Computability limits nonlocal correlations

Tanvirul Islam* and Stephanie Wehner†
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore
(Received 22 May 2012; published 10 October 2012)

If the no-signaling principle was the only limit to the strength of nonlocal correlations, we would expect that any form of no-signaling correlation can indeed be realized. That is, there exists a state and measurements that remote parties can implement to obtain any such correlation. Here, we show that in any theory in which some functions cannot be computed, there must be further limits to nonlocal correlations than the no-signaling principle alone. We proceed to argue that even in a theory such as quantum mechanics in which nonlocal correlations are already weaker, the question of computability imposes such limits.

DOI: 10.1103/PhysRevA.86.042109 PACS number(s): 03.65.Ud, 03.65.Ta, 03.67.Ac

Bell's seminal work [1] on nonlocal correlations, not only allowed us to distinguish classical from quantum mechanics, but also spurred a multitude of useful applications in quantum information theory (see, e.g., [2,3]). As a result it is important to know which nonlocal correlations can indeed be physically realized.

Let us now explain more carefully what is meant by nonlocal correlations. For simplicity, we thereby consider a bipartite system, Alice and Bob. Let $\mathcal{X}$ and $\mathcal{Y}$ denote a set of possible measurements for Alice and Bob, respectively, and let $\mathcal{A}$ and $\mathcal{B}$ denote the corresponding set of outcomes. Furthermore, let

$$\Pr[a,b|x,y] \tag{1}$$

denote the probability that Alice and Bob obtain outcomes $a \in \mathcal{A}$ and $b \in \mathcal{B}$ when making measurements $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively. When it comes to the study of nonlocal correlations, we are interested in the set of allowed values for $\Pr[a,b|x,y]$. For example, the famous CHSH inequality [4] tells us that for any classical theory

$$\frac{1}{4}\sum_{x,y\in\{0,1\}}\sum_{a\in\{0,1\}}\Pr[a,b=xy\oplus a|x,y] \leqslant \frac{3}{4}, \tag{2}$$

for any possible measurements labeled $\mathcal{X}=\{0,1\}$ and $\mathcal{Y}=\{0,1\}$, and any state shared by Alice and Bob.[1] Quantumly, however, there exist a shared state and measurements such that the sum attains the value of $1/2+1/(2\sqrt{2})\approx 0.853$. This is the highest value possible in quantum mechanics [5]. It demonstrates that in a quantum world, nonlocal correlations can be strictly stronger than is allowed classically. Much work has gone into determining bounds on quantum correlations [5–12], and investigating the difference between the classical and quantum regime (see, e.g., [13,14]).

Here, we are interested in the following question: Even if nonlocal correlations are consistent with a particular theory, should we expect them to be physical? That is, do we really expect them to exist in the sense that Alice and Bob can realize the joint state and measurements needed to obtain them? To explain this question, let us first consider the simple scenario of a world in which the only constraint on nonlocal correlations is that they must be no signaling [15–17]. That is, we have

$$\forall a,x,y,y' \quad \Pr[a|x,y]=\Pr[a|x,y'], \tag{3}$$

and similarly for all x,x'. Property (3) tells us that, by observing the outcome a, Alice can never tell what Bob's input was and vice versa.

An example of such a maximally correlated pair of nonlocal systems is the famous Popescu-Rohrlich (PR)-box [15–17], which allows the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality (2) up to the value 1. When thinking about a PR-box, one can think of the measurements more abstractly and imagine that Alice and Bob each have a terminal in which Alice can input a bit x and get as outcome a bit a. Similarly, Bob can input a bit y and get bit b as his outcome. The distribution of outcomes a and b given the inputs x and y is

$$\Pr[a,b|x,y]=\begin{cases}0, & \text{if } a\oplus b\neq xy\\ \frac{1}{2}, & \text{otherwise.}\end{cases} \tag{4}$$

