Quantum computation: harnessing the atom at the borders of paradox

Samson Abramsky

Department of Computer Science, University of Oxford

Beginnings . . .

The first axiom I learnt in Computer Science:

Computers might as well be made of green cheese

It is no longer safe to assume this!

Quantum Contextuality

Bell's theorem, spooky action at a distance, and all that ...

Quantum Mechanics is weird!

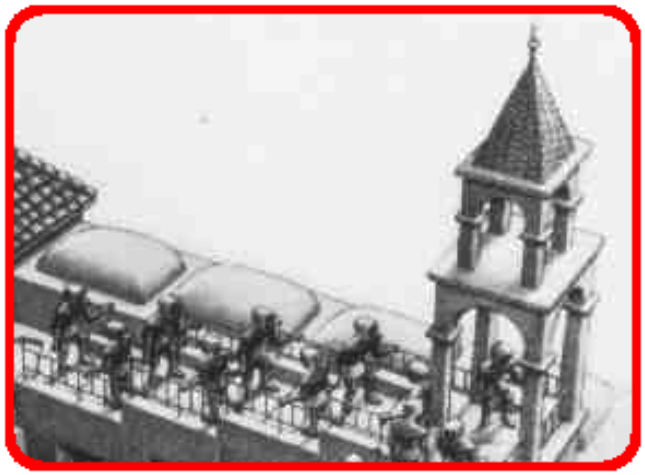
This has implications for

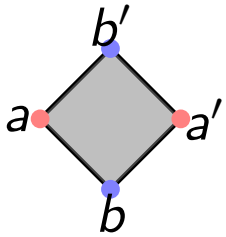
- Our very conception of reality
- The possibilities for information processing, in ways which could transform our information society

What **is** contextuality, as a problematic, non-classical phenomenon?

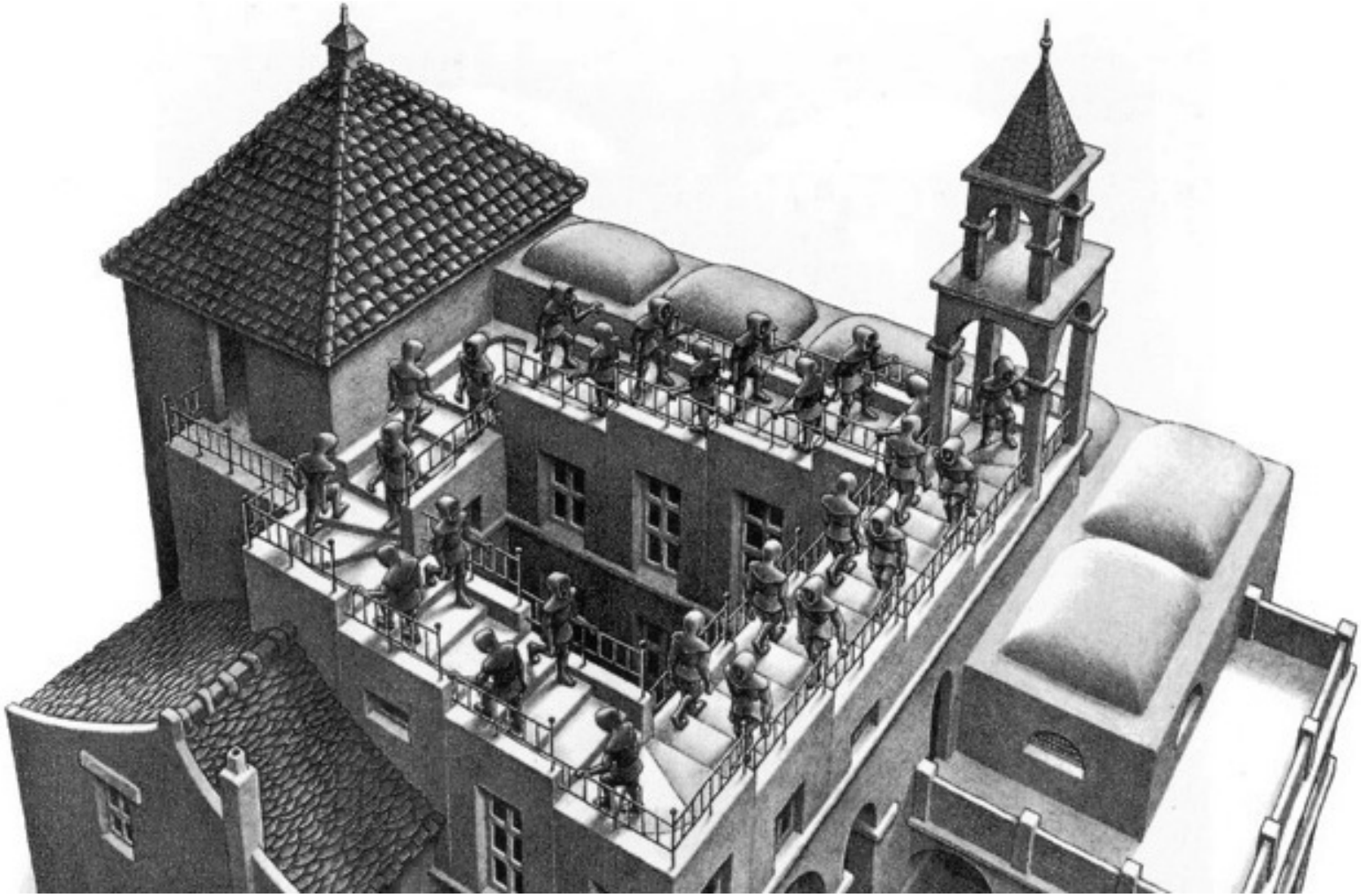
In a nutshell: where we have a family of data which is **locally consistent**, but **globally inconsistent**.

