Composite systems and their representation in quantum and classical physics

M.P. Seevinck

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

m.p.seevinck@uu.nl

March 2010

Background & Introduction

- I have an interest in, *firstly*, the study of the correlations between outcomes of measurements on subsystems of a composite system as predicted by a particular physical theory;

  secondly, the study of what this physical theory predicts for the relationships these subsystems can have to the composite system they are a part of;

  and, *thirdly*, the comparison of different physical theories with respect to these two aspects.

- The physical theories investigated and compared are generalized probability theories in a quasi-classical physics framework and non-relativistic quantum theory.

Background & Introduction

Motivation: a comparison of the relationships and predicted correlations between parts and whole as described by each theory yields a fruitful method to investigate what these physical theories say about the world.

Prospects: one then finds, independent of any physical model, relationships and constraints that capture (some of) the essential physical assumptions and structural aspects of the theory in question, i.e., a larger and deeper understanding of the different physical theories and of what they say about the world.

Today, I will not present a philosophical thesis, but only some of such structural aspects in quantum theory that could be used (by you) for new philosophical analysis.

Outline

~~(I) Composite systems and their state-space representation~~

- ~~in classical physics~~
- ~~in quantum mechanics~~
- now only some preliminaries

(II) Shareability and monogamy in classical and quantum systems

- monogamy of entanglement
- monogamy of (non-local) correlations

(III) Conclusion and discussion

Section I: Preliminaries

W.r.t. the general mereological structure of physical theories I will focus on:

1) the representation of composite systems and their subsystems on the state space of the physical theories under study.

2) the algebra of observables acting on the state space that provides us (loosely speaking) with the (dynamical) properties of the systems and the logic of true and false propositions about the systems in question.

Preliminaries: quantum physics

1. State space is a complex Hilbert space $\mathcal{H}$.

2. State space of a composite system is a *tensor product* of the individual state spaces: $\mathcal{H}_a \otimes \mathcal{H}_b$.

   (compare classically: state space Ω is a phase space or configuration space; composite state space is a *Cartesian product* of the individual state spaces: $\Omega_a \times \Omega_b$)

3. Pure states: rays $|\psi\rangle$ in $\mathcal{H}$.
   Mixed states: density operators on $\mathcal{H}$.

   (compare classically: pure physical states: points x on a phase space; mixed physical states: unique convex decomposition of pure states.)

Preliminaries: paradigmatic example

Consider a composite bipartite quantum system ab consisting of two subsystems a and b that has state space $\mathcal{H}_{ab} = \mathcal{H}_a \otimes \mathcal{H}_b$ (e.g., $\mathbb{C}^2 \otimes \mathbb{C}^2$).

Two types of bi-partite mixed states ρ_{ab}:

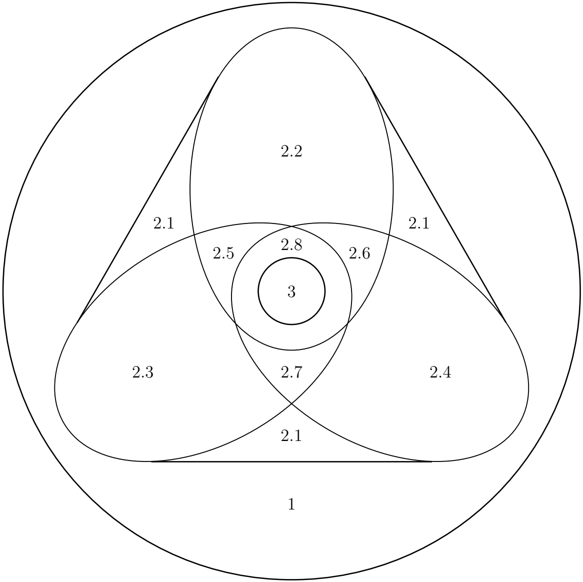
(a) <u>Separable states</u>: $\rho_{ab} = \sum_i p_i \rho_a^i \otimes \rho_b^i$

(special case: product states $\rho_{ab} = \rho_a \otimes \rho_b$)

(b) <u>Entangled states</u>: $\rho_{ab} \neq \sum_i p_i \rho_a^i \otimes \rho_b^i$

In a sense, the separable states correspond to the classical states, and the entangled states to the non-classical ones (the latter violate Bell inequalities, allow for nonclassical information theoretic tasks, etc.)

