PHILOSOPHY OF QUANTUM INFORMATION AND ENTANGLEMENT

Recent work in quantum information science has produced a revolution in our understanding of quantum entanglement. Scientists now view entanglement as a physical resource with many important applications. These range from quantum computers, which would be able to compute exponentially faster than classical computers, to quantum cryptographic techniques, which could provide unbreakable codes for the transfer of secret information over public channels. These important advances in the study of quantum entanglement and information touch on deep foundational issues in both physics and philosophy.

This interdisciplinary volume brings together fourteen of the world's leading physicists and philosophers of physics to address the most important developments and debates in this exciting area of research. It offers a broad spectrum of approaches to resolving deep foundational challenges – philosophical, mathematical, and physical – raised by quantum information, quantum processing, and entanglement. This book will interest physicists, philosophers of science, and computer scientists.

ALISA BOKULICH is a Professor in the Philosophy Department at Boston University, and the director of Boston University's Center for Philosophy and History of Science. Her research focuses on the history and philosophy of physics, as well as broader issues in the philosophy of science.

GREGG JAEGER is an Associate Professor at Boston University, where he teaches courses in the Mathematics, Natural Science, Philosophy, and Physics departments. His recent research focuses on decoherence, entanglement, quantum computing, and quantum cryptography, and in 2008 he was awarded a Kavli fellowship.

PHILOSOPHY OF QUANTUM INFORMATION AND ENTANGLEMENT

Edited by

ALISA BOKULICH
Boston University

and

GREGG JAEGER
Boston University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521898768

First published 2010

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Philosophy of quantum information and entanglement / edited by
Alisa Bokulich, Gregg Jaeger.
p. cm.
ISBN 978-0-521-89876-8 (hardback)
1. Quantum theory – Philosophy. 2. Quantum computing. 3. Information theory.
I. Bokulich, Alisa. II. Jaeger, Gregg. III. Title.
QC174.12.P435 2010
530.12–dc22
2010000125

ISBN 978 0 521 89876 8 Hardback

For our teacher, mentor, and colleague
Abner Shimony
who has contributed so much
to both the philosophy and the physics of this subject.

Contents

Contributors

Howard Barnum
CCS-3: Modeling, Algorithms, and Informatics,
Mail Stop B256,
Los Alamos National Laboratory,
Los Alamos, NM 87545, USA

Jeffrey Bub
Department of Philosophy,
University of Maryland,
College Park, MD 20742, USA

Giacomo Mauro D'Ariano
Istituto Nazionale di Fisica della Materia, Unità di Pavia,
Dipartimento di Fisica "A. Volta,"
via Bassi 6, I-27100 Pavia, Italy

Armond Duwell
Department of Philosophy,
University of Montana,
Missoula, MT 59812, USA

Lucien Hardy
Perimeter Institute,
31 Caroline Street North,
Waterloo, Ontario N2L 2Y5, Canada

Leah Henderson
Department of Linguistics and Philosophy, MIT,
77 Massachussetts Avenue 32-D808
Cambridge, MA 02139-4307, USA

Andrei Khrennikov
International Center for Mathematical Modeling in Physics and Cognitive Sciences,
University of Växjö, S-35195, Sweden

F. Hadi Madjid
82 Powers Road,
Concord, MA 01742, USA

John M. Myers
Division of Engineering and Applied Sciences,
Harvard University,
60 Oxford Street,
Cambridge, MA 02138, USA

Wayne C. Myrvold
Department of Philosophy,
Talbot College,
University of Western Ontario,
London, Ontario N6A 3K7, Canada

Sandu Popescu
H. H. Wills Physics Laboratory,
University of Bristol,
Tyndall Avenue,
Bristol, BS8 1TL, UK; and
Hewlett-Packard Laboratories,
Stoke Gifford,
Bristol, BS12 6QZ, UK

Christopher G. Timpson
Brasenose College,
University of Oxford, OX1 4AJ, UK

Lorenza Viola
Department of Physics and
Astronomy,
Dartmouth College,
6127 Wilder Laboratory,
Hanover, NH 03755, USA

Tai Tsun Wu
Harvard University,
Cambridge,
MA 02138, USA

Preface

Recently there has emerged an exciting and rapidly growing field of research known as quantum information theory. This interdisciplinary field is unified by the following two goals: first, the possibility of harnessing the principles and laws of quantum mechanics to aid in the acquisition, transmission, and processing of information; and second, the potential that these new technologies have for deepening our understanding of the foundations of quantum mechanics and computation. Many of the new technologies and discoveries emerging from quantum information theory are challenging the adequacy of our old concepts of entanglement, non-locality, and information. This research suggests that the time is ripe for a reconsideration of the foundations – and philosophical implications – of quantum information theory.

Historically, apart from a small group of physicists working on foundational issues, it was philosophers of physics who recognized the importance of the concepts of entanglement and non-locality long before the mainstream physics community. Prior to the 1980s, discussions of the infamous "EPR" paper and John Bell's seminal papers on quantum non-locality were carried out more often by such philosophers than by ordinary physicists. In the 1990s that situation rapidly changed, once the larger community of physicists had begun to realize that entanglement and non-locality were not just quirky features of quantum mechanics, but physical resources that could be harnessed for the performance of various practical tasks. Since then, a large body of literature has emerged in physics, revealing many new dimensions to our concepts of entanglement and non-locality, particularly in relation to information. Regrettably, however, only a few philosophers have followed these more recent developments, and many philosophical discussions still end with Bell's work.

The purpose of this volume is two-fold. First, our hope is to introduce more philosophers of physics to the recent discussions about entanglement and non-locality by making accessible some of the central developments in this field

"beyond Bell." While there are many excellent anthologies examining the philosophical implications of Bell's theorem, the present volume is the first interdisciplinary anthology to explore the philosophical implications of entanglement and non-locality beyond Bell. In this sense the philosophers have much to learn from the physicists. The second goal of this volume is to encourage more physicists to reflect critically on the foundations of quantum information theory. The key concepts of entanglement, non-locality, and information are in need of conceptual clarification and perhaps even bifurcation. Recent claims that quantum information science revolutionizes the foundations of quantum mechanics and solves its most basic conceptual puzzles need to be critically examined. Here the physicists have much to learn from the philosophers, who have long been engaged in such projects of conceptual clarification and logical analysis. Our hope is that pursuing these two goals together will encourage a fruitful dialogue and that a stronger interdisciplinary field in the philosophy of quantum information will be forged.

