Quantum Foundations

in the light of

Quantum Information

Gilles Brassard
Université de Montréal

Christopher Fuchs
Bell Labs, Lucent Technologies

QIP 2004, Waterloo

Quantum Foundations in the Light of Quantum Information

Christopher A. Fuchs
Computing Science Research Center
Bell Labs, Lucent Technologies
Room 2C-420, 600–700 Mountain Ave.
Murray Hill, New Jersey 07974, USA

Abstract

In this paper, I try to cause some good-natured trouble. The issue at stake is when will we ever stop burdening the taxpayer with conferences and workshops devoted—explicitly or implicitly—to the quantum foundations? The suspicion is expressed that no end will be in sight until a means is found to reduce quantum theory to two or three statements of crisp *physical* (rather than abstract, axiomatic) significance. In this regard, no tool appears to be better calibrated for a direct assault than quantum information theory. Far from being a strained application of the latest fad to a deep-seated problem, this method holds promise precisely because a large part (but not all) of the structure of quantum theory has always concerned information. It is just that the physics community has somehow forgotten this.

1 Imprimatur

im·pri·ma·tur (ĭm´pre-mä[1]ter, -mâ[1]ter)
1. Official approval or license to print or publish, especially under conditions of censorship.
— *American Heritage Dictionary*

The title of the NATO Advanced Research Workshop that gave birth to this volume was "Decoherence and its Implications in Quantum Computation and Information Transfer." It was a wonderful meeting—the kind most of us lick our lips for year after year, with little hope of ever tasting. It combined the best of science with the exotic solitude of an island far, far away. One could not help but have a creative thought shaken loose with each afternoon's gusty wind. Indeed, it was a meeting that will make NATO proud. But, as any attendee can tell you, the most popular pastime—in spite of those windy beaches and dark tans—was an

Quantum Foundations in the Light of Quantum Information

Christopher A. Fuchs

Computing Science Research Center
Bell Labs, Lucent Technologies
Room 2C-420, 600–700 Mountain Ave.
Murray Hill, New Jersey 07974, USA

Abstract

In this paper, I try to cause some good-natured trouble. The issue at stake is when will we ever stop burdening the taxpayer with conferences and workshops devoted—explicitly or implicitly—to the quantum foundations? The suspicion is expressed that no end will be in sight until a means is found to reduce quantum theory to two or three statements of crisp *physical* (rather than abstract, axiomatic) significance. In this regard, no tool appears to be better calibrated for a direct assault than quantum information theory. Far from being a strained application of the latest fad to a deep-seated problem, this method holds promise precisely because a large part (but not all) of the structure of quantum theory has always concerned information. It is just that the physics community has somehow forgotten this.

Quantum Mechanics as Quantum Information (and only a little more)

Christopher A. Fuchs

Computing Science Research Center
Bell Labs, Lucent Technologies
Room 2C-420, 600–700 Mountain Ave.
Murray Hill, New Jersey 07974, USA

Abstract

In this paper, I try once again to cause some good-natured trouble. The issue remains, when will we ever stop burdening the taxpayer with conferences devoted to the quantum foundations? The suspicion is expressed that no end will be in sight until a means is found to reduce quantum theory to two or three statements of crisp physical (rather than abstract, axiomatic) significance. In this regard, no tool appears better calibrated for a direct assault than quantum information theory. Far from a strained application of the latest fad to a time-honored problem, this method holds promise precisely because a large part—*but not all*—of the structure of quantum theory has always concerned information. It is just that the physics community needs reminding.

This paper, though taking `quant-ph/0106166` as its core, corrects one mistake and offers several observations beyond the previous version. In particular, I identify one element of quantum mechanics that I would *not* label a subjective term in the theory—it is the integer parameter D traditionally ascribed to a quantum system via its Hilbert-space dimension.

1 Introduction [1]

Quantum theory as a weather-sturdy structure has been with us for 75 years now. Yet, there is a sense in which the struggle for its construction remains. I say this because one can check that not a year has gone by in the last 30 when there was not a meeting or conference devoted to some aspect of the quantum foundations. Our meeting in Växjö, "Quantum Theory: Reconsideration of Foundations," is only one in a long, dysfunctional line.

But how did this come about? What is the cause of this year-after-year sacrifice to the "great mystery?" Whatever it is, it cannot be for want of a self-ordained solution: Go to any meeting, and it is like being in a holy city in great tumult. You will find all the religions with all their priests pitted in holy war—the Bohmians [3], the Consistent Historians [4], the Transactionalists [5], the Spontaneous Collapseans [6], the Einselectionists [7], the Contextual Objectivists [8], the outright Everettics [9, 10], and many more beyond that. They all declare to see the light, the ultimate light. Each tells us that if we will accept their solution as our savior, then we too will see the light.

[1] This paper, though substantially longer, should be viewed as a continuation and amendment to Ref. [1]. Details of the changes can be found in the Appendix to the present paper, Section 11. Substantial further arguments defending a transition from the "objective Bayesian" stance implicit in Ref. [1] to the "subjective Bayesian" stance implicit here can be found in Ref. [2].

Quantum Mechanics as Quantum Information (and only a little more)

Christopher A. Fuchs

Computing Science Research Center
Bell Labs, Lucent Technologies
Room 2C-420, 600–700 Mountain Ave.
Murray Hill, New Jersey 07974, USA

Abstract

In this paper, I try once again to cause some good-natured trouble. The issue remains, when will we ever stop burdening the taxpayer with conferences devoted to the quantum foundations? The suspicion is expressed that no end will be in sight until a means is found to reduce quantum theory to two or three statements of crisp physical (rather than abstract, axiomatic) significance. In this regard, no tool appears better calibrated for a direct assault than quantum information theory. Far from a strained application of the latest fad to a time-honored problem, this method holds promise precisely because a large part—*but not all*—of the structure of quantum theory has always concerned information. It is just that the physics community needs reminding.

This paper, though taking `quant-ph/0106166` as its core, corrects one mistake and offers several observations beyond the previous version. In particular, I identify one element of quantum mechanics that I would *not* label a subjective term in the theory—it is the integer parameter D traditionally ascribed to a quantum system via its Hilbert-space dimension.

We all of us have some idea
of what the basic axioms
in physics will turn out to be.
The quantum or the particle
will surely not be amongst them.

— Einstein, 1948

The axioms of Relativity

1. *The speed of light in empty space is independent of the speed of its source.*

2. *Physics should appear the same in all inertial reference frames.*

1. A linear vector space with complex coefficients and inner product

$$\langle \phi | \psi \rangle = \Sigma \phi_i^* \psi_i$$

2. For polarized photons two, e.g. vertical and horizonal

$$\leftrightarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \updownarrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3. E.g. for photons, other polarizations

$$\nearrow = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \searrow = \begin{pmatrix} +1 \\ -1 \end{pmatrix}$$

$$\circlearrowright = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad \circlearrowleft = \begin{pmatrix} i \\ -1 \end{pmatrix}$$

4. Unitary = Linear and inner-product preserving.

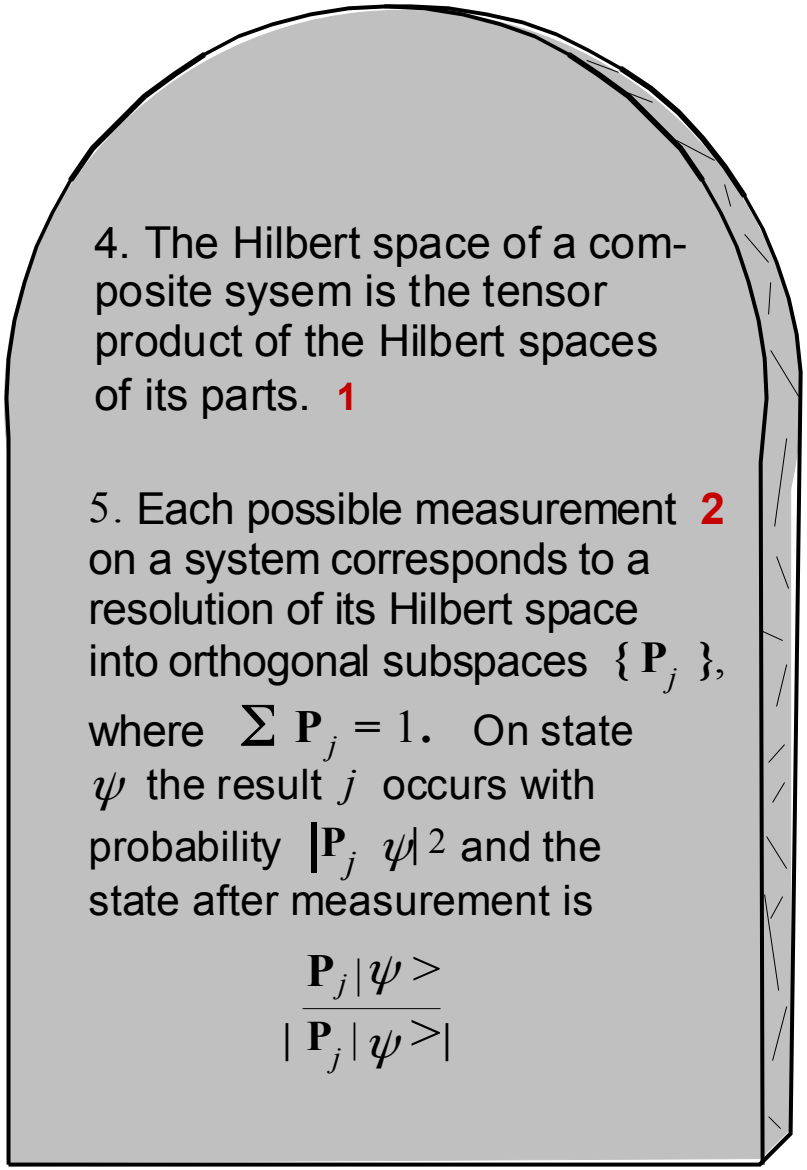
quantum laws

I. To each physical system there corresponds a Hilbert space [1] of dimensionality equal to the system's maximum number of reliably distinguishablee states. [2]

2. Each direction (ray) in the Hilbert space corresponds to a possible state of the system. [3]

3. Spontaneous evolution of an unobserved system is a unitary transformation on its Hilbert space. [4]

-- more --



4. The Hilbert space of a composite sysem is the tensor product of the Hilbert spaces of its parts. **1**

5. Each possible measurement **2** on a system corresponds to a resolution of its Hilbert space into orthogonal subspaces $\{\mathbf{P}_j\}$, where $\sum \mathbf{P}_j = 1$. On state ψ the result j occurs with probability $|\mathbf{P}_j\ \psi|^2$ and the state after measurement is