Contextuality Analogy: Local Consistency





Contextuality Analogy: Global Inconsistency



The Borders of Paradox

If this phenomenon arises with **observable data**, reflecting physical reality, it takes us to the borders of paradox.

What saves us from a direct conflict between logic and experience is that the data **cannot** be directly observed globally.
We cannot observe all the variables **at the same time**.

Quantum Paradoxes and Quantum Technologies

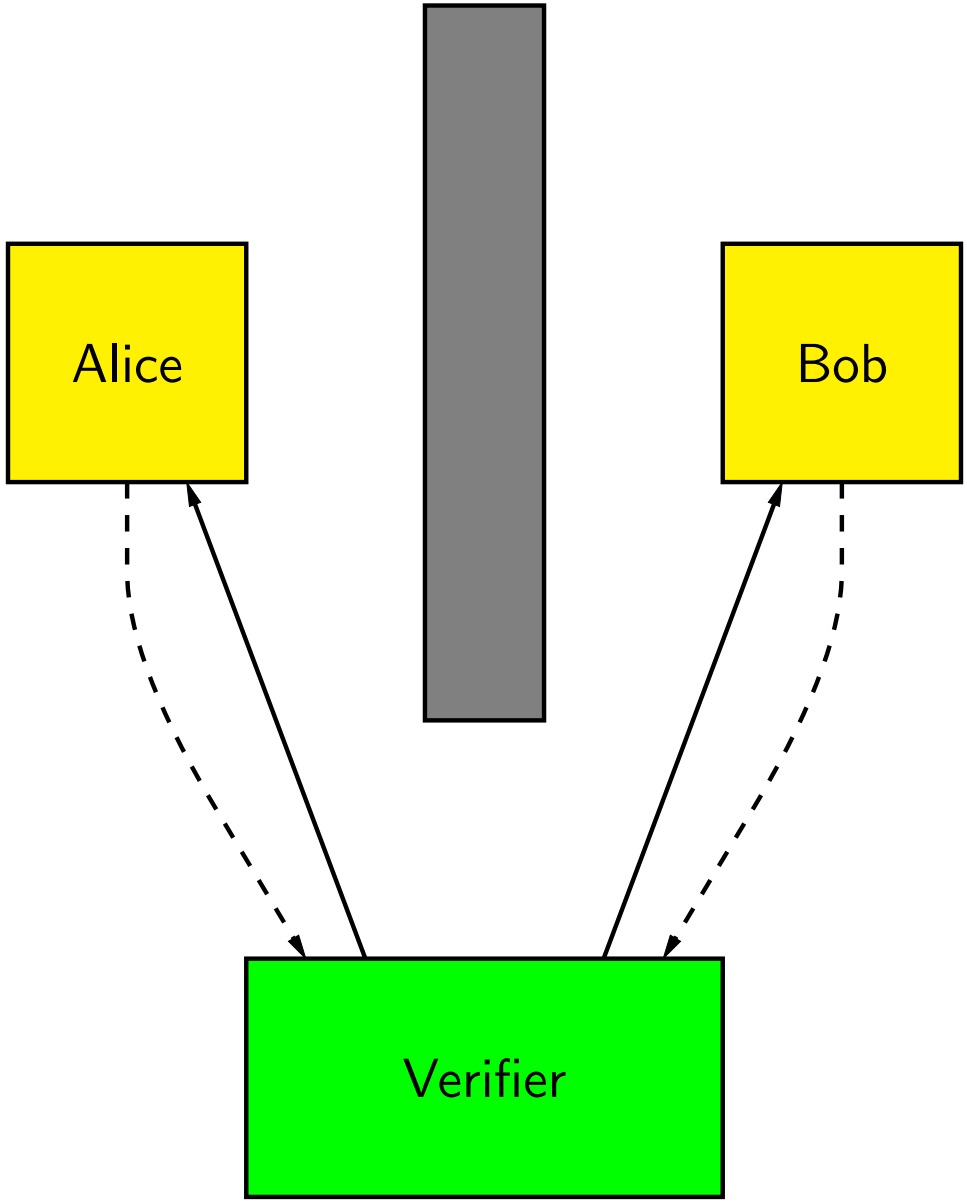
We are witnessing the beginnings of quantum technologies for information processing:

- randomness certification and amplification
- quantum key distribution and other security protocols (and post-quantum crypto)
- simulation of quantum chemistry, machine learning, optimization may soon be in reach

These remarkable developments are directly connected with ideas from quantum foundations, closely associated with paradoxes or quasi-paradoxes: Bell's theorem, Kochen-Specker paradox, Hardy's paradox, teleportation, pseudo-telepathy, non-locality, contextuality, ...

The borders of paradox are a fruitful place to be!