The idea for this volume first emerged at a conference on the foundations of quantum information and entanglement, which was held at the Center for Philosophy and History of Science at Boston University in 2006. The conference was a tremendous success, drawing over two hundred attendees, and it emphasized the need for an interdisciplinary volume in this area. Many of the speakers at this conference were chosen to be contributors to the present volume. We gratefully acknowledge the support of the Center for Philosophy and History of Science and the National Science Foundation for making this conference possible. We would also like to thank Molly Pinter for her work compiling the index.

We have gathered here twelve original papers, seven of which are by physicists and five of which are by philosophers, all of whom are actively engaged in quantum information theory. These papers, which are by many of the leading researchers in the field, represent a broad spectrum of approaches to the foundations of quantum information theory and highlight some of the most important developments and debates. While these papers assume a certain level of scientific literacy, an effort has been made to present the latest research in a way that is accessible to non-specialists, physicists and philosophers of physics alike. To this end, the volume begins with a pedagogical introduction, briefly laying out the relevant historical background, as well as defining the key philosophical and physical concepts used in the subsequent papers. While it would be impossible to cover all the important developments in this rapidly growing field, we hope this volume succeeds in laying the foundation for further interdisciplinary work in the philosophy of quantum information and entanglement, by encouraging more physicists and philosophers to enter into the debate.

Introduction

Entanglement can be understood as an extraordinary degree of correlation between states of quantum systems – a correlation that cannot be given an explanation in terms of something like a common cause. Entanglement can occur between two or more quantum systems, and the most interesting case is when these correlations occur between systems that are space-like separated, meaning that changes made to one system are immediately correlated with changes in a distant system even though there is no time for a signal to travel between them.[1] In this case one says that quantum entanglement leads to non-local correlations, or non-locality.

More precisely, entanglement can be defined in the following way. Consider two particles, A and B, whose (pure) states can be represented by the state vectors ψ_A and ψ_B. Instead of representing the state of each particle individually, one can represent the composite two-particle system by another wavefunction, Ψ_{AB}. If the two particles are *unentangled*, then the composite state is just the tensor product of the states of the components: $\Psi_{AB} = \psi_A \otimes \psi_B$; the state is then said to be factorable (or separable). If the particles are entangled, however, then the state of the composite system *cannot* be written as such a product of a definite state for A and a definite state for B. This is how an entangled state is defined for pure states: a state is entangled if and only if it cannot be factored: $\Psi_{AB} \neq \psi_A \otimes \psi_B$. For mixed states, which must be represented by density operators rather than state vectors, the definition of entanglement is generalized: an entangled mixed state is one that *cannot* be written as a convex combination of products

$$\rho_{AB} = \sum_i p_i (\rho_{Ai} \otimes \rho_{Bi}),$$

[1] On some conceptions, entanglement can occur even between the different properties of a single quantum system, such as in the case of entangling a particle's position with its spin.

Philosophy of Quantum Information and Entanglement, ed. A. Bokulich and G. Jaeger. Published by Cambridge University Press.

where the sum of the p_i is equal to unity. This definition is for a bipartite system, that is, a composite system of only two parts, A and B. For multipartite mixed quantum systems the situation is more complicated; there is no single acceptable entanglement measure applicable to the full set of possible states of systems having a greater number of parts.[2] The search for a fully general definition and measure of entanglement remains an active area of research.

Despite the fact that the phenomenon of entanglement was recognized very early on in the development of quantum mechanics, it remains one of the least understood aspects of quantum theory. It was arguably the well-known "EPR" paper,[3] by Albert Einstein, Boris Podolsky, and Nathan Rosen, published in May of 1935, that first drew attention to the phenomenon of entanglement.[4] For EPR, however, the possibility of such a phenomenon in quantum mechanics was taken to be a *reductio ad absurdum* showing that there is a fundamental flaw with the theory: "since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system" (Einstein *et al.* 1935, p. 779); since quantum mechanics implies such an "absurd" situation, quantum mechanics must be incomplete at best. Quantum entanglement, however, precisely is such a non-classical relationship between quantum particles whereby changes made to one particle of an entangled pair can lead to changes in the other particle even though they no longer interact.

Shortly after the appearance of the EPR paper, Erwin Schrödinger coined the term "entanglement" (*Verschränkung*) to describe this phenomenon. The first published occurrence of the term is in an article of his, written in English, which appeared in October of 1935. In this article, Schrödinger places the phenomenon of entanglement at the center of quantum theory:

> When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives (or ψ-functions) have become entangled (Schrödinger 1935a, p. 555).

The term appears two months later in German in the second of the triplet of papers in which he introduces his infamous cat paradox (Schrödinger 1935b).

[2] For a technical overview of basic results in entanglement and quantum information see, for example, Jaeger (2007).
[3] See Fine (2008) for a helpful overview of the EPR paper.
[4] Regarding the question of when the physics community first became aware of the phenomenon of entanglement, Don Howard (1990) has cogently argued that Einstein had recognized, and been concerned about, the phenomenon of entanglement long before the 1935 EPR paper.

Although Schrödinger recognized the importance of the phenomenon of entanglement, he certainly did not embrace this feature of quantum theory. His dissatisfaction with the phenomenon of entanglement, and with the quantum theory in general, is evident in his correspondence with Einstein during this time. In a letter to Einstein, Schrödinger writes as follows regarding the recently published EPR paper: "I was very happy that, in your work that recently appeared in *Phys. Rev*., you have publicly caught the dogmatic quantum mechanics by the collar, regarding that which we had already discussed so much in Berlin" (Schrödinger to Einstein, June 7, 1935).[5] Toward the end of the same letter he continues, "The point of my foregoing discussion is this: we do not have a quantum mechanics that takes into account relativity theory, that is, among other things, that respects the finite speed of propagation of all effects" (Schrödinger to Einstein, June 7, 1935). Schrödinger's concern is that the phenomenon of entanglement, exhibiting as it does non-local correlations between separated particles, ultimately would prove to be in conflict with the first-signal principle of special relativity.

