Randomness and non-locality

Gabriel Senno[1,2], Ariel Bendersky[1,2], and Santiago Figueira[1,2]

[1]DC, FCEyN, Universidad de Buenos Aires, Buenos Aires, Argentina
[2]CONICET, Argentina

Abstract

The concepts of randomness and non-locality are intimately intertwined: outcomes of randomly chosen measurements over entangled systems exhibiting non-local correlations are, if we preclude instantaneous influence between distant measurement choices and outcomes, random. In this paper we survey some recent advances in the knowledge of the interplay between these two important notions from a quantum information science perspective.

1 Introduction

Intuitively, one describes the output of a given process as having some degree of *randomness* when it is not completely predictable. The more random it is, the more unpredictable it gets.

There is no randomness in classical mechanics. Given the initial positions and momenta of the particles of a given classical system–which in principle we can know with arbitrarily high accuracy– and their interactions, we can perfectly predict the future positions to any desired degree of precision. Classical chaotic systems are no exception to this.

In quantum theory, on the other hand, measurement results are unpredictable. The explanation for this unpredictability comes in different flavours: in the Copenhagen interpretation, the measurement process is postulated as random, whereas, for example, in Bohmian mechanics, it is deterministic but the initial conditions are randomly distributed and fundamentally unknowable.

The question of determinism versus randomness in quantum mechanics is intrinsically related to the theory's feature that have puzzled scientists the most since its origin: non-locality, the fact that measuring a property of a quantum system can instantaneously determine the results of another property measured on a distant system. Such kind of non-local influence was part of an important debate inside the scientific community. In their article of 1935 entitled "Can quantum-mechanical description of physical reality be considered complete?",

Einstein, Podolsky and Rosen [1] argue that any theory making the same predictions as quantum theory and, at the same time, avoiding such *spooky action at a distance*, as they called these non-local influences, has to postulate the existence of "real properties" which, when taken into account, allow for the complete local determination of the observations' outcomes. Since orthodox quantum theory does not include these, from the assumption of the impossibility of non-local causation one has to conclude its incompleteness. That same year, in an article with the same title, Niels Bohr argued otherwise.

It took almost 30 years for that discussion to substantially advance with Bell's 1964 celebrated result [2], which states that the predictions of quantum mechanics for certain local measurements over spatially separated entangled systems cannot be accounted for by any local theory. Furthermore, Bell provided an experimental method to test whether Nature is, indeed, non-local or not [3–5].

One of the assumptions to derive Bell's theorem –many times implicit in the presentations– is the ability to choose the measurements in a manner which is random conditioned to any state of affairs that may have any influence on the measurement outcomes. Usually referred to as *measurement independence* or *free will*, this assumption has also been termed *no-conspiracy* [6], a name that properly describes the kind of scenario arising from rejecting it. This assumption has recently regain attention from the community [7–11] in an effort to try to characterize the amount of randomness needed in Bell experiments. We will review these results, which are not only of foundational interest, but also practical given the increasing interest in device independent quantum cryptographical protocols [12–14] basing their security in Bell's theorem.

Non-local theories can be deterministic as well as non-deterministic. It is a consequence of Bell's theorem that those which are deterministic have to allow for the statistics of local measurement outcomes to be influenced by distant measurement choices. That is, they have to violate what is usually known as *parameter independence*, also, and rather misleadingly (see Section 4), referred to as *no-signaling principle* in some of the quantum information literature [15, 16]. If one opts to preclude the existence of such dependence (even when it does not allow faster-than-light signalling, as in Bohm's theory) and, so, accepts indeterminism, as the Copenhagen interpretation does, results [15–17] in quantum information theory have shown that non-local systems can be used for the information-theoretical task of randomness amplification (a task known to be classically impossible).

Stepping up one level of abstraction, one can study how non-locality and randomness compare as a computational resource. The fact that, even if we allow our local theories the use of randomness shared amongst the systems, they cannot reproduce the predictions of quantum mechanics, hints at the possibility that non-locality, viewed as a resource for information processing tasks, is more powerful than randomness. In this review we will focus in the advances [18–20] that this realization has produced in the area of computational complexity theory known as *communication complexity*.

