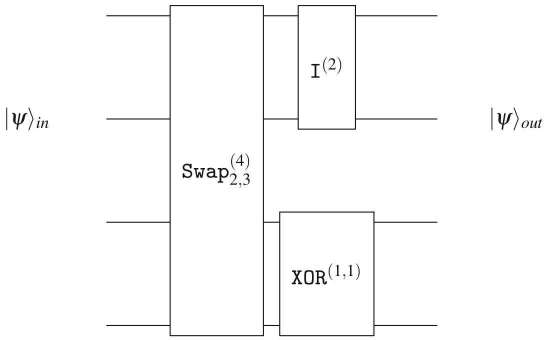



**Fig. 2.2** A quantum circuit for the gate $\mathtt{XOR}^{(2,2)}$

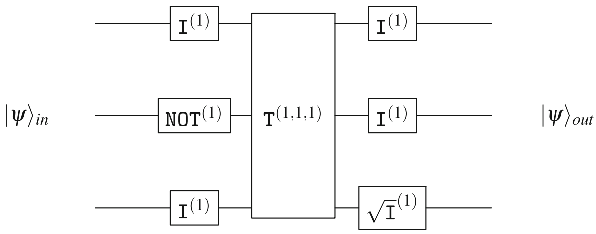



**Fig. 2.3** A circuit for the gate-sequence $(\mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)} \otimes \mathtt{I}^{(1)},\ \mathtt{T}^{(1,1,1)},\ \mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)})$

Figure 2.2 illustrates a four-wire circuit where any possible input (living in the space $\mathscr{H}^{(4)}$) is submitted to the action of the gate $\mathtt{XOR}^{(4)} = (\mathtt{I}^{(2)} \otimes \mathtt{XOR}^{(1,1)})\mathtt{Swap}_{2,3}^{(4)}$. This circuit allows us to "visualize" the role played by the $\mathtt{Swap}$-gate.

Figure 2.3 illustrates a three-wire circuit where any possible input (living in the space $\mathscr{H}^{(3)}$) is submitted to the actions of the three following gates:

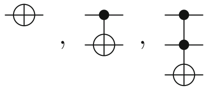
$$\mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)} \otimes \mathtt{I}^{(1)},\quad \mathtt{T}^{(1,1,1)},\quad \mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)}.$$

In the case of our third example (Fig. 2.3) it is natural to assume that each gate of the gate-sequence $(\mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)} \otimes \mathtt{I}^{(1)},\ \mathtt{T}^{(1,1,1)},\ \mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)})$ corresponds to a particular *computational step* of the circuit (also called *layer* of the circuit).

This kind of representation can be easily generalized to more complex examples of circuits, characterized by $n$ wires and by $m$ computational steps (where each particular step may involve more than one gate). Accordingly, the *computational complexity* of a given circuit turns out to depend on the following parameters:

1. the wire-number $n$ (determined by the Hilbert space $\mathscr{H}^{(n)}$ which the circuit refers to). This number is also called the *width* of the circuit.
2. The number $g$ of gates. This number is also called the *size* of the circuit.
3. The number $m$ of the computational steps. This number is also called the *depth* of the circuit.

It us useful to recall that in the literature the gates $\mathtt{NOT}^{(1)}$, $\mathtt{XOR}^{(1,1)}$, $\mathtt{T}^{(1,1,1)}$ are often represented in the following way:



This stresses the fact that XOR is a *controlled negation*, while Toffoli is a *controlled controlled negation*. Accordingly, the intended reading of our three figures is the following: $\oplus$ represents the negation-gate; a full circle represents a *control-unit*, while the operator $\oplus$ is intended to be be applied only in the case where all control-units are set to $|1\rangle$.

As expected, any quantum circuit

$$\mathscr{C} = (\mathtt{G}_1^{(n)}, \ldots, \mathtt{G}_t^{(n)})$$

(where each $\mathtt{G}_i^{(n)}$ is a unitary operator of the space $\mathscr{H}^{(n)}$) can be canonically transformed into a corresponding circuit

$$^{\mathfrak{D}}\mathscr{C} = (^{\mathfrak{D}}\mathtt{G}_1^{(n)}, \ldots, \ ^{\mathfrak{D}}\mathtt{G}_t^{(n)}),$$

where each $^{\mathfrak{D}}\mathtt{G}_i^{(n)}$ is the unitary operation corresponding to the unitary operator $\mathtt{G}_i^{(n)}$.

In the next Chapters we will see how the main features of quantum circuits can be faithfully reflected in the linguistic expressions of quantum computational logics.

## 2.4 Physical Implementations by Optical Devices

Physical implementations of quantum logical gates represent the basic issue for the technological realization of quantum computers. Among the different choices that have been investigated in the literature we will consider here the case of optical devices, where photon-beams (possibly consisting of single photons) move in different directions. Let us conventionally assume that $|0\rangle$ represents the state of a beam moving along the **x**-direction, while $|1\rangle$ is the state of a beam moving along the **y**-direction.

In the framework of this "physical semantics", one-qubit gates (like $\mathtt{NOT}^{(1)}$, $\sqrt{\mathtt{I}}^{(1)}$, $\sqrt{\mathtt{NOT}}^{(1)}$) can be easily implemented. A natural implementation of $\mathtt{NOT}^{(1)}$ can be obtained by a mirror **M** that reflects in the **y**-direction any beam moving along the **x**-direction, and vice versa. Hence we have:

$$|0\rangle \;\rightarrowtail_{\mathbf{M}}\; |1\rangle; \quad |1\rangle \;\rightarrowtail_{\mathbf{M}}\; |0\rangle$$

(the mirror transforms the state $|0\rangle$ into the state $|1\rangle$, and vice versa).

An implementation of the Hadamard-gate $\sqrt{\mathtt{I}}^{(1)}$ can be obtained by a symmetric 50 : 50 beam splitter **BS**. We have:

$$|0\rangle \;\rightarrowtail_{\mathbf{BS}}\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |1\rangle \;\rightarrowtail_{\mathbf{BS}}\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Accordingly, any beam that goes through **BS** is split into two components: one component moves along the **x**-direction, while the other component moves along the **y**-direction. And the probability of both paths (along the **x**-direction or along the **y**-direction) is $\frac{1}{2}$. Also the gate $\sqrt{\mathtt{NOT}}^{(1)}$ can be implemented in a similar way.

Other apparatuses that may be useful for optical implementations of gates are the *relative phase shifters* along a given direction. A particular example is described by the following unitary operator.

**Definition 2.13** (*The relative phase shifter along the* **y**-*direction*) The relative phase shifter along the **y**-direction is the linear operator $\mathtt{U}_{\mathtt{PS}}$ that is defined for every element $|v\rangle$ of the canonical basis of $\mathbb{C}^2$ as follows: $\mathtt{U}_{\mathtt{PS}}|v\rangle = c|v\rangle$, where $c = \begin{cases} e^{i\pi}, \text{ if } v = 1; \\ 1, \text{ otherwise.} \end{cases}$

We obtain:

$$\mathtt{U}_{\mathtt{PS}}|\mathtt{0}\rangle = |\mathtt{0}\rangle; \quad \mathtt{U}_{\mathtt{PS}}|\mathtt{1}\rangle = -|\mathtt{1}\rangle.$$

Let us indicate by **PS** a physical apparatus that realizes the phase shift described by $\mathtt{U}_{\mathtt{PS}}$.

Relative phase shifters, beam splitters and mirrors are the basic physical components of the *Mach-Zehnder interferometer* (**MZI**), an apparatus that has played a very important role in the logical and philosophical debates about the foundations of quantum theory. The physical situation can be sketched as follows (Fig. 2.4).

Consider a photon-beam that may move either along the **x**-direction or along the **y**-direction. Photons moving along the **y**-direction go through the relative phase shifter **PS** of **MZI**. We have:

$$|0\rangle \;\rightarrowtail_{\mathbf{PS}}\; |0\rangle; \quad |1\rangle \;\rightarrowtail_{\mathbf{PS}}\; -|1\rangle$$

(the phase of the beam changes only in the case where the beam is moving along the **y**-direction). Soon after the beam goes through the first beam splitter $\mathbf{BS}_1$. As a consequence, it is split into two components: one component moves along the interferometer's arm in the **x**-direction, the other component moves along the arm in the **y**-direction. We have:

$$|0\rangle \;\rightarrowtail_{\mathbf{BS}_1}\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad -|1\rangle \;\rightarrowtail_{\mathbf{BS}_1}\; \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle).$$

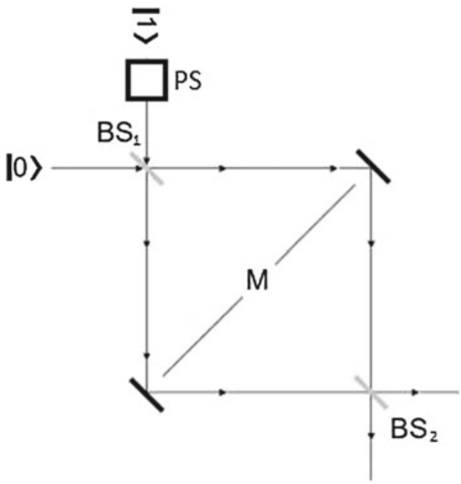



**Fig. 2.4** The Mach-Zehnder interferometer

Then, both components of the superposed beam (on both arms) are reflected by the mirrors **M**. We have:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;\rightarrowtail_{\mathbf{M}}\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \;\rightarrowtail_{\mathbf{M}}\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Finally, the superposed beam goes through the second beam splitter $\mathbf{BS}_2$, which re-composes the two components. We have:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;\rightarrowtail_{\mathbf{BS}_2}\; |0\rangle; \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \;\rightarrowtail_{\mathbf{BS}_2}\; |1\rangle.$$

Accordingly, **MZI** transforms the input $|0\rangle$ into the output $|0\rangle$, while the input $|1\rangle$ is transformed into the output $|1\rangle$.

One is dealing with a result that has for a long time been described as deeply counter-intuitive. In fact, according to a "classical way of thinking" we would expect that the outcoming photons from the second beam splitter should be detected with probability $\frac{1}{2}$ either along the **x**-direction or along the **y**-direction.

The Mach-Zehnder interferometer gives rise to a physical implementation of the following quantum logical circuit (called "the Mach-Zehnder circuit"):

$$\sqrt{\mathtt{I}}^{(1)}\,\mathtt{NOT}^{(1)}\,\sqrt{\mathtt{I}}^{(1)}.$$

We have:

$$\sqrt{\mathtt{I}}^{(1)}\,\mathtt{NOT}^{(1)}\,\sqrt{\mathtt{I}}^{(1)}|0\rangle = |0\rangle; \quad \sqrt{\mathtt{I}}^{(1)}\,\mathtt{NOT}^{(1)}\,\sqrt{\mathtt{I}}^{(1)} - |1\rangle = |1\rangle.$$

While optical implementations of one-qubit gates are relatively simple, trying to implement many-qubit gates may be rather complicated. Consider the case of the Toffoli-gate $\mathtt{T}^{(1,1,1)}$. For any element $|v_1, v_2, v_3\rangle$ of the canonical basis of the space $\mathscr{H}^{(3)}$ we have:

$$\mathtt{T}^{(1,1,1)}|v_1, v_2, v_3\rangle = \begin{cases} |v_1, v_2, v_1 \sqcap v_2\rangle, & \text{if } v_3 = 0; \\ |v_1, v_2, (v_1 \sqcap v_2)'\rangle, & \text{if } v_3 = 1. \end{cases}$$

The main problem is finding a device that can realize a physical dependence of the target-bit ($v_1 \sqcap v_2$ or $(v_1 \sqcap v_2)'$) from the control-bits ($v_1, v_2$). A possible strategy is based on an appropriate use of the optical "Kerr-effect": a substance with an intensity-dependent refractive index is placed into a given device, giving rise to an intensity-dependent phase shift.

Let us first give the mathematical definition of a unitary operator that describes a particular form of *conditional phase shift*.

**Definition 2.14** (*The relative conditional phase shifter*) The relative conditional phase shifter of the space $\mathscr{H}^{(3)}$ is the unitary operator $\mathtt{U}_{\mathtt{CPS}}$ that is defined for every element of the canonical basis as follows:

$$\mathtt{U}_{\mathtt{CPS}}|v_1, v_2, v_3\rangle = |v_1, v_2\rangle \otimes c|v_3\rangle,$$

where $c = \begin{cases} e^{i\pi}, & \text{if } v_1 = 1, v_2 = 1 \text{ and } v_3 = 0; \\ 1, & \text{otherwise}. \end{cases}$.

Let us indicate by **CPS** a physical apparatus that realizes the phase shift described by the operator $\mathtt{U}_{\mathtt{CPS}}$. Clearly, **CPS** determines a *conditional* phase shift. For, the phase of a three-beam system in state $|v_1, v_2, v_3\rangle$ is changed only in the case where both control-bits ($|v_1\rangle, |v_2\rangle$) are the state $|1\rangle$, while the target-bit $|v_3\rangle$ is the state $|0\rangle$. From a physical point of view, such a result can be obtained by using a convenient substance that produces the Kerr-effect.

In order to obtain an implementation of the Toffoli-gate $\mathtt{T}^{(1,1,1,)}$ we will now consider a "more sophisticated" version of the Mach-Zehnder interferometer that will be called "Kerr-Mach-Zehnder interferometer" (indicated by **KMZI**). Besides the relative phase shifter (**PS**), the two beam splitters ($\mathbf{BS}_1, \mathbf{BS}_2$) and the mirrors (**M**), the Kerr-Mach-Zehnder interferometer also contains a relative conditional phase shifter (**CPS**) that can produce the Kerr-effect (Fig. 2.5).

While the inputs of the canonical Mach-Zehnder interferometer are single beams (whose states live in the space $\mathscr{H}^{(1)}$), the apparatus **KMZI** acts on composite systems consisting of three beams ($\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3$), whose states live in the space $\mathscr{H}^{(3)}$. For the sake of simplicity we can assume that $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3$ are single photons that may enter into the interferometer-box either along the **x**-direction or along the **y**-direction. Let $|v_1, v_2, v_3\rangle$ be the input-state of the composite system $\mathbf{S}_1 + \mathbf{S}_2 + \mathbf{S}_3$. Photons $\mathbf{S}_1, \mathbf{S}_2$ (whose states $|v_1\rangle, |v_2\rangle$ represent the control-bits) are supposed to enter into the box along the **yz**-plane, while photon $\mathbf{S}_3$ (whose state $|v_3\rangle$ is the target-bit) will enter through the first beam-splitter $\mathbf{BS}_1$.

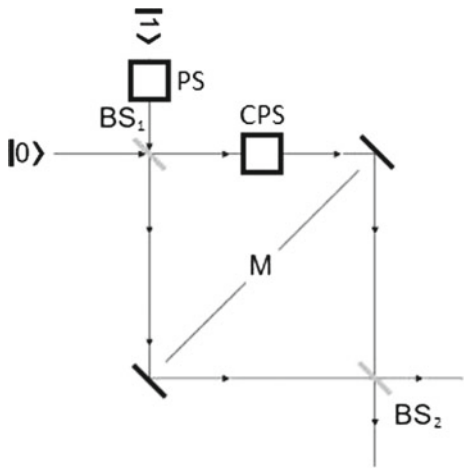



**Fig. 2.5** The Kerr-Mach-Zehnder interferometer

Mathematically, the action performed by the apparatus **KMZI** is described by the following unitary operator (of the space $\mathscr{H}^{(3)}$):

$\mathtt{U}_{\mathtt{KMZ}} = (\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)}) \circ (\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)}) \circ \mathtt{U}_{\mathtt{CPS}} \circ (\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)}) \circ (\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \mathtt{U}_{\mathtt{PS}})$.

In order to "see" how **KMZI** is working from a physical point of view, it is expedient to consider a particular example. Take the input $|v_1, v_2, v_3\rangle = |1, 1, 0\rangle$ and let us describe the physical evolution determined by the operator $\mathtt{U}_{\mathtt{KMZ}}$ for the system $\mathbf{S}_1 + \mathbf{S}_2 + \mathbf{S}_3$, whose initial state is $|1, 1, 0\rangle$. We have:

- $(\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \mathtt{U}_{\mathtt{PS}})|1, 1, 0\rangle = |1, 1, 0\rangle$. The relative phase shifter along the **y**-direction (**PS**) does not change the state of photon $\mathbf{S}_3$, which is moving along the **x**-direction.
- $(\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)})|1, 1, 0\rangle = |1, 1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Photon $\mathbf{S}_3$ goes through the first beam splitter $\mathbf{BS}_1$ splitting into two components: one component moves along the interferometer's arm along the **x**-direction, the other component moves along the arm in the **y**-direction (like in the case of the canonical Mach-Zehnder interferometer). At the same time, photons $\mathbf{S}_1$ and $\mathbf{S}_2$ (both in state $|1\rangle$) enter into the interferometer-box along the **yz**-plane.
- $\mathtt{U}_{\mathtt{CPS}}(|1, 1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = |1, 1\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$. The conditional phase shifter **CPS** determines a phase shift for the component of $\mathbf{S}_3$ that is moving along the **x**-direction; because both photons $\mathbf{S}_1$ and $\mathbf{S}_2$ (in state $|1\rangle$) have gone through the substance (contained in **CPS**) that produces the Kerr-effect.
- $(\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)})(|1, 1\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)) = |1, 1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Both components of $\mathbf{S}_3$ (on both arms) are reflected by the mirrors.
- $(\mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}^{(1)}})(|1, 1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) = |1, 1, 1\rangle$. The second beam splitter $\mathbf{BS}_2$ re-composes the two components of the superposed photon $\mathbf{S}_3$.

Consequently, we obtain:

$$\mathtt{U}_{\mathtt{KMZ}}|1, 1, 0\rangle = |1, 1, 1\rangle = \mathtt{T}^{(1,1,1)}|1, 1, 0\rangle.$$

In general, one can easily prove that $\mathtt{U}_{\mathtt{KMZ}}$ and $\mathtt{T}^{(1,1,1)}$ are one and the same unitary operator.

**Lemma 2.1** *For every element $|v_1, v_2, v_3\rangle$ of the canonical basis of the space $\mathscr{H}^{(3)}$,*

$$\mathtt{U}_{\mathtt{KMZ}}|v_1, v_2, v_3\rangle = \mathtt{T}^{(1,1,1)}|v_1, v_2, v_3\rangle.$$

Although, from a mathematical point of view, $\mathtt{U}_{\mathtt{KMZ}}$ and $\mathtt{T}^{(1,1,1)}$ represent the same gate, physically it is not guaranteed that the apparatus **KMZI** always realizes the "expected job". All difficulties are due to the behavior of the conditional phase shifter. In fact, the substances used to produce the Kerr-effect normally determine results that are only stochastic.[12] As a consequence one shall conclude that the Kerr-Mach-Zehnder interferometer allows us to obtain an *approximate* implementation of the Toffoli-gate with an accuracy that may be very good in some cases.

## References

1. Aharonov, D.: A simple proof that Toffoli and Hadamard are quantum universal (2003). arXiv:quant-ph/0301040
2. Bonzio, S., Verrucchi, P.: The rhythm of quantum algorithms. Soft Comput. **21**(6), 1515–1521 (2017)
3. Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Logics from quantum computation. Int. J. Quantum. Inf. **3**(2), 293–337 (2005)
4. Dalla Chiara, M.L., Giuntini, R., Freytes, H., Ledda, A., Sergioli, G.: The algebraic structure of an approximately universal system of quantum computational gates. Found. Phys. **39**(6), 559–572 (2009)
5. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**, 467–488 (1982)
6. Feynman, R.P.: Quantum mechanical computers. Opt. News **11**, 11–20 (1985)
7. Gudder, S.P.: Quantum computational logics. Int. J. Theor. Phys. **42**(1), 39–47 (2003)
8. Kaye, P., Laflamme, R., Mosca, M.: An Introduction to Quantum Computing. Oxford University Press, Oxford (2007)
9. Kitaev, A.Y., Shen, A.H., Vyalyi, M.N.: Classical and Quantum Computation. American mathematical society. Rhode Island, Providence (2002)
10. Matsuda, N., Shimizu, R., Mitsumori, Y., Kosaka, H., Edamatsu, K.: Observation of optical-fibre Kerr nonlinearity at the single-photon level. Nat. Photonics **3**, 95–98 (2009)
11. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
12. Shi, Y.: Both Toffoli and controlled-Not need little help to do universal quantum computation (2002). arXiv:quant-ph/0205115
13. Toffoli, T.: Reversible computing. In: de Baker, J.V., Leeuwen, J. (eds.) Automata, Languages and Programming. Lecture notes in computer science, vol. 84, pp. 632–644. Springer, Berlin (1980)

[12] See [10].

# Chapter 3
# Entanglement: Mystery and Resource

## 3.1 Entangled Pure States

*Entanglement*, one of the basic features of quantum theory, has been described as "mysterious" and "potentially paradoxical" by some of the founding fathers of quantum mechanics. The term "entanglement" (in its original German version "Verschärfung") has been first proposed by Schrödinger, who wrote:

*Entanglement is not one but rather the characteristic trait of quantum mechanics.*[1]

Although Einstein, Podolsky and Rosen did not use the term "entanglement" in their celebrated article "Can quantum mechanical description of reality be considered complete?", entangled pure states are essentially involved in the paradoxical situation discussed in their paper.[2]

While the critical concept of entanglement did not play any central role in the logico-algebraic approaches to quantum theory (developed on the lines of Birkhoff and von Neumann's quantum logic), a strong interest for entanglement-phenomena emerged again in the more recent investigations about quantum information and quantum computation. We will see how, in this framework, the "strangeness" of entangled states (which had worried Einstein) has been transformed into a powerful "resource" both for theoretic aims and for technological applications.

We will first consider the case of entangled pure states of bipartite systems consisting of two subsystems.

**Definition 3.1** Entangled pure states of a bipartite system
Let $\mathbf{S} = \mathbf{S}_1 + \mathbf{S}_2$ be a bipartite system whose Hilbert space is $\mathscr{H}_{\mathbf{S}} = \mathscr{H}_{\mathbf{S}_1} \otimes \mathscr{H}_{\mathbf{S}_2}$. A pure state $|\psi\rangle$ of $\mathbf{S}$ is called *entangled* iff $|\psi\rangle$ cannot be represented as a factorized state

$$|\psi_1\rangle \otimes |\psi_2\rangle,$$

[1] See [1].

[2] See [2].



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_3

where $|\psi_1\rangle$ is a pure state of $\mathscr{H}_{\mathbf{S}_1}$ and $|\psi_2\rangle$ is a pure state of $\mathscr{H}_{\mathbf{S}_2}$.

One can prove that for any entangled pure state $|\psi\rangle$, both $Red^1(|\psi\rangle)$ and $Red^2(|\psi\rangle)$ are proper mixtures. A typical example of an entangled pure state is the following Bell-state (which lives in the space $\mathscr{H}^{(2)} = \mathbb{C}^2 \otimes \mathbb{C}^2$):

$$|\psi\rangle = \frac{1}{\sqrt{2}}|1, 0\rangle + \frac{1}{\sqrt{2}}|0, 1\rangle.$$

As we have seen (in Sect. 1.3), we have:

$$Red^1(P_{|\psi\rangle}) = Red^2(P_{|\psi\rangle}) = \frac{1}{2}\mathtt{I}^{(1)}.$$

Thus one can say that the states of the two subsystems, which are *indistinguishable*, are *entangled* in the context $|\psi\rangle$.

The concept of *entangled pure state* can be naturally generalized to the case $n$-partite systems. In this book, for the sake of simplicity, we will not consider *entangled mixtures*.

## 3.2 The Einstein-Podolsky-Rosen Paradox

Many important applications of entanglement-phenomena refer to “EPR-situations”, where the basic concepts and arguments of the “Einstein-Podolsky-Rosen paradox” are used for positive aims.

We will briefly illustrate a simplified version of the *EPR-paradox*, which arises in the case of a composite quantum system, consisting of two subsystems where some two-valued observables can be measured.[3] A typical example is represented by a two-electron system $\mathbf{S} = \mathbf{S}_1 + \mathbf{S}_2$ and by the observable *spin* that can be measured in different directions. For any choice of a direction $\mathbf{d}$, the observable $Spin_{\mathbf{d}}$ (the *spin* in the $\mathbf{d}$-direction) can assume two possible values: either $+\frac{1}{2}$ or $-\frac{1}{2}$. It is customary to call “spin up” the value $+\frac{1}{2}$, while the value $-\frac{1}{2}$ is called “spin down”. Accordingly, any direction $\mathbf{d}$ can be associated to a particular orthonormal basis

$$\mathbf{B}_{\mathbf{d}} = \{|d_+\rangle, |d_-\rangle\}$$

of the space $\mathbb{C}^2$. The two elements of the basis $\mathbf{B}_{\mathbf{d}}$ are the two eigenvectors of the self-adjoint operator $A_{Spin_{\mathbf{d}}}$ (corresponding to the observable $Spin_{\mathbf{d}}$), while the numbers $+\frac{1}{2}$ and $-\frac{1}{2}$ are the corresponding eigenvalues. As expected, we have:

[3] See [3].

- $\mathrm{p}_{|d_+\rangle}\big(Spin_{\mathbf{d}}\big(\{+\frac{1}{2}\}\big)\big) = 1.$
  The event $Spin_{\mathbf{d}}\big(\{+\frac{1}{2}\}\big)$ is *certain* for the state $|d_+\rangle$.

- $\mathrm{p}_{|d_-\rangle}\big(Spin_{\mathbf{d}}\big(\{-\frac{1}{2}\}\big)\big) = 1.$
  The event $Spin_{\mathbf{d}}\big(\{-\frac{1}{2}\}\big)$ is *certain* for the state $|d_-\rangle$.

According to the quantum-theoretic formalism, for any choice of two different directions **d** and **e**, the two observables $Spin_{\mathbf{d}}$ and $Spin_{\mathbf{e}}$ represent two *incompatible* physical quantities that cannot be simultaneously measured. As a consequence we have:

- $\mathrm{p}_{|d_+\rangle}\big(Spin_{\mathbf{e}}\big(\{+\frac{1}{2}\}\big)\big) \neq 1, 0;\quad \mathrm{p}_{|d_+\rangle}\big(Spin_{\mathbf{e}}\big(\{-\frac{1}{2}\}\big)\big) \neq 1, 0.$
- $\mathrm{p}_{|d_-\rangle}\big(Spin_{\mathbf{e}}\big(\{+\frac{1}{2}\}\big)\big) \neq 1, 0;\quad \mathrm{p}_{|d_-\rangle}\big(Spin_{\mathbf{e}}\big(\{-\frac{1}{2}\}\big)\big) \neq 1, 0.$
- $\mathrm{p}_{|e_+\rangle}\big(Spin_{\mathbf{d}}\big(\{+\frac{1}{2}\}\big)\big) \neq 1, 0;\quad \mathrm{p}_{|e_+\rangle}\big(Spin_{\mathbf{d}}\big(\{-\frac{1}{2}\}\big)\big) \neq 1, 0.$
- $\mathrm{p}_{|e_-\rangle}\big(Spin_{\mathbf{d}}\big(\{+\frac{1}{2}\}\big)\big) \neq 1, 0;\quad \mathrm{p}_{|e_-\rangle}\big(Spin_{\mathbf{d}}\big(\{-\frac{1}{2}\}\big)\big) \neq 1, 0.$

We will now describe the physical situation which the EPR-paradox refers to. We are dealing with a composite system **S** consisting of two electrons $\mathbf{S}_1$ and $\mathbf{S}_2$ that have interacted before a given time $t_0$. As a consequence of this interaction, the spin-values of $\mathbf{S}_1$ and $\mathbf{S}_2$ (in any direction) are correlated:

the spin-value of $\mathbf{S}_1$ is up (down) iff the spin-value of $\mathbf{S}_2$ is down (up).

Suppose that at time $t_0$ the spin-value in the **x**-direction (associated to the canonical basis $\mathbf{B}_C = \{|0\rangle, |1\rangle\}$) is indeterminate for both subsystems $\mathbf{S}_1$ and $\mathbf{S}_2$. The state of the composite system **S** can be represented by the following superposition:

$$|\psi\rangle^{\mathbf{S}}(t_0) = \frac{1}{\sqrt{2}}|1, 0\rangle + \frac{1}{\sqrt{2}}|0, 1\rangle.$$

Suppose the system **S** remains isolated during the time interval $[t_0, t_1]$. According to Schrödinger's equation, for any time $t$ such that $t_0 \leq t \leq t_1$, we will have:

$$|\psi\rangle^{\mathbf{S}}(t) = |\psi\rangle^{\mathbf{S}}(t_0).$$

During the interval $[t_0, t_1]$ the two subsystems $\mathbf{S}_1$ and $\mathbf{S}_2$ (which had interacted before time $t_0$) may be "physically separated" in a very strong sense: no signal can be sent from the space-time region where $\mathbf{S}_1$ is located to the space-time region where $\mathbf{S}_2$ is located (in other words, the two regions are *space-like separated*).

Suppose now that during the time-interval $[t_1, t_2]$ an observer $\mathbf{O}_1$ (who has physical access to the subsystem $\mathbf{S}_1$) *decides* to perform on $\mathbf{S}_1$ a measurement of the observable $Spin_{\mathbf{x}}$. Suppose the outcome of this measurement is the number $+\frac{1}{2}$, which is the eigenvalue corresponding to the eigenvector $|1\rangle$ of the self-adjoint operator $A_{Spin_{\mathbf{x}}}$. By applying von Neumann-Lüders' axiom to the state of the global system **S**, we obtain:

$$\frac{1}{\sqrt{2}}|1, 0\rangle + \frac{1}{\sqrt{2}}|0, 1\rangle \quad \mapsto_M \quad |1, 0\rangle.$$

The measurement performed by the observer $\mathbf{O}_1$ has transformed a "potential" $Spin_{\mathbf{x}}$-value into an "actual" value not only for the subsystem $\mathbf{S}_1$ that is "close" to $\mathbf{O}_1$, but even for $\mathbf{S}_2$, which is "far apart".

Such a "spooky action at distance", which may appear *prima facie* strange and counter-intuitive, is not in principle contradictory. In order to derive a *formal contradiction*, Einstein, Podolsky and Rosen make recourse to three general assumptions that do not strictly belong to the quantum-theoretic formalism:

1. *the reality-principle*;
2. *the physical completeness-principle*;
3. *the locality-principle*.

### The Reality-Principle

The reality-principle represents a philosophical assumption that can be naturally connected with a "realistic" interpretation of physical theories. According to Einstein, Podolsky and Rosen:

*If, without in any way disturbing the system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exists an element of reality corresponding to that physical quantity.*

What is the exact meaning of the somewhat obscure expression "element of reality"? This question has stimulated long and deep debates in the literature about the philosophy of quantum mechanics. According to a natural interpretation, the reality-principle can be regarded as a proposal of a *sufficient condition* for a physical property to be *objective*, independently of any observer's action.

### The Physical Completeness-Principle

*Every element of physical reality must have a counterpart in the physical theory.*

This principle suggests a connection between two different domains: the "ontological" world of *elements of reality* and the mathematical world of pure states (which are maximal pieces of information): any *objective* physical property shall be reflected in an appropriate pure state of the theory. Notice that the concept of "physical completeness" should not be confused with the concept of "logical completeness": one is dealing with two conditions that are formulated in two different languages. While "logical completeness" can be described in the language of the quantum-theoretic formalism (for any quantum event $X$ and any pure state $|\psi\rangle$, either $\mathtt{p}_{|\psi\rangle}(X) = 1$ or $\mathtt{p}_{|\psi\rangle}(X^{\perp}) = 1$), "physical completeness" is formulated in a hybrid language, which refers to the mysterious "elements of reality".

### The Locality-Principle

Unlike the reality-principle and the physical completeness-principle (which are based on some deeply philosophical assumptions), the locality-principle represents a "genuine" physical assertion that is rooted in relativity theory:

*there cannot exist any superluminal interaction between physical systems that are space-like separated.*

Using the principles of reality, of physical completeness and of locality, one can now formally derive the "EPR-contradiction". By means of his (her) measurement on the "close" system $\mathbf{S}_1$, the observer $\mathbf{O}_1$ has tested that the "far" system $\mathbf{S}_2$ *certainly verifies* the event $Spin_{\mathbf{x}}(\{-\frac{1}{2}\})$ (the *spin* in the $\mathbf{x}$ direction is down). By the locality-principle, $\mathbf{O}_1$ could not physically interact with $\mathbf{S}_2$ (which is space-like separated from $\mathbf{S}_1$). Hence, by the reality-principle, the event $Spin_{\mathbf{x}}(\{-\frac{1}{2}\})$ corresponds to an *objective* property of $\mathbf{S}_2$: an element of physical reality that will be here indicated by $\mathfrak{P}_{\mathbf{x}}^-$. Since $\mathbf{S}_2$ has been isolated during the interval $[t_0, t_2]$, $\mathfrak{P}_{\mathbf{x}}^-$ must represent an objective property of $\mathbf{S}_2$ already at time $t_0$.

At this point one can apply a *counterfactual argument*. The choice of measuring on $\mathbf{S}_1$ the spin-value in the $\mathbf{x}$-direction (instead of a different direction, say $\mathbf{y}$) depends on the subjective free will of the observer $\mathbf{O}_1$. Hence, the following counterfactual implication can be asserted:

*Should* $\mathbf{O}_1$ *have chosen to measure on* $\mathbf{S}_1$ *the observable* $Spin_{\mathbf{y}}$ instead of $Spin_{\mathbf{x}}$, *either* $\mathfrak{P}_{\mathbf{y}}^+$ *or* $\mathfrak{P}_{\mathbf{y}}^-$ *would be an objective property of* $\mathbf{S}_2$ *at time* $t_0$

(where $\mathfrak{P}_{\mathbf{y}}^+$ and $\mathfrak{P}_{\mathbf{y}}^-$ correspond to the events $Spin_{\mathbf{y}}(\{+\frac{1}{2}\})$ and $Spin_{\mathbf{y}}(\{-\frac{1}{2}\})$, respectively).

By definition of objectivity, the objective properties of $\mathbf{S}_2$ at time $t_0$ cannot depend on the subjective choices taken by a "far" observer at a later time. Consequently:

either $[\mathfrak{P}_{\mathbf{x}}^-$ and $\mathfrak{P}_{\mathbf{y}}^+]$ or $[\mathfrak{P}_{\mathbf{x}}^-$ and $\mathfrak{P}_{\mathbf{y}}^-]$ is an objective property of $\mathbf{S}_2$ at time $t_0$.

Hence, by the physical completeness-principle, quantum theory must have a "counterpart" for such an objective property. Thus, there exists a pure state $|\psi\rangle$ of $\mathbf{S}_2$ such that:

$$\text{either } \left[\mathtt{p}_{|\psi\rangle}\left(Spin_{\mathbf{x}}\left(\left\{-\frac{1}{2}\right\}\right)\right) = 1 \text{ and } \mathtt{p}_{|\psi\rangle}\left(Spin_{\mathbf{y}}\left(\left\{+\frac{1}{2}\right\}\right)\right) = 1\right]$$

$$\text{or } \left[\mathtt{p}_{|\psi\rangle}\left(Spin_{\mathbf{x}}\left(\left\{-\frac{1}{2}\right\}\right)\right) = 1 \text{ and } \mathtt{p}_{|\psi\rangle}\left(Spin_{\mathbf{y}}\left(\left\{-\frac{1}{2}\right\}\right)\right) = 1\right].$$

This conclusion, however, contradicts the physical incompatibility of the two observables $Spin_{\mathbf{x}}$ and $Spin_{\mathbf{y}}$ (which is asserted by a theorem of quantum theory).

How can we block the derivation of this contradiction? The proof of a contradiction in a scientific theory is, in a sense, similar to the discovery of a murder in the framework of a detective story. And each solution that is proposed to avoid the contradiction plays the role of a detective who identifies the murderer. Of course, as happens in detective stories, scientific paradoxes also may have different solutions. In the case of the EPR-argument the possibly "guilty" hypotheses are the three principles: *reality*, *physical completeness*, *locality*. Each *solution* of the EPR-paradox is characterized by a different choice of some guilty hypotheses.

Einstein, Podolsky and Rosen did not have any doubt: the hypothesis that has to be rejected is the physical completeness-principle. The original version of the EPR-argument was presented as a kind of *proof by contradiction* whose conclusion was: *quantum theory is physically incomplete*. In other words, the pure states of the theory do not represent a *maximum of information*: one is dealing with a kind of *statistical pieces of information* that are quite similar to the mixed states of classical statistical mechanics. The article "Can quantum mechanical description of reality be considered complete?" concludes as follows:

*While we have thus proved that the wave function does not provide a complete description of the physical reality, we left open the question whether or not such a description exists. We believe, however, that such a theory is possible.*

This conclusion, however, does not seem justified from a logical point of view. In fact, the EPR-argument only proves the logical incompatibility between quantum theory and the conjunction of our three general principles, without forcing us to choose a particular "guilty hypothesis". For instance, the solution proposed by Niels Bohr and by the "Copenhagen interpretation" is based on the refusal of the reality-principle. According to Bohr, it is not reasonable to speak of "elements of reality", because *all properties of quantum objects have to be dealt with as relations that are context-dependent*.

In more recent times (in the framework of quantum information theories) the locality-principle also has been put in question. One has realized that the action performed by the observer $\mathbf{O}_1$ (on the "close" system $\mathbf{S}_1$) may have a "genuine physical influence" on the "far" system $\mathbf{S}_2$. Such a phenomenon, however, does not imply the possibility of sending a signal from $\mathbf{O}_1$ to a hypothetical observer $\mathbf{O}_2$, "close" to the system $\mathbf{S}_2$. In spite of a superficial appearance, there is no conflict between quantum non-locality and special relativity (which was Einstein's basic worry).

In 1985, half a century after the appearing of the EPR-article, Nathan Rosen was still alive. A number of conferences were organized in order to celebrate the discovery of the famous paradox; and sometimes the "honor guest" was, of course, Rosen. How did the "third man" of the *trio* regard the EPR-argument, fifty years after? The following quotation represents an interesting witnessing:

*At the time of the writing of the EPR paper I agreed with the belief expressed at the end that a complete theory is possible. Since then fifty years have passed and physics has changed greatly. In recent years doubts have arisen in my mind as to whether a theory will be found in the future that will be complete according to the criteria of the paper and will be correct in giving agreement with observations ..... Hence it is hard to believe that a theory will be found that will be complete, based on the criterion of an element of reality, used in the paper. It may also be that in the future physical theories will describe reality in different terms from those to which we are now accustomed. Does this means that the EPR paper is useless? I think not. The paper has led to a great deal of discussion that has helped to clarify the* *physical concepts. I like to believe that this has contributed, if in a small measure, to the progress of physics.*[4]

## 3.3 Quantum Teleportation

EPR-situations play an essential role in teleportation-phenomena, which may appear *prima facie* puzzling, both from a physical and from a logical point of view.[5]

Let us briefly illustrate a typical teleportation-case. We are dealing with a composite quantum system

$$\mathbf{S} = \mathbf{S}_1 + \mathbf{S}_2 + \mathbf{S}_3,$$

consisting of three particles (say, three photons) whose states are supposed to live in the space $\mathbb{C}^2$. As happens in the case of EPR-situations, the systems $\mathbf{S}_2$ and $\mathbf{S}_3$ have interacted before a given time $t_0$ and are supposed to be physically separated at time $t_0$. As a consequence of the past interaction, the state of the composite system $\mathbf{S}_2 + \mathbf{S}_3$ is the following entangled Bell-state:

$$|\psi\rangle_{t_0}^{\mathbf{S}_2+\mathbf{S}_3} = \frac{1}{\sqrt{2}}\left(|0, 0\rangle + |1, 1\rangle\right).$$

Two human agents are supposed to act in the teleportation-experiment: the observers *Alice* and *Bob*. At time $t_0$ both of them *know* that the state of the system $\mathbf{S}_2 + \mathbf{S}_3$ is $\frac{1}{\sqrt{2}}(|0, 0\rangle + |1, 1\rangle)$. While $\mathbf{S}_2$ is physically accessible to *Alice*, $\mathbf{S}_3$ is accessible to *Bob*. At the same time *Alice* has also access to $\mathbf{S}_1$, whose state is the qubit

$$|\psi\rangle_{t_0}^{\mathbf{S}_1} = a|0\rangle + b|1\rangle \ \ (\text{with } \ a, b \neq 0).$$

At any time $t$ of a given time-sequence, both observers have a global or a partial information about the state of the composite system $\mathbf{S}$. Furthermore, both of them can modify the state of $\mathbf{S}$ (or of a subsystem of $\mathbf{S}$) either by applying some gates or by performing a measurement, which induces a collapse of the wave function.

The *epistemic situation* of either observer $\mathbf{O}$ at any time $t$ (of the considered time-sequence) can be represented as a pair consisting of:

(a) the physical system $\mathbf{S}_{\mathbf{O}_t}$ that is physically accessible to our observer;
(b) a state $\rho_{\mathbf{O}_t}$ that represents the observer's information about a given system that does not necessarily coincide with $\mathbf{S}_{\mathbf{O}_t}$.

We will write:

$$Inf(\mathbf{O}_t) = (\mathbf{S}_{\mathbf{O}_t}, \rho_{\mathbf{O}_t}).$$

---

[4]See [4].

[5]See, for instance, [5–7].

We can now represent the epistemic situations of *Alice* and *Bob* at the initial time $t_0$ as follows.

**Alice at time** $t_0$

$Inf(Alice_{t_0}) = \left((\mathbf{S}_1 + \mathbf{S}_2)_{t_0}, |\psi\rangle^{\mathbf{S}}_{t_0}\right)$, where
$|\psi\rangle^{\mathbf{S}}_{t_0} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle) =$
$\frac{1}{\sqrt{2}}(a|0\rangle \otimes (|0,0\rangle + |1,1\rangle)) + \frac{1}{\sqrt{2}}(b|1\rangle \otimes (|0,0\rangle + |11\rangle))$.

Thus, *Alice* has physical access to the subsystem $\mathbf{S}_1 + \mathbf{S}_2$. At the same time, she is informed about the state of the global system $\mathbf{S}$.

**Bob at time** $t_0$

$Inf(Bob_{t_0}) = \left((\mathbf{S}_3)_{t_0}, |\psi\rangle^{\mathbf{S}_2+\mathbf{S}_3}_{t_0}\right)$, where
$|\psi\rangle^{\mathbf{S}_2+\mathbf{S}_3}_{t_0} = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$.

Thus, *Bob* has physical access to the subsystem $\mathbf{S}_3$. At the same time, he is informed about the state of the system $\mathbf{S}_2 + \mathbf{S}_3$.

The basic goal of quantum teleportation is transmitting a state to a "far" observer by means of a quantum non-locality phenomenon. In this particular case, *Alice* wants to transmit to *Bob* the qubit $a|0\rangle + b|1\rangle$, which is the pure state of particle $\mathbf{S}_1$ at time $t_0$. As expected, the operations performed by *Alice* in order to obtain this aim will transform her epistemic situation.

**Alice at time** $t_1$

In the interval $[t_0, t_1]$ *Alice* applies the gate $\mathtt{XOR}^{(1,1)}$ to the subsystem $\mathbf{S}_1 + \mathbf{S}_2$ (accessible to her). As a consequence, we obtain:

$$Inf(Alice_{t_1}) = \left((\mathbf{S}_1 + \mathbf{S}_2)_{t_1}, |\psi\rangle^{\mathbf{S}}_{t_1}\right), \text{ where:}$$

$|\psi\rangle^{\mathbf{S}}_{t_1} = \left[\mathtt{XOR}^{(1,1)} \otimes \mathtt{I}^{(1)}\right] |\psi\rangle^{\mathbf{S}}_{t_0} =$
$\frac{1}{\sqrt{2}}(a|0\rangle \otimes (|0,0\rangle + |1,1\rangle)) + \frac{1}{\sqrt{2}}(b|1\rangle \otimes (|1,0\rangle + |0,1\rangle))$.

It is worth-while noticing that *theoretically Alice* is acting on the whole system $\mathbf{S}$, while *materially* she is only acting on the subsystem $\mathbf{S}_1 + \mathbf{S}_2$ that is accessible to her.

**Alice at time** $t_2$

In the interval $[t_1, t_2]$ *Alice* applies the Hadamard-gate to the system $\mathbf{S}_1$ (whose state is to be teleported). Hence, we obtain:

$$Inf(Alice_{t_2}) = \left((\mathbf{S}_1 + \mathbf{S}_2)_{t_2}, |\psi\rangle^{\mathbf{S}}_{t_2}\right), \text{ where:}$$

$|\psi\rangle^{\mathbf{S}}_{t_2} = \left[\sqrt{\mathtt{I}}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)}\right] |\psi\rangle^{\mathbf{S}}_{t_1} =$
$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\{[a(|0\rangle + |1\rangle) \otimes (|0,0\rangle + |1,1\rangle)] + [b(|0\rangle - |1\rangle) \otimes (|1,0\rangle + |0,1\rangle)]\} =$
$\frac{1}{2}[(|0,0\rangle \otimes (a|0\rangle + b|1\rangle)) + (|0,1\rangle \otimes (a|1\rangle + b|0\rangle))+$
$(|1,0\rangle \otimes (a|0\rangle - b|1\rangle)) + (|1,1\rangle \otimes (a|1\rangle - b|0\rangle))]$.

**Alice at time $t_3$**

In the interval $[t_2, t_3]$ *Alice* decides to perform a measurement on the subsystem $\mathbf{S}_1 + \mathbf{S}_2$ (accessible to her). As a consequence (by collapse of the wave function) she will obtain with equal probability ($= \frac{1}{4}$) one of the four following quregisters:

1. $|\psi_1\rangle_{t_3}^{\mathbf{S}} = |0, 0\rangle \otimes (a|0\rangle + b|1\rangle)$
2. $|\psi_2\rangle_{t_3}^{\mathbf{S}} = |0, 1\rangle \otimes (a|1\rangle + b|0\rangle)$
3. $|\psi_3\rangle_{t_3}^{\mathbf{S}} = |1, 0\rangle \otimes (a|0\rangle - b|1\rangle)$
4. $|\psi_4\rangle_{t_3}^{\mathbf{S}} = |1, 1\rangle \otimes (a|1\rangle - b|0\rangle)$

We have:

$$Inf(Alice_{t_3}) = \left((\mathbf{S}_1 + \mathbf{S}_2)_{t_3}, |\psi_i\rangle_{t_3}^{\mathbf{S}}\right), \text{ where:}$$

$|\psi_i\rangle_{t_3}^{\mathbf{S}}$ is one of the four states considered above.

Notice that after *Alice*'s measurement (at time $t_3$) the original superposed state $a|0\rangle + b|1\rangle$ of particle $\mathbf{S}_1$ has disappeared. The state of $\mathbf{S}_1$ is now:

$$|\psi\rangle_{t_3}^{\mathbf{S}_1} = Red^1(|\psi_i\rangle_{t_3}^{\mathbf{S}}),$$

which is a bit $|x\rangle$.

As a consequence of her measurement, *Alice* also knows the qubit representing the state at time $t_3$ of particle $\mathbf{S}_3$ (accessible to *Bob*). In fact, by quantum non-locality, the state of particle $\mathbf{S}_3$ has been transformed into one of the four possible qubits:

$$|\varphi_i\rangle_{t_3}^{\mathbf{S}_3} = Red^3(|\psi_i\rangle_{t_3}^{\mathbf{S}}), \text{ with } 1 \le i \le 4.$$

Apparently, only $|\varphi_1\rangle_{t_3}^{\mathbf{S}_3}$ is the qubit $a|0\rangle + b|1\rangle$, the original state of particle $\mathbf{S}_1$ (accessible to *Alice*). Anyway, by application of a convenient gate, all states $|\varphi_i\rangle_{t_3}^{\mathbf{S}_3}$ can be transformed into the state $a|0\rangle + b|1\rangle$. We have:

- $\mathtt{I}^{(1)}(|\varphi_1\rangle_{t_3}^{\mathbf{S}_3}) = a|0\rangle + b|1\rangle$
- $\mathtt{NOT}^{(1)}(|\varphi_2\rangle_{t_3}^{\mathbf{S}_3}) = a|0\rangle + b|1\rangle$
- $\mathtt{Z}^{(1)}(|\varphi_3\rangle_{t_3}^{\mathbf{S}_3}) = a|0\rangle + b|1\rangle$
- $\mathtt{NOT}^{(1)}\mathtt{Z}^{(1)}(|\varphi_4\rangle_{t_3}^{\mathbf{S}_3}) = a|0\rangle + b|1\rangle$,

where $\mathtt{Z}^{(1)}$ is the third *Pauli matrix*, which is defined as follows on the canonical basis of $\mathbb{C}^2$:

$$\mathtt{Z}^{(1)}|0\rangle = |0\rangle; \quad \mathtt{Z}^{(1)}|1\rangle = -|1\rangle.$$

In this situation, *Alice* can give an "order" to *Bob*, by using a classical communication channel (say, a phone) during the interval $[t_3, t_4]$. The order will be:

- "apply $\mathtt{I}^{(1)}$!" (i.e. "don't do anything!"), in the first case.
- "apply $\mathtt{NOT}^{(1)}$!", in the second case.
- "apply $\mathtt{Z}^{(1)}$!", in the third case.
- "apply $\mathtt{NOT}^{(1)}\mathtt{Z}^{(1)}$!", in the fourth case.

