Full randomness from arbitrarily deterministic events

Rodrigo Gallego,[1] Lluis Masanes,[1] Gonzalo De La Torre,[1] Chirag Dhara,[1] Leandro Aolita,[1] and Antonio Acín[1,2]

[1]*ICFO-Institut de Ciencies Fotoniques, Av. Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona, Spain*
[2]*ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluís Companys 23, 08010 Barcelona, Spain*

Randomness amplification consists of generating perfect free random bits from a source of imperfect randomness. This task has implications at both fundamental and practical levels. Classically, randomness amplification is impossible; whereas with quantum resources it is only known to be possible if the randomness source is already almost perfect. In this work, we prove that full randomness amplification can be achieved in the quantum regime: Given any source of non, but arbitrarily close to, deterministic bits, we design a Bell-type experiment whose outcome is completely unpredictable. Besides the evident information-theoretic and cryptographic applications, our results rule out partially-predictive interpretations of nature. That is, either our world is fully deterministic or there exist events that are fully random.

Understanding whether nature is deterministically pre-determined or there are intrinsically random processes is a fundamental question that has attracted the interest of multiple thinkers, ranging from philosophers and mathematicians to physicists or neuroscientists. Nowadays this question is also important from a practical perspective, as random bits constitute a valuable resource for applications such as cryptographic protocols, gambling, or the numerical simulation of physical and biological systems.

Classical physics is a deterministic theory. Perfect knowledge of the positions and velocities of a system of classical particles at a given time, as well as of their interactions, allows one to predict their future (and also past) behavior with total certainty [1]. Thus, any randomness observed in classical systems is not intrinsic to the theory but just a manifestation of our imperfect description of the system.

The advent of quantum physics put into question this deterministic viewpoint, as there exist experimental situations for which quantum theory gives predictions only in probabilistic terms, even if one has a perfect description of the preparation and interactions of the system. A possible solution to this classically counterintuitive fact was proposed in the early days of quantum physics: Quantum mechanics had to be incomplete [2], and there should be a complete theory capable of providing deterministic predictions for all conceivable experiments. There would thus be no room for intrinsic randomness, and any apparent randomness would again be a consequence of our lack of control over hypothetical "hidden variables" not contemplated by the quantum formalism.

Bell's no-go theorem [3], however, implies that hidden-variable theories are inconsistent with quantum mechanics. Therefore, none of these could ever render a deterministic completion to the quantum formalism. More precisely, all hidden-variable theories compatible with a local causal structure predict that any correlations among space-like separated events satisfy a series of inequalities, known as Bell inequalities. Bell inequalities, in turn, are violated by some correlations among quantum particles. This form of correlations defines the phenomenon of quantum non-locality.

Now, it turns out that quantum non-locality does not necessarily imply the existence of fully unpredictable processes in nature. The reasons behind this are subtle. First of all, unpredictable processes could be certified only if the no-signalling principle holds. This states that no instantaneous communication is possible, which imposes in turn a local causal structure on events, as in Einstein's special relativity. In fact, Bohm's theory is both deterministic and able to reproduce all quantum predictions [4], but it is incompatible with no-signalling. Thus, we assume throughout the validity of the no-signalling principle. Yet, even within the no-signalling framework, it is still not possible to infer the existence of fully random processes only from the mere observation of non-local correlations. This is due to the fact that Bell tests require measurement settings chosen at random, but the actual randomness in such choices can never be certified. The extremal example is given when the settings are determined in advance. Then, any Bell violation can easily be explained in terms of deterministic models. As a matter of fact, super-deterministic models, which postulate that all phenomena in the universe, including our own mental processes, are fully pre-programmed, are by definition impossible to rule out.

These considerations imply that the strongest result on the existence of randomness one can hope for using quantum non-locality is stated by the following possibility: Given a source that produces an arbitrarily small but non-zero amount of randomness, can one still certify the existence of completely random processes? The main result of this work is to provide an affirmative answer to this question. Our results, then, imply that the existence of correlations as those predicted by quantum physics forces us into a dichotomic choice: Either we postulate super-deterministic models in which all events in nature are fully pre-determined, or we accept the existence of fully unpredictable events.