That is, the inputs $x,y\in\{0,1\}$ and outputs $a,b\in\{0,1\}$ always satisfy

$$a\oplus b=xy. \tag{5}$$

One can see, from Eq. (4), that the marginal of this distribution satisfies the no-signaling condition (3),

$$\forall a,b,x,y \quad \Pr[a|x,y]=\sum_b \Pr[a,b|x,y]=\frac{1}{2}. \tag{6}$$

As a result, it is impossible for them to use the PR-box to communicate instantly. Yet, if at a later time Alice and Bob meet or exchange information about the outcomes they have gotten, they will find that a, b, x, and y always satisfy Eq. (5).

I. NO-SIGNALING CORRELATIONS

In a no-signaling world, we would *a priori* expect that indeed all no-signaling correlations are realizable. That is, there exists a box similar to the PR-box to which we can give inputs x and y, and it generates some outputs a and b according to a desired no-signaling distribution $\Pr[a,b|x,y]$. Here, we show that as long as there exist uncomputable functions (see below) in such a theory, not all distributions can be realized, even if they obey the no-signaling principle. That is, the set

*tanvirul@nus.edu.sg
†wehner@nus.edu.sg
[1] $\oplus$ denotes addition modulo 2.

of allowed distributions is strictly smaller than dictated by the no-signaling principle alone.

In order to show this, we will now explain a procedure which demonstrates how any function in principle can be computed in a distributed fashion, i.e., by a PR-type box. In [18] Linden *et al.* describe a form of distributed nonlocal computation. However, in their method Alice and Bob themselves do not know the actual inputs, rather they are given an additive sharing of the inputs [18,19]. To get some intuition of how our construction works in contrast, let us first consider the PR-box in a more operational way. In particular, we will think about a procedure according to which the box generates the outputs. Note that of course the box does not follow an internal procedure, but is merely given by a set of probability distributions. Yet, this view provides us with an operational perspective on how to write down such distributions. More precisely, we imagine that

(1) upon receiving the inputs x and y from Alice and Bob, the box selects an independent and uniformly random bit $r \in_R \{0,1\}$.

(2) Then, it computes xy.

(3) Finally, it assigns $a \leftarrow r$ and $b \leftarrow r \oplus xy$.

To see why this procedure works, first observe that

$$a \oplus b = r \oplus (r \oplus xy) = xy. \tag{7}$$

And, as $r(=a)$ is an independently generated random bit, a must not be affected by the input y from Bob. On the other hand, Bob receives $b = r \oplus xy$. To him, it is also completely random because it is encrypted with a random bit r which is generated independently. So, he also does not have any information about the input x from Alice. As a result, the box is no signaling.

We have described how a PR-box can operate in principle. From this we can have a generalized version of it. Namely, we can have a box that satisfies

$$a \oplus b = f(x,y), \tag{8}$$

where $f : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}$ is any function of x and y. We achieve this by simply computing $f(x,y)$ in step 2 and assigning $a \leftarrow r$ and $b \leftarrow r \oplus f(x,y)$ in step 3. We call this the *no-signaling computation* of function $f(x,y)$, because by construction this computation is also no signaling. In fact, by the same argument we can generalize this box farther and nonlocally compute any function $f : \{0,1\}^l \times \{0,1\}^m \rightarrow \{0,1\}$, which takes strings x and y of arbitrary lengths as inputs from Alice and Bob accordingly and computes $f(x,y)$ nonlocally still satisfying the nonsignaling condition. In fact, van Dam shows in [20] that one can also perform this generalized no-signaling computation of $f(x,y)$ by using multiple copies of PR-boxes.[2]

As we have seen, if any distribution is allowed which is compatible with the no-signaling principle, then *any* function can be computed in such a nonlocally distributed manner. That is, once Alice and Bob have their outcomes a and b, respectively, they can meet or exchange these values at any later time and recover the functions value by computing $a \oplus b = f(x,y)$. This means that *if* the function f is not computable in a world where PR-boxes exist, then such correlations also cannot exist—even if they obey the principle of no signaling.