Suppose that *Bob* follows *Alice*'s order in the interval $[t_4, t_5]$. His final epistemic situation (at time $t_5$) will be:

$$Inf(Bob_{t_5}) = \left((\mathbf{S}_3)_{t_5}, |\psi\rangle_{t_5}^{\mathbf{S}_3}\right),$$

where $|\psi\rangle_{t_5}^{\mathbf{S}_3} = a|0\rangle + b|1\rangle$.

Teleportation is now completed. At the end of the process, the original qubit $a|0\rangle + b|1\rangle$ has disappeared for *Alice*, because at the final time the system $\mathbf{S}_1$ is storing a classical bit. *Bob*, instead, has acquired the information $a|0\rangle + b|1\rangle$, which is stored by "his" particle $\mathbf{S}_3$, whose original state was the proper mixture:

$$Red^2\left(|\psi\rangle_{t_0}^{\mathbf{S}_2+\mathbf{S}_3}\right) = Red^2\left(\frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)\right) = \frac{1}{2}\mathtt{I}^{(1)}.$$

Of course, what has been sent from *Alice* to *Bob* is not the "material" object $\mathbf{S}_1$, but rather the qubit $a|0\rangle + b|1\rangle$, that was the state of $\mathbf{S}_1$ at the initial time $t_0$.

When discussing teleportation, one often stresses that the qubit $a|0\rangle + b|1\rangle$, transmitted to *Bob*, might be *unknown* to *Alice*. Such observation (which may appear *prima facie* somewhat puzzling) can be interpreted as follows.

- At time $t_0$ *Alice* has physical access to particle $\mathbf{S}_1$;
- *Alice* knows that the state of $\mathbf{S}_1$ (at time $t_0$) is pure: a genuine qubit whose form is $a|0\rangle + b|1\rangle$;
- in spite of this, *Alice* ignores the actual values of the two amplitudes $a$ and $b$, which are dealt with by her as complex-number variables.

We could say that what *Alice* actually knows is not a genuine qubit-state, but rather a kind of *metastate* (which ranges over all possible genuine qubit-states). Such ignorance, however, does not prevent *Alice* to perform all operations that are needed in order to transmit a genuine qubit-state to *Bob*. She can physically act on the subsystem $\mathbf{S}_1 + \mathbf{S}_2$ (accessible to her) both by applying the convenient *material* gates and by performing the measurement that determines the final collapse of the wave function. At the same time, she can *theoretically* calculate the *metastates* that correspond to the states $|\psi\rangle_{t_1}^{\mathbf{S}}$, $|\psi\rangle_{t_2}^{\mathbf{S}}$, $|\psi\rangle_{t_3}^{\mathbf{S}}$. dealing with variable instead of constant amplitudes.

Teleportation is not only a puzzling *Gedankenexperiment*: it has been experimentally realized with greater and greater efficiency by different experimental teams in different places. The first teleportation-experiments have been performed (independently) by teams of physicists in Innsbruck and in Rome (in the Nineties).[6] In 2004 Anton Zeilinger and a group of physicists of the "Institute for Experimental Physics" in Vienna have performed a teleportation-experiment on the river Danube

[6]See [8, 9].

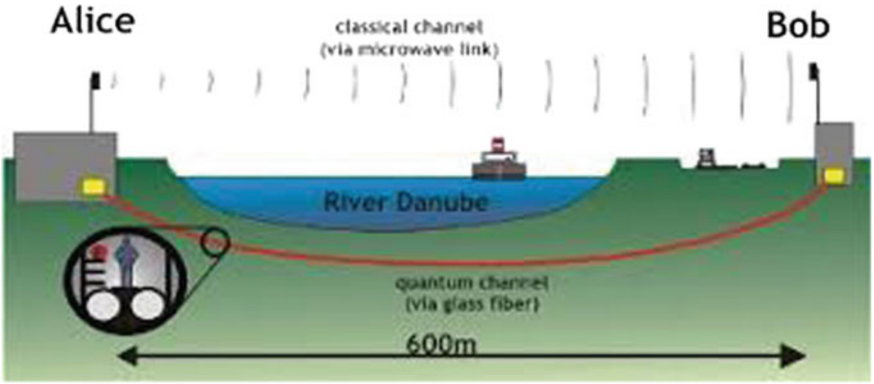



**Fig. 3.1** Teleportation on the Danube

with optimal efficiency. Three distinct photon-states were teleported over a distance of 600 meters across the river (Fig. 3.1).[7]

More recently, a group of physicists in China have experimented a long-distance teleportation of single photon-qubits from a ground observatory to a low Earth-orbit satellite with a distance up to 1400 Km.[8]

## References


1. Schrödinger, E.: Discussion of probability relations between separated systems. Proc. Camb. Philos. Soc. **31**(32), 555–563 (1936)
2. Einstein, A., Podolsky, B., Rosen, N.: Can quantum mechanical description of reality be considered complete? Phys. Rev. **47**, 777–780 (1935)
3. Bohm, D.: Quantum Theory. Prentice-Hall, Englewoods Cliffs (1951)
4. Rosen, N.: Quantum mechanics and reality. In: Lahti, P., Mittelstaedt, P. (eds.) Symposium on the Foundations of Modern Physics. World Scientific, Singapore (1985)
5. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
6. Zeilinger, A.: Einsteins Schleier. Die neue Welt der Quantenphysik. Verlag C. H. Beck oHG, München (2003)
7. Beltrametti, E., Dalla Chiara, M.L., Giuntini, R., Sergioli, G.: Quantum teleportation and quantum epistemic semantics. Math. Slovaca **62**(6), 1–24 (2012)
8. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**(6660), 575–579 (1997)
9. Boschi, D., Branca, S., De Martini, F., Hardy, L., Popescu, S.: Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **80**(6), 1121–1125 (1998)
10. Ursin, R., Jennewein, T., Aspelmeyer, M., Kaltenback, R., Lindenthal, M., Walther, P., Zeilinger, A.: Communications: Quantum teleportation across the Danube. Nature **430**(7002), 849 (2004)


[7] See [10].

[8] See [11].

11. Ren, J.G., Xu, P., Yong, H.L., Zhang, L., Liao, S.K., Yin, J., Liu, W.Y., Cai, W.Q., Yang, M., Li, L., Yang, K.X., Han, X., Yao, Y.Q., Li, J., Wu, H.Y., Wan, S., Liu, L., Liu, D.Q., Kuang, Y.W., He, Z.P., Shang, P., Guo, C., Zheng, R.-H., Tian, K., Zhu, Z.C., Liu, N.L., Lu, C.Y., Shu, R., Chen, Y.A., Peng, C.Z., Wang, J.Y., Pan, J.W.: Ground-to-satellite quantum teleportation. Nature **549**(7670), 70–73 (2017)

# Chapter 4
# From Quantum Circuits to Quantum Computational Logics

## 4.1 A New Approach to Quantum Logic: Quantum Computational Logics

The theory of quantum logical circuits has naturally inspired new forms of quantum logic that have been termed *quantum computational logics*.[1] From a semantic point of view, any formula $\alpha$ of the language of a quantum computational logic is supposed to denote a piece of quantum information: a density operator $\rho$ that lives in a Hilbert space $\mathscr{H}^{\alpha}$ whose dimension depends on the linguistic complexity of $\alpha$. At the same time, the logical connectives are interpreted as special examples of gates. Accordingly, any formula of a quantum computational language can be regarded as a synthetic logical description of a quantum circuit. In this way linguistic formulas acquire a characteristic *dynamic* meaning, representing possible computational actions.

The most natural semantics for quantum computational logics is a form of *holistic* semantics, where the puzzling entanglement-phenomena can be used as a logical resource. As is well known, classical semantics is characterized by a general principle (clearly set forth by Frege): the *compositionality principle*, according to which

> *the meaning of any compound linguistic expression shall be represented as a function of the meanings of its (well-formed) parts.*

Consider, for instance, the sentence "Alice is pretty and Bob loves her". Its meaning is determined by the meanings of its parts (the names "Alice" and "Bob", the predicates "pretty" and "to love", the logical connective "and").

In spite of their strongly non-classical features, both Birkhoff and von Neumann's quantum logic and abstract quantum logic turn out to respect the compositionality principle: the quantum events living in a Hilbert-lattice (as well as the elements of an abstract orthomodular lattice) are *composed* by the algebraic operations $^{\perp}$, $\sqcap$ and $\sqcup$. Hence, in the algebraic semantics of quantum logics the meaning of a molecular

[1] See [2, 3, 7]. Other logical approaches (inspired by quantum information theory) have been proposed, for instance, in [1, 5, 8].



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_4

sentence can always be described as a function of the meanings of its well-formed parts. Notice that only superficially the characteristic behavior of the quantum logical disjunction seems to violate the compositionality-principle. We know that in quantum logic a disjunction $\alpha \vee \beta$ may be true, even if both members ($\alpha$, $\beta$) are not true. However, such a situation would be in contrast with the compositionality-principle only in the framework of a two-valued semantics; while the semantics of all quantum logics is essentially many-valued.

The compositionality-principle breaks down in semantic situations where *meanings* of formulas are represented as *pieces of quantum information* (instead of *quantum events*). As we have seen in the previous chapters, the states of quantum systems have a characteristic *holistic and contextual* behavior. Unlike the case of classical systems, the state of a composite quantum object (say, an electron-system or an atom) determines the states of all its subsystems, and not the other way around. And, generally, the state of the global system cannot be reconstructed as a function of the states of its parts. Such an *anti-compositional* relationship between a *whole* and its *parts* can be naturally applied in order to develop a *holistic and contextual semantics*, which may find significant applications even outside the strict domain of microphysics.

## 4.2 A Sentential Quantum Computational Language

We will now introduce a particular example of a sentential *quantum computational language* $\mathscr{L}_0$, whose alphabet contains atomic formulas (say, "the spin-value in the **x**-direction is up"), including two privileged formulas **t** and **f** that represent the truth-values *Truth* and *Falsity*, respectively. In the semantics all atomic formulas will be interpreted as pieces of quantum information that live in the space $\mathscr{H}^{(1)} = \mathbb{C}^2$.

The connectives of $\mathscr{L}_0$ correspond to some gates that have a special logical and computational interest: the negation $\neg$ (corresponding to the gate *negation*), a ternary connective $\intercal$ (corresponding to the *Toffoli-gate*), the exclusive disjunction $\uplus$ (corresponding to XOR), the square root of the identity $\sqrt{id}$ (corresponding to the *Hadamard-gate*), the square root of negation $\sqrt{\neg}$ (corresponding to the gate *square root of* NOT). The notion of (well-formed) *formula* (or *sentence*) of $\mathscr{L}_0$ is inductively defined (in the expected way): for any formulas $\alpha$, $\beta$ and for any atomic formula **q**, the expressions $\neg\alpha$, $\sqrt{id}\,\alpha$, $\sqrt{\neg}\,\alpha$, $\alpha \uplus \beta$, $\intercal(\alpha, \beta, \mathbf{q})$ are formulas.

Recalling the definition of the holistic conjunction $\mathtt{AND}^{(m,n)}$ in terms of the Toffoli-gate (Definition 2.9), it is useful to introduce a binary logical conjunction $\wedge$ by means of the following metalinguistic definition:

$$\alpha \wedge \beta := \intercal(\alpha, \beta, \mathbf{f})$$

(where the false formula **f** plays the role of a *syntactical ancilla*).

On this basis, a (binary) inclusive disjunction is (metalinguistically) defined via de Morgan-law:

$$\alpha \vee \beta := \neg(\neg\alpha \wedge \neg\beta).$$

The connectives $\neg$, $\wedge$, $\vee$ and $\uplus$ will be also termed *quantum computational Boolean connectives*; while $\sqrt{id}$ and $\sqrt{\neg}$ represent *genuine quantum computational connectives*. A formula that contains at most Boolean connectives is called a *quantum computational Boolean formula* of $\mathscr{L}_0$. In the following we will use $\mathbf{q}$, $\mathbf{q}_1$, $\mathbf{q}_2$, ... as metavariables for atomic formulas, while $\alpha$, $\beta$, $\gamma$, ... will represent generic formulas.

**Definition 4.1** (*The atomic complexity of a formula*) The atomic complexity $At(\alpha)$ of a formula $\alpha$ is the number of *occurrences* of atomic formulas in $\alpha$.

For instance, $At(\top(\mathbf{q}, \mathbf{q}, \mathbf{f})) = 3$. The notion of atomic complexity plays an important semantic role. As we will see (in the next section), the meaning of any formula whose atomic complexity is $n$ shall live in the domain $\mathfrak{D}(\mathscr{H}^{(n)})$. For this reason, the space $\mathscr{H}^{(At(\alpha))}$ (briefly indicated by $\mathscr{H}^{\alpha}$) will be also called the *semantic space* of $\alpha$.

Any formula $\alpha$ can be naturally decomposed into its parts, giving rise to a special configuration called the *syntactical tree* of $\alpha$ (indicated by $STree^{\alpha}$). The configuration $STree^{\alpha}$ can be represented as a finite sequence of *levels*:

$$\begin{array}{c} Level_h^{\alpha} \\ \cdots\cdots \\ Level_1^{\alpha} \end{array}$$

where:

- each $Level_i^{\alpha}$ (with $1 \le i \le h$) is a sequence $(\beta_{i_1}, \ldots, \beta_{i_r})$ of subformulas of $\alpha$;
- the *bottom level* $Level_1^{\alpha}$ is $(\alpha)$;
- the *top level* $Level_h^{\alpha}$ is the sequence $(\mathbf{q}_1, \ldots, \mathbf{q}_k)$, where $\mathbf{q}_1, \ldots, \mathbf{q}_k$ are the atomic occurrences in $\alpha$;
- for any $i$ (with $1 \le i < h$), $Level_{i+1}^{\alpha}$ is the sequence obtained by dropping the *principal connective* in all molecular formulas occurring at $Level_i^{\alpha}$, and by repeating all atomic sentences that occur at $Level_i^{\alpha}$.

By *Height* of $\alpha$ (indicated by $Height(\alpha)$) we mean the number $h$ of levels of the syntactical tree of $\alpha$.

As an example, consider the following formula:

$$\alpha = \neg \top (\sqrt{id}\mathbf{q}, \neg\mathbf{q}, \mathbf{f}) = \neg(\sqrt{id}\mathbf{q} \wedge \neg\mathbf{q}).$$

The syntactical tree of $\alpha$ is the following sequence of levels:

$$\begin{aligned} Level_4^\alpha &= (\mathbf{q}, \mathbf{q}, \mathbf{f}) \\ Level_3^\alpha &= (\sqrt{id}\mathbf{q}, \neg\mathbf{q}, \mathbf{f}) \\ Level_2^\alpha &= (\mathsf{T}(\sqrt{id}\mathbf{q}, \neg\mathbf{q}, \mathbf{f})) \\ Level_1^\alpha &= (\neg\, \mathsf{T}\, (\sqrt{id}\mathbf{q}, \neg\mathbf{q}, \mathbf{f})) \end{aligned}$$

Clearly, $Height(\alpha) = 4$.

The syntactical tree of any formula $\alpha$ uniquely determines a sequence of gates, all defined on the semantic space of $\alpha$. As an example, consider again the formula $\alpha = \neg\, \mathsf{T}\, (\sqrt{id}\mathbf{q}, \neg\mathbf{q}, \mathbf{f})$. In the syntactical tree of $\alpha$ the third level has been obtained from the fourth level by applying the connective $\sqrt{id}$ to the first occurrence of $\mathbf{q}$, by negating the second occurrence of $\mathbf{q}$ and by repeating $\mathbf{f}$, while the second and the first level have been obtained by applying, respectively, the connectives $\mathsf{T}$ and $\neg$ to formulas occurring at the levels immediately above. Accordingly, one can say that the syntactical tree of $\alpha$ uniquely determines the following sequence consisting of three gates, all defined on the semantic space of $\alpha$:

$$\left({}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{I}^{(1)}, \quad {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}, \quad {}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\right).$$

Such a sequence is called the *gate tree* of $\alpha$. This procedure can be naturally generalized to any formula $\alpha$. The general form of the gate tree of $\alpha$ will be:

$$({}^{\mathfrak{D}}\mathtt{G}^\alpha_{(h-1)}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^\alpha_{(1)}),$$

where $h$ is the Height of $\alpha$.

Apparently, given a formula $\alpha$, its gate tree describes a particular example of a quantum circuit. This is the reason why any formula $\alpha$ of the quantum computational language can be regarded as a synthetic logical description of a corresponding quantum circuit $\mathscr{C}^\alpha$, whose possible inputs and outputs live in the semantic space $\mathscr{H}^\alpha$. Clearly, the *width* and the *depth* of $\mathscr{C}^\alpha$ are determined (respectively) by the atomic complexity of $\alpha$ and by the height of its syntactical tree.

Consider, for instance, the formula

$$\alpha = \sqrt{id}\, \mathsf{T}\, (\mathbf{q}, \neg\mathbf{q}, \mathbf{f}).$$

The quantum circuit $\mathscr{C}^\alpha$ corresponding to $\alpha$ is the circuit represented in Fig. 4.1 (which has been illustrated in Sect. 2.3).

Of course, by obvious cardinality-reasons, not all possible quantum circuits can be exactly described by formulas of a quantum computational language (whose alphabet is denumerable).

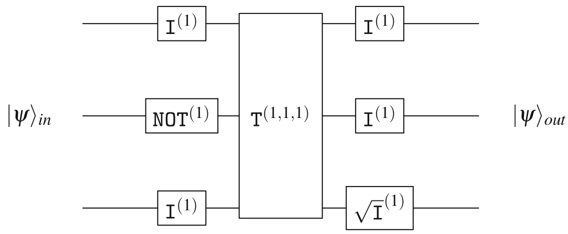



**Fig. 4.1** A circuit for the gate-sequence $(\mathtt{I}^{(1)} \otimes \mathtt{NOT}^{(1)} \otimes \mathtt{I}^{(1)},\ \mathtt{T}^{(1,1,1)},\ \mathtt{I}^{(1)} \otimes \mathtt{I}^{(1)} \otimes \sqrt{\mathtt{I}}^{(1)})$

## 4.3 A Holistic Computational Semantics

We will now introduce the basic concepts of a *holistic quantum computational semantics* for the language $\mathscr{L}_0$. The intuitive idea can be sketched as follows. Interpreting $\mathscr{L}_0$ means determining a *holistic model* that assigns to any formula $\alpha$ a *global informational meaning* living in $\mathscr{H}^\alpha$ (the semantic space of $\alpha$). This meaning determines the *contextual meanings* of all subformulas of $\alpha$ (from the whole to the parts). It may happen that one and the same model assigns to a given formula $\alpha$ different contextual meanings in different contexts.[2]

Before defining the concept of model, we will introduce the weaker notion of *holistic map* for the language $\mathscr{L}_0$.

**Definition 4.2** (*Holistic map*) A *holistic map* for $\mathscr{L}_0$ is a map $\mathtt{Hol}$ that assigns a meaning $\mathtt{Hol}(Level_i^\alpha)$ to each level $(Level_i^\alpha)$ of the syntactical tree of $\alpha$, for any formula $\alpha$. This meaning is a density operator living in the semantic space of $\alpha$.

Given a formula $\gamma$, any holistic map $\mathtt{Hol}$ determines the *contextual meaning*, with respect to the context $\mathtt{Hol}(\gamma)$, of any occurrence of a subformula $\beta$ in $\gamma$. This contextual meaning can be defined, in a natural way, by using the notion of *reduced state*.

**Definition 4.3** (*Contextual meaning*) Consider a formula $\gamma$ such that $Level_i^\gamma = (\beta_{i_1}, \ldots, \beta_{i_r})$. We have:

$$\mathscr{H}^\gamma = \mathscr{H}^{\beta_{i_1}} \otimes \ldots \otimes \mathscr{H}^{\beta_{i_r}}.$$

Let $\mathtt{Hol}$ be a holistic map. The *contextual meaning* of the occurrence $\beta_{i_j}$ with respect to the context $\mathtt{Hol}(\gamma)$ is defined as follows:

$$\mathtt{Hol}^\gamma(\beta_{i_j}) := Red^j_{[At(\beta_{i_1}),\ldots,At(\beta_{i_r})]}(\mathtt{Hol}(Level_i(\gamma))).$$

Of course, we obtain:

$$\mathtt{Hol}^\gamma(\gamma) = \mathtt{Hol}(\gamma).$$

[2] See [4, 6].

A holistic map $\mathtt{Hol}$ is called *normal for a formula* $\gamma$ iff for any subformula $\beta$ of $\gamma$, $\mathtt{Hol}$ assigns the same contextual meaning to all occurrences of $\beta$ in the syntactical tree of $\gamma$. In other words:

$$\mathtt{Hol}^\gamma(\beta_{i_j}) = \mathtt{Hol}^\gamma(\beta_{u_v}),$$

where $\beta_{i_j}$ and $\beta_{u_v}$ are two occurrences of $\beta$ in $STree^\gamma$. In such a case we will simply write: $\mathtt{Hol}^\gamma(\beta)$. A *normal holistic map* is a holistic map $\mathtt{Hol}$ that is normal for all formulas $\gamma$.

*Holistic models* of the language $\mathscr{L}_0$ can be now defined as normal holistic maps that preserve the logical form of all formulas, assigning the "right" meaning to the false sentence **f** and to the true sentence **t**.

**Definition 4.4** (*Holistic model*) A *holistic model* of $\mathscr{L}_0$ is a normal holistic map $\mathtt{Hol}$ that satisfies the following conditions for any formula $\alpha$.

(1) Let $({}^{\mathfrak{D}}\mathrm{G}^\alpha_{(h-1)}, \ldots, {}^{\mathfrak{D}}\mathrm{G}^\alpha_{(1)})$ be the gate tree of $\alpha$ and let $1 \le i < h$. Then,

$$\mathtt{Hol}(Level_i^\alpha) = {}^{\mathfrak{D}}\mathrm{G}^\alpha_{(i)}(\mathtt{Hol}(Level_{i+1}^\alpha)).$$

In other words, the meaning of each level (different from the top level) is obtained by applying the corresponding gate to the meaning of the level that occurs immediately above.

(2) Suppose that the false sentence **f** or the true sentence **t** occurs in $STree^\alpha$. Then,

$$\mathtt{Hol}^\alpha(\mathbf{f}) = P_0^{(1)}; \;\; \mathtt{Hol}^\alpha(\mathbf{t}) = P_1^{(1)}.$$

In other words, the contextual meanings of **f** and of **t** are the *Falsity* and the *Truth*, respectively.

On this basis, we put:

$$\mathtt{Hol}(\alpha) := \mathtt{Hol}(Level_1^\alpha),$$

for any formula $\alpha$.

Since all gates are reversible, assigning a value $\mathtt{Hol}(Level_i^\alpha)$ to a particular $Level_i^\alpha$ of $STree^\alpha$ determines the value $\mathtt{Hol}(Level_j^\alpha)$ for any other level $Level_j^\alpha$. Consequently, $\mathtt{Hol}(Level_i^\alpha)$ determines the contextual meaning $\mathtt{Hol}^\alpha(\beta)$ for any subformula $\beta$ of $\alpha$.

Notice that any $\mathtt{Hol}(\alpha)$ represents a kind of autonomous semantic context that is not necessarily correlated with the meanings of other formulas. Generally we have:

$$\mathtt{Hol}^\gamma(\beta) \neq \mathtt{Hol}^\delta(\beta).$$

Thus, one and the same formula may receive different contextual meanings in different contexts (as, in fact, happens in the case of our normal use of natural languages).

The characteristic *holistic* features of the models $\mathtt{Hol}$ are clearly due to the fact that any $\mathtt{Hol}$ assigns to each level of the syntactical tree of a given formula a *global* meaning that determines the contextual meanings of all subformulas occurring at that level. And, generally, this global meaning cannot be represented as the tensor product of the contextual meanings of the subformulas in question.

An interesting case arises when the meaning of the top level of the syntactical tree of a given formula is an entangled state. Consider, for instance, the contradictory formula

$$\alpha = \mathbf{q} \wedge \neg\mathbf{q} \;=\; \top(\mathbf{q}, \neg\mathbf{q}, \mathbf{f}).$$

And let $\mathtt{Hol}$ be a map that assigns the following meanings to the levels of $STree^{\alpha}$:

$$\mathtt{Hol}(Level_3^{\alpha}) = \mathtt{Hol}((\mathbf{q}, \mathbf{q}, \mathbf{f})) = P_{\frac{1}{\sqrt{2}}|1,0,0\rangle + \frac{1}{\sqrt{2}}|0,1,0\rangle}$$
$$\mathtt{Hol}(Level_2^{\alpha}) = \mathtt{Hol}((\mathbf{q}, \neg\mathbf{q}, \mathbf{f})) = P_{\frac{1}{\sqrt{2}}|1,1,0\rangle + \frac{1}{\sqrt{2}}|0,0,0\rangle}$$
$$\mathtt{Hol}(Level_1^{\alpha}) = \mathtt{Hol}((\top(\mathbf{q}, \neg\mathbf{q}, \mathbf{f})) = P_{\frac{1}{\sqrt{2}}|1,1,1\rangle + \frac{1}{\sqrt{2}}|0,0,0\rangle}$$

Clearly, $\mathtt{Hol}$ is a normal map that is also a model for the formula $\alpha$. While $\mathtt{Hol}(\alpha)$ (the meaning of $\alpha$) is a pure entangled state, the contextual meaning of the subformula $\mathbf{q}$ is a proper mixture. We have:

$$\mathtt{Hol}^{\alpha}(\mathbf{q}) = \mathtt{Hol}^{\alpha}(\neg\mathbf{q}) = \frac{1}{2}\mathtt{I}^{(1)}.$$

Consequently:

$$\mathtt{Hol}(\alpha) = \mathtt{Hol}(\top(\mathbf{q}, \neg\mathbf{q}, \mathbf{f})) = {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}((\mathbf{q}, \neg\mathbf{q}, \mathbf{f}))) \neq$$
$${}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}^{\alpha}(\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\neg\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\mathbf{f})).$$

Interestingly enough, the two states

$${}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}((\mathbf{q}, \neg\mathbf{q}, \mathbf{f}))) \text{ and } {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}^{\alpha}(\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\neg\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\mathbf{f}))$$

turn out to have different probability-values. We have:

- $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}((\mathbf{q}, \neg\mathbf{q}, \mathbf{f})))) = \frac{1}{2}$;
- $\mathtt{p}_1({}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\mathtt{Hol}^{\alpha}(\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\neg\mathbf{q}) \otimes \mathtt{Hol}^{\alpha}(\mathbf{f}))) = \frac{1}{4}$.

It is worth-while noticing that in both cases we are dealing with a contradictory sentence $(\mathbf{q} \wedge \neg\mathbf{q})$ whose meaning represents a piece of quantum information that is not *impossible*.

An important special case of the holistic quantum computational semantics is a *compositional semantics*, based on the assumption that all models behave in a compositional way.

**Definition 4.5** (*Compositional model*) A model $\mathtt{Hol}$ is called

- *compositional for a formula* $\alpha$ iff $\mathtt{Hol}$ assigns to the top level

$$Level_h^{\alpha} = (\mathbf{q}_1, \ldots, \mathbf{q}_r)$$

of the syntactical tree of $\alpha$ the following factorized state:

$$\mathtt{Hol}^{\alpha}(\mathbf{q}_1) \otimes \ldots \otimes \mathtt{Hol}^{\alpha}(\mathbf{q}_r).$$

- *compositional* iff $\mathtt{Hol}$ is compositional for all formulas $\alpha$;
- *perfectly compositional* iff $\mathtt{Hol}$ is a compositional model that satisfies the following condition for any formulas $\alpha$, $\beta$ and for any atomic formula $\mathbf{q}$ (occurring in $\alpha$ and in $\beta$):

$$\mathtt{Hol}^{\alpha}(\mathbf{q}) = \mathtt{Hol}^{\beta}(\mathbf{q}).$$

While compositional models may be context-dependent, models that are perfectly compositional are always context-independent.

One can easily show that any compositional model $\mathtt{Hol}$ for a formula $\alpha$ assigns to each level of the syntactical tree of $\alpha$ the tensor product of the contextual meanings of the subformulas occurring at that level. Suppose that $(\beta_{i_1}, \ldots, \beta_{i_r})$ is the $i$th level of $STree^{\alpha}$. We have:

$$\mathtt{Hol}(Level_i^{\alpha}) = \mathtt{Hol}^{\alpha}(\beta_{i_1}) \otimes \ldots \otimes \mathtt{Hol}^{\alpha}(\beta_{i_r}).$$

We call *compositional quantum computational semantics* the special version of the quantum computational semantics based on the hypothesis that all models are compositional.

It is worth-while noticing that the compositional semantics does not forbid the emergence of entangled meanings. An interesting example is represented by the sentence

$$\alpha = \sqrt{id}\, \mathbf{q}_1 \uplus \mathbf{q}_2,$$

whose gate tree is

$$(\sqrt{\mathtt{I}}^{(1)} \otimes \mathtt{I}^{(1)},\ \mathtt{XOR}^{(1,1)}).$$

Consider the following holistic map $\mathtt{Hol}$ for $\alpha$:

$$\mathtt{Hol}(Level_3^{\alpha}) = \mathtt{Hol}((\mathbf{q}_1, \mathbf{q}_2)) = |0, 1\rangle$$

$$\mathtt{Hol}(Level_2^{\alpha}) = \mathtt{Hol}((\sqrt{id}\, \mathbf{q}_1, \mathbf{q}_2)) = (\sqrt{\mathtt{I}}^{(1)} \otimes \mathtt{I}^{(1)})|0, 1\rangle =$$

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

$$\mathtt{Hol}(Level_1^{\alpha}) = \mathtt{Hol}((\sqrt{id}\ \mathbf{q}_1 \uplus \mathbf{q}_2)) =$$

$$\mathtt{XOR}^{(1,1)}(\frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{2}}|1,1\rangle) = \frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{2}}|1,0\rangle.$$

Apparently, this $\mathtt{Hol}$ is a compositional model for $\alpha$ that assigns a classical meaning (the register $|0,1\rangle$) to the top level of $STree^{\alpha}$. At the same time, the meaning assigned by $\mathtt{Hol}$ to $\alpha$ is the entangled Bell-state:

$$\frac{1}{\sqrt{2}}|0,1\rangle + \frac{1}{\sqrt{2}}|1,0\rangle.$$

An important question is the following: do contextual meanings and gates (associated to particular logical connectives) commute? This question receives different answers in the compositional semantics and in the more liberal holistic semantics. In both semantics, the gates corresponding to the 1-ary connectives $\neg$, $\sqrt{id}$ and $\sqrt{\neg}$ turn out to commute with the contextual meanings of the subformulas of a given formula.

**Theorem 4.1** *Consider a holistic model* $\mathtt{Hol}$ *for a formula* $\gamma$.

*(1) Let* $\neg\beta$ *be a subformula of* $\gamma$. *Then,*

$$\mathtt{Hol}^{\gamma}(\neg\beta) = {}^{\mathfrak{D}}\mathtt{NOT}^{(At(\beta))}(\mathtt{Hol}^{\gamma}(\beta)).$$

*(2) Let* $\sqrt{id}\beta$ *be a subformula of* $\gamma$. *Then,*

$$\mathtt{Hol}^{\gamma}(\sqrt{id}\beta) = {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(At(\beta))}(\mathtt{Hol}^{\gamma}(\beta)).$$

*(3) Let* $\sqrt{\neg}\beta$ *be a subformula of* $\gamma$. *Then,*

$$\mathtt{Hol}^{\gamma}(\sqrt{\neg}\beta) = {}^{\mathfrak{D}}\sqrt{\mathtt{NOT}}^{(At(\beta))}(\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta)).$$

*Thus, the contextual meaning of* $\neg\beta$, $\sqrt{id}\beta$, $\sqrt{\neg}\beta$ *can be obtained by applying the corresponding gate to the contextual meaning of* $\beta$.

*Proof* By definition of syntactical tree, of gate tree, of holistic model and of contextual meaning. □

In the holistic semantics the commutativity between contextual meanings and gates generally fails in the case of the binary connective $\uplus$ and of the ternary connective $\top$. As we have seen, the $\mathtt{XOR}$-gate and the Toffoli-gate have a characteristic holistic behavior; consequently, the following semantic situations are possible:

- $\mathtt{Hol}^{\gamma}(\alpha \uplus \beta) \neq {}^{\mathfrak{D}}\mathtt{XOR}^{(At(\alpha),At(\beta))}(\mathtt{Hol}^{\gamma}(\alpha) \otimes \mathtt{Hol}^{\gamma}(\beta))$.
- $\mathtt{Hol}^{\gamma}(\top(\alpha, \beta, \mathbf{q})) \neq {}^{\mathfrak{D}}\mathtt{T}^{(At(\alpha),At(\beta),At(\mathbf{q}))}(\mathtt{Hol}^{\gamma}(\alpha) \otimes \mathtt{Hol}^{\gamma}(\beta) \otimes \mathtt{Hol}^{\gamma}(\mathbf{q}))$.

At the same time, the connectives $\uplus$ and $\top$ turn out to satisfy a weaker condition, stated by the following theorem.

**Theorem 4.2** *Consider a holistic model* $\mathtt{Hol}$ *for a formula* $\gamma$.

*(1) Let* $\alpha_1 \uplus \alpha_2$ *be a subformula of* $\gamma$. *Thus, the syntactical tree of* $\gamma$ *shall contain two levels whose form is:*

- $Level^{\gamma}_{(i+1)} = (\beta_{(i+1)_1}, \ldots, \beta_{(i+1)_{k_1}}, \beta_{(i+1)_{k_2}}, \ldots, \beta_{(i+1)_r})$, *where* $\alpha_1 = \beta_{(i+1)_{k_1}}$, $\alpha_2 = \beta_{(i+1)_{k_2}}$.
- $Level^{\gamma}_{i} = (\beta_{i_1}, \ldots, \beta_{i_j}, \ldots, \beta_{i_s})$, *where* $\alpha_1 \uplus \alpha_2 = \beta_{i_j}$.

*We have:*

$$\mathtt{Hol}^{\gamma}(\alpha_1 \uplus \alpha_2) = {}^{\mathfrak{D}}\mathtt{XOR}^{(At(\alpha_1), At(\alpha_2))}(Red^{(k_1,k_2)}_{[At(\beta_{(i+1)_1}),\ldots,At(\beta_{(i+1)_r})]}(\mathtt{Hol}(Level_{(i+1)}(\gamma)))).$$

*(2) Let* $\mathsf{T}(\alpha_1, \alpha_2, \mathbf{q})$ *be a subformula of* $\gamma$. *Thus, the syntactical tree of* $\gamma$ *shall contain two levels whose form is.*

- $Level^{\gamma}_{(i+1)} = (\beta_{(i+1)_1}, \ldots, \beta_{(i+1)_{k_1}}, \beta_{(i+1)_{k_2}}, \beta_{(i+1)_{k_3}}, \ldots, \beta_{(i+1)_r})$, *where* $\alpha_1 = \beta_{(i+1)_{k_1}}$, $\alpha_2 = \beta_{(i+1)_{k_2}}$, $\mathbf{q} = \beta_{(i+1)_{k_3}}$.
- $Level^{\gamma}_{i} = (\beta_{i_1}, \ldots, \beta_{i_j}, \ldots, \beta_{i_s})$, *where* $\mathsf{T}(\alpha_1, \alpha_2, \mathbf{q}) = \beta_{i_j}$.

*We have:*

$$\mathtt{Hol}^{\gamma}(\mathsf{T}(\alpha_1, \alpha_2, \mathbf{q})) = {}^{\mathfrak{D}}\mathtt{T}^{(At(\alpha_1), At(\alpha_2), At(\mathbf{q}))}(Red^{(k_1,k_2,k_3)}_{[At(\beta_{(i+1)_1}),\ldots,At(\beta_{(i+1)_r})]}(\mathtt{Hol}(Level_{(i+1)}(\gamma)))).$$

*Proof* By definition of syntactical tree, of gate tree, of holistic model and of contextual meaning. □

Unlike the case of the general holistic semantics, in the less liberal compositional semantics contextual meanings turn out to commute with the gates that correspond to the connectives $\uplus$ and $\mathsf{T}$.

**Theorem 4.3** *Consider a compositional model* $\mathtt{Hol}$ *for a formula* $\gamma$.

*(1) Let* $\alpha_1 \uplus \alpha_2$ *be a subformula of* $\gamma$. *Then,*

$$\mathtt{Hol}^{\gamma}(\alpha_1 \uplus \alpha_2) = {}^{\mathfrak{D}}\mathtt{XOR}^{(At(\alpha_1),\, At(\alpha_2))}(\mathtt{Hol}^{\gamma}(\alpha_1) \otimes \mathtt{Hol}^{\gamma}(\alpha_2)).$$

*(2) Let* $\mathsf{T}(\alpha_1, \alpha_2, \mathbf{q})$ *be a subformula of* $\gamma$. *Then,*

$$\mathtt{Hol}^{\gamma}(\mathsf{T}(\alpha_1,\, \alpha_2,\, \mathbf{q})) = {}^{\mathfrak{D}}\mathtt{T}^{(At(\alpha_1), At(\alpha_2),\, At(\mathbf{q}))}(\mathtt{Hol}^{\gamma}(\alpha_1) \otimes \mathtt{Hol}^{\gamma}(\alpha_2) \otimes \mathtt{Hol}^{\gamma}(\mathbf{q})).$$

*Proof* By definition of compositional model. □

The following theorem will play an important role in the development of the holistic semantics.

**Theorem 4.4** *Consider a formula $\gamma$ and let $\eta$ be a subformula of $\gamma$. For any model* $\mathtt{Hol}$ *and for any formula $\beta$ there exists a model* $^*\mathtt{Hol}$ *such that,*

$$^*\mathtt{Hol}^{\gamma\wedge\beta}(\eta) = \mathtt{Hol}^{\gamma}(\eta).$$

*Proof* (*Sketch*) Consider two formulas $\gamma$ and $\beta$ and let $\mathtt{Hol}$ be a model. If $\beta$ is a subformula of $\gamma$ the proof is trivial (since it is sufficient to take $^*\mathtt{Hol}$ equal to $\mathtt{Hol}$). Suppose that $\beta$ is not a subformula of $\gamma$ (while $\gamma$ and $\beta$ may have some common subformulas). Consider the syntactical tree of $\gamma \wedge \beta$, which includes (in its left part) the syntactical tree of $\gamma$ (where $Level_1^{\gamma}$ appears at $Level_2^{\gamma\wedge\beta}$, while the top level of $STree^{\gamma}$ is supposed to be repeated until the Height $h$ of $STree^{\gamma\wedge\beta}$ is reached). The model $\mathtt{Hol}$ assigns a density operator $\mathtt{Hol}(Level_i^{\gamma})$ to each level of $STree^{\gamma}$ (represented as a part of $STree^{\gamma\wedge\beta}$). Let us briefly write: $^{\gamma}\rho_{i+1} = \mathtt{Hol}(Level_i^{\gamma})$. We transform $STree^{\gamma\wedge\beta}$ into a "hybrid" object $Hybr$ that is a sequence of sequences $Hybr_i$. Each $Hybr_i$ corresponds to $Level_i^{\gamma\wedge\beta}$ and is a sequence of objects that are either formulas or density operators. Taking into account the fact the $\mathsf{T}(\gamma, \beta, \mathbf{f})$ and $\beta$ are not subformulas of $\gamma$, we define the first two elements of $Hybr$ as follows:

$Hybr_1 = (\mathsf{T}(\gamma, \beta, \mathbf{f}))$; $Hybr_2 = (^{\gamma}\rho_2, \beta, P_0^{(1)})$. Then, we proceed (step by step) by replacing the first occurrence in $STree^{\gamma\wedge\beta}$ of each formula $\theta$ that is also a subformula of $\gamma$ with the density operator $\mathtt{Hol}^{\gamma}(\theta)$. Suppose, for instance, that $\theta$ occurs for the first time at $Level_i^{\gamma\wedge\beta}$, and suppose that $\theta = \mathsf{T}(\xi_1, \xi_2, \xi_3)$. Then (by definition of syntactical tree), $\xi_1$, $\xi_2$ and $\xi_3$ shall occur at $Level_{i+1}^{\gamma\wedge\beta}$. We define $Hybr_i$ and $Hybr_{i+1}$ in such a way that the following conditions are satisfied: a) in $Hybr_i$ the density operator $\mathtt{Hol}^{\gamma}(\theta)$ occurs in place of the formula $\theta$ (occurring at $Level_i^{\gamma\wedge\beta}$); b) in $Hybr_{i+1}$ the density operator $[^{\mathfrak{D}}\mathrm{T}^{(At(\xi_1), At(\xi_2), At(\xi_3))}]^{-1}(\mathtt{Hol}^{\gamma}(\theta))$ occurs in place of the subsequence $(\xi_1, \xi_2, \xi_3)$ (occurring at $Level_{i+1}^{\gamma\wedge\beta}$). We proceed in a similar way for all possible linguistic forms of $\theta$. When we finally reach the top level $Level_h^{\gamma\wedge\beta}$, the corresponding $Hybr_h$ will have the following form:

$$Hybr_h = (^{\gamma}\rho_h, Ob_1, \ldots, Ob_t, \; P_0^{(1)}),$$

where each $Ob_j$ is either a density operator or an atomic formula $\mathbf{q}$ that does not occur in $\gamma$. Now, we replace in $Hybr_h$ each "surviving" formula $\mathbf{q}$ with the density operator $\mathtt{Hol}(\mathbf{q})$ (which lives in $\mathbb{C}^2$). This operation destroys the "hybrid" form of $Hybr_h$, which is now transformed into a homogeneous sequence of density operators:

$$^{\mathfrak{D}}Hybr_h = (^{\gamma}\rho_h, \; ^{\mathfrak{D}}Ob_1, \ldots, \; ^{\mathfrak{D}}Ob_t, \; P_0^{(1)}), \quad \text{where:}$$

$$^{\mathfrak{D}}Ob_j = \begin{cases} Ob_j, \text{ if } Ob_j \text{ is a density operator;} \\ \mathtt{Hol}(\mathbf{q}), \text{ if } Ob_j = \mathbf{q}. \end{cases}$$

On this basis, we transform the whole $Hybr$ into a sequence of density operator-sequences $^{\mathfrak{D}}Hybr_i$. Let us first refer to $Hybr_{h-1}$, which may contain formulas that are not subformulas of $\gamma$. Suppose, for instance, that the first formula occurring in $Hybr_{h-1}$ is

$$\beta_{(h-1)_j} = \mathtt{T}(\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3).$$

Since $\beta_{(h-1)_j}$ is not a subformula of $\gamma$, ${}^{\mathfrak{D}}Hybr_h$ shall contain three separate density operators ${}^{\mathbf{q}_1}\rho,\ {}^{\mathbf{q}_2}\rho,\ {}^{\mathbf{q}_3}\rho$ (corresponding to the atom-sequence $(\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3)$ occurring in the right part of $STree^{\gamma\wedge\beta}$). On this basis, we replace the formula $\mathtt{T}(\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3)$ with the density operator ${}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}({}^{\mathbf{q}_1}\rho \otimes {}^{\mathbf{q}_2}\rho \otimes {}^{\mathbf{q}_3}\rho)$ in $Hybr_{h-1}$ and in all other $Hybr_i$ where $\mathtt{T}(\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3)$ possibly appears.

Then, we proceed step by step by applying the same procedure to all formulas $\beta_{i_j}$ occurring in $Hybr_i$, for any $i$ $(1 \le i < h)$. At the end of the procedure, each $Hybr_i$ $(1 < i \le h)$ has been transformed into a sequence of density operators

$$^{\mathfrak{D}}Hybr_i = ({}^{\gamma}\rho_i, \rho_{i_1}, \ldots, \rho_{i_r},\ P_0^{(1)}),$$

where any density operator is naturally associated to a segment of $Level_i^{\gamma\wedge\beta}$.

We define now the map ${}^*\mathtt{Hol}$ in the following way:

- ${}^*\mathtt{Hol}(Level_i^{\gamma\wedge\beta}) = {}^{\gamma}\rho_i \otimes \rho_{i_1} \otimes \ldots \otimes \rho_{i_r} \otimes P_0^{(1)}$, if $1 < i \le h$;
- ${}^*\mathtt{Hol}(Level_i^{\gamma\wedge\beta}) = {}^{\mathfrak{D}}\mathtt{T}^{(At(\gamma), At(\beta), 1)}({}^*\mathtt{Hol}(Level_2^{\gamma\wedge\beta}))$, if $i = 1$.

We have:

(I) by construction, ${}^*\mathtt{Hol}(Level_i^{\gamma\wedge\beta})$ is a density operator of $\mathscr{H}^{\gamma\wedge\beta}$. Hence, ${}^*\mathtt{Hol}$ is a holistic map for $\gamma \wedge \beta$;

(II) ${}^*\mathtt{Hol}$ is normal for $\gamma \wedge \beta$, by the normality of $\mathtt{Hol}$ and because different occurrences in $Hybr$ of a formula that is not a subformula of $\gamma$ have been replaced by the same density operator;

(III) by construction, ${}^*\mathtt{Hol}$ preserves the logical form of all subformulas of $\gamma \wedge \beta$. Accordingly, ${}^*\mathtt{Hol}(Level_i^{\gamma\wedge\beta}) = {}^{\mathfrak{D}}\mathtt{G}_{(i)}({}^*\mathtt{Hol}(Level_{i+1}^{\gamma\wedge\beta}))$, for any $i$ such that $1 \le i < h$, where $({}^{\mathfrak{D}}\mathtt{G}_{(h-1)}, \ldots,\ {}^{\mathfrak{D}}\mathtt{G}_{(1)})$ is the gate-tree of $\gamma \wedge \beta$. Furthermore, the sentences **f** and **t** have (trivially) the "right" contextual meanings. Hence, ${}^*\mathtt{Hol}$ is a model for $\gamma \wedge \beta$;

(IV) by construction, for any $\eta$ that is a subformula of $\gamma$:

$$^*\mathtt{Hol}^{\gamma\wedge\beta}(\eta) = \mathtt{Hol}^{\gamma}(\eta). \qquad \square$$

We can now define the basic concepts of the holistic quantum computational semantics: *truth*, *validity*, *logical consequence* and *logical equivalence*.

**Definition 4.6** (*Truth*) A formula $\alpha$ is called *true* with respect to a model $\mathtt{Hol}$ (abbreviated as $\models_{\mathtt{Hol}} \alpha$) iff $\mathtt{p}_1(\mathtt{Hol}(\alpha)) = 1$.

Apparently, the quantum computational concept of truth is a *probabilistic* notion, defined in terms of the Born-probability function $\mathtt{p}_1$.

**Definition 4.7** (*Validity*) $\alpha$ is called *valid* ($\models \alpha$) iff for any model $\mathtt{Hol}$, $\models_{\mathtt{Hol}} \alpha$.

**Definition 4.8** (*Logical consequence*) $\beta$ is called a *logical consequence* of $\alpha$ ($\alpha \vDash \beta$) iff for any formula $\gamma$ such that $\alpha$ and $\beta$ are subformulas of $\gamma$ and for any model $\mathtt{Hol}$,

$$\mathtt{Hol}^{\gamma}(\alpha) \preceq \mathtt{Hol}^{\gamma}(\beta)$$

(where $\preceq$ is the pre-order relation defined by Definition 2.3).

Apparently, the quantum computational relation of logical consequence is a *contextual* notion that refers to all possible contexts where the formulas under investigation may occur.

**Definition 4.9** (*Logical equivalence*) $\alpha$ and $\beta$ are logically equivalent ($\alpha \equiv \beta$) iff $\alpha \vDash \beta$ and $\beta \vDash \alpha$.

Although the holistic semantics is strongly context-dependent, one can prove that the logical consequence-relation is reflexive and transitive.

**Theorem 4.5** *(1)* $\alpha \vDash \alpha$*;*
*(2)* $\alpha \vDash \beta$ *and* $\beta \vDash \delta \quad \Rightarrow \quad \alpha \vDash \delta$.

*Proof* (1) Straightforward.