Despite this early recognition of the importance of the phenomenon, very little effort or progress was made over the next thirty years in developing a theory of entanglement or in answering Schrödinger's concerns regarding how this phenomenon could be consistent with relativity. It would be almost thirty years before another significant step toward a theory of entanglement would be made with John Bell's seminal 1964 paper on quantum non-locality. In that paper Bell considered a pair of particles in the singlet state that had interacted in the past, had become entangled, and then had separated. He derived an inequality involving the probabilities of various outcomes of measurements performed on these entangled particles that any local definite (i.e., hidden-variable) theory must satisfy. He then showed that quantum mechanics violates this inequality; that is, the experimentally well-confirmed quantum correlations among entangled particles cannot be locally explained. Bell's theorem does not rule out the possibility of hidden-variable theories in general, only those hidden-variable theories that are local. Indeed, Bell took the lesson of his theorem to be that any theory that reproduces the experimentally well-confirmed predictions of quantum mechanics must be non-local. He writes,

> It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty . . . This [non-locality] is characteristic, according to the result to be proved here, of any theory which reproduces exactly the quantum mechanical predictions (Bell 1964, p. 14).

[5] This translation is taken from a copy of the letter located at the Howard Gotlieb Archival Research Center at Boston University. The original letter is in German and is held in the Einstein Archives at the Hebrew University in Jerusalem.

What is remarkable about Bell's theorem is that it is a general result arising from an analysis of the relevant probabilities of various joint measurement outcomes, and does not depend on the details of any hidden-variable theory or even on the details of quantum mechanics itself.[6] Since then a number of different Bell-type inequalities have been derived, such as the Clauser, Horne, Shimony, and Holt (CHSH) inequality (1969), which has proven particularly useful for experimental tests of non-locality. Following Bell, a number of experiments demonstrated not only that non-locality is a genuine physical phenomenon characteristic of our world (e.g., Aspect *et al.* 1982), but also that non-locality can be experimentally produced, controlled, and harnessed for various applications.

Another theoretical development came with Jon Jarrett's (1984) analysis showing that Bell's locality condition can be viewed as the conjunction of two logically independent conditions: a "controllable" locality, which if violated would conflict with special relativity, and an "uncontrollable" locality whose violation might "peacefully coexist" with relativity (see also Shimony (1984); for an opposing point of view see Maudlin (1994)). Hence, the violation of Bell's inequality could logically be due to a violation of one, the other, or both of these locality conditions. Jarrett's analysis has been taken by some to provide the solution to Schrödinger's worries about a conflict between quantum theory and relativity, as long as one assumes that the violation is in fact solely a violation of the uncontrollable locality.[7]

Despite these important advances, it was still only a handful of physicists who were deeply interested in entanglement. Philosophers of physics recognized the importance of entanglement and Bell's work, but many continued to think of entanglement as an "all or nothing" phenomenon and described entanglement as simply a spooky action-at-a-distance or mysterious holism. Moreover, the bulk of philosophical work on non-locality and entanglement has considered developments only up to and including Jarrett's analysis and the experiments performed in the mid 1980s. In the last two decades new discoveries – many of which are associated with the investigation of quantum information – have shown that much philosophical and foundational work remains to be done to deepen our understanding of entanglement and non-locality.

Toward the end of the 1980s and the beginning of the 1990s a number of important transformations in our understanding of entanglement took place. First, it was recognized (e.g., Shimony (1995)) that entanglement can be quantified; that is,

[6] There are of course many subtleties in analyzing the implications of Bell's theorem that cannot be covered in this introduction, but are discussed extensively in the voluminous literature that followed Bell's work. For an introduction to the subtleties of interpreting the lessons of Bell's theorem see Cushing and McMullin (1989) and Shimony (2008).

[7] For an overview of these issues see Cushing and McMullin (1989).

it comes in degrees ranging from "maximally entangled" to not entangled at all. Moreover, entanglement can be manipulated in all sorts of interesting ways. For example, Bennett *et al.* (1996) have shown that one can take a large number of electrons that are all partly (that is, "a little bit") entangled with each other, and concentrate that entanglement into a smaller number of maximally entangled electrons, leaving the other electrons unentangled (a process known as *entanglement distillation*).[8] Conversely, one can take a pair of maximally entangled electrons and spread that entanglement out over a larger number of electrons (so that they are now only partly entangled) in such a way that the total entanglement is conserved (a process known as *entanglement dilution*).

The notion of a "degree of entanglement" seems to have been first recognized through the related notion of a degree of violation of the Bell inequalities – indeed, this was used as the first measure of entanglement in the case of pure states: the greater the degree of violation of the inequalities, the greater the amount of entanglement. Nicolas Gisin describes this "quiet revolution" as follows:

> In this brief note I prove that the product states are the only states that do not violate any Bell inequality. When I had the chance to discuss this equivalence between "states that violate the inequality" and "entangled states" (i.e., "non-product states") with John Bell last September, just before his sudden tragic death, I was surprised that he did not know this result. This motivates me to present today this little note which I have had on my shelves for many years and which may be part of the "folklore," known to many people but (apparently) never published. (Gisin 1991, p. 201)

There are, however, limitations to using a violation of Bell's inequality as a general measure of entanglement. First, there are Bell-type inequalities whose largest violation is given by a non-maximally entangled state (Acín *et al.* 2002), so entanglement and non-locality do not always vary monotonically. More troublingly, however, Reinhard Werner (1989) showed that there are some mixed states (now referred to as Werner states) that, though entangled, do not violate Bell's inequality at all; that is, there can be entanglement without non-locality. In an interesting twist, Sandu Popescu (1995) has shown that even with these local Werner states one can perform a non-ideal measurement (or series of ideal measurements) that "distills" a non-local entanglement from the initially local state. In yet a further twist, the Horodecki family (1998) subsequently showed that not all entanglement can be distilled in this way – there are some entangled states that are "bound." These bound entangled states are ones that satisfy the Bell inequalities (i.e., they are local) and cannot have maximally entangled states violating Bell's inequalities extracted from them by means of local operations.[9]

[8] It is also sometimes referred to as "entanglement concentration" or "entanglement purification."
[9] For a nice review of these developments see Werner and Wolf (2001).