Besides the philosophical and physics-foundational implications, our results provide a protocol for perfect randomness amplification using quantum non-locality. Randomness amplification is an information-theoretic task whose goal 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 $x_j = 0$ or 1 for all j. Each bit j contains some randomness, in the sense that the probability $P(x_j|e)$ that it takes a given value x_j, conditioned on any pre-existing variable e, is such that

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

for all j and e, where $0 < \epsilon \leq 1/2$. The variable e can correspond to any event that could be a possible cause of bit x_j. Therefore, e represents events contained in the space-time region lying outside the future light-cone of x_j. Free random bits correspond to $\epsilon = \frac{1}{2}$; while deterministic ones, i.e. those predictable with certainty by an observer with access to e, to $\epsilon = 0$. More precisely, when $\epsilon = 0$ the bound (1) is trivial and no randomness can be certified. We refer to $\mathcal{S}$ as an ϵ-source, and to any bit satisfying (1) as an ϵ-free bit. 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. Note that efficiency issues, such as the rate of uses of $\mathcal{S}$ required per final bit generated by $\mathcal{S}_f$ do not play any role in randomness amplification. The relevant figure of merit is just the quality, measured by ϵ_f, of the final bits. Thus, without loss of generality, we restrict our analysis to the problem of generating a single final free random bit k.

Santha and Vazirani proved that randomness amplification is impossible using classical resources [5]. This is in a sense intuitive, in view of the absence of any intrinsic randomness in classical physics. In the quantum regime, randomness amplification has been recently studied by Colbeck and Renner [6]. There, $\mathcal{S}$ is used to choose the measurement settings by two distant observers, Alice and Bob, in a Bell test [7] involving two entangled quantum particles. The measurement outcome obtained by one of the observers, say Alice, in one of the experimental runs (also chosen with $\mathcal{S}$) defines the output random bit. Colbeck and Renner proved how input bits with very high randomness, of $0.442 < \epsilon \leq 0.5$, can be mapped into arbitrarily free random bits of $\epsilon_f \to 1/2$, and conjectured that randomness amplification should be possible for any initial randomness [6]. Our results also solve this conjecture, as we show that quantum non-locality can be exploited to attain *full randomness amplification*, i.e. that ϵ_f can be made arbitrarily close to $1/2$ for any $0 < \epsilon \leq 1/2$.

Before presenting the ingredients of our proof, it is worth commenting on previous works on randomness in connection with quantum non-locality. In [8] it was shown how to bound the intrinsic randomness generated in a Bell test. These bounds can be used for device-independent randomness expansion, following a proposal by Colbeck [9], and to achieve a quadratic expansion of the amount of random bits [8] (see [10–13] for further works on device-independent randomness expansion). Note however that, in randomness expansion, one assumes instead, from the very beginning, the existence of an input seed of free random bits, and the main goal is to expand this into a larger sequence. The figure of merit there is the ratio between the length of the final and initial strings of free random bits. Finally, other recent works have analyzed how a lack of randomness in the measurement choices affects a Bell test [14–16] and the randomness generated in it [17].

Let us now sketch the realization of our final source $\mathcal{S}_f$. We use the input ϵ-source $\mathcal{S}$ to choose the measurement settings in a multipartite Bell test involving a number of observers that depends both on the input ϵ and the target ϵ_f. After verifying that the expected Bell violation is obtained, the measurement outcomes are combined to define the final bit k. For pedagogical reasons, we adopt a cryptographic perspective and assume the worst-case scenario where all the devices we use may have been prepared by an adversary Eve equipped with arbitrary non-signalling resources, possibly even supra-quantum ones. In the preparation, Eve may have also had access to $\mathcal{S}$ and correlated the bits it produces with some physical system at her disposal. Without loss of generality, we can assume that Eve can reveal the value of e at any stage of the protocol by measuring this system. Full randomness amplification is then equivalent to proving that Eve's correlations with k can be made arbitrarily small.

