eur.esis journal

eur.esis Association for the Promotion of the Scientific Endeavour

Volume 6
Winter 2014

journal homepage
www.euresisjournal.org

Randomness in quantum physics

Antonio Acín

ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
ICREA-Institució Catalana de Recerça i Estudis Avançats. 08010 Barcelona, Spain
antonio.acin@icfo.es

Abstract

This article discusses recent advances in the characterization and quantification of randomness in Quantum Physics.

1. Introduction

Randomness is an intriguing concept which has attracted and keeps attracting the interest of many different scientific communities. From a fundamental point of view, a crucial question in Physics (and even Philosophy) is whether nature is deterministic or intrinsically random. Strictly speaking, there is no such a thing as true randomness in our "classical" world. At our macroscopic scale, nature is correctly described by Newtonian Physics, where randomness is simply a consequence of lack of knowledge or control. Indeed, in any physical situation involving different particles, if an observer has a complete description of the initial positions and velocities of the particles and the interactions among them, he can predict with certainty the status of these particles at any given time. Although this may be an extremely difficult task, as it may require unlimited computational capabilities, perfect predictability is in principle possible. This (classical) determinism can be found, for instance, in the introduction to the book *A Philosophical Essay on Probabilities* by Pierre-Simon Laplace [1]:

> *We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.*

Classical Physics, thus, is inherently deterministic. Of course, there are classical processes that are hard to predict and display some apparent form of randomness. Chaotic systems probably constitute the most relevant example of these processes, as an extremely good knowledge of their initial conditions is required to predict their future behavior. Still, any form of classical randomness is not *intrinsic* to the theory, as it can always be reduced, ideally to zero, by improving the knowledge on the initial conditions.

Things become much subtler when moving to the microscopic world. At that scale, Newtonian laws cease to offer a correct description of nature and one has to adopt Quantum Physics. It is common folklore to argue that Quantum Physics is *intrinsically random*. Still, why is quantum randomness intrinsically different from any form of classical randomness? Or, in other words, why is it impossible to reduce quantum randomness to ignorance, lack of knowledge or control, as in the classical world? This is the first point we discuss in what follows. Once the presence of a new form of randomness in the quantum world has been argued, we will move to more applied issues and see how quantum randomness can be detected, quantified and used for practical applications. In fact, random numbers represent a valuable resource which find application nowadays in many tasks, from cryptographic applications, to gambling or the simulation of physical and biological systems.

2. Intrinsic Quantum Randomness

It is well known that Quantum Physics can only predict the probabilities of events. The simplest example illustrating this fact consists of a spin-one-half particle, whose spin is pointing in the z direction. If the spin of the particle is measured along the x basis, the theory predicts that the two possible results, labeled by $+1$ and -1, will occur with equal probability. In the considered scenario, there is a device that prepares the spin of the particle along the z basis, and another device that performs the measurement on the particle. The experiment is repeated many times and the frequency of ± 1 results tend to $(1/2, 1/2)$ as predicted by quantum theory.

This type of situations are often presented as paradigms of the randomness of Quantum Theory. Still, there is nothing really quantum on it. From the point of view of randomness, it is completely equivalent to flipping a perfect coin: the two results will appear with equal probabilities. As mentioned in the previous section, if we had a perfect knowledge about the coin, its initial position and velocity, we could predict the result by solving the equations of motion (even if on average the two results happen with the same probability). One cannot exclude the existence of a similar explanation for the quantum particle. Clearly, the corresponding variables and equations of motion cannot be those of Quantum Physics. Still, there may be a better theory containing the right variables and formalism to predict the result of each single measurement. These models are usually known as *hidden-variable models* for Quantum Physics. Although historically introduced in a different context, hidden-variable models have a clear interpretation in terms of randomness: their existence would imply that quantum randomness is simply a consequence of the ignorance of these hidden variables that completely specify the result of each measurement. Once a new theory based on these, at the moment, unknown or hidden variables is found, quantum randomness will disappear and become an artifact not intrinsic to the theory, as in the classical case. Actually, it is always possible to construct hidden-variable, and deterministic, models for any experiment involving measurements on a single quantum particle. The existence of these models implies that, from the point of view of randomness, there is no fundamental difference between measuring a quantum particle or flipping a coin.

