QUANTUM INFORMATION

AND SPACETIME STRUCTURE

IGOR VOLOVICH

STEKLOV MATHEMATICAL INSTITUTE, MOSCOW

- QUANTUM COMPUTERS
- QUANTUM TELEPORTATION
- QUANTUM CRYPTOGRAPHY
- ENTANGLED STATES IN SPACETIME
- NONCOMMUTATIVE SPECTRAL THEORY
- BLACK HOLES AND QUANTUM TELEPORTATION
- QUANTUM PROBABILITY AND NONCOMMUTATIVE GEOMETRY

• LECTURES :

http://arxiv.org/abs/quant-ph/0203030

. . . . 0108133

. . . . 0109004

M. OHYA , I. V.

QUANTUM COMPUTER , TELEPORTATION, INFORMATION, CRYPTOGRAPHY .

SPRINGER , 2003

OXFORD, VIEN , MOSCOW, ...

IBM, MICROSOFT, ...

EXPERIMENTS , THEORY

QUANTUM INFORMATION TECHNOLOGY

GENERAL RELATIVTY
QUANTUM THEORY
} SUPERSTRINGS

- QUANTUM GRAVITY WITHOUT DIVERGENCES
- $D = 10 = 4 + 6$

- NEW INSIGHT INTO QUANTUM MECHANICS?
- NONCOMMUTATIVE GEOMETRY AND FIELD ~~THEORY~~?

ENTANGLED STATES

IN SPACE AND TIME

•

THEORY OF INFORMATION

CLASSICAL : C. SHANNON (1948)

GENERALIZATIONS:
KHINCHIN, KOLMOGOROV, GELFAND, YAGLOM,...

CLASSICAL INFORMATION THEORY =
= THEORY OF COMMUNICATIONS

COMPUTER SCIENCE, CRYPTOGRAPHY,...

QUANTUM INFORMATION THEORY:

QUANTUM COMMUNICATIONS,
QUANTUM COMPUTERS,
QUANTUM CRYPTOGRAPHY,
. . . .
WHOLE QUANTUM THEORY ?

THEORY OF INFORMATION (CLASSICAL, QUANTUM)
IN SPACE AND TIME
RELATIVISTIC THEORY

√ WHY QUANTUM INFORMATION?
(QUANTUM GRAVITY, SUPERSTRINGS,...)

CLASSICAL PROBABILITY.

$(\Omega, \mathcal{F}, P)$ PROBABILITY SPACE

KOLMOGOROV

Ω SET (ELEMENTARY EVENTS ;

"HIDDEN VARIABLES")

$\mathcal{F}$ – σ– ALGEBRA OF SUBSETS Ω

(EVENTS)

- $\phi, \Omega \in \mathcal{F}$
- $A_n \in \mathcal{F} \Rightarrow \bigcup_n A_n \in \mathcal{F}$
- $A \in \mathcal{F} \Rightarrow \Omega \setminus A \in \mathcal{F}$

$(\Omega, \mathcal{F})$ MEASURABLE SPACE

P - MEASURE ; $P : \mathcal{F} \to [0,1]$

$P(\Omega) = 1.$ $P(\sum_n A_n) = \sum_n P(A_n)$

$P(A)$, $A \in \mathcal{F}$ PROBABILITY OF EVENT A

$$P(A|B) = \frac{P(AB)}{P(B)}$$ CONDITIONAL PROBABILITY

$\xi : \Omega \to \mathbb{R}$ RANDOM VARIABLE

$\xi = \xi(\omega)$

$$E\xi = \int_\Omega \xi(\omega)\, dP(\omega)$$

EXPECTATION OF ξ

$\xi_t : \Omega \to \mathbb{R}$ RANDOM PROCESS

$\xi_t = \xi_t(\omega)$

ALGEBRAIC FORMULATION

$\mathcal{A} = L^\infty(\Omega)$ ALGEBRA OF BOUNDED FUNCTIONS ON Ω

$a \in \mathcal{A}$, $a : \Omega \to \mathbb{C}$, $a = a(\omega)$

$\varphi(a) = Ea$; $\varphi(a^* a) \geq 0$, $\varphi(1) = 1$

LINEAR POSITIVE FUNCTIONAL : STATE

$(\mathcal{A}, \varphi) \longleftrightarrow (\Omega, \mathcal{F}, P)$

$\mathcal{A}$ - COMMUTATIVE ALGEBRA

QUANTUM PROBABILITY

$(\mathcal{A}, \varphi)$ QUANTUM PROBABILITY SPACE

$\mathcal{A}$ $*$-ALGEBRA, φ - STATE

$a \in \mathcal{A}$ RANDOM VARIABLE

$\varphi(a)$ EXPECTATION OF a

(COMPARE NONCOMMUTATIVE GEOMETRY)

EXAMPLE.

$\mathcal{H}$ HILBERT SPACE

$\mathcal{A}$ ALGEBRA OF BOUNDED OPERATORS

$\varphi(a) = Tr(\rho a)$; $\rho \geq 0$, $\rho^* = \rho$,

$Tr\, \rho = 1$

ρ DENSITY OPERATOR

(NOT ALWAYS)

L. ACCARDI, Yu. G. LU, I. V.
"QUANTUM THEORY AND ITS STOCHASTIC LIMIT"
SPRINGER, 2002

PRINCIPLES OF QUANTUM THEORY

I. PHYSICAL SYSTEM $\rightarrow$ HILBERT SPACE $\mathcal{H}$

OBSERVABLES $\rightarrow$ HERMITEAN OPERATORS

STATES $\rightarrow \varphi$; DENSITY OPERATORS (FINITE SYSTEMS)

SUPERSELECTION RULES

$\mathbb{C}^2$ -QUBIT

II. DYNAMICS $\qquad \psi \rightarrow U_t \psi$, $\psi \in \mathcal{H}$

U_t GROUP OF UNITARY OPERATORS

$t \in R$, $t \in Z$

$\varphi \rightarrow \varphi_t$

Schrödinger eq. $\quad i \frac{\partial \psi_t}{\partial t} = H \psi_t$

(NOT ALWAYS)

III. MEASUREMENTS.

$(\mathcal{B}, \Sigma)$ MEASURABLE SPACE

POVM $\{X_B\}$, $B \in \Sigma$; X_B OPERATOR IN $\mathcal{H}$

$X_B^* = X_B$, $X_B \geq 0$; $X_B = \sum_n X_{B_n}$,

$X_\Omega = 1$, $\qquad B = \bigcup_n B_n$, $B_n \cap B_m = \emptyset$

$\underline{Pr(B) = \varphi(\chi_B)}$ - PROBABILITY MEASURE ON $(\mathcal{B}, \Sigma)$.