Bell tests for which quantum correlations achieve the maximal non-signalling violation, also known as Greenberger-Horne-Zeilinger (GHZ) paradoxes [18], are necessary for randomness amplification. This is due to the fact that unless the maximal non-signalling violation is attained, for sufficiently small ϵ, Eve may fake the observed correlations with classical deterministic resources. This attack ceases to be possible when the maximal non-signalling violation is observed, as Eve is forced to prepare only those non-local correlations attaining the maximal violation. GHZ paradoxes are however not sufficient. Consider for instance the GHZ paradox given by the tripartite Mermin Bell inequality [19]. One can see that Eve can predict with certainty any function of the measurement outcomes and still deliver the maximal violation, for all $0 \leq \epsilon \leq 1/2$ (see Supplementary Material).

For more parties though, the latter happens not to hold any longer. In fact, consider any correlations attaining the maximal violation of the five-party Mermin inequality. Take the bit corresponding to the majority-vote function of the outcomes of any subset of three out of the five observers, say the first three. This function is equal to zero if at least two of the three bits are equal to zero, and equal to one otherwise. We show in the Supplementary Material that Eve's predictability on this bit is at most 3/4. This is our first result:

Result 1. Given an ϵ-source with any $0 < \epsilon \leq 1/2$, and quantum five-party non-local resources, an intermediate ϵ_i-source of $\epsilon_i = 1/4$ can be obtained.

Box 1: Protocol for Randomness Amplification

1. Every observer measures his device in one of two settings chosen at random by the input ϵ-source $\mathcal{S}$.
2. Every quintuplet whose settings combination does not appear in the five-party Mermin Bell test is discarded. If the quintuplets left are fewer than $N/3$, abort.
3. Group the quintuples left into N_b blocks of equal size N_d. Choose a *distillation block* at random with $\mathcal{S}$.
4. If the outcomes of any quintuplet not in the distillation block are inconsistent with the maximal violation of the five-party Mermin Bell test, abort.
5. Distill the final bit from the distillation block. This is done in the following way. The majority vote $\mathrm{maj}(\mathbf{a})$ among for instance the outcomes a_1, a_2 and a_3 of the first three users is computed for each quintuplet. Then, a function f maps the resulting N_d bits into the final bit k.

The partial unpredictability in the five-party Mermin Bell test is the building block of our protocol. To complete it, we must equip it with two essential components: (*i*) an *estimation procedure* that verifies that the untrusted devices do yield the required Bell violation; and (*ii*) a *distillation procedure* that, from sufficiently many ϵ_i-bits generated in the 5-party Bell experiment, distills a single final ϵ_f-source of $\epsilon_f \to 1/2$. To these ends, we consider a more complex Bell test involving N groups of five observers (quintuplets) each. The steps in the protocol are described in Box 1.

In the supplementary material of the submission we prove using techniques from [20] that, if the protocol is not aborted, the final bit produced by the protocol is indistinguishable from an ideal random bit uncorrelated to the eavesdropper. Thus, the output free random bits satisfy universally-composable security [21], the highest standard of cryptographic security, and could be used as seed for randomness expansion or any other protocol.

To end up with, we must show that quantum resources can indeed successfully implement our protocol. It is immediate to see that the qubit measurements X or Y on the quantum state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle)$, with $|0\rangle$ and $|1\rangle$ the eigenstates of the Z qubit basis, yield correlations that maximally violate the five-partite Mermin inequality in question. This completes our main result.

Result 2 (Main Result). Given an ϵ-source with any $0 < \epsilon \leq 1/2$, a perfect free random bit k can be obtained using quantum non-local correlations.

