PUBLISHED ONLINE: 1 APRIL 2014 | DOI: 10.1038/NPHYS2916
nature physics

Nonlocality beyond quantum mechanics

Sandu Popescu

Nonlocality is the most characteristic feature of quantum mechanics, but recent research seems to suggest the possible existence of nonlocal correlations stronger than those predicted by theory. This raises the question of whether nature is in fact more nonlocal than expected from quantum theory or, alternatively, whether there could be an as yet undiscovered principle limiting the strength of nonlocal correlations. Here, I review some of the recent directions in the intensive theoretical effort to answer this question.

Quantum mechanics is, without any doubt, our best theory of nature. Apart from gravity, quantum mechanics explains virtually all known phenomena, from the structure of atoms, the rules of chemistry and properties of condensed matter to nuclear structure and the physics of elementary particles. And it does all this to an unprecedented level of accuracy. Yet, almost 80 years since its discovery, there is a general consensus that we still lack a deep understanding of quantum mechanics. Indeed, novel, puzzling and even paradoxical situations are frequently discovered. And I'm not talking about the well-known interpretational puzzles related to the measurement problem, but about a variety of quantum effects, from the Aharonov–Bohm effect[1], which was hidden in plain sight, to Bell inequality violations[2], to the multitude of strange effects related to entanglement and quantum information. They are all puzzling and paradoxical only because we do not yet have the intuition and understanding that would allow us to predict and expect them.

Surprisingly however, with very few notable exceptions, for many years research on the fundamental aspects of quantum mechanics was put on the back burner; there seemed to always be more important, pressing issues. During the past couple of years, however, there has been a strong renewed interest in the subject and there seems to be hope that we will finally reach a much deeper understanding of the nature of quantum mechanics. In what follows, I will describe a small part of this research.

As was noted long ago, the axioms of quantum mechanics are far less natural, intuitive and 'physical' than those of other theories, such as special relativity. Special relativity can be completely deduced from two axioms: (1) all inertial frames of reference are equivalent and (2) there is a finite maximum speed for propagations of signals. Contrast these with the very mathematical and physically obscure axioms of quantum mechanics: every state is a vector in a complex Hilbert space, every observable corresponds to a Hermitian operator acting on that Hilbert space, and so on. Furthermore, when trying to make physical statements about nature, they are all sort of negative: nature is uncertain, we cannot predict the result of a measurement, if we measure this we disturb that, and so on. Clearly there is no way to reconstruct the whole theory from such physical statements. Yet, there is a glimmer of hope. As both Aharonov (ref. 3 and personal communication) and Shimony[4] independently noticed, the fundamental non-determinism of quantum mechanics, one of the most unpleasant aspects of the theory and the very subject of Einstein's famous complaint "God doesn't play dice", actually plays a positive role: it opens the window to a new phenomenon — nonlocality. And Aharonov even went a step further (ref. 3 and personal communication). He remarked that it is possible, in principle, to have a theory that is non-deterministic without being nonlocal. On the other hand, it is impossible to have a nonlocal theory that respects relativistic causality but is deterministic. Indeed, very roughly speaking, if by moving something here, something else instantaneously wiggles there, the only way in which this doesn't lead to instantaneous communication is if that 'wiggling thing' is uncertain and the wiggling can be only spotted *a posteriori*. The bottom line, therefore, is that if we take nonlocality to be the starting point, then fundamental non-determinism — the most characteristic property of quantum mechanics — immediately follows as a consequence. Hence, we should consider nonlocality and not non-determinism as a basic axiom of quantum mechanics.

In the years following Aharonov and Shimony's suggestion and due to the advent of quantum information and the extremely intense study of entanglement in particular, nonlocality came indeed to be appreciated as a fundamental property of nature. Yet, there is an even more interesting twist in the story. Rohrlich and I[5] took the Aharonov–Shimony suggestion seriously and investigated whether or not quantum mechanics can be deduced from the axioms of (1) relativistic causality and (2) the existence of nonlocality. In other words, we asked: "Is quantum mechanics the unique theory that allows for nonlocal phenomena consistent with special relativity?" Surprisingly, we discovered that this is not the case: nature could be even more nonlocal than that quantum mechanics predicts, yet be fully consistent with relativity! This immediately raises two questions. Perhaps nature is indeed more nonlocal than is described in quantum mechanics says, but we haven't yet observed such a situation experimentally. Alternatively, if such stronger nonlocal correlations do not exist, why don't they? Is there any deep principle that allows for nonlocality but limits its strength? This Review is dedicated to reporting the very intense present research into this question.

Before going forward, I want to reiterate that the scope of this Review is, by necessity, very limited and what is presented here is only a small part of a much larger effort to understand the foundations of quantum mechanics that is going on at present. To start with, I would like to mention the intensive work in characterizing quantum nonlocality itself[6–25], where not even the simple algebraic question — of fundamental importance — of which nonlocal correlations can be obtained from quantum mechanics is yet completely solved; see seminal works by Tsirelson[26–29] (Cirel'son) as well as others[30,31]. Another interesting direction is that of generalized probabilistic theories[32–38]. I also cannot cover the fascinating flow of ideas back from this research into quantum information theory, where it has led to a variety of new ideas, concepts and applications, out of which I would like to mention the newly emerged area of device-independent physics (including device-independent key distribution[39–49] and device-independent randomness generation[50–60]). A recent review article[61] covers these results and many more in detail. Further afield, I would like to single out the intense activity in searching for natural axioms of quantum mechanics along the lines initiated by Hardy[62–69]. Finally,

H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, UK. e-mail: S.Popescu@bristol.ac.uk

I would like to mention a completely different type of nonlocality, namely dynamic nonlocality[70].

Model-independent statements about physics

Physics is usually discussed in very concrete terms, indicating the systems of interest and the specific interactions between them. A very important recent development, however, was the realization that physics can also be presented in a 'model independent' way, that is, in a way that is largely independent of the details of the specific underlying theories; this allows one to compare various possible theories.