This paper is organized as follows. In Section 2 we give a general introduction to the theory of Bell non-locality. In Section 3 we review the recent literature

on the study of the measurement independence assumption. In Section 4 we move to the outputs and study their randomness. Section 5 is devoted to a general account of the results about how non-locality improves over randomness in communication complexity. Finally, in Section 6, we give a summary and discuss future lines of research.

2 The Bell scenarios

The typical bipartite Bell scenario consists of two experimenters, Alice and Bob, each one with a box with a finite number of inputs m (the measurement choices) and a finite number of outputs r (the measurement outcomes). Let x label Alice's input choice and let a label the output (respectively y and b for Bob). The object of interest is

$$p(a, b|x, y),$$

the joint probability distribution of the outputs given the inputs.

We say that such kind of probability distribution p is *local* when we can identify a set of past common factors (usually referred to as *hidden variables*), which we label λ, and when taken into account allow for the indeterminacies in the outputs, if any, to decouple

$$p(a, b|x, y, \lambda) = p(a|x, \lambda)p(b|y, \lambda). \tag{1}$$

Since, in general, λ need not be the same over different runs of the experiment, and since it may even be out of our control, or hidden, we let it take values over a set Λ according to a probability distribution $p(\lambda)$. Combined with the above factorized form, we can write

$$p(a, b|x, y) = \int_{\Lambda} d\lambda p(\lambda)p(a|x, \lambda)p(b|y, \lambda). \tag{2}$$

Note that in writing $p(a, b|x, y)$ as above there is an important assumption being made: the hidden variables are independent of the (future) measurement choices x and y, i.e.

$$p(\lambda|x, y) = p(\lambda). \tag{3}$$

We will discuss the implications of this assumption in Section 3.

Once we have a definition of what a local distribution is, it is easy to see that some probability distributions arising in quantum theory are not local. The way we do this is by coming up with a Bell inequality, that is, a linear constraint $I = \sum_{abxy} I_{abxy}p(a, b|x, y) \leq I_L$ over p which is satisfied by every local distribution, but which can be violated by quantum distributions, i.e., distributions of the form

$$p(a, b|x, y) = tr(\rho M_{a|x} \otimes M_{b|y}), \tag{4}$$

where $tr(\cdot)$ is the trace operation, ρ is a density operator over a joint Hilbert space $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ of arbitrary dimension and $M_{a|x}$ and $M_{b|y}$ are positive operators over $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$ respectively such that $\sum_a M_{a|x} = \sum_b M_{b|y} = \mathbb{I}$.

For ease of presentation, let's consider the simplest scenario: two inputs per party $x, y \in \{0, 1\}$ with two possible outputs $a, b \in \{-1, +1\}$ each. In this setting, there is a unique (up to relabelling of the inputs and outputs) inequality that is tight on the set of local probabilities: the CHSH inequality [21, 22]

$$I := \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2,$$

where $\langle A_x B_y \rangle = \sum_{a,b} abp(a, b|x, y)$. It is easy to see that if Alice and Bob are given pairs of qubits in the singlet state $|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ and we let x label spin measurements in orthogonal directions $\hat{e_1}$ and $\hat{e_2}$ and y label spin measurements in the directions $-(\hat{e_1} + \hat{e_2})/\sqrt{2}$ and $(-\hat{e_1} + \hat{e_2})/\sqrt{2}$, the value of I for the resulting distribution is

$$I = 2\sqrt{2} > 2, \tag{5}$$

which we know from Tsirelson [23] is the maximum achievable by any quantum distribution.

All these definitions and results about the theory of Bell non-locality, although sufficient for the purposes of this paper, are only a small part of a vast theory which, for example, considers general multipartite scenarios with not necessarily symmetric number of inputs and outputs per site, and other generalizations of the like. For a thorough and complete reference, see [24].

3 Randomness at the inputs

By Bayes' rule, equation (3) is equivalent to

$$p(x, y|\lambda) = p(x, y). \tag{6}$$

This equation expresses the assumption that the inputs to a Bell test are chosen independently of the hidden variables. In the literature, this has received various names: *measurement independence* [8], λ-*independence* [25], *free will* [15] and *no-conspiracy* [6]. Complete independence of the measurement choices from any physical parameter influencing the measurement outputs, which is typically justified by an appeal to the experimentalist's free will [26], may seem too strong of an assumption and one may wonder what happens with the validity of Bell's theorem when this requirement is, somehow, relaxed. This is of special importance in cryptographical uses of Bell's theorem, where the choice of measurement is delegated to physical systems whose random behaviour cannot be guaranteed [14, 16].

