

The role of entanglement

Alexei Grinbaum

CEA-Saclay/LARSIM

Outline

- 1 Understanding entanglement
- 2 Reconstructions of quantum mechanics
- 3 Understanding Tsirelson's bound

New type of information

Bits \rightarrow Bits and Qubits

States in quantum mechanics

- State of a qubit is a unit vector in \mathbf{C}^2 .
- Orthonormal basis of \mathbf{C}^2 is usually written as $|0\rangle$ and $|1\rangle$.
- A generic state of a qubit is $\alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$.

Measuring a quantum state

Measuring a quantum state $\alpha|0\rangle + \beta|1\rangle$ yields the result

- $|0\rangle$, with probability $|\alpha|^2$, or
- $|1\rangle$, with probability $|\beta|^2$.

Entanglement

Product state $(\alpha_1|0\rangle + \beta_1|1\rangle) \times (\alpha_2|0\rangle + \beta_2|1\rangle) =$
 $\alpha_1\alpha_2|00\rangle + \beta_1\beta_2|11\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle$

Another combination of two states

$$(\alpha|0\rangle + \beta|1\rangle) \times (\alpha|0\rangle - \beta|1\rangle) =$$
$$\alpha^2|00\rangle - \beta^2|11\rangle + \alpha\beta(|10\rangle - |01\rangle) \neq \alpha^2|00\rangle - \beta^2|11\rangle$$

Bipartite entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Maximally entangled state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

The Holevo bound and superdense coding

Theorem No more than n bits of expected classical information can be communicated between Alice and Bob by exchanging n qubits.

A. Holevo, *Problemy peredachi informatsii*, **9**, 3–11 (1973).

Theorem If the communicating parties share prior entanglement, twice as much classical information can be transmitted, but no more.

C.H. Bennett and S.J. Wiesner, *Phys. Rev. Lett.*, **69**(20), 2881–2884 (1992).

So, is there anything to win?

Outline

- 1 Understanding entanglement
- 2 Reconstructions of quantum mechanics
- 3 Understanding Tsirelson's bound

- Zieler 1961
- Varadarajan 1962
- Piron 1964
- Kochen and Specker 1965
- Guenin 1966
- Gunson 1967
- Jauch 1968
- Pool 1968
- Plymen 1968
- Marlow 1978
- Beltrametti and Casinelli 1981
- Holland 1995

Mackey's axioms, 1957

\mathfrak{B} is a set of all Borel subsets of the real line. Consider two abstract sets \mathcal{O} and \mathcal{S} and a function p which assigns a real number $0 \leq p(x, f, M) \leq 1$ to each triple x, f, M , where x is in \mathcal{O} , f is in \mathcal{S} , and M is in \mathfrak{B} .

- M1 Function p is a probability measure. Mathematically, we have $p(x, f, \emptyset) = 0$, $p(x, f, \mathbb{R}) = 1$, and $p(x, f, M_1 \cup M_2 \cup M_3 \dots) = \sum_{n=1}^{\infty} p(x, f, M_n)$ whenever the M_n are Borel sets that are disjoint in pairs.
- M2 Two states, in order to be different, must assign different probability distributions to at least one observable; and two observables, in order to be different, must have different probability distributions in at least one state. Mathematically, if $p(x, f, M) = p(x', f, M)$ for all f in \mathcal{S} and all M in \mathfrak{B} then $x = x'$; and if $p(x, f, M) = p(x, f', M)$ for all x in \mathcal{O} and all M in \mathfrak{B} then $f = f'$.
- M3 Let x be any member of \mathcal{O} and let u be any real bounded Borel

function on the real line. Then there exists y in \mathcal{O} such that $p(y, f, M) = p(x, f, u^{-1}(M))$ for all f in \mathcal{S} and all M in \mathfrak{B} .

- M4 If f_1, f_2, \dots are members of \mathcal{S} and $\lambda_1 + \lambda_2 + \dots = 1$ where $0 \leq \lambda_n \leq 1$, then there exists f in \mathcal{S} such that $p(x, f, M) = \sum_{n=1}^{\infty} \lambda_n p(x, f_n, M)$ for all x in \mathcal{O} and M in \mathfrak{B} .
- M5 Call *question* an observable e in \mathcal{O} such that $p(e, f, \{0, 1\}) = 1$ for all f in \mathcal{S} . Questions e and e' are disjoint if $e \leq 1 - e'$. Then a question $\sum_{n=1}^{\infty} e_n$ exists for any sequence (e_n) of questions such that e_m and e_n are disjoint whenever $n \neq m$.
- M6 If E is any compact, question-valued measure then there exists an observable x in \mathcal{O} such that $\chi_M(E) = E(M)$ for all M in \mathfrak{B} , where χ_M is

a characteristic function of M .