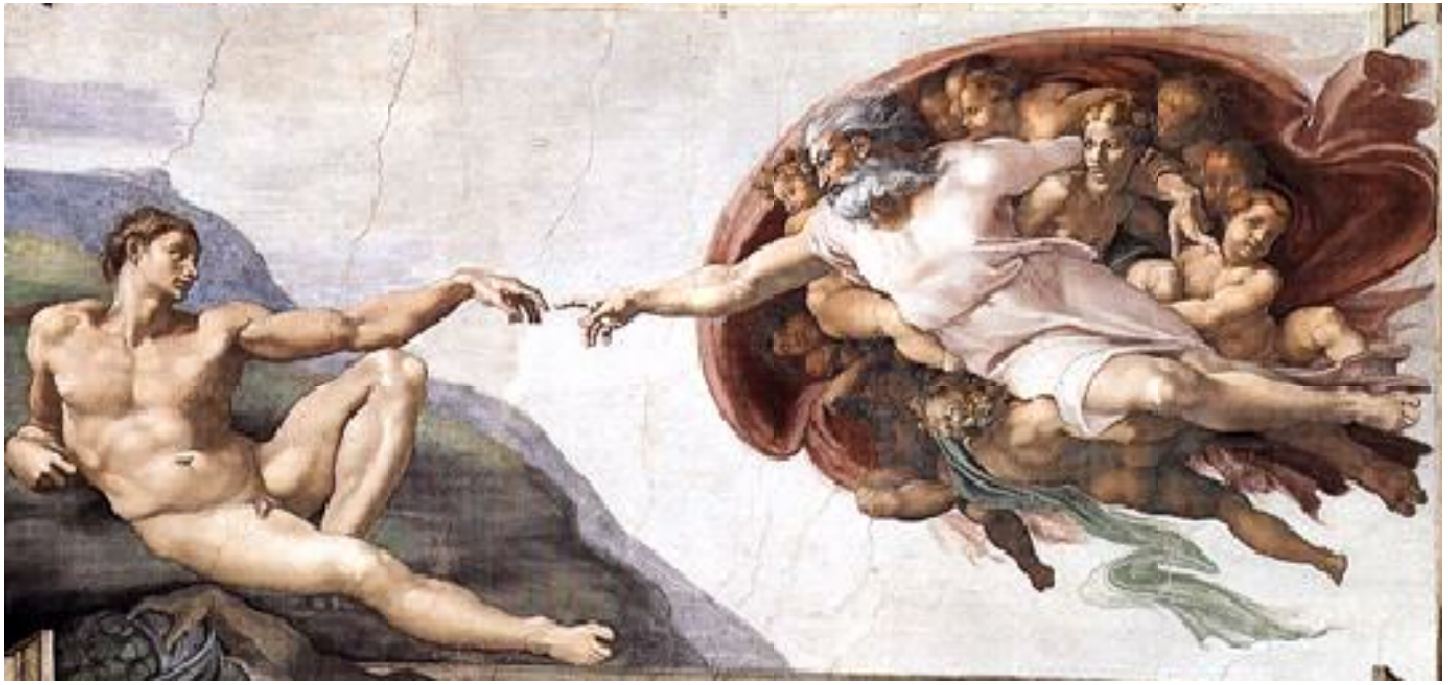
$$\frac{\mathbf{P}_j|\psi>}{|\mathbf{P}_j|\psi>|}$$

1. Thus a two-photon system can exist in "product states" such as ↔ ↔ and ↔ ⤢ but also in "entangled" states such as

$$\frac{\leftrightarrow\leftrightarrow \;-\; \updownarrow\updownarrow}{\sqrt{2}}$$

in which neither photon has a definite state even though the pair together does

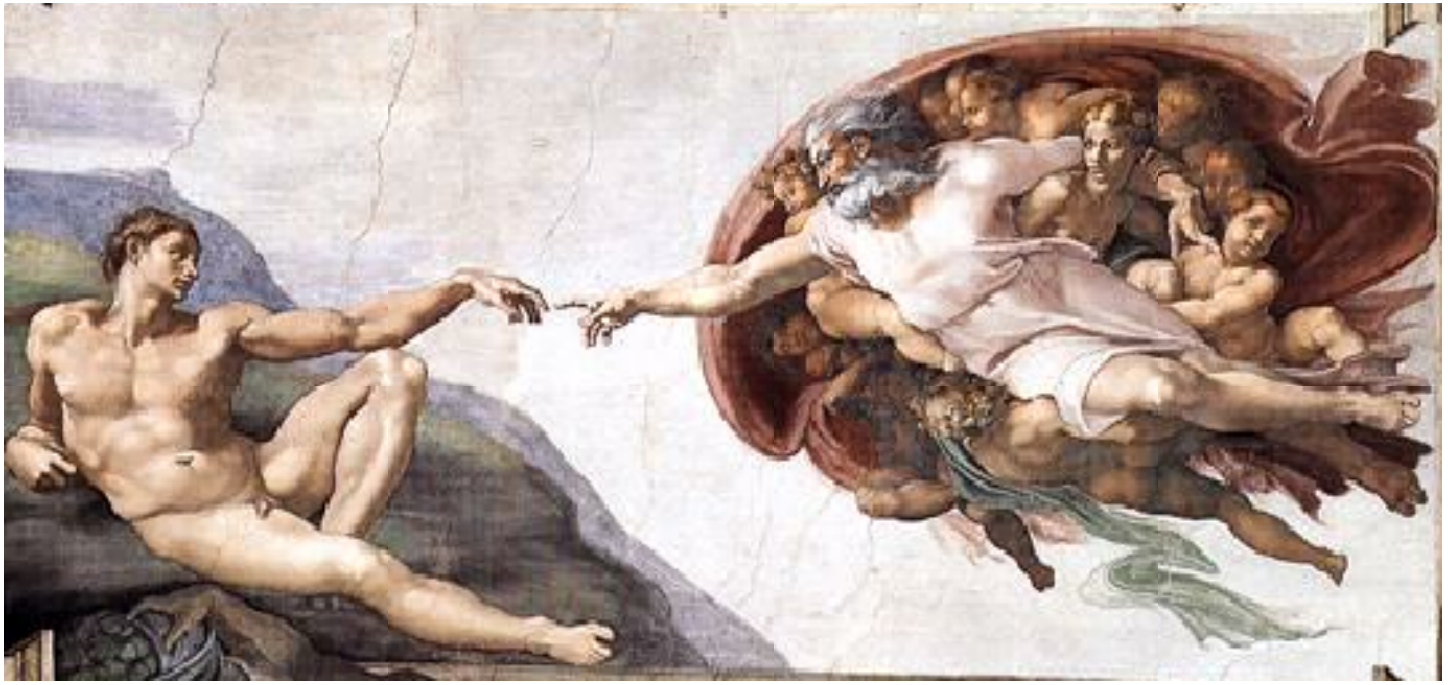
2 Believers in the "many worlds interpretation" reject this axiom as ugly and unnecessary. For them measurement is just a unitary evolution producing an entangled state of the system and measuring apparatus. For others, measurement causes the system to behave probabilistically and forget its pre-measurement state, unless that state happens to lie entirely within one of the subspaces $\mathbf{P}_j$.



And God said:

Let there be confidentiality

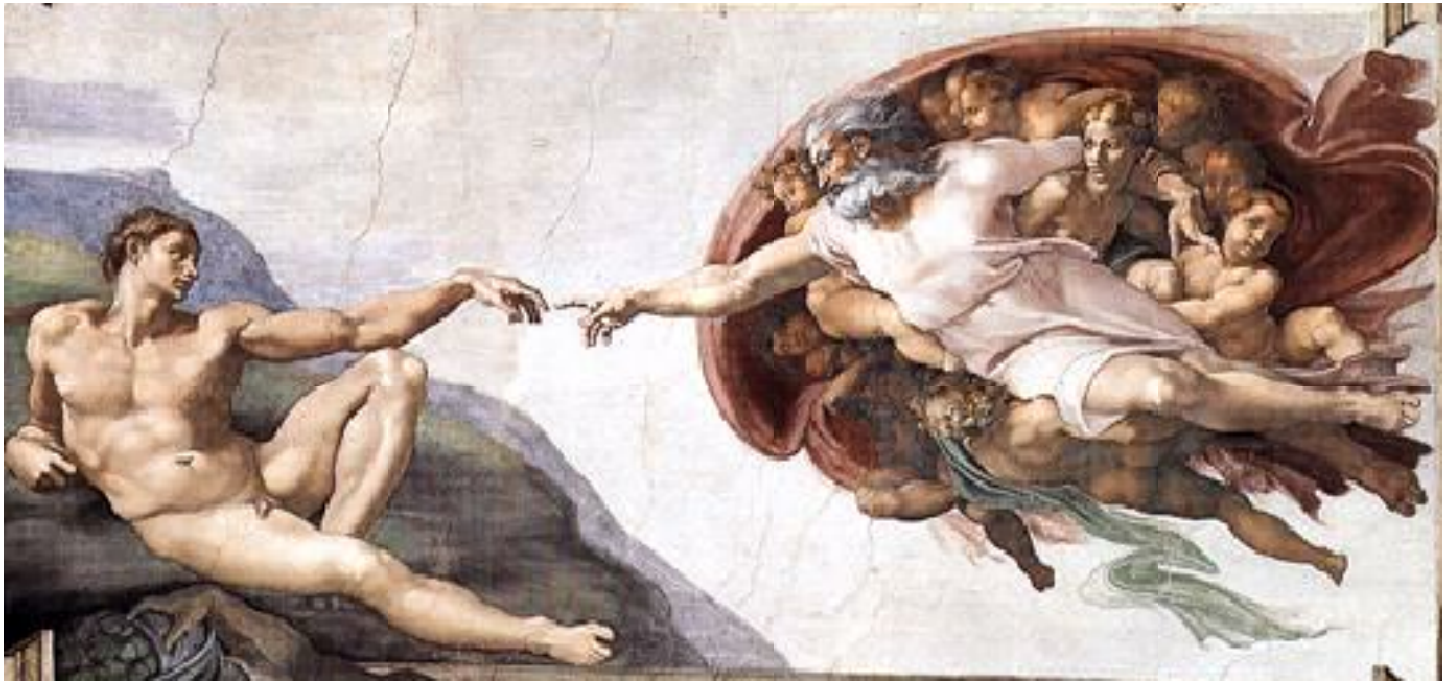
And he saw that was good



And then God said:

Let there be commitment

But he saw that was bad



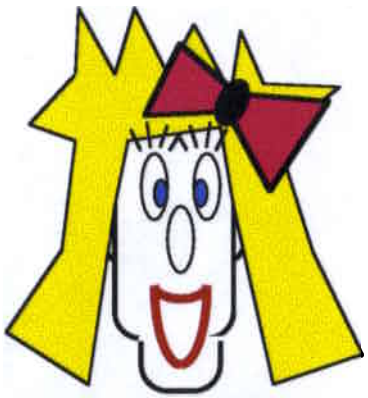
So God had no choice:

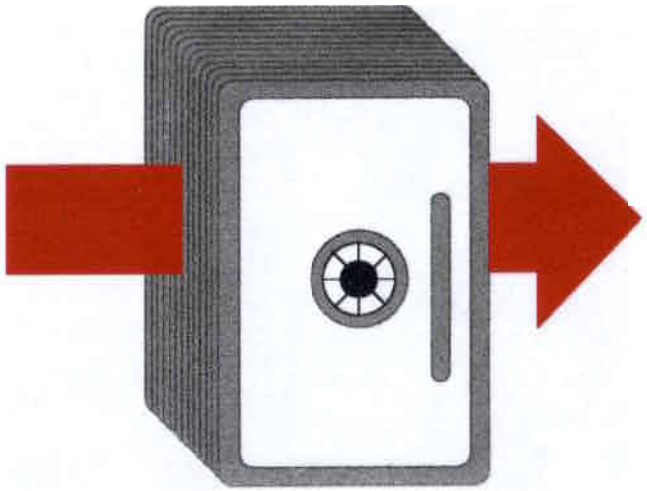
He invented Quantum Mechanics !