In order to study the possibility of relaxing assumption (6) while still being able to separate local from non-local theories, we need a way of quantifying the dependence between the measurement choices and the hidden variables. In the

following, we review the measures proposed in the literature and the quantitative results they allow to draw from Bell violations.

In [8], it is considered

$$M := \sup_{x,x',y,y'} \int d\lambda |p(\lambda|x,y) - p(\lambda|x',y')|, \tag{7}$$

the 'maximum distance' between the distributions of the underlying variable for any two pairs of measurement settings. Clearly, with $M = 0$ we have full measurement independence and with $M = 2$ we have that there are at least two particular pairs of inputs (x, y) and (x', y') such that for any λ at most one of these settings is possible and hence there is no free will in deciding between them. With this, the fraction of measurement independence can be quantified via

$$F := 1 - M/2. \tag{8}$$

It is then shown in [8] that only by giving up 14% of measurement independence (i.e. with $F \leq 86\%$), there is a local deterministic model of the singlet correlations.

Another natural way of quantifying the dependence between the hidden variables and the measurement choices is through their mutual information [7]

$$I(x, y : \lambda) = H(x, y) + H(\lambda) - H(x, y, \lambda), \tag{9}$$

where H is the Shannon entropy. When x and y are independent of λ, $I(x, y : \lambda) = 0$. On the other hand, if x and y are functions of λ, then $I(x, y : \lambda) = H(x, y)$. In [7] it is shown that for any Bell experiment with two inputs per party, as in the CHSH scenario, there is a local model accounting for the observed correlations with an amount of mutual information not bigger than one. For example, in the ideal case of $H(x, y) = 2$, the model has $I(x, y : \lambda) \approx 0.85$.

A more operational approach to the question of measurement independence is taken by the authors of this paper and collaborators in [11]. They consider the case in which the parties in a Bell test use pseudo-random numbers generators (PRNGs) to choose the inputs. They show that, in such scenario, there is local model in which the hidden variables, after finitely many rounds and without access to the PRNGs used by the parties, start to perfectly predict the future measurement choices, allowing them to fake any non-local behaviour. Granted, the possibility that physical hidden variables behave in this way is quite implausible and conspiratorial (a feature, albeit, shared with most of the other local models which exploit experimental loopholes [8, 27, 28]). However, the scenario becomes significantly plausible when we consider a cryptographical context in which we are not testing quantum mechanics but rather using devices as black boxes received from some untrusted provider and basing the security of our protocols on the observed non-local behaviour.

All these results seem to suggest that there needs to be a substantial degree of randomness in the measurement choices if we want to see non-locality. Surprisingly enough, it has been shown that, on the contrary, in some scenarios non-locality manifests even with arbitrarily small amounts of randomness [16, 29].

This is the key insight behind the theory of randomness amplification using quantum non-locality, which we review in the following section.

4 Randomness at the outputs

The factorized form (1) is equivalent to the conjunction of

$$p(a|x,y,\lambda) = p(a|x,\lambda), \qquad p(b|x,y,\lambda) = p(b|y,\lambda) \tag{10}$$

and

$$p(a|b,x,y,\lambda) = p(a|x,y,\lambda), \qquad p(b|a,x,y,\lambda) = p(b|x,y,\lambda). \tag{11}$$

Condition (10) is usually referred to as *parameter independence* [30], although it has also been dubbed *no-signaling principle* [15]. This last name is not to be confused with the related notion of a *no-signaling* distribution, i.e. those which satisfy

$$p(a|b,x,y) = p(a|x,y), \qquad p(b|a,x,y) = p(b|x,y). \tag{12}$$

Every theory that is no-signaling at the level of the hidden variables, i.e. satisfying (3), also satisfies (12), but the converse does not hold (Bohmian mechanics being the most prominent example of this).

Non-local correlations can be accounted for both by deterministic and non-deterministic theories. We say that a hidden variables theory is *deterministic* when

$$p(a|x,y,\lambda), p(b|x,y,\lambda) \in \{0,1\} \forall a,b,x,y,\lambda \tag{13}$$

It is easy to see that every deterministic theory satisfies (11) and hence any non-local deterministic theory has to violate parameter-independence. Now, the question is

> If we assume parameter-independence (10), what can we say about the amount of randomness in the outputs of non-local systems?