The situation becomes much subtler when moving to scenarios involving different measurements on two, or more, correlated quantum particles. Let's stop here for a while and make a small historical *détour* through the Foundations of Quantum Physics. Here, the discussion connects with the famous work by Einstein, Podolsky and Rosen (EPR) [2] on the existence of hidden-variable models for correlated quantum particles, also known as entangled particles, and its refutation by Bell [3]. In their seminal paper of 1935 [2], EPR introduced two main properties that, according to them, any reasonable physical theory should satisfy: locality and realism. The precise definitions of these two concepts has led to many controversies and we will not discuss them here for reasons that will become clear below. Then, EPR studied the correlations obtained by measuring a two-particle entangled state and argued that the wave function (or, more generally, quantum physics) "does not provide a complete description of the physical reality" and it has to be understood as an effective theory. They also left "open the question of whether or not such a description exists" and conjectured that "such a theory is possible." Again, this alternative description would make use of some variables that are hidden (unknown) at the moment. In 1964 Bell showed that all theories satisfying the principles of locality and realism are unable to predict the same observable quantities as Quantum Physics. More precisely, he considered a simple experiment in which a source prepares two correlated quantum particles that are sent to two distant measuring devices (see Figure 1). At these devices, two different measurements of two possible results are performed. It is assumed that the two devices do not communicate when the measurements are performed. This can be enforced by arranging the setup so that the measurements define space-like separated events. In this configuration, one can see that local-realistic models *à la* EPR predict some bounds on the correlations between the results observed in the two measuring devices that are violated by measurements on some correlated (entangled) quantum particles. These bounds are known as Bell inequalities and their experimental violation in 1982 [4] confirmed that local-realistic models are unable to predict those correlations observed in nature. The violation of Bell inequalities is often also known as non-locality, and the correlations leading to this violation as non-local.

What does all this discussion mean from the point of view of randomness? Our goal for the remaining of this section is to see how all the EPR-Bell discussion can be reinterpreted in

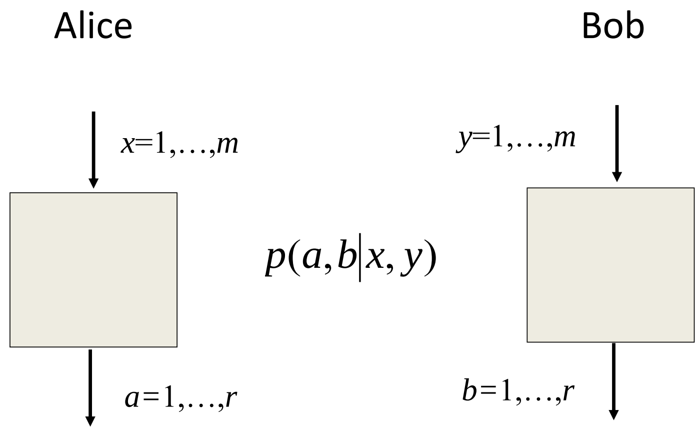

Figure 1: *Bell scenario. The standard Bell scenario consists of two distant users, Alice and Bob, who have access to two different systems. Alice and Bob can perform one out of m possible measurements on their respective systems, labeled by x and y. The results of the measurements can take r possible values and are labeled by a and b. The whole setup is described by the observed statistics $p(a,b|x,y)$, that is, the joint of probability of observing results a and b when performing measurements x and y.*

terms of randomness and implies the existence of a new form of randomness in the quantum domain with no classical analog. First of all, while the terms locality and realism are always used when referring to EPR models, it is much more convenient to replace them by more operational terms such as no-signalling and determinism. We believe these two concepts encapsulate in a clearer way the motivations behind the EPR program.

