LETTERS
PUBLISHED ONLINE: 6 MAY 2012 | DOI: 10.1038/NPHYS2300
nature physics

# Free randomness can be amplified

Roger Colbeck[1,2]* and Renato Renner[1]

**Are there fundamentally random processes in nature? Theoretical predictions, confirmed experimentally, such as the violation of Bell inequalities[1], point to an affirmative answer. However, these results are based on the assumption that measurement settings can be chosen freely at random[2], so assume the existence of perfectly free random processes from the outset. Here we consider a scenario in which this assumption is weakened and show that partially free random bits can be amplified to make arbitrarily free ones. More precisely, given a source of random bits whose correlation with other variables is below a certain threshold, we propose a procedure for generating fresh random bits that are virtually uncorrelated with all other variables. We also conjecture that such procedures exist for any non-trivial threshold. Our result is based solely on the no-signalling principle, which is necessary for the existence of free randomness.**

Physical theories enable us to make predictions. We can ask 'what would happen if …' and reason about the answer, even in scenarios that would be virtually impossible to set up in reality[2]. Each scenario corresponds to a choice of parameters, and it is usually implicitly assumed that any of the possible choices can be made—the theory prescribes the subsequent behaviour in every case. One of the main aims of this Letter is to identify (minimal) conditions under which such choices can be made freely, that is, such that they are uncorrelated with any pre-existing values (in a precise sense described later).

Free choices are important both at the level of fundamental physics, and for technological applications. In almost any cryptographic protocol, for example, some kind of randomness is needed, and if this is not generated freely, the protocol can be rendered insecure. As a simple example, consider a random number generator used by a casino. Evidently, a gambler with access to data correlated with these numbers can exploit this to their advantage.

Another reason why free choices are important is to establish symmetries on which physical theories can be based. For example, the concept of an electron is based on the implicit assumption that we could pick any of the electrons in the universe and find the same properties (such as its mass). More precisely, given a set of particles that are experimentally indistinguishable, the assumption that we can sample freely from this set establishes a symmetry between them. Following arguments by de Finetti[3,4], this symmetry implies that we can treat these particles as independent particles of the same type.

A scenario in which making free random choices is particularly relevant is in the context of Bell's theorem. Here, the statistics produced by freely chosen measurements on an entangled state are used to conclude that quantum correlations cannot be reproduced by a local hidden variable theory[1,2]. Dropping the assumption that the measurement settings are freely chosen opens a loophole, rendering the conclusion invalid. In particular, if we instead imagine that the settings were determined by events in the past (this is sometimes called 'superdeterminism') then it is easy to explain Bell inequality violations with a local classical model. However, we can ask whether the free choice assumption can be relaxed, allowing for correlations between the measurement settings and other, possibly hidden, variables, but without enabling their complete pre-determination. This has been studied in recent work[5–9], which shows that if the choice of measurement settings is not sufficiently free then particular quantum correlations can be explained with a local classical model.

This raises the question of whether established concepts in physics are rendered invalid if we relax the (standard) assumption that the experimenters' choices are perfectly free. We might imagine, for example, an experimenter who tries to generate free uniform bits, but (unbeknown to them) these bits can be correctly guessed with a probability of success greater than 1/2 using other (pre-existing) parameters. In this Letter, we show that partially free random bits can be used to produce arbitrarily free ones. This implies that a relaxed free choice assumption is sufficient to establish all results derived under the assumption of perfect free choices.

To arrive at this conclusion we need to make one assumption about the structure of any underlying physical theory, namely that it is no-signalling, which essentially implies that local parameters are sufficient to make any possible predictions within the theory. As we explain in Supplementary Information, it turns out that this assumption is necessary so that perfectly free choices can be consistently incorporated within the theory.