(2) Assume the hypothesis and suppose, by contradiction, that there exists a model $\mathtt{Hol}$ and a formula $\gamma$, where $\alpha$ and $\delta$ occur as subformulas, such that: $\mathtt{Hol}^{\gamma}(\alpha) \npreceq \mathtt{Hol}^{\gamma}(\delta)$. Consider the formula $\gamma \wedge \beta$. By Theorem 4.4 there exists a model $^{*}\mathtt{Hol}$ such that for any $\eta$ that is a subformula of $\gamma$: $^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\eta) = \mathtt{Hol}^{\gamma}(\eta)$. Thus, we have:
$^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\alpha) = \mathtt{Hol}^{\gamma}(\alpha)$ and $^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\delta) = \mathtt{Hol}^{\gamma}(\delta)$.
Since we have assumed (by contradiction) that $\mathtt{Hol}^{\gamma}(\alpha) \npreceq \mathtt{Hol}^{\gamma}(\delta)$, we obtain: $^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\alpha) \npreceq {}^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\delta)$, against the hypothesis and the transitivity of $\preceq$, which imply:
$^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\alpha) \preceq {}^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\beta)$; $^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\beta) \preceq {}^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\delta)$;
$^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\alpha) \preceq {}^{*}\mathtt{Hol}^{\gamma\wedge\beta}(\delta)$. □

The concept of logical consequence, defined in this semantics, characterizes a special form of quantum computational logic (formalized in the language $\mathscr{L}_0$) that has been called *holistic quantum computational logic* (**HQCL**). At the same time, the compositional semantics (based on the hypothesis that all models $\mathtt{Hol}$ are compositional) characterizes a different logic, termed *compositional quantum computational logic* (**CQCL**). Of course, we have:

$$\alpha \vDash_{\mathbf{HQCL}} \beta \implies \alpha \vDash_{\mathbf{CQCL}} \beta.$$

We will see that the inverse relation does not hold.

Interestingly enough, the compositional quantum computational semantics describes, as a special case, a reversible version of classical sentential semantics.

Consider the sublanguage $\mathscr{L}_0^C$ of $\mathscr{L}_0$, whose formulas are the quantum computational Boolean formulas of $\mathscr{L}_0$. The concept of *classical quantum computational model* for the language $\mathscr{L}_0^C$ can be now defined in the expected way.

**Definition 4.10** (*Classical quantum computational model*) A *classical quantum computational model* for $\mathscr{L}_0^C$ is a map `Hol` that satisfies the following conditions:

(1) `Hol` is a perfectly compositional model for all $\mathscr{L}_0^C$-formulas.
(2) For any formula $\alpha$ of $\mathscr{L}_0^C$, `Hol` assigns to the top level of $STree^\alpha$ a register that belongs to the semantic space of $\alpha$.

One immediately obtains that any classical quantum computational model assigns to any formula $\alpha$ of $\mathscr{L}_0^C$ a register of the space $\mathscr{H}^\alpha$. Furthermore, all meanings are context-independent.

As is well known an "uneasy" feature of the standard versions of classical semantics is due to the fact that interpretations of the language generally "loose the memory" of the linguistic complexity of the formulas under investigation; for, the *extensional meaning* of any formula is dealt with as a single truth-value (a single bit). In the classical quantum computational semantics, instead, the meaning of a formula $\alpha$ is represented by a register that lives in the semantic space of $\alpha$. This allows us to preserve, at least to a certain extent, the "memory" of the complexity of $\alpha$. One should notice however that a register $|x_1, \ldots, x_n\rangle$ may represent the meaning of different formulas that share the same semantic space $\mathscr{H}^{(n)}$.

We can now define a natural concept of logical consequence for the language $\mathscr{L}_0^C$.

**Definition 4.11** (*Quantum-classical logical consequence*) Let $\alpha$ and $\beta$ be two formulas of $\mathscr{L}_0^C$.
The formula $\beta$ is called a *quantum-classical logical consequence* of $\alpha$ ($\alpha \vDash_{\mathbf{QCL}} \beta$) iff for any classical quantum computational model `Hol`,

$$\mathtt{Hol}(\alpha) \preceq \mathtt{Hol}(\beta).$$

**Lemma 4.1** *For any formulas $\alpha$ and $\beta$ of $\mathscr{L}_0^C$, $\alpha \vDash_{\mathbf{QCL}} \beta$ iff $\beta$ is a logical consequence of $\alpha$ according to classical sentential logic.*

*Proof* Straightforward. □

Thus, we can say that the logic **QCL** represents a quantum computational version of classical logic, characterized by a semantics where all logical connectives are interpreted as reversible logical operations.

## 4.4 Quantum Computational Logical Arguments

Which logical arguments are either valid or possibly violated in the logics **HQCL** and **CQCL**? The following theorems give some answers to this question. We will first consider the case of **HQCL**. By simplicity we will write $\alpha \vDash \beta$ instead of $\alpha \vDash_{\mathbf{HCQL}} \beta$.

Theorem 4.6 sums up some basic arguments that hold for the quantum computational Boolean connectives and for the sentences **f**, **t**.

**Theorem 4.6** *(1)* $\alpha \wedge \beta \vDash \alpha$; $\alpha \wedge \beta \vDash \beta$
*(2)* $\alpha \vDash \beta \Rightarrow \alpha \wedge \delta \vDash \beta$
*(3)* $\neg\neg\alpha \equiv \alpha$
*(4)* $\alpha \vDash \beta \Rightarrow \neg\beta \vDash \neg\alpha$
*(5)* $\neg\alpha \vDash \neg\beta \Rightarrow \beta \vDash \alpha$
*(6)* $\mathbf{f} \vDash \beta$; $\beta \vDash \mathbf{t}$
*(7)* $\mathbf{f} \equiv \neg\mathbf{t}$; $\mathbf{t} \equiv \neg\mathbf{f}$
*(8)* $\vDash \mathbf{t}$
*(9)* $\vDash \alpha \iff \mathbf{t} \vDash \alpha$

*Proof* (1) $\alpha \wedge \beta \vDash \alpha$; $\alpha \wedge \beta \vDash \beta$.
Let $\alpha$ and $\alpha \wedge \beta$ $(= \mathsf{T}(\alpha, \beta, \mathbf{f}))$ be subformulas of $\gamma$. Suppose that $\alpha, \beta, \mathbf{f}$ occur respectively at the positions $k_1, k_2, k_3$ of $Level^{\gamma}_{i+1}$ (in the syntactical tree of $\gamma$), while $\mathsf{T}(\alpha, \beta, \mathbf{f})$ occurs at $Level^{\gamma}_{i}$. By Theorem 4.2(2), for any $\mathtt{Hol}$ we have:

$$\mathtt{Hol}^{\gamma}(\mathsf{T}(\alpha, \beta, \mathbf{f})) = {}^{\mathfrak{D}}\mathrm{T}^{(At(\alpha), At(\beta), At(\mathbf{f}))}(Red^{(k_1,k_2,k_3)}_{[1,\ldots,r]}(\mathtt{Hol}(Level^{\gamma}_{i+1})))$$

(where $r$ is the number of formulas occurring at $Level^{\gamma}_{i+1}$). Hence, by definition of contextual meaning and by Theorem 2.3(2):

$$\mathtt{Hol}^{\gamma}(\mathsf{T}(\alpha, \beta, \mathbf{f})) \preceq \mathtt{Hol}^{\gamma}(\alpha).$$

In a similar way one can prove that $\alpha \wedge \beta \vDash \beta$.
(2) $\alpha \vDash \beta \Rightarrow \alpha \wedge \delta \vDash \beta$.
Assume the hypothesis and let $\alpha \wedge \delta$, $\beta$ be subformulas of $\gamma$. Then $\alpha$ and $\delta$ also are subformulas of $\gamma$. By hypothesis, for any $\mathtt{Hol}$: $\mathtt{Hol}^{\gamma}(\alpha) \preceq \mathtt{Hol}^{\gamma}(\beta)$. By (1): $\mathtt{Hol}^{\gamma}(\alpha \wedge \delta) \preceq \mathtt{Hol}^{\gamma}(\alpha)$. Hence, by transitivity of $\preceq$: $\mathtt{Hol}^{\gamma}(\alpha \wedge \delta) \preceq \mathtt{Hol}^{\gamma}(\beta)$.
(3) $\neg\neg\alpha \equiv \alpha$.
Let $\neg\neg\alpha$ and $\alpha$ be subformulas of $\gamma$. By Theorem 4.1(1) and by the double-negation principle for the gate $\mathrm{NOT}^{(n)}$ (Theorem 2.2(1)), we obtain for any $\mathtt{Hol}$:

$$\mathtt{Hol}^{\gamma}(\neg\neg\alpha) = {}^{\mathfrak{D}}\mathrm{NOT}^{(At(\alpha))}\,{}^{\mathfrak{D}}\mathrm{NOT}^{(At(\alpha))}\mathtt{Hol}^{\gamma}(\alpha) = \mathtt{Hol}^{\gamma}(\alpha).$$

(4) $\alpha \vDash \beta \Rightarrow \neg\beta \vDash \neg\alpha$.
Assume the hypothesis and let $\neg\beta, \neg\alpha$ be subformulas of $\gamma$. Then $\alpha$ and $\beta$ also are subformulas of $\gamma$. By hypothesis, for any $\mathtt{Hol}$: $\mathtt{p}_1(\mathtt{Hol}^{\gamma}(\alpha)) \leq \mathtt{p}_1(\mathtt{Hol}^{\gamma}(\beta))$. Hence, $1 - \mathtt{p}_1(\mathtt{Hol}^{\gamma}(\beta)) \leq 1 - \mathtt{p}_1(\mathtt{Hol}^{\gamma}(\alpha))$. By Theorem 2.3(3) we have:
$1 - \mathtt{p}_1(\mathtt{Hol}^{\gamma}(\beta)) = \mathtt{p}_1({}^{\mathfrak{D}}\mathrm{NOT}^{(At(\beta))}\mathtt{Hol}^{\gamma}(\beta))$;
$1 - \mathtt{p}_1(\mathtt{Hol}^{\gamma}(\alpha)) = \mathtt{p}_1({}^{\mathfrak{D}}\mathrm{NOT}^{(At(\alpha))}\mathtt{Hol}^{\gamma}(\alpha))$.
Hence,

$${}^{\mathfrak{D}}\mathrm{NOT}^{(At(\beta))}\mathtt{Hol}^{\gamma}(\beta) \preceq {}^{\mathfrak{D}}\mathrm{NOT}^{(At(\alpha))}\mathtt{Hol}^{\gamma}(\alpha).$$

Whence, by Theorem 4.1(1): $\mathtt{Hol}^{\gamma}(\neg\beta) \preceq \mathtt{Hol}^{\gamma}(\neg\alpha)$.

(5) $\neg\alpha \vDash \neg\beta \;\Rightarrow\; \beta \vDash \alpha$.
By (4) and by (3).

(6) $\mathbf{f} \vDash \beta$; $\beta \vDash \mathbf{t}$.
Let $\beta$ and $\mathbf{f}$ be subformulas of $\gamma$. By definition of holistic model we have: $\mathtt{p}_1(\mathtt{Hol}^\gamma(\mathbf{f})) = \mathtt{p}_1(P_0^{(1)}) = 0$, for any $\mathtt{Hol}$. Hence, $\mathtt{Hol}^\gamma(\mathbf{f}) \preceq \mathtt{Hol}^\gamma(\beta)$. In a similar way one can prove that $\beta \vDash \mathbf{t}$.

(7) $\mathbf{f} \equiv \neg\mathbf{t}$; $\quad \mathbf{t} \equiv \neg\mathbf{f}$.
Straightforward.

(8) $\vDash \mathbf{t}$.
Straightforward.

(9) $\vDash \alpha \quad \Longleftrightarrow \mathbf{t} \vDash \alpha$.
Straightforward. □

The dual forms of Theorems 4.6(1) and of 4.6(2) ($\alpha \vDash \alpha \vee \beta$, $\beta \vDash \alpha \vee \beta$, $\alpha \vDash \beta \;\Rightarrow\; \alpha \vDash \beta \vee \delta$) hold by definition of the connective $\vee$.

The following theorem sums up some important classical arguments that are not valid in the logic **HQCL**.

**Theorem 4.7** *(1)* $\alpha \nvDash \alpha \wedge \alpha$
*(2)* $\alpha \wedge \beta \nvDash \beta \wedge \alpha$
*(3)* $\alpha \wedge (\beta \wedge \delta) \nvDash (\alpha \wedge \beta) \wedge \delta$
*(4)* $(\alpha \wedge \beta) \wedge \delta \nvDash \alpha \wedge (\beta \wedge \delta)$
*(5)* $\alpha \wedge (\beta \vee \delta) \nvDash (\alpha \wedge \beta) \vee (\alpha \wedge \delta)$
*(6)* $(\alpha \wedge \beta) \vee (\alpha \wedge \delta) \nvDash \alpha \wedge (\beta \vee \delta)$
*(7)* $\delta \vDash \alpha$ *and* $\delta \vDash \beta \;\not\Rightarrow\; \delta \vDash \alpha \wedge \beta$
*(8)* $\alpha \wedge \neg\alpha \nvDash \beta$
*(9)* $\alpha \uplus \beta \nvDash \beta \uplus \alpha$
*(10)* $\alpha \uplus \beta \nvDash \alpha \vee \beta$; $\quad \alpha \uplus \beta \nvDash \neg\alpha \vee \neg\beta$

*Proof* In the following counterexamples $\alpha$, $\beta$ and $\delta$ will always represent atomic formulas.

(1) $\alpha \nvDash \alpha \wedge \alpha$.
Take $\gamma = \alpha \wedge \alpha$ and consider a model $\mathtt{Hol}$ such that

$$\mathtt{Hol}(\gamma) = {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}).$$

We have: $\mathtt{p}_1(\mathtt{Hol}^\gamma(\alpha)) = \frac{1}{2} > \mathtt{p}_1(\mathtt{Hol}^\gamma(\alpha \wedge \alpha)) = \frac{1}{4}$.

(2) $\alpha \wedge \beta \nvDash \beta \wedge \alpha$.
Take $\gamma = (\alpha \wedge \beta) \wedge (\beta \wedge \alpha)$ and consider a model $\mathtt{Hol}$ such that
$\mathtt{Hol}(\gamma) = {}^{\mathfrak{D}}\mathrm{T}^{(3,3,1)}[{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(P_{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)} \otimes P_0^{(1)}) \otimes P_0^{(1)}]$.
We have: $\mathtt{p}_1(\mathtt{Hol}^\gamma(\alpha \wedge \beta)) = \frac{1}{4} > \mathtt{p}_1(\mathtt{Hol}^\gamma(\beta \wedge \alpha)) = 0$.

(3) $\alpha \wedge (\beta \wedge \delta) \nvDash (\alpha \wedge \beta) \wedge \delta$.
Take $\gamma = (\alpha \wedge (\beta \wedge \delta)) \wedge ((\alpha \wedge \beta) \wedge \delta)$ and consider a model $\texttt{Hol}$ such that
$\texttt{Hol}(\gamma) =$
${}^{\mathfrak{D}}\mathtt{T}^{(5,5,1)}[\,{}^{\mathfrak{D}}\mathtt{T}^{(1,3,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{T}^{(3,1,1)}(\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)} \otimes \mathtt{I}^{(2)}(P_{\frac{1}{\sqrt{2}}(|01010\rangle - |10000\rangle)})) \otimes P_0^{(1)}]$.
We have: $\mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \wedge (\beta \wedge \delta))) = \frac{1}{8} > \mathtt{p}_1(\texttt{Hol}^\gamma((\alpha \wedge \beta) \wedge \delta)) = 0$.
(4) $(\alpha \wedge \beta) \wedge \delta \nvDash \alpha \wedge (\beta \wedge \delta)$.
Similar to (3).
(5) $\alpha \wedge (\beta \vee \delta) \nvDash (\alpha \wedge \beta) \vee (\alpha \wedge \delta)$.
Take $\gamma = (\alpha \wedge (\beta \vee \delta)) \wedge ((\alpha \wedge \beta) \vee (\alpha \wedge \delta))$ and consider a model $\texttt{Hol}$ such that
$\texttt{Hol}(\gamma) =$
${}^{\mathfrak{D}}\mathtt{T}^{(5,7,1)}[{}^{\mathfrak{D}}\mathtt{T}^{(1,3,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(P_{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)} \otimes P_0^{(1)}) \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{NOT}^{(7)}\,{}^{\mathfrak{D}}\mathtt{T}^{(3,3,1)}(\,{}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)}) \otimes P_0^{(1)}]$.
We have: $\mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \wedge (\beta \vee \delta))) = \frac{1}{2} > \mathtt{p}_1(\texttt{Hol}^\gamma((\alpha \wedge \beta) \vee (\alpha \wedge \delta))) = \frac{7}{16}$.
(6) $(\alpha \wedge \beta) \vee (\alpha \wedge \delta) \nvDash \alpha \wedge (\beta \vee \delta)$.
Take $\gamma = (\alpha \wedge (\beta \vee \delta)) \wedge ((\alpha \wedge \beta) \vee (\alpha \wedge \delta))$ and consider a model $\texttt{Hol}$ such that $\texttt{Hol}(\gamma) =$
${}^{\mathfrak{D}}\mathtt{T}^{(5,7,1)}[{}^{\mathfrak{D}}\mathtt{T}^{(1,3,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{NOT}^{(7)}\,{}^{\mathfrak{D}}\mathtt{T}^{(3,3,1)}(\,{}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes$
${}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)}) \otimes P_0^{(1)}]$.
We have: $\mathtt{p}_1(\texttt{Hol}^\gamma((\alpha \wedge \beta) \vee (\alpha \wedge \delta))) = \frac{7}{16} > \mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \wedge (\beta \vee \delta))) = \frac{3}{8}$.
(7) $\delta \vDash \alpha$ and $\delta \vDash \beta \;\not\Rightarrow\; \delta \vDash \alpha \wedge \beta$.
Take $\gamma = (\alpha \wedge \beta) \wedge \delta$ and consider a model $\texttt{Hol}$ such that
$\texttt{Hol}(\gamma) =$
${}^{\mathfrak{D}}\mathtt{T}^{(3,1,1)}(\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)})$.
We have:
$\mathtt{p}_1(\texttt{Hol}^\gamma(\alpha)) = \mathtt{p}_1(\texttt{Hol}^\gamma(\beta)) = \mathtt{p}_1(\texttt{Hol}^\gamma(\delta)) = \frac{1}{2} > \mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \wedge \beta)) = \frac{1}{4}$.
(8) $\alpha \wedge \neg\alpha \nvDash \beta$.
Take $\gamma = (\alpha \wedge \neg\alpha) \wedge \beta$ and consider a model $\texttt{Hol}$ such that

$$\texttt{Hol}(\gamma) = {}^{\mathfrak{D}}\mathtt{T}^{(3,1,1)}(\,{}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)} \otimes P_0^{(1)}).$$

We have: $\mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \wedge \neg\alpha)) = \frac{1}{4}$ and $\mathtt{p}_1(\texttt{Hol}^\gamma(\beta)) = 0$.
(9) $\alpha \uplus \beta \nvDash \beta \uplus \alpha$.
Take $\gamma = (\alpha \uplus \beta) \wedge (\beta \uplus \alpha)$ and consider a model $\texttt{Hol}$ such that

$$\texttt{Hol}(\gamma) = {}^{\mathfrak{D}}\mathtt{T}^{(2,2,1)}[\,{}^{\mathfrak{D}}\mathtt{XOR}^{(1,1)}P_{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)} \otimes {}^{\mathfrak{D}}\mathtt{XOR}^{(1,1)}(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)}) \otimes P_0^{(1)}].$$

We have: $\mathtt{p}_1(\texttt{Hol}^\gamma(\alpha \uplus \beta)) = 1 > \mathtt{p}_1(\texttt{Hol}^\gamma(\beta \uplus \alpha)) = \frac{1}{2}$.

(10) $\alpha \uplus \beta \nvDash \alpha \vee \beta$; $\alpha \uplus \beta \nvDash \neg\alpha \vee \neg\beta$.
Take $\gamma = (\alpha \uplus \beta) \wedge (\alpha \vee \beta)$ and consider a model $\mathtt{Hol}$ such that
$\mathtt{Hol}(\gamma) =$
${}^{\mathfrak{D}}\mathtt{T}^{(2,3,1)}[{}^{\mathfrak{D}}\mathtt{XOR}^{(1,1)} P_{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)} \otimes$
${}^{\mathfrak{D}}\mathtt{NOT}^{(3)}\mathtt{T}^{(1,1,1)}(\mathtt{NOT}^{(1)} \otimes \mathtt{NOT}^{(1)} \otimes \mathtt{I}^{(1)})(\frac{1}{2}\mathtt{I}^{(1)} \otimes \frac{1}{2}\mathtt{I}^{(1)} \otimes P_0^{(1)}) \otimes P_0^{(1)}]$.
We have: $\mathtt{p}_1(\mathtt{Hol}^\gamma(\alpha \uplus \beta)) = 1 > \mathtt{p}_1(\mathtt{Hol}^\gamma(\alpha \vee \beta)) = \frac{3}{4}$.
In a similar way one can prove that $\alpha \uplus \beta \nvDash \neg\alpha \vee \neg\beta$. □

Since the conjunction $\wedge$ is generally non-associative, brackets cannot be omitted in the case of multiple conjunctions. In the following, we will use the expression $\beta_1 \wedge \ldots \wedge \beta_n$ as a metalinguistic abbreviation for any possible bracket-configuration in a multiple conjunction whose members are the elements of the sequence $(\beta_1, \ldots, \beta_n)$.

The following theorem sums up some basic arguments that hold for the genuine quantum computational connectives.

**Theorem 4.8** *(1)* $\sqrt{id}\sqrt{id}\alpha \equiv \alpha$
*(2)* $\sqrt{id}\mathbf{f} \equiv \sqrt{id}\mathbf{t}$
*(3)* $\neg\sqrt{id}\mathbf{f} \equiv \sqrt{id}\mathbf{f}$; $\neg\sqrt{id}\mathbf{t} \equiv \sqrt{id}\mathbf{t}$
*(4)* $\sqrt{id}(\alpha \wedge \beta) \equiv \sqrt{id}\mathbf{f}$
*(5)* $\sqrt{\neg}\sqrt{\neg}\alpha \equiv \neg\alpha$
*(6)* $\sqrt{\neg}\mathbf{f} \equiv \sqrt{\neg}\mathbf{t}$
*(7)* $\neg\sqrt{\neg}\mathbf{f} \equiv \sqrt{\neg}\mathbf{f}$; $\neg\sqrt{\neg}\mathbf{t} \equiv \sqrt{\neg}\mathbf{t}$
*(8)* $\neg\sqrt{\neg}\alpha \equiv \sqrt{\neg}\neg\alpha$
*(9)* $\sqrt{\neg}(\alpha \wedge \beta) \equiv \sqrt{\neg}\mathbf{f}$
*(10)* $\sqrt{id}\sqrt{\neg}\alpha \equiv \sqrt{id}\alpha$
*(11)* $\sqrt{\neg}\sqrt{id}\alpha \equiv \neg\sqrt{\neg}\alpha$
*(12)* $\sqrt{id}\sqrt{\neg}(\alpha \wedge \beta) \equiv \sqrt{\neg}\mathbf{f}$
*(13)* $\sqrt{\neg}\sqrt{id}(\alpha \wedge \beta) \equiv \sqrt{\neg}\mathbf{f}$

*Proof* (1) $\sqrt{id}\sqrt{id}\alpha \equiv \alpha$.
Let $\alpha$ and $\sqrt{id}\sqrt{id}\alpha$ be subformulas of $\gamma$. We have: $\sqrt{\mathtt{I}}^{(n)}\sqrt{\mathtt{I}}^{(n)} = \mathtt{I}^{(n)}$ (Theorem 2.2(2)). Whence, by Theorem 4.1(2): $\mathtt{Hol}^\gamma(\sqrt{id}\sqrt{id}\alpha) = \mathtt{Hol}^\gamma(\alpha)$.
(2) $\sqrt{id}\mathbf{f} \equiv \sqrt{id}\mathbf{t}$.
By definition of model, by Theorems 4.1(2) and by 2.3(9).
(3) $\neg\sqrt{id}\mathbf{f} \equiv \sqrt{id}\mathbf{f}$; $\neg\sqrt{id}\mathbf{t} \equiv \sqrt{id}\mathbf{t}$.
By definition of model, by Theorems 4.1(1, 2) and by 2.3(11).
(4) $\sqrt{id}(\alpha \wedge \beta) \equiv \sqrt{id}\mathbf{f}$.
By definition of model, by Theorems 4.1(2) and 2.3(13).
(5) $\sqrt{\neg}\sqrt{\neg}\alpha \equiv \neg\alpha$.
By Theorems 4.1(1, 3) and 2.2(3).
(6) $\sqrt{\neg}\mathbf{f} \equiv \sqrt{\neg}\mathbf{t}$.
By definition of model, by Theorems 4.1(3) and 2.3(10).
(7) $\neg\sqrt{\neg}\mathbf{f} \equiv \sqrt{\neg}\mathbf{f}$; $\neg\sqrt{\neg}\mathbf{t} \equiv \sqrt{\neg}\mathbf{t}$.
By definition of model, by Theorems 4.1(1, 3) and 2.3(12).

(8) $\neg\sqrt{\neg}\alpha \equiv \sqrt{\neg}\,\neg\alpha$.
By Theorems 4.1(1, 3) and 2.3(7).
(9) $\sqrt{\neg}(\alpha \wedge \beta) \equiv \sqrt{id}\mathbf{f}$.
By definition of model, by Theorems 4.1(2, 3) and 2.3(13).
(10) $\sqrt{id}\sqrt{\neg}\alpha \equiv \sqrt{id}\,\alpha$.
By Theorems 4.1(2, 3) and 2.3(8).
(11) $\sqrt{\neg}\sqrt{id}\alpha \equiv \neg\sqrt{\neg}\,\alpha$.
By Theorems 4.1(1, 2, 3) and 2.3(8).
(12) $\sqrt{id}\sqrt{\neg}(\alpha \wedge \beta) \equiv \sqrt{\neg}\,\mathbf{f}$.
By definition of model, by Theorems 4.1(2, 3) and 2.3(14).
(13) $\sqrt{\neg}\sqrt{id}(\alpha \wedge \beta) \equiv \sqrt{\neg}\,\mathbf{f}$.
By definition of model, by Theorems 4.1(2, 3) and 2.3(14). □

Interestingly enough, some classical arguments that may be violated in the logic **HQCL** are instead valid in the logic **CQCL**, where conjunctions and disjunctions are always commutative, associative and weakly distributive. As we have seen, unlike the holistic case, in the compositional semantics all gates that correspond to logical connectives commute with the contextual meanings of the subformulas of the formulas under investigation (Theorems 4.1 and 4.3). As a consequence, the semantic properties of all connectives turn out to "mirror" the properties of the corresponding gates.

**Theorem 4.9** *(1)* $\alpha \wedge \beta \ \vDash_{\mathbf{CQCL}} \ \beta \wedge \alpha; \quad \alpha \vee \beta \ \vDash_{\mathbf{CQCL}} \ \beta \vee \alpha$
*(2)* $\alpha \wedge (\beta \wedge \delta) \ \equiv_{\mathbf{CQCL}} \ (\alpha \wedge \beta) \wedge \delta; \quad \alpha \vee (\beta \vee \delta) \ \equiv_{\mathbf{CQCL}} \ (\alpha \vee \beta) \vee \delta$
*(3)* $\alpha \wedge (\beta \vee \delta) \ \vDash_{\mathbf{CQCL}} \ (\alpha \wedge \beta) \vee (\alpha \wedge \delta); \quad (\alpha \vee \beta) \wedge (\alpha \vee \delta) \ \vDash_{\mathbf{CQCL}} \ \alpha \vee (\beta \wedge \delta)$

*Proof* By definition of the connective $\vee$, by Theorems 4.1, 4.3 and 2.3(4). □

Thus, **CQCL** is a logic that is stronger than **HCQL**. We have:

$$\alpha \ \vDash_{\mathbf{HQCL}} \ \beta \ \Longrightarrow \ \alpha \ \vDash_{\mathbf{CQCL}} \beta; \ \ \alpha \ \vDash_{\mathbf{CQCL}} \beta \ \not\Longrightarrow \alpha \ \vDash_{\mathbf{HQCL}} \beta.$$

It is worth-while noticing that in the logic **CQCL** the weak distributive property holds in the "opposite direction" with respect to the weak distributivity of Birkhoff and von Neumann's quantum logic, where:

$$(\alpha \wedge \beta) \vee (\alpha \wedge \delta) \vDash_{\mathbf{QL^{BN}}} \ \alpha \wedge (\beta \vee \delta); \ \ \alpha \wedge (\beta \vee \delta) \nvDash_{\mathbf{QL^{BN}}} \ (\alpha \wedge \beta) \vee (\alpha \wedge \delta).$$

Quantum events and quantum pieces of information turn out to have a different behavior with respect to the distributivity-laws.

Apparently, the logic **HQCL** is very weak: important logical arguments that hold in classical logic and in many alternative logics are here violated. At the same time, the situations represented in this semantics seem to be in agreement with a number of informal ways of reasoning (expressed in the framework of natural languages), where conjunctions and disjunctions are frequently used as non-idempotent, non-commutative and non-associative logical operations.

As is well known, the semantics of natural languages is essentially holistic and contextual. We need only think how children learn their mother-language, showing an extraordinary capacity of understanding and using correctly the contextual meanings of linguistic expressions that occur in different contexts. And it often happens that the meaning of a global expression is grasped and used in a clear and correct way, while the meanings of its parts appear more vague and ambiguous. Possible applications of the holistic quantum computational semantics to different fields that may be far from microphysics will be investigated in Chap. 8.

## References

1. Baltag, A., Smets, S.: A dynamic-logical perspective on quantum behavior. Studia Logica **89**, 185–209 (2008)
2. Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Quantum computational logics. A survey. In: Hendricks, V., Malinowski, J. (eds.) 50 Years of Studia Logica, pp. 213–255. Kluwer, Dordrecht (2003)
3. Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Logics from quantum computation. Int. J. Quantum Inf. **3**(2), 293–337 (2005)
4. Dalla Chiara, M.L., Giuntini, R., Ledda, A., Leporini, R., Sergioli, G.: Entanglement as a semantic resource. Found. Phys. **40**(9–10), 1494–1518 (2010)
5. da Costa, N., de Ronde, C.: The paraconsistent logic of quantum superposition. Found. Phys. **43**(7), 845–858 (2013)
6. Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: Holistic logical arguments in quantum computation. Math. Slovaca **66**(2), 1–22 (2016)
7. Gudder, S.P.: Quantum computational logics. Int. J. Theor. Phys. **42**(1), 39–47 (2003)
8. Sozzo, S.: Conjunction and negation of natural concepts: a quantum-theoretic modeling. J. Math. Psychol. **66**, 82–102 (2015)

# Chapter 5
# Individuals, Quantifiers and Epistemic Operators

## 5.1 Introduction

The intrinsic *informational* content that characterizes quantum computational logics has naturally inspired some interesting and intriguing epistemic problems. We will investigate the possibility of a quantum computational semantics for a first-order language that can express sentences like "Alice knows that everybody knows that she is pretty".

As is well known, most semantic approaches to epistemic logics that can be found in the literature have been developed in the framework of a Kripke-style semantics. We will follow here a different approach, whose aim is representing both quantifiers and epistemic operators as "genuine" quantum concepts, living in a Hilbert-space environment. In this perspective, the basic question will be: to what extent is it possible to interpret quantifiers and epistemic operators as special examples of Hilbert-space operations? Interestingly enough, these logical operators turn out to have a similar semantic behavior, giving rise to a kind of "reversibility-breaking": unlike the case of logical connectives, both quantifiers and epistemic operators cannot be generally represented as reversible gates. The "act of knowing" and the use of universal or existential assertions seem to involve some irreversible "theoretic jumps", which are similar to quantum measurements (where the collapse of the wave function comes into play).

A characteristic feature of the epistemic quantum computational semantics is the use of the notion of *truth-perspective*: each *epistemic agent* (say, *Alice*, *Bob*,...) is supposed to be associated to a truth-perspective that is mathematically determined by the choice of a particular orthonormal basis of the two-dimensional Hilbert space $\mathbb{C}^2$. Truth-perspective changes give rise to some interesting relativistic-like epistemic effects: if *Alice* and *Bob* have different truth-perspectives, *Alice* might *see* a kind of *deformation* in *Bob*'s logical behavior. Epistemic agents are also characterized by specific *epistemic domains* that contain the pieces of information that are accessible to them. Due to the limits of such domains the unrealistic phenomenon of *logical*



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_5

*omniscience* is avoided in this semantics: *Alice* might know a given sentence without knowing all its logical consequences.[1]

As happens in the case of knowledge operators, quantifiers also can be interpreted as special examples of Hilbert-space operations that are generally irreversible. Unlike most semantic approaches, the *models* of the first-order quantum computational semantics do not refer to *domains of individuals* dealt with as *closed sets* (in a classical sense). The interpretation of a universal formula does not require any "ideal test" that should be performed for *all* elements of a collection of objects (which might be infinite or indeterminate).

## 5.2 Truth-Perspectives

In the previous Chapters we have always referred to the canonical bases of the Hilbert spaces under consideration. But, of course, the choice of a particular basis of a given Hilbert space is a matter of convention. Consider the space $\mathbb{C}^2$. Any orthonormal basis of this space can be described as determined by the application of a unitary operator $\mathfrak{T}$ to the elements of the canonical basis $\{|0\rangle, |1\rangle\}$. From an intuitive point of view, we can think that the operator $\mathfrak{T}$ gives rise to a change of *truth-perspective*. While the classical truth-values *Truth* and *Falsity* have been identified with the two bits $|1\rangle$ and $|0\rangle$, assuming a different basis corresponds to a different idea of *Truth* and *Falsity*. Since any basis-change in $\mathbb{C}^2$ is determined by the choice of a particular unitary operator, we can identify a *truth-perspective* with a unitary operator $\mathfrak{T}$ of $\mathbb{C}^2$. We will write:

$$|1_{\mathfrak{T}}\rangle = \mathfrak{T}|1\rangle; \ \ |0_{\mathfrak{T}}\rangle = \mathfrak{T}|0\rangle,$$

and we will assume that $|1_{\mathfrak{T}}\rangle$ and $|0_{\mathfrak{T}}\rangle$ represent, respectively, the truth-values *Truth* and *Falsity* of the truth-perspective $\mathfrak{T}$. The *canonical truth-perspective* is, of course, determined by the identity operator $\mathtt{I}^{(1)}$. We will indicate by $\mathbf{B}^{(1)}_{\mathfrak{T}}$ the orthonormal basis determined by $\mathfrak{T}$; while $\mathbf{B}^{(1)}_{\mathtt{I}}$ will represent the canonical basis. From a physical point of view, we can suppose that each truth-perspective is associated to an apparatus that allows one to measure a given observable.

Any unitary operator $\mathfrak{T}$ of $\mathcal{H}^{(1)}$ (representing a truth-perspective) can be naturally extended to a unitary operator $\mathfrak{T}^{(n)}$ of $\mathcal{H}^{(n)}$ (for any $n > 1$):

$$\mathfrak{T}^{(n)}|x_1, \ldots, x_n\rangle = \mathfrak{T}|x_1\rangle \otimes \cdots \otimes \mathfrak{T}|x_n\rangle.$$

[1] A different approach to epistemic quantum logics has been developed in some important contributions by A. Baltag and S. Smets (see, for instance, [1–3]). In this approach information is supposed to be stored by quantum objects; at the same time, epistemic agents are supposed to communicate in a classical way. On this basis, epistemic operators are dealt with as classical modalities in a Kripkean framework.

Accordingly, any choice of a unitary operator $\mathfrak{T}$ of $\mathcal{H}^{(1)}$ determines an orthonormal basis $\mathbf{B}^{(n)}_{\mathfrak{T}}$ for $\mathcal{H}^{(n)}$ such that:

$$\mathbf{B}^{(n)}_{\mathfrak{T}} = \left\{ \mathfrak{T}^{(n)}|x_1, \ldots, x_n\rangle : |x_1, \ldots, x_n\rangle \in \mathbf{B}^{(n)}_{\mathtt{I}} \right\}.$$

Instead of $\mathfrak{T}^{(n)}|x_1, \ldots, x_n\rangle$ we will also write: $|x_{1_{\mathfrak{T}}}, \ldots, x_{n_{\mathfrak{T}}}\rangle$. The elements of $\mathbf{B}^{(1)}_{\mathfrak{T}}$ will be called the $\mathfrak{T}$-*bits* of $\mathcal{H}^{(1)}$; while the elements of $\mathbf{B}^{(n)}_{\mathfrak{T}}$ will represent the $\mathfrak{T}$-*registers* of $\mathcal{H}^{(n)}$.

The notions of *truth*, *falsity* and *probability* can be naturally generalized to any truth-perspective $\mathfrak{T}$.

**Definition 5.1** ($\mathfrak{T}$-*true and* $\mathfrak{T}$-*false registers*)

- $|x_{1_{\mathfrak{T}}}, \ldots, x_{n_{\mathfrak{T}}}\rangle$ is a $\mathfrak{T}$-*true register* iff $|x_{n_{\mathfrak{T}}}\rangle = |1_{\mathfrak{T}}\rangle$;
- $|x_{1_{\mathfrak{T}}}, \ldots, x_{n_{\mathfrak{T}}}\rangle$ is a $\mathfrak{T}$-*false register* iff $|x_{n_{\mathfrak{T}}}\rangle = |0_{\mathfrak{T}}\rangle$.

**Definition 5.2** ($\mathfrak{T}$-*Truth and* $\mathfrak{T}$-*Falsity*)

- The $\mathfrak{T}$-*Truth* of $\mathcal{H}^{(n)}$ is the projection operator ${}^{\mathfrak{T}}P^{(n)}_1$ that projects over the closed subspace spanned by the set of all $\mathfrak{T}$- true registers;
- the $\mathfrak{T}$-*Falsity* of $\mathcal{H}^{(n)}$ is the projection operator ${}^{\mathfrak{T}}P^{(n)}_0$ that projects over the closed subspace spanned by the set of all $\mathfrak{T}$- false registers.

**Definition 5.3** ($\mathfrak{T}$-*Probability*) For any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$,

$$\mathrm{p}^{\mathfrak{T}}_1(\rho) := \mathtt{tr}(\rho\, {}^{\mathfrak{T}}P^{(n)}_1).$$

Like in the canonical case, the probability-function $\mathrm{p}^{\mathfrak{T}}_1$ allows us to define a natural pre-order relation $\preceq_{\mathfrak{T}}$ on the set $\mathfrak{D}$ of all possible pieces of quantum information.

**Definition 5.4** (*The* $\mathfrak{T}$-*pre-order relation*) For any $\rho, \sigma \in \mathfrak{D}$,

$$\rho \preceq_{\mathfrak{T}} \sigma \;\text{ iff }\; \mathrm{p}^{\mathfrak{T}}_1(\rho) \leq \mathrm{p}^{\mathfrak{T}}_1(\sigma).$$

All gates can be naturally transposed from the canonical truth-perspective to any truth-perspective $\mathfrak{T}$. Let $\mathtt{G}^{(n)}$ be a gate of $\mathcal{H}^{(n)}$ defined with respect to the canonical truth-perspective. The *twin-gate* $\mathtt{G}^{(n)}_{\mathfrak{T}}$, defined with respect to the truth-perspective $\mathfrak{T}$, is determined as follows:

$$\mathtt{G}^{(n)}_{\mathfrak{T}} := \mathfrak{T}^{(n)}\mathtt{G}^{(n)}\mathfrak{T}^{(n)\dagger}.$$

As expected, like in the case of the canonical gates, any $\mathfrak{T}$-gate $\mathtt{G}^{(n)}_{\mathfrak{T}}$ will have a corresponding $\mathfrak{T}$-unitary operation ${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}}$ such that for any $\rho \in \mathfrak{D}(\mathcal{H}^{(n)})$:

$${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}}\rho = \mathtt{G}^{(n)}_{\mathfrak{T}}\,\rho\,\mathtt{G}^{(n)\dagger}_{\mathfrak{T}}.$$

On this ground, for any choice of a truth-perspective $\mathfrak{T}$, the $\mathfrak{T}$- Toffoli-gate allows us to define a $\mathfrak{T}$- holistic conjunction:

$$\forall \rho \in \mathfrak{D}(\mathscr{H}^{(m+n)}): \quad {}^{\mathfrak{D}}\mathtt{AND}_{\mathfrak{T}}^{(m,n)}(\rho) := {}^{\mathfrak{D}}\mathtt{T}_{\mathfrak{T}}^{(m,n,1)}(\rho \otimes {}^{\mathfrak{T}}P_0^{(1)}).$$

When $\mathfrak{T} = \mathtt{I}$, we will also write: ${}^{\mathfrak{D}}\mathtt{AND}^{(m,n)}$ (instead of ${}^{\mathfrak{D}}\mathtt{AND}_{\mathtt{I}}^{(m,n)}$) and $\mathtt{p}_1$ (instead of $\mathtt{p}_1^{\mathtt{I}}$).

## 5.3 A First-Order Epistemic Quantum Computational Language

We will now introduce the language $\mathscr{L}_1$, which is a first-order epistemic extension of the sentential language $\mathscr{L}_0$ (considered in the previous Chapter).
The alphabet of $\mathscr{L}_1$ contains the following primitive symbols:

- sentential constants, including the true sentence **t** and the false sentence **f**;
- individual names (**a**, **b**, ...) and individual variables ($x$, $y$, ...);
- $m$-ary predicates $\mathbf{P}_i^m$ (with $m \geq 1$);
- the logical connectives $\neg$, $\sqrt{id}$, $\sqrt{\neg}$, $\uplus$, $\top$;
- the universal quantifier $\forall$;
- the epistemic operators $K$ (*to know*), $B$ (*to believe*), $U$ (*to understand*).

We will use $t, t_1, t_2, \ldots$ as metavariables for individual terms (either names or variables). The notions of *formula* and of *sentence* are defined in the expected way:

- sentential constants and expressions having the form $\mathbf{P}_i^m t_1 \ldots t_m$ are (atomic) formulas;
- if $\alpha$, $\beta$ are formulas and $\mathbf{q}$ is a sentential constant, then the expressions $\neg\alpha$, $\sqrt{id}\,\alpha$, $\sqrt{\neg}\,\alpha$, $\alpha \uplus \beta$, $\top(\alpha, \beta, \mathbf{q})$ are formulas;
- for any formula $\alpha(x)$ (where $x$ is a variable occurring free in $\alpha$), the expression $\forall x\alpha(x)$ is a formula;[2]
- for any term $t$ and any formula $\alpha$, the expressions $Kt\alpha$ ($t$ *knows* $\alpha$), $Bt\alpha$ ($t$ *believes* $\alpha$), $Ut\alpha$ ($t$ *understands* $\alpha$) are formulas. The subexpressions $Kt$, $Bt$, $Ut$ will be called *epistemic connectives*.

*Sentences* are formulas that do not contain any free variable.

Like in the sentential case, we will use $\mathbf{q}, \mathbf{q}_1, \mathbf{q}_2, \ldots$ as metavariables for sentential constants, while $\alpha, \beta, \gamma, \ldots$ will represent generic formulas. The binary conjunction $\wedge$, the binary inclusive disjunction $\vee$ and the existential quantifier $\exists$ are metalinguistically defined as follows:

[2]For semantic aims it is useful to assume the strict condition according to which quantifiers should always be applied to variables that occur free in the formulas in question. Accordingly, expressions like $\forall x P^1\mathbf{a}$ will not be considered well-formed formulas (in agreement with the common use of natural languages).

$$\alpha \wedge \beta := \daleth(\alpha, \beta, \mathbf{f}); \quad \alpha \vee \beta := \neg(\neg\alpha \wedge \neg\beta); \quad \exists x\alpha := \neg\forall x\neg\alpha.$$

As happens in the sentential case, any formula $\alpha$ of the language $\mathscr{L}_1$ can be decomposed into its parts, giving rise to its syntactical tree $STree^{\alpha}$:

$$\begin{array}{c} Level_h^{\alpha} \\ \cdots\cdots \\ Level_1^{\alpha} \end{array}$$

where:

- each $Level_i^{\alpha}$ (with $1 \leq i \leq h$) is a sequence $(\beta_{i_1}, \ldots, \beta_{i_r})$ of subformulas of $\alpha$;
- the *bottom level* $Level_1^{\alpha}$ is $(\alpha)$;
- the *top level* $Level_h^{\alpha}$ is the sequence $(at_1^{\alpha}, \ldots, at_k^{\alpha})$ of the atomic subformulas occurring in $\alpha$;
- for any $i$ (with $1 \leq i < h$), $Level_{i+1}^{\alpha}$ is the sequence obtained by dropping the *principal logical connective*, the *principal epistemic connective* and the *principal quantifier* in all molecular formulas occurring at $Level_i^{\alpha}$, and by repeating all atomic formulas that occur at $Level_i^{\alpha}$.

Like in the sentential case, $Height(\alpha)$ (the *Height* of $\alpha$) is the number $h$ of levels of the syntactical tree of $\alpha$.

*Example 5.1* Consider the formula

$$\alpha = K\mathbf{a}\neg\forall x K x \mathbf{P}^{(1)}\mathbf{a}$$

(say, "Alice knows that not everybody knows that she is pretty").

The syntactical tree of $\alpha$ is the following sequence of sequences of subformulas of $\alpha$:

$$\begin{aligned} Level_5^{\alpha} &= (\mathbf{P}^1\mathbf{a}) \\ Level_4^{\alpha} &= (Kx\mathbf{P}^1\mathbf{a}) \\ Level_3^{\alpha} &= (\forall x Kx\mathbf{P}^1\mathbf{a}) \\ Level_2^{\alpha} &= (\neg\forall x Kx\mathbf{P}^1\mathbf{a}) \\ Level_1^{\alpha} &= (K\mathbf{a}\neg\forall x Kx\mathbf{P}^1\mathbf{a}) \end{aligned}$$

We will now define the notion of *atomic structure* of a formula $\alpha$, a syntactical concept that will play an important semantic role. Let us first consider a simple example: the case of an atomic formula $\mathbf{P}^1 t$. The basic semantic idea is that the information corresponding to $\mathbf{P}^1 t$ can be represented by the state $\rho$ of a quantum system $\mathbf{S}$ consisting of three subsystems: the first one is supposed to store the information described by the predicate $\mathbf{P}^1$, the second one stores the information described by the term $t$, while the third one stores the "truth-degree" according to which the object denoted by $t$ satisfies the property denoted by $\mathbf{P}^1$. Notice that, according to this idea, the same type of information is supposed to store both predicates and individual terms. Unlike classical set-theoretic semantics, we do not refer to any *ontological hierarchy*.

In the case of an atomic formula whose form is $\mathbf{P}^m t_1 \dots t_m$, we will need $m + 2$ systems; while for a sentential constant, one system will be sufficient. Accordingly, we can assume that the atomic structure of $\mathbf{P}^m t_1 \dots t_m$ is $(m + 2)$, while $(1)$ is the atomic structure of a sentential constant.

In the general case, the notion of *atomic structure* of a formula $\alpha$ is defined as follows.

**Definition 5.5** (*Atomic structure*) Consider a formula $\alpha$ such that:

$$Level_h^\alpha = (at_1^\alpha, \dots, at_k^\alpha),$$

where $at_1^\alpha, \dots, at_k^\alpha$ are the atomic formulas occurring in $\alpha$ and $h$ is the Height of $\alpha$. The *atomic structure* of $\alpha$ is a sequence of natural numbers

$$AtStr(\alpha) = (n_1, \dots, n_k),$$

such that for any $n_i$ (with $1 \leq i \leq k$):

$$n_i = \begin{cases} 1, & \text{if } at_i^\alpha \text{ is a sentential constant;} \\ 2 + m, & \text{if } at_i^\alpha = \mathbf{P}^m t_1 \dots t_m. \end{cases}$$

The atomic structure of any formula $\alpha$ determines its *atomic complexity*. Let $AtStr(\alpha) = (n_1, \dots, n_k)$. The *atomic complexity* of $\alpha$ is the number

$$At(\alpha) = n_1 + \cdots + n_k.$$

As happens in the sentential case, the atomic complexity of a formula $\alpha$ determines the Hilbert space $\mathcal{H}^\alpha$, the *semantic space* where any possible meaning for $\alpha$ shall live. Let $\alpha$ be a formula such that

$$AtStr(\alpha) = (n_1, \dots, n_k); \quad At(\alpha) = n_1 + \cdots + n_k.$$

We can write:

$$\mathcal{H}^\alpha = \mathcal{H}^{(At(\alpha))} = \mathcal{H}^{(n_1)} \otimes \cdots \otimes \mathcal{H}^{(n_k)} = \mathcal{H}^{(n_1 + \cdots + n_k)}.$$

*Example 5.2* Consider the formula $\alpha = \intercal(\mathbf{P}^1\mathbf{a}, \neg\mathbf{P}^1\mathbf{a}, \mathbf{f})$.

We have:

$$AtStr(\alpha) = (3, 3, 1); \quad At(\alpha) = 7; \quad \mathcal{H}^\alpha = \mathcal{H}^{(7)}.$$

## 5.4 A Holistic Quantum Computational Semantics for a Fragment of the Language $\mathscr{L}_1$

We will first introduce the basic semantic concepts for a fragment of the full language $\mathscr{L}_1$. This fragment, indicated by $\mathscr{L}_1^-$, consists of all formulas that do not contain any occurrence either of quantifiers or of epistemic operators. In such a case, for any choice of a truth-perspective $\mathfrak{T}$, the syntactical tree of any formula $\alpha$ uniquely determines a sequence of gates, all defined on the semantic space of $\alpha$.