In summary, we have presented a protocol that, using quantum non-local resources, attains *full randomness amplification*. This task is impossible classically and was not known to be possible in the quantum regime. As our goal was to prove full randomness amplification, our analysis focuses on the noise-free case. In fact, the noisy case only makes sense if one does not aim at perfect random bits and bounds the amount of randomness in the final bit. Then, it should be possible to adapt our protocol in order to get a bound on the noise it tolerates. Other open questions that naturally follow from our results consist of studying randomness amplification against quantum eavesdroppers, or the search of protocols in the bipartite scenario.

From a more fundamental perspective, our results imply that there exist experiments whose outcomes are fully unpredictable. The only two assumptions for this conclusion are the existence of events with an arbitrarily small but non-zero amount of randomness and the validity of the no-signalling principle. Dropping the former implies accepting a superdeterminisitc view where no randomness exist, so that we experience a fully pre-determined reality. This possibility is uninteresting from a scientific perspective, and even uncomfortable from a philosophical one. Dropping the latter, in turn, implies abandoning a local causal structure for events in space-time. However, this is one of the most fundamental notions of special relativity, and without which even the very meaning of randomness or predictability would be unclear, as these concepts implicitly rely on the cause-effect principle.

Acknowledgements We acknowledge support from the ERC Starting Grant PERCENT, the EU Projects Q-Essence and QCS, the Spanish MICIIN through a Juan de la Cierva grant and projects FIS2010-14830, Explora-Intrinqra and CHIST-ERA DIQIP, an FI Grant of the Generalitat de Catalunya, CatalunyaCaixa, and Fundació Privada Cellex, Barcelona.

[1] P. S. Laplace, *A Philosophical Essay on Probabilities*, Paris (1840).
[2] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev., **47**, 777-780 (1935).
[3] J. S. Bell, Physics **1**, 195 (1964); *Speakable and unspeakable in quantum mechanics*, Cambridge University Press (Cambridge, 1987).
[4] D. Bohm, Phys. Rev. **85**, 166-179 (1952); Phys. Rev. **85**, 180-193 (1952).

[5] M. Santha and U. V. Vazirani, *in Proc. 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)*, 434 (IEEE Computer Society, 1984).

[6] R. Colbeck and R. Renner, *Free randomness can be amplied*, Nature Phys. **8**, 450 (2012).

[7] S. L. Braunstein and C. M. Caves, *Wringing out better Bell inequalities*, Ann. Phys. **202**, 22 (1990).

[8] S. Pironio *et al.*, *Random numbers certified by Bell's theorem*, Nature **464**, 1021 (2010).

[9] R. Colbeck, *Quantum and Relativistic Protocols for Secure Multi-Party Computation*, PhD dissertation, Univ. Cambridge (2007).

[10] A. Acín, S. Massar and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).

[11] S. Pironio and S. Massar, arXiv:1111.6056.

[12] S. Fehr, R. Gelles and C. Schaffner, arXiv:1111.6052.

[13] U. V. Vazirani and T. Vidick, Proceedings of the ACM Symposium on the Theory of Computing (2012).

[14] J. Kofler, T. Paterek, and C. Brukner, *Experimenter's freedom in Bell's theorem and quantum cryptography*, Phys. Rev. A **73**, 022104 (2006).

[15] J. Barrett and N. Gisin, *How much measurement independence is needed to demonstrate nonlocality?* Phys. Rev. Lett. **106**, 100406 (2011).

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

[17] D. E. Koh, M. J. W. Hall, Setiawan, J. E. Pope, C. Marletto, A. Kay, V. Scarani, and A. Ekert, *The effects of reduced 'free will" on Bell-based randomness expansion*, arxiv:1202.3571.

[18] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer, Dordrecht), p. 69 (1989).

[19] N. D. Mermin, *Simple unified form for the major no-hidden-variables theorems*, Phys. Rev. Lett. **65**, 3373 (1990).

[20] L. Masanes, *Universally-composable privacy amplification from causality constraints*, Phys. Rev. Lett. **102**, 140501 (2009).

[21] R. Canetti; Proc. 42nd IEEE Symposium on Foundations of Computer Science (FOCS), 136 (2001).