This question has led to remarkable results in the information-theoretical task of *randomness amplification*. The goal of randomness amplification is to use an input source $\mathcal{S}$ of imperfectly random bits to produce perfect random bits that are arbitrarily uncorrelated from all the events that may have been a potential cause of them, i.e. arbitrarily free. In general, $\mathcal{S}$ produces a sequence of bits $x_1, x_2, \ldots, x_j, \ldots$ with $x_j \in \{0,1\}$ for all j such that

$$\epsilon \leq p(x_j|e) \leq 1-\epsilon \tag{14}$$

for all j and e, where $0 \leq \epsilon \leq 1/2$ and where the variable e can correspond to any event that could be a possible cause of bit x_j. Free random bits correspond to $\epsilon = 1/2$; while deterministic ones, i.e. those predictable with certainty by an

observer with access to e, correspond to $\epsilon = 0$. This type of randomness sources is known as Santha-Vazirani (SV) sources [31]. The aim is then to generate, from arbitrarily many uses of $\mathcal{S}$, a final source $\mathcal{S}_f$ of ϵ_f arbitrarily close to $1/2$. If this is possible, no cause e can be assigned to the bits produced by $\mathcal{S}_f$, which are then fully unpredictable.

It is a fundamental result in classical information theory that randomness amplification is impossible using classical resources [31]. In the quantum regime, on the other hand, it has been shown in a series of remarkable results in the last years that randomness amplification is indeed possible [15, 16, 32]. The general scheme followed by all these randomness amplification quantum protocols consist on using the input SV source to choose the measurement settings in a Bell test and deriving from the observed violation a bound on the distance between the distribution of the outputs at one of the parties and the uniform distribution. This bound is then proven to go to zero as the number of inputs settings (i.e. the number of uses of the SV source) goes to infinity. In the following, and for ease of presentation, we review the first of these protocols.

In [15], the authors provide a Bell test such that if an SV source with $0.442 < \epsilon \leq 0.5$ is used to choose the measurement settings, free random bits are produced. More specifically, they consider a bipartite Bell scenario with N measurements per party $x \in \{0, 2, \ldots, 2N-2\}$ and $y \in \{1, 3, \ldots, 2N-1\}$ with two possible outcomes $a, b \in \{-1, +1\}$ each. The Bell expression used is

$$I := P(a = b \mid 0, 2N-1) + \sum_{x,y|x-y|=1} P(a \neq b \mid x, y)$$

which is lower bounded by 1 on local distributions and for which there are quantum distributions such that

$$I_N = 2N \sin^2 \frac{\pi}{4N} \tag{15}$$

which tends to 0 in the limit of large N. It is then shown that with $N = 2^r$ and choosing the measurements for each party with r uses of an SV $(1-\delta)$-source, for every $P(a, b \mid x, y, \lambda)$ satisfying parameter-independence (10)

$$D\left(P(a, \lambda \mid x, y), \lambda(a) \times P(\lambda \mid x, y)\right) \leq \frac{I_{2^r}}{2} \left(\frac{1+2\delta}{1-2\delta}\right)^{2r}$$

where $\lambda(\cdot)$ is the uniform distribution over $\{-1, +1\}$ and D is the total variation distance,

$$D(P, Q) = \sum_x \mid P(x) - Q(x) \mid . \tag{16}$$

Substituting I_{2^r} with the value of obtainable in quantum theory (15), it is easy to see that, in the limit of large r and provided $\delta < (\sqrt{2}-1)^2/2 \approx 0.086$, this bound goes to 0, implying that the distribution of Alice's outputs is indistinguishable from a fair coin.

The authors of [15] also conjectured that a similar protocol should exist to amplify randomness from arbitrarily weak randomness sources. In a remarkable result [16], this conjectured was proven true, although the protocol presented required a Bell scenario with an unbounded number of systems. Finally, this limitation was recently overcome in [32], where a protocol that uses only two systems to perform full randomness amplification of arbitrarily weak randomness sources is given.

Before ending this section, it is important to remark, once again, that the conclusions of the above reviewed works rest on the assumption of parameter-independence. The existence of interpretations of quantum mechanics violating parameter-independence, like e.g. Bohm's theory, should refrain us from extrapolating their results to quantum mechanics itself (or Nature, for that matter).

