Title: Is Information the Key?

Date: May 09, 2011 09:30 AM

URL: http://pirsa.org/11050035

Abstract: Consider the two great physical theories of the twentieth century: relativity and quantum mechanics. Einstein derived relativity from very simple principles. By contrast, the foundation of quantum mechanics is built on a set of rather strange, disjointed and ad hoc axioms, reflecting at best the history that led to discovering this new world order. The purpose of this talk is to argue that a better foundation for quantum mechanics lies within the teachings of quantum information science. The basic postulate is that the truly fundamental laws of Nature concern information, not waves or particles. For example, it is known that quantum key distribution is possible but quantum bit commitment is not and that nature is nonlocal but not as nonlocal as is imposed by causality. But should these statements be considered as theorems or axioms? It's time to pause and reflect on what is really fundamental and what are merely consequences. Could information be the key?

Is information the key?

GILLES BRASSARD

Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

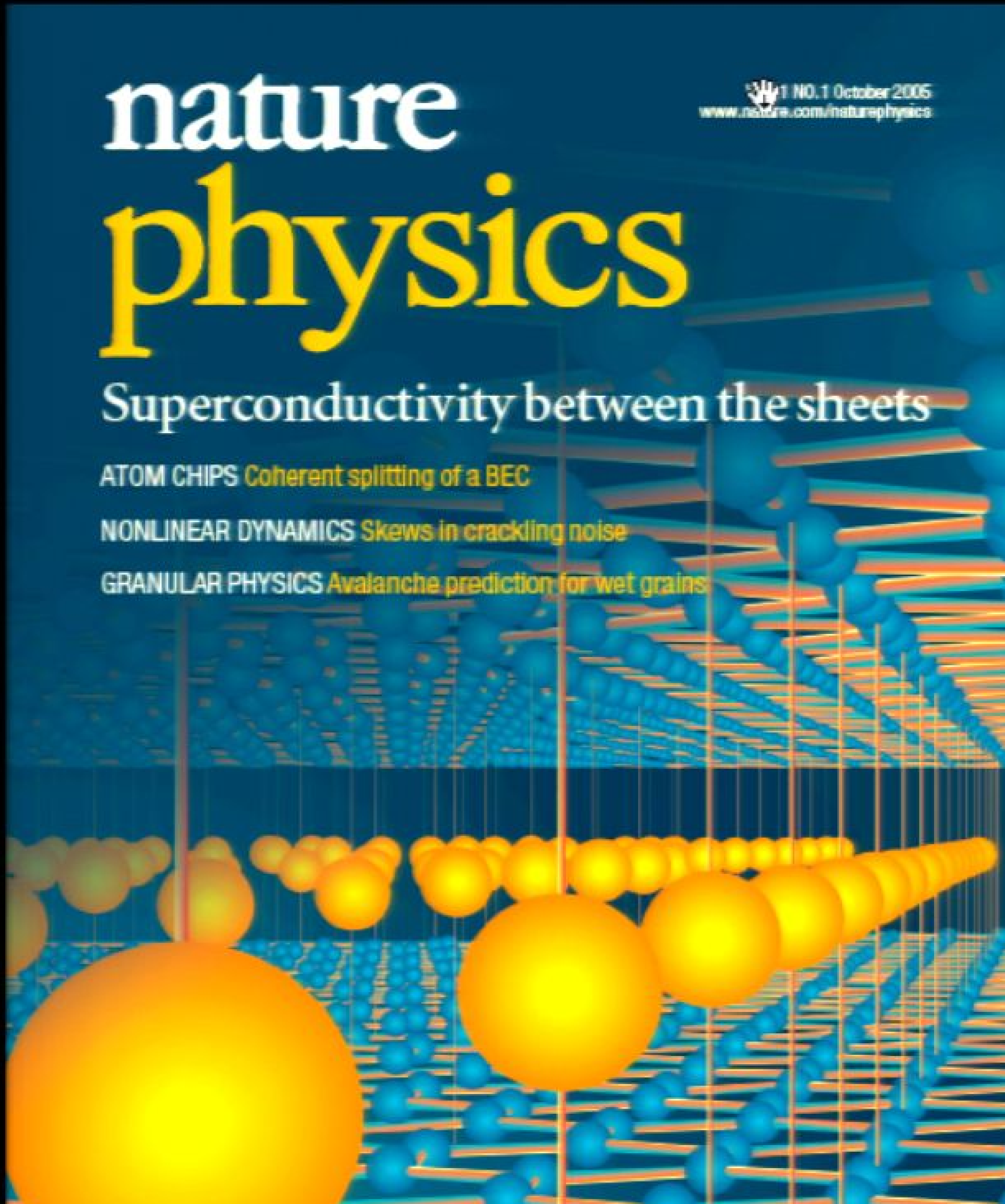
e-mail: brassard@iro.umontreal.ca

Is information the key?

GILLES BRASSARD

Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca


nature
physics
1 NO.1 October 2005
Superconductivity between the sheets
ATOM CHIPS Coherent splitting of a BEC
NONLINEAR DYNAMICS Skews in crackling noise
GRANULAR PHYSICS Avalanche prediction for wet grains

COMMENTARY

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?

COMMENTARY

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?

COMMENTARY

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?

COMMENTARY

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?

JOURNAL OF MODERN OPTICS, 2003, VOL. 50, NO. 6–7, 987–1023

Quantum mechanics as quantum information, mostly†

CHRISTOPHER A. FUCHS

Bell Labs, Lucent Technologies, 600–700 Mountain Avenue, Room 1D-236, Murray Hill, NJ 07974, USA

(*Received 9 September 2002; revision received 17 December 2002*)

Abstract. In this paper, I try to cause some good-natured trouble. The issue is, 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-honoured 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.

JOURNAL OF MODERN OPTICS, 2003, VOL. 50, NO. 6–7, 987–1023

Taylor & Francis
Taylor & Francis Group

Quantum mechanics as quantum information, mostly†

CHRISTOPHER A. FUCHS

Bell Labs, Lucent Technologies, 600–700 Mountain Avenue, Room 1D-236, Murray Hill, NJ 07974, USA

(*Received 9 September 2002; revision received 17 December 2002*)

Abstract. In this paper, I try to cause some good-natured trouble. The issue is, 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-honoured 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.

Quantum Mechanics as Quantum Information

(and only a little more)

Christopher Fuchs, quant-ph/0205039

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,

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.

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?

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?

INFORMATIONAL

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.

John Archibald Wheeler

John Archibald Wheeler

"Successful, yes, but mysterious, too. Balancing the glory of quantum achievements, we have the shame of not knowing "how come." Why does the quantum exist?"

(The New York Times, 12 Dec 2000)

John Archibald Wheeler

By the late 1970s and onward, [...] to the best students wh
came asking for a research project, Wheeler would say,

"Derive quantum theory from
an information theoretic principle".

Quantum Mechanics is About Quantum Information

Jeffrey Bub
Department of Philosophy, University of Maryland,
College Park, MD 20742
(E-mail: jbub@carnap.umd.edu)

May 30, 2006

Abstract

I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive—just as, following Einstein's special theory of relativity, a field is no longer regarded as the physical manifestation of vibrations in a mechanical medium, but recognized as a new physical primitive in its own right.

1 Introduction

In several places [9, 10, 11], Cushing speculates about the possibility of an alternative history, in which Bohm's theory [4, 16] is developed as the standard version of quantum mechanics, and suggests that in that case the Copenhagen interpretation, if it had been proposed as an alternative to a fully developed Bohmian theory, would have been summarily rejected. I quote from [10, pp. 352–353]:

> ...we can fashion a highly reconstructed but entirely plausible bit of partially 'counterfactual' history as follows (all around 1925–1927). Heisenberg's matrix mechanics and Schrödinger's wave mechanics are formulated and shown to be mathematically equivalent. Study of a classical particle subject to Brownian motion ...leads to a classical understanding of the already discovered Schrödinger equation. A stochastic mechanics underpins this interpretation with a visualizable model of microphenomena and, so, a realistic ontology remains viable. Since stochastic mechanics is quite difficult to handle mathematically, study naturally turns to the mathematically equivalent linear Schrödinger equation. Hence, the Dirac transformation theory and an operator formalism are available as a convenience for further development of the mathematics to provide algorithms for calculation.
>
> ...

Quantum Mechanics is About Quantum Information

Jeffrey Bub
Department of Philosophy, University of Maryland,
College Park, MD 20742
(E-mail: jbub@carnap.umd.edu)

May 30, 2006

Abstract

I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive—just as, following Einstein's special theory of relativity, a field is no longer regarded as the physical manifestation of vibrations in a mechanical medium, but recognized as a new physical primitive in its own right.

Abstract

I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive—just as, following Einstein's special theory of relativity, a field is no longer regarded as the physical manifestation of vibrations in a mechanical medium, but recognized as a new physical primitive in its own right.

Abstract

I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive—just as, following Einstein's special theory of relativity, a field is no longer regarded as the physical manifestation of vibrations in a mechanical medium, but recognized as a new physical primitive in its own right.

Abstract

I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive—just as, following Einstein's special theory of relativity, a field is no longer regarded as the physical manifestation of vibrations in a mechanical medium, but recognized as a new physical primitive in its own right.

We all of us have some idea of what the basic axioms in physics will turn out to be.

— Einstein, 1948

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

The Axioms of Relativity

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

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

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 [4] transformation on its Hilbert space.

-- more --

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

$$<\phi|\psi> = \Sigma\, \phi_i^* \psi_i$$

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.

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

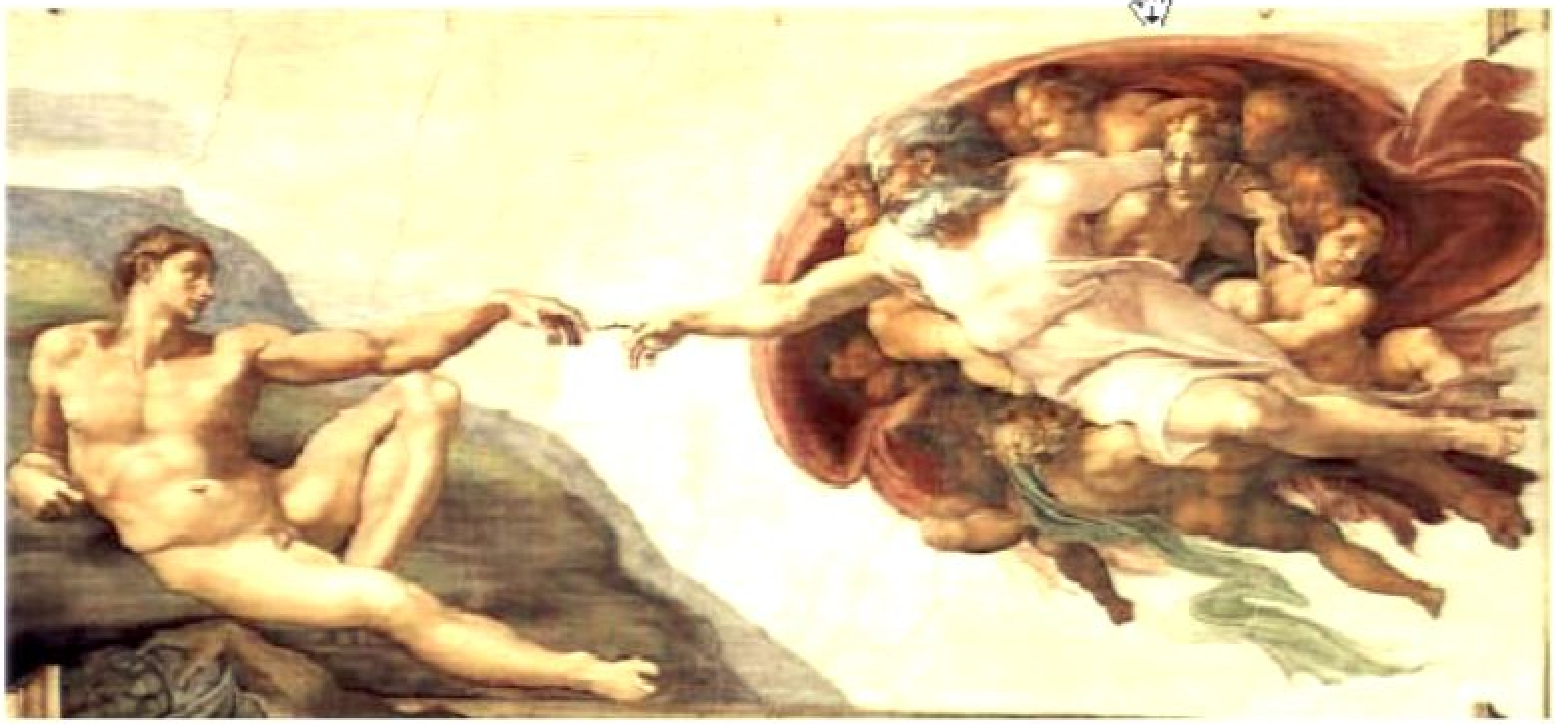
$$\frac{\mathbf{P}_j|\psi>}{|\mathbf{P}_j|\psi>|}$$

1. Thus a two-photon system can exist in "product states" such as $\leftrightarrow\leftrightarrow$ and $\leftrightarrow \nearrow$ 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 $\mathbf{P}_j$.