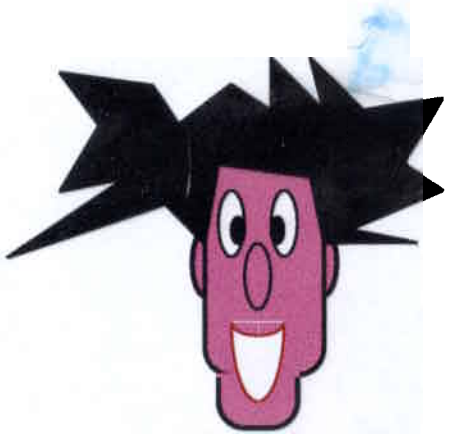
UPS and DOWNS of Quantum bit commitments

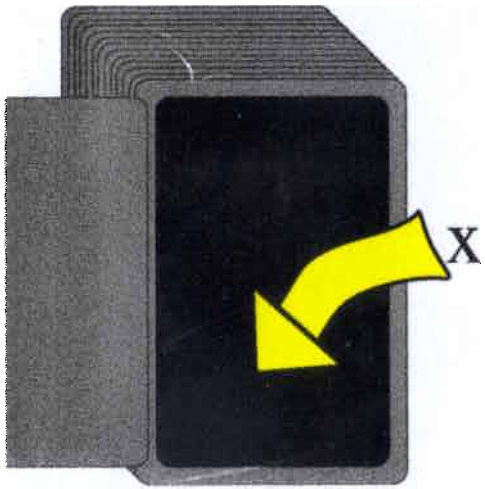
Gilles Brassard Université de Montréal
Claude Crépeau McGill University
Dominic Mayers Princeton University
Louis Salvail BRICS, Aarhus

Commit(x)

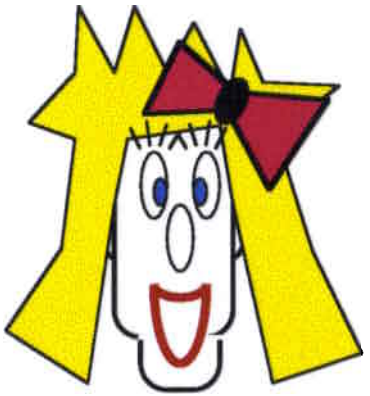


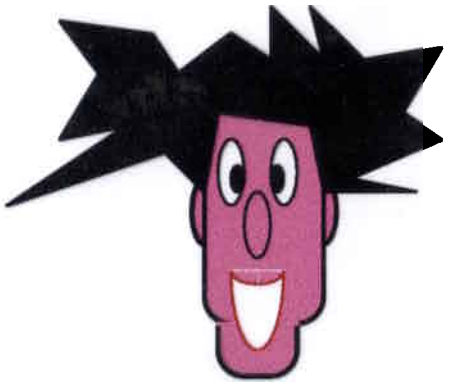


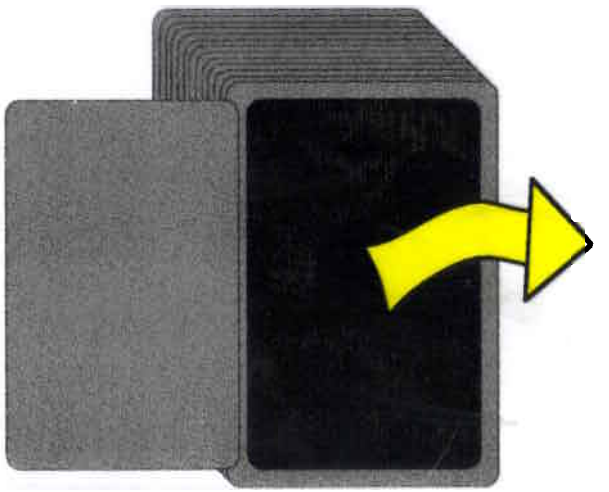




Unveil(x)







Properties of Bit Commitments

- Concealing:
  Bob cannot get information
  about x without Alice's help

- Binding:
  Alice cannot change value
  of x once committed

- Unconditional:
  Security is guaranteed
  no matter what

BB84 Bit Commitment

(coin tossing)

Fun but known to be insecure from the start!

(1984)

A QUANTUM BIT COMMITMENT SCHEME PROVABLY UNBREAKABLE BY BOTH PARTIES

Gilles Brassard
Claude Crépeau
Richard Jozsa
Denis Langlois

Reprinted from PROCEEDINGS OF THE 34th ANNUAL SYMPOSIUM
ON FOUNDATIONS OF COMPUTER SCIENCE, Palo Alto, California,
November 3 — 5, 1993

IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1264

Washington, DC • Los Alamitos • Brussels • Tokyo

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IEEE

IEEE COMPUTER SOCIETY

The Trouble with Quantum Bit Commitment

Dominic Mayers

Département IRO, Université de Montréal

C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.

(November 1, 2002)

Abstract

In a recent paper, Lo and Chau explain how to break a family of quantum bit commitment schemes, and they claim that their attack applies to the 1993 protocol of Brassard, Crépeau, Jozsa and Langlois (BCJL). The intuition behind their attack is correct, and indeed they expose a weakness common to all proposals of a certain kind, but the BCJL protocol does not fall in this category. Nevertheless, it is true that the BCJL protocol is insecure, but the required attack and proof are more subtle. Here we provide the first complete proof that the BCJL protocol is insecure.

1994 PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

The Trouble with Quantum Bit Commitment

Dominic Mayers

Département IRO, Université de Montréal

C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.

(November 1, 2002)

Is Quantum Bit Commitment Really Possible?

Hoi-Kwong Lo* and H. F. Chau†
School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540
(January 15, 2002)

We show that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can almost always cheat successfully by using an Einstein-Podolsky-Rosen type of attack and delaying her measurement until she opens her commitment.

PACS Numbers: 89.70.+c, 03.65.Bz, 89.80.+h

Work on quantum cryptography was started by S. J. Wiesner in a paper written in about 1970, but remained unpublished until 1983 [1]. Recently, there have been lots of renewed activities in the subject. The most well-known application of quantum cryptography is the so-called quantum key distribution (QKD) [2–4], which is useful for making communications between two users totally unintelligible to an eavesdropper. QKD takes advantage of the uncertainty principle of quantum mechanics: Measuring a quantum system in general disturbs it. Therefore, eavesdropping on a quantum communication channel will generally leave unavoidable disturbance in the transmitted signal which can be detected by the legitimate users. Besides QKD, other quantum cryptographic protocols [5] have also been proposed. In particular, it is generally believed [4] that quantum mechanics can protect private information while it is being used for public decision. Suppose Alice has a secret x and Bob a secret y. In a "two-party secure computation" (TPSC), Alice and Bob compute a prescribed function $f(x, y)$ in such a way that nothing about each party's input is disclosed to the other, except for what follows logically from one's private input and the function's output. An example of the TPSC is the millionaires' problem: Two persons would like to know who is richer, but neither wishes the other to know the exact amount of money he/she has.

In classical cryptography, TPSC can be achieved either through trusted intermediaries or by invoking some unproven computational assumptions such as the hardness of factoring large integers. The great expectation is that quantum cryptography can get rid of those requirements and achieve the same goal using the laws of physics alone. At the heart of such optimism has been the widespread belief that *unconditionally* secure quantum bit commitment (QBC) schemes exist [6]. Here we put such optimism into very serious doubt by showing that *all* proposed QBC schemes are insecure: A dishonest party can exploit the non-local Einstein-Podolsky-Rosen (EPR) [18] type correlations in quantum mechanics to cheat successfully. To do so, she generally needs to maintain the coherence of her share of a quantum system by using a quantum computer. We remark that all proposed QBC schemes contain an invalid implicit assumption that some measurements are performed by the two participants. This is why this EPR-type of attack was missed in earlier analysis.

Let us first introduce bit commitment. A bit commitment scheme generally involves two parties, a sender, Alice and a receiver, Bob. Suppose that Alice has a bit ($b = 0$ or 1) in mind, to which she would like to be committed towards Bob. That is, she wishes to provide Bob with a piece of evidence that she has already chosen the bit and that she cannot change it. Meanwhile, Bob should not be able to tell from that evidence what b is. At a later time, however, it must be possible for Alice to *open* the commitment. In other words, Alice must be able to show Bob which bit she has committed to and convince him that this is indeed the genuine bit that she had in mind when she committed.

A concrete example of an implementation of bit commitment is for Alice to write down her bit in a piece of paper, which is then put in a locked box and handed over to Bob. While Alice cannot change the value of the bit that she has written down, without the key to the box Bob cannot learn it himself. At a later time, Alice gives the key to Bob, who opens the box and recovers the value of the committed bit. This illustrative example of implementation is, however, inconvenient and insecure. A locked box may be very heavy and Bob may still try to open it by brute force (e.g. with a hammer).

What do we mean by cheating? As an example, a cheating Alice may choose a particular value of b during the commitment phase and tell Bob *another* value during the opening phase. A bit commitment scheme is secure against a cheating Alice only if such a fake commitment can be discovered by Bob. For concreteness, it is instructive to consider a simple QBC protocol due to Bennett and Brassard [2]. Its procedure goes as follows: Alice and Bob first agree on a security parameter, a positive integer s. The sender, Alice, chooses the value of the committed bit, b. If $b = 0$, she prepares and sends Bob a sequence

*Present Address: BRIMS, Hewlett-Packard Labs, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK. e-mail: hkl@hplb.hpl.hp.com

†Present Address: Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong. e-mail: hfchau@hkusua.hku.hk

Is Quantum Bit Commitment Really Possible?

Hoi-Kwong Lo* and H. F. Chau†
School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540
(January 15, 2002)

We show that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can almost always cheat successfully by using an Einstein-Podolsky-Rosen type of attack and delaying her measurement until she opens her commitment.

Unconditionally secure quantum bit commitment is impossible

Dominic Mayers
Département IRO, Université de Montréal
C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.
(August 9, 2002)

The claim of quantum cryptography has always been that it can provide protocols that are unconditionally secure, that is, for which the security does not depend on any restriction on the time, space or technology available to the cheaters. We show that this claim does not hold for any quantum bit commitment protocol. Since many cryptographic tasks use bit commitment as a basic primitive, this result implies a severe setback for quantum cryptography. The model used encompasses all reasonable implementations of quantum bit commitment protocols in which the participants have not met before, including those that make use of the theory of special relativity.

1994 PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

a. Introduction. Quantum cryptography is often associated with a cryptographic application called key distribution [1,2] and it has achieved success in this area [5]. However, other applications of quantum mechanics to cryptography have also been considered and a basic cryptographic primitive called bit commitment, the main focus of this letter, was at the basis of most if not all of these other applications [3,6,15,5].

In a concrete example of bit commitment, a party, Alice, writes a bit b on a piece of paper and puts it into a safe. She gives the safe to another party, Bob, but keeps the key. The objective of this scheme, and of bit commitment in general, is that Alice cannot change her mind about the value of the bit b, but meanwhile Bob cannot determine the bit b. At a later time, if Alice wants to unveil b to Bob, she gives the key to Bob.

In 1993, a protocol was proposed to realize bit commitment in the framework of quantum mechanics, and the unconditional security (see sections b and c) of this protocol has been generally accepted for quite some time. However, this result turned out to be wrong. The non security of this protocol, called the BCJL protocol, was realized in the fall of 1995 [12]. After this discovery, Brassard, Crépeau and other researchers have tried to find alternative protocols [4]. Some protocols were based on the theory of special relativity. For additional information about the history of the result see [5]. See also [11].

Here it is shown that an unconditionally secure bit commitment protocol is impossible, unless a computing device, such as a beam splitter, a quantum gate, etc. can be simultaneously trusted by both participants in the protocol. This encompasses any protocol based on the theory of special relativity. A preliminary version of the proof appeared in [13].

b. The model for quantum protocols. It is neither possible in this letter to describe in detail a model for two-party quantum protocols, nor is it is useful for the purpose of this letter. The following description includes all that is necessary for our proof.

In our model, a two-party quantum protocol is executed on a system $H_A \otimes H_B \otimes H_E$ where H_A and H_B correspond to two areas, one on Alice's side and one on Bob's side, and H_E corresponds to the environment. We adopt the "decoherence" point of view in which a mixed state ρ of $H_A \otimes H_B$ is really the reduced state of $H_A \otimes H_B$ entangled with the environment H_E, the total system $H_A \otimes H_B \otimes H_E$ always being in a pure state $|\psi\rangle$. The systems H_A and H_B contain only two dimensional quantum registers. Higher dimensional systems can be constructed out of two dimensional systems. Alice and Bob can execute any unitary transformation on their respective system. In particular, they can introduce new quantum registers in a fixed state $|0\rangle$. States that correspond to different number of registers can be in linear superposition. Any mode of quantum communication can be adopted between Alice and Bob.