The no-signalling principle states that faster-than-light communication is impossible. It is probably the most accepted physical principle as it is one of the pillars of Einstein's relativity. Actually, even if Einstein's Relativity was proven to be wrong, in the sense that there are particles traveling faster than light, the no-signalling principle only requires that this velocity is finite. In a way, it is just a consequence of the fact that energy cannot be unbounded, or, more in general, of the belief that there is a finite limitation for any physical effect. In the previous experimental configuration, the principle implies that the statistics seen by one of the observers when measuring his particle cannot depend on the choice of measurement performed by the other particle. Indeed, if this was the case, one of the observers could, by changing his choice of measurement, produce a noticeable effect on the other. This effect could be immediately used to exchange communication faster than the speed of light, as the two measurements could be arranged so that they defined space-like separated events.

Determinism states that the statistics seen in an experiment can be decomposed as mixtures of deterministic correlations in which each measurement result has a deterministic output. In deterministic models, while it is accepted that an experimental result produces a "random" result, like when flipping a coin, this is only a consequence of the ignorance of the actual state of the system. Each repetition of the experiment does have an a priori defined result, but we only have access to the average description (because of lack of control or knowledge of the setup).

It is not difficult to see that the correlations predicted by deterministic and no-signalling models are exactly the same as predicted by EPR models [5]. Once the equivalence is proven, the experimental violation of Bell inequalities automatically implies that either determinism or no-signalling has to be abandoned (or both!). Most physicists prefer to abandon determinism to save no-signalling. Thus, under the assumption that nature satisfies the no-signalling principle, the experimental violation of any Bell inequality implies that the outcomes could not be predetermined in advance. A new form of randomness, intrinsic to the theory and that cannot be reduced to ignorance, then appears. The only possible deterministic explanation is by models which use deterministic, but signalling states. In these models, randomness would disappear and the observers could deterministically predict the measurement output of each repetition of the experiment if they had access to the actual state of the system. But having access to this state would also allow them to exchange communication instantaneously. If no-signalling is assumed to be a physical principle of nature, the random character of outcomes leading to a Bell inequality violation follows.

While all the previous statements have a rigorous mathematical proof, the connection between Bell violation, no-signalling and randomness can also be understood from an intuitive point of view. Quantum Mechanics predicts a strong form of correlations that violate Bell inequalities. The correlations are so strong that they could be used for supra-luminal communication, or signalling, if we could completely monitor them. The only possibility for these correlations to be compatible with the no-signalling principle is that the observed outcomes cannot be controlled or predicted and, therefore, are random.

Before concluding this section, we come back to the assumptions that imply the existence of intrinsic randomness in any Bell experiment. As mentioned, no-signalling is one of them. Another crucial assumption is the fact that the measurements applied by each of the two measuring devices can be freely chosen. Or, in other words, it is required that the choice of these settings is random, in the sense that it cannot be predicted in advance. If this assumption is completely relaxed and the measurements that are going to be performed can be completely predicted in advance, in particular before the particles leave the source, then it is easy to construct deterministic no-signalling models leading to Bell violations. The assumption of free-choice may seem very natural, as, for instance, in the ultimate Bell experiment, where human beings could choose the measurements in two distant labs (this assumption is often referred as the free-will assumption). This is why we decided to present this assumption separately from the previous discussion. Still, the implications of Bell inequality violations are fundamentally so relevant that it is important to keep in mind that there is another possible explanation: the choice of settings was known, in the sense that could be predicted, in advance.

In the next sections, we will work under the assumption that nature is no-signalling and, thus, intrinsically random. Actually, we will assume more and impose that those correlations that are possible in nature are those of Quantum Physics. In other words, we will impose that there do not exist in nature no-signalling correlations that cannot be obtained by measuring quantum states (in principle, there could be stronger-than-quantum correlations without violating the no-signalling principle [6]. Under these assumptions, we provide tools to detect and quantify the *intrinsic quantum randomness* produced in a Bell experiment. Then, we discuss the application of these techniques to the construction of new types of random-number generators with no classical analog.

