Information and disturbance in a physical theory

Giacomo Mauro D'Ariano   Paolo Perinotti   Alessandro Tosini

QUIT group, Physics Dept., Pavia University, and INFN Sezione di Pavia, via Bassi 6, 27100 Pavia, Italy

Any experiment is intended to provide information on a system via a measurement. However, as we learn from quantum theory, it is generally not possible to extract information without disturbing the state of the system or its correlations with other systems. The interplay between information and disturbance has been largely investigated as a quantum/classical divide and the *no-information without disturbance* theorem has been proved in quantum theory. The traditional notions of information and disturbance are deeply anchored to the properties of quantum theory. In particular, the notion of disturbance considers only the fate of the system state after the measurement. However, the fact that the system state is left untouched ensures that also correlations are preserved only in the presence of local tomography. We introduce a notion of disturbance that holds for an arbitrary theory and prove that a system satisfies no-information without disturbance if and only if the identical evolution cannot result form the coarse-graining of other operations. We then prove a structure theorem for probabilistic theories, showing that any system decomposes into a classical system and a system that satisfies no-information without disturbance. Via concrete examples we exhibit the independence of no-information without disturbance from other typical quantum features as local tomography and states purification.

The possibility that gathering information on a physical system could be affected by uncertainty relations was suggested by the Heisenbergs 1927 paper [1]. Despite the arguments in Ref. [1] were semiclassical, and then non rigorously retraced within the modern quantum framework, they strongly supported the crisis of classical physics posing the basis for a new mechanics, *quantum mechanics*.

The issue raised by Heisenberg spawned a vaste literature up to present days (see Refs. [2, 3] as recent reviews), leading to several quantifications of information and disturbance and of the corresponding tradeoff relations [4–7]. More recently, the limitations enclosed in the uncertainty relations have been recast into a striking feature of quantum theory named *no-information without disturbance* [8, 9]. The proof of the theorem relies on the structure of quantum theory and this prevents from deepening the logical relation between no-information without disturbance and the other quantum features. Among them we mention *local tomography*, namely the tomography of multipartite states via local measurements only; *purification*, namely every mixed state can be obtained as the reduced state of some pure state; and *causality*, which translates the Einstein causality principle into the framework of quantum theory.

The scenario here proposed for exploring the implication of *no-information without disturbance* in an arbitrary physical theory is that of *operational probabilistic theories*. These are a setting where an arbitrary experiment corresponds to a collection of events (preparation of states, transformations and measurements) connected each other by links, which in turn represent physical systems. A theory must provide i) the rule for composing events and ii) the probabilities for any possible resulting experiment. Quantum theory and classical theory are two instances of operational probabilistic theories.

Following the experience of quantum theory, the definitions of information and disturbance involved in an experiment have been investigated for theories that satisfy local tomography, purification and causality [10–13] and for those theories the no-information without disturbance has been proved in Ref. [9]. In this work we point out the weakness of the already existing approaches in describing the information-disturbance relation in physically relevant cases. It is usually assumed that an experiment

Submitted to:
SOS 2007

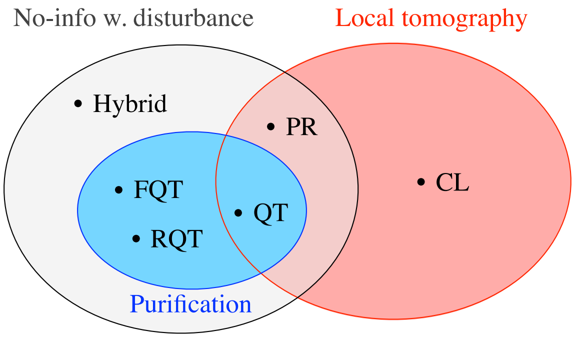

Figure 1: Comparing theories that satisfy no-information without disturbance (grey set), local tomography (red set) and purification (blu set). Quantum theory (QT) lies at the intersection of the three sets. We prove that the purification set is a proper subset of no-information without disturbance. PR-boxes theory (PR) are an example that satisfies no-information without disturbance but violates purification. Moreover, PR-boxes provide a non-trivial intersection between local tomography and no-information without disturbance in the absence of purification. We observe that no-information without disturbance is independent of local tomography and viceversa (classical theory (CL) satisfies only local tomography while Fermionic quantum theory (FQT) and real quantum theory (RQT) satisfy only no-information without disturbance. One can finally build Hybrid theories that violate both purification and local tomography but satisfy no-information without disturbance.