5 Randomness vs. non-locality in communication complexity

Communication complexity theory, introduced by Andrew Yao in 1979 [33], studies the communication requirements in the distributed computation of functions. More formally, given a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, it asks how many bits, in the worst case, have to be exchanged between Alice holding input $x \in \{0,1\}^n$ and Bob holding input $y \in \{0,1\}^n$ in order for him to output $f(x,y)$.

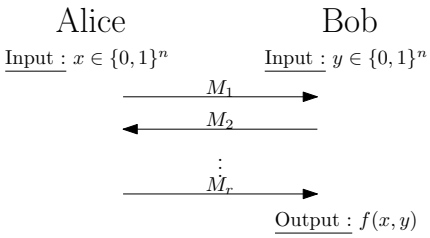

Figure 1: Illustration of Communication Complexity's model

A natural extension to this model is to allow the players to send messages which still depend on the input and the previous messages but also on some random string $\lambda \in \{0,1\}^*$. In this model, also defined by Yao [34], we allow error with small probability. Since the computation is distributed, we can imagine two kinds of randomness. The first one is *private randomness* where each player has his own source of randomness which is unknown by the other player. The second one is *public randomness* where the players share the same source of randomness and can use it to coordinate their behavior. We can simulate private randomness using public coins, and the natural question is how much one can gain by using public randomness instead of private. Newman [35] showed that the best that one can gain is logarithmic in the size of the input, so there is no

significant difference between private and public randomness in communication complexity.

The standard scenario of functions easily generalizes to the simulation of probability distributions. Now, Alice gets input x, Bob gets input y, and after exchanging bits, Alice has to output a and Bob b such that the joint distribution is some given $p(a, b \mid x, y)$.

This allows us to recast the theory of non-locality in the language of communication complexity: local distributions are those that can be simulated with zero bits of communication and access to some shared randomness λ. It then follows from its non-locality that in order to simulate the singlet correlations with shared randomness, we need to communicate at least one bit of information. In fact, one bit is sufficient as proven in [36], a result later extended in [37] to two bits for the correlations arising from two-outcome measurements over arbitrary-dimension bipartite quantum states. The fact that in order to simulate non-local correlations we need a minimal amount of communication, brings up the question of whether there are functions for which having non-locality as a resource helps reduce its communication complexity.

Indeed, the very first protocol [38] offering an advantage on communication complexity using quantum resources was based on a quantum violation of the following 2-inputs-2-outpus tripartite Bell inequality due to Mermin [39]:

$$\langle A_0 B_1 C_1 \rangle + \langle A_1 B_0 C_1 \rangle + \langle A_1 B_1 C_0 \rangle - \langle A_0 B_0 C_0 \rangle \leq 2.$$

This inequality is violated to its algebraic maximum of 4 by the correlations arising from each party measuring in the $\hat{x}$ or $\hat{y}$ spin direction over the shared tripartite GHZ [40] state $|GHZ\rangle := 1/\sqrt{2}(|000\rangle + |111\rangle)$. In [38] it is shown that players Alice, Bob and Charlie having access to these quantum correlations can compute the function $f : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,

$$f(x, y, z) = x_1 \cdot y_1 \cdot z_1 + \cdots + x_n \cdot y_n \cdot z_n$$

by communicating two bits, while the best classical strategy needs three bits. This approach of going from a Bell inequality violation to a function for which there is a quantum communication complexity advantage was later generalized to a large family of Bell inequalities in [41]. In parallel, other quantum protocols offering a communication complexity advantage were being discovered [18,42,43] for which, although suspected, it was not clear whether non-locality or other future of quantum mechanics was the responsible for the improved communication efficiency.

In a recent breakthrough, it has been shown by Buhrman et al. [44] that, indeed, non-locality is the key future of quantum mechanics responsible for the advantages in communication complexity. More formally, they have shown that for every communication complexity problem for which there is a quantum protocol achieving a (greater than quadratic) advantage over all classical strategies with shared randomness, there is a Bell inequality and a quantum distribution that violates it. This result, using different techniques, will be complemented by one of the authors and collaborators in a forthcoming paper [45].

6 Discussion

We have reviewed the relationship between the concepts of randomness and non-locality from two different perspectives.