PROBABILITY OF THE EVENT THAT THE RESULT OF MEASUREMENT BELONGS TO $\mathcal{B}$.

EXAMPLE: $A\varphi_i = \lambda_i \varphi_i$; $\psi = \sum_i c_i \varphi_i$

$\mathcal{B} = \{i\}$ $\quad Pr(i) = |\langle \psi | \varphi_i \rangle|^2 = |c_i|^2$

- $\varphi \to \mathcal{T}_B \varphi$ $\quad$ NONRELATIVISTIC **REDUCTION (COLLAPSE) OF STATE** (DIRAC, VON NEUMANN)

EXAMPLE. $A = \sum_i \lambda_i E_i$

DENSITY OPERATOR

$$\underline{\rho \to \Phi(\rho) = E_i \rho E_i / \mathrm{Tr} E_i \rho}$$

(QUANTUM CHANNEL)

MORE GENERAL QUANTUM CHANNEL:

$$\underline{\rho \to \Phi(\rho) = \sum_k V_k \rho V_k^*}, \quad \sum_k V_k^* V_k \le I$$

CP-MAP $\quad V_k(G)$?

KRAUS REPRESENTATION

IV. COMPOSITE SYSTEMS

$$\mathcal{H}_1,\ \mathcal{H}_2\ ;\quad \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

$$\psi = \sum_k \psi_k^{(1)} \otimes \psi_k^{(2)}$$ ENTANGLED STATE (NOT FACTORIZED)

V. BOSE, FERMI STATISTICS

VI. SPACE-TIME EXISTS.

M^4 MINKOWSKI SPACETIME

- $U(a, \Lambda)$ UNITARY REPRESENTATION OF POINCARE GROUP

SPECTRAL CONDITION

- $\mathcal{A}(\mathcal{O})$, $\mathcal{O} \subset M^4$ FAMILY OF ALGEBRAS OBSERVABLE IN $\mathcal{O}$.

M^{10} SUPERSTRINGS.	

VII. QFT IS A LOCAL THEORY

STRINGS.

VIII. NONCOMMUTATIVE SPECTRAL REPRESENTATION FOR LOCAL OBSERVABLES.

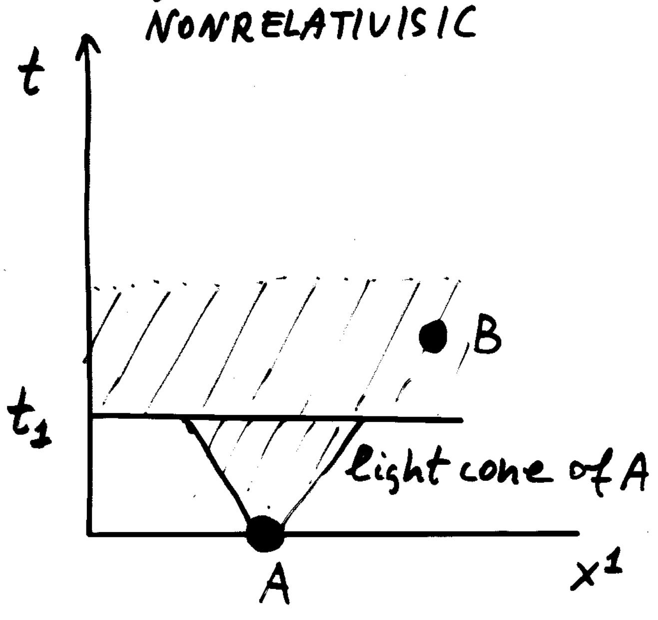
(?)

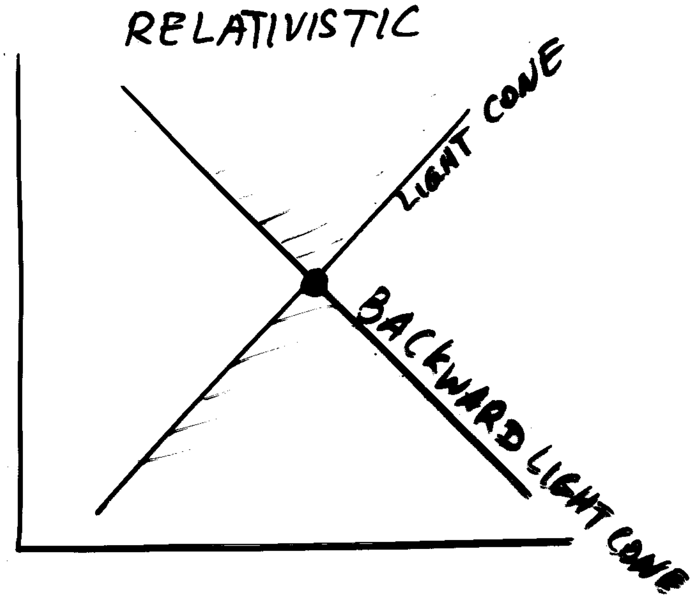
III'. STATE REDUCTION (COLLAPSE)

NONRELATIVISTIC THEORY. von Neumann, Dirac.

As a consequence of the measurement the state undergoes an instantaneous change, a discontinuous quantum jump.

Relativistic THEORY. Landau, Peierls, Bohr, Rosenfeld, Hellwig, Kraus, Aharonov, Albert, S. Mayburov, I.V, ..





LANDAUER: INFORMATION IS PHYSICAL.

RELATIVISTIC QUANTUM INFORMATION THEORY:

- QUBIT $\mathbb{C}^2$ $\Longrightarrow$ [m, s] IRREPS OF POINCARE GR.

QUANTUM COMPUTING
and
SHOR'S FACTORING ALGORITHM

Igor V. Volovich

Steklov Mathematical Institute, Moscow

- **Algorithms**
- **Quantum Circuits**
- **Quantum Fourier Transform**
- **Elements of Number Theory**
- **Modular Exponentiation**
- **Shor's Algorithm for Finding the Order**
- **Computational Complexity of Shor's Algorithm**
- **Factoring Integers**

HISTORY OF QC

IVANENKO, WHEELER, MANIN, ...
QUANTUM GRAVITY
UNIVERSE IS QUANTUM COMPUTER

~1980 FEYNMAN, BENIOFF, DEUTSCH

~1995 SHOR, GROVER, ...
EXPERIMENTAL QC
OHYA, WATANABE, ...

QUANTUM COMPUTER IS A COMPUTER WHICH USES THE LAWS OF QUANTUM MECHANICS AND QUANTUM LOGIC.