do not disturbe a system if it behaves overall as the identity for the given system, disregarding the effects of the experiment on the environment (possible ancillary systems). Whilst this definition captures the operational meaning of disturbance in quantum theory, it cannot be consistently applied to theories that lack local tomography. A significative physical example is that of Fermions [14] where, due to the parity superselection rule, an operation that do not disturb a buch of Fermions still could affect their correlations with other particles. This issue can be cured asking a non-disturbing experiment to preserve also the purifications of the states at hand. This proposal [9], which is general enough to capture the operational meaning of disturbance for Fermionic systems, is still unsatisfactory, because it cannot describe disturbance in models that do not enjoy purification, e. g. the classical theory of information.

We define disturbance in the framework of operational probabilistic theory, thus also for theories without local tomography, purification and causality. Given a system, and an operation on it, the effects of such operation on any possible *dilation* (non necessarily pure) of the states of the system are taken into account. We then prove a necessary and sufficient condition for a theory to satisfy no-information without disturbance. The condition is the impossibility of realizing the identity evolution of systems as a coarse-graining of more elementary operations. A theory might satisfy no-information without disturbance only if restricted to some collection of states, therefore we also provide a weaker necessary and sufficient condition for this to happen.

As for the Heisenberg uncertainty relations, no-information without disturbance has been considered as a quantum/classical divide and then as a characteristic quantum trait. We observe that no-information without disturbance is instead independent of most of the other features of quantum theory. We prove a structure theorem stating that any system of a probabilistic theory decomposes into a classical part and a part that satisfies no-information without disturbance, classifying this last one as a divide between classical theory and any other in principle admissible theory.

The results in this manuscript are expected to have an immediate application in the field of secure key-distribution. Indeed, a physical theory including a system (or evan a part of it, as a set of states) that satisfies no-information without disturbance is likely to guarantee an unconditionally secure channel for distributing secrete messages. The idea of studying secure key-distribution in a framework more general than the classical and the quantum ones was already proposed in Refs. [10, 12]. The present generalization of the no-information without disturbance relation to arbitrary theories represents a step forward in proving the conjecture that secure key-distribution should be possible in any non-classical theory [10].

References

[1] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3):172–198, Mar 1927.

[2] Paul Busch, Pekka Lahti, and Reinhard F. Werner. Colloquium: Quantum root-mean-square error and measurement uncertainty relations. *Rev. Mod. Phys.*, 86:1261–1281, Dec 2014.

[3] Masanao Ozawa. Uncertainty relations for noise and disturbance in generalized quantum measurements. *Annals of Physics*, 311(2):350 – 416, 2004.

[4] Christopher A. Fuchs and Asher Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Phys. Rev. A*, 53:2038–2045, Apr 1996.

[5] Lorenzo Maccone. Information-disturbance tradeoff in quantum measurements. *Phys. Rev. A*, 73:042307, Apr 2006.

[6] Giacomo Mauro D'Ariano. On the heisenberg principle, namely on the information-disturbance trade-off in a quantum measurement. *Fortschritte der Physik: Progress of Physics*, 51(4-5):318–330, 2003.

[7] Christopher A. Fuchs and Kurt Jacobs. Information-tradeoff relations for finite-strength quantum measurements. *Phys. Rev. A*, 63:062305, May 2001.

[8] Paul Busch. *"No Information Without Disturbance": Quantum Limitations of Measurement*, pages 229–256. Springer Netherlands, Dordrecht, 2009.

[9] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Phys. Rev. A*, 81:062348, Jun 2010.

[10] Jonathan Barrett. Information processing in generalized probabilistic theories. *Physical Review A*, 75(3):032304, 2007.

[11] Gen Kimura, Koji Nuida, and Hideki Imai. Distinguishability measures and entropies for general probabilistic theories. *Reports on Mathematical Physics*, 66(2):175 – 206, 2010.

[12] Howard Barnum and Alexander Wilce. Information processing in convex operational theories. *Electronic Notes in Theoretical Computer Science*, 270(1):3 – 15, 2011. Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008).

[13] Teiko Heinosaari, Leevi Leppäjärvi, and Martin Plávala. No-free-information principle in general probabilistic theories. *arXiv preprint arXiv:1808.07376*, 2018.

[14] G. M. D'Ariano, F. Manessi, P. Perinotti, and A. Tosini. Fermionic computation is non-local tomographic and violates monogamy of entanglement. *EPL (Europhysics Letters)*, 107(2):20009, jul 2014.