Without loss of generality, we can restrict ourselves to binary outcome measurements. The environment is of the form $H_E = H_S \otimes H_{E,A} \otimes H_{E,B}$ where $H_S = H_{S,A} \otimes H_{S,B}$ is a system that stores classical bits that have been transmitted from $H_{S,A}$ on Alice's side to $H_{S,B}$ on Bob's side or vice versa, and $H_{E,A}$ and $H_{E,B}$ store untransmitted classical bits that are kept on Alice's side and Bob's side respectively. To execute a binary outcome measurement, a participant $P \in \{A, B\}$, where A and B stand for Alice and Bob respectively, introduces a quantum register in a fixed state $|0\rangle$. The participant P entangles this register with the measured system initially in a state $|\phi\rangle$ and obtains a new state of the form $\alpha|0\rangle|\phi_0\rangle + \beta|1\rangle|\phi_1\rangle$. Then, he sends the new quantum register away to a measuring apparatus in $H_{E,P}$ which amplifies and stores each component $|x\rangle$ as a complex state $|x\rangle^{(E,P)}$. The resulting state is $\alpha|0\rangle^{(E,P)}|\phi_0\rangle + \beta|1\rangle^{(E,P)}|\phi_1\rangle$. Similarly, to generate a random bit one simply maps $|0\rangle$ into $\alpha|0\rangle + \beta|1\rangle$ and sends the register away in some part of $H_{E,P}$ that will amplify and store it as a state $\alpha|0\rangle^{(E,P)} + \beta|1\rangle^{(E,P)}$. The transmission of a classical bit x from Alice to Bob is represented by a transformation that maps $|x\rangle^{(E,A)}|0\rangle^{(E,B)}$ into $|x\rangle^{(S,A)}|x\rangle^{(S,B)}$. A similar transformation exists for the transmission of a classical bit from Bob to Alice.

Now, let us assume that the total system is in a super-

Unconditionally secure quantum bit commitment is impossible

Dominic Mayers
Département IRO, Université de Montréal
C.P. 6128, succursale Centre-Ville,Montréal (Québec), Canada H3C 3J7.
(August 9, 2002)

The claim of quantum cryptography has always been that it can provide protocols that are unconditionally secure, that is, for which the security does not depend on any restriction on the time, space or technology available to the cheaters. We show that this claim does not hold for any quantum bit commitment protocol. Since many cryptographic tasks use bit commitment as a basic primitive, this result implies a severe setback for quantum cryptography. The model used encompasses all reasonable implementations of quantum bit commitment protocols in which the participants have not met before, including those that make use of the theory of special relativity.

proof appeared in [13].

b. The model for quantum protocols. It is neither possible in this letter to describe in detail a model for two-party quantum protocols, nor is it is useful for the purpose of this letter. The following description includes all that is necessary for our proof.

In our model, a two-party quantum protocol is executed on a system $H_A \otimes H_B \otimes H_E$ where H_A and H_B correspond to two areas, one on Alice's side and one on Bob's side, and H_E corresponds to the environment. We adopt the "decoherence" point of view in which a mixed state ρ of $H_A \otimes H_B$ is really the reduced state of $H_A \otimes H_B$

PhysComp96
Full paper
Draft, 10 May, 1996
Revised, 21 July 1996
IASSNS-HEP-96/50
quant-ph/9605026

Why quantum bit commitment and ideal quantum coin tossing are impossible.*

Hoi-Kwong Lo† and H. F. Chau‡
School of Natural Sciences, Institute for Advanced Study, Princeton, NJ 08540

There had been well known claims of "provably unbreakable" quantum protocols for bit commitment and coin tossing. However, we, and independently Mayers, showed that all proposed quantum bit commitment (and therefore coin tossing) schemes are, in principle, insecure because the sender, Alice, can always cheat successfully by using an EPR-type of attack and delaying her measurements. One might wonder if secure quantum bit commitment and coin tossing protocols exist at all. Here we prove that an EPR-type of attack by Alice will, in principle, break any realistic quantum bit commitment and *ideal* coin tossing scheme. Therefore, provided that Alice has a quantum computer and is capable of storing quantum signals for an arbitrary length of time, all those schemes are insecure. Since bit commitment and coin tossing are useful primitives for building up more sophisticated protocols such as zero-knowledge proofs, our results cast very serious doubt on the security of quantum cryptography in the so-called "post-cold-war" applications.

1 Introduction

Quantum cryptography was first proposed by Wiesner [21] more than two decades ago in a paper that remained unpublished until 1983. Recently, there have been lots of renewed activities in the subject. The most well-known application of quantum cryptography is key distribution [1, 6, 10]. The aim of key distribution is to allow two users to generate a shared random string of information that can, for example, be used to make their messages in subsequent communication totally unintelligible to an eavesdropper. Quantum key distribution is secure [3, 9, 16, 18, 20] because, it is impossible (for an eavesdropper) to make copies (or clones) of non-orthogonal states in quantum mechanics without violating unitarity. Moreover, measuring a quantum system generally disturbs it because quantum mechanical observables can be non-commuting. For this reason, eavesdropping an a quantum communication channel will generally leave unavoidable disturbance in the transmitted signal which can be detected by the legitimate users.

In addition to key distribution, the so-called "post-cold-war" applications of quantum cryptography have also been proposed [1, 2, 4, 5, 7, 8]. A typical problem in "post-cold-war" quantum cryptography is the two-party secure computation, in which both parties would like to know the result of a computation but neither side wishes to reveal its own data. For example, two firms will embark on a joint venture if and only if their combined capital available for the project is larger than one million dollars. They would like to know if this condition is fulfilled but neither wishes to reveal the exact amount of capital it commits to the project. In classical cryptography, this can be done either through trusted intermediaries or by invoking some unproven cryptographic assumptions such as the hardness of factoring. The big question is whether quantum cryptography can get rid of those requirements and achieve the same goal using the laws of physics alone.

This paper relates to those post-cold-war applications of quantum cryptography. Until recently, there had been much optimism in the subject. Various protocols for say bit commitment, coin tossing and oblivious transfer of quantum cryptography had been proposed [1, 2, 4, 5, 7, 8]. In particular, the BCJL [8] bit commitment scheme had been claimed to be provably unbreakable. However, in our recent paper [17], we showed that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can always cheat successfully by using an EPR-type of attack and delaying her measurement until she opens her commitment. (The insecurity of the BCJL scheme was also investigated by Mayers [19] from an information-theoretic point of view.) Our result put the security of post-cold-war quantum cryptographic systems in serious doubt because bit commitment is a crucial primitive in building up more sophisticated protocols. In particular, it has been shown by Yao [22] that a secure quantum bit commitment scheme can be used to implement a secure quantum oblivious transfer scheme whereas Kilian [15] has shown that, in classical cryptography, oblivious transfer can be used to implement many protocols such as oblivious circuit evaluation, which is a close cousin of secure two-party computation. This chain of arguments, therefore, seems to suggest that quantum bit commitment alone is sufficient for implementing secure two-party computation or its close cousin. However, without quantum bit commitment, it is not clear if secure two-party com-

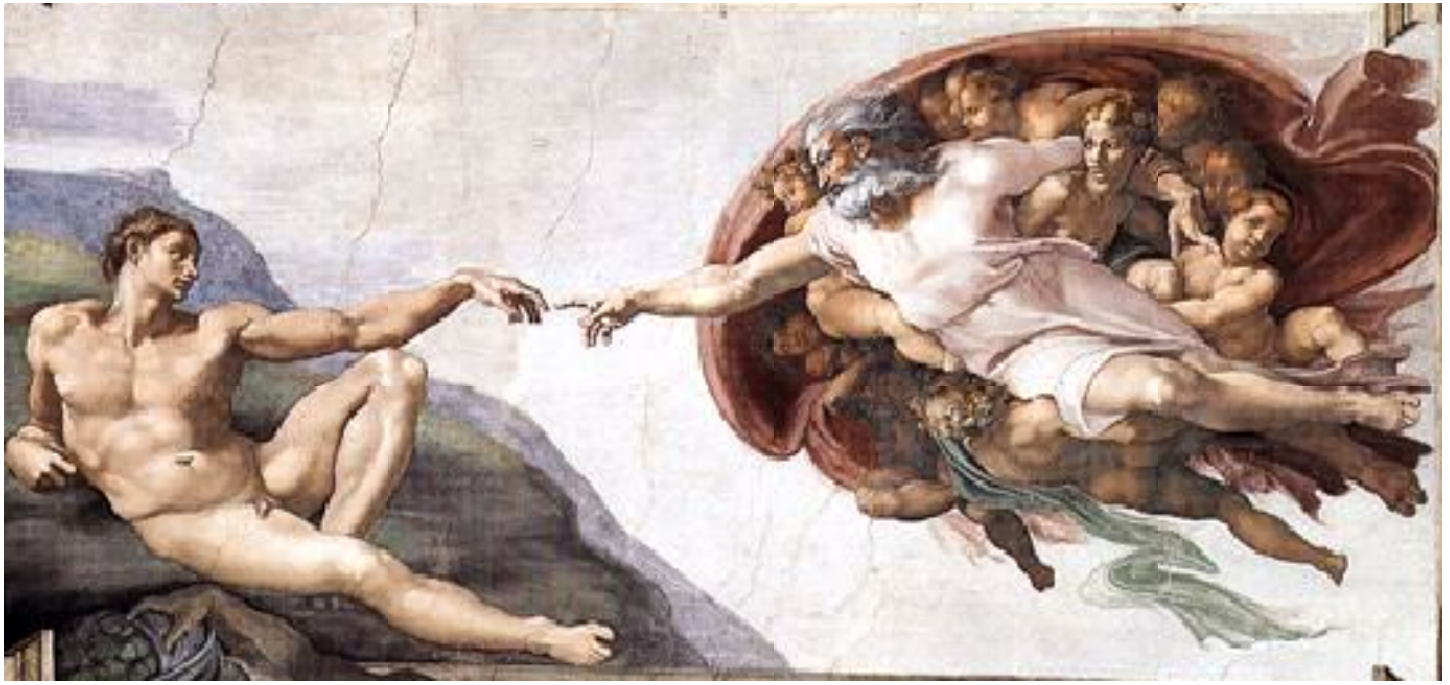
*Supported by DOE grant DE-FG02-90ER40542
†Address after 1 Oct., 96: BRIMS, Hewlett-Packard Labs, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK
‡Address after 1 July, 96: Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong

PhysComp96
Full paper
Draft, 10 May, 1996
Revised, 21 July 1996
IASSNS-HEP-96/50
quant-ph/9605026

Why quantum bit commitment and ideal quantum coin tossing are impossible.*

Hoi-Kwong Lo† and H. F. Chau‡
School of Natural Sciences, Institute for Advanced Study, Princeton, NJ 08540

There had been well known claims of "provably unbreakable" quantum protocols for bit commitment and coin tossing. However, we, and independently Mayers, showed that all proposed quantum bit commitment (and therefore coin tossing) schemes are, in principle, insecure because the sender, Alice, can always cheat successfully by using an EPR-type of attack and delaying her measurements. One might wonder if secure quantum bit commitment and coin tossing protocols exist at all. Here we prove that an EPR-type of attack by Alice will, in principle, break *any* realistic quantum bit commitment and *ideal* coin tossing scheme. Therefore, provided that Alice has a quantum computer and is capable of storing quantum signals for an arbitrary length of time, all those schemes are insecure. Since bit commitment and coin tossing are useful primitives for building up more sophisticated protocols such as zero-knowledge proofs, our results cast very serious doubt on the security of quantum cryptography in the so-called "post-cold-war" applications.