For our purpose, it is very convenient to view experiments as input–output black-box devices. Every experiment can be viewed as a 'black box'. For example, suppose Alice has a box that accepts inputs x and yields outputs a (Fig. 1). One can imagine that inside the box there is an automated laboratory, containing particles, measuring devices, and so on. The laboratory is prearranged to perform some specific experiments; the input x simply indicates which experiment is to be performed. Suppose also that for every measurement we know in advance the set of the possible outcomes; the output a is simply a label that indicates which of the results has been obtained. In this framework, the entire physics is encapsulated in $P(a|x)$, the probability that output a occurs given that measurement x was made.

In our discussion, we are interested in the constraints that relativistic causality imposes on experiments carried out by two parties, Alice and Bob, who are situated far from each other. The physics is encapsulated in $P(a,b|x,y)$, the joint probability that Alice obtains a and Bob obtains b when Alice inputs x and Bob inputs y. We are interested in the case when the experiments of Alice and Bob are space-like separated, that is, each experiment takes place before any information about the other's input and output could reach it. We allow, however, the boxes to have been prepared long in advance, so that they could have been prepared in some correlated way, and they may also be connected by radios, telephone cables and so on. Also, obviously, to determine the joint probability, we need time to collect the entire information in one place.

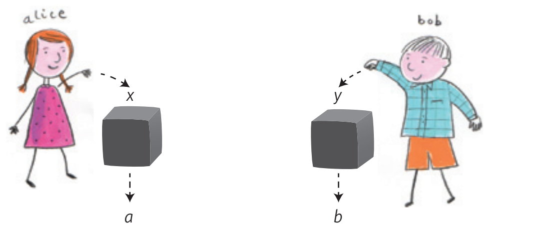
Nonlocality

Consider the simple case when x, y, a and b have only two possible values, conventionally denoted 0 and 1. Suppose that Alice and Bob would like to construct some boxes that will yield outputs a and b such that:

$$a \oplus b = xy \qquad (1)$$

where $\oplus$ denotes addition modulo 2 (that is, $a \oplus b = 0$ if $a = 0$ and $b = 0$ or $a = 1$ and $b = 1$ and $a \oplus b = 1$ if $a = 0$ and $b = 1$ or $a = 1$ and $b = 0$). In simple terms, what the above equation says is that when the inputs are $x = y = 1$, the outputs must be different from each other, whereas for any other pair of inputs, the outputs must be equal to each other. The question is, how well can they succeed?

Suppose, without loss of generality, that Alice and Bob pre-arrange that if $x = 0$ then Alice's box yields $a = 0$. Now, to ensure that they win the game when the inputs are $x = 0$ and $y = 0$, they obviously must arrange that when $y = 0$ Bob's box should yield $b = 0$. Furthermore, to ensure success when $x = 0$ and $y = 1$, they must also arrange that when $y = 1$ Bob's box must also yield $b = 0$. Now, as Bob's box will yield $b = 0$ when $y = 0$, to ensure success if the inputs are $x = 1$ and $y = 0$, Alice's box must be such that it yields $a = 0$ when $x = 1$. But by now we have fixed the behaviour of both boxes for all the inputs. And we have a problem: if $x = 1$ and $y = 1$ the outputs will be $a = 0$ and $b = 0$, which constitutes a failure. Hence for one in four inputs, Alice and Bob fail. If the inputs x and y are given at random, 0 and 1 with equal probability, then Alice and Bob's probability of success is at most 3/4.



ANNA I. POPESCU

Figure 1 | The black-box model of two experiments. Each black box is a whole laboratory. The inputs, x and y, are instructions indicating the experiment to be performed in the box and a and b are the outcomes of the experiments.

Of course, if the boxes could communicate with each other, then they could always succeed: Alice's box tells Bob's something like, "My input was $x = 0$, I output $a = 0$, take care what you do!". But, the whole point of the set-up was that Alice and Bob's experiments are space-like separated from each other, so any such signal would have to propagate faster than light. The upper bound of 3/4 on the probability of success derives from 'locality' (that is, no superluminal communication between the boxes), and it is called a Bell inequality[2]. There are many different Bell inequalities, describing constraints derived from locality in similar tasks; the particular one discussed here is the Clauser–Horne–Shimony–Holt (CHSH) inequality[71].

John Bell's seminal discovery[2] was that if the boxes contain quantum particles prepared in an appropriate entangled quantum state, and if appropriate measurements are performed on them, one can arrange a situation such that the probability of success of the above game is larger than 3/4.

Quantum particles, therefore, somehow communicate with each other superluminally. One could wonder if this doesn't immediately contradict Einstein's relativity. Here is precisely where the probabilistic nature of quantum mechanics comes into play. All that Alice and Bob can immediately see are the probabilities of their experiments; to learn the joint probabilities takes time. Suppose, for example, that for Alice the outcomes $a = 0$ and $a = 1$ are equally probable, regardless of what x and y are. Then Bob has no way of signalling superluminally to Alice: all he can do is to choose the value of y, but this doesn't affect the probabilities of Alice's outcomes. Similarly, Alice could also be prevented from signalling to Bob. So, in Shimony's words, the probabilistic nature of quantum mechanics allows for the "peaceful co-existence of relativity and nonlocality": the particles could communicate to each other superluminally, but the experimentalists cannot use them to communicate superluminally with each other.

Nonlocality beyond quantum mechanics

As discussed above, quantum mechanics allows for a probability of success larger than 3/4 in the correlation game, meaning that the boxes (or the particles contained within) somehow communicate superluminally with each other. This is now recognized as being one of the most important aspects of quantum mechanics. However, quantum mechanics cannot always win in the game — the quantum probability of success is at most $(2 + \sqrt{2})/4$, as proved by Cirel'son[29]. That this is the case is a simple consequence of the Hilbert-space structure of quantum mechanics. But the deeper question is, why?[5] Is there a deep principle of nature that limits the amount of nonlocality?