3. Random-Number Generation

Before moving to the results linking randomness and Bell inequality violation, it is worth commenting on the use and generation of random numbers for practical applications. Beyond all the previous fundamental points, randomness is also an extremely valuable resource in our society with applications in many different areas [7]. Random numbers are constantly used for cryptographic applications, gambling or numerical methods for the simulation of physical and biological systems. Due to their relevance, there is an intensive ongoing effort to (i) develop good sources of random numbers and (ii) design reliable tests to certify the random nature of the generated numbers. These two issues are strongly connected as the quality of a source is estimated using the tools developed for certification. Randomness certification is indeed a crucial question and, as discussed below, it is notoriously difficult to ascertain with the existing techniques the random properties of a device.

Nowadays, there basically exist three types of random number generators (RNG): “true” RNG, pseudo-random number generators and quantum RNG. In the first case, some initial numbers are generated by means of a physical process that is hard to predict, such as the noise in electrical circuits or the timing of user processes. Pseudo random number generators consist of the output of a deterministic function applied to a shorter seed, assumed to be random and possibly produced by a true RNG. Finally, quantum RNG uses quantum features for the generation of the random numbers. However all these solutions suffer from the following three drawbacks, which are relevant both from a conceptual and applied point of view.

The first problem concerns the issue of *randomness verification*. Although all these different approaches to randomness generation are based on different principles, they all use the same framework to certify the randomness of the produced numbers: it is always measured by a series of statistical tests [8, 9] designed to check the absence of patterns in the generated sequences. It is however unclear what passing all these tests means from the point of view of randomness. No finite set of tests can be considered complete [9], since the existence of patterns that are not covered by the existing battery of tests can never be excluded. In particular, the tests should be periodically revaluated and, if needed, corrected[1]. Thus, it is highly non-trivial, if not impossible, to ascertain with the existing techniques the random character of an experiment.

Second, many applications, especially for cryptographic purposes, require *private randomness*. In these applications, the randomness, or unpredictability, of the generated events is exploited to achieve a given task, such as secure information transmission. This requires that the numbers generated by the device should not only appear random, in the sense of hard to predict to the honest user, but also to any other, potentially adversarial, user. Unfortunately, the reliability of the statistical tests is even less clear in these applications. For instance, systematic errors in the generators can introduce patterns that may be undetected by the statistical tests applied by the honest user, but predicted by a computationally more powerful adversary. These patterns can then be exploited to break the cryptographic protocol.

Third, the situation becomes more critical in the non-trusted provider scenario, where the devices used for the generation cannot be trusted and should be seen as a black box generating the numbers. In this scenario, there cannot be any classical technique proving the presence of private randomness. Indeed, one can never exclude, for instance, that the numbers have been prepared in advance by an adversary using a very “good” RNG. These numbers have been copied into a memory inside the device and then, despite looking random, can be completely predicted by this adversary. In order to avoid this problem, the proposal for randomness generation should be *device-independent*: the random properties of the generated numbers should not rely on any modeling of the internal working of the devices used in the generation. The device-independent property provides a second advantage for randomness generation: as the scheme does not depend on the internal working of the devices, it is more robust to prepare imperfections or drifts during the generation process.

Finally, there is a fourth issue which only concerns the existing quantum solutions. It seems quite unsatisfactory, and even contradictory, to verify their quality by means of the same techniques used for classical devices, which are always of deterministic nature. It is hard to claim that an intrinsic quantum property has been used for randomness generation if this is certified by tests which are also satisfied by classical devices. It would then be desirable to derive new forms of randomness certification based on quantum principles with no classical analogue. This is intimately related to the fact that, although Quantum Physics contains an intrinsic form of randomness, in any real situation this randomness is necessarily mixed-up with an “apparent” randomness that results from noise in the system or lack of control of

[1] One of the most famous examples of bad RNG was RANDU, a RNG used in the 60-70’s which was later discovered to have a well-defined pattern, see for instance RANDU in wikipedia.

the experiment. In order to disentangle these two forms of randomness, one should derive *tools to detect and quantify the intrinsic quantum randomness* generated in an experimental setup.