Separability structure of QM state space for $N = 3$



Section II: 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'.

Note: 'sharing' is not to be understood dynamical, but kinematical.

Monogamy of quantum states

Entanglement is monogamous

If a pure quantum state of two systems is entangled, then none of the two systems can be entangled with a third system.

1. Suppose that systems a and b are in a pure entangled state.
2. Then when the system ab is considered as part of a larger system, the reduced density operator for ab must by assumption be a pure state.
3. However, for the composite system ab (or for any of its subsystems a or b) to be entangled with another system, the reduced density operator of ab must be a mixed state.
4. But since it is by assumption pure, no entanglement between ab and any other system can exist.

Monogamy because of no-cloning

This monogamy can also be understood as a consequence of the linearity of quantum mechanics that is also responsible for the no-cloning theorem.

1. For suppose that party a has a qubit which is maximally pure state entangled to both a qubit held by party b and a qubit held by party c.
2. Party a thus has a single qubit coupled to two perfect entangled quantum channels.
3. This party could exploit this to teleport two perfect copies of an unknown input state, thereby violating the no-cloning theorem, and thus the linearity of quantum mechanics.

Mixed state entanglement can be shared

The W-state $|\psi\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ has bi-partite reduced states that are all identical and entangled.

- 'sharing of mixed state entanglement', or 'promiscuity of entanglement'.

Mixed state entanglement can be shared

The W-state $|\psi\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ has bi-partite reduced states that are all identical and entangled.

► 'sharing of mixed state entanglement', or 'promiscuity of entanglement'.

But this promiscuity is not unbounded: no entangled bi-partite state can be shared with an infinite number of parties.

Here a bi-partite state ρ_{ab} is said to be <u>N-shareable</u> when it is possible to find a quantum state $\rho_{ab_1 b_2 \ldots b_N}$ such that

$$\rho_{ab} = \rho_{ab_1} = \rho_{ab_2} = \ldots = \rho_{ab_N},$$

where ρ_{ab_k} is the reduced state for parties a and b_k.

• Fannes *et al*. [1988], Raggio *et al*. [1989]: A bi-partite state is N-shareable for all N (also called ∞-shareable) iff it is separable.

Quantifying the monogamy of entanglement

Coffman, Kundu and Wootters [2000] gave a trade-off relation between how entangled a is with b, and how entangled a is with c in a three-qubit system abc that is in a pure state:

$$\tau(\rho_{ab}) + \tau(\rho_{ac}) \leq 4\,\det\rho_a$$

with $\rho_a = \mathrm{Tr}_{bc}[|\,\psi\rangle\langle\,\psi|]$ and $|\,\psi\rangle$ the pure three-qubit state, where $\tau(\rho_{ab})$ is the tangle between A and B, analogous for $\tau(\rho_{ac})$.

The multi-partite generalization has been recently proven by Osborne & Verstraete [2006].

Interlude 1: Correlations in terms of joint probabilities

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

Determined via measurement of relative frequencies.

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

Generally inaccessible, conditioned on hidden variables.

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

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

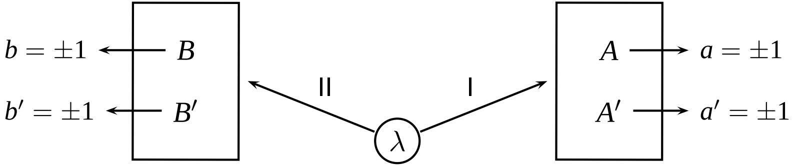
b) **Quantum**: $P(a,b|A,B) = \mathrm{Tr}[\, M_a^A \otimes M_b^B\, \rho\,]$, $\sum_a M_a^A = \mathbb{1}$.

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

Interlude 2: 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 $\wedge$ 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

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

Monogamy of non-local 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 (a vertex of the no-signalling polytope) it cannot be correlated to the third system c:

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

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*.

Note that this implies that all local Bell-type inequalities for which the maximal violation consistent with no-signalling is attained by a unique correlation have monogamy constraints. An example is the CHSH inequality, as will be shown below.

Quantifying the monogamy of non-local correlations

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

► Just as was the case for quantum states where non-extremal (mixed state) entanglement can be shared, non-extremal no-signalling correlations can be shared as well.