The first guess was that stronger nonlocal correlations would be forbidden by relativistic causality; perhaps the randomness that provides the umbrella under which nonlocality can coexist with relativistic causality is not enough to allow for stronger nonlocality. So the very first question to ask is: could — theoretically — nonlocal

NATURE PHYSICS DOI: 10.1038/NPHYS2916

Box 1 | Eliminating communication redundancy.

Suppose Alice associates a variable x_i with each of her days, $i = 1 \ldots 365$ with $x_i = 0$ if she is busy and $x_i = 1$ if she is free. Similarly, Bob defines y_i. Now, Alice and Bob could meet on the ith day if and only if the product $x_i y_i = 1$. To find out if the number of days when they can meet is even or odd, all Alice must do is establish whether the sum of the products $\Sigma_i x_i y_i$ is even or odd. Suppose now that Alice and Bob use their variables as inputs into PR boxes. By definition, PR boxes yield a_i and b_i such that the sum $a_i + b_i$ is even (odd) if the product $x_i y_i$ is even (odd). Hence, the sum of the products, $\Sigma_i x_i y_i$, is even (odd) if and only if the sum of all outputs $\Sigma_i a_i + b_i$ is even (odd). To find this out, all Alice needs to know from Bob is if the sum of his outputs, $\Sigma_i b_i$ is even or odd, that is, a single bit of information.

correlations stronger than quantum mechanical ones exist, without violating relativity? When Bell discovered nonlocality, the problem was not formulated in a model-independent way but by using the specific language of quantum mechanics: entangled quantum states, Hermitian operators, eigenvalues and so on. From this point of view, the very question of whether or not nonlocal correlations stronger than the quantum mechanical ones could exist was very difficult to even envisage, let alone to answer. In the above box framework, however, the question and its answer are almost trivial: as long as locally a and b are 0 or 1 with equal probability, there is nothing that prevents the game from being won with certainty. These particular correlations are now known as Popescu–Rohrlich (PR) boxes[5,72].

Super-quantum correlations

The existence of super-quantum nonlocal correlations shows that quantum mechanics cannot be deduced from the two axioms of (1) relativistic causality and (2) the existence of nonlocal correlations. Something else is needed. But what? What could be a supplementary, very natural, axiom that could rule out such correlations?

The statement that super-quantum correlations could — in principle — exist is very far from a fully fledged physical theory. Therefore, it may seem very unlikely that one could make further progress in answering the above question before such a full theory, which could explain all the known results — hydrogen atoms and so on — but also incorporate super-quantum correlations, is formulated. Surprisingly enough, it turns out that there is a lot one can do with even just the above particular example. Help came at first from computer science, and now this is one of the hottest areas in the foundations of physics. Various very interesting situations have been discussed, including communication complexity[73,74], nonlocal computation[75], information causality[76], macroscopic locality[77], local orthogonality[78] and nonlocality swapping[79]. In this Review, I will discuss only a few examples.

Communication redundancy

Almost all of our communication is redundant, and that is not only because some of us like to talk too much, but also because it is a law of nature. Indeed, consider the following problem. Suppose Alice and Bob would like to meet, but are both very busy. They speak on the telephone and try to find a day this year when they could meet. To make the problem more interesting, suppose that they do not want to find out a precise day, but first they want to establish whether the number of days when they could meet is even or odd (zero counting as even). To make the problem simpler, suppose it is only Bob that sends information to Alice, and Alice has to decide the result. The question is, how much information must Bob send to Alice?

We have now a problem in which the result is a single bit, a single yes or no answer: yes = even, no = odd. On the other hand, it is obvious that Bob needs to inform Alice about the status of each day of the year in his calendar. Indeed, one of the possible situations is that Alice is free only one single day. To decide whether they can meet or not, she has to know whether Bob is free that day; as Bob doesn't know anything about Alice's calendar, he has to tell her about each of his days. He has therefore to send Alice 365 bits of information, a 'yes = I'm free' or 'no = I'm not free' for each day of the year; all this for Alice to find out a single bit of information. Very redundant indeed.

Clearly, in the process Alice learns much more than what she wanted to know. Indeed, not only will she find out if the total number of days when they could meet is even or odd, but also she will know the precise days they can meet. She didn't want to learn that, but there is no other way.

Wim van Dam[73] observed in his PhD thesis, however, that if Alice and Bob have access to PR boxes, they could reduce the communication to a single bit, eliminating therefore the entire redundancy. They can do this by not attempting to directly communicate information about their calendars, but using this as input to their boxes and communicating information about their outputs.

In particular, all Alice and Bob have to do is to associate with each day i a variable x_i (y_i) that is equal to 0 if the day is busy and to 1 if the day is free and use them as inputs for their PR boxes. The sum of their outputs is even (odd) if the number of days when they can meet is even (odd). For Alice to find out whether the sum of their outputs is even or odd, Bob only needs to inform her whether the sum of his outputs is even or odd, that is, a single bit of communication (Box 1).

The result is particularly important, as the above calendar problem is not just some silly communication task; it is in fact the most difficult communication task possible (technically called the 'inner product' problem). Indeed, every other communication problem can be mapped onto this one, so removing the redundancy from this calendar problem means removing the redundancy from all communication problems.

Crucially, quantum mechanical nonlocal correlations cannot help with this task[80] (though they can help in easier communication problems[81]), hence, they cannot eliminate all redundancy from communication. Quantum nonlocal correlations (Box 2) are therefore dramatically different from PR boxes.

Prompted by the above result, Brassard *et al.*[74] raised a tantalizing possibility: maybe not only the perfect PR boxes, which are the strongest nonlocal correlations possible, but all super-quantum nonlocal correlations could eliminate all redundancy from communication. If that were the case, it would single out quantum mechanics as the maximal nonlocal theory that doesn't make all communication efficient.