4. Random numbers certified by Bell's Theorem

The scope of this section is to present the approach to randomness generation introduced in [10], that exploits the link between Bell inequality violation and randomness mentioned above. This link allows for the first time to quantify the intrinsic quantum randomness in an experimental setup, which can now be disentangled from any apparent randomness associated to imperfections or lack of knowledge. These techniques can be used to design a new type of RNG leading to numbers which are (a) certifiably random, (b) cryptographically secure and (c) device-independent. Finally, the techniques were applied in a real setup involving two distant ions to demonstrate the experimental generation of fresh quantum randomness. Without entering into the detailed explanation of this work, the main results obtained are:

Quantum non-locality and randomness. The first result consists of a link between randomness and the violation of Bell inequalities. As mentioned previously, Bell inequalities are conditions satisfied by all models à la EPR. From a more operational point of view they also define limits on the way two separated devices can be correlated by means of classical instructions. These inequalities can be violated by the results of measurements performed on systems of two quantum particles. It is shown in [10] how to derive bounds on the amount of randomness produced in a quantum setup from the observed Bell violation. These bounds can be then used to certify and quantify the presence of intrinsic quantum randomness in the setup.

The scenario is the same as in Figure 1. Two separated observers perform different measurements, labeled by x and y, on two quantum particles and get measurement results a and b. By repeating this process, they can estimate the joint probability distribution, $P(a, b|x, y)$, of getting result a and b when they applied measurements x and y. From this distribution, the observers can compute the violation of a Bell inequality. If a violation is observed, then they can guarantee that the observed outcomes have some randomness. Actually, one can establish a quantitative link between the observed Bell violation and the amount of randomness. These findings show that the more the particles are quantically correlated (in the sense of violating a Bell inequality), the more random the measurement outcomes are. That is, they constitute a fundamental link between non-local quantum correlations and randomness, two of the main intrinsic and counter-intuitive properties of Quantum Theory.

Device-Independent Quantum Random Number Generator. The previous bounds can be used to realize a new type of quantum random number generator (QRNG). As mentioned, and contrary to all previous solutions, the scheme produces randomness which is (a) certifiable, (b) private and (c) device-independent. It is based on a previous proposal by Colbeck [11].

In what follows, it is useful to work in the non-trusted provider scenario and, thus, assume that the user gets two devices from a non-trusted provider. Using these devices, the user should be able to perform a Bell test, as explained before and shown in Figure 1. The final string of perfectly random bits will be made out of N pairs of results, $(a_1, b_1, ..., a_N, b_N)$, obtained by N uses of the devices. The random character of the generated numbers is guaranteed by the violation of a Bell inequality. Importantly, this holds true in a scenario where the internal workings of the device are not known, and even if the devices were prepared by an external agent who should not be able to bias or predict the random bits. This follows from the previous analysis: whatever the adversary prepared in the device for generating the output given the input, if it violates a Bell inequality, then there is a bound on the randomness of the outputs. A memory attack, for instance, in which the provider has generated in advance and copied the numbers into memories located in the devices is impossible, as this would represent an EPR model for the measurement outcomes which is impossible because of the observed Bell violation.

There is however an important point: the user of the devices does not know a priori whether the devices violate the Bell inequality and must estimate this using a statistical test. But the estimate cannot be carried out in a predetermined way. Indeed, if the measurement settings that are going to be used are known in advance, then the external agent may have prepared a device which is completely deterministic, but which is such that on the specific sequence of inputs that are going to be used it appears to violate a Bell inequality. As mentioned above, it is always possible to mimic Bell inequality violations with a hidden-variable model if settings can be predicted in advance. There is thus an apparent contradiction between the aim of making a random number generator, and the requirement of using random settings to test the device. It is however possible to carry out the statistical test using only a very small amount of randomness, much smaller than the amount of randomness generated by the measurements. Thus, non-trusted devices that violate a Bell inequality can actually be used as *randomness expanders* in which a small random seed is expanded into a much longer random string.