Alice-Bob games



The XOR Game

Alice and Bob play a cooperative game against Verifier (or Nature!):

- Verifier chooses an input $x \in \{0,1\}$ for Alice, and similarly an input y for Bob. We assume the uniform distribution for Nature's choices.
- Alice and Bob each have to choose an output, $a \in \{0,1\}$ for Alice, $b \in \{0,1\}$ for Bob, depending on their input. They are **not allowed to communicate during the game**.
- The winning condition: $a \oplus b = x \wedge y$.

A table of conditional probabilities $p(a,b|x,y)$ defines a **probabilistic strategy** for this game. The **success probability** for this strategy is:

$$1/4[p(a=b|x=0,y=0)+p(a=b|x=0,y=1)+p(a=b|x=1,y=0)$$

$$+p(a\neq b|x=1,y=1)]$$

A Strategy for the Alice-Bob game

Example: The Bell Model

A	B	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
0	0	$1/2$	0	0	$1/2$
0	1	$3/8$	$1/8$	$1/8$	$3/8$
1	0	$3/8$	$1/8$	$1/8$	$3/8$
1	1	$1/8$	$3/8$	$3/8$	$1/8$

A	B	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
0	0	$1/2$	0	0	$1/2$
0	1	$3/8$	$1/8$	$1/8$	$3/8$
1	0	$3/8$	$1/8$	$1/8$	$3/8$
1	1	$1/8$	$3/8$	$3/8$	$1/8$

The entry in row 2 column 3 says:

A Simple Observation

Suppose we have propositional formulas $\phi_1, \ldots, \phi_N$

Suppose further we can assign a probability $p_i = \text{Prob}(\phi_i)$ to each ϕ_i.

(Story: perform experiment to test the variables in ϕ_i; p_i is the relative frequency of the trials satisfying ϕ_i.)

Suppose that these formulas are **not simultaneously satisfiable**. Then (e.g.)

$$\bigwedge_{i=1}^{N-1} \phi_i \;\Rightarrow\; \neg\phi_N, \quad \text{or equivalently} \quad \phi_N \;\Rightarrow\; \bigvee_{i=1}^{N-1} \neg\phi_i.$$

Using elementary probability theory, we can calculate:

$$p_N \;\leq\; \text{Prob}(\bigvee_{i=1}^{N-1} \neg\phi_i) \;\leq\; \sum_{i=1}^{N-1} \text{Prob}(\neg\phi_i) \;=\; \sum_{i=1}^{N-1}(1-p_i) \;=\; (N-1) - \sum_{i=1}^{N-1} p_i.$$

Hence we obtain the inequality

$$\sum_{i=1}^{N} p_i \;\leq\; N-1.$$

Logical analysis of the Bell table

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
(a_1, b_1)	**1/2**	0	0	**1/2**
(a_1, b_2)	**3/8**	1/8	1/8	**3/8**
(a_2, b_1)	**3/8**	1/8	1/8	**3/8**
(a_2, b_2)	1/8	**3/8**	**3/8**	1/8

If we read 0 as true and 1 as false, the highlighted entries in each row of the table are represented by the following propositions:

$$\begin{array}{lcccccccc}
\varphi_1 & = & (a_1 \wedge b_1) & \vee & (\neg a_1 \wedge \neg b_1) & = & a_1 & \leftrightarrow & b_1 \\
\varphi_2 & = & (a_1 \wedge b_2) & \vee & (\neg a_1 \wedge \neg b_2) & = & a_1 & \leftrightarrow & b_2 \\
\varphi_3 & = & (a_2 \wedge b_1) & \vee & (\neg a_2 \wedge \neg b_1) & = & a_2 & \leftrightarrow & b_1 \\
\varphi_4 & = & (\neg a_2 \wedge b_2) & \vee & (a_2 \wedge \neg b_2) & = & a_2 & \oplus & b_2.
\end{array}$$

These propositions are easily seen to be contradictory.
The violation of the logical Bell inequality is 1/4.

Science Fiction? – The News from Delft

First Loophole-free Bell test, 2015

NATURE | LETTER

日本語要約

Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau & R. Hanson

Nature **526**, 682–686 (29 October 2015) doi:10.1038/nature15759
Received 19 August 2015 Accepted 28 September 2015 Published online 21 October 2015

More than 50 years ago[1], John Bell proved that no theory of nature that obeys locality and realism[2] can reproduce all the predictions of quantum theory: in any local-realist theory, the correlations between outcomes of measurements on distant particles satisfy an inequality that can be violated if the particles are entangled. Numerous Bell inequality tests have been reported[3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]; however, all experiments reported so far required additional assumptions to obtain a contradiction with local realism, resulting in 'loopholes'[13, 14, 15, 16]. Here we report a Bell experiment that is free of any such additional assumption and thus directly tests the principles underlying Bell's inequality. We use an event-ready scheme[17, 18, 19] that enables the generation of robust entanglement between distant electron spins (estimated state fidelity of 0.92 ± 0.03). Efficient spin read-out avoids the fair-sampling assumption (detection loophole[14, 15]), while the use of fast random-basis selection and spin read-out combined with a spatial separation of 1.3 kilometres ensure the required locality conditions[13]. We performed 245 trials that tested the CHSH–Bell inequality[20] $S \leq 2$ and found $S = 2.42 \pm 0.20$ (where S quantifies the correlation between measurement outcomes). A null-hypothesis test yields a probability of at most $P = 0.039$ that a local-realist model for space-like separated sites could produce data with a violation at least as large as we observe, even when allowing for memory[16, 21] in the devices. Our data hence imply statistically significant rejection of the local-realist null hypothesis. This conclusion may be further consolidated in future experiments; for instance, reaching a value of $P = 0.001$ would require approximately 700 trials for an observed $S = 2.4$. With improvements, our experiment could be used for testing less-conventional theories, and for implementing device-independent quantum-secure communication[22] and randomness certification[23, 24].

