Contents lists available at ScienceDirect

Studies in History and Philosophy of Modern Physics

journal homepage: www.elsevier.com/locate/shpsb

How device-independent approaches change the meaning of physical theory

Alexei Grinbaum

CEA-Saclay/IRFU/LARSIM, 91191 Gif-sur-Yvette, France

ARTICLE INFO

Article history:
Received 15 March 2017
Accepted 17 March 2017
Available online 31 March 2017

ABSTRACT

Dirac sought an interpretation of mathematical formalism in terms of physical entities and Einstein insisted that physics should describe “the real states of the real systems”. While Bell inequalities put into question the reality of states, modern device-independent approaches do away with the idea of entities: physical theory may contain no physical systems. Focusing on the correlations between operationally defined inputs and outputs, device-independent methods promote a view more distant from the conventional one than Einstein's ‘principle theories’ were from ‘constructive theories’. On the examples of indefinite causal orders and almost quantum correlations, we ask a puzzling question: if physical theory is not about systems, then what is it about? Device-independent models suggest that physical theory can be ‘about’ languages.

1. Introduction

Often hailed as a “second quantum revolution” (Aspect, 2004), the introduction of correlation inequalities by Bell (1964) inaugurated a conceptual development whose significance took several decades to be fully appreciated. We submit that this revolution reaches a surprising summit with the development of device-independent approaches and model-independent physics, supporting a new view of physical theory.

Quantum mechanics describes the evolution of a system under a particular Hamiltonian and the results of measurements operated on this system by the observer. The concept of observer is external to the theory. Whatever its physical constitution, the observer's only role is to choose a measurement setting and register the result of the observation: an operational approach. The correlations between the observer's choices and results are intuitively taken to be mediated by information carriers: physical systems. On one view, systems are “lines” or “wires” between “boxes” in symbolic diagrams connecting various operations on the observer's information—a conception that leads to “new modes of explaining physical phenomena” (Coecke, 2010; Coecke & Duncan, 2011; Coecke, Paquette, & Pavlovic, 2010). The old explanatory mode, on the contrary, takes systems to be constituted through separation from non-systems (measurement devices or the environment): a system is a bouquet of relevant degrees of freedom jointly denoted by a single name. That such a division, although it is not a *definition* (more on this in Section 4), enables *explanation* is an idea with a long philosophical history (διεῖλεν from διαιρέω, to take apart, Plato *Timaeus* 41d). We argue, firstly, that the old explanatory mode does not apply to device-independent approaches. Secondly, in the new explanatory mode systems become auxiliary concepts and, like any accessory tool, have limited utility. Still occasionally employed in the literature, they represent little more than a remnant of the old regime. Our examples will show that, while it is not always outright wrong, thinking about physics in terms of systems sometimes hinders rather than facilitates understanding. It is significant, then, that the new explanatory mode can produce a physical theory that does not refer to systems at all.

In quantum mechanics, it is assumed that a measurement setting is chosen in earnest, i.e., the observer trusts the system to be constituted of precisely the degrees of freedom described by the theory. What the system is, is known in advance and is correct. For example, if one performs a binary measurement of photon polarization, then one expects *a priori* that the measurement device will indeed measure photons. This trust in preparation devices is usually not subject to theoretical scrutiny, yet it is in principle—and often experimentally—unfounded.

The problem of trust contains a further aspect. If the distinction between a system and a measurement device is fixed within one

E-mail address: alexei.grinbaum@cea.fr

http://dx.doi.org/10.1016/j.shpsb.2017.03.003
1355-2198/© 2017 Elsevier Ltd. All rights reserved.

laboratory, then it is usually taken for granted that all other laboratories, should they come to observe the processes in the first one, will make the same distinction along the same separation line. The identity of the system does not depend on the observer; only its state may vary in relation to the observe'r's choice of measurement. The “Wigner's friend” Gedankenexperiment (Wigner, 1961) assumes that different observers will agree on system identification but disagree on state ascriptions. It is understandable that this agreement may be a matter of unassailable trust between friends; it has been put into question and studied mathematically only recently (Grinbaum, 2013; Pienaar, 2016).

Absence of trust is a concern that quantum cryptography is designed to address. It has tools for working with systems of “unspecified character” (Bancal, Gisin, Liang, & Pironio, 2011) or “unknown nature” (Bardyn, Liew, Massar, McKague, & Scarani, 2009). A device-independent approach employs such tools: it is a theoretical investigation performed without relying on the knowledge of the laws governing the systems’ behaviour. A conventional ‘device’ refers here to any process or apparatus described by an operational theory, whether classical or quantum, which is explicitly designated. In this sense, not only a conventional optical table but something as strange as a closed timelike curve (Deutsch, 1991; Bennett, 2005) or a Malament–Hogarth spacetime (Earman & Norton, 1993; Hogarth, 1992) may be seen as a device. This terminology was first introduced by Mayers and Yao (1998), who developed device-independent quantum cryptography with imperfect sources. Their suggestion was to render, through a series of tests, an untrusted but “self-checking” source equivalent to an ideal one that can be trusted *a priori*. These tests do not rely on the degrees of freedom pertinent to the system or, to put it differently, on our knowledge of the physical theory that describes their evolution. They only involve inputs and outputs at two separate locations: a device-independent protocol (Section 2). Over the years quantum cryptography has developed an array of such methods for dealing with adversaries which, via action upon sources, effectively turn systems into untrusted entities. Device-independent protocols are important for randomness generation (Colbeck, 2006; Pironio et al., 2010), quantum key distribution (Barrett, Hardy, & Kent, 2005), estimation of the states of unknown systems (Bardyn et al., 2009), certification of multipartite entanglement (Bancal et al., 2011), and distrustful cryptography (Aharon, Massar, Pironio, & Silman, 2015).