Experimental generation of private random numbers. Finally, a proof-of-principle experiment of the theoretical formalism was demonstrated, by performing a Bell violation between two atoms located in two separated traps (see Figure 2). These traps should then be seen as the physical realizations of the abstract boxes in the Figure 1. The different measurement can be chosen by sending different micro-wave pulses into the atoms. The measurement results have two outcomes, which correspond to whether the atom emits fluorescence light back after the pulse.

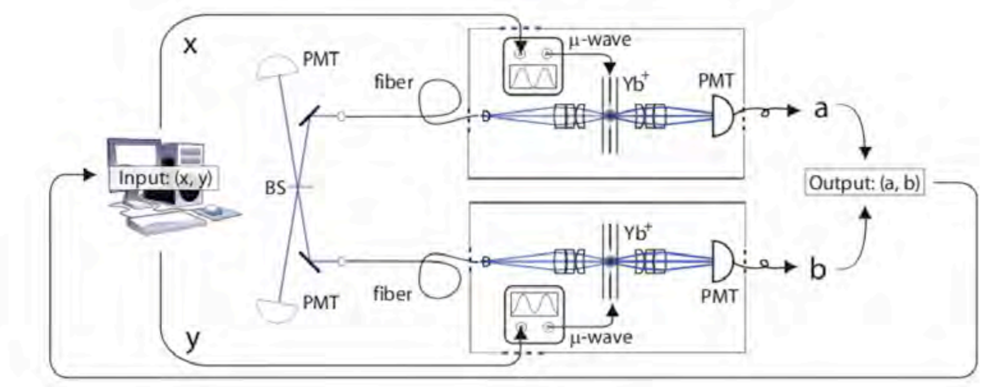

Figure 2: *Experimental setup for randomness generation. The figure shows the schematic representation of the experimental setup. The two particles in the two separated traps correspond to the two devices in Figure 1. The choice of measurements is done by micro-wave pulses impinging the particles. The outcomes can take two possible values, corresponding to whether fluorescence light is detected at the detectors.*

In the experiment, data were recorded over a period of approximately one month to observe a violation of the simplest Bell inequality, namely the Clauser-Horne-Shimony-Holt (CHSH) inequality [12]. From the observed violation, and using the previous theoretical tools, the generation of 42 new random bits in the quantum setup was certified. Admittedly, the generation rate was very, very far from being competitive when compared to any of the existing random number generators. But, for the first time, new intrinsic quantum randomness was certified in an experiment without invoking any detailed model of the devices.

5. Open questions

The results reviewed in the last section have formalized the connection between Bell violation and intrinsic quantum randomness. We are however still far from fully understanding this connection. We conclude this work with a list of open questions related to the previous discussion.

- **Bell violation versus non-locality and entanglement.** As repeatedly mentioned, Bell inequality violation and randomness are related. One could even think that the more non-local some correlations – in the sense of producing larger violations of Bell inequalities – the more random they are. This intuitive picture however has been questioned by the recent results of [13]. There, it was shown that little amounts of non-locality may be enough to certify the presence of completely random bits. It is then an open question to understand the relation between these two quantum properties, namely non-locality and randomness, and when and why a Bell inequality violation leads to perfect random outputs. Also, the extension of all these results to more complex scenarios, consisting of more than two systems, has hardly been explored.
- **More efficient schemes.** The previous point referred to the fundamental understanding of the relation between quantum non-locality and intrinsic randomness. From

a more practical point of view, it would be interesting to understand how this link can be exploited to construct very efficient protocols for randomness generation. For instance, in the scheme of [10] the improvement in terms of randomness was quadratic, in the sense that the randomness produced by the setup was of the order of the square of the initial randomness needed for the Bell test (see also [14] for a careful security analysis of this protocol). The intuition says, however, that it should be possible to get an exponential improvement, in the sense that the randomness produced is exponentially larger than the initial seed. In fact, a recent work provides a protocol attaining an exponential improvement [15], although unfortunately the security proof only works in a noiseless situation.