Not only can one have entanglement without non-locality, but also, as Bennett *et al.* (1999) have shown, one can have a kind of "non-locality without entanglement." There are systems that exhibit a type of non-local behavior even though entanglement is used neither in the preparation of the states nor in the joint measurement that discriminates the states (see also Niset and Cerf (2006)). This work highlights another facet of the concept of non-locality, which, rather than involving correlations for space-like separated systems, involves instead a kind of indistinguishability based on local operations and classical communication. The relationship between this new notion of non-locality and the traditional one involving space-like separated systems remains to be worked out.

These recent developments point to the need for a new, more adequate way of measuring and quantifying entanglement. They show that the concepts of entanglement and non-locality are much more subtle and multifaceted than earlier analyses based solely on Bell's theorem realized. Much philosophical and foundational work remains to be done on understanding precisely how the important notions of entanglement and non-locality are related.

These questions of how to quantify entanglement and non-locality – and the need to clarify the relationship between them – are important not only conceptually, but also practically, insofar as entanglement and non-locality seem to be different resources for the performance of quantum information processing tasks. As Brunner and colleagues have argued, it is important to ask "whether in a given quantum information protocol (cryptography, teleportation, and algorithm . . .) it is better to look for the largest amount of entanglement or the largest amount of non-locality" (Brunner *et al.* 2005, p. 12). Arguably it is this new emphasis on the exploitation of entanglement and non-locality for the performance of practical tasks that marks the most fundamental transformation in our understanding of these concepts.

The newly formed field of quantum information theory is devoted to using the principles and laws of quantum mechanics to aid in the acquisition, transmission, and processing of information. In particular, it seeks to harness the peculiarly quantum phenomena of entanglement, superposition, and non-locality to perform all sorts of novel tasks, such as enabling computations that operate exponentially faster or more efficiently than their classical counterparts (via quantum computers) and providing unconditionally secure cryptographic systems for the transfer of secret messages over public channels (via quantum key distribution). By contrast, classical information theory is concerned with the storage and transfer of information in classical systems. It uses the "bit" as the fundamental unit of information, where the system capable of representing a bit can take on one of two values (typically 0 or 1). Classical information theory is based largely on the concept of information formalized by Claude Shannon in the late 1940s. Quantum information theory, which was later developed in analogy with classical information theory, is concerned with the

storage and processing of information in quantum systems, such as the photon, electron, quantum dot, or atom. Instead of using the bit, however, it defines the fundamental unit of quantum information as the "qubit." What makes the qubit different from a classical bit is that the smallest system capable of storing a qubit, the two-level quantum system, not only can take on the two distinct values $|0\rangle$ and $|1\rangle$, but can also be in a state of superposition of these two states: $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Quantum information theory has opened up a whole new range of philosophical and foundational questions. The first cluster of questions concerns the nature of quantum information. For example, is quantum information just classical information stored in a quantum system, or is it a new distinctive type of information? (See Chapter 8 by Duwell.)

A second cluster of important philosophical questions concerns how it is that quantum information protocols are able to achieve more than their classical counterparts. For example, how is that quantum computers are able to compute exponentially faster than classical computers? (See Chapter 11 by Bub.) Can quantum computers perform calculations that are not Turing computable – so-called hypercomputation? Another example concerns quantum teleportation, whereby the complete state of a quantum system (something that would take a huge amount of information to specify classically) can be transferred to another distant system using only two bits of information, as long as the two parties at the different locations share a pair of entangled particles. The *prima facie* puzzle of teleportation is how so much "information" can be transferred so efficiently (see Penrose (1998), Deutsch and Hayden (2000), and, for critical analyses, Timpson (2006) and Jaeger (2009)).

Yet another example of a quantum information technology raising foundational questions is quantum cryptography or quantum key distribution, which involves using the principles of quantum mechanics to ensure secure communication (that is, the transfer of secret information over public channels in a way that cannot be successfully eavesdropped upon). Some quantum cryptographic protocols make use of entanglement to establish correlations between systems that would be lost upon eavesdropping. Moreover, a quantum principle known as the no-cloning theorem prohibits making identical copies of an unknown quantum state.[10] This theorem ensures that an eavesdropper cannot make a copy of the cryptographic key without the communicating parties knowing that this is happening. One important question is whether these quantum principles are really sufficient to provide unconditional security, that is security in the face of all conceivable attacks. (See Chapter 6 by Myers and Madjid, and Chapter 12 by Wu.)

[10] Quantum teleportation, mentioned earlier, is not in conflict with the no-cloning theorem since the initial state is automatically destroyed upon teleportation, that is, it does not involve cloning an unknown quantum state.

A third important cluster of philosophical questions concerns what new insights recent work in quantum information theory might provide into the foundations of quantum mechanics. Some authors have argued that an information-theoretic approach may provide a new axiomatic basis for quantum mechanics and provide deeper insight into what makes quantum mechanics different from classical mechanics. Anton Zeilinger (1999) has proposed a new information-theoretic "foundational principle," which he believes can explain both the intrinsic randomness of quantum theory and the phenomenon of entanglement. (For critical discussions see Chapter 10 by Timpson and Jaeger (2009).) In another approach, Chris Fuchs (2002) has adopted a Bayesian approach and argued that quantum mechanics just is quantum information theory – a more sophisticated gloss on the old idea that a quantum state is just a catalogue of expectations. (For a discussion of the Bayesian approach see Chapter 7 by Henderson.) Yet a third approach that has generated considerable discussion is a theorem proven by Rob Clifton, Jeff Bub, and Hans Halvorson (2003). In the context of a C^*-algebraic formulation, they argue that quantum theory can be characterized in terms of three information-theoretic constraints: (1) no superluminal signaling via measurement, (2) no cloning (for pure states) or no broadcasting (mixed states), and (3) no unconditionally secure bit commitment.[11] (For a discussion of the relative strengths and weaknesses of this approach see Chapter 9 by Myrvold.) Bub (2004) in particular has taken this ("CBH") theorem to show that quantum theory is best interpreted as a theory about the possibilities of information transfer rather than a theory about the non-classical mechanics of waves or particles. Much philosophical work remains to be done assessing these various claims that quantum information provides a new, more adequate way of conceiving quantum theory.

All the contributors to this volume are grappling with different facets of the challenges and opportunities that quantum information theory poses for quantum mechanics. The papers are organized into the following four topics: quantum entanglement and non-locality, quantum probability, quantum information, and quantum communication and computing.