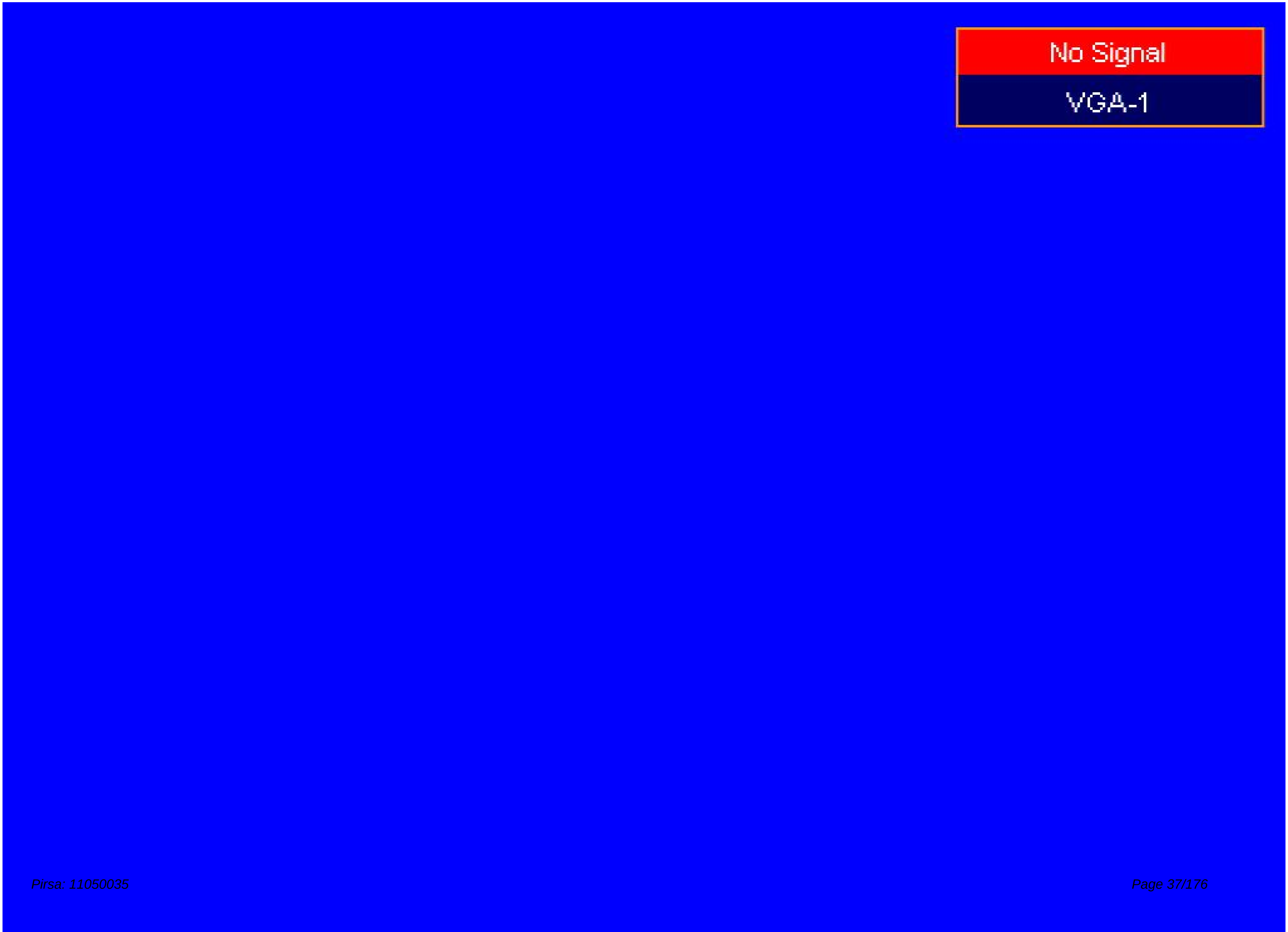


No Signal

VGA-1

No Signal

VGA-1


No Signal
VGA-1

No Signal

VGA-1


No Signal
VGA-1


No Signal
VGA-1

No Signal

VGA-1

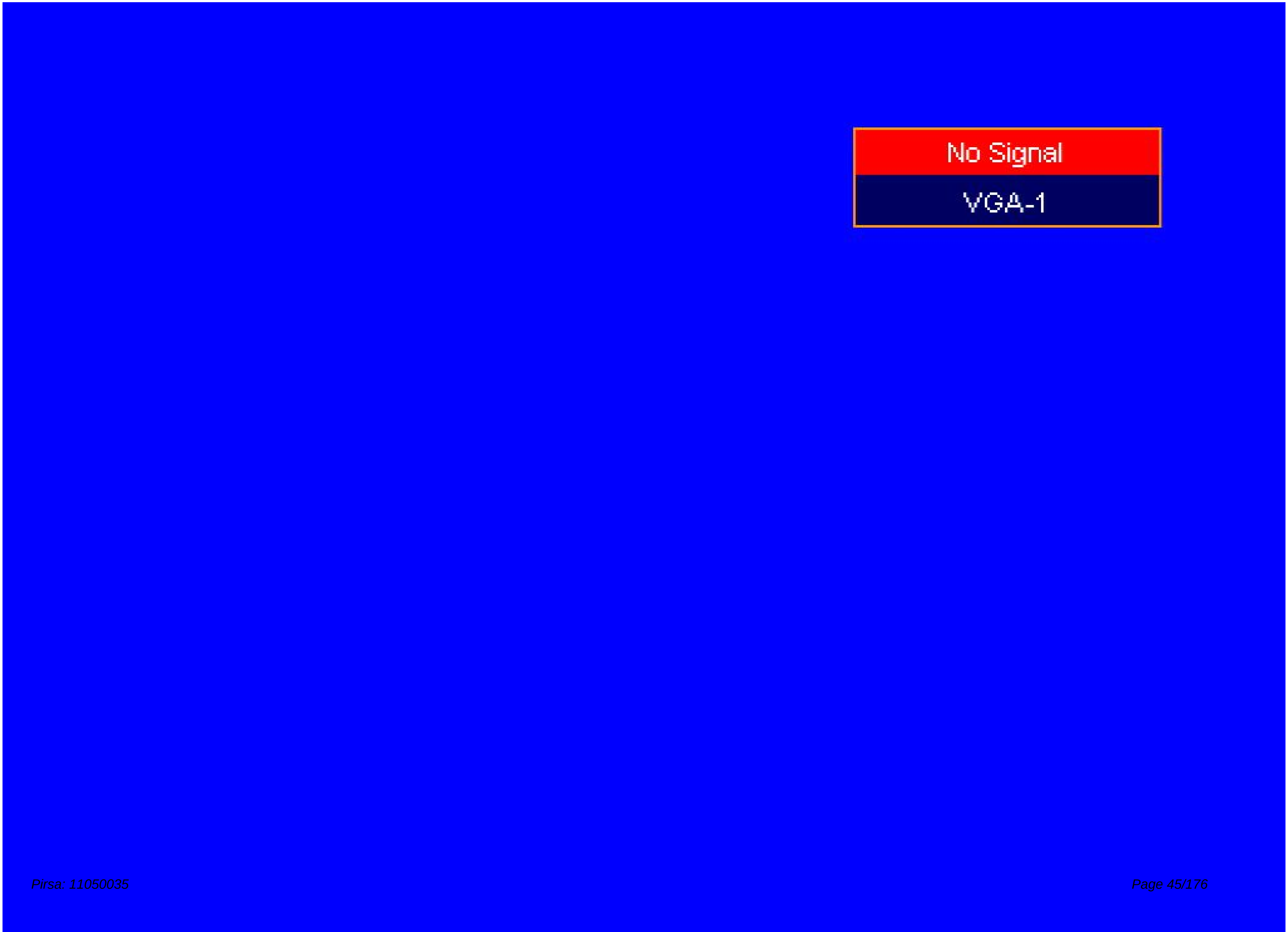
No Signal

VGA-1

No Signal

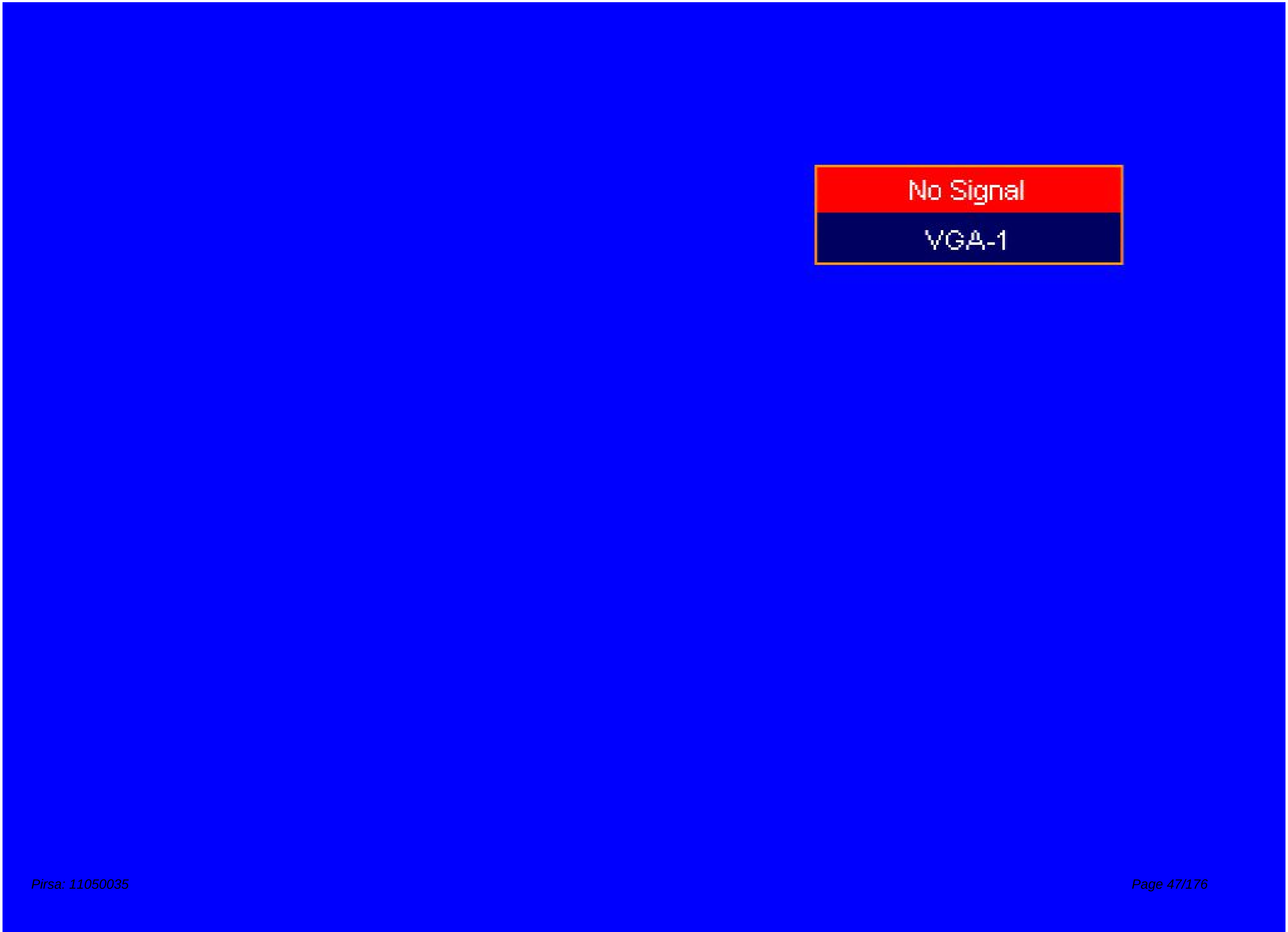
VGA-1


No Signal
VGA-1


No Signal
VGA-1

No Signal

VGA-1


No Signal
VGA-1

No Signal

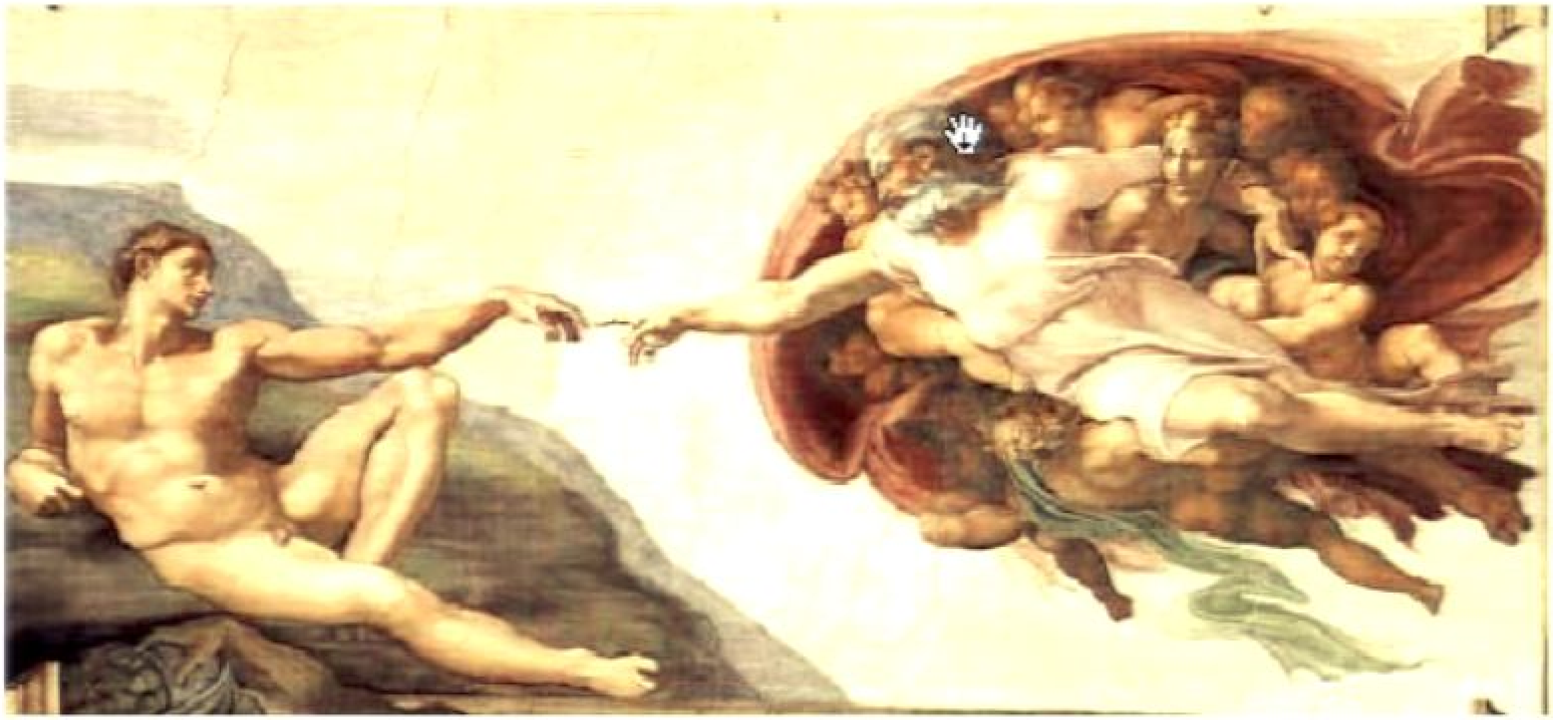
VGA-1

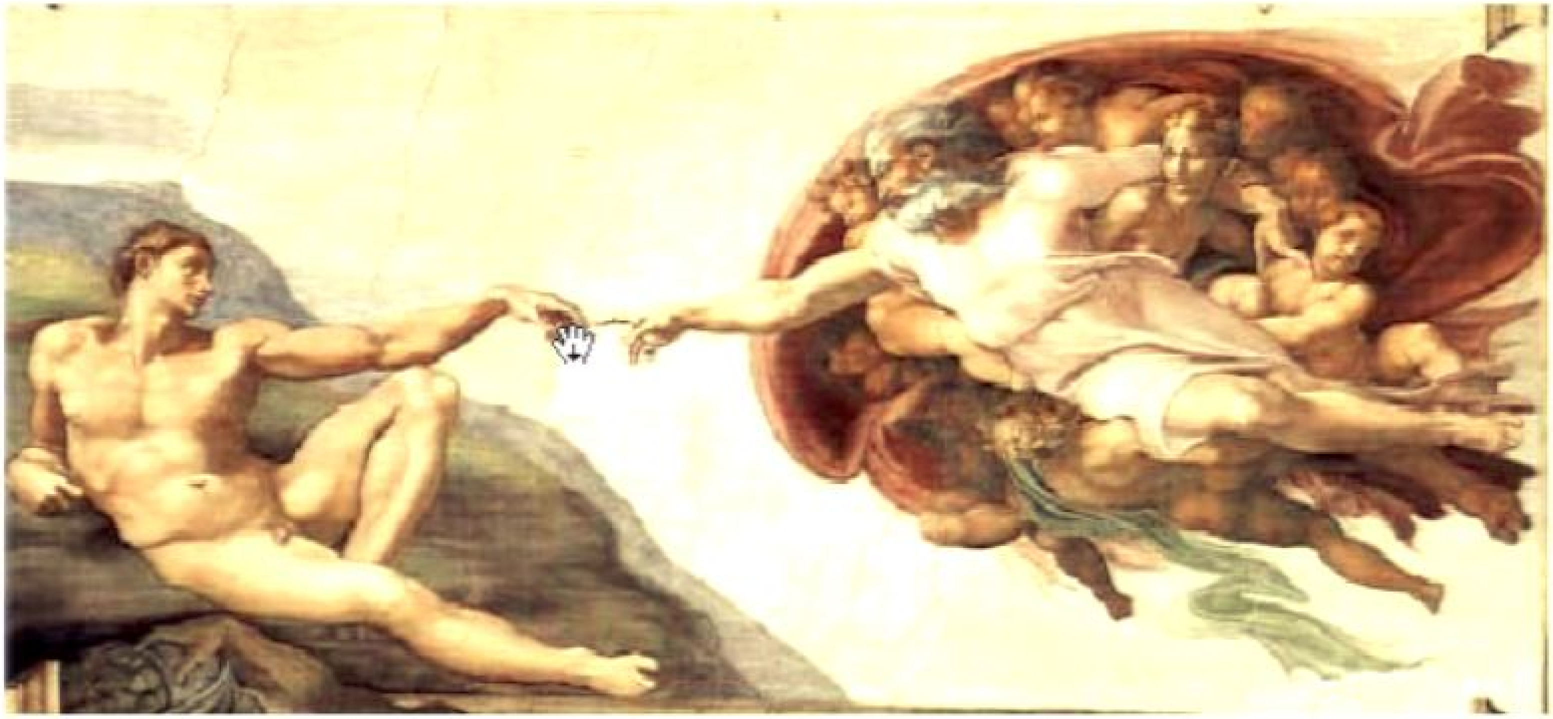
No Signal

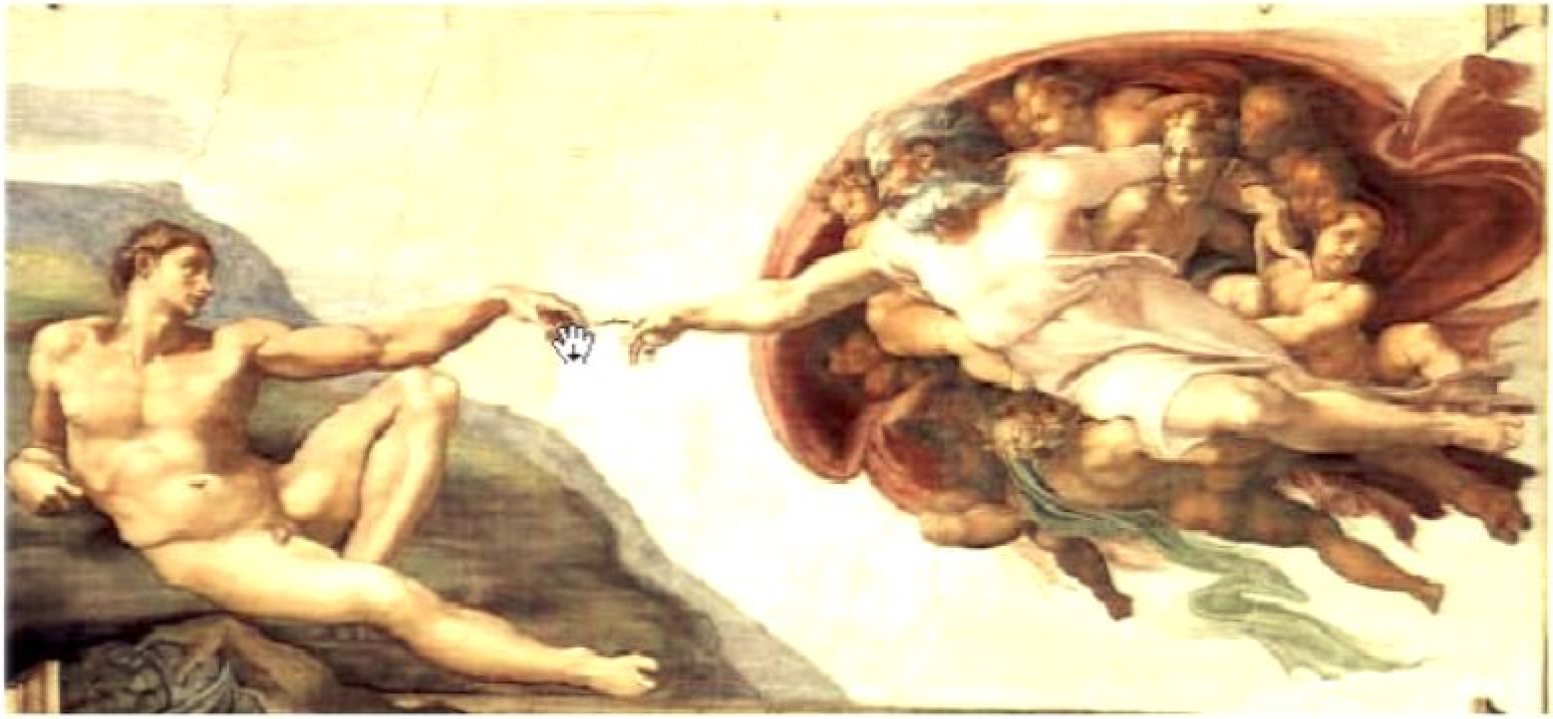