- **Imperfect randomness at the inputs.** Another interesting theoretical question is related to how the lack of randomness in the choice of the settings in the Bell experiment affects the randomness of the generated outputs. Some results in this direction were presented in [16, 17, 18]. The problem of randomness amplification, introduced in [19], is intimately connected to this point. Up to now, we have focused our analysis in randomness expansion, in which an initial seed of perfect random bits is given and the goal is to produce a larger amount of random bits. In randomness amplification, a generator of imperfect random bits is given. The goal is to improve the quality of the random bits. While expansion is more focused on quantitative statements, amplification is concerned on the quality of the random outputs. Thus, the generation rate is not an important parameter in this scheme. It is a known result that randomness amplification is impossible classically [20]. In [19] a first scheme for randomness amplification was provided using, again, Bell inequalities. While this result is remarkable, unfortunately, it only works for initial random symbols of already quite good quality and without any noise. More recently, we have derived a scheme that allows one to amplify any arbitrary initial randomness to perfect random bits [21].
- **Loopholes and Bell tests.** The described scheme for randomness generation are based on the observation of a Bell inequality violation. Strictly speaking, a proper Bell inequality violation has never been observed. All the existing experiments in this sense suffer from technological problems that do not allow excluding a deterministic and no-signalling explanation for the observed data. In other words, exploiting the imperfections in the devices, one can construct ad-hoc EPR models reproducing the measurement results. These models are highly artificial (for instance a photon deciding to produce a click in a detector depending on which measurement is applied) and have to be changed from experiment to experiment. It is hard to believe that they provide a valid model for the observed experimental data. But, in view of all the previous fundamental implications, it would be highly desirable to have a Bell experiment free of any loophole, even those that are extremely artificial.

  In the case of randomness generation, it suffices to have a Bell test which is free from the so-called detection loophole. Standard Bell tests use photons. This is often problematic because detecting a photon is challenging and many of them are actually lost.

Losses in the Bell setup is precisely what the detection loophole exploits to provide a classical explanation for some apparently non-local correlations. In the experimental demonstration discussed above, the Bell violation was observed between atoms, which have a much higher detection efficiency, and, thus, allow a proper Bell violation for randomness generation. More recently, detection-loophole-free Bell violations have been observed in a completely optical setup [22], opening the way to schemes for certified randomness generation with much higher rates.

- **Implications.** Finally, it would be interesting to interpret all these findings from a rather speculative, and even philosophical point of view. One of the merits of the previous formalism is that it offers, for the first time, a quantification of the randomness generated in physical (quantum) setups. However, the whole analysis boils down to a fundamental, still rigorously proven connection. Let's assume that the loopholes observed in experiments are just a matter of technological imperfections and that Bell violations will survive once all loopholes are closed. That is, let's assume that non-local correlations do exist in Nature. Then, as discussed above, No-signalling + Free-will → Randomness. That is, in a scenario in which observers are assumed to have free will and where instantaneous communication is impossible, the observation of non-local correlations implies the randomness of the outcomes. What are the philosophical implications of this connection? Always at a rather speculative level, it is interesting to study wether randomness can be certified from other physical principles, without resorting to some initial seed of randomness, or without invoking free will. That is, can randomness be proven "from scratch"? Probably the answer to this question is negative. In any case, the quantitative results mentioned above shed light onto it. Indeed, one could naively argue that all the randomness seen in the measurement results is a consequence of the initial assumed randomness, or free will. However, the expansion results prove that this is impossible: new non-previously-existing randomness is generated by the quantum setup.