The three papers in the first section are concerned with expanding and generalizing the central notions of entanglement and non-locality. The first paper, by Sandu Popescu, explores the notion of *degrees of non-locality* by considering the possibility of theories that exhibit even stronger non-local correlations than quantum

[11] Bit commitment is a central cryptographic protocol between two mistrusting parties (typically referred to as Bob and Alice) in which Bob obtains an encoded bit from Alice. It is secure against Bob if Bob cannot decode the bit until Alice chooses to reveal it by supplying some further information, and it is secure against Alice if Alice cannot change the bit (it is fixed between commitment and revealment). A theorem by Mayers (1997) showed that there is no unconditionally secure (i.e., secure against any conceivable attack) standard quantum bit commitment.

mechanics and yet still don't violate the first-signal principle of relativity. One can see the possibility of these "super-quantum" correlations through conceivable degrees of violation of the Clauser–Horne–Shimony–Holt (CHSH) inequality (Clauser *et al.* 1969). Like Bell's original inequality, the CHSH inequality sets a bound on a particular linear combination of the set of correlations, $E(X, Y)$, between two parties, A and B, that must be respected by any (Bell-)local theory:

$$-2 \leq E(A, B) + E(A, B') + E(A', B) - E(A', B') \leq 2.$$

If a theory produces correlations whose sum exceeds the upper bound of 2 then the theory is said to be (Bell) non-local. A theorem by Tsirel'son (also sometimes transliterated Cirel'son) states that the maximum bound on the correlations quantum mechanically is $2\sqrt{2}$; however, assuming only no signaling, the upper bound on the correlations could mathematically be as high as 4, and it is the region in between these two bounds that defines the superquantum correlations, or non-local correlations that are stronger than quantum mechanics.

A useful tool for investigating degrees of non-locality is the "PR box" named after Sandu Popescu and Daniel Rohrlich, who first formalized it in response to a question posed by Abner Shimony concerning whether the conjunction of the conditions of causality and no signaling uniquely picks out quantum mechanics from all possible correlation-predicting theories. The PR box can be thought of as a "black-box" device to which each of the two parties, A and B, has access to half of. A and B can each select an input from a range of possibilities and then obtain a particular output (which they cannot control) from the box. The central function of the box is to determine the joint probability of the two outputs given the two inputs.

An experimental arrangement to measure a quantum system in a particular state can be thought of as one example of such a box, where the input is a particular measurement choice at each wing A and B (such as measuring the polarization of a photon along a certain direction) and the output is a certain measurement outcome (such as getting a horizontal polarization). The no-signaling requirement is imposed on the boxes by requiring that the outcome at A is independent of the measurement choice at B. In their 1994 paper, Popescu and Rohrlich wrote down a correlation function for a set of measurements that yielded a value of 4 for the left-hand side of the CHSH inequality and yet still prohibited signaling, suggesting that quantum mechanics was just one among a set of possible non-local theories that are consistent with relativity theory.

These super-quantum correlations are particularly interesting from an information-theoretic point of view insofar as they would radically reduce the amount of communication needed for distributed computational tasks (Barrett *et al.* 2005). In his paper for this volume (Chapter 1), Popescu further explores what

advantage superquantum correlations would provide for performing various quantum communication and computing tasks. In particular, Popescu examines "non-local computation" whereby separated parties A and B must compute a function without either party learning anything about the inputs. Popescu demonstrates that, while neither classical mechanics nor quantum mechanics permit such non-local computations to succeed, any theory with non-locality even just infinitesimally stronger than quantum mechanics does allow non-local computation to take place.

The second contribution to this volume focuses on the concept of entanglement and how the notion of entanglement might be generalized for situations in which the overall system cannot be easily partitioned into separated subsystems A and B. The standard definition of entanglement for pure states depends on being able to define two or more subsystems for which the state cannot be factored into product states. For strongly interacting quantum systems, such as indistinguishable particles (bosons or fermions) that are close enough together for quantum statistics to be important, the entangled systems cannot easily be partitioned into subsystems in this way. In response to this problem, Lorenza Viola and Howard Barnum have developed a notion of "generalized entanglement," which depends on the expectation values of a preferred set of observables, rather than on a partitioning of the entangled system into subsystems. The intuition behind their approach is that entangled pure states look mixed to local observers, and the corresponding reduced state provides expectation values for a set of distinguished observables. They define a pure state as "generalized unentangled" relative to the distinguished observables if the reduced state is pure and "generalized entangled" otherwise (Barnum *et al.* 2004, p. 1). Similarly a mixed state is "generalized unentangled" if it can be written as a convex combination of unentangled pure states. Their hope is that this new approach will lead to a deeper understanding of entanglement by allowing it to be defined in more general contexts.

In the third chapter of this volume, Lucien Hardy explores how the concepts of entanglement and information flow will likely have to change in light of attempts to develop a quantum theory of gravity. Quantum mechanics and general relativity – though two of our most successful and well-confirmed scientific theories – are currently inconsistent with one another in certain respects: general relativity is deterministic but has a non-fixed causal structure, while quantum mechanics is inherently indeterministic but has a fixed causal structure. The hope is to find a quantum theory of gravity that unifies these two theories as limiting cases, and Hardy's bet is that such a theory will be indeterministic (probabilistic) and yet have an indefinite causal structure. In a theory with indefinite causal structure, there will be no fact of the matter about whether two systems are space-like separated, for example. Hence the notion of entanglement, which requires two space-like separated systems, and the notion of information flow, which requires a sequence of

time-like related regions, will have to be radically modified. Hardy develops a new formulation of quantum mechanics in terms of what he calls the causaloid framework and then shows how entanglement and information flow can be redefined. He demonstrates how the quantum theory of pairwise interacting qubits can be formulated in the causaloid framework, permitting universal quantum computation.

The second section of this book, on "quantum probability," contains four chapters examining various aspects of the central role that probability theory plays in quantum theory and quantum information science. Not only is quantum mechanics a probabilistic theory, but also the probabilities occurring in quantum mechanics are non-standard probabilities, whose conceptual basis has been an ongoing source of controversy ever since the theory's introduction. Moreover, in the more recent context of quantum information theory, the entropy functions involved in quantifying information in the classical and quantum contexts derive from different sorts of probability, which have distributions of different mathematical forms. Hence, analyses of probability are playing a central role in reexaminations of the foundations of quantum mechanics and quantum information theory.