So God had no choice:

He invented Quantum Mechanics !

Can Quantum Cryptography Imply Quantum Mechanics?

John A. Smolin
IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 smolin@watson.ibm.com

(Dated: October 10, 2003)

It has been suggested that the ability of quantum mechanics to allow secure distribution of secret key together with its inability to allow bit commitment or communicate superluminally might be sufficient to imply the rest of quantum mechanics. I argue using a toy theory as a counterexample that this is not the case. I further discuss whether an additional axiom (key storage) brings back the quantum nature of the theory.

One of the great desires of those who study both quantum information theory and quantum foundations has been to find simple information-theoretic axioms sufficient to imply all the rest of quantum mechanics [1]. To this end it has been suggested (private communication from Fuchs and Brassard to Bub, reported in [2] and *cf.* [3, 4]) that the existence of unconditionally secure cryptographic key distribution (of the sort granted by quantum mechanics [5, 6]), together with the impossibility of secure bit commitment (also a feature of quantum mechanics [7, 8]) might comprise just such a sufficient set. This is appealing as these two cryptographic primitives capture two of the key properties of quantum mechanics: Quantum key distribution is built on the idea that information gathering causes a necessary disturbance to quantum systems, while the bit commitment no-go theorem depends on an entanglement-based attack. More recently, this question has been rephrased slightly, and an axiom added by Clifton, Bub and Halvorson (CBH) [9]. Their axioms are:

- No broadcasting of arbitrary information [10]—In quantum mechanics, noncommuting density matrices cannot be cloned or even distributed in such a way that all marginal density matrices are correct.
- No unconditionally secure bit commitment.
- No superluminal communication transfer, *i.e.* a measurement on one system does not affect other systems.

In this paper I argue that these axioms are not sufficient to imply quantum mechanics. To make the argument, I propose an alternate toy theory of physics which satisfies these axioms but which quite obviously will not imply quantum mechanics. This result is in direct contradiction to Clifton, Bub, and Halvorson's, whose result seems to depend on the additional assumption that a physical theory must be a C^* algebra. It is unclear at this time just how much that additional assumption brings into the discussion.

LOCKBOX MODELS

I will consider a class of toy models whose basic unit of matter is the *lockbox*. A lockbox in general is an object akin to a physical box that can contain bit strings and cannot be opened except when the correct conditions exist to open the box. Depending on the model the box might be opened with a combination, a physical key, or something else. A lockbox may also perform other functions on the data within it depending on various inputs. Such boxes need not be allowed by physics, but instead are the building block of toy theories.

For example, consider a lockbox with a combination lock, that can contain a bit value b. The value cannot be read out of the lockbox except if a particular string of bits C—the combination—is presented to it. The bit b and combination C are chosen by the lockbox's creator at the time of its creation. If the lockbox is presented with an incorrect combination, the bit value is destroyed.

It can be helpful to think of such a lockbox as a physical box, that one could made of brass or steel, but it must be stressed that this can only be an approximation. The bit value in the lockbox by definition cannot be read out *by any means* other than using the correct combination, whereas a brass or steel box can always be drilled or blown open with explosives if enough effort is expended.

A true lockbox cannot exist in classical mechanics. It is often said that one way in which quantum mechanics differs from classical mechanics is that it cannot be represented by a local hidden variable theory. This statement hides a common oversight about classical mechanics. Classical mechanics also is not correctly represented by a local hidden variable theory, but by a local *unhidden* variable theory—in principle every possible property of a classical system can be measured perfectly [11] whereas the contents of a lockbox are unconditionally protected. Our example lockbox also differs from both classical and quantum theory in that its behavior when the wrong combination is applied is *irreversible*—the bit value is destroyed and cannot be recovered [12]. Thus a lockbox explicitly mimics the quantum property that unknown nonorthogonal states cannot be cloned (copied) [13, 14] or even measured without disturbance [15]. A lockbox

Can Quantum Cryptography Imply Quantum Mechanics?

John A. Smolin
IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 smolin@watson.ibm.com

(Dated: October 10, 2003)

It has been suggested that the ability of quantum mechanics to allow secure distribution of secret key together with its inability to allow bit commitment or communicate superluminally might be sufficient to imply the rest of quantum mechanics. I argue using a toy theory as a counterexample that this is not the case. I further discuss whether an additional axiom (key storage) brings back the quantum nature of the theory.

Quantum Mechanics as Quantum Information

(and only a little more)

Christopher Fuchs, quant-ph/0205039

The task is not to make sense of the quantum axioms by heaping more structure, more definitions, more science-fiction imagery on top of them, but to throw them away wholesale and start afresh.

From what deep physical principles might we derive this exquisite mathematical structure?

Those principles should be crisp [and] compelling.

They should stir the soul.

Characterizing Quantum Theory in Terms of Information-Theoretic Constraints

(Rob Clifton, Jeff Bub & Hans Halvorson, 2003)

Why the Quantum?

(Jeff Bub, 2003)

" The project was first suggested to me by remarks by Gilles Brassard at the meeting 'Quantum Foundations in the Light of Quantum Information and Cryptography' held in Montreal, May 17–19, 2000. "

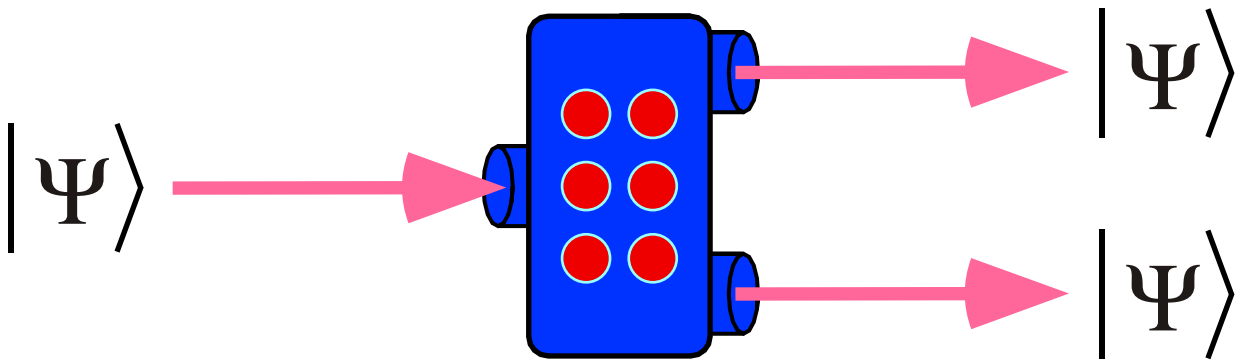
— Jeff Bub (Why the Quantum)

Email from Rob Clifton to Jeff Bub, 4 December 2001

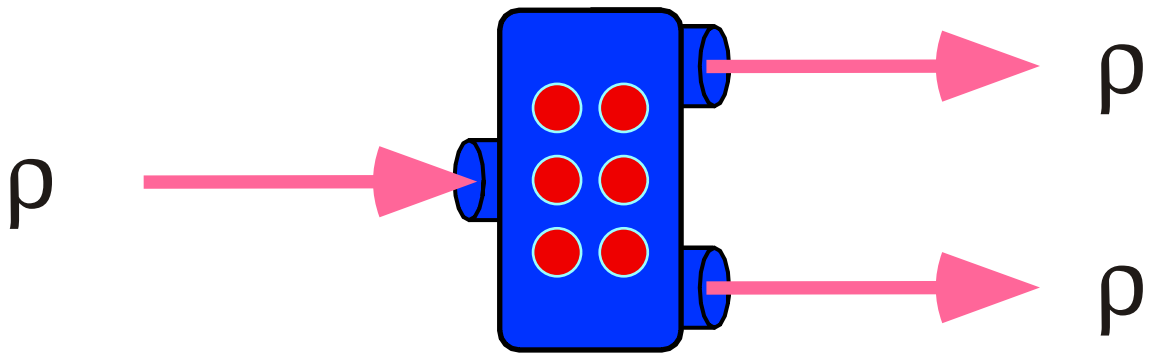
" It was good to talk to you over pizza today.
In fact, is was the most exciting 'truly quantum'
conversation I've had here with someone
since Hans [Halvorson] left in July. "

Quantum mechanics is fundamentally a theory about the possibilities and impossibilities of information transfer in our world, not a theory about the mechanics of nonclassical waves and particles.