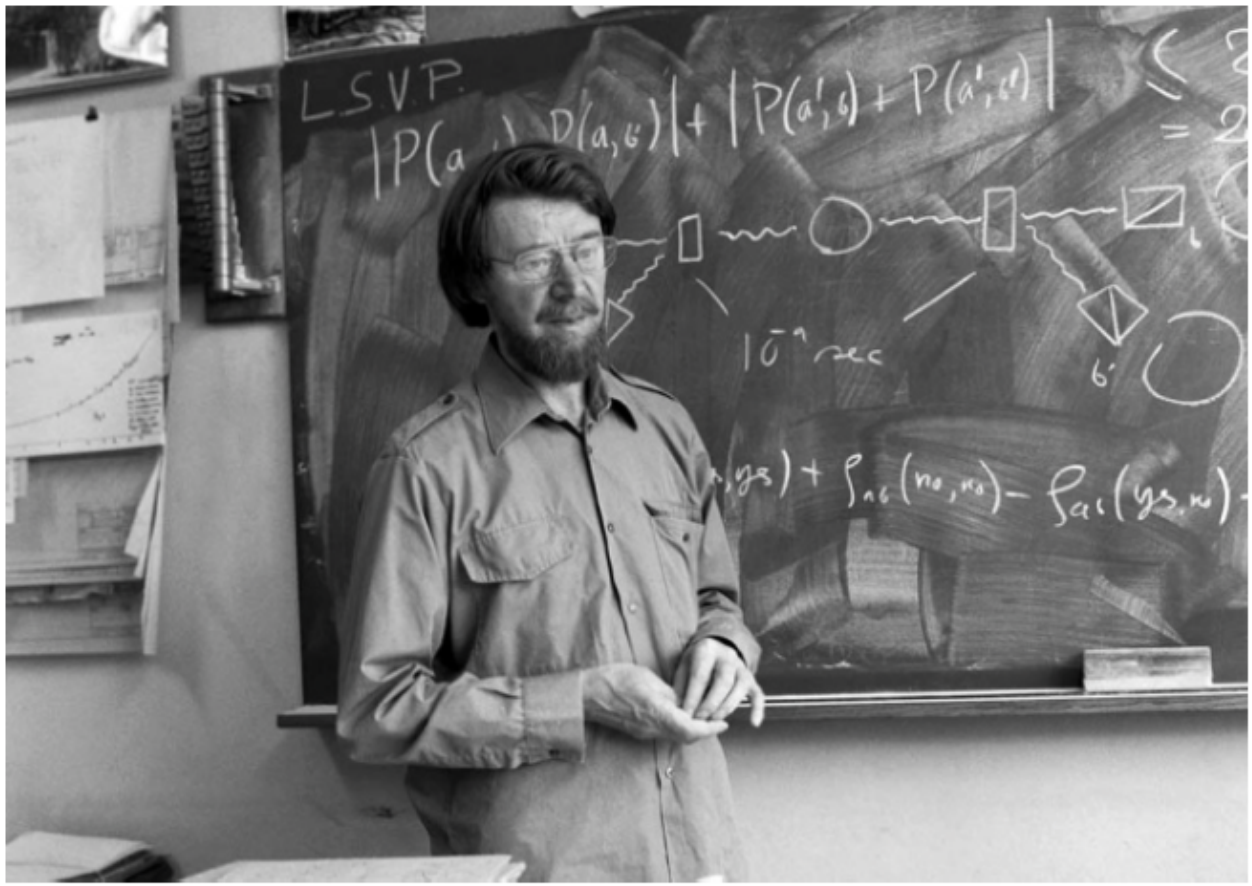
NATURE | NEWS

Quantum ‘spookiness’ passes toughest test yet

Experiment plugs loopholes in previous demonstrations of 'action at a distance', against Einstein's objections — and could make data encryption safer.