In Chapter 4, Andrei Khrennikov argues that the challenges currently facing quantum information science point to the need for a reconsideration of the very foundations of quantum mechanics. For example, the security of quantum cryptographic protocols depends on the assumption that standard quantum mechanics is complete and that the quantum probabilities involve irreducible randomness. Khrennikov argues that what is required for quantum information science to move forward is a more rigorous mathematical formulation of probability theory. Khrennikov adopts the controversial view that the experimental violations of Bell-type inequalities do not in fact demonstrate quantum non-locality because the probabilities involved in measurements to test the inequalities are not mathematically well defined. After providing a more rigorous mathematical formulation of quantum probability, he concludes that the lesson of Bell-type "no-go" theorems needs to be modified.

Recent developments in quantum information theory have renewed interest in finding a new axiomatic formulation of quantum mechanics. In his paper for this volume, Giacomo Mauro D'Ariano takes up this challenge of finding a new axiomatization. He begins by noting some of the shortcomings of other recent axiomatizations such as Hardy's (2001) and the much discussed Clifton, Bub, and Halvorson (CBH) derivation of quantum mechanics from three information-theoretic constraints (Clifton *et al.* 2003). D'Ariano argues that a more promising approach to an operational axiomatization involves situating quantum mechanics within the broader context of probabilistic theories whose non-local correlations are stronger than quantum mechanics and yet are still non-signaling (see Chapter 1 by Popescu). He outlines such an axiomatization

in which quantum mechanics is understood as the mathematical representation of a set of rules enabling experimenters to make predictions regarding future events on the basis of suitable tests – an approach he calls the "fair operational framework."

In Chapter 6, John Myers and Hadi Madjid begin by exploring the relation between quantum-mechanical operators and the outcome probabilities these operators generate. In any quantum experiment there is a state preparation, described by a density operator, and a measurement, described by a set of detection operators. Both these operators depend on parameters, which represent the choices made by the experimenters. The trace rule can then be used to determine which parameterized probabilities are the result of a given parameterized density operator and a given parameterized detection operator. After reviewing their recent result proving that any given parameterized probability can be generated by infinitely many different parameterized operators, Myers and Madjid are led to consider parameterized probability measures independently, as a useful object of study in their own right. In their contribution to this volume, Myers and Madjid show how a consideration of these parameterized probability measures leads to three important results for quantum information theory. First, they are able to strengthen Holevo's bound on quantum communication. Holevo's bound is a theorem proving that, even though an arbitrarily large amount of classical information can be encoded in a "qubit," (more precisely the state of a quantum two-level system), such as in the process of defining the direction of a quantum state vector, at most one classical bit of information can be accessed through a measurement of that state (more precisely the accessible information is limited by the von Neumann entropy). Myers and Madjid are able to strengthen the Holevo bound by deriving a stronger inequality limiting the accessible information even in cases for which the von Neumann entropy is arbitrarily large (or infinite), making the traditional formulation of the bound uninformative. Second, they show how this approach can reveal vulnerabilities in quantum key-distribution protocols. Finally, they show that an examination of the parameterized probability measures generated by entangled states can reveal hitherto overlooked topological features, thus deepening our understanding of entangled states.

Another way in which considerations of probability have been at the center of foundational debates in quantum information theory is in the analogy that has been drawn between Bayesian conditionalization and quantum state updating upon measurement (e.g., Bub (1977) and Fuchs (2002)). In the Bayesian approach, named for the eighteenth-century mathematician and theologian Thomas Bayes, probabilities are interpreted as subjective degrees of belief, rather than frequencies. According to Bayes' theorem, or rule, the probability of a hypothesis, H, given some new data, D, is equal to the probability of that data given the hypothesis (i.e., the

conditional probability or "likelihood") times the prior probability of the hypothesis (the "prior"), all divided by the marginal probability of the data:

$$P(H|D) = \frac{P(D|H)P(H)}{P(D)}.$$

In other words, Bayes' rule tells you how to go about updating a probability distribution in light of new evidence. *Prima facie* there is an analogy between Bayesian updating and quantum measurements insofar as the quantum state gives a set of probabilities for various possible measurement outcomes, and once a measurement is performed information is gained and the probabilities are updated. In Chapter 7 of this volume Leah Henderson offers a critical analysis of this analogy. Drawing on the observation that an efficient quantum measurement is not just a refinement of the probability distribution but also involves an extra unitary transformation, she argues that there is an important disanalogy. Henderson proves that the measurements which can be interpreted as a Bayesian refinement plus a unitary transformation are precisely those measurements which increase our information about the quantum state, and conversely those measurements which do not fall into this category are quantum measurements in which information is actually lost. Such measurements, which increase the uncertainty about the state of the quantum system being measured, are shown to have no direct classical analogue.

The third section of this book turns from foundational questions about probability to foundational questions about the notion of information. In Chapter 8, Armond Duwell tackles head on the question of what precisely quantum information is. There has been considerable debate in the literature over whether quantum information just is classical information stored in quantum systems or whether the classical notion of information, as elaborated by Claude Shannon (1948), is somehow inadequate in this new context. If the classical conception is inadequate, then the question becomes that of what new notion of information should replace it? In his contribution to this volume, Duwell defends what is known as the Schumacher concept of quantum information, following the coding theorem of Ben Schumacher (1995). Duwell divides this notion of quantum information into two parts: quantum quantity-information, which quantifies the resources required to communicate, and quantum type-information, which is the kind of token required to be reproduced at the destination of a communication according to the success criterion of entanglement fidelity (see Duwell (2008) for further details). After discussing the theorem of Clifton, Bub, and Halvorson (2003), which derives quantum theory from three information-theoretic constraints in the context of a C^*-algebraic framework, Duwell criticizes a proposal by Bub that quantum mechanics should be reconceived as a theory of quantum information. Specifically, he argues that Bub

fails to define what notion of quantum information he is using. In a move sympathetic to Bub's approach, Duwell substitutes his own Schumacher notion of quantum information into Bub's proposal and explores the advantages of reconceiving quantum theory in this way.