II. COMPUTABILITY

Let us now discuss in more detail what it means for a function to be computable. Intuitively, a function is computable in some particular physical theory, if this theory allows us to build a machine that takes as inputs x and y, and outputs $f(x,y)$ after a finite amount of time. Classically, it turns out that according to the *Church-Turing thesis* [21,22]: *Every "function which would naturally be regarded as computable" can be computed by the universal Turing machine.*

In [23] Deutsch states a stronger version of this thesis, known as the Church-Turing *principle*: *Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means.* Intuitively, a universal model computing machine is a machine that can simulate any other computing machine. To understand this concept, let us consider the example of the quantum Turing machines [23]. Let us call this machine U_q. We call this machine *universal*, because it can be programed to simulate all the other physically realizable computing machines operating under quantum mechanics, including itself. That is, for any machine M computing a function f there is a program P for the universal quantum Turing machine U_q which can also compute the function. In fact, it has been shown that even a *classical* Turing machine [22] can simulate the universal quantum Turing machine with an additional overhead [23]. One can thus consider the program P to be a string on a suitable finite alphabet.

It is shown that not all functions are computable by Turing machines, and we briefly sketch the argument here [24]: Without loss of generality we can assume $P \in \{0,1\}^n$ and the decision function to be $f : \{0,1\}^* \rightarrow \{0,1\}$. That is, the program is a finite string of 0's and 1's of arbitrary length n. This allows us to find a one-to-one correspondence between all the possible programs to the set of natural numbers N by ordering the program strings in lexicographic order. That is, the set of possible programs is countably infinite. On the other hand, the set of possible functions $f : \{0,1\}^* \rightarrow \{0,1\}$ is not countable. As a result no matter how powerful a computing machine is, as long as it is programed using finite strings there will always remain functions not computable by that computing model. And by the Church-Turing principle, such computations cannot be physically realized in quantum mechanics.

It is important to note that finite in the statement of the Church-Turing principle means that for any particular computation we only need a finite amount of computational resources.[3] In principle, an unlimited amount of resources

[2]Note that our result does *not* exclude the existence of PR-boxes. When it comes to no-signaling computations, PR-boxes can be understood as the analog of an AND gate in a computational circuit—the fact that some functions cannot be computed does not exclude the possibility of such elementary gates.

[3]A machine that looks up the answer in a list would need an infinite list to produce the answer for arbitrary inputs.

are available, however only a finite amount are used at any given time (see [23] for details). Further details on physical uncomputability can be found in, e.g., [23,25,26]. A treatment of classical uncomputability can be found in, e.g., [24].

Classically and quantumly, one uncomputable function is Turing's halting function $H(x,y)$ [22]. This function takes as inputs x, which is the binary encoding of any program and y, which is the input to the program x and computes a Boolean output indicating whether program x halts on input y or keeps running forever. It was shown by Alan Turing that one cannot compute this function H. That is, no matter how much resource (time and memory) is provided, if someone assumes the solution of this function one will immediately lead to a contradiction. Now, if in our construction we take $f = H$, we see that Alice and Bob upon communicating one bit in the end, can compute the halting function nonlocally. Note that for this construction to work at least one of the input sets $\mathcal{X}$ and $\mathcal{Y}$ has to be infinite.[4]

In a general theory, the input, i.e., program, to a universal computing machine may of course not only consist of classical bits, but also of more generalized bits allowed in that particular theory. However, for the special case of the halting function, Turing's argument showing that it is impossible to compute the Halting function only hinges on the fact that the machine is indeed universal and the program has a finite description *within* that theory. Hence, if the Church-Turing principle would hold in that theory, the halting function should also be uncomputable.