Zeeya Merali

27 August 2015



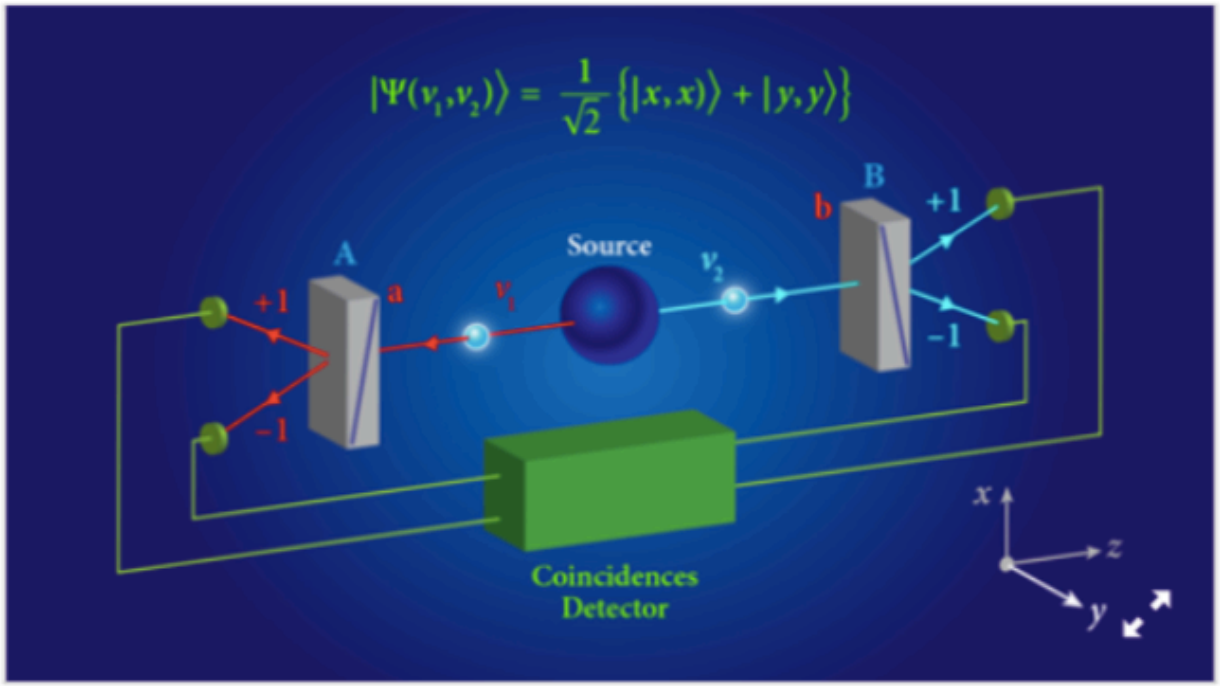
CERN

Viewpoint: Closing the Door on Einstein and Bohr's Quantum Debate

Alain Aspect, Laboratoire Charles Fabry, Institut d'Optique Graduate School, CNRS, Université Paris-Saclay, Palaiseau, France

December 16, 2015 • *Physics* 8, 123

By closing two loopholes at once, three experimental tests of Bell's inequalities remove the last doubts that we should renounce local realism. They also open the door to new quantum information technologies.



APS/Alan Stonebraker

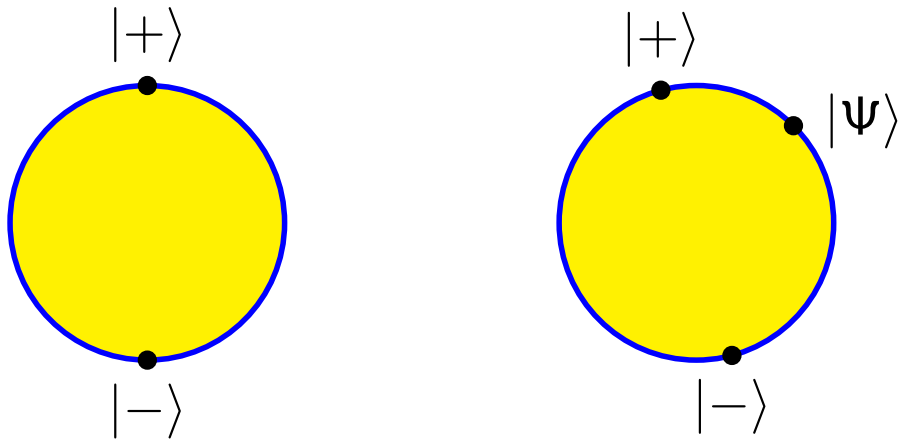
Figure 1: An apparatus for performing a Bell test. A source emits a pair of entangled photons v_1 and v_2. Their polarizations are analyzed by polarizers A and B (grey blocks), which are aligned, respectively, along directions a and b. (a and b can be along x, ... **Show more**

Timeline

1932	von Neumann's Mathematical Foundations of Quantum Mechanics
1935	EPR Paradox, the Einstein-Bohr debate
1964	Bell's Theorem
1982	First experimental test of EPR and Bell inequalities
	(Aspect, Grangier, Roger, Dalibard)
1984	Bennett-Brassard quantum key distribution protocol
1985	Deutch Quantum Computing paper
1993	Quantum teleportation
	(Bennett, Brassard, Crépeau, Jozsa, Peres, Wooters)
1994	Shor's algorithm
2015	First loophole-free Bell tests (Delft, NIST, Vienna)