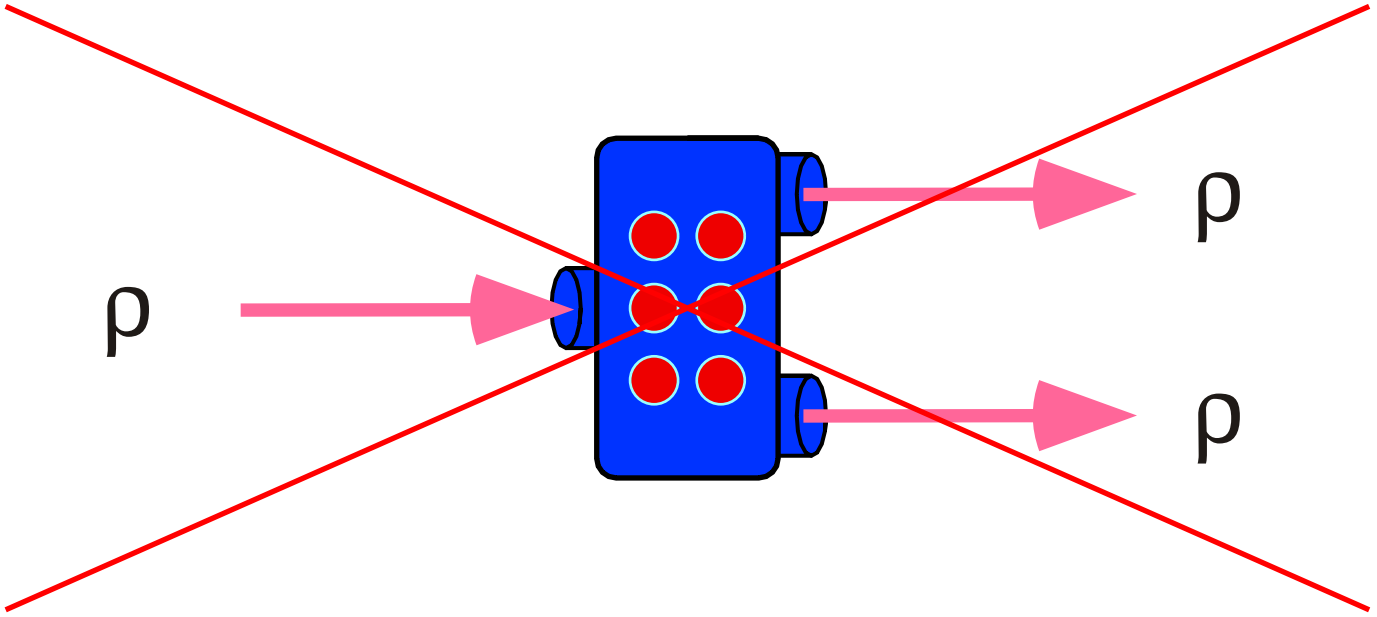
Cloning



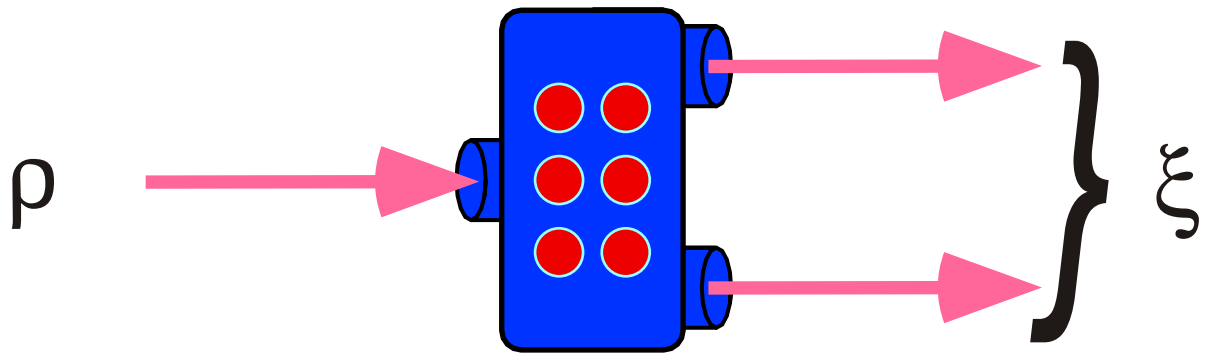
Cloning



Broadcasting



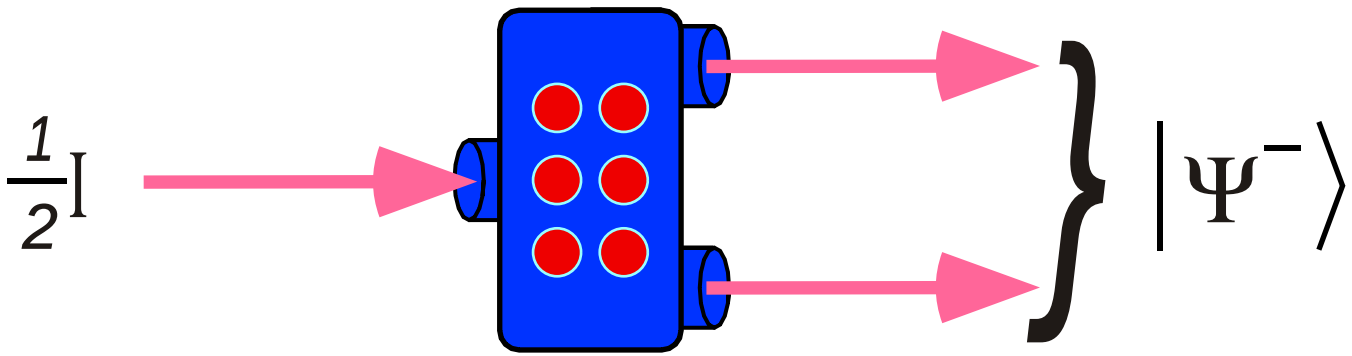
Broadcasting



$$\mathrm{Tr}_A(\xi) = \rho$$

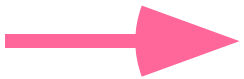
$$\mathrm{Tr}_B(\xi) = \rho$$

Broadcasting



Confidentiality
Possible

Perfect Commitment
Impossible



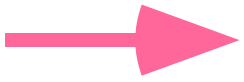
Quantum
Mechanics

Faster-than-light
Information Transfer
Impossible

Perfect Broadcasting
Impossible

Perfect Commitment
Impossible

~~*Confidentiality*~~
~~*Possible*~~



Quantum
Mechanics

G.B.: Why not "Confidentiality Possible" ?

J.B.: Because we wanted to use "Impossibility of" axioms.

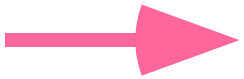
G.B.: But "Confidentiality Possible" means "Impossibility of Eavesdropping" !

J.B.: . . .

Faster-than-light
Information Transfer
Impossible

Perfect Broadcasting
Impossible

Perfect Commitment
Impossible



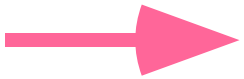
Quantum
Mechanics

Faster-than-light Information Transfer Impossible

Perfect Broadcasting Impossible

Perfect Commitment Impossible

Underlying Formalism is a C^*–algebra



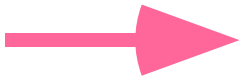
Quantum Mechanics

Faster-than-light Information Transfer Impossible

Perfect Broadcasting Impossible

Perfect Commitment Impossible

Underlying Formalism is a C^*–algebra



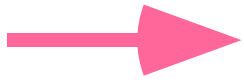
Basic Kinematic Features of Quantum Mechanics

Faster-than-light Information Transfer Impossible

Perfect Broadcasting Impossible

Perfect Commitment Impossible

Underlying Formalism is a C^*–algebra



Basic Kinematic Features of Quantum Mechanics:

Noncommutativity

Interference

Spacelike Separated Entanglement

Can Quantum Cryptography Imply Quantum Mechanics?

John A. Smolin
IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 smolin@watson.ibm.com

(Dated: October 10, 2003)

It has been suggested that the ability of quantum mechanics to allow secure distribution of secret key together with its inability to allow bit commitment or communicate superluminally might be sufficient to imply the rest of quantum mechanics. I argue using a toy theory as a counterexample that this is not the case. I further discuss whether an additional axiom (key storage) brings back the quantum nature of the theory.

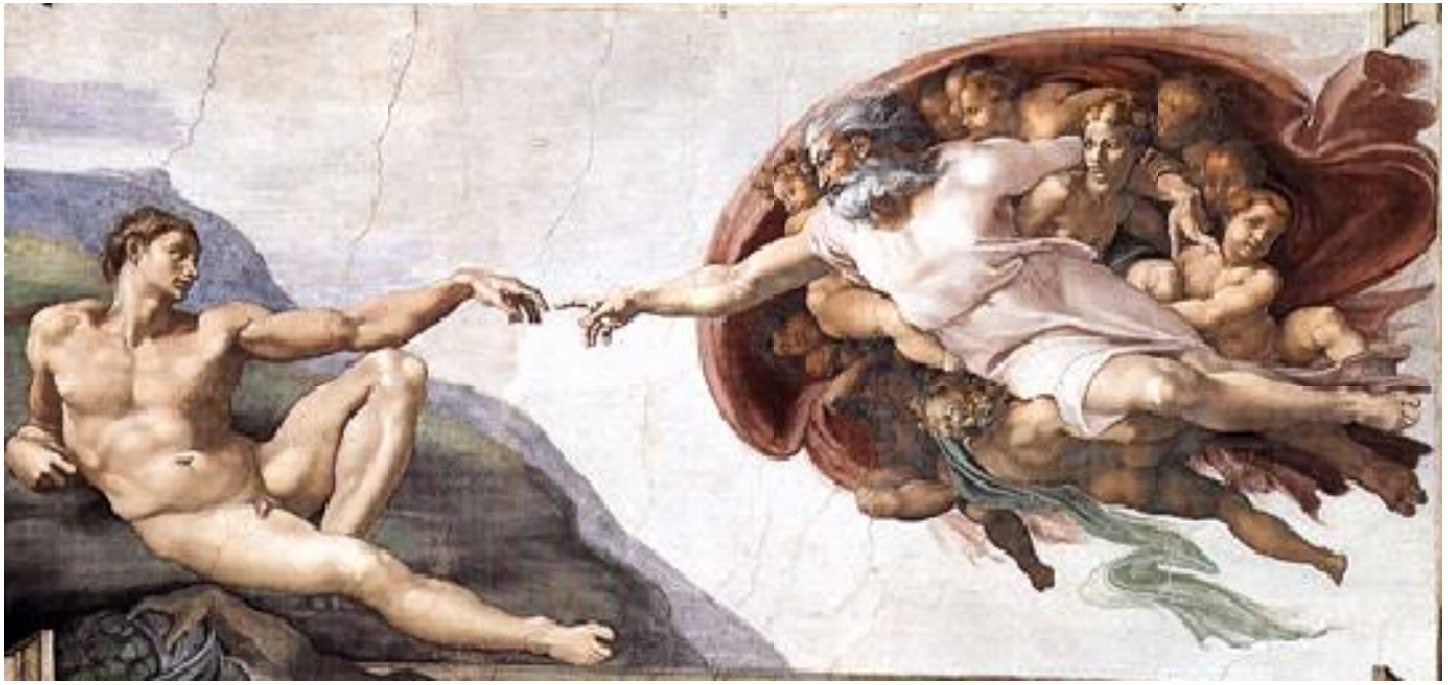
orem depends on an entanglement-based attack. More recently, this question has been rephrased slightly, and an axiom added by Clifton, Bub and Halvorson (CBH) [9]. Their axioms are:

- No broadcasting of arbitrary information [10]—In quantum mechanics, noncommuting density matrices cannot be cloned or even distributed in such a way that all marginal density matrices are correct.

- No unconditionally secure bit commitment.

- No superluminal communication transfer, *i.e.* a measurement on one system does not affect other systems.

In this paper I argue that these axioms are not sufficient to imply quantum mechanics. To make the argument, I



But did God really say:

Let the Universe be ruled

by a C*–algebra ?

Can Quantum Cryptography Imply Quantum Mechanics? Reply to Smolin

Hans Halvorson
Department of Philosophy, Princeton University, Princeton, NJ 08544 hhalvors@princeton.edu

Jeffrey Bub
Department of Philosophy, University of Maryland, College Park, MD 20742 jbub@carnap.umd.edu

(Dated: November 11, 2003)

Clifton, Bub, and Halvorson (CBH) have argued that quantum mechanics can be derived from three cryptographic, or broadly information-theoretic, axioms. But Smolin disagrees, and he has given a toy theory that he claims is a counterexample. Here we show that Smolin's toy theory violates an independence condition for spacelike separated systems that was assumed in the CBH argument. We then argue that any acceptable physical theory should satisfy this independence condition.

INTRODUCTION

In a recent note, Smolin [4] has presented a toy theory that simulates some interesting cryptographic features of quantum mechanics. Most interestingly, Smolin's toy theory satisfies the three cryptographic, or information-theoretic, axioms from which Clifton, Bub, and Halvorson (CBH) [1] have claimed to be able to derive quantum mechanics. So, Smolin argues that, *contra* CBH, QM cannot be derived from these three axioms.

We agree with Smolin that QM is not a *logical* consequence of the three information-theoretic axioms, taken in complete isolation from any theoretical context. In fact, we think that attempting such a derivation would be futile, as shown by the history of failed attempts (e.g., the quantum logic program) to derive QM from completely explicit, physically plausible axioms. When such attempts have not failed miserably, their partial successes have come at the expense of complicating the axioms to the point of destroying all physical insight.

The failure of attempts at theoretically-neutral derivations of QM does not undermine the importance of providing characterizations within some judiciously chosen framework of background assumptions — these assumptions might be explicit (as in CBH's assumption that theories permit a C^*-algebraic formulation), or they might be tacit (as, e.g., in Einstein's assumption that spacetime is continuous and not discrete). For someone concerned with diachronic relationships between theories, it is an extremely interesting question to ask whether there is a framework that encompasses both the old and the new theory, and whether there are salient physical postulates that distinguish the two theories. CBH have answered this question in the affirmative for classical and quantum mechanics: the C^*-algebraic framework encompasses both theories, and quantum mechanics is distinguished in terms of its satisfaction of the three information-theoretic axioms.

But to be more specific, we argue here that Smolin's toy theory is so remote from classical or quantum mechanics that it holds little physical interest. In particular, we show that Smolin's theory violates an independence condition for distinct systems that is taken for granted in both classical and quantum mechanics. We then argue that the failure of this independence condition leads to pathologies that are unacceptable in any physical theory.

AGAINST SERIAL NUMBERS

CBH argue that QM can be derived from three axioms: no superluminal information transfer via measurement, no cloning [7], and no bit commitment. Roughly speaking, the no cloning axiom says that there cannot be a machine that accepts arbitrary input states, and returns two copies of any state it receives. The no bit commitment axiom states that it is not possible for one observer, Alice, to send a bit value to a second observer, Bob, in such a way that Bob cannot access the bit value until Alice provides him with a key, and such that Alice cannot change her bit value after she has sent it to Bob. It is well-known that elementary QM satisfies these three cryptographic axioms. CBH claim that QM can also be derived from these three axioms, and so the conjunction of the axioms is equivalent to the claim that QM is true.