Quantum information theory is concerned with exploiting the peculiarly quantum features of quantum mechanics to store, process, and transmit information in ways that cannot be achieved classically. This raises the important perennial question of precisely what features of quantum mechanics distinguish it from classical mechanics. Indeed, recent work in quantum information theory has revealed that many features that were thought to be peculiarly quantum turn out to have a classical analogue. In Chapter 9, Wayne Myrvold takes up the task of discovering what it is that makes quantum mechanics distinctive. In his search for the differences, he considers two neutral frameworks in which the classical and quantum theories can be formulated: the algebraic approach and the convex-set approach. He considers a toy theory developed by Rob Spekkens, which he argues reveals some of the key differences between these theories when considered in the context of the convex-set approach. Myrvold draws the intriguing conclusion that, while Schrödinger was right to identify the treatment of compound systems as the distinguishing feature of quantum mechanics, he was wrong to identify entanglement per se as what is distinctively quantum.

It has been argued that quantum information theory may hold the key to solving the conceptual puzzles of quantum mechanics. In Chapter 10, Chris Timpson takes stock of such proposals, arguing that many are just the old interpretative positions of immaterialism and instrumentalism in new guise. Immaterialism is the philosophical view that the world at bottom consists not of physical objects but of immaterial ones – in this context, the immaterial stuff of the world is information. As Timpson shows, this immaterialist view can be seen underlying John Wheeler's (1990) "It from bit" proposal and Zeilinger's "foundational principle" (1999). Similarly, instrumentalism is another philosophical approach that it has long been popular to invoke in the context of quantum mechanics, and has found new life in the context of quantum information theory. Instrumentalism is the view that the task of scientific theories is simply to provide a tool for making predictions – not to be a description of the fundamental objects and laws actually operating in the world. In this context instrumentalism argues that the quantum state is merely a representation of our information, one that allows us to make predictions about experiments, but which should not be thought of as a description of any objective features of the world. Timpson argues that merely re-dressing these well-worn philosophical positions in the new language of information theory does not in fact gain any interpretive ground. After providing a detailed critical analysis of Zeilinger's foundational approach, Timpson concludes that there is indeed

great promise for gaining new insights into the structure and axiomatics of quantum mechanics by focusing on information-theoretic phenomena, as long as one steers clear of the non-starters of immaterialism and instrumentalism.

The final section of the book, on "quantum communication and computing," examines some of the philosophical and foundational questions arising from the new technologies that are emerging from quantum information theory. One of the most tantalizing technologies promised by quantum information theory is the quantum computer. A quantum computer is a computer that exploits the peculiarly quantum features of quantum systems to aid in the processing of data. Much of the interest in quantum computing arose when Peter Shor (1994) devised an algorithm showing that a quantum computer could in principle factor large numbers into primes exponentially faster than any conceivable classical computer. This application is particularly interesting because many current cryptographic protocols for keeping information secure depend on the fact that classical algorithms for factoring take exponentially long; hence, if such a quantum computer were realized, it could pose a threat to the security of the large quantities of information protected in this way.

A few other quantum algorithms have been devised for performing various computations in ways superior to their classical counterparts. Although there are practical issues surrounding the implementation of a quantum computer, one of the key foundational questions is that of determining which feature of quantum mechanics is responsible for the superior computing power of quantum computers. Surprisingly, there is very little agreement over how to answer this question: some have claimed that the speed-up is due to the superposition rule, some attribute it to entanglement, and yet others have claimed that the speed-up of a quantum computer is direct evidence for the so-called "many-worlds" interpretation of quantum mechanics (Deutsch (1997); for critical reviews see Duwell (2007) and Jaeger (2009)). In Chapter 11, Jeffrey Bub proposes a new answer to the question of where the speed-up comes from. According to Bub, the key lies in the difference between classical logic and quantum logic. More specifically, while a classical disjunction is true (or false) by virtue of the truth values of its disjuncts, a quantum disjunction can be true (or false) without any of its disjuncts taking on a truth value at all. Similarly, in the quantum case, a global or disjunctive property of a function is encoded as a subspace of Hilbert space, and a quantum state can end up in a particular subspace without representing any particular pair of input–output values. This is in contrast to a classical computation, in which a global property is represented as a subset, and a classical state can end up in that subset only by ending up at a particular point in the subset (which requires a lot more information, to exclude other points in the subset). He argues that it is not that the quantum algorithm is somehow computing

all values of a function at once that makes it more efficient, but rather that it is in a sense able to avoid computing any values of the function at all.

In the final contribution to the volume, Tai Tsun Wu argues that we need to fundamentally rethink the way we model quantum computing and quantum cryptography. In particular, he argues that the notion of a quantum memory (or quantum register) needs to be included. The content of a quantum memory is a pure state that gets updated to another pure state during a computation via a unitary transformation. The most natural way to model this updating is as a scattering interaction, which is described by the Schrödinger equation and takes the spatial variable explicitly into account. Wu argues that this more physically realistic way of modeling quantum memory leads to a number of surprising results. For example, in the case of quantum key distribution, an analysis of quantum memory using scattering reveals new insecurities. Through a careful examination of the "B92" protocol of Bennett, Wu shows that, by using scattering with one or more spatial variables, forbidden operations such as quantum cloning actually become possible.

As we have seen in this brief overview, quantum information science is in the process of transforming our understanding of both quantum mechanics and information theory. The papers collected in this volume mark an important first step, though there remain many more questions to be explored. Our hope is that this volume will provide a useful starting point for those entering this new interdisciplinary field, and will encourage more philosophers and physicists to enter into the dialogue on the exciting philosophical implications of quantum information research.

References

Acín, A., T. Durt, N. Gisin, and J. Latorre (2002), Quantum non-locality in two three-level systems, *Phys. Rev. A* **65**, 052325.

Aspect, A., J. Dalibard, and G. Roger (1982), Experimental test of Bell's inequalities using time-varying analyzers, *Phys. Rev. Lett.*, **49**, 1804–1807.

Barnum, H., E. Knill, G. Ortiz, R. Somma, and L. Viola (2004), A subsystem-independent generalization of entanglement, *Phys. Rev. Lett.* **92**, 107902.

Barrett, J., N. Linden, S. Massar, S. Pirionio, S. Popescu and D. Roberts (2005), Nonlocal correlations as an information-theoretic resource, *Phys. Rev.* A **71**, 022101.

Bell, J. S. (1964), On the Einstein–Podolsky–Rosen paradox, *Physics* **1**, 195–200. (Reprinted in J. S. Bell (1993), *Speakable and Unspeakable in Quantum Mechanics* (Cambridge: Cambridge University Press), pp. 14–21.)