MOTIVATIONS:
- MINIATURIZATION
- QC MORE POWERFUL
- SCIENCE

DEFINITION:

QUANTUM COMPUTER = QUANTUM TURING MACHINE

= UNIFORM FAMILY OF QUANTUM CIRCUITS

GREECE, ...
TURING, GÖDEL, KOLMOGOROV, ...

CLASSICAL COMPUTER	QUANTUM COMPUTER
BIT $\{0,1\}$	QUBIT $\mathbb{C}^2$
CLASSICAL LOGIC: AND, OR, NOT	QUANTUM LOGIC: ... $\sqrt{NOT}$.

COMPUTABLE NUMBERS
RATIONAL NUMBERS
p-ADIC NUMBERS (B. DRAGOVICH, ...)

1 Introduction

Introduction to quantum computing and number theory is given. Shor's algorithm for factoring integers is described.

Factoring problem.

Every integer N is uniquely decomposable into a product of prime numbers:
$6 = 2 \cdot 3,\ 35 = 5 \cdot 7, \ldots$

However we do not know *efficient* (i.e. polynomial in the number of operations) classical algorithms for factoring.

Given a large integer N, one has to find efficiently such integers p and q that

$$N = pq$$

An algorithm of factoring the number N is efficient if the number of elementary arithmetical operations which it uses for large N is bounded by a polynomial in n where $n = \log N$ is the number of digits in N.

The most naive factoring method: just divide N by each number from 1 to $\sqrt{N}$.

This requires at least $\sqrt{N}$ operations. Since

$$\sqrt{N} = 2^{\frac{1}{2}\log N}$$

is exponential in the number of digits $n = \log N$ in N this method is not an efficient algorithm.

There is no known efficient classical algorithm for factoring but the quantum polynomial algorithm does exist.

The best classical factoring algorithm is the number field sieve:

$$\exp(cn^{1/3}(\log n)^{2/3})$$

P. Shor has found a quantum algorithm which takes

$$O(n^2 \log n \log\log n)$$

operations.

Factorization of N can be reduced to finding the *order* of an arbitrary element m in the multiplicative group of residues modulo N;

that is the least integer r such that

$$m^r \equiv 1 \pmod{N}$$

To factorize N it is enough to find the order r of m.

Shor's algorithm for finding the order consists of 5 steps:

1. Preparation of quantum state.
2. Modular exponentiation.
3. Quantum Fourier transform.
4. Measurement.
5. Computation of the order at the classical computer.

2 Algorithms

Algorithm is a precise formulation of doing something.

Euclid's algorithm for finding the greatest common divisor of two numbers.

Euclid's algorithm. Given two positive integers m and n, find their greatest common divisor, i.e. the largest positive integer which divides both m and n. Here m and n are interpreted as variables which can take specific values. $m > n$

1. Divide m by n and let r be the remainder.

2. If $r = 0$, the algorithm halts; n is the answer.

3. Replace the value of variable m by the current value of variable n, also replace the value of variable n by the current value of variable r and go back to Step 1.

Input is : m and n.

Output: n in Step 2, which is the greatest common divisor of two given integers.

Exercise. Prove that the output of Euclid's algorithm is indeed the greatest common divisor.

Hint: After Step 1, we have $m = kn + r$, for some integer k.

Classical and quantum algorithms.

Turing machines. Circuits.

Classical circuits and classical Turing machines are mathematical models of classical computer.

Quantum circuits and quantum Turing machines are mathematical models of quantum computer. D. Deutsch (1985).

General Notion of Algorithm.

Two sets I and O. I - input, O - output.

$$I,\ O \subseteq \mathsf{S}$$

Gates. $G = \{g_1, \ldots, g_r\}$, $g_i : \mathsf{S} \to \mathsf{S}$.

Example: logical operations AND, OR and NOT.

$$f : I \to O.$$

Problem: To find a sequence of gates $A = \{g_{i_1}, g_{i_2}, \ldots, g_{i_k}\}$ which computes the function f.

$$f(x) = g_{i_1} g_{i_2} \ldots g_{i_k}(x), \quad x \in I$$

A is the *algorithm*.

Computational sequence, $x_0, x_1, \ldots : x_0 = x$, $x_1 = g_{i_1}(x_0), \ldots, x_m = g_{i_m}(x_{m-1}), \ldots$.

Computational sequence terminates in k steps if k is the smallest integer for which x_k is in O. In this case it produces the output $y = x_k$ from x.

More general approach: functions g_i and f are not defined everywhere, not every computational sequence terminates. Moreover, the transition $x_m = g_{i_m}(x_{m-1})$ takes place with a certain probability (random walk) and the output space O is a metric space with a metric ρ.

An algorithm makes an approximate computation of a function $f(x)$ with a certain probability if one gets a bound $\rho(f(x), x_k) < \varepsilon$.

The algorithm for the computation of the function f by using the prescribed set of gates is given by the data

$$\{S, I, O, G, A, f\}$$

The set S for the classical Turing machine: all configurations of the Turing machine, the gates g_i form the transition function. For a classical circuit the gates: logical operations AND, OR and NOT. For quantum circuit and for quantum Turing machine the set S: the Hilbert space of quantum states, the gates g_i : some unitary matrices and projection operators.

Computational complexity.

For input x let $t(x) = k$ be the number of steps until the computational sequence terminates. The computational time T

$$T(n) = \max_x \{t(x) :| x |= n\}$$

where $| x |$ is the length of the description of x.

For input x let $s(x)$ be the number of different elements in the computational sequence $x_0 = x, x_1, ...$ The computational space S :

$$S(n) = \max_x \{s(x) : s(x) = n\}$$

3 Quantum Circuits

Quantum Mechanics.

- Quantum mechanics is a statistical theory.
- Every quantum system assigns a Hilbert space.

Vectors in the Hilbert space represent states of the quantum system, self-adjoint operators represent observables.

$\mathbb{C}^n$ with the scalar product

$$(z, w) = \sum_{i=1}^{n} \bar{z}_i w_i$$

Probability to observe the state ψ given the state ϕ is $|(\psi, \phi)|^2$.

Boolean Functions.

Quantum circuits are quantum analogues of the classical circuits computing Boolean functions.

$$B = \{0, 1\}$$

$$f : B^n \to B^m$$

CLASSICAL CIRCUIT

$G = \{f_1, \dots, f_r\}$, $\quad f_i : B^{k_i} \to B^{d_i}$

Gates (NOT, OR, AND)

$$F(x_1, \dots, x_n) = f_{i_1}^{(\alpha_1)} \circ \dots \circ f_{i_M}^{(\alpha_M)} (x_1, \dots, x_n)$$

$M = M(n)$ TIME COMPLEXITY

QUANTUM CIRCUIT

$\{\mathcal{H}, G, U\}$, $\quad G = \{V_1, \dots, V_r\}$

$$U = V_{i_1}^{(\alpha_1)} \dots V_{i_L}^{(\alpha_L)}$$

$L = L(n)$ TIME COMPLEXITY

A classical circuit can be represented as a directed acyclic graph.