VGA-1

No Signal

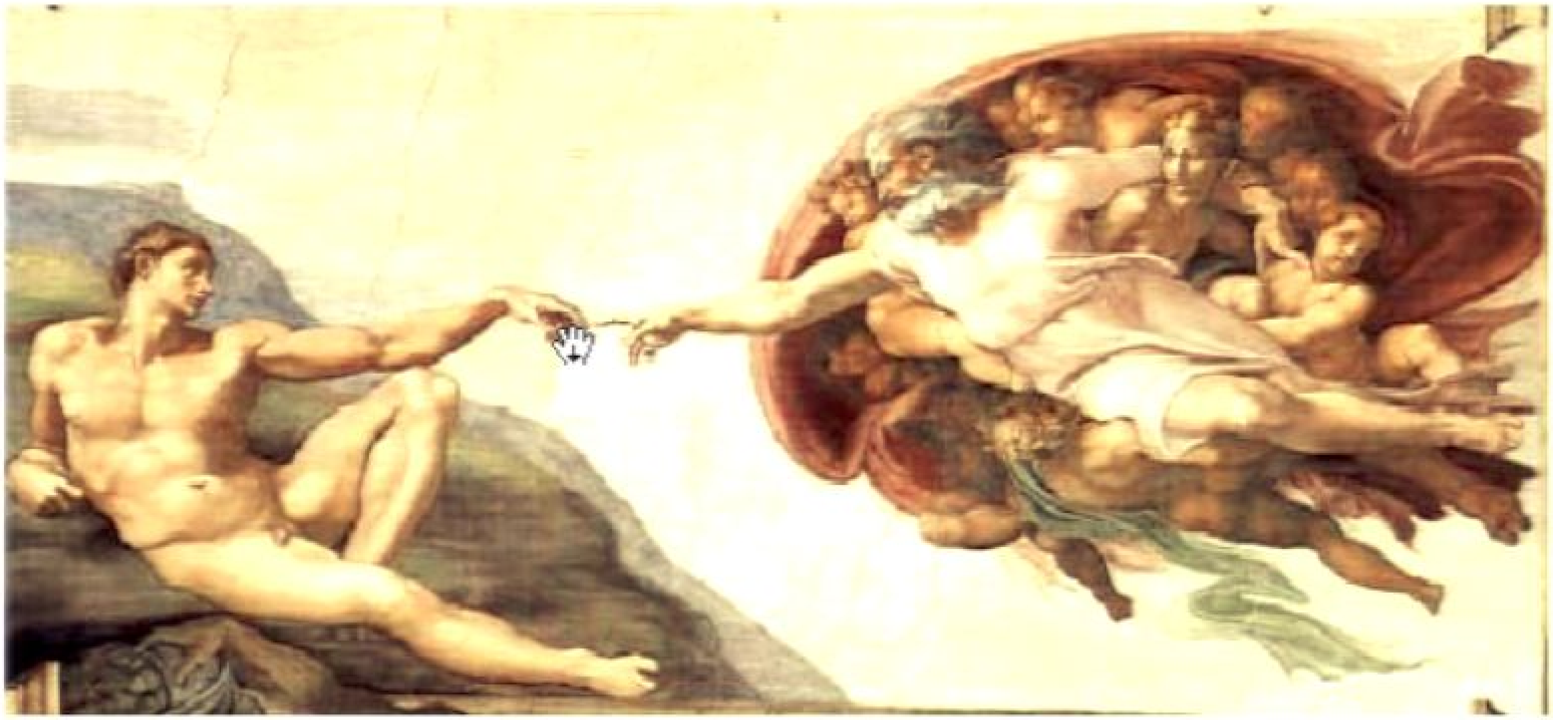
VGA-1



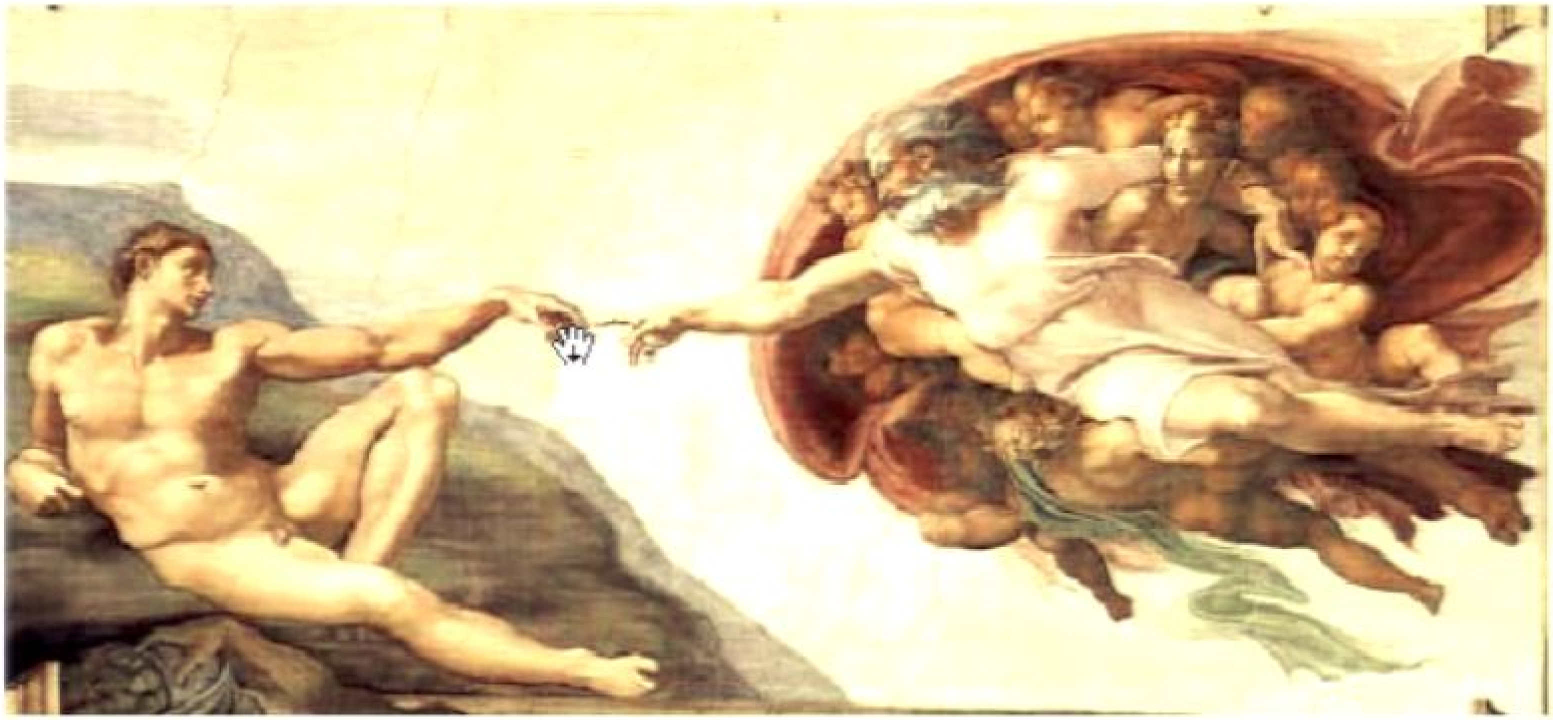





Note 11-05-0
brassard Opti
I HAD A DREAM!

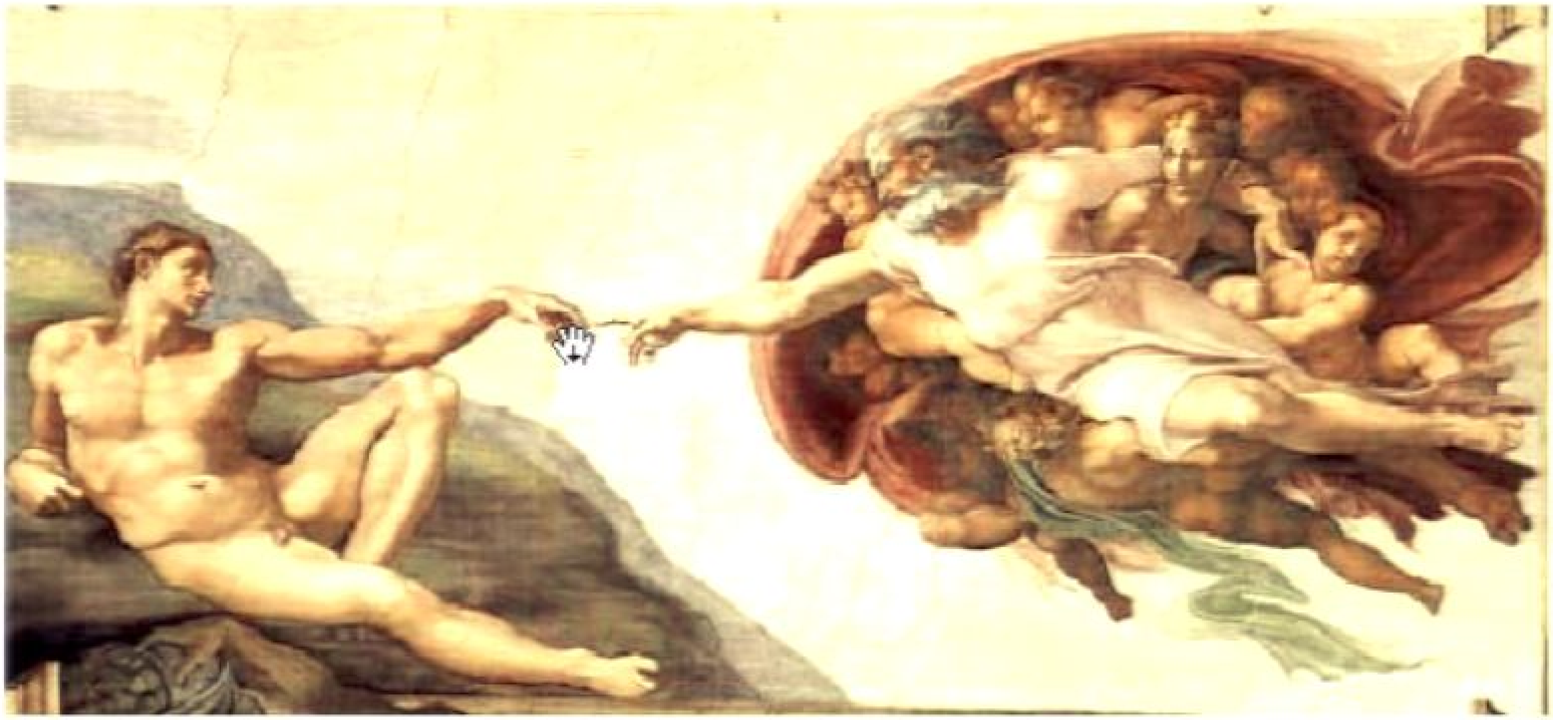


And God said:



And God said:

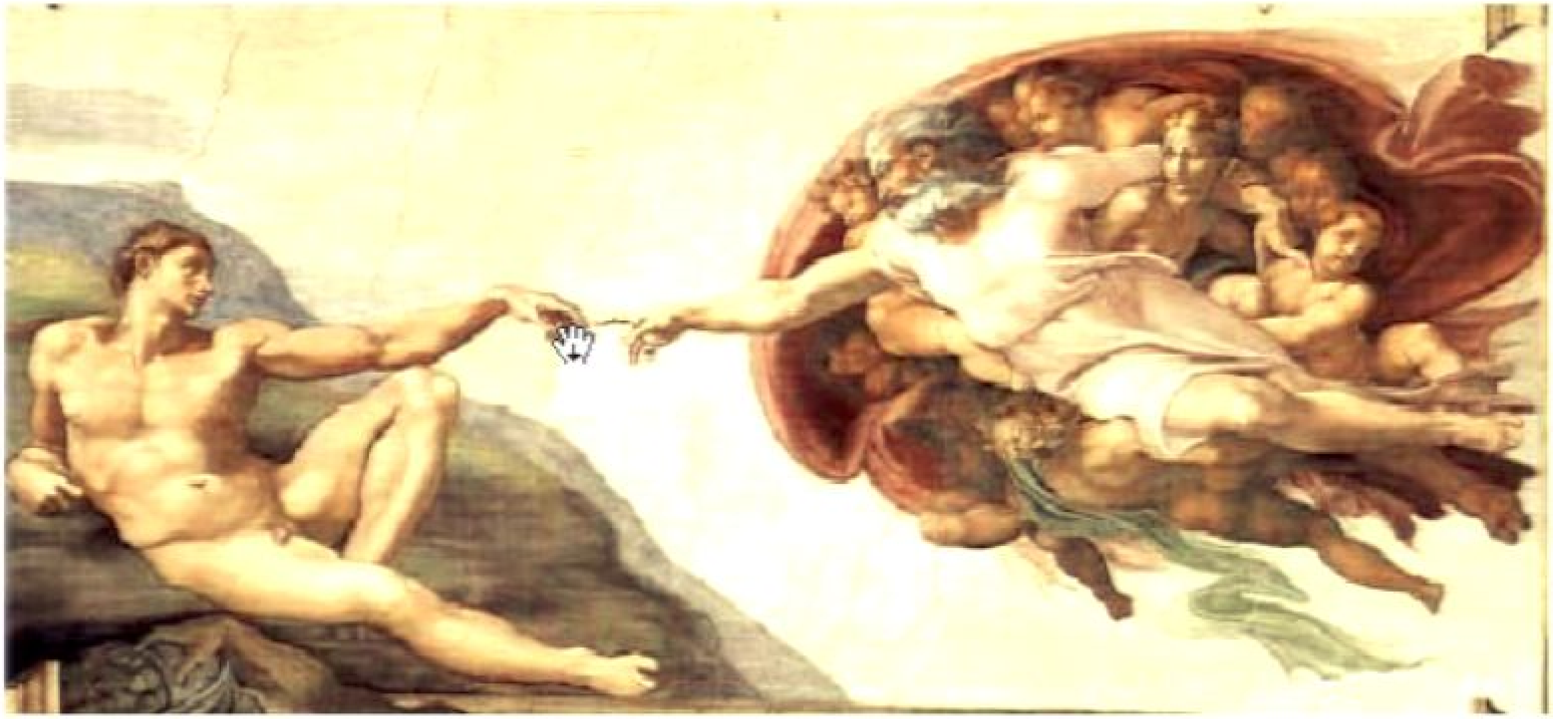
Let there be confidentiality



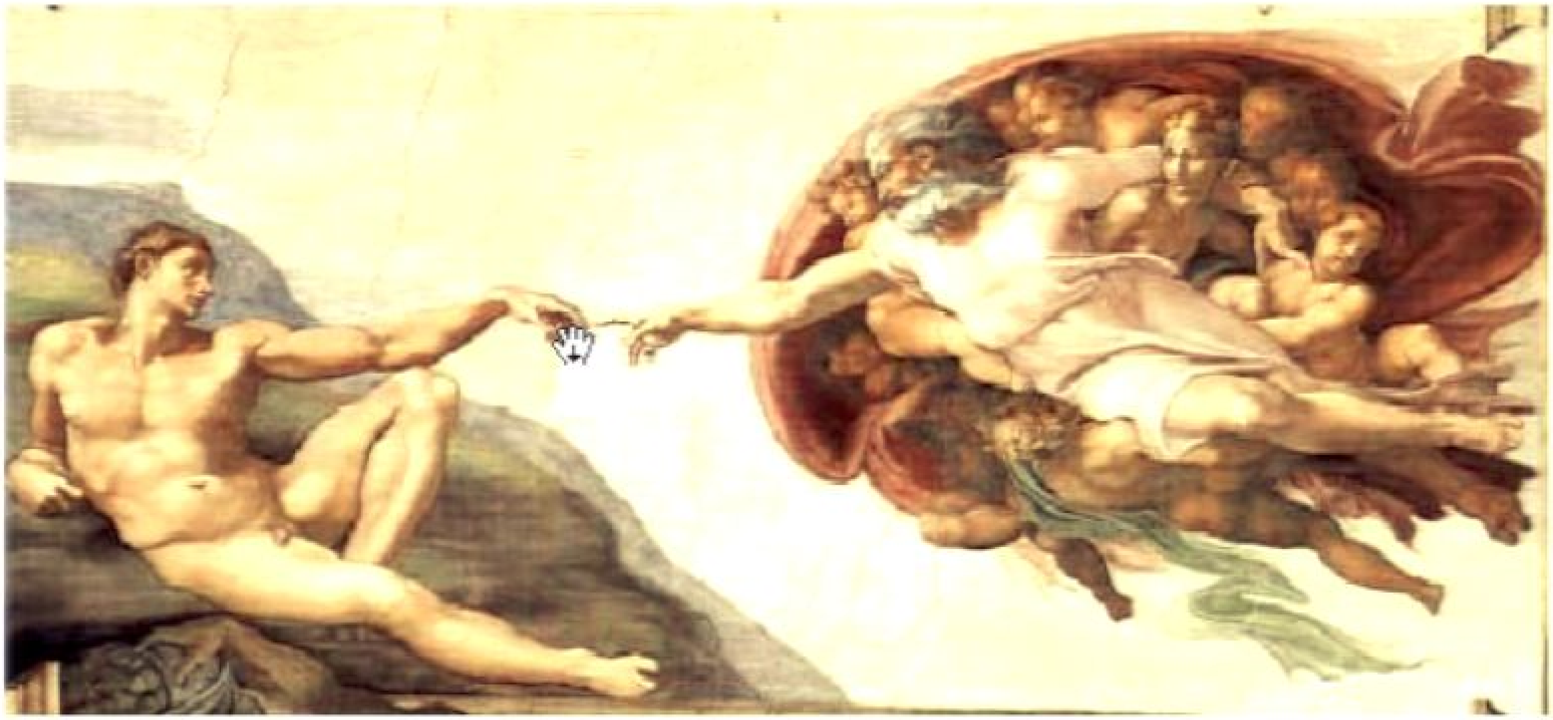
And God said:

Let there be confidentiality

And he saw that was good

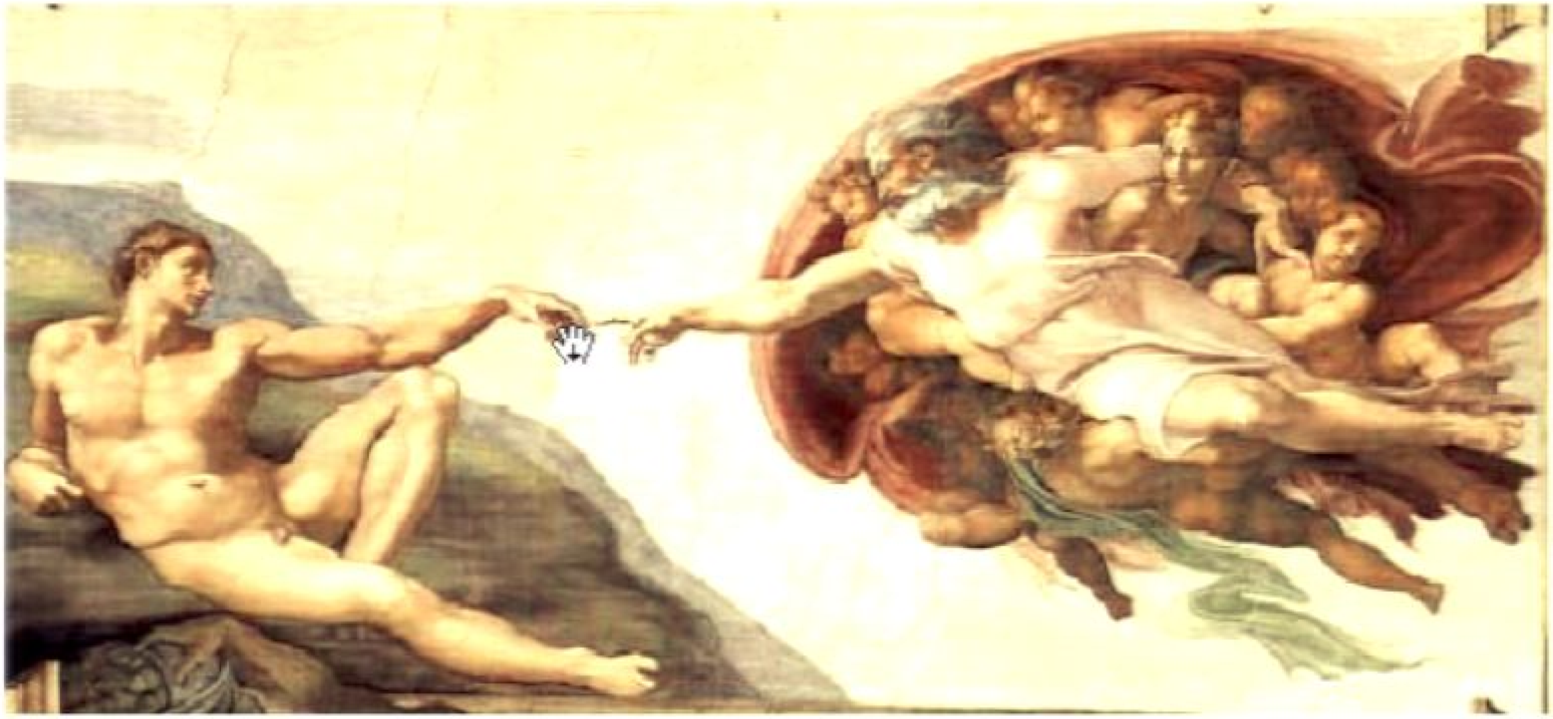


And then God said:



And then God said:

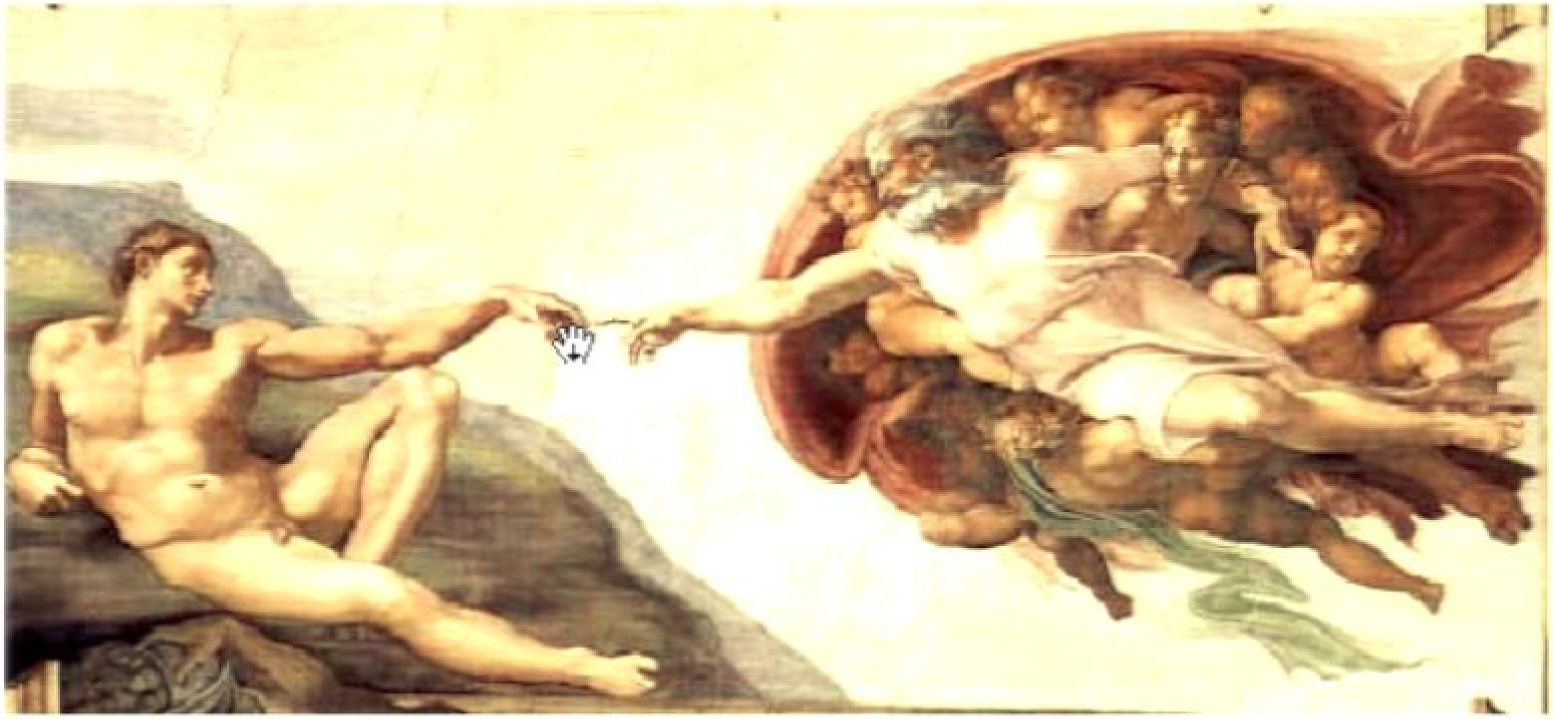
Let there be commitment



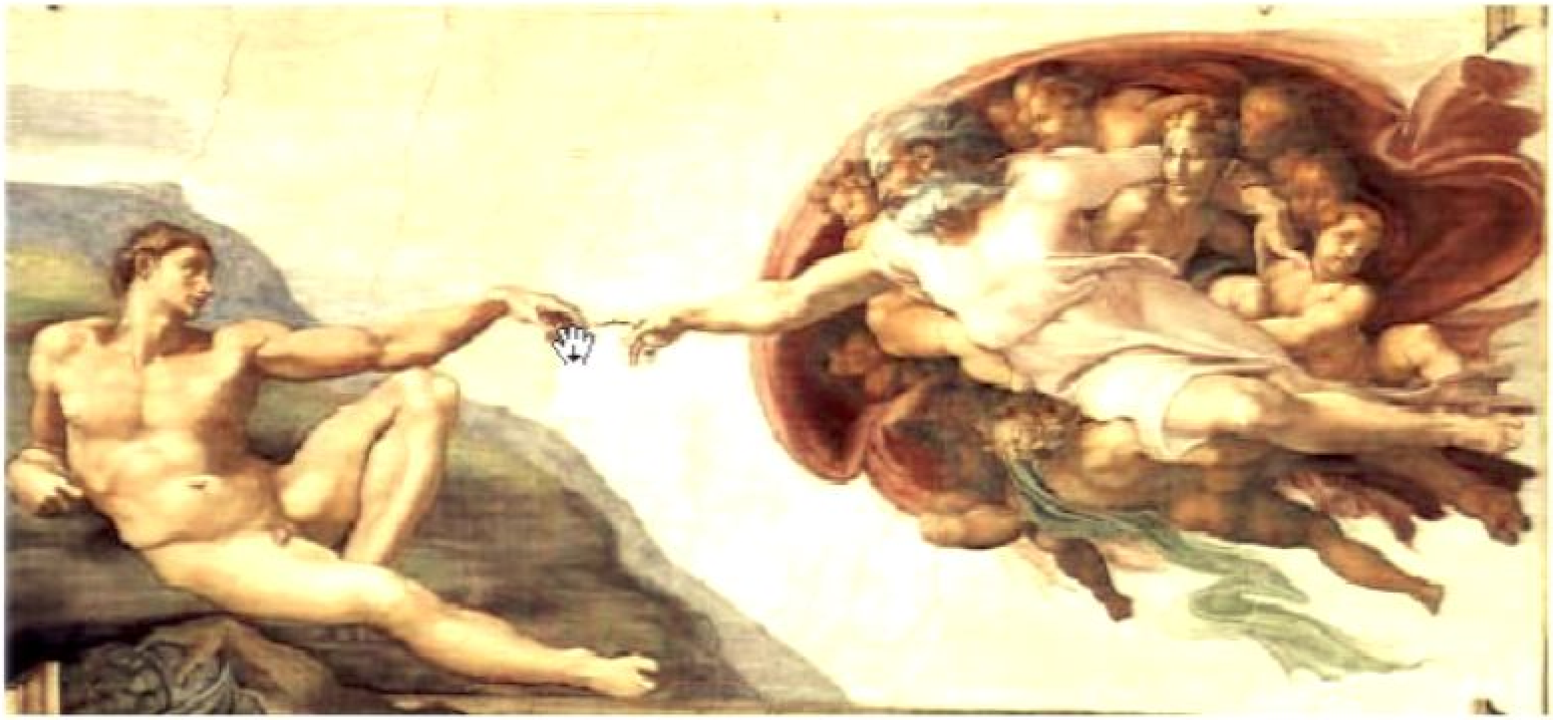
And then God said:

Let there be commitment

But he saw that was bad



So God had no choice:



So God had no choice:

He invented Quantum Mechanics !

A Famous Dispute

A Famous Dispute

God does not play dice with the Universe!

– Albert Einstein

A Famous Dispute

God does not play dice
with the Universe!

– Albert Einstein

And who are you, Mr. Einstein,
to tell God how to play?

– Niels Bohr

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 secr
key together with its inability to allow bit commitment or communicate superluminally might l
sufficient to imply the rest of quantum mechanics. I argue using a toy theory as a counterexamp
that this is not the case. I further discuss whether an additional axiom (key storage) brings ba
the quantum nature of the theory.

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 secr
key together with its inability to allow bit commitment or communicate superluminally might b
sufficient to imply the rest of quantum mechanics. I argue using a toy theory as a counterexamp
that this is not the case. I further discuss whether an additional axiom (key storage) brings ba
the quantum nature of the theory.

Characterizing Quantum Theory in Terms of Information-Theoretic Constraints

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

Why the Quantum?

(Jeff Bub, 2003)

Confidentiality
Possible

Perfect Commitment
Impossible

Quantum
Mechanics

Faster-than-light
Information Transfer
Impossible

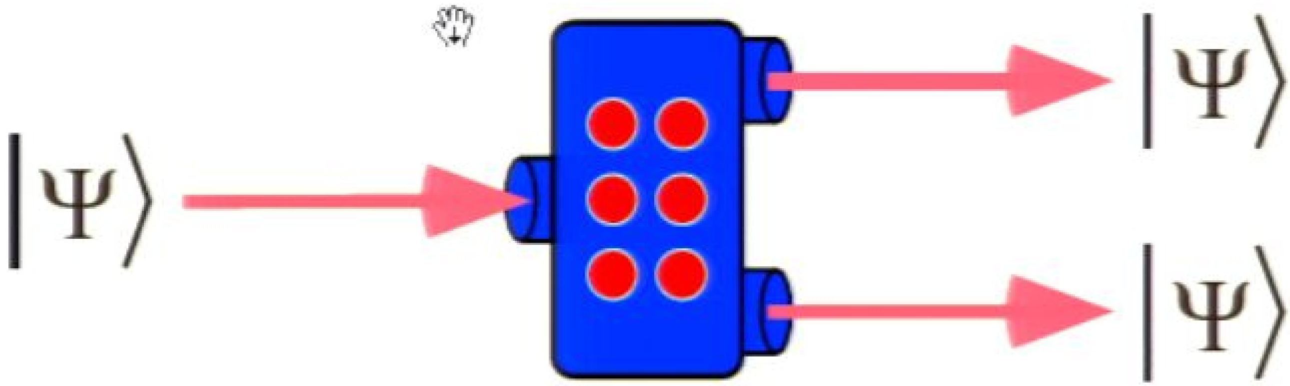
~~Confidentiality~~
~~Possible~~

→ Quantum
Mechanics

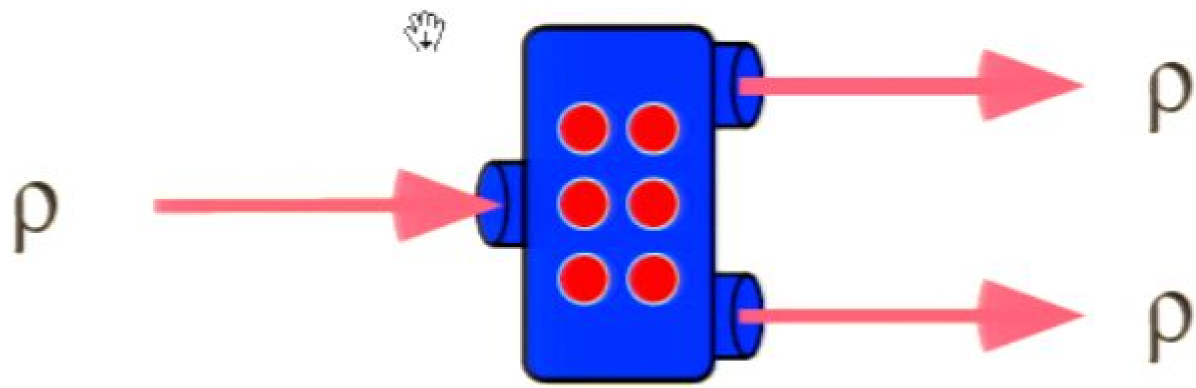
Perfect Commitment
Impossible

Perfect Broadcasting
Impossible

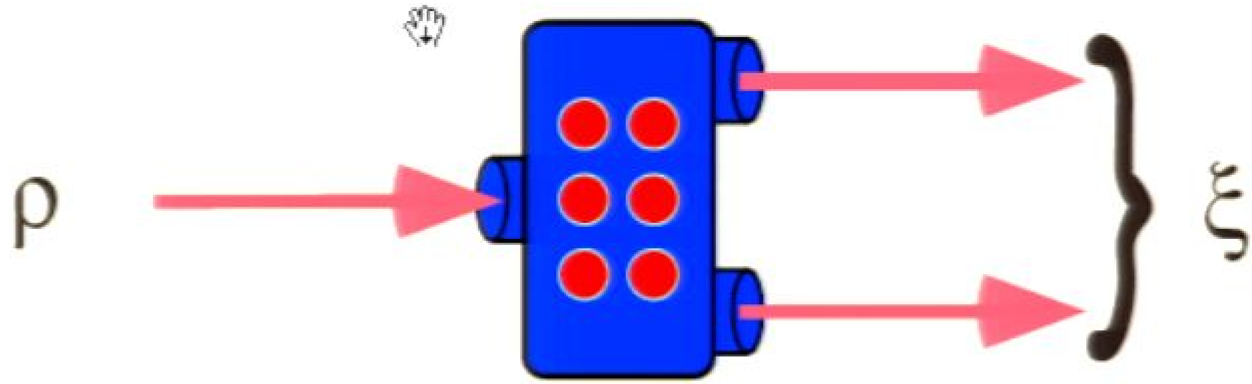
Cloning



Cloning



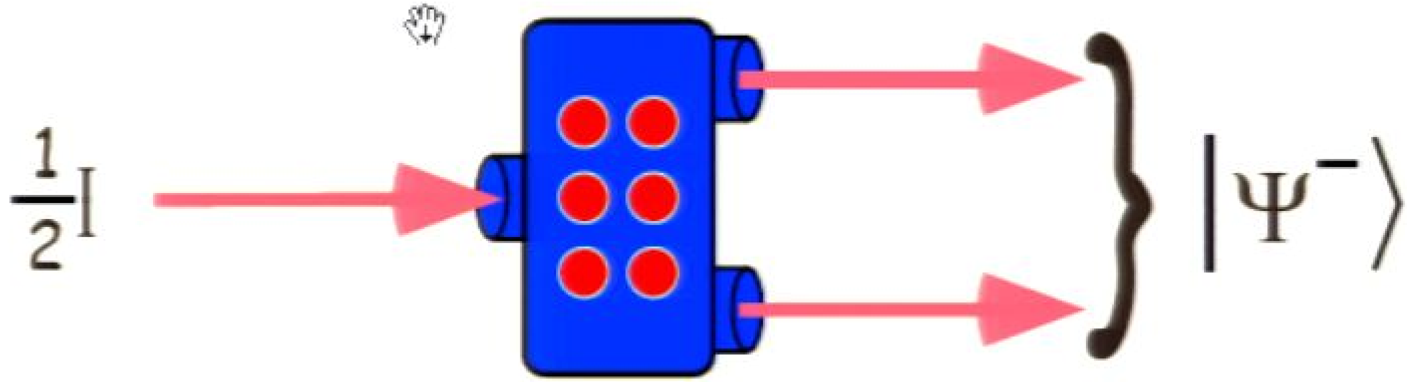
Broadcasting



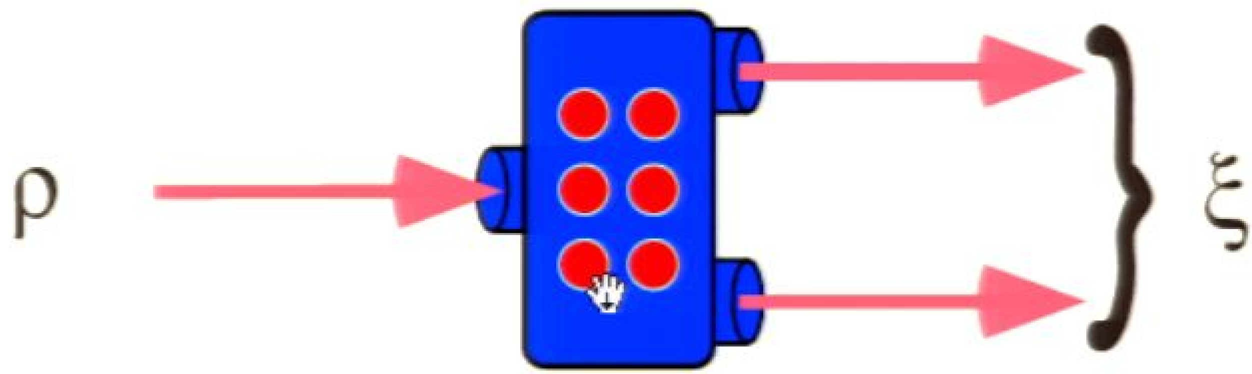
$$\mathrm{Tr}_A(\xi) = \rho$$

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

Broadcasting



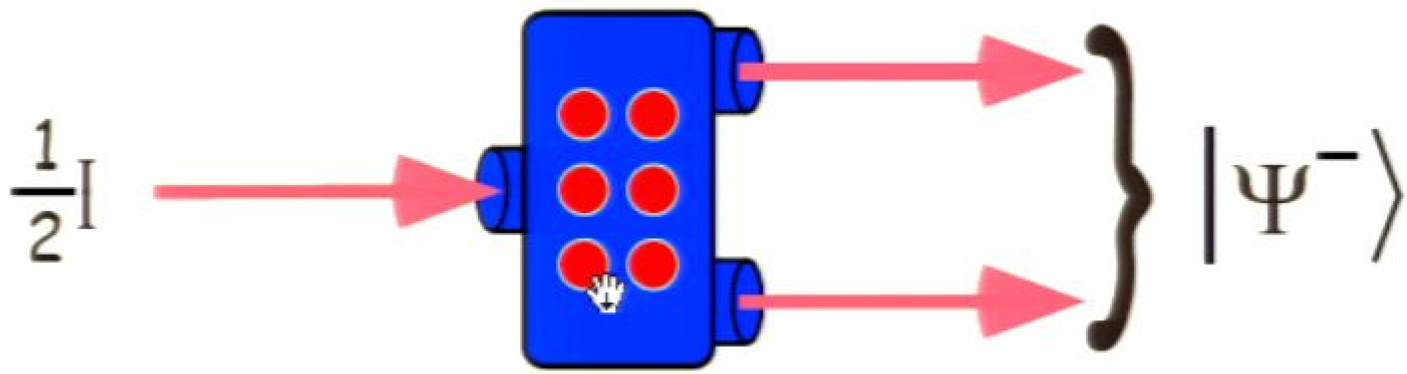
Broadcasting



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

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

Broadcasting



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

$\rightarrow$ 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

$\longrightarrow$

Basic Kinematic
Features of
Quantum
Mechanics:

Noncommutativity

Interference

Spacelike Separated
Entanglement

But did God really say:

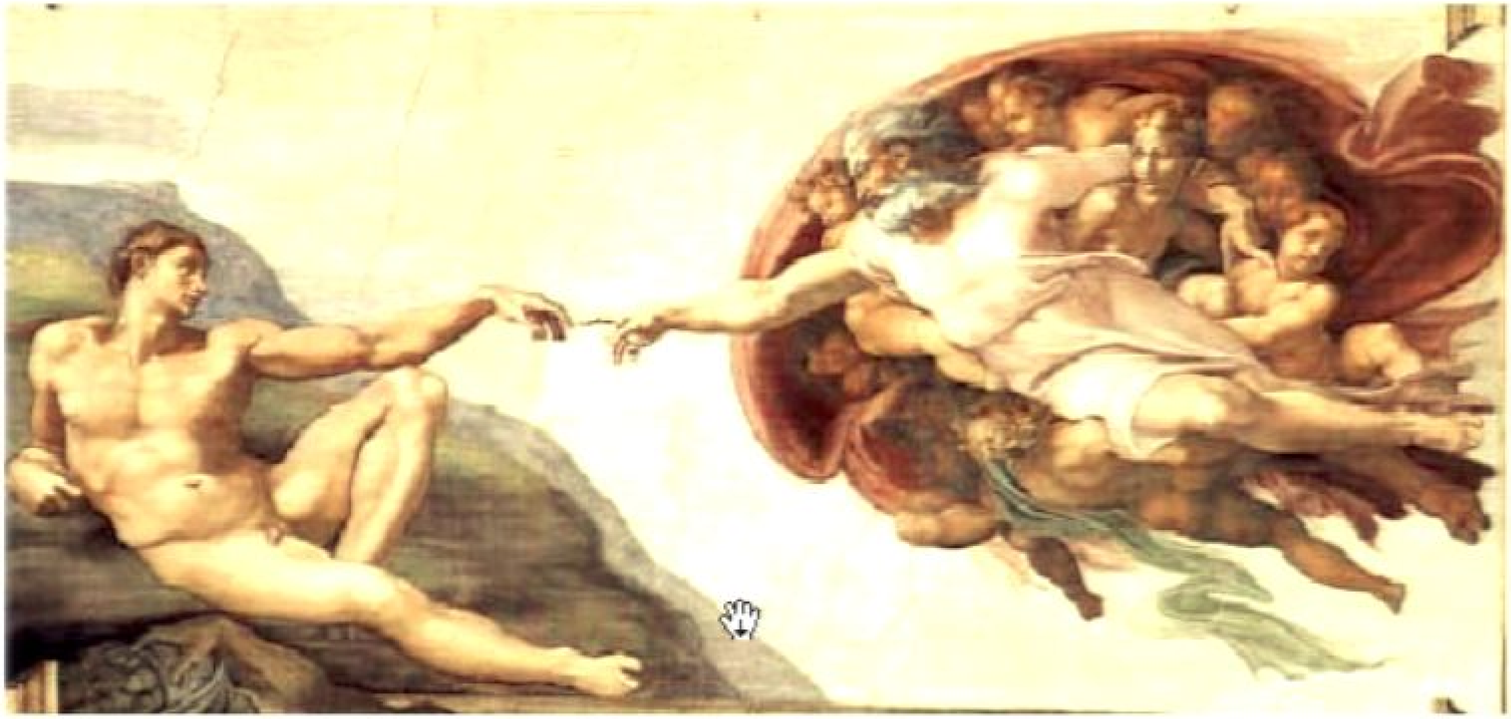
Let the Universe be ruled

by a C* algebra ?

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



But did God really say:

Let the Universe be ruled

by a C* algebra ?

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

Zur Electrodynamik Bewegter Korper

Albert Einstein, Annalen der Physik 17, 1905

On the Electrodynamics of Moving Bodies

Albert Einstein, Annalen der Physik 17, 1905

On the Electrodynamics of Moving Bodies

Albert Einstein, Annalen der Physik 17, 1905

The theory to be developed is based
-- like all electrodynamics --
on the kinematics of the rigid body

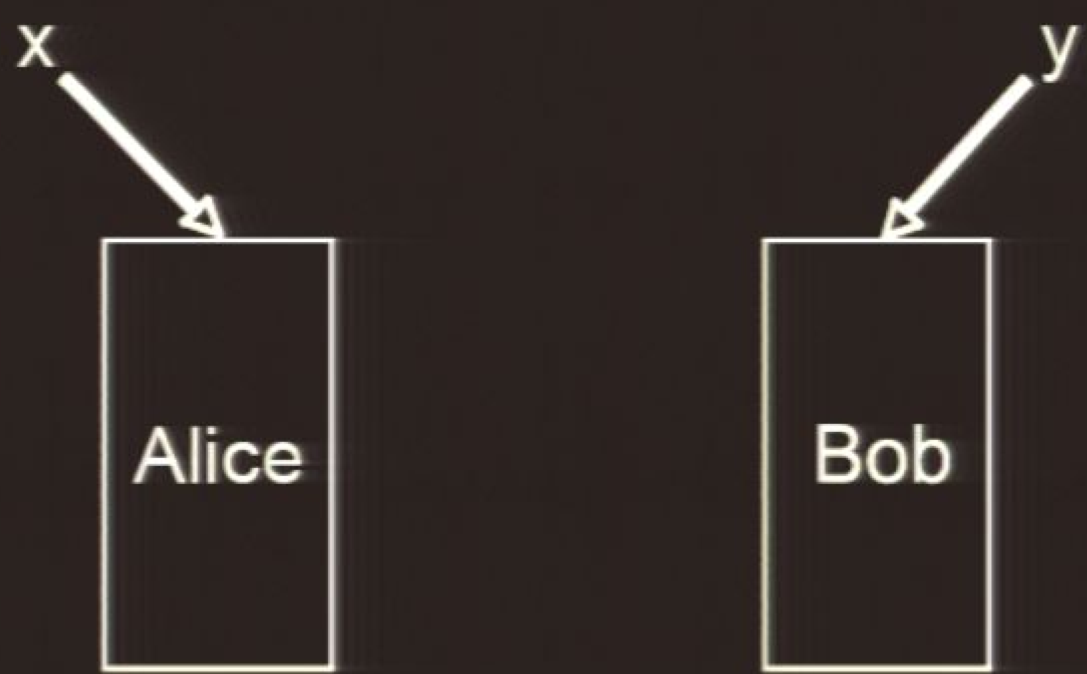
On the Electrodynamics of Moving Bodies

Albert Einstein, Annalen der Physik 17, 1905

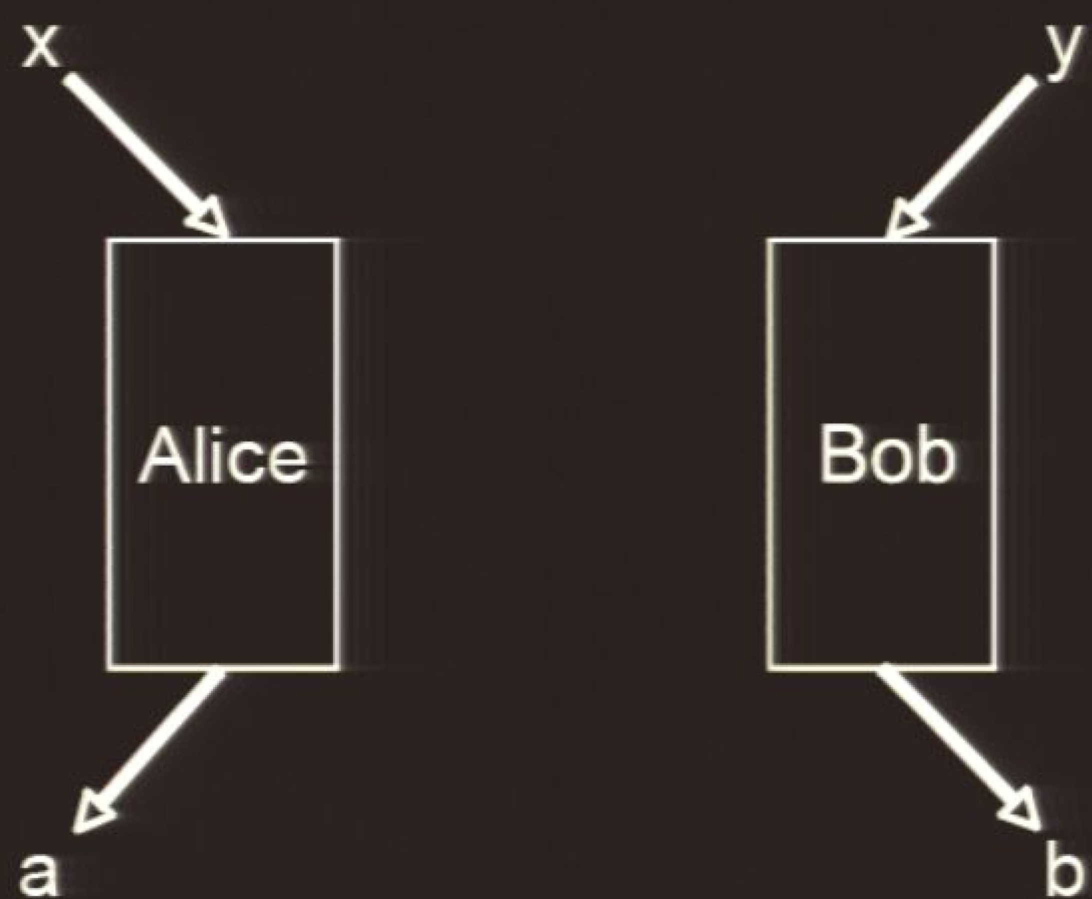
It is clear that the equations must be linear on account of the properties of homogeneity which we attribute to space and time

Non-local boxes

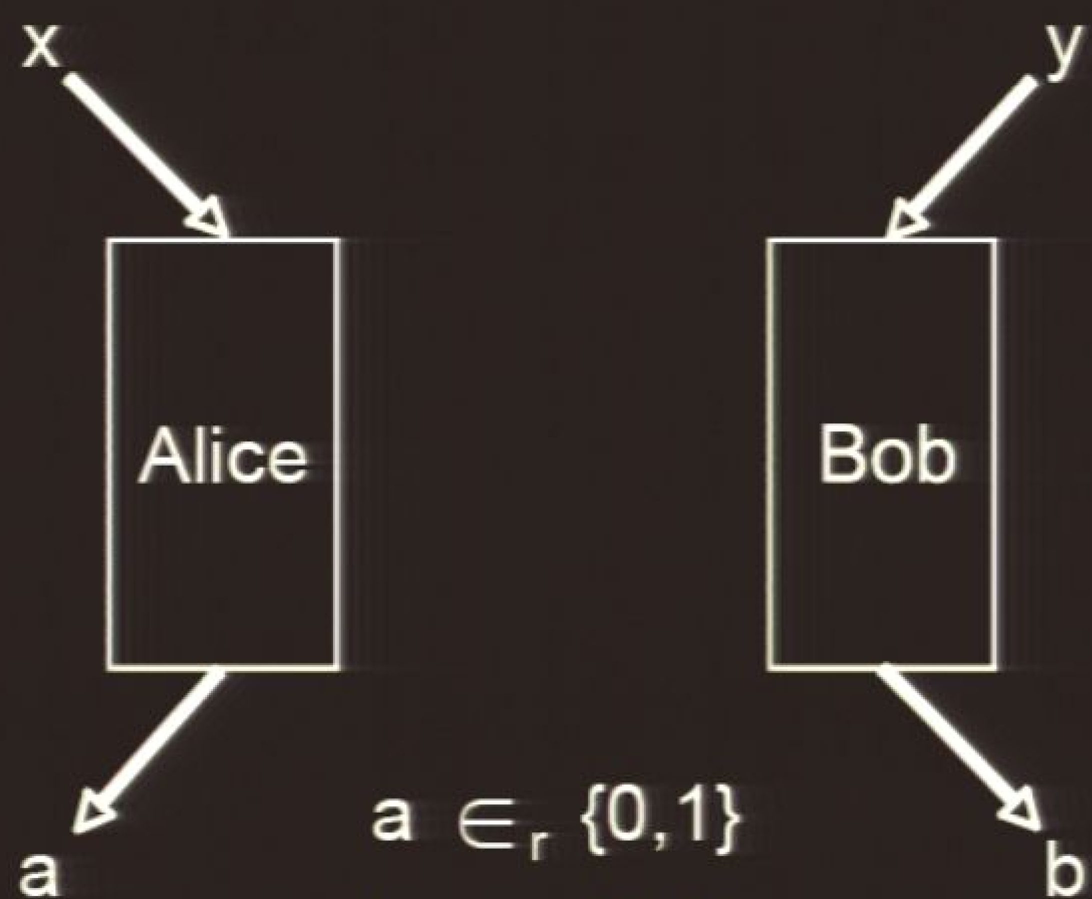
Non-local boxes



Non-local boxes

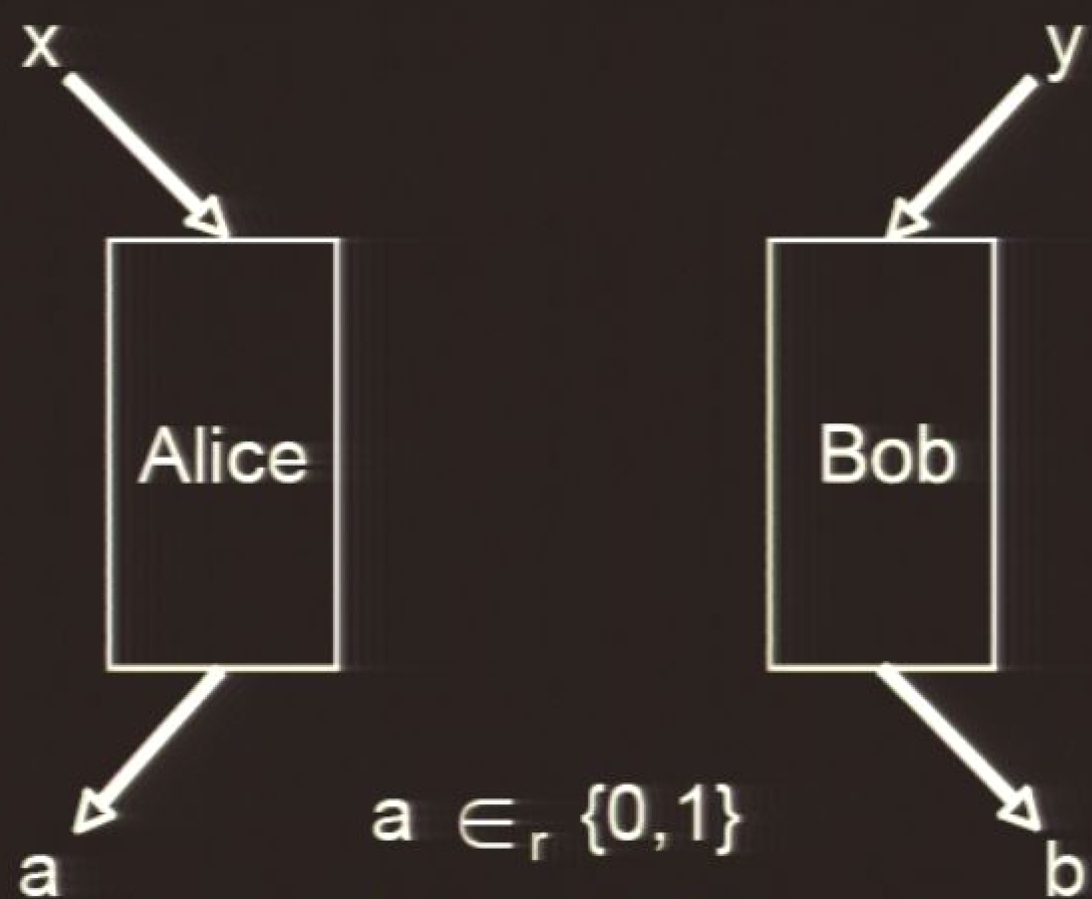


Non-local boxes



$$a \in_r \{0,1\}$$
$$b \in_r \{0,1\}$$

Non-local boxes



$$a \in_r \{0,1\}$$

$$b \in_r \{0,1\}$$

$$a \oplus b = x \wedge y$$

Non-Local Boxes

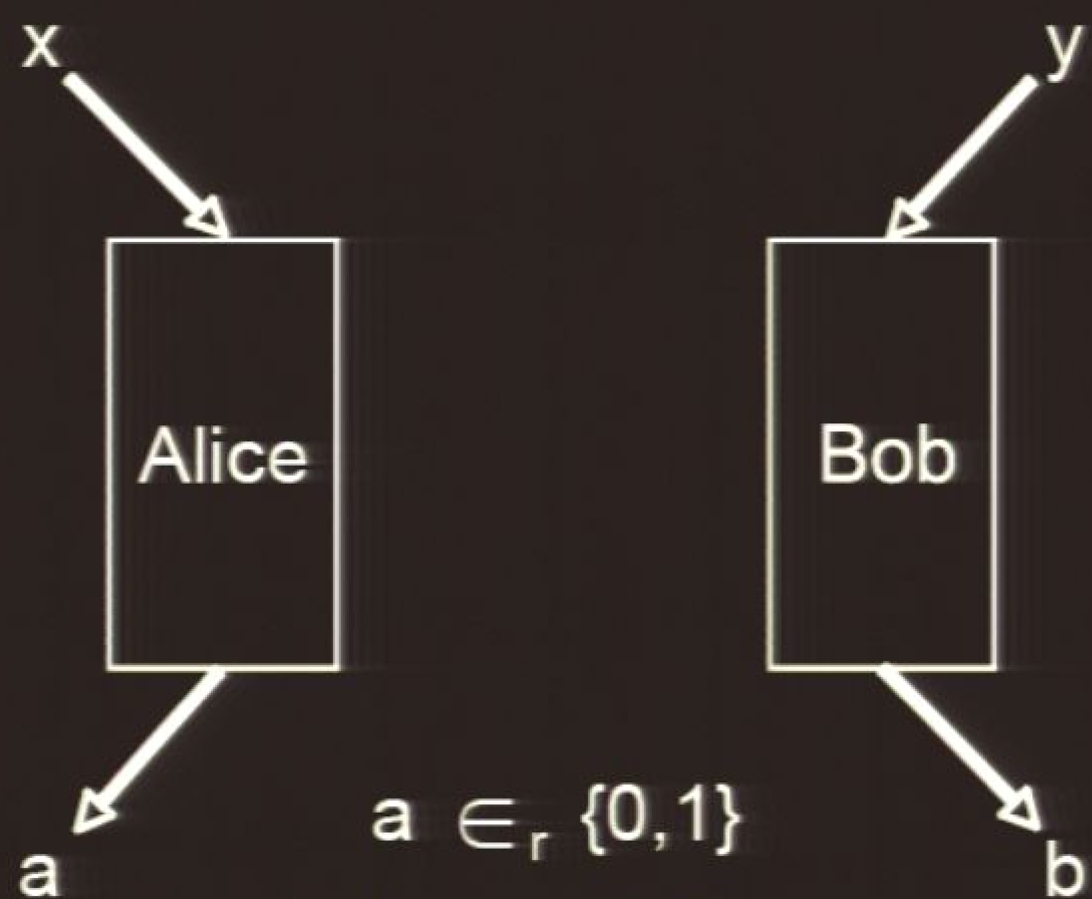
Non-Local Boxes

They cannot be used to communicate:

They are causal and atemporal

Non-Local Boxes

Non-local boxes



$$a \in_r \{0,1\}$$

$$b \in_r \{0,1\}$$

$$a \oplus b = x \wedge y$$

Non-Local Boxes

They cannot be used to communicate:
They are causal and atemporal

They can be simulated *classically*
with probability 75%

Non-Local Boxes

They cannot be used to communicate:

They are causal and atemporal

Non-Local Boxes

They cannot be used to communicate:
They are causal and atemporal

They can be simulated *classically* with probability 75%

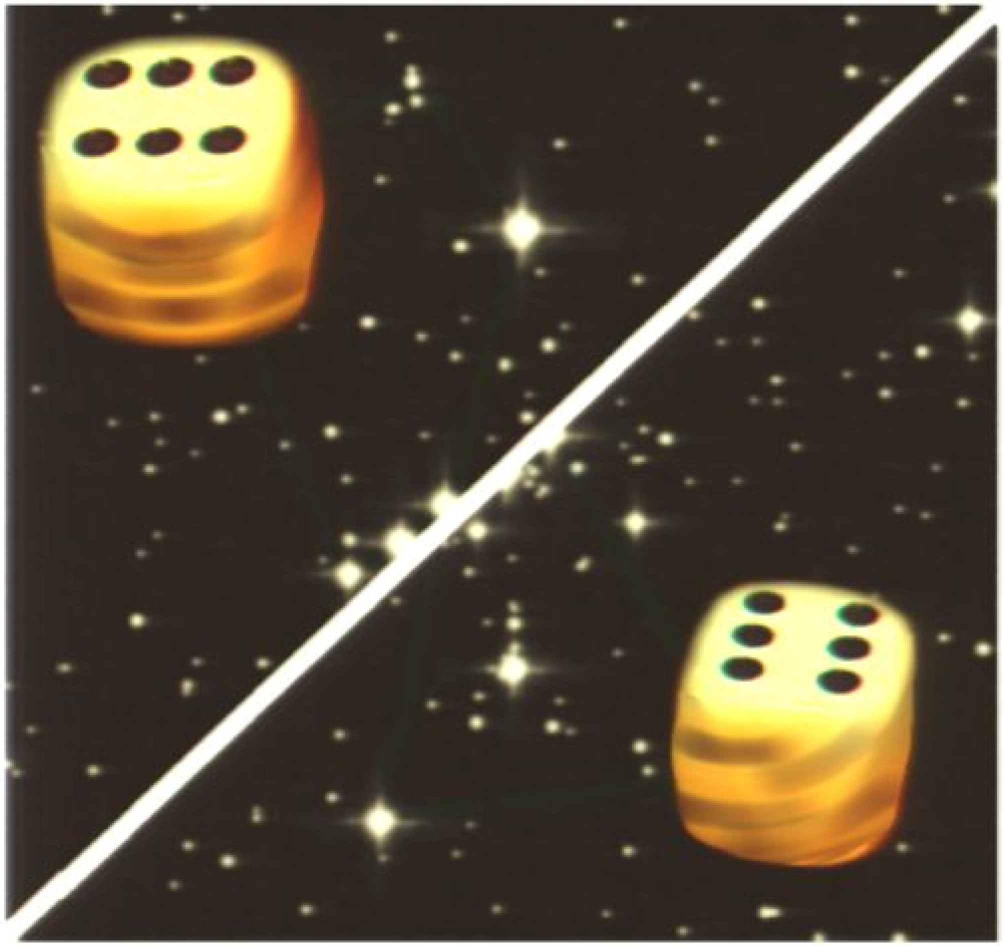
Non-Local Boxes

They cannot be used to communicate:
They are causal and atemporal

They can be simulated *classically* with probability 75%

They can be simulated *quantumly* with probability $\cos^2 \frac{\pi}{8} = \frac{2+\sqrt{2}}{4} \approx 85\%$

Entanglement



E. Schrödinger 1935

The Essence of Quantum Physics which forces us to depart from all our cherished views how the World works

© Zeilinger

The Question

The Question

Quantum mechanics *must* be causal

The Question

Quantum mechanics *must* be causal

Quantum mechanics allows for instantaneous nonlocal correlations

The Question

Quantum mechanics *must* be causal

Quantum mechanics allows for instantaneous nonlocal correlations

Why can't quantum mechanics yield the *strongest* nonlocal correlations possible among all causal theories?

[Abelson, 1978; Yao, 1979

Communication Complexity

Alice

Bob

Communication Complexity

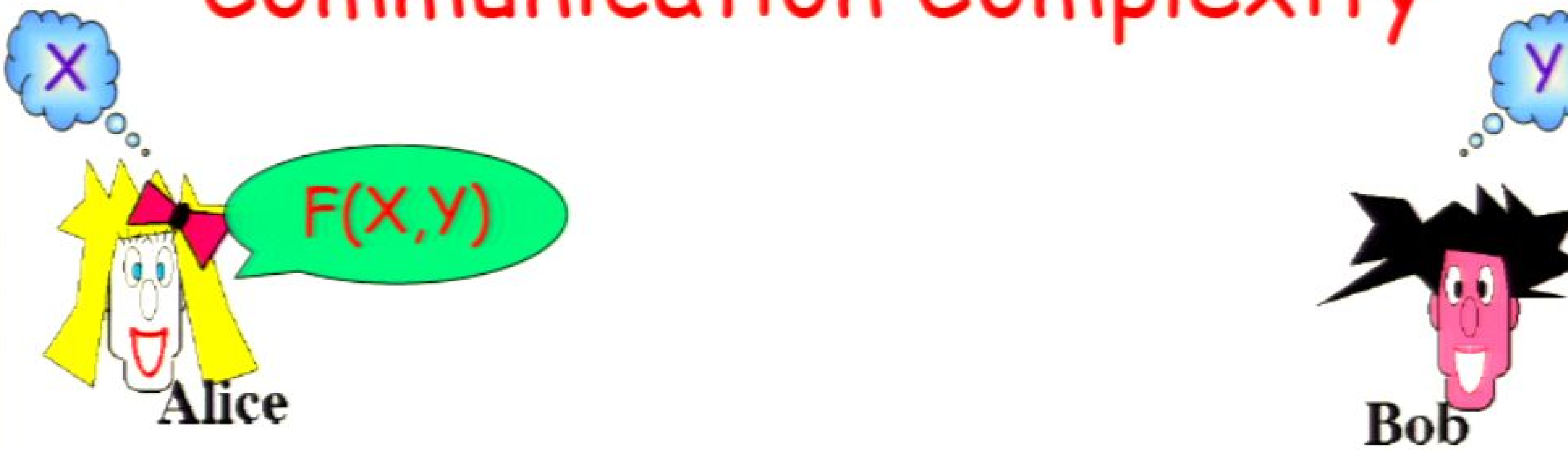
Communication Complexity

Alice

Bob

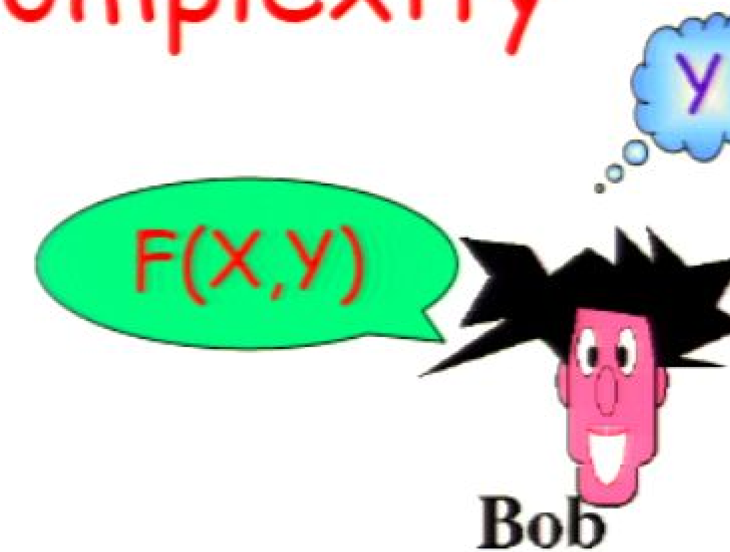
They want to compute some function F(X,Y)

Communication Complexity



They want to compute some function F(X,Y)

Communication Complexity



They want to compute some function F(X,Y)

Communication Complexity

They want to compute some function F(X,Y)

Communication Complexity

They want to compute some function F(X,Y)

Goal: minimize number of bits of communication

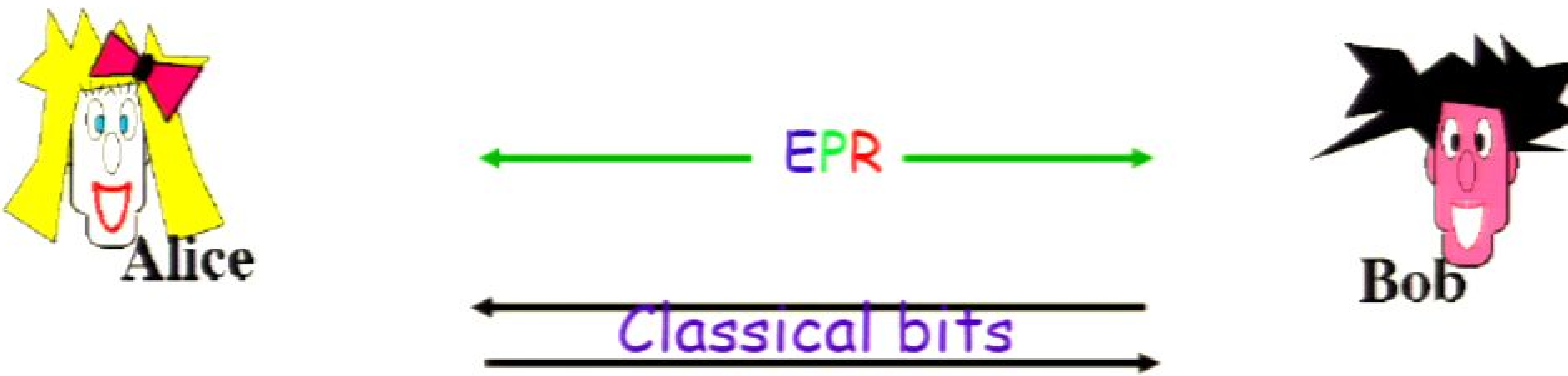
Entanglement Assisted Communication Complexity

[Cleve & Buhrman, 1997]

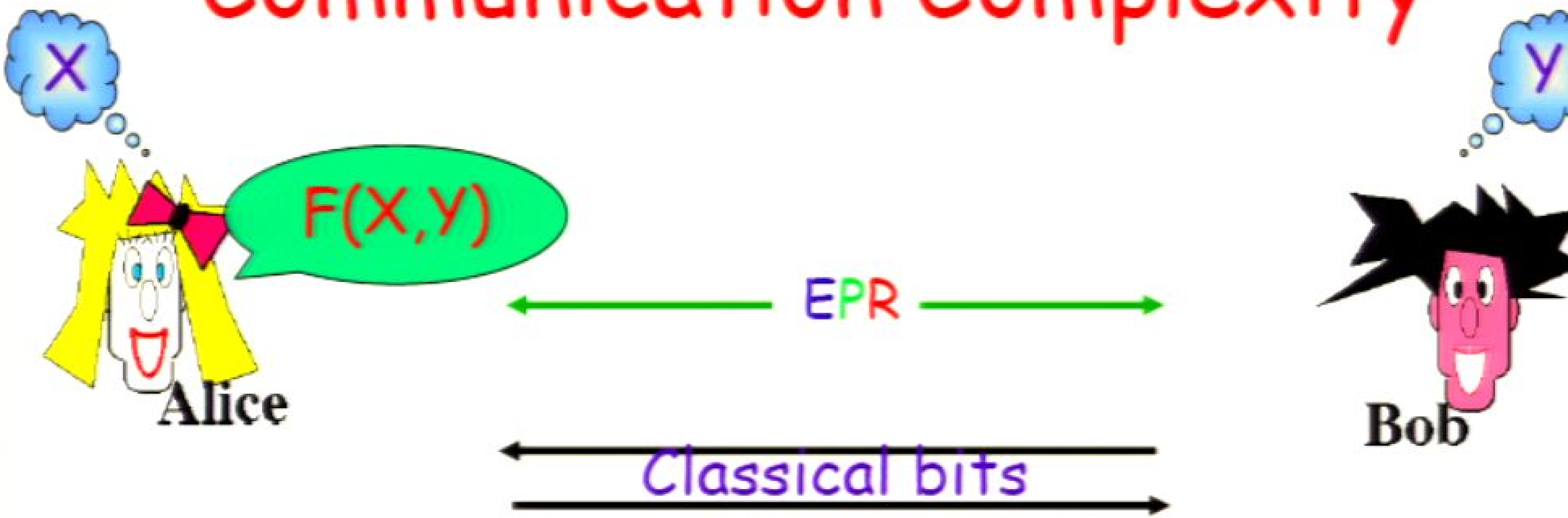
Classical bits

Entanglement Assisted Communication Complexity

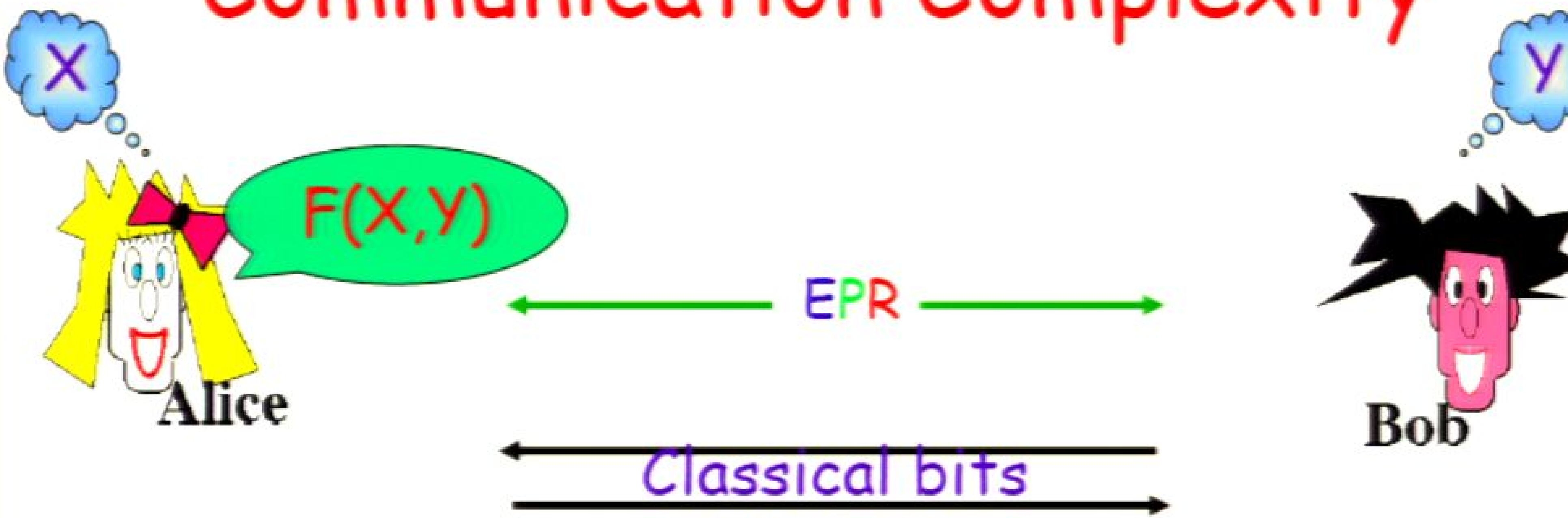
[Cleve & Buhrman, 1997]



Entanglement Assisted Communication Complexity



Entanglement Assisted Communication Complexity

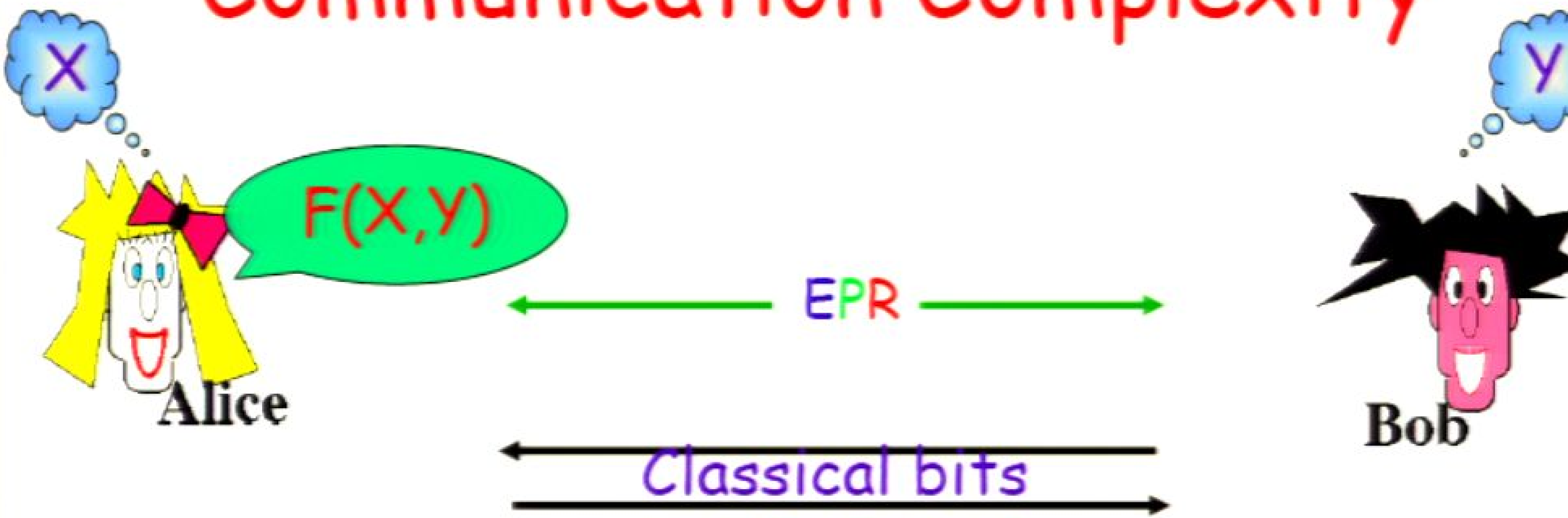


Can entanglement reduce *classical* communication needs?