Brassard *et al.*[74] took the first steps towards answering their question. Recall that quantum mechanical boxes can yield outputs a and b such that $a \oplus b = xy$ with a probability of success of at most $(2+\sqrt{2})/4 \approx 0.85$, whereas perfect PR boxes have a probability of success of 1. Using error-correction techniques, they showed that even imperfect PR boxes can eliminate all communication redundancy, as long as their probability of success is larger than approximately 0.91. However, there is still a gap, from 0.85 to 0.91, about which we know nothing. Hence, we don't know yet if the task of eliminating communication redundancy can single out quantum mechanics.

Nonlocal computation

While the status of communication complexity (as the above general problem is technically known) versus quantum mechanics is yet unsettled, a different task, nonlocal computation[75], has for the first time singled out the quantum–super-quantum transition.

Box 2 | The polytope of non-signalling correlations.

To better understand nonlocal correlations, a geometric representation is very useful[28,73]. For any given pair of boxes, the entire physics is encapsulated in the joint probabilities $P(a,b|x,y)$. We can think of these joint probabilities as coordinates of a point in an n dimensional space (16 dimensional space in the simple example considered here, corresponding to all combinations of $a,b,x,y = 0,1$). The set of all possible correlations fills a polytope, the intersection of the hypercube defined by the linear inequalities $0 \leq P(a,b|x,y) \leq 1$ and the hyperplanes corresponding to the probability normalization constraints:

$$\sum_{a,b} P(a,b|x,y) = 1 \quad (2)$$

Furthermore, we are only interested in the 'non-signalling' boxes, which do not allow Alice to signal instantaneously to Bob or vice versa, that is, the boxes that do not violate special relativity. For this to be the case, the probabilities of Alice's box outputs must be independent of Bob's input and vice versa:

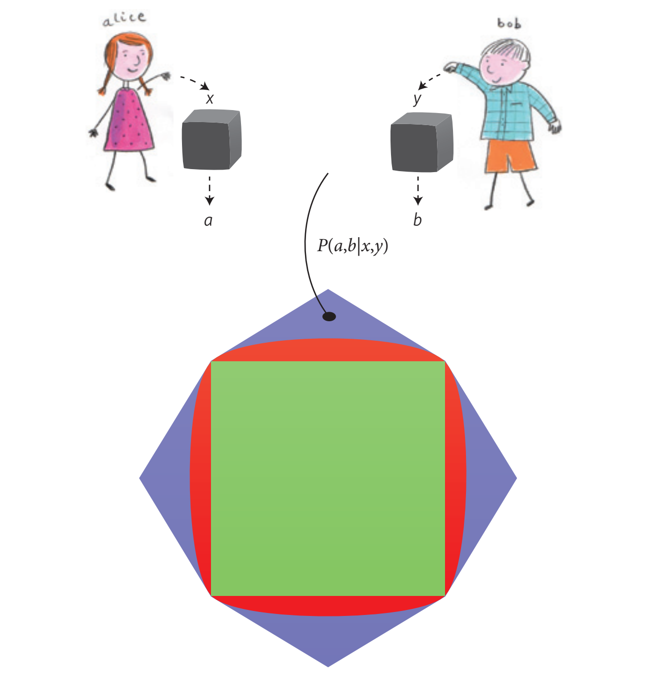
$$\sum_b P(a,b|x,y) = \sum_b P(a,b|x,y') \quad (3)$$

for any y and y', and:

$$\sum_a P(a,b|x,y) = \sum_a P(a,b|x',y) \quad (4)$$

for any x and x'. The non-signalling constraints define hyperplanes; the intersection of these hyperplanes with the polytope of all correlations defines the polytope of non-signalling correlations illustrated below.

Each point of the figure represents an entire physical set-up. The big polytope, including the purple, red and green regions, constitutes the set of all non-signalling boxes. The internal green polytope represents the set of local correlations; boxes acting according to classical mechanics can produce all the local correlations, and only these correlations. The vertices of the local polytope are deterministic correlations in which Alice's box outcome depends deterministically on her income (such as $a = x$) and similar for Bob. (Obviously these deterministic boxes are local — what Alice's box does is independent of Bob's box input and vice versa.) All other points of the classical polytope are obtained as mixtures of deterministic probabilities; more precisely, one can prepare the boxes to act, with pre-prescribed probability, according to a different deterministic strategy. The faces of the classical polytope are defined by the Bell inequalities; every correlation that is outside the local polytope is nonlocal. The round body consisting of the red and green parts represents all the quantum correlations. This body is rounded as quantum correlations obey Schwartz inequalities, due to the vector nature of the Hilbert space. All points in the red region represent nonlocal boxes, as they are outside the local polytope. The boundary of quantum mechanics is a generalized Cirel'son inequality. Incidentally, one of the great unsolved problems of fundamental quantum mechanics is to determine the boundary of quantum correlations[27–29,31,32]. In fact, it is even difficult to determine if a given correlation (that is, a point in the big polytope) is quantum or not. As the complete non-signalling set is a polytope, whereas the quantum one is a round body, it is clear that points outside quantum mechanics that are nevertheless non-signalling exist — the purple region. These are the non-signalling super-quantum correlations. The vertices of this polytope other than the local deterministic ones are 'maximal' nonlocal correlations; in the simplest case of boxes with two inputs and two outputs, these are the perfect PR boxes. The challenge is to find fundamental properties by which the purple points differentiate from all others. In the process, we learn more about what all the others — that is, the quantum mechanical ones — really are.



