On the happy marriage of quantum foundations and information theory

❧

(or why physics needs quantum foundations)

M.P. Seevinck

Institute for History and Foundations of Science
Utrecht University, The Netherlands

m.p.seevinck@uu.nl

April 2010

Prospects & Introduction

I will continue discussing foundations of quantum theory.

But I will **not** consider interpretations of quantum theory, but will focus on:

- recent methodological changes in the field, and
- novel technical breakthroughs.

(also an advertisement: this research is almost completely absent in the Netherlands)

Prospects & Introduction

I will continue discussing foundations of quantum theory.

But I will **not** consider interpretations of quantum theory, but will focus on:

- recent methodological changes in the field, and
- novel technical breakthroughs.

(also an advertisement: this research is almost completely absent in the Netherlands)

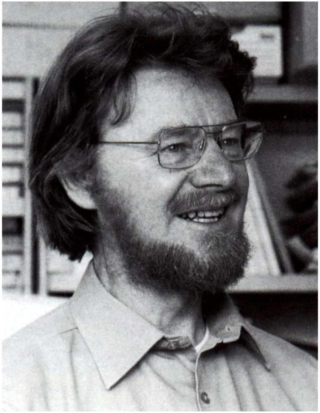
Disclaimer: this talk is not be understood as a plea against the philosophy/interpretation of quantum theory.

To the contrary, it should show how and why philosophy (asking deeper questions) is essential to any further progress in understanding physics and the world around us.

Methodological morale in foundations research

Now it is precisely in cleaning up intuitive ideas for mathematics that one is likely to throw out the baby with the bathwater.

John S. Bell (1928-1990)



Outline

Part I: Modern quantum foundations

- Why physics needs quantum foundations
  (Hardy & Spekkens: arXiv:1003.5008)

Part II: Nonlocal yet no-signalling correlations are a resource

- Example: monogamy of correlations and quantum cryptography

Conclusion and discussion

Part I: Modern quantum foundations

We have been witnessing two revolutions:

I) A ‘paradigm shift’ to study quantum mechanics (QM) ‘from the outside, not just from the inside’.

II) Quantum foundations research has delivered the essential ingredients for the new field of quantum information theory to emerge.

Background: Interpretations of Quantum Mechanics

Wheeler famously asked: “**Why the quantum?**”: How should we interpret quantum mechanics (QM)?

- Why is an interpretation needed: to solve the so-called measurement problem, to deal with the nonlocality of quantum correlations, or its alledged non-classicality, etc.

- Methodology used: ‘*study quantum physics from the inside*’ The practise of giving the theory a clear meaning using the formalism of the theory and nothing (or little) more.

A plethora of interpretations have been provided in the last 80 years.

To name a few popular interpretations:

- Many worlds interpretation
- Modal Interpretation
- Kopenhagen interpretation
- Bohmian mechanics
- Statistical interpretation
- FAPP (decoherence) interpretation
- ....(pick your own)

Background: Interpretations of Quantum Mechanics

I can be brief: This interpretation program has failed: There is no consensus on what *the* meaning of QM is.

- Why did this program fail? That would be a talk in itself.

Background: Interpretations of Quantum Mechanics

I can be brief: This interpretation program has failed: There is no consensus on what *the* meaning of QM is.

- Why did this program fail? That would be a talk in itself.

However, I believe we lack enough understanding of the theory to provide a conclusive interpretation. What is needed is *more understanding*; for we do not know what 'the quantum' is.

$\Longrightarrow$ I propose a new question: "**What is the quantum?**"

Better even: "What is essentially and uniquely quantum?"

This we do not know. But there are many recent breakthroughs.

Modern QM foundations (I):
Study QM 'from the outside, not just from the inside'

"What is essentially and uniquely quantum?"

Motto: Investigate theories that are neither classical nor quantum; explore the space of possible theories from a larger theoretical point of view.

> *"Is quantum mechanics an island in theory space?"* (Aaronson, 2004). If indeed so, where is it?

Modern QM foundations (I):
Study QM ‘from the outside, not just from the inside’

“What is essentially and uniquely quantum?”

Motto: Investigate theories that are neither classical nor quantum; explore the space of possible theories from a larger theoretical point of view.