- M7 The partially ordered set of all questions in quantum mechanics is isomorphic to the partially ordered set of all closed subspaces of a separable, infinite-dimensional Hilbert space.
- M8 If e is any question different from 0 then there exists a state f in \mathcal{S} such that $m_f(e) = 1$.
- M9 For each sequence (f_n) of members of \mathcal{S} and each sequence (λ_n) of non-negative real numbers whose sum is 1, one-parameter time evolution group $V_t : \mathcal{S} \mapsto \mathcal{S}$ acts as follows: $V_t(\sum_{n=1}^{\infty} \lambda_n f_n) = \sum_{n=1}^{\infty} \lambda_n V_t(f_n)$ for all $t \geq 0$; and for all x in \mathcal{O} , f in \mathcal{S} , and M in \mathfrak{B} , $t \mapsto p(x, V_t(f), M)$ is continuous.

Hardy's axioms, 2001

Consider natural numbers, K and N . K is the number of degrees of freedom of the system and is defined as the minimum number of probability measurements needed to determine the state. Dimension N is defined as the maximum number of states that can be reliably distinguished from one another in a single measurement.

H1 Probabilities. In the limit as n becomes infinite, relative frequencies (measured by taking the proportion of times a particular outcome is observed) tend to the same value for any case where a given measurement is performed on an ensemble of n systems prepared by some given preparation.

H2 Simplicity. K is determined by a function of N where $N = 1, 2, \dots$ and where, for each given N , K takes the minimum value consistent with the axioms.

H3 Subspaces. A system whose state is constrained to belong to an M dimensional subspace behaves like a system of dimension M .

H4 Composite systems. A composite system consisting of subsystems A and B satisfies $N = N_A N_B$ and $K = K_A K_B$.

H5 Continuity. There exists a continuous reversible transformation on a system between any two pure states of that system.

H5' Reversibility. There exists a reversible transformation on a system between any two pure states of that system.

The CBH axioms, 2003

CBH1 No superluminal information transfer via measurement.

CBH2 No broadcasting (a generalisation of no cloning).

CBH3 No bit commitment.

C^* -algebraic formalism.

Dakić-Brukner axioms, 2009

Information capacity An elementary system has the information carrying capacity of at most one bit. All systems of the same information carrying capacity are equivalent.

Locality The state of a composite system is completely determined by local measurements on its subsystems and their correlations.

Reversibility Between any two pure states there exists a reversible transformation.

Continuity Between any two pure states there exists a continuous reversible transformation.

Outline

- 1 Understanding entanglement
- 2 Reconstructions of quantum mechanics
- 3 Understanding Tsirelson's bound

PR boxes

PR box takes two inputs $x_1, x_2 \in \{0, 1\}$ and produces two outputs $a_1, a_2 \in \{0, 1\}$ according to the joint distribution

$$P(a_1 a_2 | x_1 x_2) = \begin{cases} 1/2 : & a_1 + a_2 = x_1 x_2 \pmod{2} \\ 0 : & \text{otherwise.} \end{cases}$$

S. Popescu and D. Rohrlich, *Found. Phys.* 24, 379 (1994).

PR boxes

PR box takes two inputs $x_1, x_2 \in \{0, 1\}$ and produces two outputs $a_1, a_2 \in \{0, 1\}$ according to the joint distribution

$$P(a_1 a_2 | x_1 x_2) = \begin{cases} 1/2 : & a_1 + a_2 = x_1 x_2 \pmod{2} \\ 0 : & \text{otherwise.} \end{cases}$$

Compatible with special relativity: one observer cannot signal to the other via his choice of input in the box.

S. Popescu and D. Rohrlich, *Found. Phys.* 24, 379 (1994).

PR boxes

PR box takes two inputs $x_1, x_2 \in \{0, 1\}$ and produces two outputs $a_1, a_2 \in \{0, 1\}$ according to the joint distribution

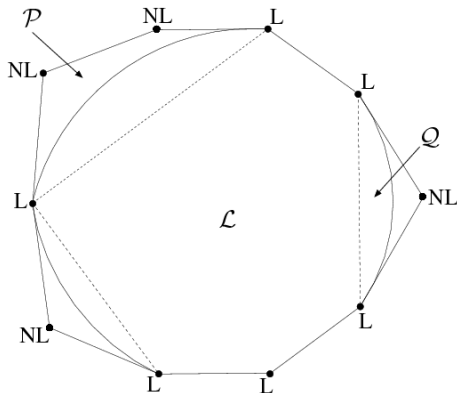
$$P(a_1 a_2 | x_1 x_2) = \begin{cases} 1/2 : & a_1 + a_2 = x_1 x_2 \pmod{2} \\ 0 : & \text{otherwise.} \end{cases}$$

Compatible with special relativity: one observer cannot signal to the other via his choice of input in the box.

	Classical	Quantum	PR Boxes
CHSH max value	2	$2\sqrt{2}$	4

Why is quantum mechanics not more nonlocal?