First, from a dependencies point of view, we have seen that, although arbitrarily small, you need randomness in the measurement choices in order for non-locality to manifest itself. We have also seen that when this happens, quantum theories complying with parameter-independence, like the Copenhagen interpretation, predict that non-local correlations can be used to certify intrinsic randomness.

Second, from a resources point of view, we have seen that non-locality is comparatively stronger than shared randomness when it comes to the distributed computation of functions. In fact, it is the key future of quantum mechanics providing its advantage over classical strategies.

Future lines of research are vast. For the measurement independence assumption, it would be interesting to understand the relationship between the computability loophole recently presented in [11] and the measures of independence studied in Section 3. It does not seem obvious how to characterize the fact that the measurement choices are made pseudo-randomly in terms of the existing dependency measures. With regard to the randomness of the outputs in Bell experiments, an interesting direction one can take is to move from a statistical approach to an instances approach. That is, instead of looking at the distribution of the outputs and studying how close it is from the uniform distribution, looking at individual sequences of outputs and studying how random (or patternless) they are. This approach has been recently taken by Wolf [46] using one of the tools that computer science provides for this task: the theory of Kolmogorov Complexity [47]. Finally, in the area of communication complexity, one of the most important open questions is whether there exists total functions for which the communication complexity using quantum resources is exponentially smaller than using shared randomness. At present the only exponential separations known are for so-called promise functions, that is, functions whose domain is a proper subset of $\{0,1\}^n \times \{0,1\}^n$. For non-promise (or total) functions, the biggest separations known are polynomial in n.

References

[1] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical review* **47** (1935) 777.

[2] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics* **1** (1964) 195–200.

[3] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten and C. ABellán, "Loophole-free Bell in-

equality violation using electron spins separated by 1.3 kilometres", *Nature* **526** (2015) 682–686.

[4] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann and A. Zeilinger, "Significant-loophole-free test of Bell's theorem with entangled photons", *Phys. Rev. Lett.* **115** (2015) 250401.

[5] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. ABellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill and S. W. Nam, "Strong loophole-free test of local realism", *Phys. Rev. Lett.* **115** (2015) 250402.

[6] T. Norsen, "John S. Bells concept of local causality", *American Journal of Physics* **79** (2011) 1261–1275.

[7] J. Barrett and N. Gisin, "How much measurement independence is needed to demonstrate nonlocality?", *Physical review letters* **106** (2011) 100406.

[8] M. J. Hall, "Local deterministic model of singlet state correlations based on relaxing measurement independence", *Physical review letters* **105** (2010) 250404.

[9] D. E. Koh, M. J. Hall, J. E. Pope, C. Marletto, A. Kay, V. Scarani and A. Ekert, "Effects of reduced measurement independence on Bell-based randomness expansion", *Physical review letters* **109** (2012) 160404.

[10] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford and T. Jennewein, "Violation of local realism with freedom of choice", *Proceedings of the National Academy of Sciences* **107** (2010) 19708–19713.

[11] A. Bendersky, G. de la Torre, G. Senno, S. Figueira and A. Acin, "Implications of computer science principles for quantum physics", *arXiv preprint arXiv:1407.0604* .

[12] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution", *Physical review letters* **113** (2014) 140501.

[13] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices", in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (ACM, 2014), pp. 417–426.

[14] L. Masanes, S. Pironio and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices", *Nature communications* **2** (2011) 238.

[15] R. Colbeck and R. Renner, "Free randomness can be amplified", *Nature Physics* **8** (2012) 450–453.

[16] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita and A. Acín, "Full randomness from arbitrarily deterministic events", *Nature communications* **4**.

[17] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski and R. Ramanathan, "Free randomness amplification using bipartite chain correlations", *Physical Review A* **90** (2014) 032322.

[18] R. Raz, "Exponential separation of quantum and classical communication complexity", in *Proceedings of the thirty-first annual ACM symposium on Theory of computing* (ACM, 1999), pp. 358–367.

[19] Z. Bar-Yossef, T. S. Jayram and I. Kerenidis, "Exponential separation of quantum and classical one-way communication complexity", in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing* (ACM, 2004), pp. 128–137.

[20] R. Cleve, W. van Dam, M. Nielsen and A. Tapp, "Quantum entanglement and the communication complexity of the inner product function", in *Quantum Computing and Quantum Communications* (Springer Berlin Heidelberg, 1999), pp. 61–74.