Consider an ordinary computation in which the input consists of N bits, $z_1, ..., z_N$ and the output is a single bit, $c = f(z_1, ..., z_N)$. To this computation we can associate a 'nonlocal computation' in the following way. The computation is carried out by two devices, one at Alice's location and one at Bob's. To each bit z_i of the original computation we associate two bits, x_i given to Alice and y_i given to Bob, such that $z_i = x_i \oplus y_i$. For each value of z_i, there are two possible combinations of x_i and y_i: $x_i = 0$, $y_i = 0$ and $x_i = 1$, $y_i = 1$ for $z_i = 0$ and $x_i = 1$, $y_i = 0$ and $x_i = 0$, $y_i = 1$ for $z_i = 1$. For a given value of z_i, each combination is selected with equal probability. As a consequence, by looking only at their own variables, neither Alice nor Bob can determine the original variables z_i. Alice is required to output a bit a and Bob a bit b such that $a \oplus b = c = f(z_1, ..., z_N)$. Alice and Bob know what the function f is and are allowed to communicate in advance and set up their devices in a correlated manner; they only don't know what the values of the inputs will be. The question is, how well can they succeed? More precisely, if the values of the original inputs z_i are chosen at random, what is the probability that the nonlocal computation gives the correct result?

An important notion is that of the 'best linear approximation' of a computation. To each function $f(z_1, ..., z_N)$ we associate a linear function $f_L(z_1, ..., z_N) = \alpha_1 z_1 \oplus \alpha_2 z_2 \oplus ... \oplus \alpha_N z_N$, where α_i are constants equal to 0 or 1. In other words, f_L is the sum of a subset of the original variables. The function f_L is chosen in such a way that it is equal to f for as many inputs as possible. For example, if f is the logical AND function, that is, the product $f^{AND} = z_1 z_2$, the best linear approximation is $f_L^{AND} = 0$. Indeed, by always yielding 0, $f_L^{AND} = f^{AND}$ in 3 out of 4 cases, the exception being $z_1 = z_2 = 1$.

NATURE PHYSICS DOI: 10.1038/NPHYS2916

Nonlinearity is the core of computation, so, in some sense, a linear approximation means no computation at all. Now, it turns out that if Alice and Bob have at their disposal only devices functioning according to the laws of classical physics, the best they can do is the best linear approximation of the desired computation. Even more surprisingly, although quantum mechanical nonlocal correlations are, in general, stronger than the classical ones — after all, this is the whole point of nonlocality — these correlations do not help nonlocal computation: quantum devices cannot do better than the best linear approximation either. On the other hand, the very moment we allow for super-quantum correlations, we can do nonlocal computation better than the best linear approximation. Hence, as far as nonlocal computation is concerned, there is a sharp transition between quantum and super-quantum correlations.

Information causality

Suppose Alice sends to Bob a message consisting of a single binary digit (0 or 1). By this procedure, Alice cannot send Bob more than one bit of classical information, even if they also share some nonlocal particles and perform measurements on them according to the information they wish to transmit or receive. Indeed, if by such a procedure Alice could communicate to Bob more than one bit of information, they could also communicate superluminally. This is easy to prove — Bob wouldn't actually need to wait for Alice's message; he could simply guess it, perform his measurements according to the guess, simultaneously with those of Alice, and learn, with a success probability of 1/2, more than one bit of information. This can then easily be converted into learning some information with certainty.

An interesting possibility emerges, however. Suppose Alice has two bits that she wants to communicate to Bob. Even though by sending a one-bit message she cannot communicate both bits to Bob, perhaps Bob could choose which bit to learn, even though he can make the decision at the last moment, long after Alice has already sent her message. Surprisingly, if Alice and Bob share a PR box, this is possible. Indeed, let x_0 and x_1 be Alice's two bits. She inputs $x = x_0 \oplus x_1$ into her box and sends Bob the message $m = x_0 \oplus a$. If Bob wants to learn x_0 he inputs in his box $y = 0$, whereas if he wants to learn x_1 he inputs $y = 1$. Bob then calculates $m \oplus b$. He obtains $m \oplus b = x_0 \oplus a \oplus b = x_0 \oplus xy = x_0 \oplus (x_0 \oplus x_1)y$. It is easy to see that if $y = 0$ then $m \oplus b = x_0$ and if $y = 1$ then $m \oplus b = x_1$.

On the other hand, one may feel uneasy with this result. Indeed, although Bob cannot find both x_0 and x_1, one may consider that even the ability of Bob to choose which bit to learn should be unphysical. Indeed, the message sent by Alice consists of just one binary digit; how can it allow Bob to retrieve information about two bits, even if he cannot read both of them? Imposing the restriction that this is impossible yields a new principle, which was proposed by Pawlowski *et al.*[76] and called 'information causality'.

As shown above, PR boxes violate information causality. However, it turns out that both classical physics and quantum mechanics obey information causality. And here comes the really exciting thing: for a restricted class of nonlocal correlations (namely the unbiased ones, where the local probabilities of all outcomes are equal), information causality breaks exactly at the boundary between quantum and super-quantum nonlocal correlations. That is, suppose we make the PR boxes weaker by adding white noise until they become only as strong as quantum mechanical correlations. Exactly here information causality ceases to be violated. Information causality is, therefore, yet another example that singles out part of the quantum–super-quantum boundary.

Quantum mechanics is special (or maybe not)

So what is the status of this research now? In this Review, I have discussed only a few examples; there is, however, intense, ongoing effort along similar lines[82–96].

Although it is early days, one can already see that quantum mechanics is special. Starting from various completely unrelated tasks that have nothing to do with the dynamics of microscopic particles, but are general purpose questions, such as nonlocal computation, information causality, macroscopic locality, the possibility of nonlocality swapping and so on, quantum mechanics emerges. It is precisely at the boundary between quantum mechanical and super-quantum correlations that qualitative changes in the performance of the above tasks occur. True, these are only glimpses — there is no known task yet that completely differentiates quantum correlations from super-quantum ones; only part of the boundary has emerged so far. Indeed, it is now known that any task that would be able to completely single out quantum mechanics has to be multipartite, as opposed to the bi-partite tasks discussed here[19]. However, it is remarkable that parts of the quantum boundary appeared at all — there was no *a priori* reason whatsoever for this to happen. Yet, quantum mechanics starts to appear from the fog. That quantum mechanics has special significance in at least some of such tasks means that quantum mechanics is special, and one should not expect that the ultimate theory of nature should be some slight deviation from quantum mechanics — there are basic statements about nature that have to be changed. It also means that quantum mechanics is probably here to stay — at least much longer than one would have imagined.