A quantum circuit is a sequence of unitary matrices of the special form associated with a (hyper)graph.

Computational basis in $n-$ qubit space.

$\mathbb{C}^2$ *qubit.*

Computational basis

$$e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The index $x = 0, 1$ in the basis (e_x) is interpreted as a Boolean variable. Dirac notations

$$e_x = \mid x > .$$

$\mathbf{C}^2 \otimes \mathbf{C}^2 ... \otimes \mathbf{C}^2 = \mathbf{C}^{2^n}$ is the $n-$ qubit space.

Computational basis $\{e_{x_1} \otimes e_{x_2} \otimes ... \otimes e_{x_n}\}$ where $x_i = 0, 1$.

$$e_{x_1} \otimes e_{x_2} \otimes ... \otimes e_{x_n} = \mid x_1, ..., x_n > .$$

If ψ is a vector of the unit length in $\mathbb{C}^{2^n}$ then the probability to observe the Boolean variables $x_1, ..., x_n$ in the state ψ is

$$|(e_{x_1} \otimes e_{x_2} \otimes ... \otimes e_{x_n}, \psi)|^2$$

$$| < x_n, ..., x_1 \mid \psi > |^2.$$

Definition. *A quantum circuit* Q is defined by the following set of data:

$$Q = \{\mathcal{H}, U, G, f\}$$

where the Hilbert space $\mathcal{H}$ is the $n-$ qubit space $\mathcal{H} = \mathbb{C}^{2^n}$, U is a unitary matrix in $\mathcal{H}$, $G = \{V_1, ..., V_r\}$ is a finite set of unitary matrices (quantum gates) and f is a classical Boolean function $f : B^k \to B^m$. Here $B = \{0, 1\}$ and one assumes $k \leq n$ and $m \leq n$. The matrix U should admit a representation as a product of unitary matrices generated by the quantum gates.

The dimension of unitary matrices V_i normally is less then 2^n and usually one takes matrices V_i which act in the $2-$ or in $3-$ qubit spaces.

Fix the computational basis $\{e_{x_1} \otimes e_{x_2} \otimes ... \otimes e_{x_n}\}$ in $\mathcal{H}$. Define an extension of the matrix V_i to a matrix in the space $\mathcal{H}$.

If V_i is an $l \times l$ matrix then we choose l vectors from the computational basis and denote them as $\alpha = \{h_1, ..., h_l\}$. Define a unitary transformation $V_i^{(\alpha)}$ in $\mathcal{H}$. The action of $V_i^{(\alpha)}$ on the subspace of $\mathcal{H}$ spanned by vectors $\{h_1, ..., h_l\}$ equals to V_i, the action of $V_i^{(\alpha)}$ on the orthogonal subspace equals to ~~0~~ 1.

$$U = V_{i_1}^{(\alpha_1)} V_{i_2}^{(\alpha_2)} ... V_{i_L}^{(\alpha_L)} \tag{1}$$

Quantum Gates.

$$G = \{V_1, V_2\}$$

V_1 is the 2×2 matrix of rotations to an irrational angle θ

V_2 is the 4×4 matrix acting to the basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$ as $(x, y = 0, 1)$

$$V_2 |x, y> = |x, x + y \pmod 2>$$

The matrix V_2 is the CNOT-operation. The matrices V_1 and V_2 gives an example of universal quantum gates. By using these gates one can construct a unitary matrix of the form (1) which is close as we wish to any unitary matrix in $\mathbb{C}^{2^n}$.

Exercise. Let $S_\theta = \{e^{2\pi i\theta n}\}$ be a set of points on the unit circle. Here θ is a fixed irrational number and $n = 0, \pm 1, \pm 2, ...$ Prove that the set S_θ is a dense set on the unit circle.

Quantum circuit Q computes the Boolean function $f : B^k \to B^m$ if the following bound is valid

$$|< 0, f(x_1, ..., x_k) \mid U \mid x_1, ..., x_k, 0 >|^2 \geq 1 - \varepsilon$$

for all $x_1, ..., x_{k_1}$ and some fixed $0 \leq \varepsilon < 1/2$.

L is the *computational time* of the quantum circuit.

Families of quantum circuits. The computational power of a family of quantum circuits should be equivalent to quantum Turing machine.

Requirement of *uniformity.* A family of quantum circuits is called uniform if its design is produced by a polynomial time classical computer and if the entries in the unitary matrices of the quantum circuits are computable numbers.

4 Quantum Fourier Transform

$\mathbb{C}^2 \otimes \mathbb{C}^2 ... \otimes \mathbb{C}^2 = \mathbb{C}^{2^s}$

Quantum Fourier transform $(q = 2^s)$:

$$F_q|a> = \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} e^{2\pi iab/q}|b>$$

$$|a> = |a_{s-1}, ..., a_0>, \quad |b> = |b_{s-1}, ..., b_0>$$

Binary representations

$$a = a_0 + a_1 2 + ... + a_{s-1}2^{s-1}, \quad a_i = 0, 1$$

$$b = b_0 + b_1 2 + ... + b_{s-1}2^{s-1}, \quad b_i = 0, 1$$

Example. Hadamard's Gate.

For $L = 1$ the quantum Fourier transform is the *Hadamard gate*, $F_2 = H$.

$$H|0> = \frac{1}{\sqrt{2}}(|0> + |1>),$$

$$H|1> = \frac{1}{\sqrt{2}}(|0> - |1>).$$

The Hadamard gate to the s-qubit space as

$$H_j = I \otimes ... \otimes H \otimes ... \otimes I, \quad j = 1, 2, ..., s.$$

The quantum Fourier transform is multiplication by an $q \times q$ unitary matrix, where the x, y matrix element is $e^{2\pi i x y/q}$. Naively, $O(q^2)$ elementary operations. However, it can be implemented by means only $O((\log q)^2)$ elementary operations.

Important factorized (unentangled) form:

$$F_{2^s}|a_{s-1}, ..., a_0 > = \frac{1}{\sqrt{2^s}}(|0> + e^{i\phi_a 2^{s-1}}|1>)$$

$$\otimes(|0> + e^{i\phi_a 2^{s-2}}|1>) \otimes ... \otimes (|0> + e^{i\phi_a}|1>)$$

where $\phi_a = 2\pi a/2^s$.