> *“Is quantum mechanics an island in theory space?”* (Aaronson, 2004). If indeed so, where is it?

► It is found that many non-classical properties of QM are *generic* within the larger family of possible physical theories.

Modern QM foundations (I):
Study QM ‘from the outside, not just from the inside’

Thus rather than regard quantum theory special for having the generic ‘quantum’ properties, a better attitude may be to regard classical theories as special for *not* having them.

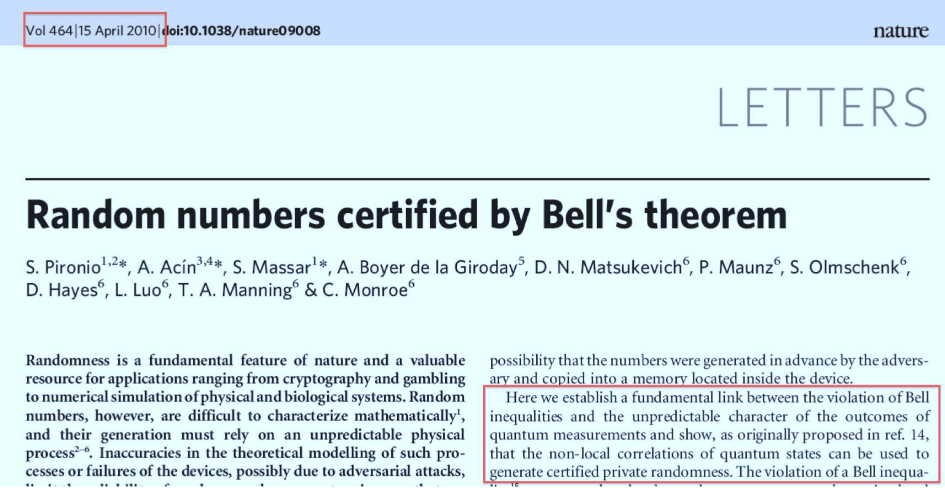
Example: *nonlocal, yet no-signalling correlations*.

► **New method**: reconstruction of quantum mechanics via operational approaches in non-classical probability theories.

Prospect: this might give us a new conceptual framework for post-quantum theories such as quantum gravity.

Modern QM foundations (II): Delivering resources for quantum information theory

In *Nature*, from last week:



Vol 464|15 April 2010|doi:10.1038/nature09008

nature

LETTERS

Random numbers certified by Bell's theorem

S. Pironio[1,2]*, A. Acín[3,4]*, S. Massar[1]*, A. Boyer de la Giroday[5], D. N. Matsukevich[6], P. Maunz[6], S. Olmschenk[6], D. Hayes[6], L. Luo[6], T. A. Manning[6] & C. Monroe[6]

Randomness is a fundamental feature of nature and a valuable resource for applications ranging from cryptography and gambling to numerical simulation of physical and biological systems. Random numbers, however, are difficult to characterize mathematically[1], and their generation must rely on an unpredictable physical process[2–6]. Inaccuracies in the theoretical modelling of such processes or failures of the devices, possibly due to adversarial attacks,

possibility that the numbers were generated in advance by the adversary and copied into a memory located inside the device.

Here we establish a fundamental link between the violation of Bell inequalities and the unpredictable character of the outcomes of quantum measurements and show, as originally proposed in ref. 14, that the non-local correlations of quantum states can be used to generate certified private randomness. The violation of a Bell inequa-

Modern QM foundations (II):
Delivering ingredients for quantum information theory

Inspired by truely foundational questions:
(Hardy & Spekkens: arXiv:1003.5008)

(1a) entanglement (EPR and Schrödinger questioning the completeness of QM (1935))

(1b) entanglement as a resource (Wootters asking himself 'how to derive the Born rule' (1980))

- *better metrology, decrease in computational complexity, novel information theoretic tasks*

(2) quantum parallelism (David Deutsch pondering over Everett's many world interpretation (1985))

- *fundamental for quantum computing*

Delivering resources for quantum information theory

(3) quantum teleportation (Asher Peres *et al.* thinking of joint measureability, and nonlocal quantum tomography (1993))

- *a primitive in quantum information*

(4a) nonlocal correlations (Bohm and Bell questioning the possibility of a (local) hidden variable completion of quantum mechanics (1956, 1964))