Some of these cryptographic protocols have found a broader use in quantum information, e.g. device-independent tests are performed on Bell inequalities, on the assumption that superluminal signaling is impossible (Bancal, 2013), or on the existence of a predefined causal structure (Section 3). But the import of device-independent methods extends even further. Device-independent methods convert the usually implicit trust of the observer into a theoretical problem. By doing so, they erase one of the main dogmas of quantum theory: that it deals with systems. To appreciate the significance of this shift, we compare it with another paradigmatic change captured by Einstein in the form of a distinction between principle and constructive theories (Section 4).

This shift is not only due to the import of device-independent methods from quantum cryptography into general quantum physics. If these methods have indeed triggered the development, the latter had been prepared by the reconstructions of quantum theory (Section 5). Operational axiomatic approaches to quantum mechanics focus on the inputs and outputs of the observer: a “box” picture. The postulates that successfully constrain the box to behave according to the rules of quantum theory become our best candidates for fundamental principles of Nature. In a device-independent approach, such postulates are also at work: they are the only content of physical theory along with the inputs and the outputs of the parties.

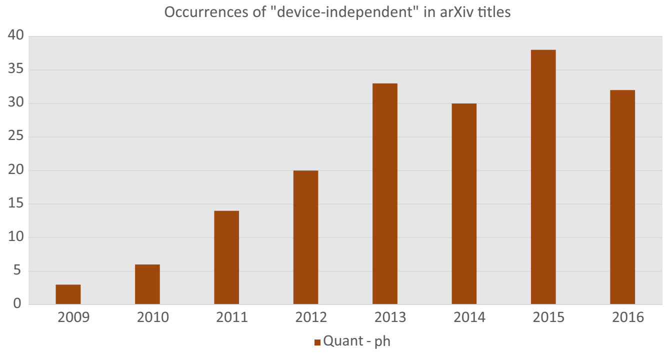

Fig. 1. Occurrences of the term “device-independent” in the titles of arXiv physics preprints.

Incompatible with the old explanatory mode, device-independent models typically do not meet the conditions for the emergence of robust theoretical constituents corresponding to real objects. By allowing no room for systems, they inaugurate the obsolescence of this elementary building block: a theory may contain no systems but remain physical. The spread of this view from quantum cryptography to general quantum physics (Fig. 1) raises a question of meaning: if a physical theory is not about systems, what is it about? This requires a philosophical (Section 6) as well as a mathematical (Section 7) investigation. Device-independent models suggest a possible answer: a physical theory can be ‘about’ languages (Section 8). Not only is such a theory possible; perhaps it indicates the right direction for moving beyond quantum theory.

2. Physics in a box

Device-independent models are defined as a set of n parties, each of which ‘selects’ a measurement setting or ‘places’ an input value $x_1 \in \mathcal{X}_1, \ldots, x_n \in \mathcal{X}_n$ respectively, and ‘subsequently’ ‘obtains’ an output value or a measurement result $a_1 \in \mathcal{A}_1, \ldots, a_n \in \mathcal{A}_n$. The sets $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{A}_1, \ldots, \mathcal{A}_n$ are alphabets of finite cardinality. The verbs used in these expressions merely convey an operational meaning of the inputs and outputs; they do not imply that any party exercises free will or has conscious decision-making procedures. The term ‘subsequently’ introduces a local time arrow pointing from each party's input to its output. Although such local time arrows seem quite intuitive, in full generality they need not be assumed either. A fully general setting requires, therefore, that absolutely nothing be postulated about the way inputs are transformed into outputs, except two conditions: (a) these two types of data are clearly distinguished; (b) the process of transformation is physical. Physics is contained in the probability distribution $\mathbf{p} = P(a_1, \ldots, a_n | x_1, \ldots, x_n)$ (Fig. 2).

All device-independent models studied in the literature

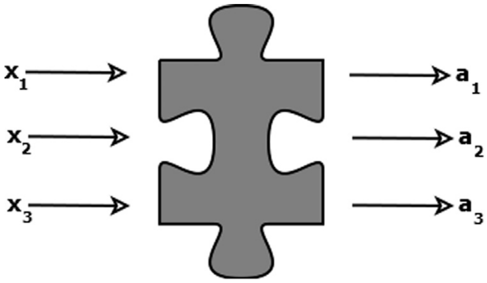

Fig. 2. In the case of $n=3$ parties, physics is fully contained in the probabilities $\mathbf{p} = P(a_1a_2a_3|x_1x_2x_3)$.