To describe our result in detail, we need a precise notion of what partially free randomness is. The main idea is that, given a particular causal structure, a variable is free if it is uncorrelated with all other values except those that lie in its causal future. Our main results are valid independently of the exact causal structure, but it is natural to consider the causal structure arising from relativistic spacetime, which has the property that $Y$ cannot be caused by $X$ if $Y$ lies outside the future light cone of $X$.

Given a causal structure, we say that $X$ is perfectly free if it is uniformly distributed conditioned on any variables that cannot be caused by $X$. This definition, together with the relativistic understanding of cause above, captures the idea that $X$ is free if there is no reference frame in which it is correlated with variables in its past, which corresponds to the notion used by Bell[2]. Note that the definition includes that $X$ is uniformly distributed, as well as that it is independent of other values. Whereas, in other contexts, it may be useful to separate these properties, in the present work such a distinction is not needed.

We also need a notion of partial freedom. We say that $X$ is $\varepsilon$-free if it is $\varepsilon$-close in variational distance to being perfectly free (see Methods). This measure of closeness is chosen because of its operational significance: if two distributions have variational distance at most $\varepsilon$, then the probability that we ever notice a difference between them is at most $\varepsilon$. As an example, if a

[1]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland, [2]Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada. *e-mail: colbeck@phys.ethz.ch.

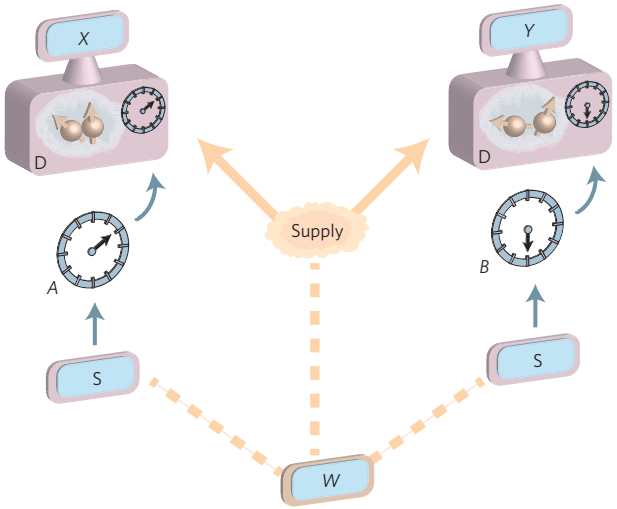


**Figure 1 | Illustration of the bipartite set-up.** Spacelike-separated measurements are carried out using devices denoted D. The choices of measurement, *A* and *B*, are derived from bits generated by two sources of weak randomness, denoted S. These bits are only partially free; that is, they may be correlated (represented by the dashed line) with each other and with some other variables *W* (to be interpreted as parameters provided by a possible higher theory), which may also influence the supply of states being measured. By exploiting correlations between the outcomes, *X* and *Y*, we show that, in spite of the lack of perfectly free randomness to choose settings, the outcome *X* is arbitrarily close to being uniform and uncorrelated with *W*.

uniformly random bit $X$ is correlated to a pre-existing bit $W$ such that $P_{X|W=0}(0) = 3/4$ and $P_{X|W=1}(1) = 3/4$ then we say that $X$ is $\varepsilon$-free for $\varepsilon = 1/4$.

The idea of the present work is to exploit a particular set of non-local correlations found in quantum theory that can be quantified using the chained Bell inequalities[10,11]. If we have perfect free randomness to choose measurements, then the violation of a Bell inequality indicates that the measurement outcomes cannot be completely pre-determined[1]. Bell's arguments have recently been extended to show that, again under the assumption that we have perfect free randomness, there is no way to improve on the predictions that quantum theory makes about measurement outcomes[12]. Here, we show that quantum correlations can be so strong that, even if we cannot choose the measurements perfectly freely, the outputs are nevertheless perfectly free.