At the same time, one can legitimately question the relevance of such computer science-inspired tasks in the grand scheme of things. Why should we care about such things as communication complexity, nonlocal computation or information causality? Why should we let our quest for a new theory of nature — or the justification for the present one — be guided by such ideas?

The very first indication that this line of thought is good is the simple fact that it seems to work. Quantum mechanics appears unexpectedly in various contexts. The fact that it does so is fascinating, and certainly non-trivial.

Second, whereas the tasks discussed here may appear quite random and completely insignificant from the point of view of hardcore physics — certainly they tell us nothing about the spectra of atoms or about phase transitions — from the point of view of information theory they are actually fundamental. (A pair of perfect PR boxes is a device that transforms the basic nonlinear function, the product, into a linear one, $xy = a \oplus b$. At the same time, it can be viewed as the maximal zero-capacity communication channel.)

Yet again, it might not be quantum mechanics that we see emerging, but something altogether different. A few years ago Navascués and collaborators[30] discovered a hierarchy of sets of 'self-consistent' nonlocal correlations, each set is larger than quantum mechanics, but their boundaries coincide with quantum mechanics in some places. Maybe it is one of these sets that we are starting to see. These sets were discovered based on some rather obscure mathematical considerations, going opposite to the direction of considering natural tasks, which was the whole point of the research discussed above.

But recently, quantum gravity led to a tantalizing result: motivated by considerations of quantum gravity, a class of generalized theories was proposed by Gell-Mann and Hartle[97,98], which was further developed by Sorkin[99]. And in a very recent (yet unpublished) paper[100], it was shown that these theories lead to stronger-than-quantum correlations, namely to the Navascués-Pironio-Acín set known as Q(1+AB), which is known to coincide with quantum mechanics in most of the places where the information tasks indicated quantum mechanics. Hence, maybe what those tasks indicate is Q(1+AB), not quantum mechanics. The jury is still out.

To conclude, all the above is great fun. Each answer raises new questions, completely different in nature from the ones one started with; this, more than anything else, indicates that finally we might be on the right track.

Received 26 November 2013; accepted 12 February 2014; published online 1 April 2014