Quantum Fourier transform can be written as a product of matrices generated by Hadamard's gates and 4×4 matrix B,

$$B|a_1, a_0> = \begin{cases} e^{i\pi/2}|a_1, a_0>, & \text{if } a_1 = a_0 = 1, \\ |a_1, a_0>, & \text{otherwise.} \end{cases}$$

$$B_{j,k}|a_{s-1}, \ldots, a_k, \ldots, a_j, \ldots, a_0>$$
$$= e^{i\theta_{k-j}}|a_{s-1}, \ldots, a_k, \ldots, a_j, \ldots, a_0>$$

where

$$e^{i\theta_{k-j}} = \begin{cases} (e^{i\pi/2})^{(k-j)}, & \text{if } a_1 = a_0 = 1, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 4.1. Quantum Fourier transform in the space $\mathbb{C}^{2^s}$ can be represented as a product of $O(s^2)$ operators H_j and $B_{j,k}$.

Therefore there is a quantum algorithm for implementation of quantum Fourier transform which is polynomial as the function of the input size.

EINSTEIN-PODOLSKY-ROSEN PARADOX

„ANYBODY WHO IS NOT SHOCKED BY QUANTUM THEORY HAS NOT UNDERSTOOD IT'

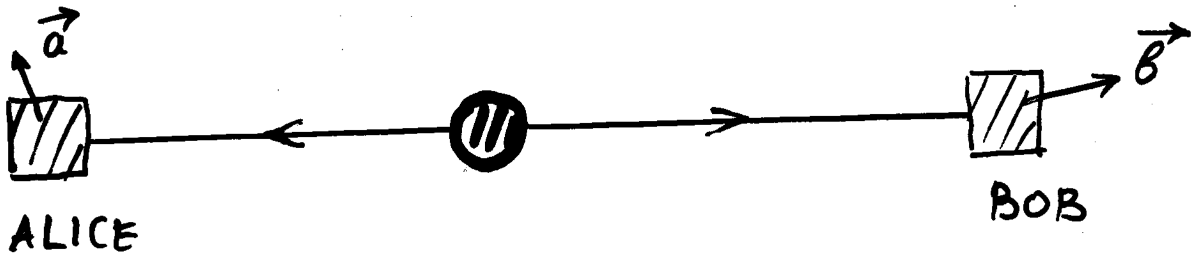
NIELS BOHR

REALITY (LOCAL REALISM)

EPR : „IF, WITHOUT DISTURBING A SYSTEM, ONE CAN PREDICT WITH CERTAINTY THE VALUE OF A PHYSICAL QUANTITY THEN THERE EXISTS AN ELEMENT OF PHYSICAL REALITY ASSOCIATED WITH THE QUANTITY"

EPR PAIRS

PREPARE A PAIR OF SPIN 1/2 PARTICLES FORMED IN THE SINGLET SPIN STATE $|\Psi_0\rangle$ AND MOVING FREELY IN OPPOSITE DIRECTIONS (EPR PAIR, BOHM)



$$\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$$

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right] =$$

$$= \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right)$$

ENTANGLED STATE

SPIN. PAULI MATRICES:

$$\underset{x}{\sigma_1} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \quad \underset{y}{\sigma_2} = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}, \quad \underset{z}{\sigma_3} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$$

$$\sigma_z = (+1)\,E^{(+)} + (-1)\,E^{(-)}$$

SPECTRAL REPRESENTATION

$$E^{(+)} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad E^{(-)} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

MEASUREMENT (ALICE) $E^{(+)}$ projection

REDUCTION (COLLAPSE) OF WAVE FUNCTION

$$|\Psi_0\rangle \rightarrow \left(E^{(+)} \otimes 1\right) |\Psi_0\rangle = \frac{1}{\sqrt{2}}\, |10\rangle$$

MEASUREMENT (BOB)

$$|10\rangle \rightarrow \left(1 \otimes E^{(+)}\right) |10\rangle = 0$$

$$\left(|10\rangle \rightarrow \left(1 \otimes E^{(-)}\right) |10\rangle = |10\rangle\right)$$

ALICE BOB

$\sigma_z \to +1 \quad \Longrightarrow \quad \sigma_z \to -1$

$\sigma_z \to -1 \quad \Longrightarrow \quad \sigma_z \to +1$

$\sigma_x \to +1 \quad \Longrightarrow \quad \sigma_x \to -1$

$\sigma_x \to -1 \quad \Longrightarrow \quad \sigma_x \to +1$

PARADOX. ALICE CAN CHOOSE BETWEEN $z, x, \ldots$ SHE COULD INFLUENCE BOB'S SPIN STATE.
MOREOVER σ_z AND σ_x DO NOT COMMUTE.

EPR : QM IS NOT COMPETE.

MOST PHYSICISTS DID NOT ACCEPT THIS REASONING.

J. BELL (1964)

WHERE IS SPACE TIME / MOMENTUM ?
IN THIS CONSIDERATION

QUANTUM TELEPORTATION

PROCEDURE FOR MOVING QUANTUM STATES AROUND.