Smolin's toy theory consists of symmetric pairs of lockboxes, where each pair of lockboxes has a unique serial number. Furthermore, each lockbox contains a bit value, which is accessible to inspection only when the lockbox is in the presence of its partner. For the details of how the lockbox theory satisfies the three axioms, we refer the reader to Smolin's paper. But note that the assumption of unique serial numbers is needed to ensure that cloning is impossible.

Most of the details of Smolin's lockbox theory are irrelevant to his argument against the CBH characterization

Can Quantum Cryptography Imply Quantum Mechanics? Reply to Smolin

Hans Halvorson
Department of Philosophy, Princeton University, Princeton, NJ 08544 hhalvors@princeton.edu

Jeffrey Bub
Department of Philosophy, University of Maryland, College Park, MD 20742 jbub@carnap.umd.edu

(Dated: November 11, 2003)

Clifton, Bub, and Halvorson (CBH) have argued that quantum mechanics can be derived from three cryptographic, or broadly information-theoretic, axioms. But Smolin disagrees, and he has given a toy theory that he claims is a counterexample. Here we show that Smolin's toy theory violates an independence condition for spacelike separated systems that was assumed in the CBH argument. We then argue that any acceptable physical theory should satisfy this independence condition.

In defense of the epistemic view of quantum states: a toy theory

R. W. Spekkens
Perimeter Institute for Theoretical Physics,
35 King St. North, Waterloo, Canada N2J 2W9
(Dated: January 9, 2004)

We present a toy theory that is based on a simple principle: the number of questions about the physical state of a system that are answered must always be equal to the number that are unanswered in a state of maximal knowledge. A wide variety of quantum phenomena are found to have analogues within this toy theory. Such phenomena include: the noncommutativity of measurements, interference, the multiplicity of convex decompositions of a mixed state, the impossibility of discriminating nonorthogonal states, the impossibility of a universal state inverter, the distinction between bi-partite and tri-partite entanglement, the monogamy of pure entanglement, no cloning, no broadcasting, remote steering, teleportation, dense coding, mutually unbiased bases, unextendible product bases, and many others. The diversity and quality of these analogies is taken as evidence for the view that quantum states are states of incomplete knowledge rather than states of reality. A consideration of the phenomena that the toy theory fails to reproduce, notably, violations of Bell inequalities and the existence of a Kochen-Specker theorem, provides clues for how to proceed with a research program wherein the quantum state being a state of incomplete knowledge is the idea upon which one never compromises.

PACS numbers: 03.65.Ta,03.67.-a

Contents

I. INTRODUCTION

In this article, we introduce a simple toy theory based on a principle that restricts the amount of knowledge an observer can acquire about reality. This theory, although not *equivalent* to quantum theory nor even competitive as an explanation of empirical phenomena, bears an uncanny resemblance to the latter insofar as it reproduces in detail a large number of phenomena that are typically taken to be characteristically quantum. This, and the fact that the object analogous to the quantum state in the toy theory is a state of incomplete knowledge, are the grounds upon which we argue for our thesis, that quantum states are also states of incomplete knowledge.

We begin by clarifying the dichotomy between states of reality and states of knowledge. To be able to refer to this distinction conveniently, we introduce the qualifiers

In defense of the epistemic view of quantum states: a toy theory

R. W. Spekkens
Perimeter Institute for Theoretical Physics,
35 King St. North, Waterloo, Canada N2J 2W9
(Dated: January 9, 2004)

We present a toy theory that is based on a simple principle: the number of questions about the physical state of a system that are answered must always be equal to the number that are unanswered in a state of maximal knowledge. A wide variety of quantum phenomena are found to have analogues within this toy theory. Such phenomena include: the noncommutativity of measurements, interference, the multiplicity of convex decompositions of a mixed state, the impossibility of discriminating nonorthogonal states, the impossibility of a universal state inverter, the distinction between bi-partite and tri-partite entanglement, the monogamy of pure entanglement, no cloning, no broadcasting, remote steering, teleportation, dense coding, mutually unbiased bases, unextendible product bases, and many others. The diversity and quality of these analogies is taken as evidence for the view that quantum states are states of incomplete knowledge rather than states of reality. A consideration of the phenomena that the toy theory fails to reproduce, notably, violations of Bell inequalities and the existence of a Kochen-Specker theorem, provides clues for how to proceed with a research program wherein the quantum state being a state of incomplete knowledge is the idea upon which one never compromises.

PACS numbers: 03.65.Ta,03.67.-a

A note on information theoretic characterizations of physical theories

Hans Halvorson*
Department of Philosophy, Princeton University

Abstract

Clifton, Bub, and Halvorson [*Foundations of Physics* 33, 1561–1591, (2003)] have recently argued that quantum theory is characterized by its satisfaction of three information-theoretic axioms. However, it is not difficult to construct apparent counterexamples to the CBH characterization theorem. In this paper, we discuss the limits of the characterization theorem, and we provide some technical tools for checking whether a theory (specified in terms of the convex structure of its state space) falls within these limits.

1 Introduction

Some would like to argue that quantum information theory has revolutionary implications for the philosophical foundations of QM (see, e.g., Bub, 2004; Fuchs, 2003). Whether or not this claim is true, there is no doubt that quantum information theory presents us with new perspectives from which we can approach traditional questions about the interpretation of QM. One such question asks whether there are natural physical postulates that capture the essence of QM — postulates that tell us what sets QM apart from other physical theories, and in particular from its predecessor theories. The advent of quantum information theory suggests that we look for *information-theoretic* postulates that characterize (i.e., are equivalent to) QM.

A positive answer to this question has been supplied by Clifton, Bub, and Halvorson (2003). Clifton, Bub and Halvorson (CBH) show that, within the C^*-algebraic framework for physical theories, quantum theories are singled out by their satisfaction of three information-theoretic axioms: 1. no

*hhalvors@princeton.edu. This is version 2.

A note on information theoretic characterizations of physical theories

Hans Halvorson*
Department of Philosophy, Princeton University

Abstract

Clifton, Bub, and Halvorson [*Foundations of Physics* 33, 1561–1591, (2003)] have recently argued that quantum theory is characterized by its satisfaction of three information-theoretic axioms. However, it is not difficult to construct apparent counterexamples to the CBH characterization theorem. In this paper, we discuss the limits of the characterization theorem, and we provide some technical tools for checking whether a theory (specified in terms of the convex structure of its state space) falls within these limits.

Quantum Theory From Five Reasonable Axioms

Lucien Hardy*
Centre for Quantum Computation,
The Clarendon Laboratory,
Parks road, Oxford OX1 3PU, UK

May 27, 2003

Abstract

The usual formulation of quantum theory is based on rather obscure axioms (employing complex Hilbert spaces, Hermitean operators, and the trace formula for calculating probabilities). In this paper it is shown that quantum theory can be derived from five very reasonable axioms. The first four of these axioms are obviously consistent with both quantum theory and classical probability theory. Axiom 5 (which requires that there exist continuous reversible transformations between pure states) rules out classical probability theory. If Axiom 5 (or even just the word "continuous" from Axiom 5) is dropped then we obtain classical probability theory instead. This work provides some insight into the reasons why quantum theory is the way it is. For example, it explains the need for complex numbers and where the trace formula comes from. We also gain insight into the relationship between quantum theory and classical probability theory.

1 Introduction

Quantum theory, in its usual formulation, is very abstract. The basic elements are vectors in a complex Hilbert space. These determine measured probabilities by means of the well known trace formula - a formula which has no obvious origin. It is natural to ask why quantum theory is the way it is. Quantum theory is simply a new type of probability theory. Like classical probability theory it can be applied to a wide range of phenomena. However, the rules of classical probability theory can be determined by pure thought alone without any particular appeal to experiment (though, of course, to develop classical probability theory, we do employ some basic intuitions about the nature of the world). Is the same true of quantum theory? Put another way, could a 19th century theorist have developed quantum theory without access to the empirical data that later became available to his 20th century descendants? In this paper it will be shown that quantum theory follows from five very reasonable axioms which might well have been posited without any particular access to empirical data. We will not recover any specific form of the Hamiltonian from the axioms since that belongs to particular applications of quantum theory (for example - a set of interacting spins or the motion of a particle in one dimension). Rather we will recover the basic structure of quantum theory along with the most general type of quantum evolution possible. In addition we will only deal with the case where there are a finite or countably infinite number of distinguishable states corresponding to a finite or countably infinite dimensional Hilbert space. We will not deal with continuous dimensional Hilbert spaces.

The basic setting we will consider is one in which we have preparation devices, transformation devices, and measurement devices. Associated with each preparation will be a state defined in the following

*hardy@qubit.org. This is version 4

Quantum Theory From Five Reasonable Axioms

Lucien Hardy*
Centre for Quantum Computation,
The Clarendon Laboratory,
Parks road, Oxford OX1 3PU, UK

May 27, 2003

Axiom 1 *Probabilities.* Relative frequencies (measured by taking the proportion of times a particular outcome is observed) tend to the same value (which we call the probability) for any case where a given measurement is performed on a ensemble of n systems prepared by some given preparation in the limit as n becomes infinite.

Axiom 2 *Simplicity.* K is determined by a function of N (i.e. $K = K(N)$) where $N = 1, 2, \ldots$ and where, for each given N, K takes the minimum value consistent with the axioms.

Axiom 3 *Subspaces.* A system whose state is constrained to belong to an M dimensional subspace (i.e. have support on only M of a set of N possible distinguishable states) behaves like a system of dimension M.

Axiom 4 *Composite systems.* A composite system consisting of subsystems A and B satisfies $N = N_A N_B$ and $K = K_A K_B$

Axiom 5 *Continuity.* There exists a continuous reversible transformation on a system between any two pure states of that system.

- The *number of degrees of freedom*, K, is defined as the minimum number of probability measurements needed to determine the state, or, more roughly, as the number of real parameters required to specify the state.

- The *dimension*, N, is defined as the maximum number of states that can be reliably distinguished from one another in a single shot measurement.

Quantum theory from four of Hardy's axioms

Rüdiger Schack
Department of Mathematics, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
E-mail: r.schack@rhul.ac.uk

In a recent paper [e-print quant-ph/0101012], Hardy has given a derivation of "quantum theory from five reasonable axioms." Here we show that Hardy's first axiom, which identifies probability with limiting frequency in an ensemble, is not necessary for his derivation. By reformulating Hardy's assumptions, and modifying a part of his proof, in terms of Bayesian probabilities, we show that his work can be easily reconciled with a Bayesian interpretation of quantum probability.

I. INTRODUCTION

In Bayesian probability theory [1, 2], probabilities are not objective states of nature, but rather are taken to be degrees of belief that determine an agent's decisions in the face of uncertainty. It can be shown that degrees of belief must obey the usual rules of the probability calculus if the agent's decisions are rational (for references and a summary of the argument, see [3]). In a Bayesian framework, probabilities and measured frequencies are strictly separate concepts. This leads to conceptual clarity in statements that involve both probabilities and frequencies. Furthermore, adopting the Bayesian viewpoint has important practical consequences in the field of statistics [2, 4].

If the Bayesian interpretation is applied to quantum mechanical probabilities, one is led naturally to the viewpoint that quantum states represent states of belief. This viewpoint is attractive for many reasons. For instance, it eliminates the difficulties associated with regarding quantum state collapse as a real physical process. Within the Bayesian framework, one can account effortlessly for the tight connection between measured frequencies and the probabilities obtained from the quantum probability rule [5]. The Bayesian approach has led to new mathematical results [3, 6], a better understanding of prior information in quantum tomography [7], and an optimized entanglement purification protocol [8].