Of course a world where any nonsignaling correlation is allowed, has many unusual and unexpected properties [27–30]. So it is not inconceivable that the Church-Turing principle should also break down. It could be, for example, that there does *not* exist a universal computing machine that can simulate any other machine in that physical theory, or in other words, not all finitely realizable processes are simulatable. We emphasize that we make no statement about whether the Church-Turing principle holds in any other theories. Our result merely implies that we must make a choice: Either the Church-Turing principle *does* hold and some functions are not computable, but then it imposes an additional limit on possible nonlocal correlations; or, all correlations compatible with the no-signaling principle are allowed, but then all functions[5] are computable and the Church-Turing principle does not hold.[6]

[4]This construction works even if one of the input sets $\mathcal{X}$ and $\mathcal{Y}$ is fixed and finite. As long as at least one of them is countably infinite, we can consider that as the set of programs and the other as inputs. It is known whether a program halts even on a fixed input is undecidable [24, Theorem 5.4.2].

[5]Note that one can always split the argument to make a multivalued function.

[6]We also emphasize that whenever the Church-Turing principle holds, one cannot even write down the no-signaling distribution corresponding to the box in Fig. 1 for all possible inputs x and y as this would be equivalent to computing the function manually for all inputs. Note, however, that just with the halting function itself we do not need to write down the function in order to achieve a contradiction. Rather, one argues that if the halting function were computable, then we would obtain a contradiction.

III. APPROXIMATE CASES

Let us now consider the case where our correlations are nonsignaling, but not *super strong*. That is, we consider approximate versions of PR-type boxes for which for some probability $p > \frac{1}{2}$ we have

$$\forall a,b,x,y \quad p \leqslant \Pr[a \oplus b = f(x,y)] < 1. \tag{9}$$

As a result by computing $a \oplus b$ Alice and Bob can compute the function f with probability at least p of giving the correct outcome. We denote this by $f_p(x,y)$. Quantum mechanics can provide us with such approximate boxes. For example, we know that for $x,y \in \{0,1\}$ the function $f(x,y) = xy$ can be computed in a distributed manner with $p = 1/2 + 1/(2\sqrt{2}) \approx 0.85$ for all x and y—this is just the quantum violation of the CHSH inequality. For any p, we can thus again ask the question: Should we expect such approximate boxes to exist?

Evidently, for any $p > 1/2$ it is possible to approximate any computable function with correctness $1 - \epsilon$ for any $\epsilon > 0$ by repeating the process many times. Yet, one can also show directly that there exist undecidable problems for which even such probabilistic versions cannot be computed. That is, one cannot compute that function with some constant probability p of correctness. As an example, let us consider the probabilistic halting function $H_p(x,y)$ which tells us with probability of correctness p whether program x halts on input y with probability p. Using a similar argument that was used by Turing to prove the uncomputability of the deterministic halting function, it can be shown that even this probabilistic function cannot be computed [26, Exercise 3.6]. We thus conclude that the question of computability imposes constraints on nonlocal correlations even for the approximate case of $1 > p > 1/2$.[7]

IV. DISCUSSION

We have shown that if the Church-Turing principle holds in a particular physical theory, then it imposes additional constraints on the existence of nonlocal correlations. Here we emphasize that this result holds for any general theory that is constrained by the no-signaling principle.

For example, in a world where PR-type boxes [15–17] exist, we previously worked with the assumption that all nonlocal correlations are allowed, as long as they obey the no-signaling principle. However, we now know that there *may* be further constraints: Either the Church-Turing principle does not hold, or nonlocal correlations really are strictly more limited—at least if Alice and Bob can meet again to combine their inputs. Of course, locally our box from Fig. 1 yields fully random outputs and neither Alice nor Bob can determine $f(x,y)$ on their own. This means that locally their outcomes are not constrained by the question whether f is computable.

In the quantum case, our result should be compared to [25] in which it is shown that if the Church-Turing principle holds, then there are measurements and unitary operators that cannot

[7]Note that p here is not an average as in the CHSH inequality (2). That is, here we require for each pair of x and y, the probability p of getting outcome $a \oplus b = f(x,y)$ to be strictly greater than $1/2$.