(4b) nonlocal no-signalling correlations (Popescu and Rohrlich ask "Why is quantum mechanics not more nonlocal?" (1996))

- *nonlocality is a resource for quantum secure keys, pure randomness, and quantum cryptography*

Recent fundamental breakthroughs

- Monogamy of non-local correlations as the principle behind the security of quantum cryptography. (*this talk*)
- Going beyond Heisenberg's uncertainty principle:
  - No nonlocal theory can exist that is no-signalling and allows perfect predictability of measurement outcomes. (*this talk*)
  - If quantum were more nonlocal it would violate the uncertainty relations. This holds in any no-signalling theory.
- There is limit on nonlocality in any world in which communication complexity is not trivial
- Measurements that are incompatible in quantum theory cannot be measured jointly in any other no-signalling theory.
- The study of correlations that need communication to be created, but that cannot be used to communicate. (a strictly weaker resource than communication)

Why physics needs quantum foundations

(Hardy & Spekkens: arXiv:1003.5008)

(1) Not just to tidy up the mess left behind after the physics has been done.

Rather it should be regarded as part and parcel of the great project of theoretical physics – to gain an ever better understanding of the world around us.

- Evidence: the compelling application in quantum information theory.

Why physics needs quantum foundations

(Hardy & Spekkens: arXiv:1003.5008)

(1) Not just to tidy up the mess left behind after the physics has been done.

Rather it should be regarded as part and parcel of the great project of theoretical physics – to gain an ever better understanding of the world around us.

- Evidence: the compelling application in quantum information theory.

(2) Quantum theory is likely not the end of the road. If we are to move beyond it, then it is important to know which parts can be changed or generalized or abandoned.

- *Speculation*: it might provide a mathematical framework that is rich enough to contain a theory of quantum gravity.

part II: nonlocal no-signalling correlations as a resource

Surface correlations: $P(a,b|A,B)$

Determined via measurement of relative frequencies.

Subsurface correlations: $P(a,b|A,B,\lambda)$

Generally inaccessible, conditioned on some physical state λ.

- Definitions of different kinds of bi-partite surface correlations:

a) **Local**: $P(a,b|A,B) = \int_\Lambda d\lambda\, \rho(\lambda)\, P(a|A,\lambda) P(b|B,\lambda)$.

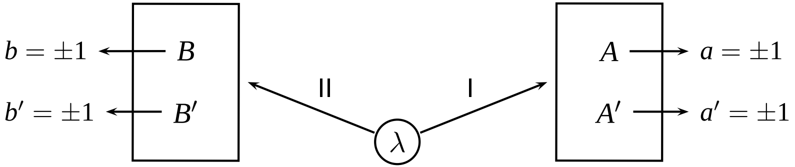
b) **Quantum**: $P(a,b|A,B) =$Tr$[\, M_a^A \otimes M_b^B\, \rho\,]$, $\sum_a M_a^A = \mathbb{1}$.

c) **No-signalling**: $P(a|A)^B = P(a|A)^{B'} := P(a|A)$

where $P(a|A)^B = \sum_b P(a,b|A,B)$, etc.

d) **Deterministic**: $P(a,b|A,B) \in \{0,1\}$.

Non-local correlations and Bell's inequality



– 'local causality': $P(a,b|A,B,\lambda) = P(a|A,\lambda)P(b|B,\lambda)$.

– Independence of the Source (IS): $\rho(\lambda|A,B) = \rho(\lambda)$.

- ▶ local causality ∧ IS $\implies P(a,b|A,B) = \int_\Lambda P(a|A,\lambda)P(b|B,\lambda)\rho(\lambda)d\lambda$

  (all correlations are *local correlations*)

- ▶ Consider the Bell-polynomial $\mathcal{B}_{ab} = AB + AB' + A'B - A'B'$, then

$$|\langle \mathcal{B}_{ab} \rangle_{\text{lhv}}| = |\langle AB \rangle_{\text{lhv}} + \langle AB' \rangle_{\text{lhv}} + \langle A'B \rangle_{\text{lhv}} - \langle A'B' \rangle_{\text{lhv}}| \leq 2$$

What is λ ? What is quantum nonlocality?