Hardy [9] (see also [10]) has recently given a derivation of the mathematical structure of quantum theory from five simple axioms. In his first axiom, Hardy identifies probability with measured frequency in the limit of an infinite number of repetitions of a given experiment. In Hardy's formulation, a quantum state is a property of a preparation device. This is a problematical notion. Attempts to base probability theory on a definition of probability as frequency in infinite ensembles [11] have largely failed (see, e.g., [12, 13]). For instance, without further complicating assumptions, a relative frequency specified for an infinite ensemble does not in any way restrict the corresponding frequency for a finite subensemble. Furthermore, attaching the notion of a quantum state to a preparation device appears to limit quantum theory to the description of laboratory experiments. But surely one would

Quantum theory from four of Hardy's axioms

Rüdiger Schack
Department of Mathematics, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
E-mail: r.schack@rhul.ac.uk

In a recent paper [e-print quant-ph/0101012], Hardy has given a derivation of "quantum theory from five reasonable axioms." Here we show that Hardy's first axiom, which identifies probability with limiting frequency in an ensemble, is not necessary for his derivation. By reformulating Hardy's assumptions, and modifying a part of his proof, in terms of Bayesian probabilities, we show that his work can be easily reconciled with a Bayesian interpretation of quantum probability.

I have a dream

I've had dreams before

Will this one be granted too ?

JOURNAL OF MODERN OPTICS, 1994, VOL. 41, NO. 12, 2521–2535

Oracle quantum computing†

ANDRÉ BERTHIAUME‡ and GILLES BRASSARD§
Département IRO, Université de Montréal, C.P. 6128,
succursale centre-ville, Montréal, Québec, Canada H3C 3J7

(*Received 22 November 1993; revision received 6 April 1994
and accepted 13 April 1994*)

Abstract. Building on the work of Deutsch and Jozsa, we construct oracles relative to which (1) there is a decision problem that can be solved with certainty in worst-case polynomial time on the quantum computer, yet it cannot be solved classically in *probabilistic* expected polynomial time if errors are not tolerated, nor even in *nondeterministic* polynomial time, and (2) there is a decision problem that can be solved in exponential time on the quantum computer, which requires *double* exponential time on *all but finitely many* instances on any classical deterministic computer.

1. Introduction

In his 1982 keynote address to the first workshop on the physics of computation, Richard Feynman asked the question of whether or not physics can be simulated with computers [15]. Although he considered the idea of using a quantum computer for this purpose, he called it 'a side remark', whereas he considered the question of simulating quantum processes with a classical computer to be 'the interesting' question. He expressed the belief that it is not possible to simulate physics *in real time* with a classical computer, whereas it may be possible with a quantum computer. If true, this would imply that there are tasks the quantum computer can handle significantly faster than any classical computer ever could. Feynman discussed quantum computers in more detail in a plenary talk he presented at the 1984 CLEO/IQEC Meeting [16]. Soon thereafter, David Deutsch formalized the concept of the quantum computer and the question of whether it might be more powerful than classical computers from a computational complexity point of view [11, 12].

What makes the quantum computer different from a classical computer is the possibility it offers for massive parallelism within a single piece of hardware. Let f be a computable function. If you have to compute it on two different inputs x and y, you may have to compute $f(x)$ and then start afresh to compute $f(y)$, thus requiring about twice as long as if you had needed only one of these values. The quantum computer allows you to prepare an input that encodes both x and y in *quantum superposition*. If you run your program that computes f on that input, and if your

† The results given in this paper have been presented at the *7th Annual IEEE Symposium on Structure in Complexity Theory*, Boston, June 1992, and at the *Workshop on Physics and Computation, PhysComp '92*, Dallas, October 1992; they have appeared in preliminary form in those Proceedings [7, 8].

‡ Supported in part by an NSERC postgraduate fellowship.

§ Supported in part by Canada's NSERC E. W. R. Steacie Memorial Fellowship and Québec's FCAR.

JOURNAL OF MODERN OPTICS, 1994, VOL. 41, NO. 12, 2521–2535

Oracle quantum computing†

ANDRÉ BERTHIAUME‡ and GILLES BRASSARD§
Département IRO, Université de Montréal, C.P. 6128,
succursale centre-ville, Montréal, Québec, Canada H3C 3J7

(*Received 22 November 1993; revision received 6 April 1994
and accepted 13 April 1994*)

Abstract. Building on the work of Deutsch and Jozsa, we construct oracles relative to which (1) there is a decision problem that can be solved with certainty in worst-case polynomial time on the quantum computer, yet it cannot be solved classically in *probabilistic* expected polynomial time if errors are not tolerated, nor even in *nondeterministic* polynomial time, and (2) there is a decision problem that can be solved in exponential time on the quantum computer, which requires *double* exponential time on *all but finitely many* instances on any classical deterministic computer.

preferably, that **BPP** $\subset$ **BQP**, under a classical computational complexity assumption more natural than **P** $\subset$ **C**$_{=}$**P**[half]. For instance, can the desired conclusion be established under the sole assumption that **P** $\neq$ **NP** or, failing this, that one-way functions exist? (A one-way function is easy to compute but computationally infeasible to invert.) The other promising direction for investigation is to find a *really* useful problem that the quantum computer can solve efficiently, for which no efficient classical algorithms are known. This would be interesting even lacking a proof that the problem in question is genuinely hard for classical computers.

Although building a quantum computer is beyond current technology (but see [23] for a proposal), this should not discourage research into quantum computing. Indeed, quantum physics has been used successfully for purposes closely related to computation in a prototype that demonstrates the technological feasibility of quantum cryptography [4, 5]. Ten years ago, quantum cryptography was still pure science-fiction. A good way of pumping funding into the building of an actual quantum computer would be to find an efficient quantum factoring algorithm!

It is our hope that quantum computers will come into existence during our lifetime and that they will be harnessed to computational tasks beyond the reach of even the fastest possible classical computers. But should it turn out that there is nothing 'useful' the quantum computer can do faster than a classical computer, or should building it remain forever beyond the reach of technology, the words of Feynman would echo in our minds: 'Such nonsense is very entertaining to professors like me. I hope you will find it interesting and entertaining also' [16].

Note added in proof.—Our conclusion that 'A good way of pumping funding into the building of an actual quantum computer would be to find an efficient quantum factoring algorithm!' was prophetic. Peter Shor discovered such an algorithm within hours of our writing this sentence and sending the final version of our paper to the Editors. Shor's striking result will be presented on 20 November 1994 at the *36th Annual IEEE Symposium on the Foundations of Computer Science*, Santa Fe, New Mexico, and it will appear in the Proceedings, published by the IEEE Computer Society Press. It remains to see what effect this result will have on funding.

Acknowledgements

This work has benefited from discussions with Charles H. Bennett, Ethan Bernstein, Claude Crépeau, David Deutsch, Artur Ekert, Lane Hemaspaandra, Richard Jozsa, Dan Simon, Seinosuke Toda and Umesh Vazirani. The idea of considering oracle worlds was sparked by the need to give a talk at the first New Mexico Theory Day, organized by Tim Long. The seed for Corollary 3 was planted by a question asked by Lane Hemaspaandra during that talk, and he also deserves our thanks for suggesting that we investigate the relevance of the class **C**$_{=}$**P**. We are grateful to Charles H. Bennett for pointing out to us that our original relativized separation between **EQP** and **ZQP** (Theorem 7) actually provided a separation between **EQP** and **NP**. The observation that an exponential number of processors working in parallel for exponential time would not suffice to simulate the quantum computer's calculation of V_Z is due to Lev Levitin.

We are also grateful to the Rank Foundation (England), the ISI & Elsag-Baley (Italy), and the IESS (Germany) for making possible the 1993 workshops on quantum information theory, quantum computing and quantum cryptography,

Although building a quantum computer is beyond current technology (but see [23] for a proposal), this should not discourage research into quantum computing. Indeed, quantum physics has been used successfully for purposes closely related to computation in a prototype that demonstrates the technological feasibility of quantum cryptography [4, 5]. Ten years ago, quantum cryptography was still pure science-fiction. A good way of pumping funding into the building of an actual quantum computer would be to find an efficient quantum factoring algorithm!

It is our hope that quantum computers will come into existence during our lifetime and that they will be harnessed to computational tasks beyond the reach of even the fastest possible classical computers. But should it turn out that there is nothing 'useful' the quantum computer can do faster than a classical computer, or should building it remain forever beyond the reach of technology, the words of Feynman would echo in our minds: 'Such nonsense is very entertaining to professors like me. I hope you will find it interesting and entertaining also' [16].

Workshop on Quantum Foundations in the Light of Quantum Information

Centre de Recherches Mathématiques
Université de Montréal

16–19 May 2000

Charles Bennett

Herbert Bernstein

Gilles Brassard

Jeffrey Bub

Christophe Fuchs

(Lucien Hardy)

Patrick Hayden

Richard Jozsa

David Mermin

Ruediger Schack

Benjamin Schumacher

William Wootters

Shannon meets Bohr: Quantum Foundations in the Light of Quantum Information

Växjö University, Sweden

17–21 June 2001

Herbert Bernstein
Doug Bilodeau
Jeffrey Bub
Carlton Caves
Henry Folse
Christopher Fuchs
Daniel Greenberger
Lucien Hardy
Peter Harremoes
Richard Jozsa
David Mermin
Asher Peres
Itamar Pitowsky
Arkady Plotnitsky
Joseph Renes
Ruediger Schack
Ben Schumacher
John Smolin
Daniel Terno

Workshop on Quantum Foundations
in the Light of Quantum Information II

Centre de Recherches Mathématiques
Université de Montréal

13 October — 3 November 2002

Who \ Date	S 1 3	1 4	1 5	1 6	1 7	1 8	S 1 9	S 2 0	2 1	2 2	2 3	2 4	2 5	S 2 6	S 2 7	2 8	2 9	3 0	3 1	S 0 1	S 0 2	0 3
1) Marcus Appleby	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X
2) Howard Barnum	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	X	X
3) Charles Bennett	-	-	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4) Gilles Brassard	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
5) Hans Briegel	X	X	X	X	X	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6) Jeffrey Bub	-	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	-	-	-
7) Adan Cabello	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8) Carlton Caves	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
9) Claude Crépeau	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	X	X
10) José Fernandez	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
11) R. Floreanini	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	-	
12) Chris Fuchs	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
13) Ernesto Galvao	-	-	-	-	-	-	-	-	X	X	X	X	X	X	-	-	-	-	-	-	-	-
14) Nicolas Gisin	X	X	X	X	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15) Lucien Hardy	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
16) Patrick Hayden	X	X	X	X	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
17) F. Markopoulou	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	X	X	-	-	-	
18) Dominic Mayers	-	X	X	X	X	X	X	X	X	X	X	X	X	X	-	-	-	-	-	-	-	-
19) David Mermin	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	
20) David Poulin	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
21) Ruediger Schack	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	-	-	
22) Ben Schumacher	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
23) John Smolin	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	X	X	X	X	X	X	
24) Robert Spekkens	-	X	X	X	X	X	X	X	X	X	X	X	X	-	-	-	-	-	-	-	-	-
25) Chris Timpson	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	X	X	X	X	X	
26) Stefan Wolf	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
27) William Wootters	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Quantum Logic

Meets

Quantum Information

Växjö University, Sweden

1–6 June 2003

Scott Aaronson

Guido Bacciagaluppi

Howard Barnum

Stephen Bartlett

Paul Busch

Bob Coecke

Christopher Fuchs

Alexei Grinbaum

Hans Halvorson

Lucien Hardy

Piero Mana

Marcos Perez-Suarez

Ruediger Schack

John Smolin

Robert Spekkens

Alexander Wilce

Rolf Landauer has once claimed that

" information is physical "

The main thesis of this talk is that

" physics is informational "