Definition

A Boolean function is *trivial* (in terms of communication complexity) if it can be computed with *a single bit* of communication

Entanglement Assisted Communication Complexity



Can entanglement reduce *classical* communication needs?

Definition

A Boolean function is *trivial* (in terms of communication complexity) if it can be computed with *a single bit* of communication

Definition

A Boolean function is *trivial* (in terms of communication complexity) if it can be computed with *a single bit* of communication

Note that *zero* communication is impossible in any causal theory if the function depends on both inputs

Theorem

Some Boolean functions are nontrivial: they require more than one bit of classical communication

Theorem

Some Boolean functions are nontrivial: they require more than one bit of classical communication

Some Boolean functions remain nontrivial with shared entanglement

The Question

Quantum mechanics *must* be causal

Quantum mechanics allows for instantaneous nonlocal correlations

Why can't quantum mechanics yield the *strongest* nonlocal correlations possible among all causal theories?

Implausible Consequences of Superstrong Nonlocality

Wim van Dam[a]
Department of Computer Science, University of California at Santa Barbara, Santa Barbara, CA 93106-5110, USA

This Letter looks at the consequences of so-called 'superstrong nonlocal correlations', which are hypothetical violations of Bell/CHSH inequalities that are stronger than quantum mechanics allows, yet weak enough to prohibit faster-than-light communication. It is shown that the existence of maximally superstrong correlated bits implies that all distributed computations can be performed with a trivial amount of communication, i.e. with one bit. If one believes that Nature does not allow such a computational 'free lunch', then the result in the Letter gives a reason why superstrong correlation are indeed not possible.

PACS numbers: 03.65.Ud, 03.65.Ta, 03.67.Hk, 03.67.Mn
Keywords: foundations of quantum mechanics, nonlocality, communication complexity

The Clauser-Horne-Shimony-Holt (CHSH) inequality [6] for classical theories gives the following upper bound on the strength of correlations between two space-like separated experiments, which can be violated by quantum mechanics. Imagine two parties Alice and Bob (A and B) that share a distributed system Φ_{AB}. Each party can independently perform one out of two measurements on their part of the system, such that in total there are four experimental set-ups that can apply to the combined system: (m_0^A, m_0^B), (m_0^A, m_1^B), (m_1^A, m_0^B) and (m_1^A, m_1^B). For each measurement on each side there are two possible outcomes, which are labeled "0" and "1". The parties repeat the experiment many times using the different settings, thus obtaining an accurate estimation of all the possible correlations between the different measurements and their outcomes. As it is understood that for each trial A and B always use the same state-preparation of Φ_{AB}, the conditional part will be omitted when expressing the probabilities of the various outcomes. Hence, the probability that both Alice and Bob measure a "one" when they use the measurement settings m_0^A and m_1^B is denoted simply by $\text{Prob}(m_0^A = 1, m_1^B = 1)$.

The main result of Bell [2] and CHSH [6] is that for any local, hidden variable theory about Φ_{AB} and the measurements m^A and m^B, the following inequality must hold:

$$\sum_{x,y\in\{0,1\}} \text{Prob}(m_x^A + m_y^B \equiv x \cdot y) \ \leq \ 3, \qquad (1)$$

where we interpret the binary values as elements of 'modulo 2 calculations' such that $1+1 \equiv 0$. Quantum mechanics allows a violation of the bound of Equation [1] by

$$\sum_{x,y\in\{0,1\}} \text{Prob}(m_x^A + m_y^B \equiv x \cdot y) \ = \ 2 + \sqrt{2} \approx 3.41,$$

if A and B use, for example, the entangled pair of quantum bits $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and a suitable set of measurement projectors m. Besides the fact that this result proves that the theory of quantum mechanics cannot be phrased as a local theory, the more important conclusion is that the nonlocality of Nature can be verified experimentally (as has been done many times [1, 10]). This experimental aspect is the more relevant side of the matter as it is not inconceivable that in the future we will have to replace the theory of quantum mechanics by a more accurate or more general model of Nature, making the nonlocality of quantum mechanics irrelevant. But no matter its exact formulation, the succeeding theory will have to agree with our experimental results; and as the empirical data by itself rules out a local explanation, any proper future candidate theory will have to be nonlocal as well. From this perspective, which we could call 'nonlocality-without quantum physics', we should consider all possible violations of Equation [1] not just the "$2+\sqrt{2} \not\leq 3$" violation of quantum mechanics. In this Letter we look at the plausibility of *superstrong nonlocality* where the nonlocal correlations are stronger than those allowed by the theory of quantum physics.

In a series of articles [12, 13, 14], Sandu Popescu and Daniel Rohrlich ask the question why Nature seems to allow a violation of the CHSH inequality with a correlation term of $2+\sqrt{2}$, but not with more. (See the article by Boris Cirel'son [5] for a proof that $2+\sqrt{2}$ is indeed the quantum mechanical limit.) They ask themselves [13]: "…Could the requirement of relativistic causality restrict the violation to $[2+\sqrt{2}]$ instead of 4?" Such a result would be great step towards a better understanding of Nature for "…If so, then nonlocality and causality would together determine the quantum violation of the CHSH inequality, and we would be closer to a proof that they determine all of quantum mechanics." Perhaps surprisingly, this turns out not to be the case. The authors prove this by constructing a toy-theory where the nonlocality Inequality [1] is surpassed by a correlation value of 4. The non-zero probabilities of this super-nonlocal theory are simply

$$\left.\begin{array}{l}\text{Prob}(m_x^A = 0, m_y^B = 0) = \frac{1}{2} \\ \text{Prob}(m_x^A = 1, m_y^B = 1) = \frac{1}{2}\end{array}\right\} \quad \text{if } xy \in \{00, 01, 10\},$$

$$\left.\begin{array}{l}\text{Prob}(m_1^A = 0, m_1^B = 1) = \frac{1}{2} \\ \text{Prob}(m_1^A = 1, m_1^B = 0) = \frac{1}{2}\end{array}\right\} \quad \text{if } xy = 11. \qquad (2)$$

This leads indeed to the maximally violating correlation value

$$\sum_{x,y\in\{0,1\}} \text{Prob}(m_x^A + m_y^B \equiv x \cdot y) \ = \ 4, \qquad (3)$$

while the randomization of the outcomes still prevents Alice or Bob from transferring information to the other party without the use of conventional communication. In fact, the probability distribution of Equation [2] is the only possible solution

Implausible Consequences of Superstrong Nonlocality

Wim van Dam*
Department of Computer Science, University of California at Santa Barbara, Santa Barbara, CA 93106-5110, USA

This Letter looks at the consequences of so-called 'superstrong nonlocal correlations', which are hypothetical violations of Bell/CHSH inequalities that are stronger than quantum mechanics allows, yet weak enough to prohibit faster-than-light communication. It is shown that the existence of maximally superstrong correlated bits implies that all distributed computations can be performed with a trivial amount of communication, i.e. with one bit. If one believes that Nature does not allow such a computational 'free lunch', then the result in the Letter gives a reason why superstrong correlation are indeed not possible.

PACS numbers: 03.65.Ud, 03.65.Ta, 03.67.Hk, 03.67.Mn
Keywords: foundations of quantum mechanics, nonlocality, communication complexity

Partial Answer (van Dam)

Some Boolean functions are nontrivial: they require more than one bit of classical communication

Some Boolean functions remain nontrivial with shared entanglement

Partial Answer (van Dam)

Some Boolean functions are nontrivial: they require more than one bit of classical communication

Some Boolean functions remain nontrivial with shared entanglement

All Boolean functions would become trivial were nonlocal boxes available!

New Axiom

New Axiom

Some Boolean functions have nontrivial communication complexity

New Axiom

Some Boolean functions have nontrivial communication complexity

Consequence

New Axiom

Some Boolean functions have nontrivial communication complexity

Consequence

Quantum mechanics cannot be maximally nonlocal among causal theories

Yes, but...

Yes, but...

This "explains" why quantum mechanics is not 100% nonlocal

Yes, but...

This "explains" why quantum mechanics is not 100% nonlocal

But why is it 85% nonlocal?

Yes, but...

This "explains" why quantum mechanics is not 100% nonlocal

But why is it 85% nonlocal?

Recall that classical mechanics is 75% nonlocal in this measure

Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial

Gilles Brassard,[1] Harry Buhrman,[2,3] Noah Linden,[4] André Allan Méthot,[1] Alain Tapp,[1] and Falk Unger[3]
[1]Département IRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal, Québec H3C 3J7, Canada
[2]ILLC, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
[3]Centrum voor Wiskunde en Informatica (CWI), Post Office Box 94079, 1090 GB Amsterdam, The Netherlands
[4]Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom
(Received 2 March 2006; published 27 June 2006)

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable, they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

DOI: 10.1103/PhysRevLett.96.250401 PACS numbers: 03.65.Ud, 03.67.Hk, 03.67.Mn

Entanglement can be harnessed to accomplish amazing information processing feats. The first proof that genuinely nonclassical behavior could be produced by quantum-mechanical devices was given by Bell, who proved that entanglement enables two spacelike separated parties to exhibit correlations that are stronger than anything allowed by classical physics [1]. Later, Clauser, Horne, Shimony, and Holt (CHSH), inspired by the work of Bell, proposed another inequality [2], which was easier to translate into a feasible experiment to test local hidden-variable theories. Their proposal fits nicely into the more modern framework of nonlocal boxes, introduced by Popescu and Rohrlich [[3], Eq. (7)].

A *nonlocal box* (NLB) is an imaginary device that has an input-output port at Alice's location and another one at Bob's, even though Alice and Bob can be spacelike separated. Whenever Alice feeds a bit x into her input port, she gets a uniformly distributed random output bit a, locally uncorrelated with anything else, including her own input bit. The same applies to Bob, whose input and output bits we call y and b, respectively. The "magic" appears in the form of a correlation between the pair of outputs and the pair of inputs: the exclusive OR (sum modulo two, denoted "$\oplus$") of the outputs is always equal to the logical AND of the inputs: $a \oplus b = x \wedge y$. Much like the correlations that can be established by use of quantum entanglement, this device is atemporal: Alice gets her output as soon as she feeds in her input, regardless of if and when Bob feeds in *his* input, and vice versa. Also inspired by entanglement, this is a *one-shot* device: the correlation appears only as a result of the first pair of inputs fed in by Alice and Bob. Of course, they can have more than one NLB at their disposal, which is then seen as a *resource* [4] of a different nature than entanglement [5].

NLBs cannot be used by Alice and Bob to signal instantaneously to one another. This is because the outputs that can be observed are purely random from a local perspective. In other words, NLBs are nonlocal, yet they are *causal*: they cannot make an effect precede its cause in the context of special relativity. We are interested in the question of how well the correlation of NLBs can be *approximated* by devices that follow the laws of physics.

Although originally presented differently, the CHSH inequality can be recast in terms of imperfect NLBs. The availability of shared entanglement allows Alice and Bob to approximate NLBs with success probability

$$\wp = \cos^2 \frac{\pi}{8} = \frac{2 + \sqrt{2}}{4} \approx 85.4\%.$$

This can be used to test local hidden-variable theories because it follows also from CHSH that no local realistic (classical) theory can succeed with probability greater than 3/4 if Alice and Bob are spacelike separated. Later, Tsirelson [6] proved the optimality of the CHSH inequality, which translates into saying that quantum mechanics does not allow for a success probability greater than $\wp$ at the game of simulating NLBs. See also Ref. [7] for an information-theoretic proof of the same result.

There are two questions of interest in this Letter: (1) Considering that perfect NLBs would not violate causality, why do the laws of quantum mechanics only allow us to implement NLBs better than anything classically possible, yet not perfectly? (2) Why do they provide us with an approximation of NLBs that succeeds with probability $\wp$ rather than something better?

Before we can pursue this line of thought further, we need to review briefly the field of *communication complexity* [8–11]. Assume Alice and Bob wish to compute some Boolean function $f(x, y)$ of input x, known to Alice only, and input y, known to Bob only. Their concern is to minimize the amount of communication required between them for Alice to learn the answer. It is clear that this task

PRL 96, 250401 (2006) PHYSICAL REVIEW LETTERS week ending 30 JUNE 200

Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial

Gilles Brassard,[1] Harry Buhrman,[2,3] Noah Linden,[4] André Allan Méthot,[1] Alain Tapp,[1] and Falk Unger[3]
[1]*Département IRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal, Québec H3C 3J7, Canada*
[2]*ILLC, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands*
[3]*Centrum voor Wiskunde en Informatica (CWI), Post Office Box 94079, 1090 GB Amsterdam, The Netherlands*
[4]*Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom*
(Received 2 March 2006; published 27 June 2006)

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable, they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

DOI: 10.1103/PhysRevLett.96.250401 PACS numbers: 03.65.Ud, 03.67.Hk, 03.67.Mn

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

Bell proved that quantum entanglement enables two spacelike separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable, they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

Probabilistic Definition

Probabilistic Definition

A Boolean function is *probabilistically computed* if its value can be guessed with probability at least p of being correct for some *constant* $p > 1/2$

Probabilistic Definition

A Boolean function is *probabilistically computed* if its value can be guessed with probability at least p of being correct for some *constant* $p > 1/2$

A Boolean function is probabilistically trivial if it can be probabilistically computed with *a single bit* of comm.

Probabilistic Theorems

Probabilistic Theorems

All Boolean functions can be computed with probability 1/2

Probabilistic Theorems

All Boolean functions can be computed with probability 1/2

All Boolean functions can be computed with probability larger than 1/2

Probabilistic Theorems

All Boolean functions can be computed with probability 1/2

All Boolean functions can be computed with probability larger than 1/2

WITHOUT ANY COMMUNICATION

Probabilistic Theorems

All Boolean functions can be computed with probability 1/2

All Boolean functions can be computed with probability larger than 1/2

Some Boolean functions are probabilistically nontrivial

Probabilistic Theorems

All Boolean functions can be computed with probability 1/2

All Boolean functions can be computed with probability larger than 1/2

Some Boolean functions are probabilistically nontrivial even if shared entanglement is available

BBLMTU Theorem

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *at least 75%*

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *at least 75%*

Of course not!
That would be classical

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *at least* $\frac{2+\sqrt{2}}{4} \approx 85\%$

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *at least* $\frac{2+\sqrt{2}}{4} \approx 85\%$

Of course not!
That would be quantum

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *better than* $\frac{2+\sqrt{2}}{4} \approx$ *85%*

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *better than* $\frac{2+\sqrt{2}}{4} \approx$ *85%*

Who knows?

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *better than* $\frac{2+\sqrt{2}}{4} \approx$ *85%*

Who knows?

THAT WOULD BE WONDERFUL!

BBLMTU Theorem

All Boolean functions would become probabilistically trivial were *imperfect* nonlocal boxes available, which work with probability *better than*

$$\frac{3+\sqrt{6}}{6} \approx 90.8\%$$

Vol 461 | 22 October 2009 | doi:10.1038/nature08400 nature

LETTERS

Information causality as a physical principle

Marcin Pawłowski[1], Tomasz Paterek[2], Dagomir Kaszlikowski[2], Valerio Scarani[2], Andreas Winter[2,3] & Marek Żukowski[1]

Quantum physics has remarkable distinguishing characteristics. For example, it gives only probabilistic predictions (non-determinism) and does not allow copying of unknown states (no-cloning[1]). Quantum correlations may be stronger than any classical ones[2], but information cannot be transmitted faster than light (no-signalling). However, these features do not uniquely define quantum physics. A broad class of theories exist that share such traits and allow even stronger (than quantum) correlations[3]. Here we introduce the principle of 'information causality' and show that it is respected by classical and quantum physics but violated by all no-signalling theories with stronger than (the strongest) quantum correlations. The principle relates to the amount of information that an observer (Bob) can gain about a data set belonging to another observer (Alice), the contents of which are completely unknown to him. Using all his local resources (which may be correlated with her resources) and allowing classical communication from her, the amount of information that Bob can recover is bounded by the information volume (m) of the communication. Namely, if Alice communicates m bits to Bob, the total information obtainable by Bob cannot be greater than m. For $m = 0$, information causality reduces to the standard no-signalling principle. However, no-signalling theories with maximally strong correlations would allow Bob access to all the data in any m-bit subset of the whole data set held by Alice. If only one bit is sent by Alice ($m = 1$), this is tantamount to Bob's being able to access the value of any single bit of Alice's data (but not all of them). Information causality may therefore help to distinguish physical theories from non-physical ones. We suggest that information causality—a generalization of the no-signalling condition—might be one of the foundational properties of nature.

Classical (as opposed to quantum) physics rests on the assumption that all physical quantities have well-defined values simultaneously. Relativity is based on clear-cut physical statements: the speed of light and the electric charge are the same for all observers. In contradistinction, the definition of quantum physics is still a description of its formalism: the theory in which systems are described by Hilbert spaces and dynamics is reversible. This situation is all the more unexpected because quantum physics is the most successful physical theory and quite a lot is known about it. Some of its counterintuitive features are almost popular knowledge: all scientists, and many laymen as well, know that quantum physics predicts only probabilities, that some physical quantities (such as position and momentum) cannot be simultaneously well defined and that the act of measurement generically modifies the state of the system. Entanglement and no-cloning are rapidly claiming their place in the list of well-known quantum features; in next place are the feats of quantum information such as the possibility of secure cryptography[4,5] or the teleportation of unknown states[6].

These features are so striking that one could hope that some of them provide the physical ground behind the formalism. Is quantum physics, for instance, the most general theory that allows violations of Bell inequalities, while satisfying no-signalling? When this question was investigated[3] the answer was found to be negative: impossibility of being represented in terms of local variables is a property shared by a broad class of no-signalling theories. Such theories predict intrinsic randomness, no-cloning[7,8] and an information-disturbance trade-off[9] and permit secure cryptography[9–12]. As regards teleportation and entanglement swapping[13], after a first negative attempt[14], it seems that they can also be defined within the general no-signalling framework[15,16]. In summary, most of the features that have been highlighted as 'typically quantum' are shared by all possible no-signalling theories. Only a few discrepancies have been noticed: some no-signalling theories would lead to an implausible simplification of distributed computational tasks[17,18] and would have very limited dynamics[19]. This highlights the importance of the no-signalling principle but leaves us still uncertain about the specificity of quantum theory.

Here we define and study a previously unnoticed feature, which we call 'information causality'. Information causality generalizes no-signalling and is respected by both classical and quantum physics. However, as we shall show, it is violated by all no-signalling theories that are endowed with correlations that are stronger than the strongest quantum correlations. It can therefore be used as a principle to distinguish physical theories from non-physical ones and is a good candidate for one of the foundational assumptions that are at the very root of quantum theory.