References

1. Aharonov, Y. & Bohm, D. Significance of electromagnetic potentials in the quantum theory. *Phys. Rev.* **115,** 485–491 (1959).
2. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1,** 195–200 (1964).
3. Aharonov, Y. & Rohrlich, D. *Quantum Paradoxes: Quantum Theory for the Perplexed* (Wiley-VCH, 2005).
4. Shimony, A. in *Proc. Int. Symp. Foundations of Quantum Mechanics* (eds Kamefuchi, S. *et al.*) 225–230 (Physical Society of Japan, 1983).
5. Popescu, S. & Rohrlich, D. Causality and non-locality as axioms for quantum mechanics. *Found. Phys.* **24,** 379–385 (1994).
6. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81,** 865–942 (2009).
Extensive review of the characterization of quantum nonlocality.
7. Gisin, N. Bell inequality holds for all non-product states. *Phys. Lett. A* **154,** 201–202 (1991).
8. Popescu, S. & Rohrlich, D. Generic quantum nonlocality. *Phys. Lett. A* **166,** 293–297 (1992).
9. Barrett, J., Collins, D., Hardy, L., Kent, A. & Popescu, S. Quantum nonlocality, Bell inequalities and the memory loophole. *Phys. Rev. A* **66,** 42111 (2002).
10. Brunner, N., Gisin, N. & Scarani, V. Entanglement and non-locality are different resources. *New J. Phys.* **7,** 88 (2005).
11. Cerf, N. J., Gisin, N., Massar, S. & Popescu, S. Simulating maximal quantum entanglement without communication. *Phys. Rev. Lett.* **94,** 220403 (2005).
12. Almeida, M., Pironio, S., Barrett, J., Tóth, G. & Acín, A. Noise robustness of the nonlocality of entangled quantum states. *Phys. Rev. Lett.* **99,** 040403 (2007).
13. Brunner, N., Gisin, N., Popescu, S. & Scarani, V. Simulation of partial entanglement with no-signaling resources. *Phys. Rev. A* **78,** 52111 (2008).
14. Allcock, J., Brunner, N., Pawlowski, M. & Scarani, V. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A* **80,** 040103(R) (2009).
15. Acín, A. *et al.* Unified framework for correlations in terms of local quantum observables. *Phys. Rev. Lett.* **104,** 140404 (2010).
16. Barnum, H., Beigi, S., Boixo, S., Elliott, M. B. & Wehner, S. Local quantum measurement and no signaling imply quantum correlations. *Phys. Rev. Lett.* **104,** 140401 (2010).
17. Oppenheim, J. & Wehner, S. The uncertainty principle determines the nonlocality of quantum mechanics. *Science* **330,** 1072–1074 (2010).
18. Barrett, J. & Gisin, N. How much measurement independence is needed to demonstrate nonlocality? *Phys. Rev. Lett.* **106,** 100406 (2011).
19. Gallego, R., Würflinger, L. E., Acín, A. & Navascués, M. Quantum correlations require multipartite information principles. *Phys. Rev. Lett.* **107,** 210403 (2011).
20. Bancal, J-D. *et al.* Quantum non-locality based on finite-speed causal influences leads to superluminal signalling. *Nature Phys.* **8,** 867–870 (2012).
21. Liang, Y-C., Masanes, L. & Rosset, D. All entangled states display some hidden nonlocality. *Phys. Rev. A* **86,** 052115 (2012).
22. Palazuelos, C. Superactivation of quantum nonlocality. *Phys. Rev. Lett.* **109,** 190401 (2012).
23. Vértesi, T. & Brunner, N. Quantum nonlocality does not imply entanglement distillability. *Phys. Rev. Lett.* **108,** 030403 (2012).
24. Cavalcanti, D., Acín, A., Brunner, N. & Vértesi, T. All quantum states useful for teleportation are nonlocal resources. *Phys. Rev. A* **87,** 042104 (2013).
25. Hirsch, F., Quintino, M. T., Bowles, J. & Brunner, N. Genuine hidden quantum nonlocality. *Phys. Rev. Lett.* **111,** 160402 (2013).
26. Khalfin, L. A. & Tsirelson, B. S. Quantum/classical correspondence in the light of Bell's inequalities. *Found. Phys.* **22,** 879–948 (1992).
27. Tsirelson, B. S. Some results and problems on quantum Bell-type inequalities. *Hadronic J. Suppl.* **8,** 329–345 (1993).
28. Tsirelson, B. S. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Sov. Math.* **36,** 557–570 (1987).
29. Tsirelson, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4,** 93–100 (1980).
30. Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98,** 10401 (2007).
31. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10,** 73013 (2008).
32. Barnum, H., Barrett, J., Leifer, M. S. & Wilce, A. Generalized no-broadcasting theorem. *Phys. Rev. Lett.* **99,** 240501 (2007).
33. Barrett, J. Information processing in generalized probabilistic theories. *Phys. Rev. A* **75,** 32304 (2007).
34. Barrett, J. & Short, A. J. Strong non-locality: a tradeoff between states and measurements. *New J. Phys.* **12,** 33034 (2010).
35. Barnum, H. *et al.* Entropy and information causality in general probabilistic theories. *New J. Phys.* **12,** 033024 (2010).
36. Short, A. J. & Wehner, S. Entropy in general physical theories. *New J. Phys.* **12,** 33023 (2010).
37. Gross, D., Mueller, M., Colbeck, R. & Dahlsten, O. C. O. All reversible dynamics in maximally nonlocal theories are trivial. *Phys. Rev. Lett.* **104,** 80402 (2010).
38. Janotta, P., Gogolin, C., Barrett, J. & Brunner, N. Limits on nonlocal correlations from the structure of the local state space. *New J. Phys.* **13,** 063024 (2011).
39. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 10503 (2005).
40. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 120405 (2006).
41. Scarani, V. *et al.* Secrecy extraction from no-signaling correlations. *Phys. Rev. A* **74,** 42339 (2006).
42. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
43. Hänggi, E. & Renner, R. Device-independent quantum key distribution with commuting measurements. Preprint at http://arxiv.org/abs/1009.1833 (2010).
44. Franz, T., Furrer, F. & Werner, R. F. Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.* **106,** 250502 (2011).
45. Masanes, L., Pironio, S. & Acín, A. Secure device independent quantum key distribution with causally independent measurement devices. *Nature Commun.* **2,** 238 (2011).
46. Barrett, J., Colbeck, R. & Kent, A. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A* **86,** 062326 (2012).
47. Vazirani, U. & Vidick, T. Certifiable quantum dice. *Phil. Trans. R. Soc. A.* **370,** 3432–3448 (2012).
48. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110,** 010503 (2013).
49. Huber, M. & Pawlowski, M. Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement. *Phys. Rev. A* **88,** 032309 (2013).
50. Colbeck, R. *Quantum And Relativistic Protocols For Secure Multi-Party Computation* PhD thesis, Univ. Cambridge (2007).
51. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).
52. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A* **44,** 095305 (2011).
53. Acín, A., Massar, S. & Pironio, S. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.* **108,** 100402 (2012).
54. Colbeck, R. & Renner, R. Free randomness can be amplified. *Nature Phys.* **8,** 450–454 (2012).
55. Vazirani, U. & Vidick, T. in *Proc. 44th Symp. Theory Comput. STOC 2012* (eds Pitassi, T. *et al.*) 61–76 (ACM Press, 2012).
56. Gallego, R. *et al.* Full randomness from arbitrarily deterministic events. *Nature Commun.* **4,** 2654 (2013).
57. Pironio, S. & Massar, S. Security of practical private randomness generation. *Phys. Rev. A* **87,** 012336 (2013).
58. Rabelo, R., Ho, M., Cavalcanti, D., Brunner, N. & Scarani, V. Device-independent certification of entangled measurements. *Phys. Rev. Lett.* **107,** 050502 (2011).
59. Bancal, J-D., Gisin, N., Liang, Y-C. & Pironio, S. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.* **106,** 250404 (2011).
60. Moroder, T., Bancal, J-D., Liang, Y-C., Hofmann, M. & Gühne, O. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.* **111,** 030501 (2013).
61. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. Preprint at http://arxiv.org/abs/1303.2849 (2013).
62. Hardy, L. Quantum theory from five reasonable axioms. Preprint at http://arxiv.org/abs/quantph/0101012 (2001).
63. Chiribella, G., D'Ariano, G. M. & Perinotti, P. Probabilistic theories with purification. *Phys. Rev. A* **81,** 062348 (2010).
64. Paterek, T., Dakić, B. & Brukner, C. Theories of systems with limited information content. *New J. Phys.* **12,** 053037 (2010).
65. Chiribella, G., D'Ariano, G. M. & Perinotti, P. Informational derivation of quantum theory. *Phys. Rev. A* **84,** 012311 (2011).
66. Masanes, L. & Müller, M. P. A derivation of quantum theory from physical requirements. *New J. Phys.* **13,** 063001 (2011).
67. de la Torre, G., Masanes, L., Short, A. J. & Müller, M. P. Deriving quantum theory from its local structure and reversibility. *Phys. Rev. Lett.* **109,** 090403 (2012).