Bibliography

1 Laplace, P.S. (1840). *A Philosophical Essay on Probabilities* (Paris).

2 Einstein, A., B. Podolsky, and N. Rosen (1935). "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", *Phys. Rev.* 47: 777.

3 Bell, J.S. (1987). *Speakable and unspeakable in quantum mechanics* (Cambridge: Cambridge University Press).

4 Aspect, A., Dalibard, A. and G. Roger (1982). "Experimental test of Bell's inequalities using time-varying analyzers", *Phys. Rev. Lett.* 49: 1804.

5 Valentini, A. (2002). "Signal-locality in hidden-variables theories", *Phys. Lett. A* 297: 273.

6 Popescu, S. and D. Rohrlich (1994). “Nonlocality as an axiom”, *Found. Phys.* 24 (3): 379385.

7 Knuth, D. (1981). *The Art of Computer Programming* (Reading:Addison-Wesley).

8 Marsaglia, G. (2008). “The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness”, http://www.stat.fsu.edu/pub/diehard/

9 Rukhin, A. et al. (2008). “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, *National Institute of Standards and Technology*, Special Publication 800-22 Revision 1, http://csrc.nist.gov/publications/PubsSPs.html

10 Pironio, S., A. Acin, S. Massar A. Boyer de la Giroday, D.N. Matsukevitch, P. Maunz, S. Olmschenk, S. Hayes, L. Luo, T.A. Manning and C. Monroe (2010) “Random numbers certified by Bell’s theorem”, *Nature* 464: 1021-1024.

11 Colbeck, R. (2006). PhD Thesis, University of Cambridge.

12 Clauser, J.F., M.A. Horne, A. Shimony and R.A. Holt (1969). “Proposed experiment to test local hidden-variable theories”, *Phys. Rev. Lett.* 23: 880.

13 Acin, A., S. Massar and S. Pironio (2012). “Randomness vs Non Locality and Entanglement”, *Phys. Rev. Lett.* 108: 100402.

14 Pironio, S. and S. Massar (2013). “Security of practical private randomness generation”, *Phys. Rev. A* 87: 012336; Fehr, S., R. Gelles and C. Schaffner (2011). “Security and Composability of Randomness Expansion from Bell Inequalities, http://arxiv.org/abs/1111.6052.

15 Vazirani, U.V. and T. Vidick (2011). “Certifiable Quantum Dice - Or, testable exponential randomness expansion”, http://arxiv.org/abs/1111.6054.

16 Hall, M.J.W. (2010). “Local deterministic model of singlet state correlations based on relaxing measurement independence”, *Phys. Rev. Lett.* 105: 250404.

17 Barrett, J. and N. Gisin (2010). “How Much Measurement Independence Is Needed to Demonstrate Nonlocality?”, *Phys. Rev. Lett.* 106: 100406.

18 Koh, D.E., M.J.W. Hall, J. Setiawan, E. Pope, C. Marletto, A. Kay, V. Scarani and A. Ekert (2012). “The effects of reduced ”free will” on Bell-based randomness expansion”, *Phys. Rev. Lett.* 109: 160404.

19 Colbeck, R. and R. Renner (2012). “Free randomness can be amplified”, *Nature Phys.* 8: 450-454.

20 Santha, M. and U.V. Vazirani (1984). “Generating quasi-random sequences from slightly-random sources”, in *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science* (FOCS-84), 434.

21 Gallego, R., L. Masanes, G. de la Torre, C. Dhara, L. Aolita and A. Acin (2012). “Full randomness from arbitrarily deterministic events”, http://arxiv.org/abs/1210.6514.

22 Giustina, M., A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. Woo Nam, R. Ursin and A. Zeilinger (2013). “Bell violation using entangled photons without the fair-sampling assumption”, *Nature* 497: 227-230; Christensen, B.G., K.T. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P.

G. Kwiat. (2013). "Detection-Loophole-Free Test of Quantum Nonlocality, and Applications", http://arxiv.org/abs/1306.5772.