[21] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical review letters* **23** (1969) 880.

[22] A. Fine, "Hidden variables, joint probability, and the Bell inequalities", *Physical Review Letters* **48** (1982) 291.

[23] B. S. Cirel'son, "Quantum generalizations of Bell's inequality", *Letters in Mathematical Physics* **4** (1980) 93–100.

[24] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, "Bell nonlocality", *Reviews of Modern Physics* **86** (2014) 419.

[25] A. Brandenburger and N. Yanofsky, "A classification of hidden-variable properties", *Journal of Physics A: Mathematical and Theoretical* **41** (2008) 425302.

[26] J. S. Bell, A. Shimony, M. A. Horne and J. F. Clauser, "An exchange on local beables", *Dialectica* **39** (1985) 85–110.

[27] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories", *Phys. Rev. D* **10** (1974) 526–535.

[28] J.-Å. Larsson and R. D. Gill, "Bell's inequality and the coincidence-time loophole", *EPL (Europhysics Letters)* **67** (2004) 707.

[29] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang and N. Gisin, "Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality", *Physical review letters* **113** (2014) 190402.

[30] A. Shimony, "Events and processes in the quantum world", in *Quantum Concepts in Space and Time*, eds. R. Penrose and C. J. Isham (New York ;Oxford University Press, 1986), pp. 182–203.

[31] M. Santha and U. V. Vazirani, "Generating quasi-random sequences from semi-random sources", *Journal of Computer and System Sciences* **33** (1986) 75–87.

[32] R. Ramanathan, F. G. Brandão, K. Horodecki, M. Horodecki, P. Horodecki and H. Wojewódka, "Randomness amplification against no-signaling adversaries using two devices", *arXiv preprint arXiv:1504.06313* .

[33] A. C.-C. Yao, "Some complexity questions related to distributive computing (preliminary report)", in *Proceedings of the eleventh annual ACM symposium on Theory of computing* (ACM, 1979), pp. 209–213.

[34] A. C.-C. Yao, "Lower bounds by probabilistic arguments", in *Foundations of Computer Science, 1983., 24th Annual Symposium on* (IEEE, 1983), pp. 420–428.

[35] I. Newman, "Private vs. common random bits in communication complexity", *Information processing letters* **39** (1991) 67–71.

[36] B. F. Toner and D. Bacon, "Communication cost of simulating Bell correlations", *Physical Review Letters* **91** (2003) 187904.

[37] O. Regev and B. Toner, "Simulating quantum correlations with finite communication", *SIAM Journal on Computing* **39** (2009) 1562–1580.

[38] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Physical Review A* **56** (1997) 1201.

[39] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states", *Phys. Rev. Lett.* **65** (1990) 1838–1840.

[40] D. M. Greenberger, M. A. Horne and A. Zeilinger, "Going beyond Bell's theorem", in *Bells theorem, quantum theory and conceptions of the universe* (Springer, 1989), pp. 69–72.

[41] Č. Brukner, M. Żukowski, J.-W. Pan and A. Zeilinger, "Bell's inequalities and quantum communication complexity", *Physical review letters* **92** (2004) 127901.

[42] H. Buhrman, R. Cleve, S. Massar and R. de Wolf, "Nonlocality and communication complexity", *Rev. Mod. Phys.* **82** (2010) 665–698.

[43] H. Buhrman, R. Cleve and W. van Dam, "Quantum entanglement and communication complexity", *SIAM Journal on Computing* **30** (2001) 1829–1841.

[44] H. Buhrman, Ł. Czekaj, A. Grudka, M. Horodecki, P. Horodecki, M. Markiewicz, F. Speelman and S. Strelchuk, "Quantum communication complexity advantage implies violation of a Bell inequality", *Proceedings of the National Academy of Sciences* **113** (2016) 3191–3196.

[45] S. Laplante, M. Laurière, A. Nolin, J. R. Roland and G. Senno, "Inefficiency resistant exponential Bell inequality violations from communication complexity", *In preparation* .

[46] S. Wolf, "Nonlocality without counterfactual reasoning", *Physical Review A* **92** (2015) 052102.

[47] M. Li and P. Vitányi, *An introduction to Kolmogorov complexity and its applications* (Springer Science & Business Media, 2013).