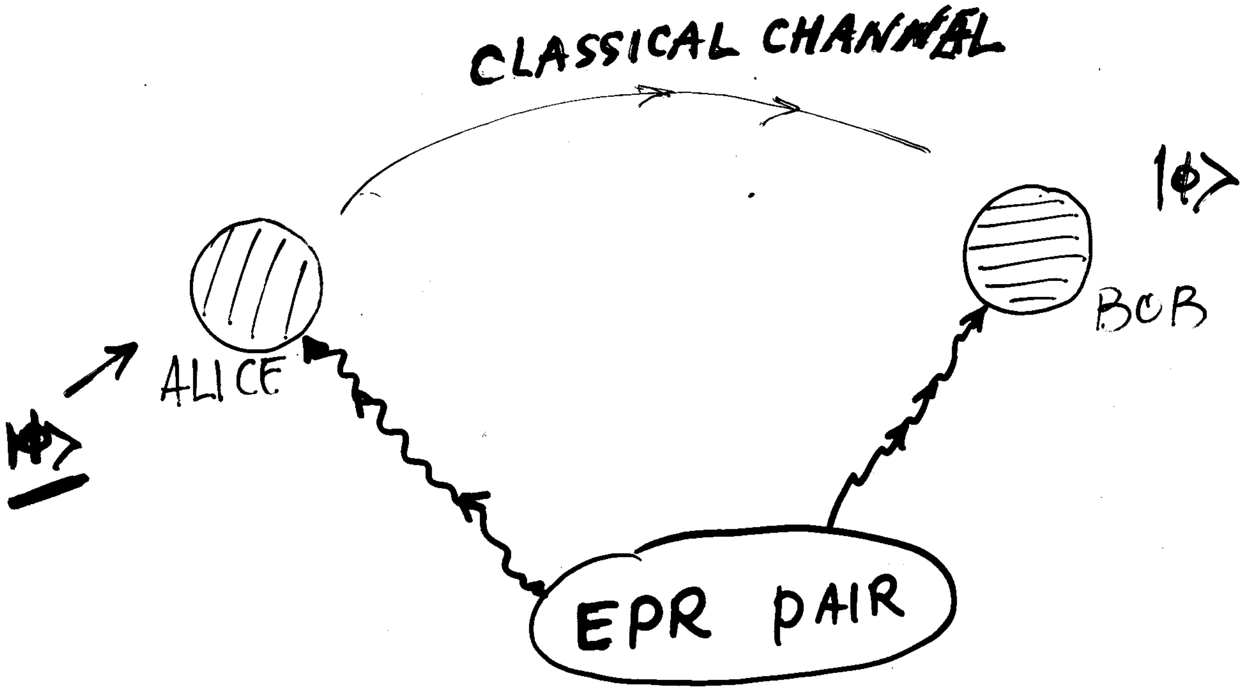
ONE MOVES AN UNKNOWN STATE :
NO CLONING THEOREM

EXPERIMENTS : ROME , GENEVE, ...

Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters (1993)

„TELEPORTING AN UNKNOWN QUANTUM STATE VIA DUAL CLASSICAL AND EPR CHANNELS"

QUANTUM TELEPORTATION



ALICE : BELL'S BASIS MEASUREMENT

SPACE PART OF WAVE FUNCTION

BLACK HOLE. HORIZON.

EPR-PARADOX FOR BLACK HOLES.

QUANTUM TELEPORTATION FROM BLACK HOLE?

QUANTUM NONLOCALITY.

$$\mathcal{H} = \underbrace{\mathbb{C}^2_{A_1} \otimes \mathbb{C}^2_{A_2}}_{\text{ALICE}} \otimes \underbrace{\mathbb{C}^2_{B}}_{\text{BOB}}$$

TH. IF

$$|\phi\rangle = a|0\rangle + b|1\rangle \in \mathbb{C}^2_{A_1}$$

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_{A_2} \otimes |0\rangle_B - |0\rangle_{A_2} \otimes |1\rangle_B\right) \in \mathbb{C}^2_{A_2} \otimes \mathbb{C}^2_B$$

THEN

$$\underset{a,b}{|\phi\rangle} \otimes |\psi_{AB}\rangle = \sum_{i=1}^{4} g_i \otimes f_i(a,b)$$

WHERE

$$g_i \in \mathbb{C}^2_{A_1} \otimes \mathbb{C}^2_{A_2}$$ Bell basis

$$f_i(a,b) \in \mathbb{C}^2_B$$

$$|\psi_{AB}\rangle = |\psi_0\rangle = |\psi_{SPIN}\rangle$$

Black Holes, Information, Coherence

Wheeler, Hawking, 't Hooft, Susskind, Strominger,...

Hawking: Black holes and quantum mechanics cannot coexist.
Black holes swallow information and then dissapear without releasing it.

Compare: EPR-paradox. Entangled states. Bell's theorem.

- Quantum Information in Space and Time

••• QUANTUM TELEPORTATION AND BLACK HOLE COHERENCE/INFORMATION LOSS

Bell's Theorem (1964)

$$\boxed{\cos(t-s) \neq E x_t y_s}$$

if $x_t = x_t(\omega)$, $y_s = y_s(\omega)$ stochastic processes such that

$$|x_t(\omega)| \leq 1, \quad |y_s(\omega)| \leq 1.$$

Bell's theorem states that some quantum correlations can not be represented by classical correlations of separated random variables. It has been interpreted as incompatibility of the requirement of locality with quantum mechanics.

(Ω, Σ, P) - **Probability Space**

$$\cos(t-s) \neq \int_\Omega x_t(\omega) y_s(\omega) dP(\omega)$$

if

$$|x_t(\omega)| \leq 1, \quad |y_s(\omega)| \leq 1.$$

Theorem

If f_1, f_2, g_1, g_2 random variables on (Ω, Σ, P) such that

$$|f_i(\omega)g_j(\omega)| \leq 1, \quad i,j = 1,2$$

and

$$P_{ij} = Ef_ig_j, \quad i,j = 1,2.$$

Then

$$|P_{11} - P_{12}| + |P_{21} + P_{22}| \leq 2.$$

Proof. $P_{11} - P_{12} =$

$$= Ef_1g_1 - Ef_1g_2 = E(f_1g_1(1 \pm f_2g_2)) - E(f_1g_2(1 \pm f_2g_1)),$$

$$|P_{11} - P_{12}| \leq E(1 \pm f_2g_2) + E(1 \pm f_2g_1) = 2 \pm (P_{22} + P_{21}).$$

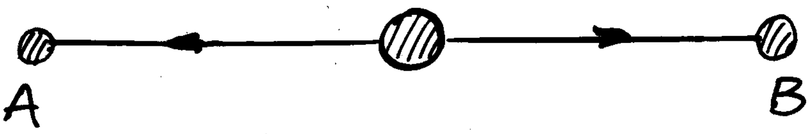
$$|x| \leq 2 \pm y \quad \rightarrow \quad |x| + |y| \leq 2.$$

Therefore Theorem is proved (CHSH inequality):

$$|P_{11} - P_{12}| + |P_{21} + P_{22}| \leq 2.$$

Quantum Mechanics

Consider a pair of spin one-half particles formed in the singlet spin state and moving freely in opposite directions (EPR pair).



PARADOX

If one neglects the space part of the wave function then the quantum mechanical correlation of two spins in the singlet state ψ_{spin} is

$$D_{spin}(a,b) = \langle \psi_{spin} | \sigma \cdot a \otimes \sigma \cdot b | \psi_{spin} \rangle = -a \cdot b$$

Here a and b are two unit vectors in three-dimensional space and $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli matrices. Since

$$-a \cdot b = \cos(t - s)$$

Bell's theorem states that the function $D_{spin}(a,b)$ can not be represented in the form

$$D_{spin}(a,b) \neq Ex(a)y(b)$$

where $x(a)$ and $y(b)$ are random fields on the two dimensional sphere.

$$\boxed{Quantum\ Correlation \neq Classical\ Correlation}$$

It is now widely accepted, as a result of Bell's theorem and related experiments, that Einstein's "local realism" must be rejected.