As an example, consider the (contradictory) formula

$$\alpha = \mathbf{P}^1\mathbf{a} \wedge \neg\mathbf{P}^1\mathbf{a} = \top(\mathbf{P}^1\mathbf{a}, \neg\mathbf{P}^1\mathbf{a}, \mathbf{f}).$$

In the syntactical tree of $\alpha$ the second level has been obtained from the third level by repeating the first occurrence of $\mathbf{P}^1\mathbf{a}$, by negating the second occurrence of $\mathbf{P}^1\mathbf{a}$ and by repeating $\mathbf{f}$, while the first level has been obtained by applying the connective $\top$ to the sequence of formulas occurring at the second level. Accordingly, one can say that, for any choice of a truth-perspective $\mathfrak{T}$, the syntactical tree of $\alpha$ uniquely determines the following sequence consisting of two gates, both defined on the semantic space of $\alpha$:

$$\left({}^{\mathfrak{D}}\mathtt{I}^{(3)}_{\mathfrak{T}} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(3)}_{\mathfrak{T}} \otimes {}^{\mathfrak{D}}\mathtt{I}^{(1)}_{\mathfrak{T}},\ {}^{\mathfrak{D}}\mathtt{T}^{(3,3,1)}_{\mathfrak{T}}\right).$$

Such a sequence is called the $\mathfrak{T}$-*gate tree* of $\alpha$. This procedure can be naturally generalized to any formula $\alpha$. The general form of the $\mathfrak{T}$- gate tree of $\alpha$ will be:

$$({}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{\mathfrak{T}_{(h-1)}}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{\mathfrak{T}_{(1)}}),$$

where $h$ is the Height of $\alpha$.

Now the concepts of *holistic map*, *contextual meaning* and *holistic model* for the language $\mathscr{L}_1^-$ can be defined, like in the sentential case, *mutatis mutandis*.

**Definition 5.6** (*Holistic map*) A *holistic map* for $\mathscr{L}_1^-$, associated to a truth-perspective $\mathfrak{T}$, is a map $\mathtt{Hol}_{\mathfrak{T}}$ that assigns a meaning $\mathtt{Hol}_{\mathfrak{T}}(Level_i^{\alpha})$ to each level of the syntactical tree of $\alpha$, for any formula $\alpha$. This meaning is a density operator living in the semantic space of $\alpha$.

On this basis, the meaning assigned by $\mathtt{Hol}_{\mathfrak{T}}$ to the formula $\alpha$ is defined as follows:

$$\mathtt{Hol}_{\mathfrak{T}}(\alpha) := \mathtt{Hol}_{\mathfrak{T}}(Level_1^{\alpha}).$$

Given a formula $\gamma$, any holistic map $\mathtt{Hol}_{\mathfrak{T}}$ determines the *contextual meaning*, with respect to the context $\mathtt{Hol}_{\mathfrak{T}}(\gamma)$, of any occurrence in $\gamma$ of a subformula, of a predicate, of a term.

**Definition 5.7** (*Contextual meaning of an occurrence of a subformula*) Consider a formula $\gamma$ such that $Level_i^{\gamma} = (\beta_{i_1}, \ldots, \beta_{i_r})$. We have:

$$\mathscr{H}^{\gamma} = \mathscr{H}^{\beta_{i_1}} \otimes \cdots \otimes \mathscr{H}^{\beta_{i_r}}.$$

Let $\mathtt{Hol}_{\mathfrak{T}}$ be a holistic map. The *contextual meaning* of the occurrence $\beta_{i_j}$ with respect to the context $\mathtt{Hol}_{\mathfrak{T}}(\gamma)$ is defined as follows:

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta_{i_j}) := Red^{(j)}_{[At(\beta_{i_1}),\ldots,At(\beta_{i_r})]}(\mathtt{Hol}_{\mathfrak{T}}(Level_i(\gamma))).$$

Of course, we obtain:

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\gamma) = \mathtt{Hol}_{\mathfrak{T}}(\gamma).$$

**Definition 5.8** (*Contextual meaning of an occurrence of a predicate and of a term*) Consider a formula $\gamma$ such that $Level^{\gamma}_i = (\beta_{i_1}, \ldots, \beta_{i_r})$ and let $\beta_{i_j} = \mathbf{P}^m t_1 \ldots t_m$. Consider a holistic map $\mathtt{Hol}_{\mathfrak{T}}$. The *contextual meanings* of the occurrences of $\mathbf{P}^m$ and of $t_k$ (with $1 \le k \le m$) in $\beta_{i_j}$ with respect to the context $\mathtt{Hol}_{\mathfrak{T}}(\gamma)$ are defined as follows:

$$\mathtt{Hol}^{(\gamma,\beta_{i_j})}_{\mathfrak{T}}(\mathbf{P}^m) := Red^{(1)}_{[1,m+1]}(\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta_{i_j}));$$

$$\mathtt{Hol}^{(\gamma,\beta_{i_j})}_{\mathfrak{T}}(t_k) := Red^{(2)}_{[k,1,m+2-(k+1)]}(\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta_{i_j})).$$

A holistic map $\mathtt{Hol}_{\mathfrak{T}}$ is called *normal for a formula* $\gamma$ iff $\mathtt{Hol}_{\mathfrak{T}}$ assigns the same contextual meaning to all occurrences of a subformula, of a predicate, of a term in the syntactical tree of $\gamma$. A *normal holistic map* is a holistic map $\mathtt{Hol}_{\mathfrak{T}}$ that is normal for all formulas $\gamma$.

Like in the sentential case, *holistic models* of the language $\mathscr{L}_1^-$ can be now defined as normal holistic maps that preserve the logical form of all formulas, assigning the "right" meaning to the false sentence **f** and to the true sentence **t**.

**Definition 5.9** (*Holistic model*) A *holistic model* of $\mathscr{L}_1^-$ is a normal holistic map $\mathtt{Hol}_{\mathfrak{T}}$ that satisfies the following conditions for any formula $\alpha$.

(1) Let $({}^{\mathfrak{D}}\mathrm{G}^{\alpha}_{\mathfrak{T}_{(h-1)}}, \ldots, {}^{\mathfrak{D}}\mathrm{G}^{\alpha}_{\mathfrak{T}_{(1)}})$ be the $\mathfrak{T}$-gate tree of $\alpha$ and let $1 \le i < h$. Then,

$$\mathtt{Hol}_{\mathfrak{T}}(Level^{\alpha}_i) = {}^{\mathfrak{D}}\mathrm{G}^{\alpha}_{\mathfrak{T}_{(i)}}(\mathtt{Hol}_{\mathfrak{T}}(Level^{\alpha}_{i+1})).$$

In other words, the meaning of each level (different from the top level) is obtained by applying the corresponding gate to the meaning of the level that occurs immediately above.

(2) The contextual meanings assigned by $\mathtt{Hol}_{\mathfrak{T}}$ to the false sentence **f** and to the true sentence **t** are the $\mathfrak{T}$-Falsity ${}^{\mathfrak{T}}P^{(1)}_0$ and the $\mathfrak{T}$-Truth ${}^{\mathfrak{T}}P^{(1)}_1$, respectively.

On this basis, we put:

$$\mathtt{Hol}_{\mathfrak{T}}(\alpha) := \mathtt{Hol}_{\mathfrak{T}}(Level^{\alpha}_1),$$

for any formula $\alpha$.

As happens in the sentential case, any $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$ represents a kind of autonomous semantic context that is not necessarily correlated with the meanings of other formulas. Generally we have:

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta) \neq \mathtt{Hol}^{\delta}_{\mathfrak{T}}(\beta).$$

Thus, one and the same formula may receive different contextual meanings in different contexts.

Now the concepts of *truth*, *validity* and *logical consequence* for the language $\mathscr{L}_1^-$ can be defined like in the sentential case, *mutatis mutandis*.

**Definition 5.10** (*Truth*) A formula $\alpha$ is called *true* with respect to a model $\mathtt{Hol}_{\mathfrak{T}}$ (abbreviated as $\models_{\mathtt{Hol}_{\mathfrak{T}}} \alpha$) iff $\mathtt{p}_1^{\mathfrak{T}}(\mathtt{Hol}_{\mathfrak{T}}(\alpha)) = 1$.

**Definition 5.11** (*Validity*)

(1) $\alpha$ is called $\mathfrak{T}$-*valid* ($\models_{\mathfrak{T}} \alpha$) iff for any model $\mathtt{Hol}_{\mathfrak{T}}$, $\models_{\mathtt{Hol}_{\mathfrak{T}}} \alpha$.
(2) $\alpha$ is called *valid* ($\models \alpha$) iff for any truth-perspective $\mathfrak{T}$, $\models_{\mathfrak{T}} \alpha$.

**Definition 5.12** (*Logical consequence*)

(1) $\beta$ is called a $\mathfrak{T}$-*logical consequence* of $\alpha$ ($\alpha \vDash_{\mathfrak{T}} \beta$) iff for any formula $\gamma$ such that $\alpha$ and $\beta$ are subformulas of $\gamma$ and for any model $\mathtt{Hol}_{\mathfrak{T}}$,

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\alpha) \preceq_{\mathfrak{T}} \mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta).$$

(2) $\beta$ is called a *logical consequence* of $\alpha$ ($\alpha \vDash \beta$) iff for any truth-perspective $\mathfrak{T}$, $\alpha \vDash_{\mathfrak{T}} \beta$.

When $\alpha \vDash_{\mathtt{I}} \beta$, we say that $\beta$ is a *canonical logical consequence* of $\alpha$.

Interestingly enough, the concept of logical consequence turns out to be invariant with respect to truth-perspective changes.

**Theorem 5.1** *For any truth-perspective $\mathfrak{T}$ and for any formulas $\alpha$, $\beta$:*

$$\alpha \vDash_{\mathfrak{T}} \beta \ \textit{iff} \ \alpha \vDash_{\mathtt{I}} \beta.$$

*Proof* Consider a truth-perspective $\mathfrak{T}$. In any space $\mathscr{H}^{(n)}$, any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$ has a $\mathfrak{T}$-*twin* ${}^{\mathfrak{T}}\rho$ such that:

$${}^{\mathfrak{T}}\rho = \mathfrak{T}\rho\mathfrak{T}^{\dagger}.$$

Of course, ${}^{\mathfrak{T}}\rho = \rho$, if $\mathfrak{T} = \mathtt{I}$. Consider the map

$$\mathfrak{t} : \mathfrak{D}(\mathscr{H}^{(n)}) \ \rightarrow \ \mathfrak{D}(\mathscr{H}^{(n)}),$$

such that $\mathfrak{t}(\rho) = {}^{\mathfrak{T}}\rho$, for any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$. Since $\mathfrak{T}$ is a unitary operator, the map $\mathfrak{t}$ is a bijection from $\mathfrak{D}(\mathscr{H}^{(n)})$ onto itself. One can prove that:

(1) for any gate ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ of $\mathscr{H}^{(n)}$ and any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$,

$$\mathfrak{t}({}^{\mathfrak{D}}\mathtt{G}^{(n)}\rho) = {}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}}\mathfrak{t}(\rho)$$

(where ${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}}$ is the *twin-gate* of ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ with respect to the truth-perspective $\mathfrak{T}$). Thus, the map $\mathfrak{t}$ preserves all gates.

(2) For any $\rho, \sigma \in \mathfrak{D}(\mathscr{H}^{(n)})$,

$$\rho \preceq_{\mathtt{I}} \sigma \ \text{ iff } \ \mathfrak{t}(\rho) \preceq_{\mathfrak{T}} \mathfrak{t}(\sigma).$$

Thus, the map $\mathfrak{t}$ preserves the pre-order relation.

On this basis, one can easily prove the following conditions ((3), (4)).

(3) For any canonical model $\mathtt{Hol}_{\mathtt{I}}$ there exists a $\mathfrak{T}$-model ${}^{(\mathfrak{t})}\mathtt{Hol}_{\mathfrak{T}}$ such that for any formula $\gamma$ and any subformula $\alpha$ of $\gamma$,

$$\mathtt{Hol}^{\gamma}_{\mathtt{I}}(\alpha) = \rho \implies {}^{(\mathfrak{t})}\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\alpha) = \mathfrak{t}(\rho).$$

Whence (by (2)):

$$\mathtt{Hol}^{\gamma}_{\mathtt{I}}(\alpha) \preceq_{\mathtt{I}} \mathtt{Hol}^{\gamma}_{\mathtt{I}}(\beta) \ \text{ iff } \ {}^{(\mathfrak{t})}\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\alpha) \preceq_{\mathfrak{T}} {}^{(\mathfrak{t})}\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta).$$

(4) For any $\mathfrak{T}$- model $\mathtt{Hol}_{\mathfrak{T}}$ there exists a canonical model ${}^{(\mathfrak{t}^{-1})}\mathtt{Hol}_{\mathtt{I}}$ such that for any formula $\gamma$ and any subformula $\alpha$ of $\gamma$,

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\alpha) = \rho \implies {}^{(\mathfrak{t}-1)}\mathtt{Hol}^{\gamma}_{\mathtt{I}}(\alpha) = \mathfrak{t}^{-1}(\rho).$$

Whence (by (2)):

$$\mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\alpha) \preceq_{\mathfrak{T}} \mathtt{Hol}^{\gamma}_{\mathfrak{T}}(\beta) \quad \text{iff} \quad {}^{(\mathfrak{t}-1)}\mathtt{Hol}^{\gamma}_{\mathtt{I}}(\alpha) \preceq_{\mathtt{I}} {}^{(\mathfrak{t}-1)}\mathtt{Hol}^{\gamma}_{\mathtt{I}}(\beta).$$

Consequently, by definition of $\mathfrak{T}$-logical consequence we obtain:

$$\alpha \models_{\mathfrak{T}} \beta \quad \text{iff} \quad \alpha \models_{\mathtt{I}} \beta.$$

□

An immediate consequence of Theorem 5.1 is the following Corollary.

**Corollary 5.1** $\alpha \models \beta$ *iff* $\alpha \models_{\mathtt{I}} \beta$ *iff* $\alpha \models_{\mathfrak{T}} \beta$, *for some truth-perspective* $\mathfrak{T}$.

Like in the sentential case, one can prove that the logical consequence-relation is reflexive and transitive.

**Theorem 5.2**

*(1)* $\alpha \models \alpha$;

*(2)* $\alpha \models \beta$ *and* $\beta \models \delta \Rightarrow \alpha \models \delta$.

## 5.5 An Epistemic Quantum Computational Semantics

We will now define the basic semantic concepts for a richer fragment of the language $\mathscr{L}_1$. This fragment, indicated by ${}^{Ep}\mathscr{L}_1^-$ represents an epistemic extension of $\mathscr{L}_1^-$ that includes all quantifier-free epistemic formulas of $\mathscr{L}_1$.

The main intuitive idea of the epistemic quantum computational semantics can be sketched as follows: any occurrence of an epistemic operator $(K, B, U)$ in a formula $\alpha$ is interpreted as a special example of a quantum map, representing an *epistemic operation* associated to a given epistemic agent, which is characterized by a particular truth-perspective. Of course "real" agents evolve in time, changing their *epistemic status*. For the sake of simplicity, however, we will abstract from time, considering all agents during "short" time-intervals, where their epistemic status is supposed to remain constant.[3]

We will start by analyzing the most significant epistemic operations, represented by *knowledge-operations*.

**Definition 5.13** (*Knowledge-operation*) A *knowledge-operation* of a Hilbert space $\mathscr{H}^{(n)}$ with respect to a truth-perspective $\mathfrak{T}$ is a map

$$\mathfrak{K}_{\mathfrak{T}}^{(n)} : \mathscr{B}(\mathscr{H}^{(n)}) \to \mathscr{B}(\mathscr{H}^{(n)}),$$

where $\mathscr{B}(\mathscr{H}^{(n)})$ is the set of all bounded operators of $\mathscr{H}^{(n)}$. The following conditions are required:

(1) for any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$, $\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$;
(2) $\mathfrak{K}_{\mathfrak{T}}^{(n)}$ is associated with an *epistemic domain* $EpD(\mathfrak{K}_{\mathfrak{T}}^{(n)})$ that is a subset of $\mathfrak{D}(\mathscr{H}^{(n)})$;
(3) $\mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho) \leq \mathtt{p}_1^{\mathfrak{T}}(\rho)$, for any $\rho \in EpD(\mathfrak{K}_{\mathfrak{T}}^{(n)})$.

As expected, the intuitive interpretation of $\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho$ is the following: the piece of information $\rho$ is known according to the truth-perspective $\mathfrak{T}$. The knowledge described by $\mathfrak{K}_{\mathfrak{T}}^{(n)}$ is limited by a given epistemic domain, which is intended to represent the information accessible to a given agent, relatively to the space $\mathscr{H}^{(n)}$.[4]

When $\rho$ belongs to the epistemic domain of $\mathfrak{K}_{\mathfrak{T}}^{(n)}$, it seems reasonable to assume that the probability-values of $\rho$ and $\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho$ are correlated: the probability of the quantum information asserting that "$\rho$ is known" should always be less than or equal to the probability of $\rho$. Hence, in particular, we have:

$$\mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho) = 1 \ \Rightarrow\ \mathtt{p}_1^{\mathfrak{T}}(\rho) = 1.$$

[3] See [4–8].

[4] The *epistemic domain* of $\mathfrak{K}_{\mathfrak{T}}^{(n)}$ should not be confused with the *domain* of $\mathfrak{K}_{\mathfrak{T}}^{(n)}$, which coincides with the set of all bounded operators of the space: $\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho$ is defined, even if $\rho$ does not belong to the epistemic domain of $\mathfrak{K}_{\mathfrak{T}}^{(n)}$.

But, generally, not the other way around. In other words, pieces of quantum information that are certainly known are certainly true (with respect to the truth-perspective in question). This condition is clearly in agreement with a general principle of standard epistemic logics, according to which “knowledge implies truth, but generally not the other way around”.

A knowledge-operation $\mathfrak{K}_{\mathfrak{T}}^{(n)}$ is called

- *non-trivial* iff for at least one density operator $\rho \in EpD(\mathfrak{K}_{\mathfrak{T}}^{(n)})$,

$$\mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}_{\mathfrak{T}}^{(n)}\rho) < \mathtt{p}_1^{\mathfrak{T}}(\rho);$$

- *strong* iff $EpD(\mathfrak{K}_{\mathfrak{T}}^{(n)}) = \mathfrak{D}(\mathcal{H}^{(n)})$ (thus, the agent in question has access to all pieces of quantum information of the space).

Can knowledge-operations be always represented as (reversible) gates? We will prove that this question has a negative answer. To this aim, we will first introduce the concept of *probabilistic identity* with respect to a truth-perspective $\mathfrak{T}$ (briefly, $\mathfrak{T}$-*probabilistic identity*).

**Definition 5.14** ($\mathfrak{T}$-*probabilistic identity*) A linear operator $A$ of a space $\mathcal{H}^{(n)}$ is called a $\mathfrak{T}$-*probabilistic identity* iff for any quregister $|\psi\rangle$ of the space,

$$\mathtt{p}_1^{\mathfrak{T}}(A|\psi\rangle) = \mathtt{p}_1^{\mathfrak{T}}(|\psi\rangle).$$

Thus, $\mathfrak{T}$-probabilistic identities preserve all $\mathfrak{T}$-probability values.

Some characteristic properties of $\mathfrak{T}$-probabilistic identities of the space $\mathcal{H}^{(1)}$ are described by the two following Theorems.

**Theorem 5.3** *A linear operator $A$ of $\mathcal{H}^{(1)}$ is a $\mathfrak{T}$-probabilistic identity iff $A$ can be represented as a matrix (with respect to the basis $\mathbf{B}_{\mathfrak{T}}^1$) whose form is:*

$$A = \begin{bmatrix} e^{\imath\theta} & 0 \\ 0 & e^{\imath\eta} \end{bmatrix},$$

*where $\theta, \eta \in \mathbb{R}$ and $\imath$ is the imaginary unit.*[5]

*Proof* 1. Suppose that

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is a $\mathfrak{T}$-probabilistic identity. We have:

- $A|0\rangle_{\mathfrak{T}} = a|0\rangle_{\mathfrak{T}} + c|1\rangle_{\mathfrak{T}}; \quad A|1\rangle_{\mathfrak{T}} = b|0\rangle_{\mathfrak{T}} + d|1\rangle_{\mathfrak{T}}.$

[5]For the concept of *matrix-representation* of a linear operator $A$ on a finite-dimensional Hilbert space see Sect. 10.2 (of the *Mathematical Survey* in Chap. 10).

- $\mathtt{p}_1^{\mathfrak{T}}(A|0\rangle_{\mathfrak{T}}) = \mathtt{p}_1^{\mathfrak{T}}(|0\rangle_{\mathfrak{T}}) = 0$;   $\mathtt{p}_1^{\mathfrak{T}}(A|1\rangle_{\mathfrak{T}}) = \mathtt{p}_1^{\mathfrak{T}}(|1\rangle_{\mathfrak{T}}) = 1$.

Hence, $b = 0$, $d = e^{\iota\eta}$ (for some $\eta \in \mathbb{R}$) and $c = 0$, $a = e^{\iota\theta}$ (for some $\theta \in \mathbb{R}$). Thus,

$$A = \begin{bmatrix} e^{\iota\theta} & 0 \\ 0 & e^{\iota\eta} \end{bmatrix}.$$

2. Suppose that

$$A = \begin{bmatrix} e^{\iota\theta} & 0 \\ 0 & e^{\iota\eta} \end{bmatrix}.$$

Consider a generic qubit $|\psi\rangle = a_0|0\rangle_{\mathfrak{T}} + a_1|1\rangle_{\mathfrak{T}}$ of $\mathscr{H}^{(1)}$. We have:

$$A|\psi\rangle = a_0 e^{\iota\theta}|0\rangle_{\mathfrak{T}} + a_1 e^{\iota\eta}|1\rangle_{\mathfrak{T}}.$$

Thus,

$$\mathtt{p}_1^{\mathfrak{T}}(A|\psi\rangle) = |a_1 e^{\iota\eta}|^2 = |a_1|^2 = \mathtt{p}_1^{\mathfrak{T}}(|\psi\rangle).$$

Hence, $A$ is a $\mathfrak{T}$-probabilistic identity.

□

**Theorem 5.4** *Let* $\mathtt{U}$ *be a unitary operator of* $\mathscr{H}^{(1)}$ *such that for any qubit* $|\psi\rangle$ *of the space,*

$$\mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|\psi\rangle) \leq \mathtt{p}_1^{\mathfrak{T}}(|\psi\rangle).$$

*Then,* $\mathtt{U}$ *is a* $\mathfrak{T}$*-probabilistic identity of* $\mathscr{H}^{(1)}$.

*Proof* Let

$$\mathtt{U} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Thus, $\mathtt{U}|0\rangle_{\mathfrak{T}} = a|0\rangle_{\mathfrak{T}} + c|1\rangle_{\mathfrak{T}}$ and $\mathtt{U}|1\rangle_{\mathfrak{T}} = b|0\rangle_{\mathfrak{T}} + d|1\rangle_{\mathfrak{T}}$.

By hypothesis we have:

$$\mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|0\rangle_{\mathfrak{T}}) = \mathtt{p}_1^{\mathfrak{T}}(a|0\rangle_{\mathfrak{T}} + c|1\rangle_{\mathfrak{T}}) \leq \mathtt{p}_1^{\mathfrak{T}}(|0\rangle_{\mathfrak{T}}) = 0.$$

Hence, $\mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|0\rangle_{\mathfrak{T}}) = 0$, $c = 0$ and $a = e^{\iota\theta}$ (for some $\theta \in \mathbb{R}$). Consequently,

$$\mathtt{U} = \begin{bmatrix} e^{\iota\theta} & b \\ 0 & d \end{bmatrix}.$$

Since $\mathtt{U}$ is unitary, we have: $\mathtt{U}\mathtt{U}^{\dagger} = \mathtt{I}^{(1)}$. Thus,

$$\begin{bmatrix} e^{\iota\theta} & b \\ 0 & d \end{bmatrix} \begin{bmatrix} (e^{\iota\theta})^* & 0 \\ b^* & d^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, $dd^* = 1$ and $d = e^{\imath\eta}$ (for some $\eta \in \mathbb{R}$). Moreover, $b = 0$, because $e^{\imath\theta}(e^{\imath\theta})^* + bb^* = 1$. Whence,

$$\mathtt{U} = \begin{bmatrix} e^{\imath\theta} & 0 \\ 0 & e^{\imath\eta} \end{bmatrix}.$$

Consequently, by Theorem 5.3, $\mathtt{U}$ is a $\mathfrak{T}$-probabilistic identity.

□

**Theorem 5.5** *Non-trivial strong knowledge-operations of the space $\mathscr{H}^{(1)}$ cannot be represented as unitary operations.*

*Proof* Let $\mathfrak{K}_{\mathfrak{T}}^{(1)}$ be a non-trivial strong knowledge operation of $\mathscr{H}^{(1)}$ and suppose by contradiction that $\mathfrak{K}_{\mathfrak{T}}^{(1)}$ is a unitary operation. Hence, there exists a unitary operator $\mathtt{U}$ of $\mathscr{H}^{(1)}$ such that for any $\rho \in \mathfrak{D}(\mathscr{H}^{(1)})$:

$$\mathfrak{K}_{\mathfrak{T}}^{(1)}\rho = \mathtt{U}\rho\mathtt{U}^{\dagger}.$$

If $\rho$ is a pure state $P_{|\psi\rangle}$, we have:

$$\mathfrak{K}_{\mathfrak{T}}^{(1)} P_{|\psi\rangle} = \mathtt{U}P_{|\psi\rangle}\mathtt{U}^{\dagger} = P_{\mathtt{U}|\psi\rangle}.$$

Thus,

$$\mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}^{(1)} P_{|\psi\rangle}) = \mathtt{p}_1^{\mathfrak{T}}(P_{\mathtt{U}|\psi\rangle}) = \mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|\psi\rangle).$$

Since $\mathfrak{K}_{\mathfrak{T}}^{(1)}$ is a strong knowledge operation, any pure state $|\psi\rangle$ of $\mathscr{H}^{(1)}$ shall satisfy the condition:

$$\mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|\psi\rangle) \leq \mathtt{p}_1^{\mathfrak{T}}(|\psi\rangle).$$

Consequently, by Theorem 5.4, the unitary operator $\mathtt{U}$ turns out to behave as a $\mathfrak{T}$-probabilistic identity. We obtain:

$$\mathtt{p}_1^{\mathfrak{T}}(\mathtt{U}|\psi\rangle) = \mathtt{p}_1^{\mathfrak{T}}(|\psi\rangle);\;\; \mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}^{(1)} P_{|\psi\rangle}) = \mathtt{p}_1^{\mathfrak{T}}(P_{|\psi\rangle}).$$

One can show that a similar equality holds for all density operators $\rho \in \mathfrak{D}(\mathscr{H}^{(1)})$:

$$\mathtt{p}_1^{\mathfrak{T}}(\mathfrak{K}_{\mathfrak{T}}^{(1)}\rho) = \mathtt{p}_1^{\mathfrak{T}}(\rho).$$

But this contradicts the hypothesis that $\mathfrak{K}_{\mathfrak{T}}^{(1)}$ is a non-trivial knowledge operation. □

Generally, the *act of knowing* seems to be characterized by an intrinsic irreversibility that is quite similar to what happens in the case of quantum-measurement phenomena.

We will now analyze the behavior of two other important epistemic operations: *believing* and *understanding*. As is well known, a rich literature on epistemic logics has deeply studied the critical relationships between *knowledge* and *beliefs*. And in this connection different intuitive ideas and different abstract approaches have been proposed. A crucial question concerns the "degree of rationality" that should be attributed to beliefs. Shall we assume, for instance, that beliefs always respect some "minimal" logical requirements? To what extent can beliefs be represented as particular forms of *subjective knowledge*?

We will follow here a somewhat "pessimistic" view about the rationality of beliefs, which (unfortunately) seems to be frequently confirmed by many forms of individual and collective behaviors in our present society. Epistemic agents seem to be often inclined to *believe* a lot of assertions, whose meanings are not necessarily understood by them. Beliefs are not generally based either on empirical evidence or on rational arguments. Accordingly, in the framework of the epistemic quantum computational semantics the abstract behavior of *belief-operations* will be sharply distinguished from the abstract behavior of *knowledge-operations*. Unlike knowledge-operations, belief-operations will not be associated either to epistemic domains or to probabilistic constraints.

**Definition 5.15** (*Belief-operation*) A *belief-operation* of a Hilbert space $\mathscr{H}^{(n)}$ with respect to a truth-perspective $\mathfrak{T}$ (indicated by $\mathfrak{B}_{\mathfrak{T}}^{(n)}$) is any map that transforms density operators into density operators of the space.

The expected intuitive interpretation of $\mathfrak{B}_{\mathfrak{T}}^{(n)}\rho$ is: the piece of information $\rho$ is believed according to the truth-perspective $\mathfrak{T}$. Unlike knowledge-operations, belief-operations (which are not supposed to satisfy any particular restriction) can be represented as (reversible) gates. A somewhat curious example of a belief-operation might be the following:

$$\mathfrak{B}_{\mathtt{I}}^{(n)} = {}^{\mathfrak{D}}\mathtt{NOT}_{\mathtt{I}}^{(n)}.$$

An agent whose belief-operation is $\mathfrak{B}_{\mathtt{I}}^{(n)}$ behaves as a person characterized by a "perfect spirit of contradiction". Whenever a piece of information $\rho$ is proposed, his/her reaction will be an opposition to $\rho$. Thus, such an agent will *certainly believe* some pieces of information that are *certainly false*!

It is worth-while noticing that the quantum computational approach to epistemic logic does not oppose *beliefs* (which may correspond to irrational behaviors) to a kind of *absolute* (or *dogmatic*) concept of knowledge. As we have seen, according to our definition of *knowledge-operation*, any $\mathfrak{K}_{\mathfrak{T}}^{(n)}$ turns out to depend on the choice of a truth-perspective and of a particular information-domain that is assumed to be accessible to the epistemic agent under consideration. Hence, knowledge is here described as a *probabilistic valuation* that is essentially *relativistic and context-dependent*, in perfect agreement with the characteristic "spirit" of quantum theory.

Let us now analyze the behavior of our third epistemic operation: *understanding*. As happens in the case of knowledge-operations, it seems reasonable to assume that the *understanding-operation* $\mathfrak{U}_{\mathfrak{T}}^{(n)}$ of a given epistemic agent (with respect to a truth perspective $\mathfrak{T}$, in a Hilbert space $\mathscr{H}^{(n)}$) is associated to an epistemic domain $EpD(\mathfrak{U}_{\mathfrak{T}}^{(n)})$, consisting of all pieces of information that our agent is able to understand.

**Definition 5.16** (*Understanding-operation*) An *understanding-operation* of a Hilbert space $\mathscr{H}^{(n)}$ with respect to a truth-perspective $\mathfrak{T}$ is a map

$$\mathfrak{U}_{\mathfrak{T}}^{(n)} : \mathscr{B}(\mathscr{H}^{(n)}) \to \mathscr{B}(\mathscr{H}^{(n)}),$$

that satisfies the following conditions:

(1) for any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$, $\mathfrak{U}_{\mathfrak{T}}^{(n)}\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$;
(2) $\mathfrak{U}_{\mathfrak{T}}^{(n)}$ is associated with an *epistemic domain* $EpD(\mathfrak{U}_{\mathfrak{T}}^{(n)})$ that is a subset of $\mathfrak{D}(\mathscr{H}^{(n)})$;
(3) $\rho \in EpD(\mathfrak{U}_{\mathfrak{T}}^{(n)}) \;\Rightarrow\; \mathtt{p}_1^{\mathfrak{T}}(\mathfrak{U}_{\mathfrak{T}}^{(n)}\rho) = 1.$

Thus, the information $\mathfrak{U}_{\mathfrak{T}}^{(n)}\rho$ ($\rho$ is understood according to the truth-perspective $\mathfrak{T}$) is *certain*, whenever $\rho$ is a piece of information epistemically accessible to the agent under consideration.

On this basis we can now define the concept of *epistemic situation* of a given agent. From an intuitive point of view it seems reasonable to assume that the epistemic situation of an agent $\mathfrak{i}$ (say, *Alice*, *Bob*,...) is characterized by the following elements:

- the truth-perspective of $\mathfrak{i}$;
- the pieces of information that are epistemically accessible to $\mathfrak{i}$;
- the probabilistic behavior of $\mathfrak{i}$ with respect to *knowledge*, *belief* and *understanding* in any information-environment $\mathfrak{D}(\mathscr{H}^{(n)})$.

**Definition 5.17** (*Epistemic situation of an agent*) Let $\mathfrak{i}$ represent an epistemic agent. An *epistemic situation* for $\mathfrak{i}$ is a system

$$\mathfrak{EpSit}_{\mathfrak{i}} = (\mathfrak{T}_{\mathfrak{i}},\ EpD_{\mathfrak{i}},\ \mathfrak{K}_{\mathfrak{i}},\ \mathfrak{B}_{\mathfrak{i}}\ \mathfrak{U}_{\mathfrak{i}}),$$

where:

(1) $\mathfrak{T}_{\mathfrak{i}}$ represents the truth-perspective of $\mathfrak{i}$.
(2) $EpD_{\mathfrak{i}}$ is a map that assigns to any $n \geq 1$ a set $EpD_{\mathfrak{i}}^{(n)} \subseteq \mathfrak{D}(\mathscr{H}^{(n)})$ that represents the information accessible to $\mathfrak{i}$ in the information-environment $\mathfrak{D}(\mathscr{H}^{(n)})$.
(3) $\mathfrak{K}_{\mathfrak{i}}$ is a map that assigns to any $n \geq 1$ a knowledge-operation $\mathfrak{K}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}$ (defined on $\mathscr{H}^{(n)}$), which describes the knowledge of $\mathfrak{i}$ with respect to the information-environment $\mathfrak{D}(\mathscr{H}^{(n)})$. The epistemic domain associated to the operation $\mathfrak{K}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}$ is the set $EpD_{\mathfrak{i}}^{(n)}$.
(4) $\mathfrak{B}_{\mathfrak{i}}$ is a map that assigns to any $n \geq 1$ a belief-operation $\mathfrak{B}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}$ (defined on $\mathscr{H}^{(n)}$), which describes the beliefs of $\mathfrak{i}$ with respect to the information-environment $\mathfrak{D}(\mathscr{H}^{(n)})$.
(5) $\mathfrak{U}_{\mathfrak{i}}$ is a map that assigns to any $n \geq 1$ an understanding-operation $\mathfrak{U}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}$ (defined on $\mathscr{H}^{(n)}$), which describes the pieces of information understood by $\mathfrak{i}$ with respect to the information-environment $\mathfrak{D}(\mathscr{H}^{(n)})$. The epistemic domain associated to the operation $\mathfrak{U}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}$ is the set $EpD_{\mathfrak{i}}^{(n)}$.

The following conditions are required:

(a) $\forall \rho \in \mathfrak{D}(\mathscr{H}^{(n)}) : \mathtt{p}_1^{\mathfrak{T}_{\mathfrak{i}}}(\mathfrak{K}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}\rho) \;\leq\; \mathtt{p}_1^{\mathfrak{T}_{\mathfrak{i}}}(\mathfrak{U}_{\mathfrak{T}_{\mathfrak{i}}}^{(n)}\rho).$

The probability of knowing a given information is less than or equal to the probability of understanding it. Hence, in particular, what is certainly known is certainly understood. But, generally, not the other way around.

(b) $\forall \rho \in \mathfrak{D}(\mathscr{H}^{(n)}) : \mathtt{p}_1^{\mathfrak{T}_\mathrm{i}}(\mathfrak{K}_{\mathfrak{T}_\mathrm{i}}^{(n)} \rho) \ \leq \ \mathtt{p}_1^{\mathfrak{T}_\mathrm{i}}(\mathfrak{B}_{\mathfrak{T}_\mathrm{i}}^{(n)} \rho)$.
The probability of knowing a given information is less than or equal to the probability of believing it. Hence, in particular, what is certainly known is certainly believed. But, generally, not the other way around.

We can now define the main semantic concepts of the epistemic quantum computational semantics for the language ${}^{Ep}\mathscr{L}_1^-$.

The notions of *normal holistic map* ($\mathtt{Hol}_{\mathfrak{T}}$) and of *contextual meanings* ($\mathtt{Hol}_{\mathfrak{T}}^{\gamma}(t)$, $\mathtt{Hol}_{\mathfrak{T}}^{\gamma}(\mathbf{P}^m)$, $\mathtt{Hol}_{\mathfrak{T}}^{\gamma}(\beta)$) can be defined like in the case of the language $\mathscr{L}_1^-$. Before defining the concept of *holistic model* for the language ${}^{Ep}\mathscr{L}_1^-$, we will first introduce the notion of *epistemic realization*.

**Definition 5.18** (*Epistemic realization*) An *epistemic realization* for the language ${}^{Ep}\mathscr{L}_1^-$ is a pair

$$\mathfrak{EpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathtt{Ep}),$$

where $\mathtt{Hol}_{\mathfrak{T}}$ is a normal holistic map for the language ${}^{Ep}\mathscr{L}_1^-$ and $\mathtt{Ep}$ is a map that associates to any pair $(\alpha, t)$ consisting of a formula $\alpha$ and of a term $t$ occurring in an epistemic connective of $\alpha$ (either $Kt$ or $Bt$ or $Ut$) an epistemic situation

$$\mathtt{Ep}(\alpha, t) = \mathfrak{EpSit}_{(\alpha,t)} = (\mathfrak{T}_\mathrm{i}, \ EpD_\mathrm{i}, \ \mathfrak{K}_\mathrm{i}, \ \mathfrak{B}_\mathrm{i}, \ \mathfrak{U}_\mathrm{i}),$$

where $\mathrm{i} = \mathtt{Hol}_{\mathfrak{T}}^{\alpha}(t)$ (in other words, $\mathrm{i}$ represents the agent that corresponds to the contextual meaning of the term $t$ in the context $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$).

Notice that generally

$$\mathfrak{T} \neq \mathfrak{T}_\mathrm{i}.$$

Thus, the truth-perspective of the agent denoted by the term $t$ (according to the map $\mathtt{Hol}_{\mathfrak{T}}$) does not necessarily coincide with the truth-perspective of the holistic map $\mathtt{Hol}_{\mathfrak{T}}$. In the next section we will see how these truth-perspective differences may cause some interesting *relativistic-like epistemic effects*.

Any epistemic realization $\mathfrak{EpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathtt{Ep})$ determines for any formula $\alpha$ a special gate tree, called the $\mathfrak{EpReal}$-*epistemic pseudo gate tree of* $\alpha$. As an example, consider the following epistemic sentence:

$$\alpha = K\mathbf{a}\neg K\mathbf{b}\mathbf{P}^1\mathbf{a}$$

(say, "Alice knows that Bob does not know that she is pretty").

We have: $\mathscr{H}^{\alpha} = \mathscr{H}^{(3)}$. The syntactical tree of $\alpha$ is:

$$Level_4^{\alpha} = (\mathbf{P}^1\mathbf{a})$$
$$Level_3^{\alpha} = (K\mathbf{b}\mathbf{P}^1\mathbf{a})$$
$$Level_2^{\alpha} = (\neg K\mathbf{b}\mathbf{P}^1\mathbf{a})$$
$$Level_1^{\alpha} = (K\mathbf{a}\neg K\mathbf{b}\mathbf{P}^1\mathbf{a})$$

Consider the two following epistemic situations (determined by $\mathfrak{EpReal}$):

$$\mathfrak{EpSit}_{(\alpha,\mathbf{a})} = (\mathfrak{T}_{\mathfrak{a}},\ EpD_{\mathfrak{a}},\ \mathfrak{K}_{\mathfrak{a}},\ \mathfrak{B}_{\mathfrak{a}},\ \mathfrak{U}_{\mathfrak{a}});$$

$$\mathfrak{EpSit}_{(\alpha,\mathbf{b})} = (\mathfrak{T}_{\mathfrak{b}},\ EpD_{\mathfrak{b}},\ \mathfrak{K}_{\mathfrak{b}},\ \mathfrak{B}_{\mathfrak{b}},\ \mathfrak{U}_{\mathfrak{b}}),$$

where $\mathfrak{a}$ is the agent (*Alice*), corresponding to the contextual meaning of the name **a** in the context $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$, while $\mathfrak{b}$ is the agent (*Bob*), corresponding to the contextual meaning of the name **b** in the context $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$.

In such a case the $\mathfrak{EpReal}$-epistemic pseudo gate tree of $\alpha$ can be naturally identified with the following sequence of operations:

$$(\mathfrak{K}^{(3)}_{\mathfrak{T}_{\mathfrak{b}}},\ {}^{\mathfrak{D}}\mathtt{NOT}^{(3)}_{\mathfrak{T}},\ \mathfrak{K}^{(3)}_{\mathfrak{T}_{\mathfrak{a}}}).$$

This procedure can be obviously generalized. For any formula $\alpha$, the choice of an epistemic realization $\mathfrak{EpReal}$ determines the $\mathfrak{EpReal}$-epistemic pseudo gate tree of $\alpha$, indicated as follows:

$$({}^{\mathfrak{D}}\mathtt{G}^{\mathfrak{EpReal}}_{\mathfrak{T}_{(h-1)}},\ \ldots,\ {}^{\mathfrak{D}}\mathtt{G}^{\mathfrak{EpReal}}_{\mathfrak{T}_{(1)}}).$$

Notice that in such a case $\mathfrak{T}_{(j)}$ and $\mathfrak{T}_{(k)}$ (where $j \neq k$ and $1 \leq j, k \leq h-1$) may be two different truth-perspectives.

Of course, the elements of epistemic pseudo gate trees are generally irreversible operations. Furthermore, unlike the case of the language $\mathscr{L}_1^-$, epistemic pseudo gate trees are not uniquely determined by the syntactical trees of the formulas under investigation. Any epistemic realization $\mathfrak{EpReal}$ chooses for any $\alpha$ a particular interpretation of the epistemic connectives occurring in $\alpha$.

Now the concept of *holistic model* for the language ${}^{Ep}\mathscr{L}_1^-$ can be defined in the expected way. Like in the case of $\mathscr{L}_1^-$, any model shall preserve the logical form of all formulas and shall assign the "right" meanings to the sentences **f** and **t**. Furthermore, any model shall interpret the epistemic connectives occurring in a given formula as convenient epistemic operations.

**Definition 5.19** (*Holistic model of* ${}^{Ep}\mathscr{L}_1^-$) A *holistic model* of ${}^{Ep}\mathscr{L}_1^-$ is an epistemic realization

$$\mathfrak{EpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathtt{Ep})$$

that satisfies the following conditions for any formula $\alpha$.

(1) Let $({}^{\mathfrak{D}}\mathtt{G}^{\mathfrak{EpReal}}_{\mathfrak{T}_{(h-1)}}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^{\mathfrak{EpReal}}_{\mathfrak{T}_{(1)}})$ be the $\mathfrak{EpReal}$-epistemic pseudo gate tree of $\alpha$ and let $1 \leq i < h$. Then,

$$\mathtt{Hol}_{\mathfrak{T}}(Level_i(\alpha)) = {}^{\mathfrak{D}}\mathtt{G}^{\mathfrak{EpReal}}_{\mathfrak{T}_{(i)}}(\mathtt{Hol}_{\mathfrak{T}_{(i+1)}}(Level_{i+1}(\alpha))).$$

In other words, the meaning of each level (different from the top level) is obtained by applying the corresponding gate (or pseudo gate) to the meaning of the level that occurs immediately above.

(2) The contextual meanings assigned by $\mathtt{Hol}_{\mathfrak{T}}$ to the false sentence **f** and to the true sentence **t** are the $\mathfrak{T}$-Falsity ${}^{\mathfrak{T}}P_0^{(1)}$ and the $\mathfrak{T}$-Truth ${}^{\mathfrak{T}}P_1^{(1)}$, respectively.

On this basis the concepts of *truth*, *validity* and *logical consequence* are defined like in the case of the language $\mathscr{L}_1^-$, *mutatis mutandis*.

It is interesting to classify some special kinds of epistemic models that satisfy particular restrictions.

**Definition 5.20** (*Special models*) Let $\mathfrak{EpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathtt{Ep})$ be a model of ${}^{Ep}\mathscr{L}_1^-$.

(1) $\mathfrak{EpReal}$ is called *harmonic* iff in all epistemic situations determined by $\mathfrak{EpReal}$ all agents have the truth-perspective $\mathfrak{T}$.

(2) $\mathfrak{EpReal}$ is called *sound* iff all epistemic situations

$$\mathfrak{EpSit}_{\mathfrak{i}} = (\mathfrak{T}_{\mathfrak{i}},\ EpD_{\mathfrak{i}},\ \mathfrak{K}_{\mathfrak{i}},\ \mathfrak{B}_{\mathfrak{i}}\ \mathfrak{U}_{\mathfrak{i}})$$

determined by $\mathfrak{EpReal}$ satisfy the following conditions:

(2.1) ${}^{\mathfrak{T}_{\mathfrak{i}}}P_0^{(1)},\ {}^{\mathfrak{T}_{\mathfrak{i}}}P_1^{(1)} \in EpD_{\mathfrak{i}}^{(1)}$;

(2.2) $\mathfrak{K}^{(1)}_{\mathfrak{T}_{\mathfrak{i}}}({}^{\mathfrak{T}_{\mathfrak{i}}}P_1^{(1)}) = {}^{\mathfrak{T}_{\mathfrak{i}}}P_1^{(1)}; \quad \mathfrak{K}^{(1)}_{\mathfrak{T}_{\mathfrak{i}}}({}^{\mathfrak{T}_{\mathfrak{i}}}P_0^{(1)}) = {}^{\mathfrak{T}_{\mathfrak{i}}}P_0^{(1)}.$

In other words, any agent $\mathfrak{i}$ has access to the Truth and to the Falsity of his/her truth-perspective, assigning to them the "right" probability-values.

(3) $\mathfrak{EpReal}$ is called *falsity-based* iff for any epistemic situation

$$\mathfrak{EpSit}_{\mathfrak{i}} = (\mathfrak{T}_{\mathfrak{i}},\ EpD_{\mathfrak{i}},\ \mathfrak{K}_{\mathfrak{i}},\ \mathfrak{B}_{\mathfrak{i}}\ \mathfrak{U}_{\mathfrak{i}})$$

determined by $\mathfrak{EpReal}$, the following condition is satisfied:

$$\rho \notin EpD_{\mathfrak{i}}^{(n)} \implies \mathfrak{K}^{(n)}_{\mathfrak{T}_{\mathfrak{i}}}\rho = \frac{1}{2^n}\,{}^{\mathfrak{T}_{\mathfrak{i}}}P_0^{(n)}$$

(thus, $\rho \notin EpD_{\mathfrak{i}}^{(n)} \implies \mathtt{p}_1^{\mathfrak{T}_i}(\mathfrak{K}^{(n)}_{\mathfrak{T}_{\mathfrak{i}}}\rho) = 0$).

(4) $\mathfrak{EpReal}$ is called *perfect* iff any agent $\mathfrak{i}$ of an epistemic situation determined by $\mathfrak{EpReal}$ has a *perfect epistemic capacity*, satisfying the following conditions:

(4.1) for any $n \geq 1$, the epistemic domain $EpD_{\mathfrak{i}}^{(n)}$ coincides with the set of all density operators of $\mathscr{H}^{(n)}$. Hence, any $\mathfrak{K}^{(n)}_{\mathfrak{T}_{\mathfrak{i}}}$ is a strong knowledge-operation;

(4.2) for any $\rho \in \mathfrak{D}(\mathscr{H}^{(n)})$, $\mathfrak{K}^{(n)}_{\mathfrak{T}_{\mathfrak{i}}}\rho = \rho$. Hence, the probability of knowing a given information coincides with the "right" probability of the information in question.

Notice that a perfect epistemic capacity does not imply *omniscience* (i.e. the capacity of *semantically deciding* any sentence). For, the *semantic excluded-middle principle* does not generally hold. Of course, both human and artificial intelligences cannot be represented as *perfect* epistemic agents: the global epistemic domain $\bigcup_n EpD^{(n)}_{\mathfrak{i}}$ of a "real mind" is unavoidably finite.

Models that are at the same time harmonic, sound and falsity-based will be called *simple*. By *simple epistemic (quantum computational) semantics* we will mean the special case of the epistemic semantics based on the assumption that all models are simple.

When $\alpha$ is valid or $\beta$ is a logical consequence of $\alpha$ in the simple semantics we will write:

$$\models^{Simple} \alpha; \qquad \alpha \models^{Simple} \beta.$$

Let us finally sum up some significant examples of epistemic arguments that are either valid or possibly violated in the epistemic quantum computational semantics.