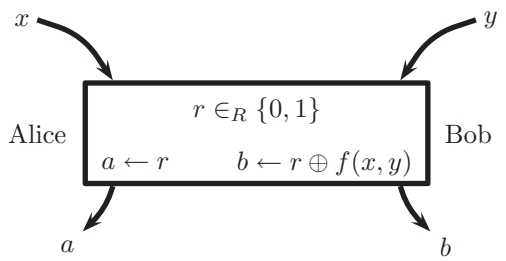

FIG. 1. No-signaling computation of the function $f(x,y)$.

be performed on a local quantum system. Here, we show that indeed in any theory in which the Church-Turing principle holds, certain states and/or measurements are not available to us as otherwise any (approximate) no-signaling computation could be performed. As such, our result can also be understood as imposing a limit on the kind of states and measurements permissible. It is an interesting open question to identify the class of theories for which the Church-Turing principle holds, and thus imposes a strict limit on physical observations.

ACKNOWLEDGMENTS

We thank CQT's nonlocal club for interesting discussions and comments. This research was supported by the National Research Foundation and Ministry of Education, Singapore.

[1] J. S. Bell, Physics **1**, 195 (1965).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] T. S. Cubitt, D. W. Leung, W. Matthews, and A. Winter, IEEE Trans. Inf. Theory **57**, 5509 (2011).
[4] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[5] B. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[6] L. Landau, Found. Phys. **18**, 449 (1988).
[7] L. Landau, Phys. Lett. A **123**, 115 (1987).
[8] Y.-C. Liang and A. C. Doherty, Phys. Rev. A **75**, 042103 (2007).
[9] S. Wehner, Phys. Rev. A **73**, 022110 (2006).
[10] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[11] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).
[12] A. C. Doherty, Y. Liang, B. Toner, and S. Wehner, in *Proceedings of the 23rd IEEE Conference on Computational Complexity, 2008* (IEEE Computer Society, Washington, DC, 2008), pp. 199–210.
[13] M. Junge and C. Palazuelos, Commun. Math. Phys. **306**, 695 (2011).
[14] M. Junge, C. Palazuelos, D. Perez-Garcia, I. Villanueva, and M. M. Wolf, Commun. Math. Phys. **300**, 715 (2010).
[15] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[16] S. Popescu and D. Rohrlich, in *The Dilemma of Einstein, Podolsky and Rosen, 60 years Later: International Symposium in Honour of Nathan Rosen*, edited by A. Mann and M. Revzen (Israel Physical Society, Haifa, Israel, 1996).
[17] S. Popescu and D. Rohrlich, in *Proceedings of the Symposium on Causality and Locality in Modern Physics and Astronomy: Open Questions and Possible Solutions* (York University, Toronto, August 25–29, 1997), arXiv:quant-ph/9709026.
[18] N. Linden, S. Popescu, A. J. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
[19] N. Brunner and P. Skrzypczyk, Phys. Rev. Lett. **102**, 160403 (2009).
[20] W. van Dam, arXiv:quant-ph/0501159.
[21] A. Church, Am. J. Math. **58**, 345 (1936).
[22] A. M. Turing, Proc. London Math. Soc. **42**, 230 (1936).
[23] D. Deutsch, in *Proceedings of the Royal Society of London, 1985*, Vol. A400, pp. 97–117.
[24] H. R. Lewis and C. H. Papadimitriou, *Elements of the Theory of Computation*, 2nd ed. (Prentice Hall, Englewood Cliffs, NJ, 1997).
[25] M. A. Nielsen, Phys. Rev. Lett. **79**, 2915 (1997).
[26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[27] G. V. Steeg and S. Wehner, Quantum Inf. Comput. **9**, 801 (2009).
[28] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, Nature (London) **461**, 1101 (2009).
[29] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner, Phys. Rev. Lett. **104**, 140401 (2010).
[30] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).