Evidently, the very formulation of the problem of locality in quantum mechanics is based on ascribing a special role to the position in ordinary three-dimensional space. It is rather surprising therefore that the space dependence of the wave function is neglected in discussions of the problem of locality in relation to Bell's inequalities. Actually it is the space part of the wave function which is relevant to the consideration of the problem of locality.

We point out that the space part of the wave function leads to an extra factor in quantum correlation and as a result the ordinary proof of Bell's theorem fails in this case. We present a criterium of locality (or nonlocality) of quantum theory in a realist model of hidden variables. We argue that predictions of quantum mechanics can be consistent with Bell's inequalities for Gaussian wave functions and hence Einstein's local realism is restored in this case.

This leads also to a new approach to problems in quantum information theory such as quantum cryptography, quantum teleportation and quantum computing. The crucial new point is the consideration of the space and time dependence of the wave functions.

Locality in Space

In the previous discussion the space part of the wave function of the particles was neglected. However exactly the space part is relevant to the discussion of locality. The complete wave function is $\psi = (\psi_{\alpha\beta}(\mathbf{r}_1, \mathbf{r}_2))$ where α and β are spinor indices and $\mathbf{r}_1$ and $\mathbf{r}_2$ are vectors in three-dimensional space.

We suppose that detectors are located within the two localized regions $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, well separated from one another. Quantum correlation describing the measurements of spins at the localized detectors is

$$D(a, \mathcal{O}_1, b, \mathcal{O}_2) = \langle \psi | \sigma \cdot a P_{\mathcal{O}_1} \otimes \sigma \cdot b P_{\mathcal{O}_2} | \psi \rangle$$

Here $P_{\mathcal{O}}$ is the projection onto the region $\mathcal{O}$. Let us consider the case when the wave function has the form $\psi = \psi_{spin} \phi(\mathbf{r}_1, \mathbf{r}_2)$. One has

$$D(a, \mathcal{O}_1, b, \mathcal{O}_2) = g(\mathcal{O}_1, \mathcal{O}_2) D_{spin}(a, b)$$

where the function

$$g(\mathcal{O}_1, \mathcal{O}_2) = \int_{\mathcal{O}_1 \times \mathcal{O}_2} |\phi(\mathbf{r}_1, \mathbf{r}_2)|^2 d\mathbf{r}_1 d\mathbf{r}_2$$

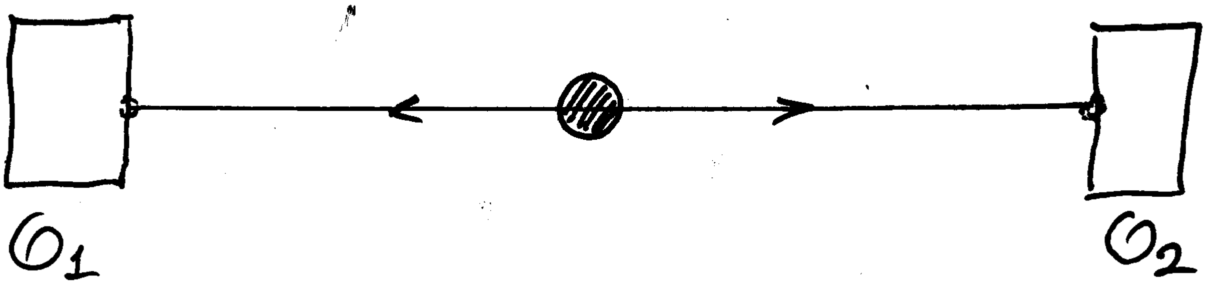
describes correlation of particles in space. Note that one has

$$0 \leq g(\mathcal{O}_1, \mathcal{O}_2) \leq 1$$

Remark. In relativistic quantum field theory there is no nonzero strictly localized projection operator that annihilates the vacuum. It is a consequence of the Reeh-Schlieder theorem. Therefore, apparently, the function $g(\mathcal{O}_1, \mathcal{O}_2)$ should be always strictly smaller than 1.

To investigate the property of locality in a realist theory of hidden variables we will study whether the quantum correlation can be represented in the form of classical correlations. One inquires whether one can write the representation

$$g(\mathcal{O}_1, \mathcal{O}_2) D_{spin}(a, b) = E x(a) y(b)$$



BELL'S EQUATION

$$\cos(\alpha-\beta) = \int x(\alpha,\lambda)\, y(\beta,\lambda)\, d\rho(\lambda)$$

MODIFIED EQUATION (LOCAL)

$$|\phi(r_1,r_2,t)|^2 \cos(\alpha-\beta) = \int x(\alpha,r_1,t,\lambda)\, y(\beta,r_2,t,\lambda)\, d\rho(\lambda)$$

SIMPLE MODIFIED EQUATION

$$g \cos(\alpha-\beta) = \int x(\alpha,\lambda)\, y(\beta,\lambda)\, d\rho(\lambda)$$

$$|x| \le 1, \quad |y| \le 1, \quad \int d\rho = 1, \quad d\rho \ge 0$$

$$\int |\phi(r_1,r_2,t)|^2\, dr_1\, dr_2 = 1$$

RELATIVISTIC EQUATION ?

$$|\phi(r_1,t_1,r_2,t_2)|^2 (a,b) = \int x(a,r_1,t_1,\lambda)\, y(b,r_2,t_2,\lambda)\, d\rho(\lambda)$$

TH. 1. CONSIDER EQUATION

$$g \cos(\alpha-\beta) = \int_{\Lambda} x(\alpha,\lambda)\, y(\beta,\lambda)\, d\rho(\lambda)$$

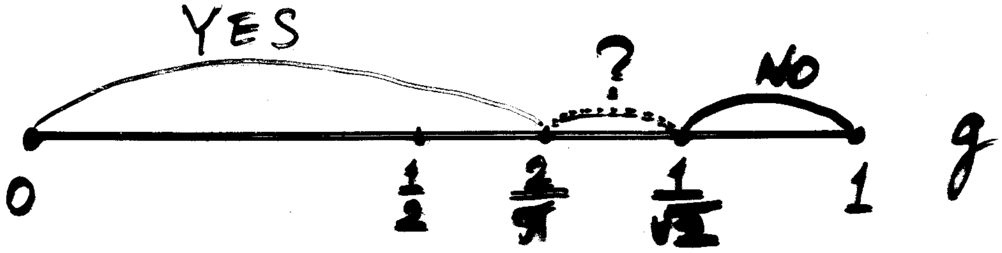
WHERE $0 \le g \le 1$ IS FIXED.