68. Masanes, L., Müller, M. P., Augusiak, R. & Pérez-García, D. Existence of an information unit as a postulate of quantum theory. *Proc. Natl Acad. Sci. USA.* **110,** 16373–16377 (2013).
69. Müller, M. P. & Masanes, L. Three-dimensionality of space and the quantum bit: an information-theoretic approach. *New J. Phys.* **15,** 053040 (2013).
70. Popescu, S. Dynamical quantum non-locality. *Nature Phys.* **6,** 151–153 (2010).
71. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880 (1969).
72. Barrett, J., Linden, N., Massar, S., Pironio, S., Popescu, S. & Roberts, D. Non-local correlations as an information theoretic resource. *Phys. Rev. A* **71,** 22101 (2005).
73. van Dam, W. Implausible consequences of superstrong nonlocality. Preprint at http://arxiv.org/abs/quant-ph/0501159 (2005).
74. Brassard, G. *et al.* Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.* **96,** 250401 (2006).
75. Linden, N., Popescu, S., Short, A. J. & Winter, A. Quantum nonlocality and beyond: limits from nonlocal computation. *Phys. Rev. Lett.* **99,** 180502 (2007).
76. Pawlowski, M. *et al.* Information causality as a physical principle. *Nature* **461,** 1101–1104 (2009).
77. Navascués, M. & Wunderlich, H. A glance beyond the quantum model. *Proc. R. Soc. A* **466,** 881 –890 (2010).
78. Fritz, T. *et al.* Local orthogonality as a multipartite principle for quantum correlations. *Nature Commun.* **4,** 2263 (2013).
79. Skrzypczyk, P., Brunner, N. & Popescu, S. Emergence of quantum correlations from nonlocality swapping. *Phys. Rev. Lett.* **102,** 110402 (2009).
80. Cleve, R., van Dam, W., Nielsen, M. & Tapp, A. *Quantum Computing and Quantum Communication, Lecture Notes in Computer Science* Vol. 1509 (Springer, 1999).
81. Cleve, R. & Buhrman, H. Substituting quantum entanglement for communication. *Phys. Rev. A* **56,** 1201–1204 (1997).
82. Barrett, J. & Pironio, S. Popescu-Rohrlich correlations as a unit of nonlocality. *Phys. Rev. Lett.* **95,** 140401 (2005).
83. Methot, A. A. & Scarani, V. An anomaly of nonlocality. *Quantum Inform. Compu.* **7,** 157–170 (2007).
84. Forster, M., Winkler, S. & Wolf, S. Distilling nonlocality. *Phys. Rev. Lett.* **102,** 120401 (2009).
85. Brunner, N. & Skrzypczyk, P. Nonlocality distillation and postquantum theories with trivial communication complexity. *Phys. Rev. Lett.* **102,** 160403 (2009).
86. Pawlowski, M. & Brukner, C. Monogamy of Bell's inequality violations in nonsignaling theories. *Phys. Rev. Lett.* **102,** 30403 (2009).
87. Cavalcanti, D., Salles, A. & Scarani, V. Macroscopically local correlations can violate information causality. *Nature Commun.* **1,** 136 (2010).
88. Fitzi, M., Hänggi, E., Scarani, V. & Wolf, S. The nonlocality of n noisy Popescu–Rohrlich boxes. *J. Phys. A* **43,** 465305 (2010).
89. Brunner, N., Cavalcanti, D., Salles, A. & Skrzypczyk, P. Bound nonlocality and activation. *Phys. Rev. Lett.* **106,** 20402 (2011).
90. Gallego, R., Würflinger, L. E., Acín, A. & Navascués, M. Operational framework for nonlocality. *Phys. Rev. Lett.* **109,** 70401 (2012).
91. Borsten, L., Bradler, K. & Duff, M. J. Tsirelson's bound and supersymmetric entangled states. Preprint at http://arxiv.org/abs/1206.6934 (2012).
92. Short, A. J., Popescu, S. & Gisin, N. Entanglement swapping for generalized nonlocal correlations. *Phys. Rev. A* **73,** 12101 (2006).
93. Branciard, C., Gisin, N. & Pironio, S. Characterizing the nonlocal correlations created via entanglement swapping. *Phys. Rev. Lett.* **104,** 170401 (2010).
94. Bancal, J-D., Brunner, N., Gisin, N. & Liang, Y-C. Detecting genuine multipartite quantum nonlocality: a simple approach and generalization to arbitrary dimensions. *Phys. Rev. Lett.* **106,** 020405 (2011).
95. Branciard, C., Rosset, D., Gisin, N. & Pironio, S. Bilocal versus nonbilocal correlations in entanglement swapping experiments. *Phys. Rev. A* **85,** 032119 (2012).
96. Bancal, J-D., Barrett, J., Gisin, N. & Pironio, S. Definitions of multipartite nonlocality. *Phys. Rev. A* **88,** 014102 (2013).
97. Gell-Mann, M. & Hartle, G. B. in *Complexity, Entropy and the Physics of Information: SFI Studies in the Sciences of Complexity* Vol VIII (ed. Zurek, W.) 150–173 (Addison Wesley, 1990).
98. Hartle, J. B. in *Proc. 1992 Les Houches Summer School on Gravitation and Quantization* (eds Zinn-Justin, J. & Julia, B.) 285–480 (North-Holland, 1995).
99. Sorkin, R. D. Quantum mechanics as quantum measure theory. *Mod. Phys. Lett. A* **9,** 3119–3128 (1994).
100. Dowker, F. Henson, J. & Wallden, P. A histories perspective on characterising quantum non-locality. Preprint at http://arxiv.org/abs/1311.6287 (2013).

Additional information

Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to S.P.

Competing financial interests

The authors declare no competing financial interests.