(1) $Kt\alpha \models Ut\alpha$.
Knowing implies understanding. But not the other way around!

(2) $Kt\alpha \models Bt\alpha$.
Knowing implies believing. But not the other way around!

(3) $Kt\alpha \models^{Simple} \alpha$.
In the simple semantics, knowing a formula implies the formula itself. Of course this relation does not hold in the general epistemic semantics, where non-harmonic models may refer to different truth-perspectives of different agents.

(4) As a particular case of (3) we obtain:
$KtKt\alpha \models^{Simple} Kt\alpha$.
Knowing of knowing implies knowing. But not the other way around!

(5) $Kt_1Kt_2\alpha \models^{Simple} \alpha$.
In the simple semantics, knowing that another agent knows a given formula implies the formula in question. At the same time, we have:
$Kt_1Kt_2\alpha \not\models^{Simple} Kt_1\alpha$.
Alice might know that Bob knows a given formula, without knowing herself the formula in question!

(6) $\models^{Simple} Kt\mathbf{t}$.
Hence, there are sentences that everybody knows.

(7) $Kt(\alpha \wedge \beta) \not\models Kt\alpha$; $Kt(\alpha \wedge \beta) \not\models Kt\beta$.
Knowing a conjunction does not generally imply knowing its members.

(8) $Kt\alpha \wedge Kt\beta \not\models Kt(\alpha \wedge \beta)$.
Knowledge is not generally closed under conjunction.

(9) $\not\models_{\mathfrak{EpReal}} Kt(\alpha \wedge \neg\alpha)$, for any model $\mathfrak{EpReal}$
Contradictions are never known with certainty.

(10) In the non-simple semantics (where models are not necessarily harmonic) the following situation is possible:
$\vDash_{\mathfrak{EpReal}} K\mathbf{a}K\mathbf{bf}$.
In other words, according to *Alice*'s truth-perspective it is true that *Alice* knows that *Bob* knows *Alice*'s *Falsity*. Roughly, we might say: *Alice* knows that *Bob* is wrong, although *Bob* is not aware of being wrong!

The examples illustrated above seem to reflect pretty well some characteristic features and limitations of the real processes of acquiring information and knowledge. "Knowing" and "knowing of knowing" are sharply distinguished: in fact, from an intuitive point of view, "knowing of knowing" generally corresponds to a stronger form of knowledge that often involves a kind of "awareness". Apparently, any abstract representation of the epistemic operator "to know" as an $S4$-like *necessity-operator* $\Box$ (such that $\Box\alpha$ is logically equivalent to $\Box\Box\alpha$) is only compatible with a highly idealized concept of knowledge.[6]

Owing to the limits of epistemic domains, quantum knowledge operators are not generally closed under logical consequence. Hence, the unpleasant phenomenon of *logical omniscience* is here avoided: *Alice* might know a given sentence without knowing *all* its logical consequences. We have, in particular, that knowledge is not generally closed under logical conjunction, in accordance with what happens in the case of concrete memories both of human and of artificial intelligence. It is also admitted that an agent knows a conjunction, without knowing its members. Such a situation that might appear *prima facie* somewhat "irrational" is instead consistent with our use of natural languages: in fact, it often happens that agents understand and use correctly some *global* expressions without being able to properly understand their (meaningful) parts.

## 5.6 Physical Examples and Relativistic-Like Epistemic Effects

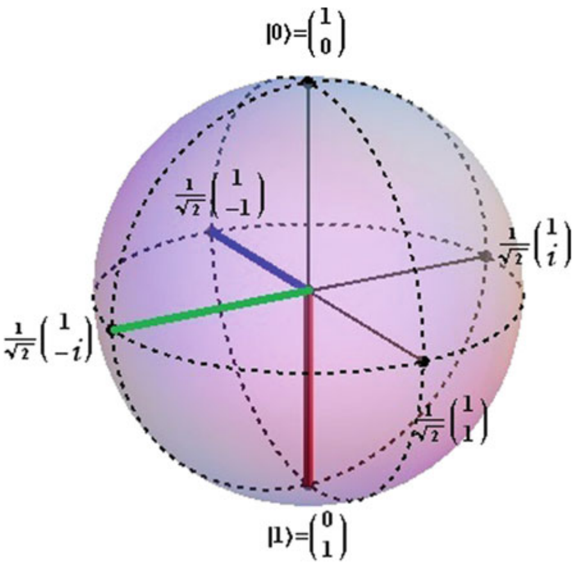
We will now illustrate some examples of knowledge-operations that may be interesting from a physical point of view. To this aim it is expedient to recall an useful representation of the set of all density operators of the Hilbert space $\mathbb{C}^2$ as vectors of the three-dimensional Bloch-sphere **BS** of radius 1 (Fig. 5.1).

For any $\rho \in \mathfrak{D}(\mathbb{C}^2)$, the corresponding *Bloch-vector* $\mathbf{v}^\rho$ is a vector of the three-dimensional real vector space $\mathbb{R}^3$ with norm at most 1, which is determined as follows:

$$\mathbf{v}^\rho = (v_1^\rho, v_2^\rho, v_3^\rho),$$

[6] It may be amusing to recall how the difference between "knowing" and "knowing of knowing" has been used as "an investigation-tool" in some detective-stories by Agatha Christie. In the novel "The ABC murders" the famous Hercule Poirot says: "I make the assumption that one-or possibly *all* of you - *knows something that they do not know they know*."

**Fig. 5.1** The Bloch-sphere



where:

$$v_1^\rho = \mathtt{tr}(\rho\,\mathtt{X}),\ \ v_2^\rho = \mathtt{tr}(\rho\,\mathtt{Y}),\ \ v_3^\rho = \mathtt{tr}(\rho\,\mathtt{Z}).$$

The operators X, Y, Z are the three *Pauli-matrices* that are defined as follows:

$$\mathtt{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \mathtt{Y} = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}; \quad \mathtt{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Conversely, for any Bloch-vector $\mathbf{v} = (v_1, v_2, v_3)$ the corresponding density operator $\rho^{\mathbf{v}}$ is determined by the following matrix:

$$\frac{1}{2}\begin{bmatrix} 1 + v_3 & v_1 - \imath v_2 \\ v_1 + \imath v_2 & 1 - v_3 \end{bmatrix}.$$

We have:

$$\rho^{(\mathbf{v}^\rho)} = \rho; \qquad \mathbf{v}^{(\rho^\mathbf{v})} = \mathbf{v}.$$

Via the Bloch-representation, any density operator $\rho$ of $\mathbb{C}^2$ can be canonically represented as a combination of four unitary operators: the identity operator $\mathtt{I}^{(1)}$ and the three Pauli-matrices. For any $\rho$ we have:

$$\rho = \frac{1}{2}(\mathtt{I}^{(1)} + v_1^\rho \mathtt{X} + v_2^\rho \mathtt{Y} + v_3^\rho \mathtt{Z}).$$

We will now introduce a class of quantum operations that have a special physical interest. Let $a, b, c$ be complex numbers such that $|a|^2 + |b|^2 + |c|^2 \leq 1$. Consider the following system of Kraus-operators[7] of $\mathbb{C}^2$:

$$\begin{aligned} E_0 &= \sqrt{1 - |a|^2 - |b|^2 - |c|^2}\, \mathtt{I}^{(1)} \\ E_1 &= |a| \mathtt{X} \\ E_2 &= |b| \mathtt{Y} \\ E_3 &= |c| \mathtt{Z} \end{aligned}$$

Define ${}^{a,b,c}\mathfrak{E}^{(1)}$ as follows for any $\rho \in \mathfrak{D}(\mathbb{C}^2)$:

$${}^{a,b,c}\mathfrak{E}^{(1)} \rho = \sum_{i=0}^{3} E_i \, \rho \, E_i^{\dagger}.$$

We have:

$${}^{a,b,c}\mathfrak{E}^{(1)} \rho = (1 - |a|^2 - |b|^2 - |c|^2)\rho + |a|^2 \mathtt{X}\rho\mathtt{X} + |b|^2 \mathtt{Y}\rho\mathtt{Y} + |c|^2 \mathtt{Z}\rho\mathtt{Z}.$$

One can prove that for any choice of $a, b, c$ (such that $|a|^2 + |b|^2 + |c|^2 \leq 1$), the map ${}^{a,b,c}\mathfrak{E}^{(1)}$ is a quantum operation of the space $\mathbb{C}^2$.

Let us now refer to the Bloch-sphere. Any map ${}^{a,b,c}\mathfrak{E}^{(1)}$ induces the following vector-transformation:

$$(v_1, v_2, v_3) \;\; \mapsto \;\; ((1 - 2|b|^2 - 2|c|^2)\, v_1, \;(1 - 2|a|^2 - 2|c|^2)\, v_2, \;(1 - 2|a|^2 - 2|b|^2)\, v_3)$$

(for any vector $(v_1, v_2, v_3)$ of the sphere). Hence, the sphere is deformed into an ellipsoid centered at the origin.

For particular choices of $a$, $b$ and $c$, one obtains some special cases of quantum operations.

- For $a = b = c = 0$, one obtains the identity operator.
- For $b = c = 0$, one obtains the *bit-flip quantum operation* ${}^{a}\mathfrak{BF}^{(1)}$ that flips with probability $|a|^2$ the two canonical bits (${}^{\mathtt{I}}P_0^{(1)}$ and ${}^{\mathtt{I}}P_1^{(1)}$) as follows:

  $${}^{\mathtt{I}}P_0^{(1)} \mapsto (1 - |a|^2)\, {}^{\mathtt{I}}P_0^{(1)} + (|a|^2)\, {}^{\mathtt{I}}P_1^{(1)}; \quad {}^{\mathtt{I}}P_1^{(1)} \mapsto (1 - |a|^2)\, {}^{\mathtt{I}}P_1^{(1)} + (|a|^2)\, {}^{\mathtt{I}}P_0^{(1)}.$$

  The sphere is mapped into an ellipsoid with **x** as symmetry-axis (see Fig. 5.2).
- For $a = c = 0$, one obtains the *bit-phase-flip quantum operation* ${}^{b}\mathfrak{BPF}^{(1)}$ that flips both bits and phase with probability $|b|^2$. The sphere is mapped into an ellipsoid with **y** as symmetry-axis.

[7] The concepts of *quantum operation* and *system of Kraus-operators* have been introduced in Sect. 1.4.

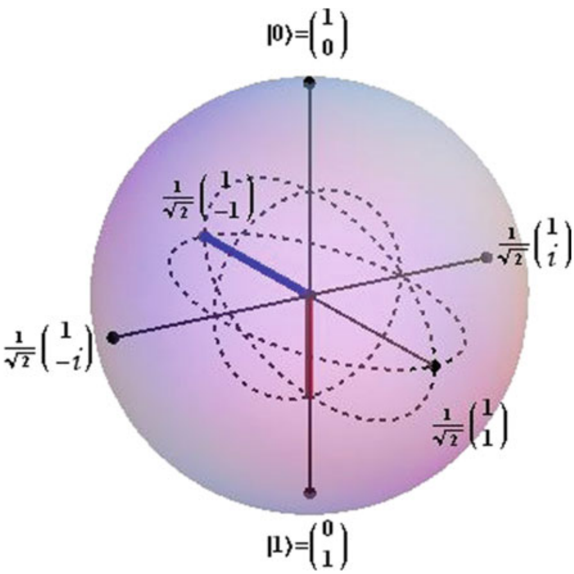



**Fig. 5.2** The bit-flip quantum operation

- For $a = b = 0$, one obtains the *phase-flip quantum operation* ${}^{c}\mathfrak{P}\mathfrak{F}^{(1)}$ that flips the phase with probability $|c|^2$. The sphere is mapped into an ellipsoid with **z** as symmetry-axis.
- For $|a|^2 = |b|^2 = |c|^2 = \frac{p}{4}$ (with $p \leq 1$), one obtains the *depolarizing quantum operation* ${}^{p}\mathfrak{D}^{(1)}$. If $p = 1$, the polarization along any direction is equal to 0. The sphere is contracted by a factor $1 - p$ and the center of the sphere is a fixed point.

The quantum operations considered above have been defined with respect to the canonical truth-perspective $\mathtt{I}$. However, as expected, they can be naturally transposed to any truth-perspective $\mathfrak{T}$. Given $\mathfrak{E}^{(1)}$ such that

$$\mathfrak{E}^{(1)}\rho = \sum_{i=0}^{3} E_i\, \rho\, E_i^{\dagger},$$

the twin-quantum operation $\mathfrak{E}^{(1)}_{\mathfrak{T}}$ of $\mathfrak{E}^{(1)}$ can be defined as follows:

$$\mathfrak{E}^{(1)}_{\mathfrak{T}}\rho := \sum_{i} \mathfrak{T} E_i \mathfrak{T}^{\dagger}\, \rho\, \mathfrak{T} E_i^{\dagger} \mathfrak{T}^{\dagger}.$$

So far we have considered quantum operations of the space $\mathbb{C}^2$. But, of course, any operation $\mathfrak{E}^{(1)}_{\mathfrak{T}}$ (defined on $\mathbb{C}^2$) can be canonically extended to an operation $\mathfrak{E}^{(n)}_{\mathfrak{T}}$ defined on the space $\mathscr{H}^{(n)}$ (for any $n > 1$). Consider a density operator $\rho$ of $\mathscr{H}^{(n)}$ and the reduced state $Red^{(2)}_{[n-1,1]}(\rho)$ (which describes the $n$th subsystem of the composite system described by $\rho$). We have:

$$\mathtt{p}_1^{\mathfrak{T}}(\rho) = \mathtt{tr}(Red^{(2)}_{[n-1,1]}(\rho)\, {}^{\mathfrak{T}}P_1^{(1)}).$$

Thus, the $\mathfrak{T}$-probability of $\rho$ only depends on the $\mathfrak{T}$-probability of the reduced state that describes the $n$th subsystem. On this basis, it is reasonable to define $\mathfrak{E}_{\mathfrak{T}}^{(n)}$ as follows:

$$\mathfrak{E}_{\mathfrak{T}}^{(n)} = \mathtt{I}^{(n-1)} \otimes \mathfrak{E}_{\mathfrak{T}}^{(1)}.$$

Notice that, generally, a quantum operation does not represent a knowledge-operation. We may have, for instance, for some density operators $\rho$:

$$\mathtt{p}_1^{\mathtt{I}}({}^{a}\mathfrak{BF}^{(1)}\rho) \not\leq \mathtt{p}_1^{\mathtt{I}}(\rho),$$

against the definition of knowledge-operation (in the case where $\rho$ is supposed to belong to the epistemic domain of ${}^{a}\mathfrak{BF}^{(1)}$). At the same time, by convenient choices of the epistemic domains, quantum operations can be easily transformed into knowledge-operations. An interesting example is represented by the class of all *bit-flip knowledge-operations*.

**Definition 5.21** (*A bit-flip knowledge-operation* ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$) Consider a bit-flip operation ${}^{a}\mathfrak{BF}_{\mathfrak{T}}^{(n)}$ (with $a \neq 0$). Define ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ as follows:

(1) $EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}) \subseteq D = \{\rho \in \mathfrak{D}(\mathscr{H}^{(n)}) \,:\, \mathtt{p}_1^{\mathfrak{T}}(\rho) \geq \frac{1}{2}\}$.
In other words, an agent (whose knowledge-operation is ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$) has only access to pieces of information that are not "too far from the truth".
(2) $\rho \in EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}) \;\Rightarrow\; {}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho = {}^{a}\mathfrak{BF}_{\mathfrak{T}}^{(n)}\rho$.
(3) $\rho \notin EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}) \;\Rightarrow\; {}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho = \frac{1}{2^n}\, {}^{\mathfrak{T}}P_0^{(n)}$.

**Theorem 5.6**

*(1) Any ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ is a knowledge-operation. In particular, ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ is a non-trivial knowledge-operation, if there exists at least one $\rho \in EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)})$ such that $p_1^{\mathfrak{T}}(\rho) > \frac{1}{2}$;*
*(2) the set $D$ is the maximal set such that the corresponding ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ is a knowledge-operation;*
*(3) let $|a|^2 \leq \frac{1}{2}$ and let $EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}) = D$. The following closure property holds: for any $\rho \in D$, ${}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho \in D$.*

*Proof* (1)–(2) Suppose that $\rho \in EpD({}^{a}\mathfrak{KBF}_{\mathfrak{T}}^{(n)}) \subseteq D$ and let us represent the density operator $\mathfrak{T}^{\dagger} Red^{(2)}_{[n-1,1]}(\rho)\mathfrak{T}$ as

$$\frac{1}{2}(\mathtt{I}^{(1)} + v_1\mathtt{X} + v_2\mathtt{Y} + v_3\mathtt{Z}).$$

We have:

- $\mathtt{p}_1^{\mathfrak{T}}({}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho) = \mathtt{tr}({}^{\mathfrak{T}}P_1^{(n)}\,{}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho) =$
  $\mathtt{tr}(\mathfrak{T}\,{}^{\mathtt{I}}P_1^{(1)}\mathfrak{T}^{\dagger}\sum_i \mathfrak{T}E_i\mathfrak{T}^{\dagger}\, Red_{[n-1,1]}^{(2)}(\rho)\mathfrak{T}E_i^{\dagger}\mathfrak{T}^{\dagger}) =$
  $\mathtt{tr}({}^{\mathtt{I}}P_1^{(1)}\sum_i E_i\mathfrak{T}^{\dagger}\, Red_{[n-1,1]}^{(2)}(\rho)\,\mathfrak{T}E_i^{\dagger}) = \frac{1-(1-2|a|^2)v_3}{2}$.
- $\mathtt{p}_1^{\mathfrak{T}}(\rho) = \mathtt{tr}({}^{\mathfrak{T}}P_1^{(n)}\rho) = \mathtt{tr}(\mathfrak{T}\,{}^{\mathtt{I}}P_1^{(1)}\mathfrak{T}^{\dagger} Red_{[n-1,1]}^{(2)}(\rho)) = \frac{1-v_3}{2}$.

Hence, $\mathtt{p}_1^{\mathfrak{T}}({}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho) \leq \mathtt{p}_1^{\mathfrak{T}}(\rho) \Leftrightarrow (1-2|a|^2)v_3 \geq v_3 \Leftrightarrow v_3 \in [-1,0] \Leftrightarrow \mathtt{p}_1^{\mathfrak{T}}(\rho) \geq \frac{1}{2}$.
Thus, ${}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ is a knowledge-operation and the set $D$ is the maximal set such that the corresponding ${}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}$ is a knowledge-operation.

(3) $\mathtt{p}_1^{\mathfrak{T}}({}^a\mathfrak{KBF}_{\mathfrak{T}}^{(n)}\rho) = \frac{1-(1-2|a|^2)v_3}{2} \geq \frac{1}{2}$, since $|a|^2 \leq \frac{1}{2}$ and $v_3 \in [-1,0]$.

□

In a similar way one can define knowledge-operations that correspond to the phase-flip operation, the bit-phase-flip operation and the depolarizing operation.

Truth-perspectives are, in a sense, similar to different reference-frames in relativity theory. Accordingly, one could try and apply a "relativistic" way of thinking in order to describe how a given agent can "see" the logical behavior of another agent.

As an example let us refer to two agents *Alice* and *Bob*, whose truth-perspectives are $\mathfrak{T}_{Alice}$ and $\mathfrak{T}_{Bob}$, respectively. Let $\{|1_{Alice}\rangle, |0_{Alice}\rangle\}$ and $\{|1_{Bob}\rangle, |0_{Bob}\rangle\}$ represent the systems of truth-values of our two agents. Furthermore, for any canonical gate ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ (defined with respect to the canonical truth-perspective $\mathtt{I}$), let ${}^{\mathfrak{D}}\mathtt{G}_{Alice}^{(n)}$ and ${}^{\mathfrak{D}}\mathtt{G}_{Bob}^{(n)}$ represent the corresponding *twin-gates* for *Alice* and for *Bob*, respectively.

We have:

$$ {}^{\mathfrak{D}}\mathtt{G}_{Alice}^{(n)} = {}^{\mathfrak{D}}(\mathfrak{T}_{Alice}^{(n)}\mathtt{G}^{(n)}\mathfrak{T}_{Alice}^{(n)\dagger}); \quad {}^{\mathfrak{D}}\mathtt{G}_{Bob}^{(n)} = {}^{\mathfrak{D}}(\mathfrak{T}_{Bob}^{(n)}\mathtt{G}^{(n)}\mathfrak{T}_{Bob}^{(n)\dagger}). $$

We will adopt the following conventional terminology.

- When $|1_{Bob}\rangle = a_0|0_{Alice}\rangle + a_1|1_{Alice}\rangle$, we will say that Alice *sees* that Bob's *Truth* is $a_0|0_{Alice}\rangle + a_1|1_{Alice}\rangle$. In a similar way, for Bob's *Falsity*.
- When ${}^{\mathfrak{D}}\mathtt{G}_{Alice}^{(n)} = {}^{\mathfrak{D}}(\mathfrak{T}_{Alice}^{(n)}\mathtt{G}^{(n)}\mathfrak{T}_{Alice}^{(n)\dagger})$ and ${}^{\mathfrak{D}}\mathtt{G}_{Bob}^{(n)} = {}^{\mathfrak{D}}(\mathfrak{T}_{Bob}^{(n)}\mathtt{G}^{(n)}\mathfrak{T}_{Bob}^{(n)\dagger}) = {}^{\mathfrak{D}}\mathtt{G}_{1_{Alice}}^{(n)}$ (where ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ and ${}^{\mathfrak{D}}\mathtt{G}_1^{(n)}$ are canonical gates), we will say that *Alice sees Bob using the gate* ${}^{\mathfrak{D}}\mathtt{G}_{1_{Alice}}^{(n)}$ *in place of her gate* ${}^{\mathfrak{D}}\mathtt{G}_{Alice}^{(n)}$.
- When ${}^{\mathfrak{D}}\mathtt{G}_{Alice}^{(n)} = {}^{\mathfrak{D}}\mathtt{G}_{Bob}^{(n)}$ we will say that Alice and Bob *see and use the same gate*, which represents (in their truth-perspective) the canonical gate ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$.

On this basis, one can conclude that, generally, *Alice sees* a kind of "deformation" in *Bob*'s logical behavior. As an example, suppose that *Alice* has the canonical truth-perspective (i.e. $\mathfrak{T}_{Alice} = \mathtt{I}^{(1)}$), while *Bob*'s truth-perspective is the Hadamard-operator (i.e. $\mathfrak{T}_{Bob} = \sqrt{\mathtt{I}}^{(1)}$). Accordingly, the truth-value systems of *Alice* and of *Bob* are the following:

- $\{|1_{Alice}\rangle, |0_{Alice}\rangle\} = \{|1\rangle, |0\rangle\}$;
- $\{|1_{Bob}\rangle, |0_{Bob}\rangle\} = \left\{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right\}$.

In such a case, *Alice* will *see* a quite strange behavior in *Bob*'s use of the logical connective *negation*. Since ${}^{\mathfrak{D}}\mathtt{NOT}^{(1)}_{Bob} = {}^{\mathfrak{D}}(\sqrt{\mathtt{I}}^{(1)}\,\mathtt{NOT}^{(1)}\sqrt{\mathtt{I}}^{(1)\dagger})$, we will obtain, for instance, that:

$$^{\mathfrak{D}}\mathtt{NOT}^{(1)}_{Bob}\ {}^{\mathtt{I}}P^{(1)}_1 = {}^{\mathtt{I}}P^{(1)}_1 = P^{(1)}_{\frac{1}{\sqrt{2}}(|0_{Bob}\rangle - |1_{Bob}\rangle)}.$$

In other words, *Alice sees* that *Bob*'s negation of her *Truth* is her *Truth* itself, which represents instead an intermediate truth-value for *Bob*.

We can also consider a third agent *EVE* whose truth-perspective is the following:

$$\mathfrak{T}_{Eve} = \begin{bmatrix} \cos(\frac{\pi}{8}) & \sin(\frac{\pi}{8}) \\ -\imath\sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{bmatrix}.$$

In such a case, *Alice* will *see Eve* using the Hadamard-gate in place of her negation, i.e.,

$$^{\mathfrak{D}}\mathtt{NOT}^{(1)}_{Eve} = {}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(1)}_{Alice}.$$

As expected, generally, different agents with different truth-perspectives will see and use different gates. An interesting question is the following: can different agents (with different truth-perspectives) *see and use* the same gate corresponding to a given canonical gate? The following theorem gives a positive answer to this question, in the case of same special gates.

**Theorem 5.7** *Let* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$ *be one of the following canonical gates: the negation* ${}^{\mathfrak{D}}\mathtt{NOT}^{(n)}$, *the Hadamard-gate* ${}^{\mathfrak{D}}\sqrt{\mathtt{I}}^{(n)}$.

*(1) There is an infinite set of agents such that for any* $\mathfrak{i}$ *and* $\mathfrak{j}$ *belonging to this set:*

*(1.1)* $\mathfrak{i}$ *and* $\mathfrak{j}$ see and use *the same gate corresponding to the canonical gate* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$*;*

*(1.2) if* $\mathfrak{i} \neq \mathfrak{j}$*, then* $\mathfrak{T}_\mathfrak{i}$ *and* $\mathfrak{T}_\mathfrak{j}$ *are not probabilistically equivalent (in other words,* $\mathtt{p}_1^{\mathfrak{T}_\mathfrak{i}}(\rho) \neq \mathtt{p}_1^{\mathfrak{T}_\mathfrak{j}}(\rho)$*, for some* $\rho$*).*

*(2) There is an infinite set of agents (with different truth-perspectives* $\mathfrak{T}_\mathfrak{i}$*) who* see and use *different gates* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}_\mathfrak{i}}$*, all different from the canonical gate* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}$*. In other words, for any* $\mathfrak{i}$ *and* $\mathfrak{j}$ *belonging to this set:*

*(2.1) if* $\mathfrak{i} \neq \mathfrak{j}$*, then* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}_\mathfrak{i}} \neq {}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}_\mathfrak{j}}$*;*

*(2.2)* ${}^{\mathfrak{D}}\mathtt{G}^{(n)}_{\mathfrak{T}_\mathfrak{i}} \neq {}^{\mathfrak{D}}\mathtt{G}^{(n)}$.

*Proof* (1) Consider the set of truth-perspectives having the following form:

$$\mathfrak{T}(\theta) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -\imath \sin(\frac{\theta}{2}) \\ -\imath \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}.$$

There are infinitely many $\theta \in [0, 2\pi)$ such that:

(1.1) ${}^{\mathfrak{D}}\mathrm{G}^{(n)}_{\mathfrak{T}(\theta)} = {}^{\mathfrak{D}}\mathrm{G}^{(n)}$.
(1.2) If $\theta \neq \theta'$, then $\mathfrak{T}(\theta)$ and $\mathfrak{T}(\theta')$ are not probabilistically equivalent.

(2) Consider the set of truth-perspectives having the following form:

$$\mathfrak{T}'(\theta) = \begin{bmatrix} \cos(\frac{\theta}{2}) - \frac{\imath}{\sqrt{2}} \sin(\frac{\theta}{2}) & -\frac{\imath}{\sqrt{2}} \sin(\frac{\theta}{2}) \\ -\frac{\imath}{\sqrt{2}} \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) + \frac{\imath}{\sqrt{2}} \sin(\frac{\theta}{2}) \end{bmatrix}.$$

There are infinitely many $\theta \in (0, 2\pi)$ such that:

(2.1) if $\theta \neq \theta'$, then ${}^{\mathfrak{D}}\mathrm{G}^{(n)}_{\mathfrak{T}(\theta)} \neq {}^{\mathfrak{D}}\mathrm{G}^{(n)}_{\mathfrak{T}(\theta')}$;
(2.2) ${}^{\mathfrak{D}}\mathrm{G}^{(n)}_{\mathfrak{T}(\theta)} \neq {}^{\mathfrak{D}}\mathrm{G}^{(n)}$.

□

## 5.7 Quantifiers as Quantum Maps

Now we want to extend our semantics to the full first-order language $\mathscr{L}_1$. As is well known, in most semantic approaches the interpretation of the universal quantifier $\forall$ generally involves an infinitary procedure that cannot be represented as a finite computational step.

What are the intuitive reasons that induce us to assert the truth of a universal sentence (say, "All humans are mortal", "All neutrinos have a non-null mass",….)? In the happiest situations we can base our assertion on a theoretical proof (which generally gives rise to a kind of "by-pass"). In other situations we may refer to an empirical evidence or to an inductive extrapolation. Sometimes we are simply proposing a conjecture or even an act of faith.

Consider the following simple example of a universal sentence:

$$\alpha = \forall x \mathbf{P}^1 x.$$

We have: $AtStr(\alpha) = (3)$; $\mathscr{H}^{\alpha} = \mathscr{H}^{(3)}$.

The syntactical tree of $\alpha$ is:

$$Level_2^\alpha = (\mathbf{P}^1 x)$$
$$Level_1^\alpha = (\forall x \mathbf{P}^1 x)$$

Once chosen a truth-perspective $\mathfrak{T}$, is it possible to obtain an appropriate $\mathfrak{T}$-gate tree for $\alpha$? Any holistic map $\mathtt{Hol}_\mathfrak{T}$ will assign a density operator to the top level of the syntactical tree of $\alpha$:

$$\mathtt{Hol}_\mathfrak{T} : \ (\mathbf{P}^1 x) \ \mapsto \ \rho \in \mathfrak{D}(\mathscr{H}^{(3)}).$$

Hence, we shall look for an operation ${}^\forall\mathfrak{Q}_\mathfrak{T}$ (which is defined on $\mathscr{H}^{(3)}$ and depends on $\mathfrak{T}$) such that:

$$\mathtt{Hol}_\mathfrak{T}((\forall x \mathbf{P}^1 x)) = {}^\forall\mathfrak{Q}_\mathfrak{T}\rho.$$

A very reasonable condition that should be required seems to be the following:

$$\mathtt{p}_1^\mathfrak{T}({}^\forall\mathfrak{Q}_\mathfrak{T}\rho) \ \leq \ \mathtt{p}_1^\mathfrak{T}(\rho).$$

Semantically, this condition is important because it is connected with the validity of the *Dictum de omni-principle* ( $\forall x \mathbf{P}^1 x \ \models \ \mathbf{P}^1 x$).

Interestingly enough, one is dealing with a requirement that also characterizes knowledge-operations. As we have seen, by definition of *knowledge-operation*, for any $\rho \in EpD(\mathfrak{K}_\mathfrak{T}^{(n)})$ we have:

$$\mathtt{p}_1^\mathfrak{T}(\mathfrak{K}_\mathfrak{T}^{(n)}\rho) \leq \mathtt{p}_1^\mathfrak{T}(\rho).$$

And we already know that knowledge-operations cannot be generally represented as unitary operations (by Theorem 5.5). As happens in the case of epistemic operators, quantifiers also can be interpreted as special examples of operations that are generally irreversible. Unlike logical connectives, the use of quantifiers seems to involve a kind of theoretic "jumps", which are quite similar to what happens in the case of quantum measurement-phenomena.

Of course, not all universal formulas are so simple as $\forall x \mathbf{P}^1 x$. Consider, for instance, the following sentence:

$$\alpha = \forall x(\mathbf{P}^1 x \wedge \mathbf{P}^2 \mathbf{a} x) = \forall x(\mathsf{T}(\mathbf{P}^1 x, \mathbf{P}^2 \mathbf{a} x, \mathbf{f}))$$

(say, *All are nice and Alice likes them*).

We have: $AtStr(\alpha) = (3, 4, 1)$; $\mathscr{H}^\alpha = \mathscr{H}^{(3)} \otimes \mathscr{H}^{(4)} \otimes \mathscr{H}^{(1)} = \mathscr{H}^{(8)}$.

Here $\forall$ binds the variable $x$ in two different occurrences of $x$ in two different subformulas of $\alpha$. How can such syntactical features be reflected at a semantic level? Fortunately (unlike classical semantics), the quantum computational semantics has an *intensional* character that allows us to "preserve the memory" of the linguistic complexity of all formulas.

In the case of the sentence $\alpha = \forall x(\intercal(\mathbf{P}^1 x, \mathbf{P}^2 \mathbf{a}x, \mathbf{f}))$, the behavior of the quantifier $\forall$ can be associated to a syntactical configuration, formally described by the following conventional notation:

$$(1[1], 2[2], (3, 4, 1)).$$

The interpretation of (1[1], 2[2], (3, 4, 1)) is the following: $\forall$ binds the first variable of the first atomic subformula occurring in $\alpha$ and the second variable of the second atomic subformula occurring in $\alpha$, while (3, 4, 1) is the atomic structure of $\alpha$.

This notation can be naturally generalized. Any universal formula

$$\alpha = \forall x \delta$$

can be associated to a syntactical configuration (called *quantifier-configuration*) that will be represented as follows:

$$qconf^\alpha = (m_1[j_1^{m_1}, \ldots, j_u^{m_1}], \ldots, m_r[j_1^{m_r}, \ldots, j_v^{m_r}], (n_1, \ldots, n_k)),$$

where: $r \leq At(\alpha) = n_1 + \cdots + n_k$.

The interpretation of $qconf^\alpha$ is the expected one: $\forall$ binds the $j_1^{m_1}$th variable of the $m_1$th atomic subformula occurring in $\alpha$, ..., the $j_u^{m_1}$th variable of the $m_1$th atomic subformula occurring in $\alpha$, .... , the $j_1^{m_r}$th variable of the $m_r$th atomic subformula occurring in $\alpha$, ..., the $j_v^{m_r}$th variable of the $m_r$th atomic subformula occurring in $\alpha$; while $(n_1, \ldots, n_k)$ is the atomic structure of $\alpha$.

Of course, different formulas may have the same quantifier configuration $qconf$. Since any quantifier configuration $qconf$ refers to a particular atomic structure, it turns out that $qconf$ determines the semantic space $\mathcal{H}_{qconf}$ of all formulas whose quantifier-configuration is $qconf$.

On this basis, we can now introduce the notions of $\mathfrak{T}$-*quantifier map* and of *first-order epistemic realization* for the language $\mathcal{L}_1$.

**Definition 5.22** ($\mathfrak{T}$-*Quantifier map*) A $\mathfrak{T}$-*quantifier map* is a map $\mathfrak{Q}_\mathfrak{T}$ that associates to any quantifier-configuration $qconf$ an operation $\mathfrak{Q}_\mathfrak{T}(qconf)$, defined on the space $\mathcal{H}_{qconf}$. The following condition is required for any density operator $\rho$ of $\mathcal{H}_{qconf}$:

$$\mathtt{p}_1^\mathfrak{T}([\mathfrak{Q}_\mathfrak{T}(qconf)]\rho) \leq \mathtt{p}_1^\mathfrak{T}(\rho).$$

**Definition 5.23** (*First-order epistemic realization*) A *first-order epistemic realization* for the language $\mathcal{L}_1$ is a triplet

$$\mathfrak{FEpReal} = (\mathtt{Hol}_\mathfrak{T}, \mathfrak{EpReal}, \mathfrak{Q}_\mathfrak{T}),$$

where:

- $\mathtt{Hol}_\mathfrak{T}$ is a holistic map for the language $\mathcal{L}_1$;
- $\mathfrak{EpReal} = (\mathtt{Hol}_\mathfrak{T}, \mathtt{Ep})$ is an epistemic realization for the language ${}^{Ep}\mathcal{L}_1^-$;

- $\mathfrak{Q}_{\mathfrak{T}}$ is a quantifier map for the language $\mathscr{L}_1$.

As happens for the language ${}^{Ep}\mathscr{L}_1^-$, any first-order epistemic realization

$$\mathfrak{FEpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathfrak{EpReal}, \mathfrak{Q}_{\mathfrak{T}}),$$

determines for any formula $\alpha$ a special gate tree, called the $\mathfrak{FEpReal}$-*first-order epistemic pseudo gate tree of* $\alpha$. As an example, consider the sentence:

$$\alpha = \neg\forall x \mathbf{P}^1 x.$$

The syntactical tree of $\alpha$ is:

$$\begin{aligned} Level_3^\alpha &= (\mathbf{P}^1 x) \\ Level_2^\alpha &= (\forall x \mathbf{P}^1 x) \\ Level_1^\alpha &= (\neg\forall x \mathbf{P}^1 x) \end{aligned}$$

Accordingly, the $\mathfrak{FEpReal}$-first-order epistemic pseudo gate tree of $\alpha$ can be naturally identified with the following pseudo-gate sequence:

$$(\mathfrak{Q}_{\mathfrak{T}}(qconf^{\forall x \mathbf{P}^1 x}),\ {}^{\mathfrak{D}}\mathtt{NOT}_{\mathfrak{T}}^{(3)}).$$

This procedure can be generalized to any formula $\alpha$.

On this basis, we can now define the concept of *holistic model* for the language $\mathscr{L}_1$.

**Definition 5.24** (*Holistic model of* $\mathscr{L}_1$) A *holistic model* of $\mathscr{L}_1$ is a first-order epistemic realization

$$\mathfrak{FEpReal} = (\mathtt{Hol}_{\mathfrak{T}}, \mathfrak{EpReal}, \mathfrak{Q}_{\mathfrak{T}})$$

that satisfies the following conditions for any formula $\alpha$.

(1) Let $({}^{\mathfrak{D}}\mathtt{G}_{\mathfrak{T}_{(h-1)}}^{\mathfrak{FEpReal}}, \ldots, {}^{\mathfrak{D}}\mathtt{G}_{\mathfrak{T}_{(1)}}^{\mathfrak{FEpReal}})$ be the $\mathfrak{FEpReal}$-first-order epistemic pseudo gate tree of $\alpha$ and let $1 \leq i < h$. Then,

$$\mathtt{Hol}_{\mathfrak{T}}(Level_i(\alpha)) = {}^{\mathfrak{D}}\mathtt{G}_{\mathfrak{T}_{(i)}}^{\mathfrak{FEpReal}}(\mathtt{Hol}_{\mathfrak{T}_{(i+1)}}(Level_{i+1}(\alpha))).$$

The meaning of each level (different from the top level) is obtained by applying the corresponding gate (or pseudo-gate) to the meaning of the level that occurs immediately above.

(2) The contextual meanings assigned by $\mathtt{Hol}_{\mathfrak{T}}$ to the false sentence $\mathbf{f}$ and to the true sentence $\mathbf{t}$ are the $\mathfrak{T}$-Falsity ${}^{\mathfrak{T}}P_0^{(1)}$ and the $\mathfrak{T}$-Truth ${}^{\mathfrak{T}}P_1^{(1)}$, respectively.

(3) *Contextual Dictum de omni*
Suppose that $\forall x\beta(x)$ and $\beta(t_1) \wedge \ldots \wedge \beta(t_n)$ are both subformulas of $\alpha$. Then,

$$\mathtt{p}_1^{\mathfrak{T}}(\mathtt{Hol}_{\mathfrak{T}}^{\alpha}(\forall x\beta(x))) \leq \mathtt{p}_1^{\mathfrak{T}}(\mathtt{Hol}_{\mathfrak{T}}^{\alpha}(\beta(t_1)\wedge\ldots\wedge\beta(t_n))).$$

The concepts[8] of *truth*, *validity* and *logical consequence* for the language $\mathscr{L}_1$ can be now defined like in the case of ${}^{Ep}\mathscr{L}_1^-$, *mutatis mutandis*.

It is worth-while noticing that, unlike most first-order semantic approaches, these quantum models do not refer to *domains of individuals* dealt with as closed sets (in a classical sense). Generally, any context $\gamma$ may contain a finite number of individual terms for which any model provides contextual meanings. At the same time, the interpretation of a universal formula does not require "ideal tests" that should be performed on *all* elements of a hypothetical domain (which might be highly indeterminate). In a sense, we could say that the *universe of discourse* associated to a given holistic model behaves here as a kind of *open set*. This way of thinking seems to be in agreement with a number of concrete semantic phenomena, where domains of individuals cannot be precisely determined in an extensional way. In fact, many universal sentences that are currently asserted either in common-life contexts or in scientific theories (say, "All teenagers like danger", "All photons are bosons") do not generally refer to closed domains. Such situations, however, do not prevent a correct use of the universal quantifier.

## References

1. Baltag, A., Smets, S.: Complete axiomatizations for quantum actions. Int. J. Theor. Phys. **44**(12), 2267–2282 (2005)
2. Baltag, A., Smets, S.: LQP: the dynamic logic of quantum information. Math. Struct. Comput. Sci. **16**(3), 491–525 (2006)
3. Baltag, A., Smets, S.: Correlated knowledge, an epistemic-logic view on quantum entanglement. Int. J. Theor. Phys. **49**(12), 3005–3021 (2010)
4. Beltrametti, E., Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: Epistemic quantum computational structures in a Hilbert-space environment. Fundam. Inform. **115**(1), 1–14 (2012)
5. Beltrametti, E., Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: A quantum computational semantics for epistemic logical operators. Part I: epistemic structures. Int. J. Theor. Phys. **53** (10), 3279-3292 (2014)
6. Beltrametti, E., Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: A quantum computational semantics for epistemic logical operators. Part II: semantics. Int. J. Theor. Phys. **53** (10), 3293-3307 (2014)
7. Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: A first-order epistemic quantum computational semantics with relativistic-like epistemic effects. Fuzzy Sets Syst. **298**, 69–90 (2016)
8. Sergioli, G., Leporini, R.: Quantum approach to epistemic semantics. Soft Comput. **21**(6), 1381–1390 (2017)

[8]We recall that the connective conjunction of holistic quantum computational logics does not generally satisfy associativity. Accordingly, we have assumed that any expression $\beta_1 \wedge \ldots \wedge \beta_n$ is here used as a metalinguistic abbreviation for any possible bracket-configuration in a multiple conjunction whose members are the elements of the sequence $(\beta_1, \ldots, \beta_n)$ (see Sect. 4.4).

# Chapter 6
# From Qubits to Qudits

## 6.1 Introduction

All quantum logics (from Birkhoff and von Neumann's quantum logic to the more recent quantum computational logics) are characterized by forms of semantics that are intrinsically many-valued. Against the classical *tertium non datur*-principle quantum logical sentences are not necessarily either *true* or *false*. Such a semantic indetermination is a natural consequence of the characteristic quantum uncertainties. As we have seen (in Chaps. 4 and 5) any interpretation of a quantum computational language acts on two different levels: the first level refers to pieces of quantum information (represented by density operators of convenient Hilbert spaces), while the second level refers to probability-values (real numbers in the [0, 1]-interval). Consider a model $\mathtt{Hol}_{\mathfrak{T}}$ and a sentence $\alpha$. The density operator $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$ (assigned by $\mathtt{Hol}_{\mathfrak{T}}$ to $\alpha$) represents a kind of *intensional meaning* that preserves the linguistic complexity of $\alpha$. At the same time, $\mathtt{Hol}_{\mathfrak{T}}(\alpha)$ determines the probability-value of $\alpha$ (under the interpretation $\mathtt{Hol}_{\mathfrak{T}}$), which can be regarded as a kind of *extensional meaning*. As happens in classical semantics, the *intension* determines the corresponding *extension*, but not the other way around. However, unlike classical semantics, the intensional meanings of quantum computational logics represent concepts that may be *vague and ambiguous*, while extensional meanings are not necessarily dichotomic. Furthermore, both intensional and extensional meanings may violate the *compositionality-principle*, against Frege's basic assumption.

In spite of its strongly non-classical features, quantum computational semantics includes a subtheory that behaves classically, both from a logical and from a computational point of view. As we have seen in Chap. 4, the holistic quantum computational semantics has a special fragment where pieces of information are represented by classical bits and registers, while the basic Boolean functions are represented as reversible gates. Of course, in this framework, the cardinality of the set of bits is determined by the dimension of the Hilbert space $\mathbb{C}^2$. One can wonder whether such a restriction is really useful for the aims of quantum computation. A natural "many-valued generalization" of the classical part of quantum computation might assume any $\mathbb{C}^d$ (where $d \geq 2$) as a basic Hilbert space. In this way, *bits* might be generalized to *dits*, represented by the elements of the canonical orthonormal basis of a space



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_6

$\mathbb{C}^d$. Interestingly enough, such a generalization can give rise to some useful physical implementations.

## 6.2 Qudit-Spaces

Consider a Hilbert space $\mathbb{C}^d$, where $d \geq 2$. The elements of the canonical basis of $\mathbb{C}^d$ can be regarded as different truth-values, which can be conventionally indicated in the following way:

$$\begin{aligned}
&|0\rangle = |\tfrac{0}{d-1}\rangle = (1, 0, \ldots, 0)\\
&|\tfrac{1}{d-1}\rangle = (0, 1, 0, \ldots, 0)\\
&|\tfrac{2}{d-1}\rangle = (0, 0, 1, 0, \ldots, 0)\\
&\vdots\\
&|1\rangle = |\tfrac{d-1}{d-1}\rangle = (0, \ldots, 0, 1).
\end{aligned}$$

While $|0\rangle$ and $|1\rangle$ represent the truth-values *Falsity* and *Truth*, all other basis-elements correspond to *intermediate* truth-values. For instance, the truth-values of the space $\mathbb{C}^3$ (whose unit-vectors are also called *qutrits*) will be:

$$\begin{aligned}
&|0\rangle = |\tfrac{0}{2}\rangle = (1, 0, 0)\\
&|\tfrac{1}{2}\rangle = (0, 1, 0)\\
&|1\rangle = |\tfrac{2}{2}\rangle = (0, 0, 1).
\end{aligned}$$

Generally, a *qudit-space* can be represented as a product-space whose form is:

$$\mathscr{H}_d^{(n)} = \underbrace{\mathbb{C}^d \otimes \ldots \otimes \mathbb{C}^d}_{n-times}, \quad \text{where } n \geq 1.$$

While $d$ represents the number of truth-values (corresponding to the dimension of $\mathbb{C}^d$), $n$ represents the number of the components of a quantum system that can store a quantum information living in the space $\mathscr{H}_d^{(n)}$. Of course, qubit-spaces represent particular examples of qudit-spaces $\mathscr{H}_d^{(n)}$, where $d = 2$.

The elements $|v_1, \ldots, v_n\rangle$ of the canonical basis of $\mathscr{H}_d^{(n)}$ represent the *registers* of the space and *dits* are special examples of registers living in the space $\mathscr{H}_d^{(1)} = \mathbb{C}^d$. The *quregisters* of $\mathscr{H}_d^{(n)}$ are identified with the unit vectors $|\psi\rangle$ of $\mathscr{H}_d^{(n)}$ (or, equivalently, with the corresponding projections $P_{|\psi\rangle}$), while any density operator $\rho$ of the space will represent a possible piece of quantum information (which may be either a pure state or a proper mixture).

In any qudit-space $\mathscr{H}_d^{(n)}$, each truth-value $|\frac{j}{d-1}\rangle$ determines a corresponding *truth-value projection* $P^{(n)}_{\frac{j}{d-1}}$, whose range is the closed subspace spanned by the set of all registers $|v_1, \ldots, v_n\rangle$ where $v_n = \frac{j}{d-1}$. From an intuitive point of view, $P^{(n)}_{\frac{j}{d-1}}$ represents the property "having the truth-degree $\frac{j}{d-1}$". In particular, $P^{(n)}_0 = P^{(n)}_{\frac{0}{d-1}}$ and $P^{(n)}_1 = P^{(n)}_{\frac{d-1}{d-1}}$ represent the *Falsity-property* and the *Truth-property*, respectively. On this basis, one can naturally apply the Born-rule and define for any state $\rho$ (of $\mathscr{H}_d^{(n)}$) the probability that $\rho$ satisfies the property $P^{(n)}_{\frac{j}{d-1}}$:

$$\mathtt{p}_{\frac{j}{d-1}}(\rho) := \mathtt{tr}\Big(\rho\, P^{(n)}_{\frac{j}{d-1}}\Big).$$

The *probability tout court* of $\rho$ can be then defined as the weighted mean of all truth-degrees.

**Definition 6.1** The probability of a density operator $\rho$ of $\mathscr{H}_d^{(n)}$

$$\mathtt{p}^{(d)}(\rho) := \frac{1}{d-1}\sum_{j=1}^{d-1} j\, \mathtt{p}_{\frac{j}{d-1}}(\rho).$$

One can prove that:

$$\mathtt{p}^{(d)}(\rho) = \mathtt{tr}\Big(\rho\,(\mathtt{I}^{(n-1)} \otimes E)\Big),$$

where $E$ is the *effect* (of $\mathbb{C}^d$) represented by the following matrix[1]:

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{d-1} & 0 & \cdots & 0 \\ 0 & 0 & \frac{2}{d-1} & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

As expected, in the particular case where $\rho$ corresponds to the qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, we obtain that $\mathtt{p}^{(2)}(\rho) = |c_1|^2$.