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

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

Extremal no-signalling correlations can attain $|\langle \mathcal{B}_{ab} \rangle_{\mathrm{ns}}| = 4$ so that necessarily $|\langle \mathcal{B}_{ac} \rangle_{\mathrm{ns}}| = 0$, and vice versa (this is monogamy of extremal no-signalling correlations), whereas non-extremal ones are shareable.

Monogamy for other kinds of correlations

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

- 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: $\langle\mathcal{B}_{ab}\rangle^2_{\mathrm{qm}} + \langle\mathcal{B}_{ac}\rangle^2_{\mathrm{qm}} \leq 8$.
- Classical correlations are not monogamous. It is possible to have both $|\langle\mathcal{B}_{ab}\rangle_{\mathrm{lhv}}| = 2$ and $|\langle\mathcal{B}_{ac}\rangle_{\mathrm{lhv}}| = 2$.
- Separable quantum state are neither monogamous: $|\langle\mathcal{B}_{ab}\rangle_{\mathrm{qm}}|, |\langle\mathcal{B}_{ac}\rangle_{\mathrm{qm}}| \leq 2$, $\rho \in \mathcal{Q}_{\mathrm{sep}}$.

(For orthogonal measurements a stronger bound holds: $\leq \sqrt{2}$)

Monogamy of correlations

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

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

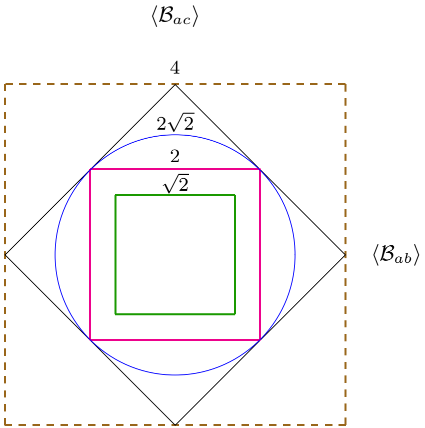
$|\langle\mathcal{B}_{ab}\rangle_{\text{ns}}| + |\langle\mathcal{B}_{ac}\rangle_{\text{ns}}| \leq 4$ [a]

$\langle\mathcal{B}_{ab}\rangle^2_{\text{qm}} + \langle\mathcal{B}_{ac}\rangle^2_{\text{qm}} \leq 8 \quad \rho \in \mathcal{Q}$ [b]

$|\langle\mathcal{B}_{ab}\rangle_{\text{lhv}}|, \ |\langle\mathcal{B}_{ac}\rangle_{\text{lhv}}| \leq 2$

For $A \perp A', B \perp B', C \perp C'$:

$|\langle\mathcal{B}_{ab}\rangle_{\text{qm}}|, \ |\langle\mathcal{B}_{ac}\rangle_{\text{qm}}| \leq \sqrt{2} \quad \rho \in \mathcal{Q}_{\text{sep}}$



[a] Toner [2006]

[b] Toner & Verstraete [2006]

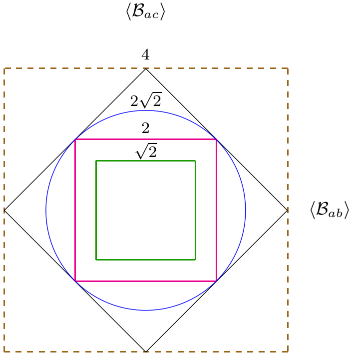
Consequences of this monogamy of correlations

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

- 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).



Shareability of correlations

A **general unrestricted distribution** $P(a, b_1|A, B_1, \ldots, B_N)$ is N-shareable with respect to the second party if an $(N+1)$-partite distribution

$$P(a, b_1, \ldots, b_N|A, B_1, \ldots, B_N)$$

exists, symmetric with respect to $(b_1, B_1), (b_2, B_2), \ldots, (b_N, B_N)$ and with marginals $P(a, b_i|A, B_1, \ldots, B_N)$ equal to the original distribution $P(a, b_1|A, B_1, \ldots, B_N)$, for all i.

- If a distribution is shareable for all N it is called ∞-shareable.

Analogously: **a no-signalling distribution** $P(a, b_1|A, B_1)$ is N-shareable if the $(N+1)$-partite distribution has marginals $P(a, b_i|A, B_i)$ equal to the original distribution $P(a, b_1|A, B_1)$, for all i.