Bennett, C., G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, (1996), Purification of noisy entanglement and faithful teleportation via noisy channels, *Phys. Rev. Lett.* **76**, 722–725.

Bennett, C., D. DiVincenzo, C. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. Wootters (1999), Quantum non-locality without entanglement, *Phys. Rev. A* **59**, 1070–1091.

Brunner, N., N. Gisin, and V. Scarani (2005), Entanglement and non-locality are different resources, *New J. Phys.* **7**, 88.

Bub, J. (1977), Von Neumann's projection postulate as a probability conditionalization rule in quantum mechanics, *J. Philos. Logic* **6**, 381–390.

(2004), Why the quantum?, *Studies History Philos. Mod. Phys.* **35**, 241–266.

Clauser, J., M. Horne, A. Shimony, and R. Holt (1969), Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.* **23**, 880–884.

Clifton, R., J. Bub, and H. Halvorson (2003), Characterizing quantum theory in terms of information-theoretic constraints, *Foundations Phys.* **33**, 1561–1591.

Cushing, J. and E. McMullin (eds.), (1989), *Philosophical Consequences of Quantum Theory: Reflections on Bell's Theorem* (Notre Dame: University of Notre Dame Press).

Deutsch, D. (1997), *The Fabric of Reality* (New York: The Penguin Press).

Deutsch, D. and P. Hayden (2000), Information flow in entangled quantum systems, *Proc. Roy. Soc. London A*, **456**, 1759–1774.

Duwell, A. (2007), The many-worlds interpretation and quantum computation, *Philos. Sci.* **74**, 1007–1018.

(2008), Quantum information does exist, *Studies History Philos. Mod. Phys.* **39**, 195–216.

Einstein, A., B. Podolsky, and N. Rosen (1935), Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47**, 777–780.

Fine, A. (2008), The Einstein–Podolsky–Rosen argument in quantum theory, in *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, E. N. Zalta (ed.), URL <http://plato.stanford.edu/archives/fall2008/entries/qt-epr/>.

Fuchs, C. (2002), Quantum mechanics as quantum information (and only a little more), arXiv:quant-ph/0205039v1.

Gisin, N. (1991), Bell's inequality holds for all non-product states, *Phys. Lett. A* **154**, 201–202.

Hardy, L. (2001), Quantum theory from five reasonable axioms, arXiv:quant-ph/0101012v4.

Howard, D. (1990), 'Nicht sein kann was nicht sein darf,' or the prehistory of EPR, 1909–1935: Einstein's early worries about the quantum mechanics of composite systems, in *Sixty-Two Years of Uncertainty: Historical, Philosophical, and Physical Inquiries into the Foundations of Quantum Mechanics*, A. Miller (ed.) (New York: Plenum), pp. 61–111.

Horodecki, M., P. Horodecki, and R. Horodecki (1998), Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? *Phys. Rev. Lett.* **80**, 5239–5242.

Jaeger, G. (2007), *Quantum Information: An Overview* (New York: Springer).

(2009), *Entanglement, Information, and the Interpretation of Quantum Mechanics* (New York: Springer).

Jarrett, J. (1984), On the physical significance of the locality conditions in the Bell arguments, *Noûs* **18**, 569–589.

Maudlin, T. (1994), *Quantum Nonlocality and Relativity* (Oxford: Blackwell).

Mayers, D. (1997), Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78**, 3414–3417.

Niset, J. and N. Cerf (2006), Multipartite non-locality without entanglement in many dimensions, *Phys. Rev. A* **74**, 052103.

Penrose, R. (1998), Quantum computation, entanglement and state reduction. *Philos. Trans. Roy. Soc. London A* **356**, 1927–1939.

Popescu, S. (1995), Bell's inequalities and density matrices: revealing 'hidden' non-locality, *Phys. Rev. Lett.* **74**, 2619–2622.
Popescu, S. and D. Rohrlich (1994), Nonlocality as an axiom, *Foundations Phys.* **24**, 379–385.
Schrödinger, E. (1935a), Discussion of probability relations between separated systems, *Proc. Cambridge Philos. Soc.*, **31**, 555–562.
Schrödinger, E. (1935b), Die gegenwärtige Situation in der Quantenmechanik, *Naturwissenschaften*, **23**, 807–812, 823–828, 844–849; English translation by J. D. Trimmer (1980), The present situation in quantum mechanics: a translation of Schrödinger's 'cat paradox' paper, *Proc. Am. Philos. Soc.* **124**, 323–338.
Schumacher, B. (1995), Quantum coding, *Phys. Rev. A* **51**, 2738–2747.
Shannon, C. (1948), A mathematical theory of communication, *Bell Syst. Techn. J.* **27**, 379–423, 623–656.
Shimony, A. (1984), Controllable and uncontrollable non-locality, in *Foundations of Quantum Mechanics in Light of the New Technology*, S. Kamefuchi *et al.* (eds.) (Tokyo: Physical Society of Japan), pp. 225–230. (Reprinted in A. Shimony (1993), *Search for Naturalistic World View*, Vol. 2 (Cambridge: Cambridge University Press), pp. 130–139.)
(1995), Degree of entanglement, *Annals New York Acad. Sci.* **755**, 675–679.
(2008), Bell's theorem, in *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)*, E. N. Zalta (ed.), URL <http://plato.stanford.edu/archives/fall2008/entries/bell-theorem/>.
Shor, P. (1994), Algorithms for quantum computation: discrete log and factoring, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S. Goldwasser (ed.) (New York: IEEE Computer Society Press), pp. 124–134.
Timpson, C. (2006), The grammar of teleportation, *Brit. J. Philos. Sci.* **57**, 587–621.
Werner, R. (1989), Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model, *Phys. Rev. A* **40**, 4277–4281.
Werner, R. and M. Wolf (2001), Bell inequalities and entanglement, arXiv:quant-ph/0107093v2.
Wheeler, J. (1990), Information, physics, quantum: the search for links, in *Complexity, Entropy and the Physics of Information*, W. Zurek (ed.) (Redwood City, CA: Addison-Wesley), pp. 3–28.
Zeilinger, A. (1999), A foundational principle for quantum mechanics, *Foundations Phys.* **29**, 631–643.