The variable λ: Don't think of λ as an old fashioned local hidden variable. Think of λ as the complete physical state of the systems as proposed by *any possible future theory*.

- For example, this could be QM with the identification $\lambda = |\,\psi\rangle$.

Bell's theorem is **general**: not based on the assumed truth of any particular candidate theory.

Quantum nonlocality: $\exists$ quantum state : $|\langle\mathcal{B}_{ab}\rangle_{\rm qm}| = 2\sqrt{2} > 2$.

$\Longrightarrow$ QM is nonlocal, but note: it does not allow no-signalling.

How to understand this quantum nonlocality?
(experimental metaphysics: not action but passion at a distance)

A result beyond QM

Theorem [Masanes et al. (2006)]: No physical theory can be deterministic, non-local and no-signalling.

$\Longrightarrow$ Any deterministic non-local correlation must be signalling.

$\Longrightarrow$ Any non-local correlation that is no-signalling must be indeterministic, i.e., the outcomes are only probabilistically predicted. (e.g., quantum mechanics, Bohmian mechanics)

Determinism, yet indeterminism

Now again consider Bohmian mechanics: because it obeys no-signalling and gives rise to non-local correlations it **must** predict the outcomes only probabilistically.

In other words, although fundamentally (at the deeper HV level) deterministic it must necessarily be predictively indeterministic.

Determinism, yet indeterminism

Now again consider Bohmian mechanics: because it obeys no-signalling and gives rise to non-local correlations it **must** predict the outcomes only probabilistically.

In other words, although fundamentally (at the deeper HV level) deterministic it must necessarily be predictively indeterministic.

► Thus no ‘Bohmian demon’ can have perfect control over the hidden variables and still be non-local and no-signalling at the surface (as QM requires).

- This is not specific to Bohmian mechanics, it holds for any such theory. And this is *independent* of whether the theory is required to reproduce QM.

Shareability and monogamy of classical and quantum states

What are the structural limitations in the way parts and wholes can be configurated according to physical theories?

- **To be presented**: a study of this question by focusing on the limitations set by physical theories on the *shareability* of subsystem states and of the correlations present in a composite system.

Or, can we build up particular composite systems (in particular configurations) by sharing/duplicating a subsystem, while maintaining the original configuration (of physical states and/or correlations) between the initial subsystems?

- If this is not possible this is referred to as 'monogamy'.

Monogamy of non-local no-signalling correlations

Suppose one has some no-signalling three-party probability distribution $P(a_1, a_2, a_3|A_1, A_2, A_3)$ for parties a, b and c.

- Then in case the marginal distribution $P(a_1, a_2|A_1, A_2)$ for ab is extremal it cannot be correlated to the third system c:

$$P(a_1, a_2, a_3|A_1, A_2, A_3) = P(a_1, a_2|A_1, A_2) \cdot P(a_3|A_3),$$

which implies that party c is completely uncorrelated with party ab: the extremal correlation $P(a_1, a_2|A_1, A_2)$ is completely *monogamous*.

Quantifying the monogamy of non-local correlations

Extremal no-signalling correlations thus show monogamy, but what about non-extremal no-signalling correlations?

- ▶ Non-extremal no-signalling correlations can be shared.

- Toner [2006] proved a tight trade-off relation:

$$|\langle \mathcal{B}_{ab} \rangle_{\text{ns}}| + |\langle \mathcal{B}_{ac} \rangle_{\text{ns}}| \leq 4.$$

For extremal no-signalling correlations: $|\langle \mathcal{B}_{ab} \rangle_{\text{ns}}| = 4$ so that necessarily $|\langle \mathcal{B}_{ac} \rangle_{\text{ns}}| = 0$, and vice versa (=monogamy), whereas non-extremal ones are shareable.

($|\langle \mathcal{B}_{ab} \rangle| = |\langle AB \rangle + \langle AB' \rangle + \langle A'B \rangle - \langle A'B' \rangle|$ quantifies nonlocality.)