Formulated as a principle, information causality states: "the information gain that Bob can reach about a previously unknown to him data set of Alice, by using all his local resources and m classical bits communicated by Alice, is at most m bits". The standard no-signalling condition is just information causality for $m = 0$. The principle assumes classical communication: if quantum bits were allowed to be transmitted, the information gain could be higher, as demonstrated in the quantum super-dense coding protocol[20]. The efficiency of this protocol is based on the use of quantum entanglement, and information causality holds true even if the quantum bits are transmitted provided that they are disentangled from the systems of the receiver. This follows from the Holevo bound, which limits information gain after transmission of m such qubits to m classical bits.

We show that in a world in which certain tasks are 'too simple' (compare with refs 17, 18) and there exists implausible accessibility of remote data, information causality is violated. Consider a generic situation in which Alice has a database of N bits described by a string $\vec{a}$. She would like to grant Bob access to a big a portion of the database as possible within a fixed amount of classical communication. If there were no pre-established correlations between them, communication of m bits would open access to at most m bits of the database. With previously shared correlations they could expect to do better (however, as we show here, in the real world they would be mistaken). For concreteness, consider a generic task illustrated in Fig. 1. It is a

[1]Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland. [2]Centre for Quantum Technologies and Department of Physics, National University

Vol 461|22 October 2009|doi:10.1038/nature08400

natur

LETTERS

Information causality as a physical principle

Marcin Pawłowski[1], Tomasz Paterek[2], Dagomir Kaszlikowski[2], Valerio Scarani[2], Andreas Winter[2,3] & Marek Żukowski[1]

A derivation of quantum theory from physical requirements

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Markus P. Müller
Institute of Mathematics, Technical University of Berlin, 10623 Berlin, Germany, and
Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany
(Dated: October 5, 2010)

Quantum theory is derived from five requirements which are imposed on the framework of generalized probabilistic theories. These requirements are simple and have a clear physical meaning, in terms of basic operational procedures. They do not refer to the mathematical structure and representation of states and measurements.

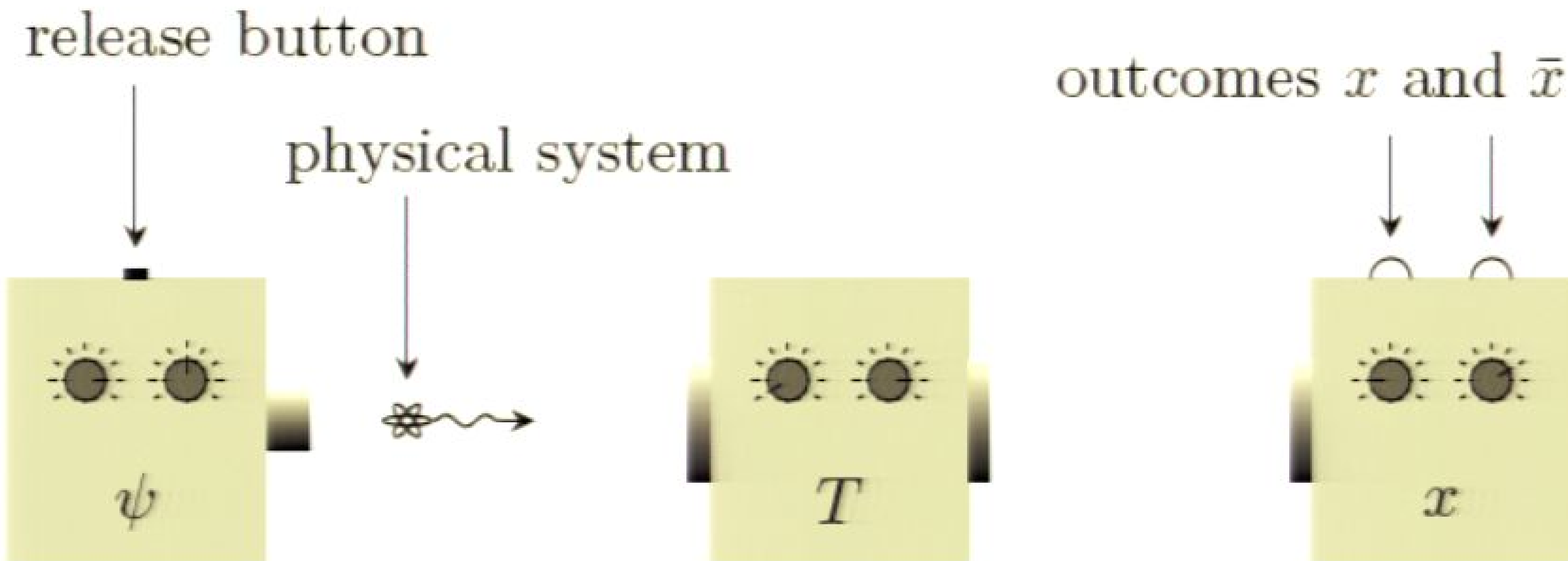


FIG. 1: This is a pictorial representation of a general experimental set up; with preparation, transformation and measurement devices (from left to right). As soon as the release button is pressed, the preparation device outputs a physical system in the state specified by the knobs. The next device performs the transformation specified by its knobs (which can be "do nothing"). The next device performs the measurement specified by its knobs, and the outcome (x or $\bar{x}$) is indicated by the corresponding light (on the top).

A derivation of quantum theory from physical requirements

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Markus P. Müller
Institute of Mathematics, Technical University of Berlin, 10623 Berlin, Germany, and
Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany

(Dated: October 5, 2010)

Quantum theory is derived from five requirements which are imposed on the framework of generalized probabilistic theories. These requirements are simple and have a clear physical meaning, in terms of basic operational procedures. They do not refer to the mathematical structure and representation of states and measurements.

I. INTRODUCTION

Quantum theory is usually formulated by postulating the mathematical structure and representation of states, measurements, and transformations. The general physical consequences that follow (possibility of local tomography, violation of Bell-type inequalities [1], factorization of integers in polynomial time [2], etc.) come as theorems which use the postulates as premises. In this work this procedure is reversed: we impose five simple physical requirements, and this suffices to single out quantum theory and derive its mathematical formalism uniquely. This is more similar to the usual formulation of Special Relativity, where two simple physical requirements are used to derive the mathematical structure of Minkowski space-time and its transformations.

The requirements can be schematically stated as:

1. In systems that carry one bit of information, each state is characterized by a finite set of outcome probabilities.

2. The state of a composite system is characterized by the statistics of measurements on the individual components.

3. All systems that effectively carry the same amount of information have equivalent state spaces.

4. Any pure state of a system can be reversibly transformed into any other.

5. In systems that carry one bit of information, all mathematically well-defined measurements are allowed by the theory.

These requirements are imposed on the framework of generalized probabilistic theories [3–5], which already assumes that some operational notions (preparation, mixture, measurement, and counting relative frequencies of measurement outcomes) make sense. Due to its conceptual simplicity, this framework leaves room for an infinitude of possible theories, allowing for weaker- or stronger-than-quantum non-locality [6, 10–14]. In this work, we show that quantum theory (QT) and classical probability theory (CPT) are very special among those theories: they are the only general probabilistic theories that satisfy the five requirements stated above. In addition, we show below that this claim may be reformulated in a way which makes Requirement 5 unnecessary.

The non-uniqueness of the solution is not a problem, since CPT is embedded in QT. One can also proceed as Hardy in [4]: if Requirement 4 is strengthened by imposing continuity of the reversible transformations, then CPT is ruled out and QT is the only theory satisfying the requirements. This strengthening can be justified by the continuity of time evolution in physical systems.

It is conceivable that in the future, another theory may replace or generalize QT. Such a theory must violate at least one of our assumptions. The clear meaning of our requirements allows to straightforwardly explore potential features of such a theory. The relaxation of each of the requirements constitutes a different way to go beyond QT. Most attempts to modify QT have been based on altering its mathematical formalism [15]. A derivation of QT in terms of physical requirements may provide a more transparent approach for this endeavor.

The search for alternative axiomatizations of QT is an old topic, which has been approached in many different ways: extending propositional logic [7, 8], using operational primitives [3–6, 9], searching for information-theoretic principles [5, 6, 10, 11, 16–18], building upon the phenomenon of quantum nonlocality [6, 10–13]. Alfsen and Shultz [19] have accomplished a complete characterization of the state spaces of QT from a geometric point of view, but the result does not seem to have an immediate physical meaning. In particular, the fact that the state space of a generalized bit is a three-dimensional ball is an assumption there, while here it is derived from physical requirements.

This work is particularly close to [4, 16], from where it takes some material. More concretely, the multiplicativity of capacities and the Simplicity Axiom from [4] are replaced by Requirement 5. In comparison with [16], the fact that each state of a generalized bit is the mixture of two distinguishable ones, the group of reversible transformations and its orthogonality, and the multiplicativity of capacities, are replaced by Requirement 5.

Summary of the paper. Section II contains an introduc-

Vol 461|22 October 2009|doi:10.1038/nature08400

natur

LETTERS

Information causality as a physical principle

Marcin Pawłowski[1], Tomasz Paterek[2], Dagomir Kaszlikowski[2], Valerio Scarani[2], Andreas Winter[2,3]
& Marek Żukowski[1]

A derivation of quantum theory from physical requirements

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Markus P. Müller
Institute of Mathematics, Technical University of Berlin, 10623 Berlin, Germany, and
Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany
(Dated: October 5, 2010)

Quantum theory is derived from five requirements which are imposed on the framework of generalized probabilistic theories. These requirements are simple and have a clear physical meaning, in terms of basic operational procedures. They do not refer to the mathematical structure and representation of states and measurements.

I. INTRODUCTION

Quantum theory is usually formulated by postulating the mathematical structure and representation of states, measurements, and transformations. The general physical consequences that follow (possibility of local tomography, violation of Bell-type inequalities [1], factorization of integers in polynomial time [2], etc.) come as theorems which use the postulates as premises. In this work this procedure is reversed: we impose five simple physical requirements, and this suffices to single out quantum theory and derive its mathematical formalism uniquely. This is more similar to the usual formulation of Special Relativity, where two simple physical requirements are used to derive the mathematical structure of Minkowski space-time and its transformations.

The requirements can be schematically stated as:

1. In systems that carry one bit of information, each state is characterized by a finite set of outcome probabilities.
2. The state of a composite system is characterized by the statistics of measurements on the individual components.
3. All systems that effectively carry the same amount of information have equivalent state spaces.
4. Any pure state of a system can be reversibly transformed into any other.
5. In systems that carry one bit of information, all mathematically well-defined measurements are allowed by the theory.

These requirements are imposed on the framework of generalized probabilistic theories [3–9], which already assumes that some operational notions (preparation, mixture, measurement, and counting relative frequencies of measurement outcomes) make sense. Due to its conceptual simplicity, this framework leaves room for an infinitude of possible theories, allowing for weaker- or stronger-than-quantum non-locality [6, 10–14]. In this work, we show that quantum theory (QT) and classical probability theory (CPT) are very special among those theories: they are the only general probabilistic theories that satisfy the five requirements stated above. In addition, we show below that this claim may be reformulated in a way which makes Requirement 5 unnecessary.

The non-uniqueness of the solution is not a problem, since CPT is embedded in QT. One can also proceed as Hardy in [4]: if Requirement 4 is strengthened by imposing continuity of the reversible transformations, then CPT is ruled out and QT is the only theory satisfying the requirements. This strengthening can be justified by the continuity of time evolution in physical systems.

It is conceivable that in the future, another theory may replace or generalize QT. Such a theory must violate at least one of our assumptions. The clear meaning of our requirements allows to straightforwardly explore potential features of such a theory. The relaxation of each of the requirements constitutes a different way to go beyond QT. Most attempts to modify QT have been based on altering its mathematical formalism [15]. A derivation of QT in terms of physical requirements may provide a more transparent approach for this endeavor.

The search for alternative axiomatizations of QT is an old topic, which has been approached in many different ways: extending propositional logic [7, 8], using operational primitives [3–6, 9], searching for information-theoretic principles [5, 6, 10, 11, 16–18], building upon the phenomenon of quantum nonlocality [6, 10–13]. Alfsen and Shultz [19] have accomplished a complete characterization of the state spaces of QT from a geometric point of view, but the result does not seem to have an immediate physical meaning. In particular, the fact that the state space of a generalized bit is a three-dimensional ball is an assumption there, while here it is derived from physical requirements.

This work is particularly close to [4, 16], from where it takes some material. More concretely, the multiplicativity of capacities and the Simplicity Axiom from [4] are replaced by Requirement 5. In comparison with [16], the fact that each state of a generalized bit is the mixture of two distinguishable ones, the group of reversible transformations and its orthogonality, and the multiplicativity of capacities, are replaced by Requirement 5.

Summary of the paper. Section II contains an introduc-

A derivation of quantum theory from physical requirements

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Markus P. Müller
Institute of Mathematics, Technical University of Berlin, 10623 Berlin, Germany, and
Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany
(Dated: October 5, 2010)

Quantum theory is derived from five requirements which are imposed on the framework of generalized probabilistic theories. These requirements are simple and have a clear physical meaning, in terms of basic operational procedures. They do not refer to the mathematical structure and representation of states and measurements.

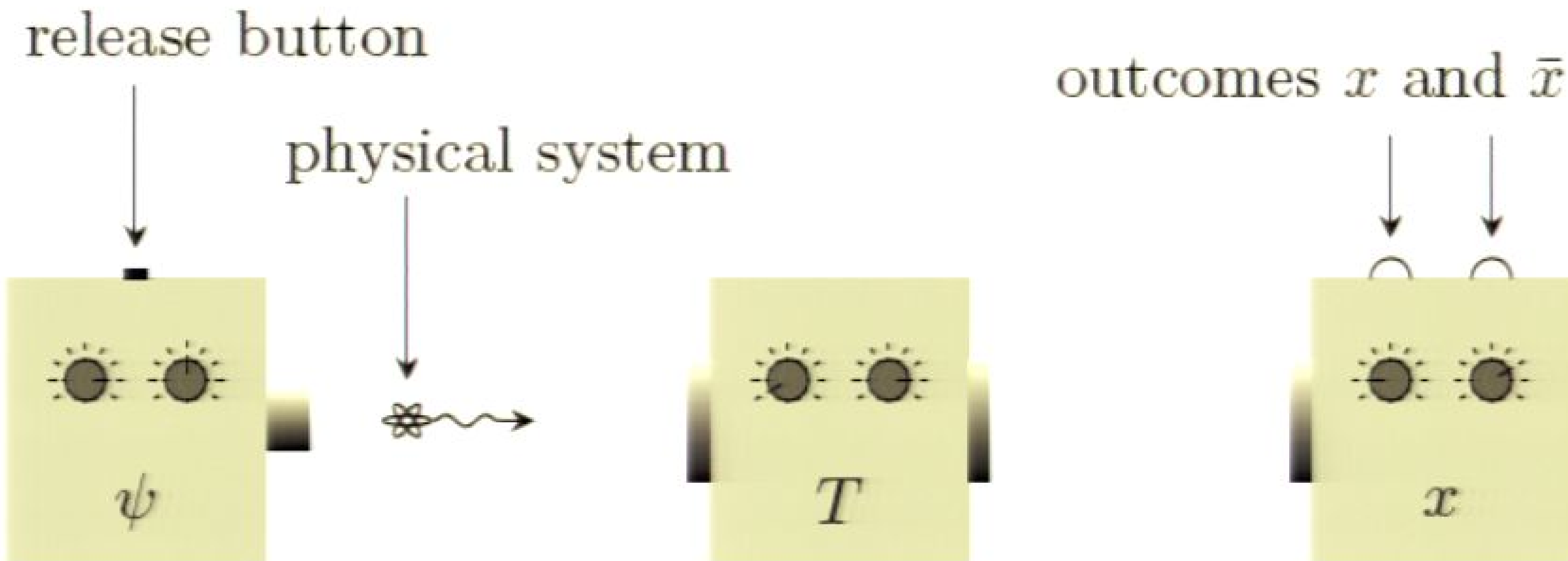


FIG. 1: This is a pictorial representation of a general experimental set up; with preparation, transformation and measurement devices (from left to right). As soon as the release button is pressed, the preparation device outputs a physical system in the state specified by the knobs. The next device performs the transformation specified by its knobs (which can be "do nothing"). The next device performs the measurement specified by its knobs, and the outcome (x or $\bar{x}$) is indicated by the corresponding light (on the top).

Four Requirements

- State spaces and subspaces with the same number of distinguishable states are equivalent.
- Any pure state can be reversibly transformed into any other.
- States of bipartite systems are fully characterized by correlations between local measurements.
- All mathematically well-defined measurements are allowed by the theory.

Informational derivation of Quantum Theory

Giulio Chiribella[*]
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Ontario, Canada N2L 2Y5.[†]

Giacomo Mauro D'Ariano[‡] and Paolo Perinotti[§]
QUIT Group, *Dipartimento di Fisica "A. Volta" and INFN Sezione di Pavia, via Bassi 6, 27100 Pavia, Italy*[¶]
(Dated: March 22, 2011)

We derive Quantum Theory from purely informational principles. Five elementary axioms—causality, perfect distinguishability, ideal compression, local distinguishability, and pure conditioning—define a broad class of theories of information-processing that can be regarded as standard. One postulate—purification—singles out quantum theory within this class.

PACS numbers: 03.67.-a, 03.67.Ac, 03.65.Ta

CONTENTS

I. INTRODUCTION

More than eighty years after its formulation, quantum theory is still mysterious. The theory has a solid mathe-

* gchiribella@perimeterinstitute.ca
† http://www.perimeterinstitute.ca
‡ dariano@unipv.it
§ paolo.perinotti@unipv.it
¶ http://www.qubit.it

Informational derivation of Quantum Theory

Giulio Chiribella[*]
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Ontario, Canada N2L 2Y5.[†]

Giacomo Mauro D'Ariano[‡] and Paolo Perinotti[§]
QUIT Group, *Dipartimento di Fisica "A. Volta" and INFN Sezione di Pavia, via Bassi 6, 27100 Pavia, Italy*[¶]
(Dated: March 22, 2011)

We derive Quantum Theory from purely informational principles. Five elementary axioms—causality, perfect distinguishability, ideal compression, local distinguishability, and pure conditioning—define a broad class of theories of information-processing that can be regarded as standard. One postulate—purification—singles out quantum theory within this class.

PACS numbers: 03.67.-a, 03.67.Ac, 03.65.Ta

- Causality
- Fine-grained composition
- Perfect distinguishability
- Ideal compression
- Local distinguishability

- Causality
- Fine-grained composition
- Perfect distinguishability
- Ideal compression
- Local distinguishability
- PURIFICATION POSTULATE

COMMENTARY

Is information the key?

GILLES BRASSARD

is in the Département d'informatique et de recherche opérationnelle, Université de Montréal, Québec H3C 3J7, Canada.

e-mail: brassard@iro.umontreal.ca

Quantum information science has brought us novel means of calculation and communication. But could its theorems hold the key to understanding the quantum world at its most profound level? Do the truly fundamental laws of nature concern — not waves and particles — but information?