Notice that in the qudit-framework registers represent "classical" pieces of information, although based on many-valued systems of truth-values. At the same time, the probabilistic behavior of registers is generally different in the qubit-case and in the qudit-case. In qubit-spaces probabilities of registers are dichotomic: for any register $|v_1, \ldots, v_n\rangle$, either $\mathtt{p}_1(|v_1, \ldots, v_n\rangle) = 1$ or $\mathtt{p}_1(|v_1, \ldots, v_n\rangle) = 0$. In the qudit-case, instead, there are registers $|v_1, \ldots, v_n\rangle$ such that $\mathtt{p}^{(d)}(|v_1, \ldots, v_n\rangle) \neq 1, 0$. A typical example is represented by the dit $|\frac{1}{2}\rangle$ of the space $\mathbb{C}^3$, where

[1] The notion of *effect* has been defined in Sect. 1.5.

$$\mathtt{p}^{(3)}\left(|\frac{1}{2}\rangle\right) = \frac{1}{2}.$$

Thus, in qudit-spaces "classical" pieces of information may have an indeterminate probability-value.

## 6.3 Quantum Logical Gates in Qudit-Spaces

In qudit-spaces quantum information is processed by quantum logical gates (as happens in the case of qubit-spaces). Of course, when the truth-value number $d$ is greater than 2, one shall take into account the characteristic "many-valued features" of the space $\mathbb{C}^d$.

Before introducing some interesting examples of qudit-gates it is useful to recall what happens in the semantics of Łukasiewicz' logics (which represent special examples of fuzzy logics).[2] In the standard models of these logics the set **TV** of truth-values is identified either with the real interval [0, 1] or with a finite subset thereof (conventionally indicated as a set $\left\{\frac{0}{d-1}, \frac{1}{d-1}, \ldots, \frac{d-1}{d-1}\right\}$, where $d \geq 2$). For our aims it will be sufficient to refer to the finite case. The negation-operation is defined like in the classical case:

$$v' := 1 - v, \quad \text{for any truth-value} \quad v \in \mathbf{TV}.$$

At the same time conjunction is split into two different irreversible operations, the *min-conjunction* $\sqcap$ (also called *lattice-conjunction*) and the Ł*ukasiewicz-conjunction* $\odot$:

$$u \sqcap v := min(u, v), \quad u \odot v := max(0, u + v - 1), \quad \text{for any } \ u, v \in \mathbf{TV}.$$

While $\sqcap$ and $\odot$ are the same operation in the two-valued semantics, when $d > 2$ our two conjunctions turn out to satisfy different semantic properties. The min-conjunction gives rise to possible violations of the non-contradiction principle. We may have:

$$v \sqcap v' \neq 0.$$

Hence, contradictions are not necessarily false, as happens in the case of most fuzzy logics whose basic aim is modeling ambiguous and unsharp semantic situations. At the same time, $\sqcap$ behaves as a lattice-operation in the truth-value partial order $(\mathbf{TV}, \leq)$. The Łukasiewicz-conjunction, instead, is generally non-idempotent. We may have:

$$v \odot v \neq v.$$

[2] See [1, 2, 4].

Apparently, one is dealing with a kind of conjunction that can be usefully applied to model semantic situations where "repetita iuvant!"("repetitions are useful!").

As expected, the two conjunctions $\sqcap$ and $\odot$ allow us to define two different kinds of (inclusive) disjunctions (via de Morgan-law):

$$u \sqcup v := (u' \sqcap v')' = max(u, v); \quad u \oplus v := (u' \odot v')' = min(1, u + v).$$

All these logical operations (which are generally dealt with as irreversible) can be simulated by convenient (reversible) gates.

As happens in the case of qubit-spaces the negation-operation has a natural gate-counterpart.

**Definition 6.2** (*The negation-gate on the space* $\mathcal{H}_d^{(1)}$) The *negation-gate* on $\mathcal{H}_d^{(1)}$ is the linear operator $\mathtt{NOT}^{(1)}$ that satisfies the following condition for every element $|v\rangle$ of the canonical basis:

$$\mathtt{NOT}^{(1)}|v\rangle := |1 - v\rangle.$$

Thus, $\mathtt{NOT}^{(1)}$ behaves as the standard fuzzy negation.

The gate $\mathtt{NOT}^{(1)}$ can be naturally generalized to higher-dimensional spaces. Like in the case of qubit-spaces we will indicate by $\mathtt{NOT}^{(n)}$ the negation-gate that can be defined on the space $\mathcal{H}_d^{(n)}$ (in terms of $\mathtt{NOT}^{(1)}$ and of the identity operator $\mathtt{I}^{(n-1)}$).

How to deal, in this framework, with the irreversible conjunctions $\sqcap$ and $\odot$? A reversible counterpart for these operations can be obtained by using two special versions of the Toffoli-gate, that will be called the *Toffoli-gate* and the *Toffoli–Łukasiewicz gate*, respectively.

**Definition 6.3** (*The Toffoli-gate on the space* $\mathcal{H}_d^{(3)}$) The Toffoli-gate on $\mathcal{H}_d^{(3)}$ is the linear operator $\mathtt{T}^{(1,1,1)}$ that satisfies the following condition for every element $|u, v, w\rangle$ of the canonical basis:

$$\mathtt{T}^{(1,1,1)}|u, v, w\rangle := |u, v, (u \sqcap v \widehat{+}_d w)\rangle,$$

where $\widehat{+}_d$ is the addition modulo $d$.

**Definition 6.4** (*The Toffoli–Łukasiewicz gate on the space* $\mathcal{H}_d^{(3)}$) The Toffoli–Łukasiewicz gate on $\mathcal{H}_d^{(3)}$ is the linear operator $\mathtt{TŁ}^{(1,1,1)}$ that satisfies the following condition for every element $|u, v, w\rangle$ of the canonical basis:

$$\mathtt{TŁ}^{(1,1,1)}|u, v, w\rangle := |u, v, (u \odot v \widehat{+}_d w)\rangle.$$

Clearly, $\mathtt{T}^{(1,1,1)}$ and $\mathtt{TŁ}^{(1,1,1)}$ are the same gate when $d = 2$.

The gates $\mathtt{T}^{(1,1,1)}$ and $\mathtt{TŁ}^{(1,1,1)}$ can be naturally generalized to higher-dimensional spaces. Like in the case of qubit-spaces we will indicate by $\mathtt{T}^{(m,n,1)}$ and by $\mathtt{TŁ}^{(m,n,1)}$ (respectively) the two Toffoli-gates that can be defined on the space $\mathcal{H}_d^{(m+n+1)}$ (in terms of $\mathtt{T}^{(1,1,1)}$, $\mathtt{TŁ}^{(1,1,1)}$, the identity operator $\mathtt{I}^{(m+n-2)}$ and the gate $\mathtt{Swap}_{m,m+n-1}^{(m+n+1)}$).

The two Toffoli-gates naturally give rise to two different kinds of reversible conjunctions, that will be called the *Toffoli-conjunction* and the *Toffoli–Łukasiewicz conjunction*, respectively.

**Definition 6.5** (*The Toffoli-conjunction on the space $\mathscr{H}_d^{(m+n)}$*) For any $m, n \geq 1$ and for any quregister $|\psi\rangle$ of $\mathscr{H}_d^{(m+n)}$,

$$\mathtt{AND}^{(m,n)}|\psi\rangle := \mathtt{T}^{(m,n,1)}(|\psi\rangle \otimes |0\rangle).$$

**Definition 6.6** (*The Toffoli–Łukasiewicz conjunction on the space $\mathscr{H}_d^{(m+n)}$*) For any $m, n \geq 1$ and for any quregister $|\psi\rangle$ of $\mathscr{H}_d^{(m+n)}$,

$$\text{Ł}\mathtt{AND}^{(m,n)}|\psi\rangle := \mathtt{T}\text{Ł}^{(m,n,1)}(|\psi\rangle \otimes |0\rangle).$$

The gates Negation, Toffoli and Toffoli–Łukasiewicz are examples of semiclassical gates, that are unable to "create" superpositions: whenever the information-input is a register, the information-output also will be a register. How can we generalize *genuine* quantum gates to qudit-spaces?

A "natural" Hadamard-gate for a qudit-space $\mathscr{H}_d^{(1)} = \mathbb{C}^d$ can be defined as follows.

**Definition 6.7** (*The Hadamard-gate on the space $\mathscr{H}_d^{(1)}$*) The *Hadamard-gate* on $\mathscr{H}_d^{(1)}$ is the linear operator $\sqrt{\mathtt{I}}^{(1)}$ that satisfies the following condition for every element $|v\rangle$ of the canonical basis:

$$\sqrt{\mathtt{I}}^{(1)}|v\rangle = \frac{1}{\sqrt{2}}(c|v\rangle + |1-v\rangle),$$

where $c = \begin{cases} 1, & \text{if } v < \frac{1}{2}; \\ \sqrt{2}-1, & \text{if } v = \frac{1}{2}; \\ -1, & \text{if } v > \frac{1}{2}. \end{cases}$

As happens in the case of the qubit-space $\mathscr{H}_2^{(1)}$, $\sqrt{\mathtt{I}}^{(1)}$ transforms each element $|v\rangle$ of the canonical basis of $\mathscr{H}_d^{(1)}$ into a superposition of $|v\rangle$ and of its negation $|1-v\rangle$.

As an example consider the qutrit-space $\mathbb{C}^3$. We obtain:

- $\sqrt{\mathtt{I}}^{(1)}\left|\frac{0}{2}\right\rangle = \frac{1}{\sqrt{2}}(\left|\frac{0}{2}\right\rangle + \left|1-\frac{0}{2}\right\rangle) = \frac{1}{\sqrt{2}}(\left|\frac{0}{2}\right\rangle + \left|\frac{2}{2}\right\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$;
- $\sqrt{\mathtt{I}}^{(1)}\left|\frac{1}{2}\right\rangle = \frac{1}{\sqrt{2}}((\sqrt{2}-1)\left|\frac{1}{2}\right\rangle + \left|1-\frac{1}{2}\right\rangle) = \left|\frac{1}{2}\right\rangle$;
- $\sqrt{\mathtt{I}}^{(1)}\left|\frac{2}{2}\right\rangle = \frac{1}{\sqrt{2}}(-\left|\frac{2}{2}\right\rangle + \left|1-\frac{2}{2}\right\rangle) = \frac{1}{\sqrt{2}}(\left|\frac{0}{2}\right\rangle - \left|\frac{2}{2}\right\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Of course, $\sqrt{\mathtt{I}}^{(1)}\left|\frac{1}{2}\right\rangle$ represents a special case of a superposition, whose elements $\left|\frac{1}{2}\right\rangle$ and $\left|1-\frac{1}{2}\right\rangle$ are one and the same dit.

The following Theorem shows that $\sqrt{\mathtt{I}}^{(1)}$ represents a "good" generalization of the Hadamard-gate of the space $\mathbb{C}^2$.

**Theorem 6.1** *In any qudit-space $\mathcal{H}_d^{(1)}$ the gate $\sqrt{\mathtt{I}}^{(1)}$ satisfies the following conditions:*

*(1) $\sqrt{\mathtt{I}}^{(1)}$ transforms each element $|v\rangle$ of the canonical basis of $\mathcal{H}_d^{(1)}$ into a superposition of $|v\rangle$ and of its negation $|1-v\rangle$, assigning to both elements of the superposition the probability-value $\frac{1}{2}$.*

*(2) When $d = 2$, the gate $\sqrt{\mathtt{I}}^{(1)}$ coincides the standard Hadamard-gate of $\mathbb{C}^2$.*

*(3) $\sqrt{\mathtt{I}}^{(1)}\sqrt{\mathtt{I}}^{(1)} = \mathtt{I}^{(1)}$.*

*Proof* Straightforward.

As expected, the gate $\sqrt{\mathtt{I}}^{(1)}$ can be naturally generalized to higher-dimensional spaces. Like in the case of qubit-spaces we will indicate by $\sqrt{\mathtt{I}}^{(n)}$ the Hadamard-gate that can be defined on the space $\mathcal{H}_d^{(n)}$ (in terms of $\sqrt{\mathtt{I}}^{(1)}$ and of the identity operator $\mathtt{I}^{(n-1)}$).

In a similar way one can define a "natural" square root of negation for a qudit space $\mathcal{H}_d^{(1)}$.

**Definition 6.8** (*The square root of negation on the space $\mathcal{H}_d^{(1)}$*) The *square root of negation* on $\mathcal{H}_d^{(1)}$ is the linear operator $\sqrt{\mathtt{NOT}}^{(1)}$ such that for every element $|v\rangle$ of the canonical basis:

$$\sqrt{\mathtt{NOT}}^{(1)}|v\rangle = \frac{1}{2}((1+\imath)|v\rangle + (1-\imath)|1-v\rangle).$$

Like $\sqrt{\mathtt{I}}^{(1)}$, the gate $\sqrt{\mathtt{NOT}}^{(1)}$ can be generalized to higher-dimensional spaces. We will indicate by $\sqrt{\mathtt{NOT}}^{(n)}$ the square root of negation-gate that can be defined on the space $\mathcal{H}_d^{(n)}$ (in terms of $\sqrt{\mathtt{NOT}}^{(1)}$ and of the identity operator $\mathtt{I}^{(n-1)}$).

So far we have considered examples of gates that are unitary operators of a qudit-space $\mathcal{H}_d^{(n)}$. But of course, as happens in the case of qubit-spaces, any gate $\mathtt{G}$ (that is a unitary operator of $\mathcal{H}_d^{(n)}$) can be canonically associated to a unitary operation ${}^{\mathfrak{D}}\mathtt{G}$ that transforms all density operators of the space in a reversible way.

An important question concerns the possibility of physical implementations of qudit-spaces and qudit-gates. We will mention here only one significant example that concerns the qutrit-space $\mathbb{C}^3$. From a physical point of view, this space can be naturally used to represent the spin-values of bosons. Consider the observable $Spin_{\mathbf{z}}$ (the spin in the $\mathbf{z}$-direction, representing the $\mathbf{z}$-component of the angular momentum of a boson-particle). The three eigenvectors corresponding to the eigenvalues of $Spin_{\mathbf{z}}$ can be associated to the three elements of the canonical basis of the space $\mathbb{C}^3$. At the same time, the spin-observable in any other direction will be associated to a different basis of the space. On this ground, qutrits (living in the space $\mathbb{C}^3$) can be naturally stored by pure (or mixed) states of boson particles.

## 6.4 Łukasiewicz-Quantum Computational Logics

Qudit-spaces naturally give rise to a special variant of the holistic quantum computational semantics that will be called Ł*ukasiewicz-quantum computational semantics*.[3] We consider a "minimal" sentential Łukasiewicz *quantum computational language* $\mathscr{L}^{Ł}$, whose alphabet contains atomic formulas, including the two privileged sentences **t** and **f**. The connectives of $\mathscr{L}^{Ł}$ are: the negation $\neg$ (corresponding to the gate $\mathtt{NOT}^{(n)}$), the ternary Toffoli-connective $\intercal$ (corresponding to the gate $\mathtt{T}^{(m,n,1)}$), the ternary Toffoli–Łukasiewicz connective $\intercal_{Ł}$ (corresponding to the gate $\mathtt{TŁ}^{(m,n,1)}$), the Hadamard-connective $\sqrt{id}$ (corresponding to the Hadamard-gate $\sqrt{\mathtt{I}}^{(n)}$), the connective square root of negation $\sqrt{\neg}$ (corresponding to the gate $\sqrt{\mathtt{NOT}}^{(n)}$). The concept of *formula* of $\mathscr{L}^{Ł}$ is defined in the expected way.

The two Toffoli-connectives allow us to define two binary conjunctions:

$$\alpha \wedge \beta := \intercal(\alpha, \beta, \mathbf{f}); \qquad \alpha \wedge_{Ł} \beta := \intercal_{Ł}(\alpha, \beta, \mathbf{f}),$$

where the false sentence **f** plays the role of a *syntactical ancilla*.

The notions of *atomic complexity* and of *syntactical tree* of a given formula are supposed to be defined like in the case of standard sentential quantum computational languages. On this basis, for any choice of a truth-value number $d$, the *semantic space* $\mathscr{H}_d^{\alpha}$ of a formula $\alpha$ is identified with the qudit-space $\mathscr{H}_d^{(At(\alpha))}$, where $At(\alpha)$ is the atomic complexity of $\alpha$.

For any number $d \geq 2$ and for any formula $\alpha$, $STree^{\alpha}$ (the syntactical tree of $\alpha$) uniquely determines the *gate tree* of $\alpha$: a sequence of gates all defined on the space $\mathscr{H}_d^{\alpha}$. Consider, for instance, the formula

$$\alpha = \mathbf{q} \ \wedge_{Ł} \ \neg\mathbf{q} = \intercal_{Ł}(\mathbf{q}, \neg\mathbf{q}, \mathbf{f}).$$

The gate-tree of $\alpha$ can be naturally identified with the following gate-sequence:

$$({}^{\mathfrak{D}}\mathtt{I}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{I}^{(1)}, \ {}^{\mathfrak{D}}\mathtt{TŁ}^{(1,1,1)}).$$

This procedure can be generalized to any $\alpha$, whose gate tree will be indicated by $({}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{(h-1)}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{(1)})$ (where $h$ is the Height of $\alpha$).

As expected, the basic notions of the Łukasiewicz-quantum computational semantics depend on the choice of the truth-value number $d$. The concept of ($d$-valued) *holistic model* of $\mathscr{L}^{Ł}$ is based on the weaker notion of ($d$-valued) *holistic map* for $\mathscr{L}^{Ł}$. This is a map $\mathtt{Hol}_d$ that assigns to each level of the syntactical tree of any formula $\alpha$ a density operator living in the semantic space of $\alpha$. We have:

$$\mathtt{Hol}_d(Level_i^{\alpha}) \in \mathfrak{D}(\mathscr{H}_d^{\alpha})$$

[3] See [3].

(for any $Level_i^\alpha$ of $STree^\alpha$).

The concept of *contextual meaning* assigned by a holistic map $\mathtt{Hol}_d$ to an occurrence of a subformula in the syntactical tree of a given formula $\alpha$ and the concept of *normal holistic map* are defined like in the case of the two-valued holistic quantum computational semantics.

Now the concepts of *holistic model*, *truth* and *logical consequence* (in the Łukasiewicz-quantum computational semantics) can be defined as follows.

**Definition 6.9** (*Holistic model*) A *holistic model* of the language $\mathscr{L}^{Ł}$ is a normal holistic map $\mathtt{Hol}_d$ that satisfies the following conditions for any formula $\alpha$.

(1) Let $({}^{\mathfrak{D}}\mathtt{G}^\alpha_{(h-1)}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^\alpha_{(1)})$ be the gate tree of $\alpha$ and let $1 \le i < h$). Then,

$$\mathtt{Hol}_d(Level_i^\alpha) = {}^{\mathfrak{D}}\mathtt{G}_i^\alpha(\mathtt{Hol}_d(Level_{i+1}^\alpha)).$$

In other words, the meaning of each level (different from the top level) is obtained by applying the corresponding gate to the meaning of the level that occurs immediately above.

(2) The contextual meanings assigned by $\mathtt{Hol}_d$ to the false sentence **f** and to the true sentence **t** are the Falsity $P_0^{(1)}$ and the Truth $P_1^{(1)}$, respectively.

On this basis, we put:

$$\mathtt{Hol}_d(\alpha) := \mathtt{Hol}_d(Level_1^\alpha), \quad \text{for any formula } \alpha.$$

**Definition 6.10** (*Truth*) A formula $\alpha$ is called *true* with respect to a model $\mathtt{Hol}_d$ iff $\mathtt{p}^{(d)}(\mathtt{Hol}_d(\alpha)) = 1$.

**Definition 6.11** (*d-Logical consequence*) A formula $\beta$ is called a *d-logical consequence* of a formula $\alpha$ (abbreviated as $\alpha \vDash_d \beta$) iff for any formula $\gamma$ such that $\alpha$ and $\beta$ are subformulas of $\gamma$ and for any model $\mathtt{Hol}_d$,

$$\mathtt{p}^{(d)}(\mathtt{Hol}_d^\gamma(\alpha)) \le \mathtt{p}^{(d)}(\mathtt{Hol}_d^\gamma(\beta)).$$

**Definition 6.12** (*Logical consequence*) A formula $\beta$ is called a *logical consequence* of a formula $\alpha$ (abbreviated as $\alpha \vDash \beta$) iff for any $d \ge 2$, $\alpha \vDash_d \beta$.

We call *d-valued Łukasiewicz-quantum computational logic* (${}^d$**ŁQCL**) the logic that is semantically characterized by the $d$-logical consequence relation (where $d \ge 2$); while the logic characterized by the stronger notion of logical consequence is termed *Łukasiewicz-quantum computational logic* (**ŁQCL**).

Consider now two formulas $\alpha$ and $\beta$ that belong to the common language of **ŁQCL** and of the (sentential) holistic quantum computational logic **HQCL**. We have (trivially):

$$\alpha \vDash_{\mathbf{ŁQCL}} \beta \;\Rightarrow\; \alpha \vDash_{\mathbf{HQCL}} \beta.$$

The validity of the inverse implication represents a reasonable conjecture that is, so far, an open problem.

## References


1. Chang, C.C.: Algebraic analysis of many valued logics. Trans. Am. Math. Soc. **88**, 74–80 (1958)
2. Cignoli, R., D'Ottaviano, I., Mundici, D.: Algebraic Foundations of Many-Valued Reasoning. Kluwer, Dordrecht (2000)
3. Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: A many-valued approach to quantum computational logics. Fuzzy Sets Syst. (2016). https://doi.org/10.1016/j.fss.2016.12.015
4. Hájek, P.: Metamathematics of Fuzzy Logic. Kluwer, Dordrecht (1998)

# Chapter 7
# What Exactly Are Quantum Computations? Classical and Quantum Turing Machines

## 7.1 Introduction

Classical computers have a perfect abstract model represented by the concept of *Turing machine*. Due to the intuitive strength of this concept and to 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 pioneering work,[1] the abstract mathematical model for quantum computers has been often represented in terms of the notion of *quantum Turing machine*, the quantum counterpart of the classical notion of *Turing machine*.[2] 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.

[1]See [4, 5].

[2]See, for instance, [2, 3, 6–9].



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_7

Both in the classical and in the quantum case, it is expedient to consider a more abstract concept: the notion of *state machine*, which neglects both tapes and moving heads. Every finite computational task realized in different computational models proposed in the literature can be simulated by a state machine.[3] In order to compare classical and quantum computations, we will analyze the concepts of (*classical*) *deterministic state machine*, (*classical*) *probabilistic state machine* and *quantum state machine*. On this basis we will discuss the question: to what extent can quantum state machines be simulated by classical probabilistic state machines?

Each state machine is devoted to a single task determined by its program. Real computers, however, behave differently, being able to solve different kinds of problems, which may be chosen by computer-users. In the quantum case, such concrete computation-situations can be modeled by the mathematical notion of *abstract quantum computing machine*, whose different programs determine different quantum state machines. We will see how quantum computations performed by quantum computing machines can be linguistically described by formulas of quantum computational logics.[4]

## 7.2 Classical Deterministic and Probabilistic Machines

We will first introduce the notion of *deterministic state machine*. On this basis, *probabilistic state machines* will be represented as stochastic variants of deterministic machines that are able to calculate different outputs with different probability-values.

**Definition 7.1** (*Deterministic state machine*) A *deterministic state machine* is an abstract system **M** based on the following elements:

(1) A finite set $\mathscr{S}$ of *internal states*, which contains an *initial state* $s_{in}$ and includes a set of *halting states* $\mathscr{S}_{halt} = \{s_{halt_j} : j \in J\}$.
(2) A finite alphabet, which can be identified with the set $\{0, 1\}$ of the two classical bits. Any *register* represented by a bit-sequence $w = (x_1, \ldots, x_n)$ is a *word* (of length $n$).[5] Any pair $(s, w)$ consisting of an internal state $s$ and of a word $w$ represents a possible *configuration* of **M**, which is interpreted as follows: **M** is in the internal state $s$ and $w$ is the word written on an ideal tape.
(3) A set of words that represent possible *word-inputs* for **M**.
(4) A *program*, which is identified with a finite sequence $(R_0, \ldots, R_t)$ of rules. Each $R_i$ is a partial function: a well-determined instruction that transforms configurations into configurations. We may have: $R_i = R_j$ with $i \neq j$. The number $i$,

[3] See, for instance, [10].

[4] See [1].

[5] In order to emphasize the comparison between deterministic state machines and quantum state machines, *words* are here identified with *registers* (although, in the framework of classical computation, the concept of "word" is often defined as a sequence of registers).

corresponding to the rule $R_i$, represents the $i$th step of the program. The following conditions are required:

(4.1) The rule $R_0$ is defined for any configuration $(s_0, w_0)$, where $s_0$ is the initial state $s_{in}$ and $w_0$ is a possible word-input. We have: $R_0 : (s_0, w_0) \mapsto (s_1, w_1)$, where $s_1$ is different from the initial state and from all halting states (if $t \neq 0$).

(4.2) For any $i$ $(0 < i < t)$, $R_i : (s_i, w_i) \mapsto (s_{i+1}, w_{i+1})$, where $s_{i+1}$ is different from all $s_i, \ldots, s_0$ and from all halting states.

(4.3) $R_t : (s_t, w_t) \mapsto (s_{t+1}, w_{t+1})$, where $s_{t+1}$ is a halting state.

Each configuration $(s_{i+1}, w_{i+1})$ represents the *output* for the step $i$ and the *input* for the step $i + 1$.

Apparently, each deterministic state machine is devoted to a single task that is determined by its program. The concept of *computation* of a deterministic state machine can be then defined as follows.

**Definition 7.2** (*Computation of a deterministic state machine*) A *computation* of a deterministic state machine **M** is a finite sequence of configurations $((s_0, w_0), \ldots, (s_{t+1}, w_{t+1}))$, where:

(1) $w_0$ is a possible word-input of **M**.

(2) $s_0, \ldots, s_{t+1}$ are different internal states of **M** such that: $s_0 = s_{in}$ and $s_{t+1}$ is a halting state.

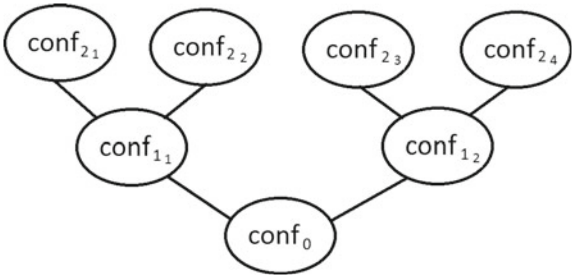
(3) For any $i$ (such that $0 \leq i \leq t$), $(s_{i+1}, w_{i+1}) = R_i((s_i, w_i))$, where $R_i$ is the $i$th rule of the program.

The configurations $(s_0, w_0)$ and $(s_{t+1}, w_{t+1})$ represent, respectively, the *input* and the *output* of the computation; while the words $w_0$ and $w_{t+1}$ represent, respectively, the *word-input* and the *word-output* of the computation.

Let us now turn to the concept of *probabilistic state machine*. The only difference between deterministic and probabilistic state machines concerns the program, which may be stochastic in the case of a probabilistic state machine (**PM**). In such a case, instead of a sequence of rules, we will have a sequence $(Seq_0, \ldots, Seq_t)$ of sequences of rules such that: $Seq_0 = (R_{0_1}, \ldots, R_{0_r}), \ldots, Seq_t = (R_{t_1}, \ldots, R_{t_l})$. Each rule $R_{i_j}$ (occurring in the sequence $Seq_i$) is associated to a probability-value $\mathtt{p}_{i_j}$ such that: $\sum_j \mathtt{p}_{i_j} = 1$. From an intuitive point of view, $\mathtt{p}_{i_j}$ represents the probability that the rule $R_{i_j}$ be applied at the $i$th step. A deterministic state machine is, of course, a special case of a probabilistic state machine characterized by the following property: each sequence $Seq_i$ consists of a single rule $R_i$.

Any probabilistic state machine naturally gives rise to a graph-structure for any choice of an input-configuration $conf_0 = (s_0, w_0)$. As an example, consider the following simple case: a probabilistic state machine **PM** whose program consists of two sequences, each consisting of two rules: $Seq_0 = (R_{0_1}, R_{0_2})$, $Seq_1 = (R_{1_1}, R_{1_2})$, such that $\mathtt{p}_{0_1} = \mathtt{p}_{0_2} = \mathtt{p}_{1_1} = \mathtt{p}_{1_2} = \frac{1}{2}$. The graph associated to **PM** for the configuration $conf_0$ is illustrated by Fig. 7.1.

**Fig. 7.1** The graph of the machine **PM**




How do probabilistic machines compute? In order to define the concept of *computation* of a probabilistic machine, let us first introduce the notions of *program-path* and of *computation-path* of a given probabilistic machine.

**Definition 7.3** (*Program-path and computation-path*) Let **PM** be a probabilistic state machine with program $(Seq_0, \ldots, Seq_t)$.

- A *program-path* of **PM** is a sequence $\mathscr{P} = (R_{0_h}, \ldots, R_{i_j}, \ldots, R_{t_k})$ of rules, where each $R_{i_j}$ is a rule from $Seq_i$.
- For any choice of an input $(s_0, w_0)$, any program-path $\mathscr{P}$ determines a sequence of configurations $\mathscr{C}\mathscr{P} = ((s_0, w_0), \ldots, (s_i, w_i), \ldots, (s_{t+1}, w_{t+1}))$, where $(s_{i+1}, w_{i+1}) = R_{i_j}(s_i, w_i)$ and $R_{i_j}$ is the $i$th element of $\mathscr{P}$. This sequence is called the *computation-path* of **PM** determined by the program-path $\mathscr{P}$ and by the input $(s_0, w_0)$.
  The configuration $(s_{t+1}, w_{t+1})$ represents the output of $\mathscr{C}\mathscr{P}$.

Any program-path $\mathscr{P} = (R_{0_h}, \ldots, R_{i_j}, \ldots, R_{t_k})$ has a well determined probability-value $\mathtt{p}(\mathscr{P})$, which is defined as follows (in terms of the probability-values of its rules): $\mathtt{p}(\mathscr{P}) := \mathtt{p}_{0_h} \cdot \ldots \cdot \mathtt{p}_{i_j} \cdot \ldots \cdot \mathtt{p}_{t_k}$. As expected, the probability-value of a program-path $\mathscr{P}$ naturally determines the probability-values of all corresponding computation-paths. It is sufficient to put: $\mathtt{p}(\mathscr{C}\mathscr{P}) := \mathtt{p}(\mathscr{P})$. Consider now the set $\mathbf{P_{PM}}$ of all program-paths and the set $\mathbf{CP_{PM}}$ of all computation-paths of a probabilistic machine **PM**. One can easily show that:

$$\sum_i \{\mathtt{p}(\mathscr{P}_i) : \mathscr{P}_i \in \mathbf{P_{PM}}\} = \sum_i \{\mathtt{p}(\mathscr{C}\mathscr{P}_i) : \mathscr{C}\mathscr{P}_i \in \mathbf{CP_{PM}}\} = 1.$$

On this basis the concept of *computation* of a probabilistic state machine can be defined as follows.

**Definition 7.4** (*Computation of a probabilistic state machine*) A *computation* of a probabilistic state machine **PM** with input $(s_0, w_0)$ is the system of all computation-paths of **PM** with input $(s_0, w_0)$.

Unlike the case of deterministic state machines, a computation of a probabilistic state machine does not yield a unique output. For any choice of a configuration-input $(s_0, w_0)$, the computation-output is a system of possible configuration-outputs

$(s^i_{t+1}, w^i_{t+1})$, where each $(s^i_{t+1}, w^i_{t+1})$ corresponds to a computation-path $\mathscr{CP}_i$. As expected, each $(s^i_{t+1}, w^i_{t+1})$ has a well determined probability-value that is defined as follows: $\mathtt{p}((s^i_{t+1}, w^i_{t+1})) := \sum_i \{\mathtt{p}(\mathscr{CP}_i)$ : the configuration-output of $\mathscr{CP}_i$ is $(s^i_{t+1}, w^i_{t+1})\}$ .One can easily show that the sum of the probability-values of all configuration-outputs of any machine **PM** is 1.

## 7.3 Quantum State Machines

We will now introduce the concept of *quantum state machine*, which can be intuitively regarded as a kind of quantum superposition of "many" classical deterministic state machines. For the sake of simplicity, we will consider here quantum state machines whose possible inputs and outputs are represented by pure states of a qubit-space. A generalization to the case of density operators and to qudit-spaces can be obtained in a natural way.

**Definition 7.5** (*Quantum state machine*) A *quantum state machine* is an abstract system **QM** associated to a Hilbert space $\mathscr{H}^{\mathbf{QM}} = \mathscr{H}^H \otimes \mathscr{H}^{\mathscr{S}} \otimes \mathscr{H}^W$, whose unit-vectors $|\psi\rangle$ represent possible pure states of a quantum system that could physically implement the computations of the state machine. The following conditions are required:

(1) $\mathscr{H}^H$ (which represents the halting-space) is the space $\mathscr{H}^{(1)} (= \mathbb{C}^2)$, where the two elements of the canonical basis $(\{|0\rangle_H, |1\rangle_H\})$ correspond to the states "the machine does not halt" and "the machine halts", respectively.
(2) $\mathscr{H}^{\mathscr{S}}$ (which represents the internal-state space) is associated to a finite set $\mathscr{S}$ of classical internal states. We require that $\mathscr{H}^{\mathscr{S}} = \mathscr{H}^{(m)}$, where $2^m$ is the cardinal number of $\mathscr{S}$. Accordingly, the set $\mathscr{S}$ can be one-to-one associated to a basis of $\mathscr{H}^{\mathscr{S}}$.
(3) $\mathscr{H}^W$ (which represents the word-space) is identified with a Hilbert space $\mathscr{H}^{(n)}$ (for a given $n \geq 1$). The number $n$ determines the length of the registers $|x_1, \ldots, x_n\rangle$ that may occur in a computation. Shorter registers $|x_1, \ldots, x_h\rangle$ (with $h < n$) can be represented in the space $\mathscr{H}^{(n)}$ by means of convenient *ancillary bits*. Let $\mathbf{B}^{\mathbf{QM}}$ be a basis of $\mathscr{H}^{\mathbf{QM}}$, whose elements are unit-vectors having the following form: $|\varphi_i\rangle = |h_i\rangle|s_i\rangle|x_{i_1}, \ldots, x_{i_n}\rangle$, where $|h_i\rangle$ belongs to the basis of $\mathscr{H}^H$, while $|s_i\rangle$ belongs to the basis of $\mathscr{H}^{\mathscr{S}}$. Any unit-vector $|\psi\rangle$ of $\mathscr{H}^{\mathbf{QM}}$ that is a superposition of basis-elements $|\varphi_i\rangle$ represents a possible *computational state* of **QM**. The expected interpretation of a computational state $|\psi\rangle = \sum_i c_i |h_i\rangle|s_i\rangle|x_{i_1}, \ldots, x_{i_n}\rangle$ is the following: the machine in state $|\psi\rangle$ might be in the halting state $|h_i\rangle$ and might correspond to the classical configuration $(s_i, (x_{i_1}, \ldots, x_{i_n}))$ with probability $|c_i|^2$. Hence, the state $|\psi\rangle$ describes a kind of *quantum co-existence* of different classical deterministic configurations.
(4) The set of *possible inputs* of **QM** is identified with the set of all computational states that have the following form: $|\psi\rangle = \sum_i c_i |0_H\rangle|s_{in}\rangle|x_{i_1}, \ldots, x_{i_n}\rangle$ (where $|s_{in}\rangle$ is the initial internal state in $\mathscr{S}$).

(5) Like a deterministic state machine, a quantum state machine **QM** is characterized by a *program*. In the quantum case a program is identified with a sequence $(\mathtt{U}_0, \ldots, \mathtt{U}_t)$ of unitary operators of $\mathscr{H}^{\mathbf{QM}}$, where we may have: $\mathtt{U}_i = \mathtt{U}_j$ with $i \neq j$. The following conditions are required:

   (a) for any possible input $|\psi_0\rangle$, $\mathtt{U}_0(|\psi_0\rangle) = |\psi_1\rangle$ is a superposition of basis-elements having the following form: $|h_i^1\rangle|s_i^1\rangle|x_{i_1}^1, \ldots, x_{i_n}^1\rangle$, where all $s_i^1$ are different from $s_{in}$ and $|h_i^1\rangle = |0_H\rangle$, if $t \neq 0$.
   (b) For any $j$ (such that $0 < j < t$), $\mathtt{U}_j(|\psi_j\rangle) = |\psi_{j+1}\rangle$ is a superposition of basis-elements having the following form: $|0_H\rangle|s_i^{j+1}\rangle|x_{i_1}^{j+1}, \ldots, x_{i_n}^{j+1}\rangle$.
   (c) $\mathtt{U}_t(|\psi_t\rangle) = |\psi_{t+1}\rangle$ is a superposition of basis-elements having the following form: $|1_H\rangle|s_{halt_j}\rangle|x_{i_1}^{t+1}, \ldots, x_{i_n}^{t+1}\rangle$ (where $|s_{halt_j}\rangle$ is an internal halting state in $\mathscr{S}$).

The concept of *computation* of a quantum state machine can be now defined in a natural way.

**Definition 7.6** (*Computation of a quantum state machine*) Let **QM** be a quantum state machine, whose program is the operator-sequence $(\mathtt{U}_0, \ldots, \mathtt{U}_t)$ and let $|\psi_0\rangle$ be a possible input of **QM**. A *computation* of **QM** with input $|\psi_0\rangle$ is a sequence $\mathscr{QC} = (|\psi_0\rangle, \ldots, |\psi_{t+1}\rangle)$ of computational states such that: $|\psi_{i+1}\rangle = \mathtt{U}_i(|\psi_i\rangle)$, for any $i$ $(0 \leq i \leq t)$. The vector $|\psi_{t+1}\rangle$ represents the output of the computation, while the density operator $Red^3(|\psi_{t+1}\rangle)$ (the reduced state of $|\psi_{t+1}\rangle$ with respect to the third subsystem) represents the word-output of the computation.

Consider now a quantum state machine whose program is $(\mathtt{U}_0, \ldots, \mathtt{U}_t)$. Each $\mathtt{U}_i$ naturally determines a corresponding word-operator $\mathtt{U}_i^W$, defined on the word-space $\mathscr{H}^W$. Generally, it is not guaranteed that all word-operators are unitary. But it is convenient to refer to quantum state machines that satisfy this condition. In this way, any quantum state machine (whose word-space is $\mathscr{H}^{(n)}$) determines a *quantum circuit*, consisting of a sequence $(\mathtt{U}_0^W, \ldots, \mathtt{U}_t^W)$ of gates, where $n$ represents the *width*, while $t + 1$ represents the *depth* of the circuit. Conversely, we can assume that any circuit $(\mathtt{U}_0^W, \ldots, \mathtt{U}_t^W)$ gives rise to a quantum state machine, whose halting states and whose internal states are supposed to be chosen in a conventional way.

To what extent can quantum state machines be simulated by classical probabilistic state machines? It is interesting to discuss this question by referring to the *Mach-Zehnder circuit* $(\sqrt{\mathtt{I}}^{(1)}, \mathtt{NOT}^{(1)}, \sqrt{\mathtt{I}}^{(1)})$, where:

$$\sqrt{\mathtt{I}}^{(1)}\mathtt{NOT}^{(1)}\sqrt{\mathtt{I}}^{(1)}|0\rangle = |0\rangle; \quad \sqrt{\mathtt{I}}^{(1)}\mathtt{NOT}^{(1)}\sqrt{\mathtt{I}}^{(1)} - |1\rangle = |1\rangle.$$

As we have seen in Sect. 2.4 this characteristic quantum circuit can be physically implemented by a *Mach-Zehnder interferometer* (Fig. 7.2).

One is dealing with a physical situation that for a long time has been described as deeply counterintuitive. For, according to a "classical way of thinking" one would expect that when a photon-beam has entered into the interferometer along the **x**-direction, the outcoming photons from the second beam splitter should be detected

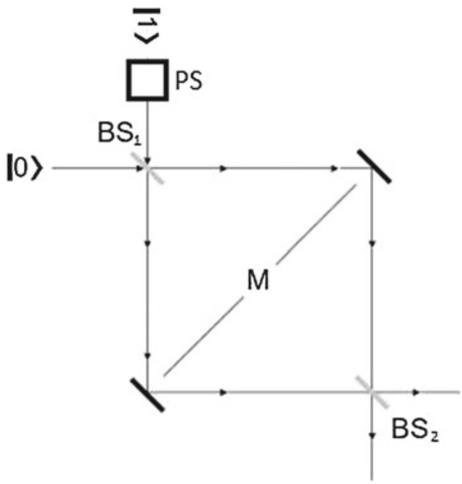



**Fig. 7.2** The Mach–Zehnder interferometer

with probability $\frac{1}{2}$ either along the **x** direction or along the **y**-direction. And, in fact, this is precisely what happens whenever a measurement is performed inside the interferometer-box; in such a case, photons are detected either along the **x** direction or along the **y**-direction with a frequency that is approximately equal to $\frac{1}{2}$.

Is it possible to describe the behavior of the Mach–Zehnder circuit by means of a classical probabilistic state machine? Is there any natural "classical counterpart" for the Hadamard-gate? A natural candidate might be a particular example of a probabilistic state machine that can be conventionally called the *classical probabilistic* NOT-*state machine* ($\mathbf{PM}^{\mathrm{NOT}}$). Such machine can be defined as follows:

- The set of possible word-inputs of $\mathbf{PM}^{\mathrm{NOT}}$ is the set of words $\{(0), (1)\}$.
- The program of $\mathbf{PM}^{\mathrm{NOT}}$ consists of the following sequence of rules:

$$Seq_0 = (R_{0_1}, R_{0_2}),$$

where:

$R_{0_1} : (s_{in}, (x)) \mapsto (s_{halt_j}, (x))$ and $\mathtt{p}_{0_1} = \frac{1}{2}$;
$R_{0_2} : (s_{in}, (x)) \mapsto (s_{halt_j}, (1 - x))$ and $\mathtt{p}_{0_2} = \frac{1}{2}$.

Consider, for instance, the input $(s_{in}, (0))$. The output will be the following set:

$$\left\{(s_{halt_j}, (0)), (s_{halt_j}, (1))\right\}.$$

On this basis, a "classical probabilistic Mach–Zehnder state machine" would determine (for the word-input (0)) the word-graph illustrated by Fig. 7.3.

Such a machine turns out to compute both the words (0) and (1) with probability $\frac{1}{2}$. And, interestingly enough, this is the same probabilistic result that is obtained in the quantum case, when a measurement is performed inside the interferometer-box. The

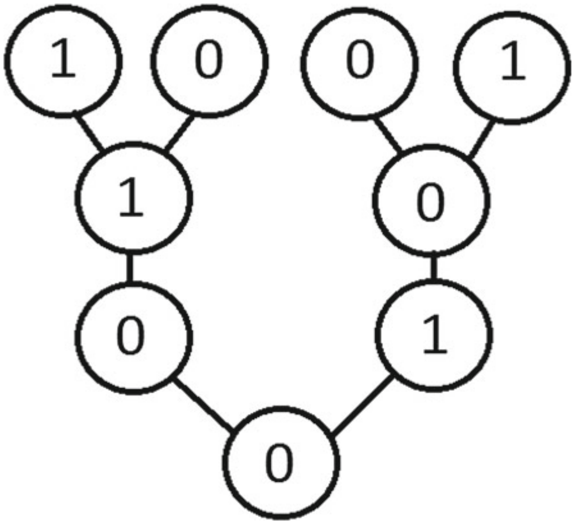



**Fig. 7.3** A word-graph for a "classical probabilistic Mach–Zehnder state machine"

example of the Mach–Zehnder circuit seems to confirm the following conjecture: the characteristic superposition-patterns, that may occur during a quantum computation (when no measurement is performed during the computation-process), cannot be generally represented by probabilistic state machines. This conclusion seems to be in agreement with a position defended by Feynman:

*Can a quantum system be probabilistically simulated by a classical (probabilistic, I'd assume) universal computer? In other words, a computer which will give the same probabilities as the quantum system does. If you take the computer to be the classical kind I've described so far [....] and there're no changes in any laws, and there's no hocus-pocus, the answer is certainly, No! This is called the hidden-variable problem: it is impossible to represent the results of quantum mechanics with a classical universal device.*[6]

The basic reason why quantum parallelism and classical parallelism are deeply different depends on the fact that quantum parallelism is essentially based on superpositions, which give rise to a strange co-existence of different alternatives. For instance, in the Mach–Zehnder interferometer photons behave as if each photon should travel along the **x**-direction and along the **y**-direction *at the same time*. While the parallel configuration of different computational paths in a classical probabilistic machine can be easily transformed into a *linear order*, in the case of quantum machines such a linearization cannot be generally performed, without destroying the quantum probabilistic predictions.

[6]See [4].

## 7.4 Abstract Quantum Computing Machines

State machines represent *rigid* systems: each machine has a definite program, devoted to a single task. Real computers, however, behave differently, being able to solve different kinds of problems (which can be chosen by computer-users). We will now investigate a "more liberal" concept of machine that will be called *abstract quantum computing machine*. The intuitive idea can be sketched as follows. Consider a finite gate-system $\mathfrak{G} = (\mathtt{G}_1^{(n_1)}, \ldots, \mathtt{G}_t^{(n_t)})$, where each $\mathtt{G}_i^{(n_i)}$ is defined on a word-space $\mathscr{H}^{(n_i)}$.[7] The system $\mathfrak{G}$ determines an infinite set of *derived gates* that can be obtained as appropriate combinations of elements of $\mathfrak{G}$, by using gate-tensor products and gate-compositions. An interesting example is represented by the gate system

$$\mathfrak{G}^* = (\mathtt{I}^{(1)}, \mathtt{NOT}^{(1)}, \sqrt{\mathtt{I}}^{(1)}, \mathtt{T}^{(1,1,1)}).$$

As we have learnt in Sect. 2.2, for any $n, m \geq 1$, the gates $\mathtt{NOT}^{(n)}, \sqrt{\mathtt{I}}^{(n)}, \mathtt{T}^{(m,n,1)}$ can be represented as derived gates of the system $\mathfrak{G}^*$.

Any gate-system $\mathfrak{G}$ gives rise to an infinite family $\mathfrak{C}^{\mathfrak{G}}$ of circuits

$${}^{\mathfrak{G}}\mathscr{C}_j^{(n)} = ({}^{\mathfrak{G}}\mathtt{G}_1^{(n)}, \ldots, {}^{\mathfrak{G}}\mathtt{G}_t^{(n)}),$$

where each ${}^{\mathfrak{G}}\mathtt{G}_i^{(n)}$ is a derived gate of $\mathfrak{G}$, defined on the space $\mathscr{H}^{(n)}$. For instance, the Mach–Zehnder circuit $(\sqrt{\mathtt{I}}^{(1)}, \mathtt{NOT}^{(1)}, \sqrt{\mathtt{I}}^{(1)})$ represents an example of a circuit that belongs to $\mathfrak{C}^{\mathfrak{G}^*}$ (the circuit-family determined by the gate-system $\mathfrak{G}^*$).

On this basis, it seems reasonable to assume that any choice of a finite gate-system $\mathfrak{G}$ determines an *abstract quantum computing machine* $\mathbf{AbQCM}^{\mathfrak{G}}$ whose programs correspond to the circuits that belong to the family $\mathfrak{C}^{\mathfrak{G}}$. Since any circuit can be associated to a particular quantum state machine, any abstract quantum computing machine can be also regarded as an infinite family of quantum state machines, corresponding to different programs that the abstract machine can perform. Accordingly, any circuit ${}^{\mathfrak{G}}\mathscr{C} \in \mathfrak{C}^{\mathfrak{G}}$, applied to an appropriate input, represents a *computation* of the abstract machine $\mathbf{AbQCM}^{\mathfrak{G}}$. We can say that $\mathbf{AbQCM}^{\mathfrak{G}}$ *computes* the output $|\psi\rangle_{out}$ for the input $|\psi\rangle_{in}$ iff there is a circuit ${}^{\mathfrak{G}}\mathscr{C} \in \mathfrak{C}^{\mathfrak{G}}$ such that ${}^{\mathfrak{G}}\mathscr{C}|\psi\rangle_{in} = |\psi\rangle_{out}$.

Abstract quantum computing machines clearly represent mathematical models for possible physical quantum computers. A unitary operator $\mathtt{U} = \mathtt{U}_t \ldots \mathtt{U}_0$ determined by a program $(\mathtt{U}_0, \ldots, \mathtt{U}_t)$ of an abstract machine $\mathbf{AbQCM}^{\mathfrak{G}}$ can be regarded as the mathematical description of a possible time-evolution of a quantum system **S** that is able to implement such a program for convenient inputs.

A crucial problem (which does not represent a difficulty in the case of classical computers) concerns the *reading* of the result of a computation performed by a quantum computer. While the physical process that corresponds to the performance

[7] For the sake of simplicity, we are considering here gates $\mathtt{G}$ that are unitary operators (of a given Hilbert space). Of course, the procedure can be easily generalized to the case of gates ${}^{\mathfrak{D}}\mathtt{G}$ that are unitary quantum operations.

of a given computation is a reversible phenomenon (mathematically described by a unitary operator), the final reading of the computation-result involves a *measurement*, which gives rise to a (generally irreversible) *collapse of the wave function*. Such a *reading-measurement* can be performed by an apparatus that is associated to a particular basis of the Hilbert space associated to the quantum state machine under consideration.