S. Popescu and D. Rohrlich, *Found. Phys.* 24, 379 (1994).



L and NL: local and non-local. Bell inequalities are the facets represented in dashed lines. The set bounded by these is \mathcal{L} . The region accessible to quantum mechanics is \mathcal{Q} . A general non-signalling box $\in \mathcal{P}$.

Property	GLT	GNST	QM	Classical
Non-unique decomposition of mixed states into pure states	yes	yes	yes	no
Cloning of single states	yes	yes	no	yes
Joint broadcasting of states	no	no	no	yes
Some pure states cannot be distinguished with nondisturbing operations	yes	yes	yes	no
Measurements on bipartite systems decompose trivially	no	yes	no	yes
Secure key distribution for quantum cryptography	yes	yes	yes	no
Continuous transformation between pure states	no	no	yes	no

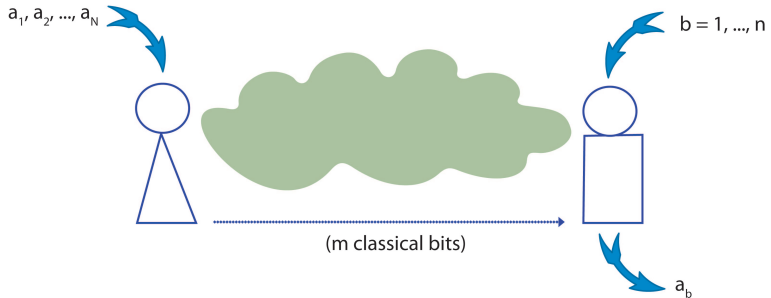
Alice wants to send Bob a love letter.

If she writes him “I lov”, Bob will understand what she meant.

But if she only writes “I l”, he won't get it.

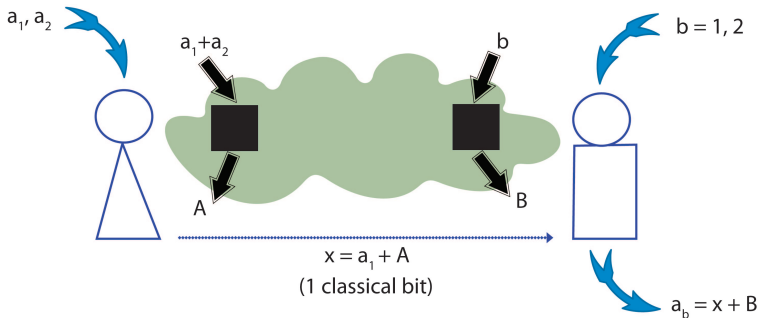
Maintaining communication complexity allows to lower the limit to 91% of maximal non-locality.

W. van Dam, arXiv: quant-ph/0501159.



Alice receives N random and independent bits a_1, \dots, a_N . In a separate location, Bob receives a random variable $b \in \{1, \dots, N\}$. Alice sends m classical bits to Bob, with the help of which Bob is asked to guess the value of the b th bit in Alice's list, a_b . Alice and Bob can share any non-signalling resources. Information causality bounds the mutual information between Alice's data and all that Bob has at hand after receiving the message.

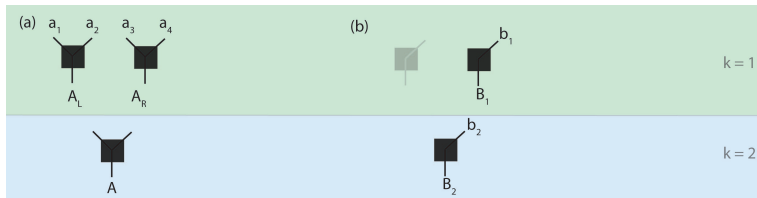
M. Pawłowski *et al.*, *Nature* **461**, 1101, 2009



Alice uses $a = a_0 \oplus a_1$ as an input to the shared PR-box and obtains the outcome A , which is used to compute her message $x = a_0 \oplus A$ for Bob. On his side, Bob inputs $b = 0$ if he wants to learn a_0 , and $b = 1$ if he wants to learn a_1 ; he gets the outcome B . On receiving x from Alice, Bob computes his guess

$$x \oplus B = a_0 \oplus A \oplus B = a_0 \oplus (a_0 \oplus a_1)b = a_b.$$

W. van Dam, PhD thesis, Univ. Oxford, 2000



Alice and Bob encode 2^n bits using $2^n - 1$ pairs of boxes in van Dam's chain. Alice sends only one bit to Bob at the last stage of the chain. Bob then uses it to decode the value of bits back from the bottom to the bit he is interested in. The final guess is correct if

$$1 \geq (2E^2)^n \quad \forall n,$$

where E is the bias of the box's success probability: $p = \frac{1+E}{2}$. Hence the Tsirelson bound $E \leq \frac{1}{\sqrt{2}}$.

M. Pawłowski *et al.*, *Nature* **461**, 1101, 2009