WE WANT TO FIND A SOLUTION $(\Lambda, x, y, d\rho)$, I.E. A SET Λ, FUNCTIONS $x(\alpha,\lambda)$, $y(\beta,\lambda)$ AND MEASURE $d\rho$ SUCH THAT

$$|x(\alpha,\lambda)| \le 1, \quad |y(\beta,\lambda)| \le 1, \quad \int_{\Lambda} d\rho(\lambda) = 1, \quad d\rho(\lambda) \ge 0.$$

IF $0 \le g \le \frac{2}{\pi}$ THEN THERE EXISTS A SOLUTION.

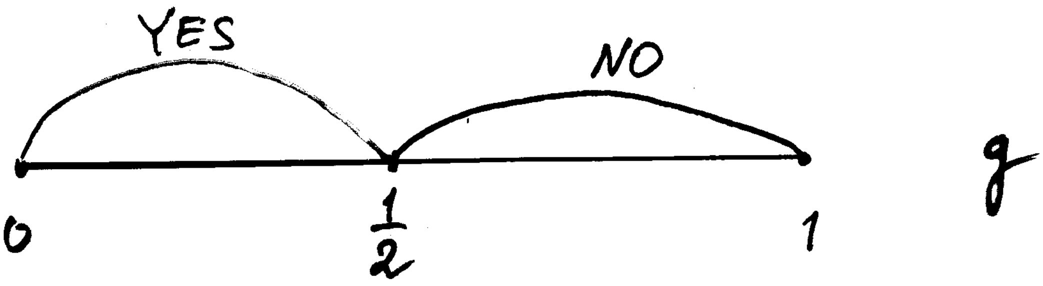
IF $\frac{1}{\sqrt{2}} < g$ THEN THERE IS NO SOLUTION.



TH 2. CONSIDER EQUATION

$$g \cos(\alpha-\beta) = \int_{\Lambda} x(\alpha,\lambda)\, x(\beta,\lambda)\, d\rho(\lambda)$$

THEN THE SOLUTION $(\Lambda, x, d\rho)$ EXISTS IF AND ONLY IF $0 \le g \le \frac{1}{2}$.



TH 1 VS. TH 2 : ASYMMETRY ?

A. KHRENNIKOV, D. PROKHORENKO
S. BOCHKAREV, I.V.

J.-A. LARSSON
E. SANTOS

$g = g(\omega_1, \omega_2)$ CONTRIBUTES TO THE EFFICIENCY OF DETECTORS

In another form: For which constants g we can find a representation

$$\boxed{g\cos(t-s) = Ex_t y_s?}$$

where

$$|x_t(\omega)| \leq 1, \quad |y_s(\omega)| \leq 1.$$

Example. If $g = 1/2$ then there exists such a representation:

$$\frac{1}{2}\cos(t-s) = \int_0^{2\pi} \cos(t-\omega)\cos(s-\omega)\frac{d\omega}{2\pi}$$

Problem of locality in quantum mechanics and theory of stochastic processes.

Which functions $f(t,s)$ can be represented in the form

$$\boxed{f(t,s) = Ex_t y_s}$$

Restrictions on x_t, y_s?

$$f(t_1, \ldots t_n) = Ex_{t_1} \ldots z_{t_n}$$

Note that if we set $g(\mathcal{O}_1, \mathcal{O}_2) = 1$ as it was

SUMMARY.

- BELL'S INEQUALITIES DO NOT INCLUDE SPACETIME VARIABLES. THEREFORE THEY DO NOT DIRECTLY RELEVANT TO THE PROBLEM OF LOCALITY OF QUANTUM THEORY.

MODIFIED EQUATION

$$|\phi(r_1, r_2, t)|^2 \cdot (a,b) = \int_\Lambda \xi(a, r_1, t, \lambda)\,\eta(b, r_2, t, \lambda)\,d\rho(\lambda)$$

EXPERIMENTAL STUDY OF SPATIAL DEPENDENCE

- RELATIVISTIC PARTICLES : PHOTONS, DIRAC.

NO FACTORIZATION OF WAVE FUNCTION INTO THE SPIN AND SPACETIME PARTS.

NEW EQUATION

$$g_{ij}(k_1, k_2)\,a_i\,b_j = \int \xi(a, k_1, \lambda)\,\eta(b, k_2, \lambda)\,d\rho(\lambda)$$

- PASSIVE SYSTEMS: VLADIMIROV V.S. LOCALITY IN SPACE TIME FOR CLASSICAL CHANNELS

• QUANTUM FIELD THEORY –

– LOCAL THEORY:

$$[\varphi(x), \varphi(y)] = 0, \quad (x-y)^2 < 0.$$

• ENTANGLED STATES IN SPACETIME

• QUANTUM INFORMATION IN SPACETIME.

(CLASSICAL THEORY OF INFORMATION IN SPACETIME. RELATIVISTIC INFORMATION THEORY)

QUANTUM CRYPTOGRAPHY, TELEPORTATION, COMPUTING, ... IN SPACETIME

• (?) SPECULATION. PRINCIPLE:

IN QUANTUM PHYSICS ONLY SUCH STATES AND OBSERVABLES EXIST WHICH SATISFY THE REQUIREMENT OF EINSTEIN–BELL LOCAL REALISM:

$$\langle\psi| A_{i_1} \dots A_{i_k} |\psi\rangle = \int \xi_{i_1}(\lambda) \dots \xi_{i_k}(\lambda)\, d\rho(\lambda)$$

("NONCOMMUTATIVE SPECTRAL THEOREM")

• QUANTUM INFORMATION IN CURVED SPACETIME AND PHYSICS OF BLACK HOLES.

QUANTUM MUTUAL INFORMATION

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$$

$$\rho_{AB}$$

$$\rho_A = \mathrm{Tr}_{\mathcal{H}_B} \rho_{AB} \quad , \quad \rho_B = \mathrm{Tr}_{\mathcal{H}_A} \rho_{AB}$$

$$S(A:B) = \mathrm{Tr}\left(\rho_{AB} \log \rho_{AB}\right) -$$

$$- \mathrm{Tr}\left(\rho_A \log \rho_A\right) - \mathrm{Tr}\left(\rho_B \log \rho_B\right)$$

Describes how much information systems A and B have in common.

SUMMARY

- REDUCTION POSTULATE
- QUANTUM COMPUTER
  QUANTUM CIRCUIT $\{\mathcal{H}, \{V_1, \ldots, V_r\}, U\}$
  SHOR FACTORING ALGORITHM
  NP - COMPLETE PROBLEMS
  NMR, ION TRAPS, ATOM, ...
- EPR PAIR / ENTANGLED STATES
- QUANTUM TELEPORTATION
- BELL'S THEOREM
- SPACE DEPENDENCE OF ENTANGLED STATES