Monogamy for other kinds of correlations

- For general unrestricted correlations no monogamy holds, i.e., $|\langle\mathcal{B}_{ab}\rangle|$ and $|\langle\mathcal{B}_{ac}\rangle|$ are not mutually constrained.
- Quantum correlations are monogamous: $\langle\mathcal{B}_{ab}\rangle^2_{\text{qm}} + \langle\mathcal{B}_{ac}\rangle^2_{\text{qm}} \leq 8$.
- Classical correlations are not monogamous. It is possible to have both $|\langle\mathcal{B}_{ab}\rangle_{\text{lhv}}| = 2$ and $|\langle\mathcal{B}_{ac}\rangle_{\text{lhv}}| = 2$.
- Separable quantum state are neither monogamous: $|\langle\mathcal{B}_{ab}\rangle_{\text{qm}}|, |\langle\mathcal{B}_{ac}\rangle_{\text{qm}}| \leq 2, \quad \rho \in \mathcal{Q}_{\text{sep}}$.

Monogamy of correlations

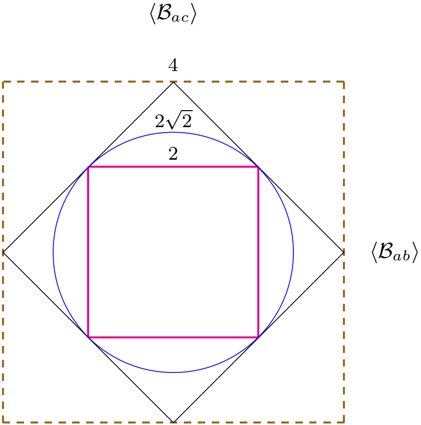
$$\mathcal{B}_{ab} = AB + AB' + A'B - A'B' \quad , \quad \mathcal{B}_{ac} = AC + A'C + AC' - A'C'$$

$|\langle \mathcal{B}_{ab} \rangle|, \ |\langle \mathcal{B}_{ac} \rangle| \le 4$

$|\langle \mathcal{B}_{ab} \rangle_{\text{ns}}| + |\langle \mathcal{B}_{ac} \rangle_{\text{ns}}| \le 4$ [a]

$\langle \mathcal{B}_{ab} \rangle^2_{\text{qm}} + \langle \mathcal{B}_{ac} \rangle^2_{\text{qm}} \le 8$ [b]

$|\langle \mathcal{B}_{ab} \rangle_{\text{lhv}}|, \ |\langle \mathcal{B}_{ac} \rangle_{\text{lhv}}| \le 2$ [c]


$\langle \mathcal{B}_{ac} \rangle$
4
$2\sqrt{2}$
2
$\langle \mathcal{B}_{ab} \rangle$

[a] Toner [2006]

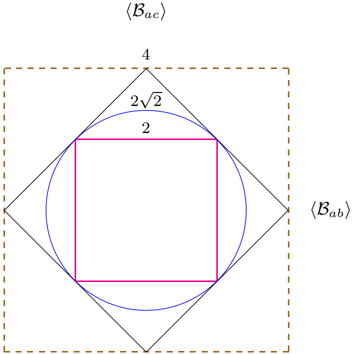
[b] Toner & Verstraete [2006]

[c] Bell [1964], CHSH [1969]

Consequences of this monogamy of correlations

In case the no-signalling correlations are non-local they can not be shared (it is impossible that both $|\langle\mathcal{B}_{ab}\rangle_{\text{ns}}| \geq 2$ and $|\langle\mathcal{B}_{ac}\rangle_{\text{ns}}| \geq 2$).

- ► The monogamy bound therefore gives a way of discriminating no-signalling from general correlations: if the bound is violated the correlations cannot be no-signalling (i.e., they must be signalling).
- ► Extremal quantum and no-signalling correlations are fully monogamous.
- ► This allows for secure key-distribution protocols that are based on the laws of physics only (and not on some computationally hard procedure).



$\langle\mathcal{B}_{ac}\rangle$
4
$2\sqrt{2}$
2
$\langle\mathcal{B}_{ab}\rangle$

Conclusion

Physics needs quantum foundations. Foundations research is essential for future developments.

Reasonable expectation: apart from quantum information theory there will be other great fruits from quantum foundations.

- For the construction of a theory of quantum gravity.
- New fields of research that we cannot currently think of.

Conclusion

David Mermin; attitude towards QM: “Shut up and calculate!”.

Suggestion for alternative slogan (Hardy & spekkens):

“**Shut up and contemplate!**”