Consider a computation determined by the program $(\mathtt{U}_0, \dots, \mathtt{U}_t)$ of a quantum state machine **QM** (with associated Hilbert space $\mathscr{H}^{\mathbf{QM}}$) and let $|\psi\rangle_{in}$ a possible input for **QM**. The output of the computation will be the state

$$|\psi\rangle_{out} = \mathtt{U}|\psi\rangle_{in},$$

where $\mathtt{U} = \mathtt{U}_t \dots \mathtt{U}_0$. For any choice of a basis **B** of the Hilbert space $\mathscr{H}^{\mathbf{QM}}$ the state $|\psi\rangle_{out}$ can be represented as a superposition $\sum_i c_i|\varphi_i\rangle$ of elements of **B**, where each $|\varphi_i\rangle$ has the form $|1_H\rangle|s_{halt_j}\rangle|x_{i_1}, \dots, x_{i_n}\rangle$. Hence, any reading-measurement $M$ (associated to the basis **B**) will determine a state-transformation

$$\sum_i c_i|\varphi_i\rangle \;\mapsto_M\; |\varphi_i\rangle.$$

Accordingly, in order to obtain an experimental result that can approximately reproduce the probabilistic predictions of the superposition $\sum_i c_i|\varphi_i\rangle$, we shall repeat our measurement (a given number of times), always using equi-prepared input-states.

A peculiar difficulty of the reading-procedure in quantum computation concerns the choice of the "right time" when the final measurements should be performed. In some cases the reading-measurement is not problematic. For instance, in the computation of the Mach–Zehnder circuit one shall simply wait for the "clicks" of the detectors located along the **x**-direction and along the **y**-direction. Generally, however, the situation may be more complicated and the choice of the right time when the final measurement should be performed (in order to obtain the expected result) may be critical. Of course, the number of computational steps of a program $(\mathtt{U}_0, \dots, \mathtt{U}_t)$ does not generally determine the length of the time-interval during which a physical machine **S** evolves to a final halting state $\sum_i c_i|1_H\rangle|s_{halt_j}\rangle|x_{i_1}, \dots, x_{i_n}\rangle$. And, unlike the case of classical computers, one cannot *look* inside the "computer-box"; for, any observation would generally destroy the superpositions that determine the quantum parallel configurations. Different tools have been proposed and discussed in order to overcome this special experimental difficulty. An ingenious method proposed by Feynman can be roughly illustrated as follows. One introduces an auxiliary quantum system **C**, called *the clock*, whose aim is keeping track of the time-evolution of the quantum system **S** that performs the computation (from the initial time to the time when the system **S** reaches a halting state). The states of the clock **C** are supposed to be entangled with the states of the system **S**. Hence, by performing on the clock a measurement that yields a discrete result $j$, one obtains that the state of **S** *collapses* into a corresponding state $|\psi_{j+1}\rangle = \mathtt{U}_j \dots \mathtt{U}_0|\psi_0\rangle$. In this way, any measurement on the clock does not destroy the superpositions representing the state of the quantum system that is performing the computation.

An interesting question concerns the possibility of a *universal abstract quantum computing machine* that could play the role of the universal Turing machine in classical computation. This question has a negative answer. As we have seen in Sect. 2.2, by trivial cardinality-reasons it is impossible to define all gates of a space $\mathscr{H}^{(n)}$ by means of a finite set of gates. As a consequence, no abstract quantum computing machine can be *perfectly universal*.

In spite of this negative result, one can usefully have recourse to the notion of *approximately universal gate system*, which is justified by the Shi- Aharonov Theorem (Theorem 2.4). Consider the gate-system

$$\mathfrak{G}^* = (\mathtt{I}^{(1)}, \mathtt{NOT}^{(1)}, \sqrt{\mathtt{I}}^{(1)}, \mathtt{T}^{(1,1,1)}).$$

As we have learnt in Sect. 2.2, for any gate $\mathtt{G}$ of a Hilbert space $\mathscr{H}^{(n)}$ and for any choice of a non-negative real number $\varepsilon$ there is a finite sequence of gates $(\mathtt{G}_1, \ldots, \mathtt{G}_u)$ (of $\mathscr{H}^{(n)}$) such that: 1) $(\mathtt{G}_1, \ldots, \mathtt{G}_u)$ is a circuit belonging to the family $\mathfrak{C}^{\mathfrak{G}^*}$; 2) for any vector $|\psi\rangle$ of $\mathscr{H}^{(n)}$, $\|\mathtt{G}|\psi\rangle - \mathtt{G}_1 \ldots \mathtt{G}_u|\psi\rangle\| \leq \varepsilon$.

Thus, the family $\mathfrak{C}^{\mathfrak{G}^*}$ has the capacity of approximating with arbitrary accuracy any possible gate. On this basis, the machine $\mathbf{AbQCM}^{\mathfrak{G}^*}$ can be reasonably represented as an *approximately universal abstract quantum computing machine*. Notice that all circuits in the family $\mathfrak{C}^{\mathfrak{G}^*}$ (hence all programs of $\mathbf{AbQCM}^{\mathfrak{G}^*}$) can be syntactically represented by means of formulas expressed in the language $\mathscr{L}_0$ of the sentential version of *holistic quantum computational logic*. Both $\mathfrak{C}^{\mathfrak{G}^*}$ and the set of all formulas of $\mathscr{L}_0$ are denumerable sets. At the same time, the set of all possible inputs and outputs of quantum computations is, obviously, non-denumerable. Unlike classical computations, quantum computations cannot be faithfully represented in a purely syntactical way (in the framework of a denumerable language). One of the basic tasks of quantum computational semantics is creating a link between the (denumerable) world of circuits and the (non-denumerable) world of possible inputs and outputs of quantum computations.

What can be said about the computational power of $\mathbf{AbQCM}^{\mathfrak{G}^*}$? One can easily realize that $\mathbf{AbQCM}^{\mathfrak{G}^*}$ is able to compute in an *exact* way all recursive numerical functions. For, any sequence of natural numbers can be represented as a register and any computation of a recursive function (applied to a register-input) can be represented as an appropriate combination of the "Boolean" gates (the negation and the Toffoli-gate). Thus, the machine $\mathbf{AbQCM}^{\mathfrak{G}^*}$ is able to compute whatever the universal Turing machine is able to compute. Is $\mathbf{AbQCM}^{\mathfrak{G}^*}$ able to compute anything else in the domain of natural numbers? As we have seen, the Hadamard-gate (which plays an essential role in quantum computation) seems to be hardly realizable (in a faithful way) by a classical probabilistic state-machine. But, of course, this argument is not sufficient to prove that abstract models of quantum computers go beyond the computational capacities of classical Turing machines. In order to show that quantum computation theories bring about a *refutation* of the Church-Turing thesis, we should provide an example of a non-recursive function $f$ that is, in principle, computable by an abstract quantum computing machine. As far as we know, no examples that have been proposed and discussed in the literature have found a definite approval of the scientific community.

## References


1. Dalla Chiara, M.L., Giuntini, R., Leporini, R., Sergioli, G.: Abstract quantum computing machines and quantum computational logics. Int. J. Quantum Inf. **14**(4), 1640019-1-15 (2016)
2. Deutsch, D.: Quantum theory, the church-turing principle and the universal quantum computer. Proc. R. Soc. A **400**, 97–117 (1985)
3. Deutsch, D., Barenco, A., Ekert, A.: Universality in quantum computation (1995). arXiv:quant-ph/9505018v1
4. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**, 467–488 (1982)
5. Feynman, R.P.: Quantum mechanical computers. Opt. News **11**, 11–20 (1985)
6. Fouchè, W., Heidema, J., Jones, G., Potgieter, P.H.: Deutsch's universal quantum turing machine (Revisited), 1–7 (2007). arXiv:quant-ph/0701108v1
7. Gudder, S.P.: Quantum automata: an overview. Int. J. Theor. Phys. **38**(9), 2261–2282 (1999)
8. Gudder, S.P.: Quantum computers. Int. J. Theor. Phys. **39**, 2151–2177 (2000)
9. Nishimura, H., Ozawa, M.: Perfect computational equivalence between quantum turing machines and finitely generated uniform quantum circuit families. Quantum Inf. Process **8**(1), 13–24 (2009)
10. Savage, J.E.: Models of Computation: Exploring the Power of Computing. Addison Wesley, Boston (1997)

# Chapter 8
# Ambiguity in Natural and Artistic Languages: A Quantum Semantic Analysis

## 8.1 Introduction

In the previous chapters we have seen how the mathematical formalism of quantum theory and of quantum information have inspired new forms of quantum semantics. Interestingly enough, some phenomena that had for a long time been regarded as strange and mysterious in the domain of physical objects appear instead quite natural and, in a sense, expected in the framework of some "human" conceptual domains, where *ambiguity*, *vagueness*, *holism*, and *contextuality* play an essential semantic role. Some characteristic ideas of the quantum-theoretic formalism have recently been applied to a number of fields that are far apart from microphysics: from economy to social and political sciences, from cognition and perception-theories to the semantics of natural and artistic languages.[1]

As is well known human perception and thinking seem to be essentially *synthetic*. We never perceive an object by *scanning* it point by point. We instead form right away a *Gestalt*, i.e. a global idea of it. Rational activity as well seems to be often based on *gestaltic patterns*. We need only think, for instance, of what happens in the case of chess games: strong players certainly must perform some rapid computations, but above all they must be able first to perceive a *Gestalt* of the position and then to assess by experience the probability of its different issues.[2]

In this chapter we will discuss the possibility of applying some basic concepts of the quantum computational semantics to a general theory of *vague possible worlds*. We will see how in this framework one can develop a formal representation of some characteristic features of musical languages. This approach will also allow us to understand some abstract reasons why a "metaphorical thinking" often plays an important role in the languages of art and sometimes even in the field of exact sciences.

---

[1] See, for instance, [1, 2, 7, 10].

[2] See [12].



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_8

## 8.2 Vague Possible Worlds and Metaphors

In the tradition of scientific thought metaphorical arguments have often been regarded as fallacious and dangerous. There is a deep logical reason that justifies such "suspicions". Metaphors and allusions are generally based on *similarity-relations*: when an idea $A$ is used as a metaphor for another idea $B$, the two ideas $A$ and $B$ are supposed to be similar with respect to something. And we know that similarity-relations are *weak* relations: they are reflexive and symmetric; but generally they are not transitive and they do not preserve the properties of the objects under investigation. If *Alice* is similar to *Beatrix* and *Alice* is clever, it is not guaranteed that *Beatrix* also is clever. Wrong extrapolations of properties from some objects to other similar objects are often used in rhetoric contexts, in order to obtain a kind of *captatio benevolantiae*. We need only think of the soccer-metaphors that are so frequently used by many politicians!

In spite of their possible "dangers", metaphors have sometimes played an important role even in exact sciences. An interesting example in logic is represented by the current use of the metaphor of *possible world*, based on a general idea that has been deeply investigated by Leibniz. In some situations possible worlds, which correspond to special examples of *semantic models*, can be imagined as a kind of "ideal scenes", where abstract objects behave as if they were playing a theatrical play. And a "theatrical imagination" has sometimes represented an important tool for scientific creativity, also in the search for solutions of logical puzzles and paradoxes. A paradigmatic case can be recognized in the discussions about a celebrated set-theoretic paradox, the *Skolem-paradox*. Consider an axiomatic version of set theory **T** (say, Zermelo–Fraenkel theory) formalized in (classical) first-order logic and assume that **T** is non-contradictory. By purely logical reasons, we know that **T** has at least one "strange" model $\mathscr{M}^*$, where both the domain and all its elements are denumerable sets. In this model $\mathscr{M}^*$ the *continuum* (the set $\mathbb{R}$ of all real numbers) seems to be, at the same time,

- denumerable, because everything is denumerable in $\mathscr{M}^*$;
- non-denumerable, because $\mathscr{M}^*$ must verify Cantor's theorem, according to which the continuum $\mathbb{R}$ is non-denumerable.

In order to "see" a possible way-out from this paradoxical conclusion, we can imagine an ideal scene where all actors are denumerable sets. Some actors are supposed to "wear a mask", playing the role of non-denumerable sets. As happens in real theatrical plays, characters and actors do not generally share the same properties. The actor who plays the role of Othello is not necessarily jealous himself! In the same way, a denumerable set can play the role of the non-denumerable continuum on the stage represented by the non-standard model $\mathscr{M}^*$. The Skolem-paradox is one of the possible examples that show us how a recourse to a "metaphorical thinking" may sometimes improve abstract imagination-capacities even in the field of exact sciences.

To what extent is "a logic of metaphors" possible? The quantum computational semantics seems to provide a useful tool for discussing this question. As we have seen in the previous chapters, the basic idea of this semantics is that the *meanings* of well-formed linguistic expressions can be formally represented as (pure or mixed) states of special quantum systems. Of course, like formulas, sequences of formulas also can be interpreted according to the quantum computational rules. As expected, a possible meaning of a sequence $(\alpha_1, \ldots, \alpha_n)$ of formulas will be a density operator $\rho_{(\alpha_1,\ldots,\alpha_n)}$ living in a Hilbert space $\mathscr{H}^{(\alpha_1,\ldots,\alpha_n)}$, whose dimension depends on the linguistic complexity of the formulas $\alpha_1, \ldots, \alpha_n$. In this framework one can naturally develop an abstract theory of *vague possible worlds*. Consider a pair

$$W = ((\alpha_1, \ldots, \alpha_n),\ \rho_{(\alpha_1,\ldots,\alpha_n)}),$$

consisting of a sequence of formulas and of a density operator that represents a possible meaning for our sequence. It seems reasonable to assume that $W$ describes a *vague possible world*, a kind of *abstract scene* where most events are characterized by a "cloud of ambiguities", due to quantum uncertainties. In some cases $W$ might be exemplified as a "real" scene of a theatrical play or as a vague situation that is described either in a novel or in a poem. And it is needless to recall how ambiguities play an essential role in literary works.

As a simple example, consider the following vague possible world:

$$W = ((\mathbf{Pab}), \rho_{(\mathbf{Pab})}),$$

where **Pab** is supposed to formalize the sentence "Alice is kissing Bob", while $\rho_{\mathbf{Pab}}$ corresponds to the pure state

$$|\Psi\rangle_{\mathbf{Pab}} = |\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0, 1\rangle + |1, 0\rangle) \otimes |1\rangle,$$

where $|\varphi\rangle$ lives in the space $\mathscr{H}^{(1)} = \mathbb{C}^2$, while $|\Psi\rangle_{\mathbf{Pab}}$ lives in the space $\mathscr{H}^{(4)} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Here each reduced state of $|\Psi\rangle_{\mathbf{Pab}}$ that describes the pair consisting of the two individuals *Alice* and *Bob* is an entangled Bell-state; consequently, the reduced states that describe the two subsystems *Alice* and *Bob* are two identical mixed states. In the context $|\Psi\rangle_{\mathbf{Pab}}$ *Alice* and *Bob* turn out to be indistinguishable: it is not determined "who is who" and "who is kissing whom". It is not difficult to imagine some "real" theatrical scenes representing ambiguous situations of this kind.

The quantum-theoretic formalism can be naturally applied to an abstract analysis of metaphors. Both in the case of natural languages and of literary contexts metaphorical correlations generally involve some allusions that are based on particular similarity-relations. Ideas that are currently used as possible metaphors are often associated with concrete and visual features. As observed by Aristotle, a characteristic property of metaphors is "putting things under our eyes".[3] Let us think, for instance, of a visual idea that is often used as a metaphor: the image of the sea,

[3] See Aristotle, *Meteorologica*, 357.

correlated to the concepts of immensity, of infinity, of obscurity, of pleasure or fear, of places where we may get lost and die.

The concept of quantum superposition can represent a natural and powerful semantic tool in order to represent the ambiguous allusions that characterize metaphorical correlations. Consider a quregister

$$|\psi\rangle = \sum_i c_i |\psi_i\rangle, \quad \text{where} \quad c_i \neq 0.$$

In such a case any $|\psi_i\rangle$ turns out to be *non-orthogonal to* $|\psi\rangle$. We have:

$$|\psi_i\rangle \not\perp |\psi\rangle$$

(i.e. the inner product of $|\psi_i\rangle$ and $|\psi\rangle$ is different from 0). And we know that the non-orthogonality relation $\not\perp$ represents a typical similarity-relation (which is reflexive, symmetric and generally non-transitive). Hence, in particular semantic applications, the idea $|\psi_i\rangle$ (which $|\psi\rangle$ alludes to) might represent a *metaphor* for $|\psi\rangle$, or vice versa.

## 8.3 A Quantum Semantics for Musical Languages

Musical languages represent an interesting field where the basic concepts of the quantum computational semantics can be applied in a natural way.[4] Any musical composition (say, a sonata, a symphony, a lyric opera,...) is, generally, determined by three elements:

- a *score*;
- a set of *performances*;
- a set of musical *thoughts* (or *ideas*), which represent possible *meanings* for the *musical phrases* written in the score.

While scores represent the syntactical component of musical compositions, performances are physical events that occur in space and time. From a logical point of view, we could say that performances are, in a sense, similar to *extensional meanings*, i.e. well determined systems of objects which the linguistic expressions refer to. Musical thoughts (or ideas) represent, instead, a more mysterious element. Is it reasonable to assume the existence of such ideal objects that are, in a sense, similar to the *intensional meanings* investigated by logic? Is there any danger to adhere, in this way, to a form of *Platonism*? When discussing semantic questions, one should not be "afraid" of Platonism. In the particular case of music, a composition cannot be simply reduced to a score and to a system of sound-events. Between a score

[4]See [4–6]. For some other applications of quantum ideas to a formal analysis of music see, for instance, [3, 8].

(which is a system of signs) and the sound-events created by a performance there is something intermediate, represented by the musical ideas that underlie the different performances. This is the abstract environment where normally live both composers and conductors, who are accustomed to study scores without any help of a material instrument.

Following the rules of the quantum computational semantics, *musical ideas* can be naturally represented as superpositions that ambiguously describe a variety of co-existent thoughts. Accordingly, we can write:

$$|\mu\rangle = \sum_i c_i |\mu_i\rangle,$$

where:

- $|\mu\rangle$ is an abstract object representing a musical idea that *alludes* to other ideas $|\mu_i\rangle$ (possible *variants* of $|\mu\rangle$ that are, in a sense, all co-existent);
- the number $c_i$ measures the "importance" of the component $|\mu_i\rangle$ in the context $|\mu\rangle$.

As happens in the case of composite quantum systems, musical ideas (which represent possible meanings of *musical phrases* written in a score) have an essential *holistic* behavior: the meaning of a global musical phrase determines the *contextual meanings* of all its parts (and not the other way around).

As an example, we can refer to the notion of *musical theme*. What exactly are musical themes? The term "theme" has been used for the first time in a musical sense by Gioseffo Zarlino, in his *Le istitutioni harmoniche* (1558), as a melody that is repeated and varied in the course of a musical work. Generally a theme appears in a musical composition with different "masks". In some cases it can be easily recognized even in its transformations; sometimes it is disguised and can be hardly discovered. Of course, a theme cannot be identified with a particular (syntactical) phrase written in the score; for, any theme essentially alludes to a (potentially) infinite set of possible variants. One is dealing with a vague musical idea that cannot be either played or written. At the same time, it is interesting to investigate (by scientific methods) the musical parameters that represent a kind of *invariant*, characteristic of a given theme. In different situations the relevant parameters may concern the melody or the harmony or the rhythm or the timbre.

The ambiguous correlations between a theme and its possible variants turn out to be exalted in the fascinating musical form that is called *Theme and Variations*. By using the superposition-formalism, we can represent the abstract form of a theme as follows:

$$|\mu\rangle = c_0|\mu_0\rangle + c_1|\mu_1\rangle + \cdots + c_n|\mu_n\rangle,$$

where:

- $|\mu_0\rangle$ represents the *basic theme* (a precise musical idea, written in the score).
- $|\mu_1\rangle, \ldots, |\mu_n\rangle$ represent the variations of $|\mu_0\rangle$.

- $|\mu\rangle$ represents an ambiguous musical idea that is correlated to the basic theme and to all its variations.

Of course the basic theme $|\mu_0\rangle$ has a privileged role, while the global theme $|\mu\rangle$ seems to behave like a kind of "ghost", which is somehow mysteriously present even if it appears hidden.

As is well known, an important feature of music is the capacity of *evoking* extra-musical meanings: subjective feelings, situations that are vaguely imagined by the composer or by the interpreter or by the listener, real or virtual theatrical scenes (which play an essential role in the case of lyric operas and of *Lieder*). The interplay between musical ideas and extra-musical meanings can be naturally represented in the framework of our quantum semantics, where extra-musical meanings can be dealt with as special examples of vague possible worlds. We can refer to the tensor product of two spaces

$$MSpace \otimes WSpace,$$

where:

- $MSpace$ represents the space of musical ideas $|\mu\rangle$;
- $WSpace$ represents the space of vague possible worlds, dealt with as special examples of abstract objects $|w\rangle$ that can be evoked by musical ideas.

Following the quantum-theoretic formalism, we can distinguish between *factorized* and *non-factorized* global musical ideas. As expected, a factorized global musical idea will have the form:

$$|M\rangle = |\mu\rangle \otimes |w\rangle.$$

But we might also meet "Bell-like" entangled global musical ideas, having the form:

$$|M\rangle = c_1(|\mu_1\rangle \otimes |w_1\rangle) + c_2(|\mu_2\rangle \otimes |w_2\rangle).$$

In the case of lyric operas and of *Lieder* musical ideas and vague possible worlds are, in fact, always *entangled* (in an intuitive sense). We need only think how some opera-librettos may appear naive and, in some parts, even funny, if they are read as pieces of theatre, separated from music. Also *Lieder*, whose texts have often been written by great authors (Goethe, Schiller, Heine, etc.) give rise to similar "entangled" situations. Generally a musical intonation of a given poem transforms the text into a new *global semantic object* that somehow absorbs and renews all meanings of the original literary work.

To what extent can some musical ideas be interpreted as *musical metaphors* for *extra-musical meanings*?[5] Is it possible to recognize any natural similarity-relations that connect ideal objects living in two different worlds that seem to be deeply far apart? In order to discuss this question it is expedient to refer to some interesting musical examples. Significant cases can be found in the framework of Schubert's

[5] For an interesting discussion of this problem see [11].

*Lieder*, where some musical figures and themes based on *sextuplets* often evoke images of water and of events that take place in water. Let us refer, for instance, to the celebrated *Lieder*-cycle "Die Schöne Müllerin" ("The Beautiful Miller's Daughter"). The story told in the poems of the German poet Wilhelm Müller is very simple. A young man, a miller, falls in love with the beautiful daughter of the mill's owner. But the girl refuses him and prefers a wild hunter. The young miller cannot overcome his love's pains and finally dies. During his *Wandern* (wandering) his only true friend is *der Bach*, the mill's brook that has a constant dialog with him. The flowing of the brook's water represents a clear poetic and musical metaphor for the flowing of time and for the changing feelings of the young lover.

When in the second *Lied* of the cycle, "Wohin" ("Whereto"), the miller meets the brook for the first time, singing "Ich hört' ein Bächlein rauschen wohl aus dem Felsenquell" ("I heard a brooklet rushing right out of the rock's spring"), the piano-accompaniment begins playing a sequence of sextuplets that will never be interrupted until the end of the *Lied*. Even the graphical shape of the sextuplets in the score suggests a natural similarity with a sinusoidal form representing the water's wave-movement (Fig. 8.1).

This creates a complex network of dynamic interactions among different elements:

- the musical thoughts that become "real" musical events during a performance of the *Lied*;
- the graphical representation of the musical phrases written in the score;
- the poetic metaphors, suggested both by the text and by the music, that allude to the flowing of time, to changing subjective feelings and to a mysterious fear for an uncertain future.

In many of his *Lieder* Schubert has often associated sextuplet-figures with images of water and with abstract ideas that refer to the flowing of time. Wonderful (and famous) examples are, for instance, the two *Lieder* "Auf dem Wasser zu singen" ("Singing on the water") and "Die Forelle" ("The Trout").

We will now consider another significant case that concerns Robert Schumann's compositions. We will refer to a very special musical theme that has been called "Clara's theme".[6] Clara is Clara Wieck, the great pianist and composer who has been the wife of Schumann. One is dealing with a somewhat mysterious theme that appears as a kind of "hidden thought" in different works by Schumann, by Clara herself and by Johannes Brahms, three great musicians whose lives have been in a sense "entangled" even outside the sphere of music.

Unlike the basic theme of a "Theme and Variations"- composition, Clara's theme cannot be identified with a precise musical phrase written in a particular score: many different variants of this theme have been recognized in different contexts, associated to different semantic connotations. It is well known that Schumann liked the use of "secret codes": special musical ideas whose aim was an ambiguous allusion to some extra-musical situations. The code of Clara's theme is based on the letters that occur in the name "CLARA", where "A" and "C" correspond to musical notes, while "L"

[6] See [9].


**Fig. 8.1** Sextuplets in the *Lied* "Wohin"

and "R" do not have any musical correspondence. In spite of this, one can create some interpolation, giving rise to different variants, all inspired by the name "Clara". An interesting example is the following note-sequence, which belongs to the *F* sharp minor-tonality:

**C♯ (B) A (G♯) A**

**[ C L A R A ]**

Like in the case of Schubert's sextuplets we can ask: is it reasonable to interpret Clara's theme as a kind of *musical metaphor*? Using a code (in a musical form) clearly suggests a reference to some extra-musical ideas. But what exactly is evoked by means of this special code? Of course, the aim cannot be a realistic description of the person denoted by the name "Clara" (a kind of *extensional reference* in logical sense). Let us consider some significant examples where Clara's theme has played an important role. In 1853 Clara Wieck composed the piano-piece *Variationen op. 20, über ein Thema von Robert Schumann, ihm gewidmet*, dedicated to her husband in occasion of his birthday. One year later Brahms wrote his own *Variations* on the same theme and dedicated his composition to Clara. Schumann's theme, which Clara and Brahms present exactly in the same way, is drawn from *Bunte Blätter*, a composition that Schumann wrote in 1841 (Fig. 8.2).

One can easily see that this "Schumann's theme" is based on one of the possible variants of Clara's theme (in $F$ sharp minor):

**C♯ C♯ C♯ (B) A (G♯) A.**

Is it possible to recognize, in a natural way, some extra-musical meanings, connected with Clara's personality, that might be correlated as vague allusions to the musical features of Schumann's theme? A reasonable conjecture seems to be the following: Clara is here evoked as a kind of "consoling figure", who inspires serene and peaceful feelings. It is not a chance that in one of the most famous Schumann's *Lieder*, "Widmung" ("Dedication"), the voice sings with the words of the poet Rückert "Du bist die Ruh, du bist der Frieden" ("You are the rest, you are the peace"), while in the piano conclusion the consoling theme of Schubert's *Ave Maria*, which is repeated twice, suddenly appears as a somewhat hidden quotation. The hypothesis that a vague consolation-idea represents an important semantic connotation associated to Clara seems to be confirmed by some *Lieder* where Clara's theme can be easily recognized. Of course, metaphorical correlations that emerge in *Lieder* are often somewhat cryptic, also because musical metaphors turn out to be ambiguously interlaced with the poetic metaphors that are expressed in the literary text. An interesting example is represented by the eighth *Lied* ("Und wüssten's die Blumen") of the famous *Lieder*-cycle "Dichterliebe" Op. 48, based on Heine's poems. Clara's theme appears here at the very beginning of the first phrase sung by the voice. In the version "für mittlere und tiefe Stimme" (baritone and bass) we find the same tonality of Schumann's theme ($F$ sharp minor) and the same descending note-sequence that in this case reaches the tonic (Fig. 8.3).

The leading idea expressed by Heine's poem is the search for a consolation that might be offered by a friendly Nature:


**Fig. 8.2** Schumann’s theme


**Fig. 8.3** Und wüssten’s die Blumen

*Und wüssten’s die Blumen, die kleinen,*
*Wie tief verwundet mein Herz,*
*Sie würden mit mir weinen,*

*Zu heilen meinen Schmerz.*[7]

One first addresses the flowers that could "heilen meinen Schmerz", but then the same request is turned to the nightingales and to the golden stars:

*Sie kämen aus ihrer Höhe,*
*Und sprächen Trost mir ein.*[8]

And significantly enough the first three stanzas of Heine's poem are all set to music by means of one and the same musical phrase (based on Clara's theme) that is repeated three times.

We have seen how metaphorical correlations can be described, from an abstract point of view, as very special cases where ideas belonging to different conceptual domains are connected by means of vague allusions. The occurrence of a metaphor in a given context is generally characterized by a "cloud" of ambiguity and indetermination that can be naturally analyzed by using quantum-theoretic concepts. The strength of the quantum computational semantics depends on the fact that meanings are, in this framework, represented as relatively simple and cognitively accessible ideal objects that ambiguously allude to a potentially infinite variety of alternative ideas. We know that any pure state of a Hilbert space can be represented as a superposition of elements of infinitely many possible bases of the space. And we have seen (in Chap. 5) how any choice of a particular basis can be intuitively regarded as a possible *perspective* from which we are looking at the phenomena under investigation.

As is well known, semantic phenomena of ambiguity and vagueness have been investigated in the literature by a number of different approaches. In classical logical frameworks one has often referred to complex systems of possible worlds, where each particular world is characterized by sharp and deterministic features, according to the excluded-middle principle. This gives rise to a "multiplication of entities" that may represent a shortcoming from a cognitive point of view. More natural theories of vagueness have been developed in the framework of fuzzy logics. But what is generally missing in the standard many-valued semantics is the capacity of representing holistic aspects of meanings, which play an important role either in natural languages or in the languages of art. Of course, recognizing the advantages of a quantum semantics does not imply any "ideological" conclusion, according to which the quantum-theoretic formalism should have a kind of privileged position in the rich variety of semantic theories that have been proposed in the contemporary literature.

## References

1. Aerts, D., Sozzo, S.: Quantum entanglement in conceptual combinations. Int. J. Theo. Phys. **53**, 3587–3603 (2014)

[7] *If the little flowers knew / How deeply wounded is my heart, / They would weep with me, / to soothe my pain.*

[8] *They would come down from their height, /and speak words of comfort to me.*

2. Aerts, D., Gabora, L., Sozzo, S.: Concepts and their dynamics: a quantum-theoretic modeling of human thought. Top. Cogn. Sci. **5**(4), 737–772 (2013)
3. Butner, R.: Modelling tonal attraction: tonal hierarchies, interval cycles and quantum probabilities. Soft Comput. **21**(6), 1401–1419 (2017)
4. Dalla Chiara, M.L., Giuntini, R., Negri, E.: From quantum mechanics to music. Adv. Sci. Lett. **1**(2), 169–178 (2008)
5. Dalla Chiara, M.L., Giuntini, R., Luciani, A.R., Negri, E.: From Quantum Information to Musical Semantics. College Publications, London (2012)
6. Dalla Chiara, M.L., Giuntini, R., Luciani, R., Negri, E.: A quantum-like semantic analysis of ambiguity in music. Soft Comput. **21**(6), 1473–1481 (2017)
7. Haven, E., Khrennikov, A.: Quantum Social Science. Cambridge University Press, Cambridge (2013)
8. Putz, V., Svozil, K.: Quantum music. Soft Comput. **21**(6), 1467–1471 (2017)
9. Sams, E.: The Songs of Robert Schumann. Faber (1993)
10. Sergioli, G., Santucci, E., Didaci, L., Miszczak, J., Giuntini, R.: A quantum-inspired version of the nearest mean classifier. Soft Comput. **22**(3), 691–705 (2018)
11. Spitzer, M.: Metaphors and Musical Thoughts. The University of Chicago Press, Chicago (2004)
12. Toraldo di Francia, G.: Deep Blue and the strategy of human thought. Found. Sci. **4**, 83–93 (1999)

# Chapter 9
# Quantum Information in the Foundational and Philosophical Debates About Quantum Theory

## 9.1 Information Interpretations of Quantum Theory

The intense investigations that have recently been developed in the field of quantum information and quantum computation have naturally stimulated new debates about foundational and philosophical questions of quantum theory. "Information interpretations", according to which quantum theory should be mainly regarded as a "revolutionary information theory" that has deeply changed some classical ideas about knowledge, have sometimes been opposed to more traditional "realistic views", according to which the pure states of the quantum-theoretic formalism should always "mirror" *objective properties* of physical systems that exist (or may exist) in the physical world.

One of the most influential defenders of an information interpretation of quantum theory is Anton Zeilinger, the Austrian physicist who has played a leading role in some important quantum experiments performed by scientific teams of the "Institute for Quantum Optics and Quantum Information" in Innsbruck and of the "Institute for Experimental Physics" in Vienna. The basic idea of Zeilinger's philosophical position is that we cannot have any direct access to what is usually called "reality", which can only be grasped by means of *images*, *ideas*, *thoughts* constructed on the basis of our experiences. All that we have at our disposal are *pieces of information*, *impressions*, *answers* to *questions* that have been formulated by us.[1] In this respect Zeilinger's general views seem to be close to Kant's basic ideas, according to which *knowledge* can only concern *phenomena*, while the ontological "things-in-themselves" (*noumena*) are inaccessible to human minds.

At the same time, the information interpretation of quantum theory can be also regarded as a new development of the "Copenhagen interpretation" that had been proposed by Niels Bohr between the Twenties and the Thirties (of the last Century). And it is not by chance that in his book "Einstein's Schleier" ("Einstein's Veil") Zeilinger begins his discussion about "information and reality" by quoting an

[1] See [24].

 
M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_9

assertion by Bohr: *it is wrong to think that the task of physics is to find out how Nature is. Physics concerns what we can say about Nature*.

As is well known, a core-idea of the Copenhagen interpretation is that quantum systems do not generally possess independent objective properties. What we call "quantum properties" are, in fact, *relations* with possible observers and measurement-apparatuses. The *collapse of the wave function-principle* has brought into light the role of observers, whose choices can, in some situations, determine which observable (from a system of pairwise incompatible observables) has an *actual* value, even in the case of physical systems that are far apart from the observers. And we have seen (in Chap. 3) how such subjective choices had worried Einstein, Podolsky and Rosen in their celebrated paradoxical argument.[2]

## 9.2 The Collapse-Problems

To what extent shall the collapse of the wave function be necessarily performed by a human intelligence? This question had been deeply discussed in the early debates about the foundations of quantum theory, giving rise to some interpretations that have been regarded as "strongly idealistic". A significant example is represented by the position of the scientist who has introduced the collapse-principle as an axiom of quantum theory: John von Neumann.[3] The basic idea of von Neumann's interpretation is that the collapse of the wave function does not represent a physical phenomenon, but rather an "epistemic event" that occurs inside the observer's consciousness; and this provides a solution for the quantum measurement-paradox. Consider a composite system $\mathbf{S} + \mathbf{A}$ (consisting of a quantum system $\mathbf{S}$ and of an apparatus $\mathbf{A}$ that performs a measurement of an observable $O$ on $\mathbf{S}$) and suppose that the initial state of this system is pure. As we have seen (in Chap. 1), Schrödinger's equation and the collapse-principle generally predict two different time-evolutions for the initial state of our system. While the Schrödinger-evolution may leave indeterminate the value of $O$ for $\mathbf{S}$, the collapse-principle transforms the initial state of the composite system into a factorized state that assigns a definite value to $O$. According to von Neumann this logical conflict can be solved by interpreting the collapse-phenomenon as a purely epistemic event: the observer's consciousness is something external with respect to the physical system $\mathbf{S} + \mathbf{A}$ and it is not necessary to assume that human minds are submitted to the laws of quantum physics.

Such an "idealistic" solution of the measurement-problem has raised a number of objections in the physical community. Interestingly enough, however, von Neumann's interpretation can be transformed into a purely logical argument, which turns

---

[2] An "extreme" form of informational approach to quantum theory has been proposed by the so called "Quantum Bayesianism" (briefly, "QBism"), developed on the lines of a subjectivistic interpretation of probability theory (Ramsey, de Finetti). The basic idea of "quantum bayesianists" is that quantum states have to be interpreted as "belief-degrees" of particular epistemic agents. See, for instance, [9].

[3] See [22, 23].

out to be independent of the philosophical discussions about the dilemma "idealism or realism?". The basic idea of a possible "logical reinterpretation" of von Neumann's solution can be sketched as follows. Any application of the collapse-principle shall refer to an apparatus **A** that is *external* with respect to the quantum systems under consideration. Such an apparatus turns out to have a kind of *metatheoretic role* with respect to the universe of the *object-systems* investigated by the theory. Of course, nothing forbids us to consider the apparatus itself as a particular quantum object, by studying the behavior of $\mathbf{S}+\mathbf{A}$. In such a case, however, in order to apply the collapse-principle to $\mathbf{S}+\mathbf{A}$, we shall use a different apparatus $\mathbf{A}'$ that should be *external* with respect to the universe of discourse (which $\mathbf{S}+\mathbf{A}$ belongs to). One obtains in this way a kind of *regressus ad infinitum* that allows us to locate where we want the dividing line between *object-physical systems* and *metatheoretic systems*. Such a representation of quantum phenomena seems to be close to some situations that arise in logic as a consequence of the celebrated *limitative theorems* (proved by Gödel and by Tarski). The quantum uncertainty about the value of the observable $O$ (value that is not decided by the pure state predicted by Schrödinger's equation and can be decided by collapse of the wave function by means of an external apparatus $\mathbf{A}'$) can be compared to the logical *status* of a sentence asserting the consistency of a given mathematical theory (sentence that is *undecidable* in the framework of the theory and becomes *decidable* in a convenient metatheory).

In more recent times different interpretations of the collapse-principle have been proposed and developed. One has pointed out that measurement-procedures do not necessarily require a human awareness. What is really important is the role of a measuring apparatus (associated to a basis of a given Hilbert space) that detects a final result. All these questions have, of course, a bearing for quantum computation theory. As we have seen (in Chap. 7) quantum computers represent special examples of quantum systems, whose states finally *collapse*, giving rise to the *reading* of a given computation-output; and such a "reading" is not necessarily bound to a human consciousness. The apparatus itself or a "robot-reader" can perfectly do the required job. The physical interaction that occurs between a quantum system **S** and an apparatus **A** (which is performing a measurement on **S**) can be naturally described as a special example of an interaction between a micro-system and its macro-environment. During the last decades such interactions have been intensively investigated in the framework of the so called "decoherence theories".[4]

## 9.3 Determinism, Indeterminism, Realism

In contrast with the "Copenhagen-spirit" and with all information interpretations of quantum theory, other approaches have defended the thesis according to which, in spite of the apparently strange behavior of the quantum world, quantum theory is compatible with a "realistic conception" of physics.

[4] See, for instance, [25].

Many debates about the dilemma “realism or anti-realism?” have often referred to the historical controversy between Einstein and Bohr. The discussions between these two great physicists had animated their extraordinary relationship for many years, since the Solvay-congress (1927) until the early Forties, when both Einstein and Bohr (who had left Europe under the Nazi domain) were working at the “Institute for Advanced Study” in Princeton. And, significantly enough, their deeply divergent ideas about some basic questions concerning physics and philosophy never cast shadows on their warm friendship, their sense of humour and their open-minded critical attitude. As is well known, Einstein never accepted the essential *indeterminism* of the quantum world, which represents instead a characteristic feature of quantum theory according to Bohr’s views. To Einstein’s famous claim “I cannot believe that God plays dice!” (so often repeated in the philosophical debates about quantum theory) Bohr’s ironical response had been “Don’t give orders to God!”.

Is there any natural correlation between a *deterministic* conception of the physical world and a *realistic* philosophical position? Apparently, one is dealing with two different assumptions that are characterized by different logical properties. While *determinism* admits precise scientific explanations, *realism*, instead, seems to be a more vague and nebulous philosophical concept, which has been associated to a number of somewhat ambiguous interpretations.[5]

What does it mean that a given physical theory **T** (say, classical particle mechanics or special relativity or quantum mechanics) is *deterministic* or *indeterministic*? A reasonable answer to this question (which seems to be in agreement with what is generally accepted by the scientific community) can be formulated as follows.

**T** *is a deterministic physical theory iff for any physical system* **S** *(which belongs to the universe of systems investigated by* **T**) *and for any possible pure state* **s** *(which represents a maximal information about* **S**) **s** *decides all relevant physical events X that may occur to* **S** *(when* **S** *is in the state* **s***). In other words,* **s** *determines whether X holds for* **S** *or X does not hold for* **S**.[6]

Accordingly, physical determinism seems to be strongly connected with the validity of a classical logical principle: the semantic *“tertium non datur!”*. Probability-values (different from the two extreme values 0 and 1) do not play any role for the pure states of a deterministic theory. In such a case “God does not play dice!” according to Einstein’s desire. Of course, this idea of determinism does not forbid successful applications of probability theory in the framework of deterministic theories. In such cases, however, non-trivial probability-values only concern proper mixtures, which can always be interpreted as “imperfect” pieces of information due to human ignorance.

---

[5]For an interesting discussion about the possibility of “realistic” interpretations of quantum theory see, for instance, [21].

[6]It is worth-while noticing that this definition of *deterministic theory* corresponds to a form of *determinism* that is sometimes called “static”. By “dynamic determinism” one usually means the idea according to which the dynamic equations of the theory under consideration determine for any pure state $\mathbf{s}(t)$ (representing the state of a system **S** at time $t$) the pure state $\mathbf{s}(t')$ of **S** at any other time $t'$ (where $t < t'$ or $t' < t$). In this sense one can say that Schrödinger’s equation guarantees a form of *probabilistic dynamic determinism* for quantum theory.

While classical particle mechanics or special relativity can be naturally represented as important examples of deterministic theories, quantum theory (according to its standard axiomatization) is clearly non-deterministic. We know that, due to the uncertainty-principles, *no pure state* $|\psi\rangle$ *of a quantum system* **S** *can decide all relevant physical events that may occur to* **S**.

A possible way-out from the essential indeterminism of quantum theory had been discussed by Einstein, Podolsky and Rosen in their celebrated article. As we have seen (in Chap. 3), the basic aim of the paper was proving (by a contradiction-argument) that *quantum mechanics is a physically incomplete theory*, whose pure states cannot represent *maximal pieces of information* about quantum objects.[7]

To what extent is a *deterministic completion* of quantum theory logically possible, since the uncertainty-principles are theorems of the theory? The most serious attempts to restore determinism in quantum theory have been proposed by the *hidden-variable approaches*, whose basic ideas can be sketched as follows.[8]

(1) Quantum theory is a physically incomplete theory, whose pure and mixed states only provide statistical predictions (as happens in the case of classical statistical mechanics).
(2) It is possible to add to quantum theory a set $\Lambda$ of parameters (*hidden variables*) in such a way that:
   (2.1) for every pure quantum state $|\psi\rangle$ there exists a dichotomic (*dispersion-free*) state $(|\psi\rangle, \lambda)$ (with $\lambda \in \Lambda$), which *decides* all events that may occur to the physical system **S** described by $(|\psi\rangle, \lambda)$;
   (2.2) the statistical predictions of standard quantum theory shall be recovered by averaging over these dichotomic states;
   (2.3) the algebraic structures determined by the events that may occur to quantum systems shall be preserved in the hidden-variable extensions.

The hidden-variable theories based on assumptions (1) and (2) are usually called "non-contextual", because they require the existence of a unique hidden-variable space $\Lambda$ that determines all dispersion-free states. A weaker position is represented by the so called "contextual hidden-variable theories", according to which the choice of $\Lambda$ may depend on the choice of the observables that are considered in particular situations.

The logical possibility of a non-contextual hidden variable theory (satisfying conditions (1) and (2)) has been put in question by some important mathematical theorems that have been called "no-go theorems".[9] In the late Sixties (of the last Century) Kochen and Specker published a series of articles developing a purely logical argument for a *no-go theorem*, whose proof is based on a variant of Birkhoff and von Neumann's quantum logic, called *partial classical logic* (**PCL**).[10] While

[7] See [8].

[8] See [4–6, 13].

[9] The first *no-go theorem* has been proved by von Neumann. His proof, however, is based on some general assumptions that have later been considered too strong.

[10] See [16, 17].

Birkkhoff and von Neumann's quantum logic (as well as *abstract quantum logic*) are *total logics* in the sense that *meanings* of sentences are always defined in any semantic model, the molecular sentences of **PCL** may be semantically undefined. The crucial relation in the semantics of **PCL** is represented by a *compatibility-relation* that may hold between the meanings of two sentences. As expected, from an intuitive point of view, two sentences $\alpha$ and $\beta$ are supposed to have *compatible meanings* if and only if $\alpha$ and $\beta$ can be simultaneously tested for a quantum system. Models of **PCL** are special kinds of algebraic models, based on *partial Boolean algebras*, where the operations *infimum* and *supremum* are only defined for pairs of compatible elements.[11] One can prove that for any quantum system **S** (with associated Hilbert space $\mathscr{H}_{\mathbf{S}}$) the set $\mathscr{P}(\mathscr{H}_{\mathbf{S}})$ of all projections of $\mathscr{H}_{\mathbf{S}}$ (representing the set of all possible sharp events that may occur to **S**) can be naturally structured as a special example of a partial Boolean algebra.

The *no-go theorem* proved by Kochen and Specker asserts that:

*All quantum systems* **S**, *whose associated Hilbert space* $\mathscr{H}_{\mathbf{S}}$ *has a dimension greater than 2, do not admit dichotomic states* $(|\psi, \lambda\rangle)$ *that satisfy conditions* (1) *and* (2).

As a consequence, one can conclude that non-contextual hidden variable theories are logically incompatible with standard quantum theory. Interestingly enough, these investigations have brought into light a deep logical connection between the two following questions[12]:

(I) is quantum theory compatible with a non-contextual hidden-variable theory?
(II) Does **PQL** satisfy the metalogical "Lindenbaum-property"? In other words, can any non-contradictory set $T$ of sentences of **PQL** be extended to a *logically complete* set $T'$ (such that for any sentence $\alpha$ of **PQL**, either $\alpha \in T'$ or $\neg\alpha \in T'$)?

At the same time, Kochen and Specker's theorem does not forbid the logical possibility of contextual hidden-variable theories. From an intuitive point of view, however, *contextuality-assumptions* seem to be somewhat far from the "spirit" of a deterministic conception of physics.

Besides the logical incompatibilities shown by the *no-go theorems*, other difficulties for the hidden-variable approaches have emerged at an experimental level. Some important optical experiments (performed in the Eighties by a team of physicists of the "Institut d'Optique Théorique et Appliquée" in Paris) have confirmed the statistical predictions of standard quantum theory against the corresponding statistical predictions that can be derived in the framework of non-contextual hidden-variable theories.[13]

While the advocates of the hidden-variable approaches have been inspired by Einstein's views and by the thesis defended in the EPR-paper, Einstein himself did not adhere to any hidden-variable program. During the last period of his life his main

[11] For the concept of *partial Boolean algebra* see Definition 10.9 (in the *Mathematical Survey* of Chap. 10).

[12] See [13].

[13] See [1–3].

interests and efforts were devoted to a more general project: the creation of a *unified field theory*. And we know that he died without accomplishing his ambitious project.