Qubits: Spin Measurements

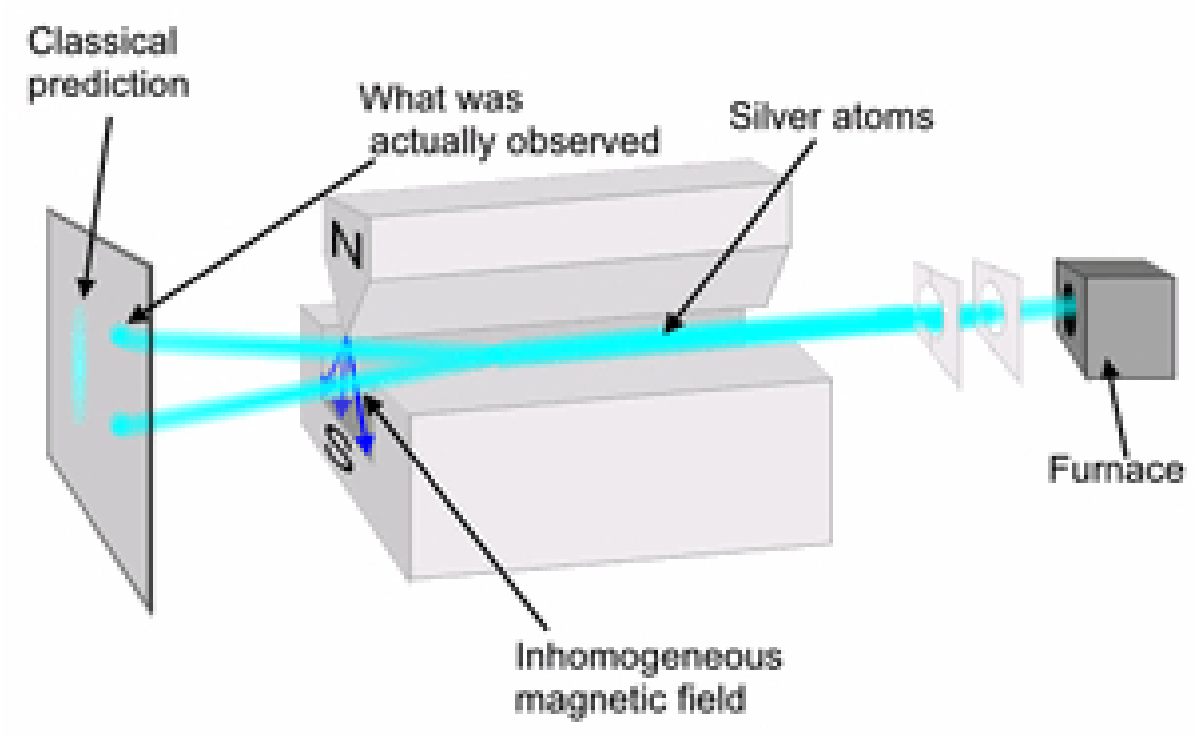
States of the system can be described by complex unit vectors in $\mathbb{C}^2$. These can be visualized as points on the unit 2-sphere:



Spin can be measured in any direction; so there are a continuum of possible measurements. There are **two possible outcomes** for each such measurement; spin in the specified direction, or in the opposite direction. These two directions are represented by a pair of orthogonal vectors. They are represented on the sphere as a pair of **antipodal points**.

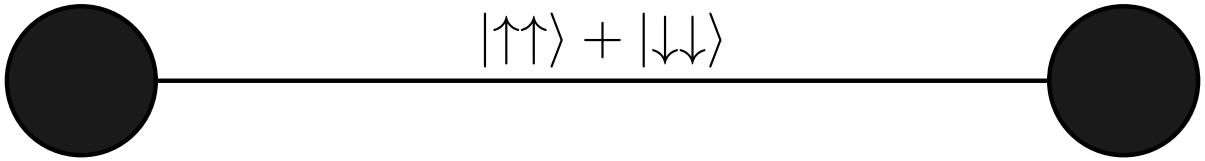
Note the appearance of **quantization** here: there are not a continuum of possible outcomes for each measurement, but only two!

The Stern-Gerlach Experiment



Quantum Entanglement

Bell state:



Compound systems are represented by **tensor product**: $\mathcal{H}_1 \otimes \mathcal{H}_2$. Typical element:

$$\sum_i \lambda_i \cdot \phi_i \otimes \psi_i$$

Superposition encodes **correlation**.

Einstein's 'spooky action at a distance'. Even if the particles are spatially separated, measuring one has an effect on the state of the other.

Entangled pairs of qubits provide **quantum resources** which can be used to gain **quantum advantage** in information processing tasks.

The Mermin Magic Square

A	B	C
D	E	F
G	H	I

The values we can observe for these variables are 0 or 1.

We require that each row and the first two columns have even parity, and the final column has odd parity.

This translates into 6 linear equations over $\mathbb{Z}_2$:

$$A \oplus B \oplus C = 0 \qquad A \oplus D \oplus G = 0$$

$$D \oplus E \oplus F = 0 \qquad B \oplus E \oplus H = 0$$

$$G \oplus H \oplus I = 0 \qquad C \oplus F \oplus I = 1$$

Of course, the equations are not satisfiable in $\mathbb{Z}_2$!

Alice-Bob games for binary constraint systems

Alice and Bob can share prior information, but cannot communicate once the game starts.

Verifier sends an **equation** to Alice, and a **variable** to Bob.

They win if Alice returns a satisfying assignment for the equation, and Bob returns a value for the variable consistent with Alice's assignment.

A perfect strategy is one which wins with probability 1.

Classically, A-B have a perfect strategy if and only if there is a satisfying assignment for the equations.

Mermin's construction shows that there is a quantum perfect strategy for the magic square.

Recent results

These games for general binary constraint systems studied by Cleve, Mittal, Liu and Slofstra.

They show that have a quantum perfect strategy is equivalent to a purely group-theoretic condition on a **solution group** which can be associated to each system of binary equations.