Consider a general **unrestricted** correlation $P(a, b_1|A, B_1, \dots, B_N)$. We can then construct

$$P(a, b_1, \dots, b_N|A, B_1, \dots, B_N) = P(a, b_1|A, B_1, \dots, B_N)\delta_{b_1,b_2} \cdots \delta_{b_1,b_N},$$

which has the same marginals $P(a, b_i|A, B_1, \dots, B_N)$ equal to the original distribution $P(a, b_1|A, B_1, \dots, B_N)$. This holds for all i, thereby proving the ∞-shareability, i.e., it can be shared for all N.

If we restrict the distributions to be **no-signalling**, Masanes, *et al* [2006] proved that ∞-shareability implies that the distribution is local, i.e., it can be written as

$$P(a, b_1, \dots, b_N|A, B_1 \dots, B_N) = \int_\Lambda d\lambda p(\lambda) P(a|A, \lambda) P(b_1|B_1, \lambda) \cdots P(b_N|B_N, \lambda),$$

for some local distributions $P(a|A, \lambda), P(b_1|B_1, \lambda), \dots, P(b_N|B_N, \lambda)$ and hidden-variable distribution $p(\lambda)$.

local realism $\iff$ ∞-shareability of correlations

$\exists$ local model for $P(a, b|A, B)$ when party 1 has an arbitrary number and party 2 has N possible measurements

$\iff$

N-shareability of correlations

- Proof:

$\implies$ classical information can be cloned indefinitely.

$\impliedby$ Since $P(a, b|A, B)$ is shareable to N parties (labelled $\mathcal{B}_i$, $i = 1, \dots, N$), the correlations between A performed on party 1 and B_i on party 2 are the same as the correlations between measurements of A on party 1 and B_i on the extra party $\mathcal{B}_i$.

Therefore, the N measurements $B_1, \dots, B_N$ performed by party 2 can be viewed as one large measurement performed on the N parties $\mathcal{B}_i$ ($i = 1, \dots, N$). Lastly, there always exists a local hidden variable model when one of the two parties has only one measurement.

Interlude: Interpreting Bell's Theorem

- ► Schumacher [2008]: Bell's theorem is about the shareability of correlations; its real physical message is *not* about local realism, since we don't need ∞-shareable (i.e., local realism) to obtain the CHSH inequality that quantum mechanics violates.

- Claim: 2-shareability is sufficient to obtain the CHSH inequality ; and this is a weaker claim than the assumption of local realism.

Interlude: 2-shareability implies CHSH inequality

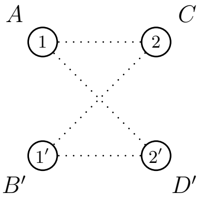
Consider an EPR-Bohm setup for parties 1 and 2.

Assume that all possible correlations between 1 and 2 are shareable to another party 1' and 2' that conceivably exist. Then for the outcomes:

$$a(c+d')+b'(c-d')=\pm 2$$

which implies for the expectation values

$$|\langle AC\rangle+\langle AD'\rangle+\langle B'C\rangle-\langle B'D'\rangle|\leq 2$$



2-shareability implies

$$|\langle AC\rangle+\langle AD\rangle+\langle BC\rangle-\langle BD\rangle|\leq 2$$

The shareability justifies the counterfactual reasoning.

Interlude: critique

1) Despite Schumacher's argument, it is indeed still the case that quantum mechanics is non-local in the sense that some quantum correlations cannot be given a factorisable form in terms of local correlations.

2) The argument is not logically weaker than standard derivations of Bell's theorem. For all that is needed to get Bell's theorem is the CHSH inequality, and in order to get this from the requirements of the doctrine of local realism we only need to assume that local realism holds *just* for measurement of four different observables: two for party 1 (e.g., A, A') and two for party 2 (e.g., B, B').

It is thus not necessary to assume full blown local realism for an *unlimited* number of observables and parties.

Section III: Discussion: Interpreting the world

Thus: according to modern physics the world is such that in general we encounter limits on the shareability of the subsystem-structure of composite systems.

- Indeed: local realism $\iff$ ∞-shareability of correlations

However, quantum correlations are not always shareable, let alone ∞-shareable. Furthermore, the same holds for more general no-signalling correlations.

$\Longrightarrow$ Technical breakthrough: such correlations can be used to distribute a secret key which is secure against eavesdroppers which are only constrained by the fact that any information accessible to them must be compatible with no-signalling, i.e., roughly the impossibility of arbitrarily fast signalling.

- Future work: What philosophical/metaphysical repercussions does all this have (if any)?