Deterministic conceptions of physics have often been associated with "realistic" philosophical positions; although *determinism* and *realism* are, clearly, two independent ideas. A position that appears at the same time "strongly realistic" and "strongly indeterministic" has recently been defended by a scientist who has played a leading role in quantum computation theory: David Deutsch. His approach represents a development of the *many-worlds theories*, which have proposed a very peculiar interpretation of quantum superpositions.[14] As we have seen (in Chap. 1), according to the standard interpretation of the quantum formalism, any superposition $|\psi\rangle = \sum_i c_i|\varphi_i\rangle$ (where every amplitude $c_i$ is different from 0) can be intuitively regarded as a description of a "cloud of potentialities". Each superposition-component $|\varphi_i\rangle$ corresponds to a possible *state of affairs* that becomes *actual*, if the physical system described by $|\psi\rangle$ interacts with a measuring apparatus (or, more generally, with an environment) that gives rise to a collapse:

$$\sum_i c_i|\varphi_i\rangle \quad \mapsto_M \quad |\varphi_i\rangle.$$

The many-worlds theories assert, instead, that all superposition-components $|\varphi_i\rangle$ describe *real* physical objects that live in different parallel universes; in the same way as the superpositions that describe different *computational paths* of a quantum computer perform, at the same time, "real" computations in parallel. There is no *collapse* that transforms *potential* states of affairs into *actual* ones, because all *quantum possibilities* are equally *real*. The world turns out to be split into different alternative worlds and such a splitting concerns even the observers. Consider, for instance, the case of the Mach–Zehnder interferometer. As we have seen (in Chap. 2), all photons that have entered into the interferometer-box through the first beam-splitter have an indeterminate trajectory: each photon seems to behave as if it could simultaneously go along the **x**-direction and along the **y**-direction. However, if an observer (say, $Alice$) performs a measurement inside the box, the superposition disappears and each photon is detected either along the **x**-direction or along the **y**-direction (and "or" corresponds here to an *exclusive disjunction*). According to the many-worlds interpretation, instead, both photon-trajectories (along the **x**-direction and along the **y**-direction) are equally real. Consequently, also the observer ($Alice$) shall be split into two different observers: $Alice_{\mathbf{x}}$ and $Alice_{\mathbf{y}}$. While $Alice_{\mathbf{x}}$ will "see" the photon travelling along the **x**-direction, $Alice_{\mathbf{y}}$ will "see" the photon travelling along the **y**-direction. All human beings have, in fact, a number of different "counterparts", living in different universes. Such a strange "multiplication of entities", which apparently contradicts Ockham's "razor-principle" ("entia non sunt multiplicanda praeter necessitatem") has naturally raised a number of objections of the scientific community. Another difficulty is due to the fact that the many-worlds theories cannot be

[14] See [7].

either confirmed or refuted by experimental evidence: $Alice_{\mathbf{x}}$ will never meet her counterpart $Alice_{\mathbf{y}}$, who lives in a parallel universe.[15]

A completely different approach (which has raised a great attention) is the *dynamic reduction theory*, proposed in a series of articles by GianCarlo Ghirardi, Alberto Rimini and Tullio Weber.[16] This theory (often termed "GRW" in the physical jargon) is based on a stochastic and non-linear correction of Schrödinger's equation, where *dynamic evolutions* turn out to inglobe the casual irreversible transformations that are induced by measurement-procedures. This allows us to overcome the logical conflict between Schrödinger's equation and the collapse-principle, which gives rise to the measurement-paradox. The collapse-principle disappears as an independent axiom of quantum theory and a single equation turns out to govern all quantum dynamic processes.

A similar approach has been proposed by Roger Penrose,[17] who has often pointed out that the most unsatisfactory feature of the standard versions of quantum theory is the conflict between Schrödinger's equation and the collapse-principle. According to Penrose, one should try and solve this conflict in the framework of a new unified theory, where the collapse-phenomena might be explained as due to gravitational effects. However, unlike the case of the GRW-theory, Penrose's project has never been developed in a precise mathematical form.

Both the GRW-theory and Penrose's proposal have often been represented as based on a conception of the quantum world that is at the same time "indeterministic" and "realistic". One should notice, however, that the physical interest of these approaches is, in fact, independent of any philosophical assumption about realism.

Surprisingly enough, a number of foundational and philosophical debates about quantum theory have dealt with the concept of "realism" in a somewhat naive and rough way, in contrast with the rigorous analysis that has been devoted to the basic logical, mathematical and physical concepts of the theory. As observed by Bas van Fraassen, in this field many discussions about the dilemma "realism or anti-realism" seem to be inspired by a kind of "pre-Kantian" philosophical attitude.

Is it possible to assign precise meanings to "realistic assertions" in the framework of physical theories? Of course, it is quite improbable that scientists working in the physical community deny the existence of an *external world*. What physicists often call "Nature" cannot be reasonably represented as a mere "creation " of human minds. At the same time, the "external world" appears as a kind of *magma* that is not intrinsically organized as a system of sharply distinguished *material objects*. What physicists usually do in their experimental activity is *isolating* some special fragments of such a "magmatic reality", by choosing some relevant parameters (*observables*), which can

[15] One can recognize some significant similarities between the many-worlds interpretations and the *consistent-histories approaches* to quantum mechanics. These latter theories, however, are not necessarily bound to the strong ontological assumptions that characterize the many-worlds interpretations. See, for instance, [14, 15].

[16] See [10–12].

[17] See [19, 20].

be measured on the *physical systems* individuated by them.[18] On this basis, as a result of the interaction with some measuring apparatuses, they can assert that some physical systems (isolated from the original magna) have been *prepared* in some *experimental states*, which are determined by special sequences of measurement-outputs. Then, at a finer theoretic level, experimental states are associated to *abstract states*: special mathematical objects representing pieces of information in the mathematical formalism of a given theory. In this way, *experimental structures* are embedded into a theoretical framework. And it is well known that experiments cannot generally determine the choice of a "correct" theory. Different (even incompatible) theories can be *verified* by one and the same experimental evidence. The division of the world into sharply distinguished material objects seems to be only a "projection" of human experimental and theoretic constructions over an original magmatic reality. Asking "does a wave function mirror objective properties of some material entities living in the real world?" seems to be a somewhat naive question that does not admit any reasonable precise answer.

## 9.4 A "Quantum Logical Thinking" in Different Fields

In this book we have tried to show how the quantum-theoretic formalism (which in the early debates about quantum theory had often been described as "strange" and "potentially paradoxical") may have a universal value, giving rise to interesting applications even beyond the domain of microphysics.

The developments of quantum mechanics and of quantum information theory have led us to overcome a "classical attitude" both in physics and in logic. An interesting view, in this connection, has been recently proposed by Peter Mittelstaedt, the German physicist who has represented an important point of reference in the quantum-logical investigations. In his last book "Rational Reconstruction of Modern Physics" Mittelstaedt has observed:

*The three leading theories of modern physics, Special Relativity, General Relativity, Quantum Mechanics cannot be adequately understood as an increase of knowledge about various empirical facts. In contrast, the very progress of these transitions consists of a stepwise reduction of prejudices, i.e. of quite general hypothetical assumptions of classical mechanics, that can be traced back to the metaphysics of the 17th and 18th centuries. [....] The classical ontology assumes that there are individual objects* $S_i$ *and that these objects possess elementary properties* $P_\lambda$*. An elementary property* $P_\lambda$ *refers to an object such that either* $P_\lambda$ *or the counterproperty* $\overline{P_\lambda}$ *pertains to the system. [....] The strict postulates of classical ontology are neither*

[18] As is well known, the concept of *isolated physical system* is an *approximated* concept: all physical systems are, in fact, embedded in an environment and the borders between a system and its environment cannot be generally determined in a sharp way. The approximation involved in this particular case depends on the choice of the relevant parameters and by the *resolving power* of the instruments used in the measurement-procedures.

*both intuitive and plausible nor can they be confirmed and justified by experimental means.*[19]

Both classical physics and classical logic seem to be based on a kind of oversimplified representation of the *world* and of our *way of reasoning* about the world. Of course, this does not force us to abandon either classical physics or classical logic that preserve their validity in special theoretic domains where some "simplifications" turn out to be useful. As is well known, contemporary logical investigations have taught us that *pluralism* in logic and in science (in general) does not represent a "danger" for rationality. In the wide "population" of different logics, studied by logicians, classical logic still preserves a central role, representing also a useful metalogical tool.

A question that has often been discussed in connection with the logical problems of quantum theory concerns the compatibility between quantum logics and the mathematical formalism of quantum theory, based on classical logic. Is the quantum physicist bound to a kind of "logical schizophrenia"? At first sight the co-existence of different logics in one and the same theory may give a sense of uneasiness. However the splitting of the basic logical operators into different abstract operations with different meanings and uses is now a well accepted logical phenomenon that admits consistent descriptions. Classical logic and quantum logics turn out to apply to different sublanguages of quantum theory, that must be carefully distinguished.

We have seen (in Chaps. 4 and 5) how quantum computational logics have naturally emerged from the mathematical formalism of quantum computation theory. Unlike Birkhoff and von Neumann's quantum logic (and its further developments), in these logics the basic logical operators (connectives, quantifiers, epistemic operators) have *dynamic meanings* that correspond to different ways of processing pieces of quantum information. We have also seen how these logics can be naturally applied to some "human" conceptual domains, where ambiguity, vagueness, holism and contextuality play an essential role (natural languages, cognitive and social sciences, literature, music).

As happens in the case of many-valued and fuzzy logics, quantum computational logics provide a rigorous abstract framework that allows us to develop an *exact scientific analysis* for some *inexact* concepts and problems that play an important role in many fields. According to some traditional philosophical views, *ambiguity* and *holism* represent characteristic features of human thought that cannot be adequately analyzed in the framework of scientific theories, whose semantics is supposed to be essentially "sharp" and "analytical". Interestingly enough, fuzzy logics and quantum logics (in their different versions) have provided a significant bridge that might fill a gap between humanistic and scientific disciplines.

While *fuzziness*, *vagueness* and *ambiguity* have become an important object of scientific investigations, paradoxically enough an oversimplified dichotomic way of reasoning (which systematically avoids any shade or nuance) seems to be a winning trend in our present society. Even school-systems and academic institutions make too often recourse to simple *yes-no tests*, a kind of "caricature" of classical semantics,

[19]See [18].

in contrast with any search for a deeper critical thinking. We all know how nowadays the quick communications based on modern technologies have favoured such simple ways of reasoning, which may even influence political behaviors, possibly perturbing the rules of democracy. In this situation, trying to educate people to simple forms of “quantum thinking” might perhaps help us in the search for some useful social transformations.

## References

1. Aspect, A.: Experimental tests of Bell’s Inequalities with correlated photons. In: Pratesi, R., Ronchi, L. (eds.) Waves, Information and Foundations of Physics. A Tribute to Giuliano Toraldo di Francia on his 80th Birthday. Italian Physical Society, Bologna (1998)
2. Aspect, A., Grangier, P., Roger, G.: Experimental tests of realistic local theories via Bell’s theorem. Phys. Rev. Lett. **47**, 460–463 (1981)
3. Aspect, A., Grangier, P., Roger, G.: Experimental realization of Einstein-Podolosky-Rosen-Bohm Gedankenexperiment: a new violation of Bell’Inequalities. Phys. Rev. Lett. **49**, 91–94 (1981)
4. Bell, J.S.: On the problem of hidden variables in quantum mechanics. Rev. Mod. Phys. **38**, 447–452 (1966)
5. Beltrametti, E., Cassinelli, G.: The Logic of Quantum Mechanics. Encyclopedia of mathematics and its applications, vol. 15, Addison-Wesley, Cambridge (1981)
6. Bohm, D.: Quantum Theory. Prentice-Hall, Englewoods Cliffs (1951)
7. Deutsch, D.: The Fabric of Reality. Penguin Books, London (1997)
8. Einstein, A., Podolsky, B., Rosen, N.: Can quantum mechanical description of reality be considered complete? Phys. Rev. **47**, 777–780 (1935)
9. Fuchs, C., Mermin, D., Schack, R.: An introduction to QBism with an application to the locality of quantum mechanics. Am. J. Phys. **82**(8), 749–754 (2014)
10. Ghirardi, G., Rimini, A., Weber, T.: Unified dynamics for microscopic and macroscopic systems. Phys. Rev. **34 D**, 470–491 (1986)
11. Ghirardi, G., Rimini, A., Weber, T.: A general argument against superluminal transmission through the quantum mechanical measurement process. Lettere al Nuovo Cimento **27**, 293–298 (1980)
12. Ghirardi, G., Rimini, A., Weber, T.: A model for a unified quantum description of macroscopic and microscopic systems. In: Accardi, L., et al. (eds.) Quantum Probability and Applications. Springer, Berlin (1985)
13. Giuntini, R.: Quantum Logic and Hidden Variables. Bibliographisches Institut, Mannheim (1991)
14. Griffiths, R.B.: Consistent histories and the interpretation of quantum mechanics. J. Stat. Phys. **36**, 219–272 (1984)
15. Isham, C.J.: Quantum logic and the histories approach to quantum theory. J. Math. Phys. **35**, 2157–2185 (1994)
16. Kochen, S., Specker, E.P.: Logical structures arising in quantum theory. In: Addison, J., Henkin, L., Tarski, A. (eds.) The Theory of Models, pp. 177–189. North-Holland, Amsterdam (1965)
17. Kochen, S., Specker, E.P.: The problem of hidden variables in quantum mechanics. J. Math. Mech. **17**, 59–87 (1967)
18. Mittelstaedt, P.: Rational Reconstruction of Modern Physics. Springer, Heidelberg (2011)
19. Penrose, R.: The Emperor’s New Mind. Oxford University Press, Oxford (1990)
20. Penrose, R.: Shadows of the Mind. Oxford University Press, Oxford (1994)
21. van Fraassen, B.C.: Quantum Mechanics. An empiricist view. Clarendon Press, Oxford (1991)
22. von Neumann, J.: Mathematische Grundlagen der Quantenmechanik. Springer, Berlin (1932)

23. von Neumann, J.: Mathematical Foundations of Quantum Theory. Princeton University Press, Princeton (1996)
24. Zeilinger, A.: Einsteins Schleier. Verlag C. H. Beck oHG, München, Die neue Welt der Quantenphysik (2003)
25. Zurek, W.H.: Decoherence and the transition from quantum to classical - Revisited (2003). arXiv:quant-ph/0306072

# Chapter 10
# Mathematical Survey

## 10.1 Introduction

This chapter is devoted to a survey of the definitions for the basic mathematical concepts used in this book. We will first define the algebraic concepts that play an important role in the quantum-theoretic formalism and in the semantics of quantum logics. Then, we will introduce the notion of Hilbert space and we will define the Hilbert-space concepts that represent the main "mathematical characters" of quantum mechanics and of quantum information theory.

## 10.2 Algebraic Concepts

**Definition 10.1** (*Pre-ordered sets and partially ordered sets*) Let $\mathfrak{A} = (\mathbf{A}, R)$ be a structure where $R$ is a binary relation defined on $\mathbf{A}$.

- $\mathfrak{A}$ is called a *pre-ordered set* iff $R$ satisfies the following conditions:

(1) $\forall a \in \mathbf{A} : Raa$ (reflexivity);
(2) $\forall a, b, c \in \mathbf{A} : Rab \text{ and } Rbc \implies Rac$ (transitivity).

- $\mathfrak{A}$ is called a *partially ordered set* (briefly, *poset*) iff $\mathfrak{A}$ is a pre-ordered set where $R$ satisfies the condition:

$$\forall a, b \in \mathbf{A} : Rab \text{ and } Rba \implies a = b \text{ (antisymmetry).}$$

**Definition 10.2** (*Lattice*) A *lattice* is a structure

$$\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup),$$

where $\sqcap$ and $\sqcup$ are two binary operations that satisfy the following conditions for any $a, b \in \mathbf{A}$:



M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8_10

(1) $a \sqcap b = b \sqcap a$; $a \sqcup b = b \sqcup a$ (commutativity);
(2) $a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$; $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$ (associativity);
(3) $a \sqcap (a \sqcup b) = a$; $a \sqcup (a \sqcap b) = a$ (absorption).

One can prove that the lattice-operations $\sqcap$ and $\sqcup$ are idempotent:

$$\forall a \in \mathbf{A} : a \sqcap a = a \quad \text{and} \quad a \sqcup a = a.$$

A partial order relation $\sqsubseteq$ can be defined in any lattice $\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup)$ as follows:

$$\forall a, b \in \mathbf{A} : \ a \sqsubseteq b \ \text{ iff } \ a \sqcap b = a.$$

One can prove that for any $a, b \in \mathbf{A}$, $a \sqcap b$ and $a \sqcup b$ represent respectively the *infimum* and the *supremum* (of $a$ and $b$) with respect to the partial order $\sqsubseteq$. We have:

- $\forall a, b, c \in \mathbf{A} : c \sqsubseteq a \text{ and } c \sqsubseteq b \implies c \sqsubseteq a \sqcap b$;
- $\forall a, b, c \in \mathbf{A} : a \sqsubseteq c \text{ and } b \sqsubseteq c \implies a \sqcup b \sqsubseteq c$.

**Definition 10.3** (*Distributive lattice*) A *lattice* $\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup)$ is called *distributive* iff $\sqcap$ distributes over $\sqcup$ and $\sqcup$ distributes over $\sqcap$:

$$\forall a, b, c \in \mathbf{A} : a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c);$$

$$\forall a, b, c \in \mathbf{A} : a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c).$$

**Definition 10.4** (*Complete lattice and $\sigma$-complete lattice*) Let $\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup)$ be a lattice.

- $\mathfrak{A}$ is called *complete* iff for any $X \subseteq \mathbf{A}$ the infimum $\bigsqcap X$ and the supremum $\bigsqcup X$ belong to $A$. Thus, for any $a \in A$ we have:
  $\forall x \in X (a \sqsubseteq x) \implies a \sqsubseteq \bigsqcap X$; $\forall x \in X (x \sqsubseteq a) \implies \bigsqcup X \sqsubseteq a$.
- $\mathfrak{A}$ is called *$\sigma$-complete* iff for any denumerable subset $X$ of $\mathbf{A}$, the infimum $\bigsqcap X$ and the supremum $\bigsqcup X$ belong to $\mathbf{A}$.

**Definition 10.5** (*Bounded lattice*) A *bounded lattice* is a structure

$$\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup, \underline{0}, \underline{1}), \quad \text{where:}$$

(1) $(\mathbf{A}, \sqcap, \sqcup)$ is a lattice;
(2) $\underline{0}$ and $\underline{1}$ are special distinct elements that represents the *minimum* and the *maximum* with respect to the partial order $\sqsubseteq$. Thus:

$$\forall a \in A : \underline{0} \sqsubseteq a \quad \text{and} \quad a \sqsubseteq \underline{1}.$$

**Definition 10.6** (*Ortholattice*) An *ortholattice* is a structure

$$\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup, {}', \underline{0}, \underline{1}), \quad \text{where:}$$

(1) $\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup, \underline{0}, \underline{1})$ is a bounded lattice;
(2) $'$ is a 1-ary operation, called *orthocomplement* (or *orthocomplementation*), that satisfies the following conditions for any $a, b \in \mathbf{A}$:

  (2.1) $a'' = a$ (double negation);
  (2.2) $a \sqcap a' = \underline{0}$ (non-contradiction);
  (2.3) $a \sqcup a' = \underline{1}$ (excluded middle);
  (2.4) $a \sqsubseteq b \implies b' \sqsubseteq a'$ (contraposition).

**Definition 10.7** (*Orthomodular lattice*) An *orthomodular lattice* is an ortholattice

$$\mathfrak{A} = (\mathbf{A}, \sqcap, \sqcup, {}', \underline{0}, \underline{1})$$

that satisfies the *orthomodular property*:

$$\forall a, b \in \mathbf{A} : a \sqsubseteq b \implies b = a \sqcup (b \sqcap a').$$

**Definition 10.8** (*Boolean algebra*) A *Boolean algebra* is a distributive ortholattice.

Any Boolean algebra is an orthomodular lattice, but not the other way around.

**Definition 10.9** (*Partial Boolean algebra*) A *partial Boolean algebra* is a partial structure

$$\mathfrak{A} = (\mathbf{A}, \heartsuit, \underline{\sqcap}, \underline{\sqcup}, {}', \underline{0}, \underline{1}),$$

where $\heartsuit$ is a binary relation on $\mathbf{A}$ (called *compatibility*), $\underline{\sqcap}$ and $\underline{\sqcup}$ are two partial binary operations whose domain is $\heartsuit$, $\underline{0}$ and $\underline{1}$ are special distinct elements of $\mathbf{A}$. The following conditions are required:

(1) $\heartsuit$ is reflexive and symmetric;
(2) $\forall a \in \mathbf{A} : a \heartsuit \underline{0}$ and $a \heartsuit \underline{1}$;
(3) $\forall a, b, c \in \mathbf{A} : a \heartsuit b, \; a \heartsuit c, \; b \heartsuit c \implies (a \underline{\sqcap} b) \heartsuit c, \; (a \underline{\sqcup} b) \heartsuit c, \; a' \heartsuit b$;
(4) $\forall a, b, c \in \mathbf{A}$ : if $a \heartsuit b, \; a \heartsuit c, \; b \heartsuit c$, then the Boolean polynomials in $a, b, c$ form a Boolean algebra with minimum $\underline{0}$ and maximum $\underline{1}$. In other words, the set $\{a, b, c\}$ generates a Boolean algebra with respect to the operations $\underline{\sqcap}, \underline{\sqcup}, {}'$.

**Definition 10.10** (*Effect algebra*) An *effect algebra* is a partial structure

$$\mathfrak{A} = (\mathbf{A}, \boxplus, \underline{0}, \underline{1}),$$

where $\boxplus$ is a partial binary operation on $\mathbf{A}$, while $\underline{0}$ and $\underline{1}$ are special distinct elements of $\mathbf{A}$. When $\boxplus$ is defined for a pair $a, b \in \mathbf{A}$, we write: $\exists(a \boxplus b)$. The following conditions are required:

(1) $\exists(a \boxplus b) \implies \exists(b \boxplus a)$ and $a \boxplus b = b \boxplus a$ (weak commutativity);
(2) $\exists(b \boxplus c)$ and $\exists(a \boxplus (b \boxplus c)) \implies \exists(a \boxplus b)$ and $\exists((a \boxplus b) \boxplus c)$ and $a \boxplus (b \boxplus c) = (a \boxplus b) \boxplus c$ (weak associativity);

(3) For any $a \in \mathbf{A}$, there exists a unique $x$ such that $a \boxplus x = \underline{1}$ (strong excluded middle);
(4) $\exists(a \boxplus \underline{1}) \implies a = \underline{0}$ (weak consistency).

An *orthogonality relation* $\perp$, a partial order $\sqsubseteq$ and a generalized complement $'$ (which generally behaves as a fuzzy complement) can be defined in any effect algebra $\mathfrak{A} = (\mathbf{A}, \boxplus, \underline{0}, \underline{1})$ as follows:

- $\forall a, b \in \mathbf{A} : a \perp b$ iff $\exists(a \boxplus b)$;
- $\forall a, b \in \mathbf{A} : a \sqsubseteq b$ iff $\exists c \in \mathbf{A}[a \perp c$ and $b = a \boxplus c]$;
- $\forall a \in \mathbf{A} : a'$ is the unique element such that $a \boxplus a' = \underline{1}$.

**Definition 10.11** (*Group*) A *group* is a structure

$$\mathfrak{A} = (\mathbf{A}, +, -, \underline{0}),$$

where $+$ is a binary operation, $-$ is a unary operation, $\underline{0}$ is a special element. The following conditions hold:

(1) the operation $+$ is associative:

$$\forall a, b, c \in \mathfrak{A} : a + (b + c) = (a + b) + c;$$

(2) $\underline{0}$ is the *neutral element*:

$$\forall a \in \mathbf{A} : a + \underline{0} = a;$$

(3) for any $a \in \mathbf{A}$, $-a$ is the *inverse* of $a$:

$$a + (-a) = \underline{0}.$$

We abbreviate $a + (-b)$ by $a - b$.

An *abelian group* is a group where the operation $+$ is commutative:

$$\forall a, b \in \mathbf{A} : a + b = b + a.$$

**Definition 10.12** (*Ring*) A *ring* is a structure

$$\mathfrak{A} = (\mathbf{A}, +, \cdot, -, \underline{0})$$

that satisfies the following conditions:

(1) $\mathfrak{A} = (\mathbf{A}, +, -, \underline{0})$ is an Abelian group;
(2) the operation $\cdot$ is associative:

$$\forall a, b, c \in \mathbf{A} : a \cdot (b \cdot c) = (a \cdot b) \cdot c;$$

(3) the operation $\cdot$ distributes over $+$ on both sides:

$$\forall a, b, c \in \mathbf{A} : a \cdot (b + c) = (a \cdot b) + (a \cdot c) \ \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

A *commutative ring* is a ring in which the operation $\cdot$ is commutative.

**Definition 10.13** (*Ring with unity*) A *ring with unity* is a structure

$$\mathfrak{A} = (\mathbf{A}, \ +, \ \cdot, \ -, \ \underline{0}, \underline{1}), \quad \text{where:}$$

(1) $\mathfrak{A} = (\mathbf{A}, \ +, \ \cdot, \ -, \ \underline{0})$ is a ring;
(2) $\underline{1}$ is a special element that is the neutral element for the operation $\cdot$ . Thus:

$$\forall a \in \mathbf{A} : a \cdot \underline{1} = a.$$

A ring with unity is called *non-trivial* iff $\underline{0} \neq \underline{1}$.

**Definition 10.14** (*Division ring*) A *division ring* is a non-trivial ring with unity $\mathfrak{A} = (\mathbf{A}, \ +, \ \cdot, \ -, \ \underline{0}, \underline{1})$ such that any non-zero element is *invertible* with respect to the operation $\cdot$. In other words:

$$\forall a \in \mathbf{A} : \ a \neq \underline{0} \implies \exists b \in \mathbf{A}(a \cdot b = \ b \cdot a = \underline{1}).$$

**Definition 10.15** (*Field*) A *field* is a commutative division ring.

Both the set $\mathbb{R}$ of the real numbers and the set $\mathbb{C}$ of the complex numbers give rise to a field. An example of a genuine division ring (where $\cdot$ is not commutative) is given by the set of the quaternions.

## 10.3 Hilbert-Space Concepts

Before introducing the concept of *Hilbert space* we will first recall the definition of *vector space*.

**Definition 10.16** (*Vector space*) A *vector space* over a division ring $\mathfrak{A} = (\mathbf{A}, \ +, \ \cdot, \ -, \ \underline{0}, \underline{1})$ is a structure

$$\mathscr{V} = (\mathbf{V}, +, \ -, \ \mathbf{0})$$

that satisfies the following conditions:

(1) $\mathscr{V} = (\mathbf{V}, +, \ -, \ \mathbf{0})$ (the *vector structure*) is an Abelian group, where $\mathbf{0}$ (the *null vector*) is the neutral element;
(2) for any element $a \in \mathbf{A}$ (called *scalar*) and any vector $\mathbf{v} \in \mathbf{V}$, $a\mathbf{V}$ (called the *scalar product* of $a$ and $\mathbf{v}$) is a vector in $\mathbf{V}$. The following conditions hold for any $a, b \in \mathbf{A}$ and for any $\mathbf{u}, \mathbf{v} \in \mathbf{V}$:

(2.1) $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + b\mathbf{v}$;[1]
(2.2) $(a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$;
(2.3) $a(b\mathbf{v}) = (a \cdot b)\mathbf{v}$;
(2.4) $\underline{1}\mathbf{v} = \mathbf{v}$.

We can now introduce the notion of *pre-Hilbert space*. Hilbert spaces are then defined as special examples of pre-Hilbert spaces. For the sake of simplicity, we will always refer to pre-Hilbert spaces and to Hilbert spaces whose division ring is either the field of the real numbers or the field of the complex numbers. By adopting Dirac's notation, the vectors of pre-Hilbert spaces and of Hilbert spaces will be indicated by $|\psi\rangle, |\varphi\rangle, |\chi\rangle, \ldots$ .

**Definition 10.17** (*Pre-Hilbert space*) Let $\mathfrak{A} = (\mathbf{A}, +, \cdot, -, \underline{0}, \underline{1})$ be either the real or the complex field. A *pre-Hilbert space* over $\mathfrak{A}$ is a vector space

$$\mathscr{H} = (\mathbf{V}_{\mathscr{H}}, +, -, \mathbf{0}),$$

equipped with an *inner product*, a map that associates to any pair of vectors $|\psi\rangle$ and $|\varphi\rangle$ of $\mathbf{V}_{\mathscr{H}}$ a scalar $\langle\psi \mid \varphi\rangle$ of the field $\mathfrak{A}$. The following conditions hold for any $|\psi\rangle, |\varphi\rangle \in \mathbf{V}_{\mathscr{H}}$ and any $a \in \mathbf{A}$:

(1) $\langle\psi \mid \psi\rangle \geq 0$;
(2) $\langle\psi \mid \psi\rangle = 0$ iff $|\psi\rangle = \mathbf{0}$;
(3) $\langle\psi \mid a\varphi\rangle = a\langle\psi \mid \varphi\rangle$;
(4) $\langle\psi \mid \varphi + \chi\rangle = \langle\psi \mid \varphi\rangle + \langle\psi \mid \chi\rangle$;
(4) $\langle\psi \mid \varphi\rangle = \langle\varphi \mid \psi\rangle^*$, where $^*$ is the identity if $\mathfrak{A}$ is the real field and the complex conjugation if $\mathfrak{A}$ is the complex field.

The inner product permits one to generalize some geometrical notions of ordinary 3-dimensional spaces.

**Definition 10.18** (*Norm of a vector*) The norm $||\ |\psi\rangle\ ||$ of a vector $|\psi\rangle$ is the number $\sqrt{\langle\psi \mid \psi\rangle}$.

Note that the norm of any vector is a real number greater than or equal to 0.

A *unit vector* is a vector $|\psi\rangle$ such that $||\ |\psi\rangle\ || = 1$.

Two vectors $|\psi\rangle$ and $|\varphi\rangle$ are called *orthogonal* iff $\langle\psi \mid \varphi\rangle = 0$.

A set of vectors is called *orthonormal* iff its elements are pairwise orthogonal unit vectors.

In any pre-Hilbert space $\mathscr{H}$ the norm $||\ .\ ||$ induces a metric $d$:

$$\forall|\psi\rangle, |\varphi\rangle \in \mathbf{V}_{\mathscr{H}} : d(|\psi\rangle, |\varphi\rangle) = ||\ |\psi\rangle - |\varphi\rangle\ || .$$

We say that a sequence $\{|\psi_i\rangle\}_{i\in\mathbb{N}}$ of vectors of a pre-Hilbert space $\mathscr{H}$ *converges* to a vector $|\psi\rangle$ of $\mathscr{H}$ iff $lim_{i\to\infty}\ d(|\psi_i\rangle, |\psi\rangle) = 0$. In other words,

[1]Since no confusion is possible, it is customary to use the same symbol + for the vector-sum and for the ring-sum.

$$\forall \varepsilon \in \mathbb{R}^+ \exists n \in \mathbb{N}\, \forall k > n : d(|\psi_k\rangle, |\psi\rangle) < \varepsilon.$$

A *Cauchy sequence* is a sequence $\{|\psi_i\rangle\}_{i \in \mathbb{N}}$ of vectors of $\mathscr{H}$ such that

$$\forall \varepsilon \in \mathbb{R}^+ \exists n \in \mathbb{N}\, \forall h > n\, \forall k > n : d(|\psi_h\rangle, |\psi_k\rangle) < \varepsilon.$$

It is easy to see that whenever a sequence $\{|\psi_i\rangle\}_{i \in \mathbb{N}}$ converges to a vector $|\psi\rangle$ of $\mathbf{V}_{\mathscr{H}}$, then $\{|\psi_i\rangle\}_{i \in \mathbb{N}}$ is a Cauchy sequence. The crucial question is the converse one: *which are the pre-Hilbert spaces in which every Cauchy sequence converges to an element of the space?*

**Definition 10.19** (*Metrically complete pre-Hilbert space*) A pre-Hilbert space $\mathscr{H}$ with inner product $\langle . \mid . \rangle$ is *metrically complete* with respect to the metric $d$ induced by $\langle . \mid . \rangle$ iff every Cauchy sequence of vectors in $\mathscr{H}$ converges to a vector in $\mathscr{H}$.

On this basis we can finally define the notion of Hilbert space.

**Definition 10.20** (*Hilbert space*) A *Hilbert space* is a metrically complete pre-Hilbert space.

A *real (complex) Hilbert space* is a Hilbert space whose division ring is the real field (the complex field).

Since the set of vectors of a Hilbert space $\mathscr{H}$ has a group-structure, any finite sum of vectors of $\mathscr{H}$ is a vector of $\mathscr{H}$. When $|\psi\rangle = a_1|\psi_1\rangle + \ldots + a_k|\psi_k\rangle$, we say that $|\psi\rangle$ is a *superposition* (or a *linear combination*) of $|\psi_1\rangle, \ldots, |\psi_k\rangle$, with scalars $a_1, \ldots, a_k$ . Instead of $a_1|\psi_1\rangle + \ldots + a_k|\psi_k\rangle$ we also write: $\sum_{i \in I} a_i|\psi_i\rangle$, where $I = \{1, \ldots, k\}$.

If $I$ is an infinite set of indexes, the superposition $\sum_{i \in I} a_i|\psi_i\rangle$ does not generally exist in $\mathscr{H}$. One can prove that the expression $\sum_{i \in I} a_i|\psi_i\rangle$ represents a vector $|\psi\rangle$ of $\mathscr{H}$ iff the set of vectors $\{a_i|\psi_i\rangle\}_{i \in I}$ satisfies the following *convergence-condition*: $\forall \varepsilon \in \mathbb{R}^+$ there exists a finite $J \subseteq I$ such that for any finite subset $K$ of $I$ including $J$:

$$\|\, |\psi\rangle - \sum_{i \in K} a_i|\psi_i\rangle \,\| \leq \varepsilon.$$

**Definition 10.21** (*Orthonormal basis*) An *orthonormal basis* of a Hilbert space $\mathscr{H}$ is a *maximal orthonormal set* $\{|\psi_i\rangle\}_{i \in I}$ of $\mathscr{H}$. In other words, $\{|\psi_i\rangle\}_{i \in I}$ is an orthonormal set such that no orthonormal set includes $\{|\psi_i\rangle\}_{i \in I}$ as a proper set.

One can prove that every Hilbert space $\mathscr{H}$ has an orthonormal basis and that all orthonormal bases of $\mathscr{H}$ have the same cardinality. The *dimension* of $\mathscr{H}$ is then defined as the cardinal number of any orthonormal basis of $\mathscr{H}$.

Let $\{|\psi_i\rangle\}_{i \in I}$ be any orthonormal basis of $\mathscr{H}$. One can prove that every vector $|\psi\rangle$ of $\mathscr{H}$ can be expressed in the following form:

$$|\psi\rangle = \sum_{i \in I} \langle \psi_i \mid \psi \rangle |\psi_i\rangle.$$

Thus, $|\psi\rangle$ is a superposition of $\{|\psi_i\rangle\}_{i\in I}$ with scalars $\langle\psi_i \mid \psi\rangle$ (also called *Fourier-coefficients*).

A Hilbert space $\mathscr{H}$ is called *separable* iff $\mathscr{H}$ has a countable orthonormal basis. Since quantum theory only uses separable Hilbert spaces, in the following we will always refer to Hilbert spaces whose orthonormal bases are countable.

**Definition 10.22** (*Closed subspace*) A *closed subspace* of a Hilbert space $\mathscr{H}$ is a set of vectors $X$ that satisfies the following conditions:

(1) $X$ is a *subspace* of $\mathscr{H}$. Hence, for any vectors $|\psi\rangle, |\varphi\rangle$ and for any scalars $a, b$:

$$|\psi\rangle, |\varphi\rangle \in X \implies a|\psi\rangle + b|\varphi\rangle \in X;$$

(2) $X$ is closed under limits of Cauchy sequences. In other words, if each element of a Cauchy sequence belongs to $X$, then also the limit of the sequence belongs to $X$.

The set of all closed subspace of $\mathscr{H}$ will be indicated by $\mathscr{C}(\mathscr{H})$. For any vector $|\psi\rangle$, we will indicate by $X_{|\psi\rangle}$ the unique 1-dimensional closed subspace that contains $|\psi\rangle$.

**Definition 10.23** (*Operator*) An *operator* of a Hilbert space $\mathscr{H}$ is a map

$$A : Dom(A) \rightarrow \mathbf{V}_{\mathscr{H}},$$

where $Dom(A)$ (the *domain* of $A$) is a subset of $\mathbf{V}_{\mathscr{H}}$.
When $Dom(A) = \mathbf{V}_{\mathscr{H}}$, $A$ is called *everywhere defined*.

**Definition 10.24** (*Eigenvector and eigenvalue*) Let $A$ be an operator of a Hilbert space $\mathscr{H}$. A non-null vector $|\psi\rangle \in Dom(A)$ is called an *eigenvector* of $A$ with *eigenvalue* $a$ iff

$$A|\psi\rangle = a|\psi\rangle.$$

**Definition 10.25** (*Linear operator*) A *linear operator* of a Hilbert space $\mathscr{H}$ is an operator $A$ that satisfies the following conditions:

(1) $Dom(A)$ is a closed subspace of $\mathscr{H}$;
(2) for any vectors $|\psi\rangle, |\varphi\rangle$ in the domain of $A$ and for any scalars $a, b$:

$$A(a|\psi\rangle + b|\varphi\rangle) = aA|\psi\rangle + bA|\varphi\rangle.$$

Thus, the characteristic property of linear operators is preserving all finite linear combinations.

Linear operators of finite-dimensional Hilbert spaces can be usefully represented as special matrices. Let $A$ be a linear operator of a space $\mathscr{H}$ whose dimension is $n$. For any choice of an orthonormal basis $\mathbf{B} = \{|\varphi_1\rangle, \ldots, |\varphi_n\rangle\}$ of $\mathscr{H}$, we have:

$$A|\varphi_1\rangle = a_{11}|\varphi_1\rangle + \ldots + a_{1n}|\varphi_n\rangle$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$A|\varphi_n\rangle = a_{n1}|\varphi_1\rangle + \ldots + a_{nn}|\varphi_n\rangle.$$

Accordingly, the operator $A$ can be represented as the following matrix (with respect to the basis **B**):

$$A = \begin{bmatrix} a_{11} & \ldots & a_{n1} \\ \ldots & \ldots & \ldots \\ a_{1n} & \ldots & a_{nn} \end{bmatrix}.$$

Conversely, any $n \times n$ matrix of $\mathscr{H}$ determines a linear operator of $\mathscr{H}$.

**Definition 10.26** (*Bounded operator*) A linear operator $A$ of a Hilbert space $\mathscr{H}$ is called *bounded* iff there exists a positive real number $a$ such that for every vector $|\psi\rangle$ of $\mathscr{H}$:

$$\|\ A|\psi\rangle\ \| \leq \|\ a|\psi\rangle\ \|\ .$$

**Definition 10.27** (*Positive operator*) A bounded operator $A$ of a Hilbert space $\mathscr{H}$ is called *positive* iff for every vector $|\psi\rangle$ of $\mathscr{H}$:

$$\langle\psi \mid A\psi\rangle \ \geq\ 0.$$

One can prove that for any positive operator $A$ there exists a unique positive operator (denoted by $A^{\frac{1}{2}}$) such that:

$$(A^{\frac{1}{2}})^2 = A.$$

**Definition 10.28** (*Densely defined operator*) A *densely defined operator* of a Hilbert space $\mathscr{H}$ is an operator $A$ that satisfies the following condition:

$$\forall\varepsilon \in \mathbb{R}^+ \forall|\psi\rangle \in \mathbf{V}_{\mathscr{H}} \exists|\varphi\rangle \in Dom(A) :\ d(|\psi\rangle, |\varphi\rangle)\ \leq\ \varepsilon.$$

**Definition 10.29** (*The adjoint operator*) Let $A$ be a densely defined operator of a Hilbert space $\mathscr{H}$. The *adjoint* of $A$ is the unique operator $A^\dagger$ such that:

$$\forall|\psi\rangle \in Dom(A)\, \forall|\varphi\rangle \in Dom(A^\dagger) : \langle A\psi \mid \varphi\rangle = \langle\psi \mid A^\dagger\varphi\rangle.$$

Notice that the adjoint $A^\dagger$ of a densely defined operator $A$ is not necessarily densely defined. Moreover, if $A$ is a (not necessarily positive) bounded operator, then $A^\dagger A$ is positive.

**Definition 10.30** (*Self-adjoint operator*) A *self-adjoint operator* is a densely defined linear operator $A$ such that $A = A^\dagger$.

If $A$ is self-adjoint, then $\forall|\psi\rangle, |\varphi\rangle \in Dom(A) : \langle A\psi \mid \varphi\rangle = \langle\psi \mid A\varphi\rangle$.

If $A$ is self-adjoint and everywhere defined, then $A$ is bounded.

One can prove that any self-adjoint operator $A$ of a finite-dimensional Hilbert space $\mathscr{H}$ satisfies the following conditions:

- there is an orthonormal basis of $\mathscr{H}$ in which each element is a unit eigenvector of $A$;
- all eigenvalues of $A$ are real numbers.

**Definition 10.31** (*Projection operator*) A *projection operator* (briefly, *projection*) of $\mathscr{H}$ is an everywhere defined self-adjoint operator $P$ that satisfies the *idempotence-property*:

$$\forall|\psi\rangle \in \mathbf{V}_{\mathscr{H}} : P|\psi\rangle = PP|\psi\rangle.$$

There are two special projections $\mathtt{O}$ and $\mathtt{I}$, called the *null projection* and the *identity-projection* that are defined as follows:

$$\forall|\psi\rangle \in \mathbf{V}_{\mathscr{H}} : \mathtt{O}|\psi\rangle = \mathbf{0} \;\text{ and }\; \mathtt{I}|\psi\rangle = |\psi\rangle.$$

Any projection other than $\mathtt{O}$ and $\mathtt{I}$ is called a *non-trivial projection*.

The set of all projection operators of a Hilbert space $\mathscr{H}$ will be indicated by $\mathscr{P}(\mathscr{H})$. One can prove that the set $\mathscr{P}(\mathscr{H})$ and the set $\mathscr{C}(\mathscr{H})$ of all closed subspaces of $\mathscr{H}$ are in one-to-one correspondence. Let $X$ be a closed subspace of $\mathscr{H}$. By the *projection-theorem* every vector $|\psi\rangle$ of $\mathscr{H}$ can be uniquely expressed as a linear combination $|\psi_1\rangle + |\psi_2\rangle$, where $|\psi_1\rangle \in X$, while $|\psi_2\rangle$ is orthogonal to all vectors of $X$. Accordingly, one can define an operator $P_X$ on $\mathscr{H}$ such that

$$\forall|\psi\rangle \in \mathbf{V}_{\mathscr{H}} : \; P_X|\psi\rangle = |\psi_1\rangle$$

(in other words, $P_X$ transforms any vector $|\psi\rangle$ into the "$X$-component" of $|\psi\rangle$). It turns out that $P_X$ is a projection of $\mathscr{H}$.

Conversely, we can associate to any projection $P$ its range:

$$X_P = \{|\psi\rangle \in \mathbf{V}_{\mathscr{H}} : \exists|\varphi\rangle \in \mathbf{V}_{\mathscr{H}} (P|\varphi\rangle = |\psi\rangle)\},$$

which turns out to be a closed subspace of $\mathscr{H}$.

For any closed subspace $X$ and for any projection $P$, we have:

$$X_{(P_X)} = X; \qquad P_{(X_P)} = P.$$

**Definition 10.32** (*Unitary operator*) An operator $\mathtt{U}$ of a Hilbert space $\mathscr{H}$ is called *unitary* iff $\mathtt{U}$ satisfies the following conditions:

(1) $\mathtt{U}$ is defined on the whole space;
(2) $\mathtt{U}$ is linear;
(3) $\mathtt{U}\mathtt{U}^\dagger = \mathtt{U}^\dagger\mathtt{U} = \mathtt{I}$.

One can show that any unitary operator $\mathtt{U}$ satisfies the following conditions:

1. $\mathtt{U}$ preserves the inner product:

$$\forall |\psi\rangle, |\varphi\rangle \in \mathbf{V}_{\mathscr{H}} : \langle \mathtt{U}\psi | \, \mathtt{U}\varphi\rangle = \langle \psi | \varphi\rangle.$$

   Consequently, $\mathtt{U}$ preserves the length of all vectors;
2. $\mathtt{U}$ is reversible:

$$\mathtt{U}^{-1}\mathtt{U} = \mathtt{U}\mathtt{U}^{-1} = \mathtt{I} \text{ (with } \mathtt{U}^{-1} = \mathtt{U}^{\dagger}).$$

**Definition 10.33** (*Trace-class operator*) A linear bounded operator $A$ of a Hilbert space $\mathscr{H}$ is called a *trace-class operator* iff for some orthonormal basis $\{|\varphi_i\rangle\}_{i\in I}$,

$$\sum_{i\in I} \langle (A^{\dagger}A)^{\frac{1}{2}} \varphi_i \mid \varphi_i\rangle$$

is a finite number.

One can prove that for any trace-class operator $A$ of $\mathscr{H}$, the number

$$\sum_{i\in I} \langle A \, \varphi_i \mid \varphi_i\rangle$$

is finite and independent of the choice of the basis $\{|\varphi_i\rangle\}_{i\in I}$.

On this ground one can define the notion of *trace-functional*.

**Definition 10.34** (*The trace-functional*) Let $\{|\varphi_i\rangle\}_{i\in I}$ an orthonormal basis for a Hilbert space $\mathscr{H}$ and let $A$ be a trace-class operator of $\mathscr{H}$. The *trace* of $A$ (indicated by $\mathtt{tr}(A)$) is defined as follows:

$$\mathtt{tr}(A) := \sum_{i\in I} \langle A\varphi_i \mid \varphi_i\rangle.$$

Due to the properties of trace-class operators, the definition of *trace-functional* turns out to be independent of the choice of the basis.

**Definition 10.35** (*Density operator*) A *density operator* of a Hilbert $\mathscr{H}$ is a positive, self-adjoint, trace-class operator $\rho$ such that $\mathtt{tr}(\rho) = 1$.

**Definition 10.36** (*Effect*) An *effect* of a Hilbert $\mathscr{H}$ is a self-adjoint operator $E$ that satisfies the following condition for any density operator $\rho$ of $\mathscr{H}$:

$$\mathtt{tr}(\rho E) \in [0, 1].$$

One can prove that the set of all projections of $\mathscr{H}$ is a proper subset of the set of all effects of $\mathscr{H}$.

Any pair of Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$ (over the same field) gives rise to a new Hilbert space $\mathscr{H}_1 \otimes \mathscr{H}_2$ that represents the *tensor product* of $\mathscr{H}_1$ and $\mathscr{H}_2$.

**Definition 10.37** (*Tensor product*) Let $\mathscr{H}_1$ and $\mathscr{H}_2$ be two Hilbert spaces over the same field (the real or the complex field). A Hilbert space $\mathscr{H}$ is the *tensor product* of $\mathscr{H}_1$ and $\mathscr{H}_2$ iff there is an injective map $\otimes$ that associates to every element $(|\psi^{(1)}\rangle, |\varphi^{(2)}\rangle)$ of the cartesian product $\mathbf{V}_{\mathscr{H}_1} \times \mathbf{V}_{\mathscr{H}_2}$ an element $|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle$ of $\mathbf{V}_{\mathscr{H}}$. The following conditions are required:

(1) for any vector $|\psi^{(1)}\rangle$ of $\mathscr{H}_1$, for any vector $|\varphi^{(2)}\rangle$ of $\mathscr{H}_2$ and for any scalar $a$:

$$a(|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle) = a|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle = |\psi^{(1)}\rangle \otimes a|\varphi^{(2)}\rangle;$$

(2) for any vectors $|\psi^{(1)}\rangle, |\varphi^{(1)}\rangle$ of $\mathscr{H}_1$, for any vectors $|\sigma^{(2)}\rangle, |\tau^{(2)}\rangle$ of $\mathscr{H}_2$ and for any scalars $a, b$:

- $|\psi^{(1)}\rangle \otimes (a|\sigma^{(2)}\rangle + b|\tau^{(2)}\rangle) = (|\psi^{(1)}\rangle \otimes a|\sigma^{(2)}\rangle) + (|\psi^{(1)}\rangle \otimes b|\tau^{(2)}\rangle)$;
- $(a|\psi^{(1)}\rangle + b|\varphi^{(1)}\rangle) \otimes |\sigma^{(2)}\rangle = (a|\psi^{(1)}\rangle \otimes |\sigma^{(2)}\rangle) + (b|\varphi^{(1)}\rangle \otimes |\sigma^{(2)}\rangle)$;

(3) every vector of $\mathscr{H}$ can be expressed as a finite or infinite superposition of vectors of the set

$$\left\{|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle : |\psi^{(1)}\rangle \in \mathbf{V}_{\mathscr{H}_1}, |\varphi^{(2)}\rangle \in \mathbf{V}_{\mathscr{H}_2}\right\}.$$

One can prove that the tensor product $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$ is unique up to isomorphism.

If $\left\{|\psi_i^{(1)}\rangle\right\}_{i\in I}$ is an orthonormal basis for $\mathscr{H}_1$ and $\left\{|\varphi_j^{(2)}\rangle\right\}_{j\in J}$ is an orthonormal basis of $\mathscr{H}_2$, then the set

$$\left\{|\psi_i^{(1)}\rangle \otimes |\varphi_j^{(2)}\rangle : i \in I, j \in J\right\}$$

is an orthonormal basis for the product space $\mathscr{H}_1 \otimes \mathscr{H}_2$.

While every vector of $\mathscr{H}_1 \otimes \mathscr{H}_2$ can be expressed as a superposition of vectors $|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle$, there are vectors of $\mathscr{H}_1 \otimes \mathscr{H}_2$ that cannot be written as a single product $|\psi^{(1)}\rangle \otimes |\varphi^{(2)}\rangle$, for any $|\psi^{(1)}\rangle \in \mathbf{V}_{\mathscr{H}_1}$, $|\varphi^{(2)}\rangle \in \mathbf{V}_{\mathscr{H}_2}$. These vectors (which play an important role in quantum entanglement) are called *non-factorizable*.

# Index





M. L. Dalla Chiara et al., *Quantum Computation and Logic*,
Trends in Logic 48, https://doi.org/10.1007/978-3-030-04471-8