Major recent result by Slofstra:

Theorem

Every finitely presented group can be embedded in a solution group.

Corollaries:

- There are finite systems of boolean equations which have quantum perfect strategies in infinite-dimensional Hilbert space, but not in any finite dimension.
- The question:

  Given a binary constraint system, does a quantum perfect strategy exist?

  is undecidable.

Alice-Bob games for Graph Homomorphisms[1]

Given graphs G and H, does there exist a homomorphism $G \to H$?

Verifier sends a vertex of G to Alice, and a vertex to Bob. They output vertices of H.

They win if . . . ?

So we get a notion of "quantum graph homomorphism". What does it mean?

What is the general underlying notion? How far can we generalize? Does it lead to a notion of "quantum mathematics"?

There is an underlying "graded monad" (graded by dimension) . . .

Are there connections to description in various kinds of logic? E.g. a kind of "quantum finite model theory"?

[1] Studied by Mancinska and Robertson, following Cameron, Montanaro, Newman, Severini and Winter on the quantum chromatic number.

Strong Contextuality[2]

A	B	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
a_1	b_1	1	0	0	1
a_1	b_2	1	0	0	1
a_2	b_1	1	0	0	1
a_2	b_2	0	1	1	0

The PR Box: winning conditions for the XOR game!

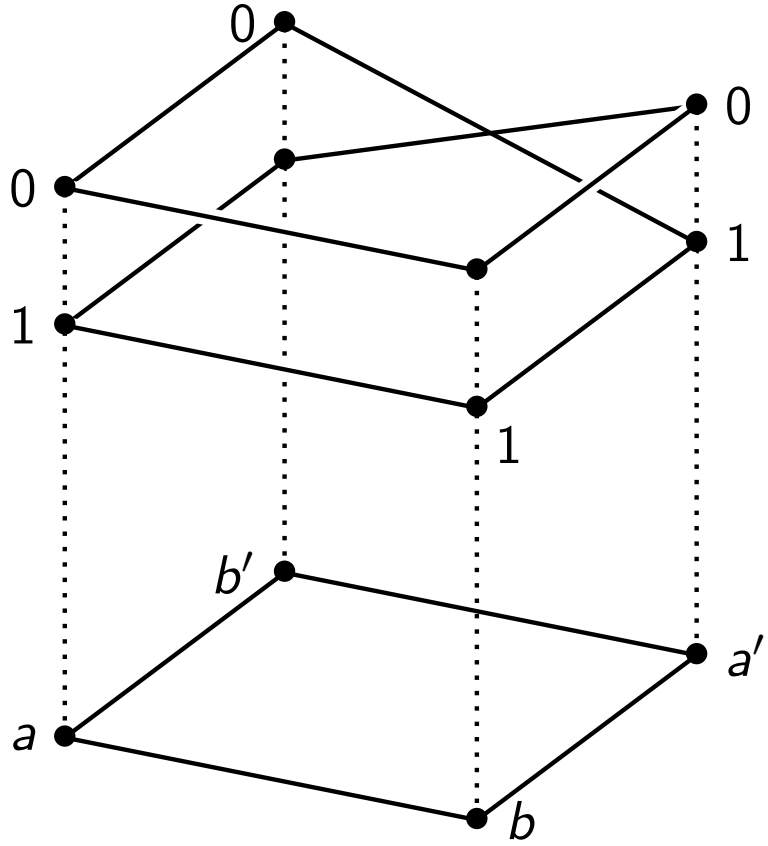
[2] SA and A. Brandenburger, The Sheaf-theoretic structure of non-locality and contextuality

Bundle Pictures[3]

Strong Contextuality

- E.g. the PR box:

	00	01	10	11
ab	✓	×	×	✓
ab'	✓	×	×	✓
$a'b$	✓	×	×	✓
$a'b'$	×	✓	✓	×



[3] SA, R. Barbosa, K. Kishida, R. Lal, S. Mansfield, Contextuality, Cohomology and Paradox.

Contextuality, Logic and Paradoxes

Liar cycles. A Liar cycle of length N is a sequence of statements

$$\begin{aligned} S_1 &: \ S_2 \text{ is true}, \\ S_2 &: \ S_3 \text{ is true}, \\ &\vdots \\ S_{N-1} &: \ S_N \text{ is true}, \\ S_N &: \ S_1 \text{ is false}. \end{aligned}$$

For $N = 1$, this is the classic Liar sentence

$$S : \ S \text{ is false}.$$

We can model the situation by boolean equations:

$$x_1 = x_2, \ \ \ldots, \ \ x_{n-1} = x_n, \ \ x_n = \neg x_1$$

The "paradoxical" nature of the original statements is captured by the inconsistency of these equations.

Contextuality in the Liar; Liar cycles in the PR Box

We can regard each of these equations as fibered over the set of variables which occur in it:

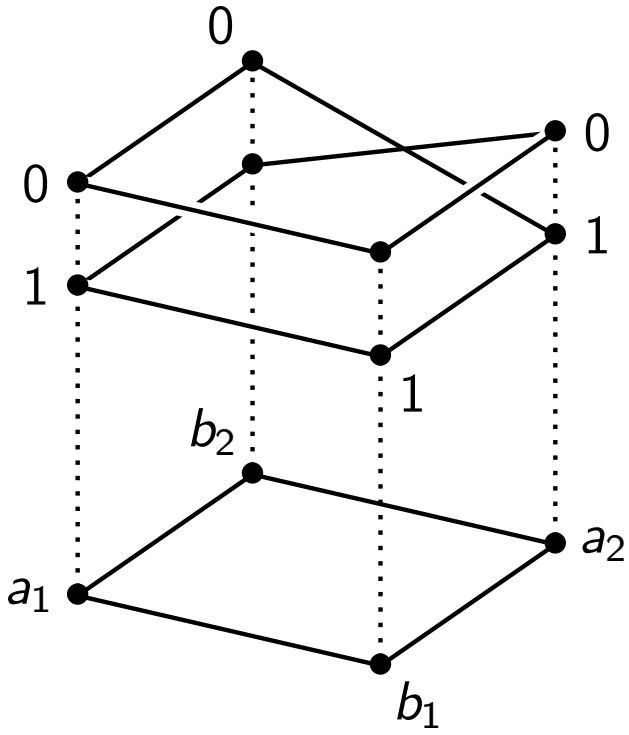
$$\begin{aligned}
\{x_1, x_2\} : \quad & x_1 = x_2 \\
\{x_2, x_3\} : \quad & x_2 = x_3 \\
& \vdots \\
\{x_{n-1}, x_n\} : \quad & x_{n-1} = x_n \\
\{x_n, x_1\} : \quad & x_n = \neg x_1
\end{aligned}$$

Any subset of up to $n-1$ of these equations is consistent; while the whole set is inconsistent.

Up to rearrangement, **the Liar cycle of length 4 corresponds exactly to the PR box**.

The usual reasoning to derive a contradiction from the Liar cycle corresponds precisely to the attempt to find a univocal path in the bundle diagram.

Paths to contradiction



Suppose that we try to set a_2 to 1. Following the path on the right leads to the following local propagation of values:

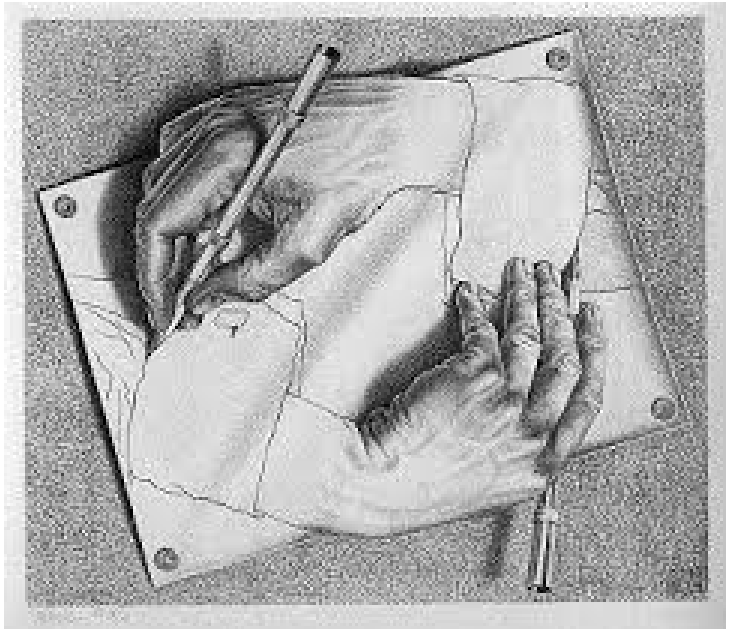
$$a_2 = 1 \rightsquigarrow b_1 = 1 \rightsquigarrow a_1 = 1 \rightsquigarrow b_2 = 1 \rightsquigarrow a_2 = 0$$

$$a_2 = 0 \rightsquigarrow b_1 = 0 \rightsquigarrow a_1 = 0 \rightsquigarrow b_2 = 0 \rightsquigarrow a_2 = 1$$

We have discussed a specific case here, but the analysis can be generalised to a large class of examples.

From paradox to technology

"Strange loops" (Hofstadter)



- "It's not a bug, it's a feature".
- Resolution of the paradox — add new values.

Envoi

Contextuality in physics raises deep questions about the nature of reality. But it is also a new kind of resource, which yields new possibilities in information processing tasks.
The challenge is to find methods to harness this resource, and understand its structure.

By using these notions, we may come to understand them better. This may be the only way!

Under the rubric of "local consistency, global inconsistency" contextuality is a pervasive notion, arising e.g. in constraint satisfaction, databases, distributed computation and elsewhere in classical computation.

People

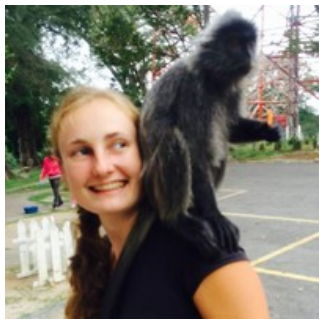











Adam Brandenburger, Lucien Hardy, Shane Mansfield, Rui Soares Barbosa, Ray Lal, Mehrnoosh Sadrzadeh, Phokion Kolaitis, Georg Gottlob, Carmen Constantin, Kohei Kishida. Giovanni Caru, Linde Wester, Nadish de Silva

The Penrose Tribar