To generate these correlations, we consider an experimental set-up where local measurements are made on a pair of maximally entangled qubits (Fig. 1). We first make the (temporary) assumption that the joint distribution of measurement outcomes conditioned on the choices, $P_{XY|AB}$, is the one predicted by quantum theory for this set-up. Crucially, however, we do not require completeness of quantum theory; that is, that quantum theory is maximally informative about the measurement outcomes. Instead, we consider arbitrary further parameters, $W$, that may be provided by a higher theory. Within this set-up, our assumptions can be stated as follows.

NS: $P_{XY|AB\,W=w}$ is no-signalling for all $w$ (that is, $P_{X|AB\,W=w} = P_{X|A\,W=w}$ and $P_{Y|AB\,W=w} = P_{Y|B\,W=w}$).

QT: $P_{XY|AB}$ is that predicted by quantum theory.

Our first main result is that, under the above assumptions, there exists a protocol that uses sources of $\varepsilon$-free bits to generate arbitrarily free bits for any $\varepsilon < (\sqrt{2}-1)^2/2 \approx 0.086$ (see Theorem 1 in the Methods).

It is natural to ask whether the assumption that quantum theory correctly predicts the correlations (assumption QT) is necessary, or whether, instead, the presence of sufficiently strong correlations can be certified using $\varepsilon$-free bits. By certification, we mean a procedure to test the correlations such that it is essentially impossible that the test passes without the generated bits being arbitrarily free. This is also relevant in a cryptographic context, where the states and measurements are not trusted, and could have been chosen by an adversary with partial knowledge, $W$, of the measurement settings.

Our second main result is that, under assumption NS alone, there exists a protocol that uses $\varepsilon$-free bits to certify the generation of arbitrarily free bits for any $\varepsilon < 0.058$ (see Theorem 2 in Methods). In other words, there exists a device-independent protocol for free-randomness amplification. Clearly this second scenario, where the assumption that the correlations are those predicted by quantum theory is dropped, is more demanding, hence the smaller range of $\varepsilon$ for which free-randomness amplification is successful. Nevertheless, the fact that it is possible at all is already fascinating.

It is an open question as to how far the threshold on $\varepsilon$ can be pushed such that free-randomness amplification remains possible (in either scenario). It turns out that using chained Bell correlations there is a limit, because (as shown in Supplementary Information) for $\varepsilon \geq (1-1/\sqrt{2})/2 \approx 0.146$ these correlations admit a local classical explanation. However, we conjecture that there exist protocols based on other correlations such that, for any $\varepsilon < 1/2$, $\varepsilon$-free bits can be used to generate arbitrarily free bits. We give some evidence for this in Supplementary Information.

Before discussing the implications of these results, we first remark that the use of no-signalling conditions for information processing tasks was first observed in ref. 13 in the context of key distribution. We also note that what we call free randomness has sometimes been called 'free will' in the literature (for example refs 14,15). In this language, we could restate our main result as a proof that free will can be amplified.

A sequence of bits $S_1, S_2, \ldots$ for which each $S_i$ is $\varepsilon$-free is known in classical computer science as a Santha–Vazirani source[16]. It has been shown that no classical algorithm can extract even a single uniform bit from such a source (without an extra seed; we elaborate on this point in Supplementary Information). In contrast, our main result implies that such a bit can be generated using a quantum algorithm.

It is worth comparing randomness amplification, as considered here, with randomness expansion, introduced in ref. 17 and further developed in refs 18,19. There, an initial perfectly random finite seed is used within a protocol to generate a longer sequence of random bits using untrusted devices. By contrast, we do not require such a seed in the present work, but instead have an arbitrarily large supply of imperfect randomness.

A potential application of our protocol is as a method for generating a seed, to be used with an extractor to extract further randomness from a partially free source, or to seed a randomness expansion protocol. Using Trevisan's extractor[20,21], for example, in the first case we could generate random bits at the entropy rate of the partially free source. In the second case, provided that the protocols can be securely composed, a secure randomness expansion protocol may enable a large amount of free randomness to be derived from a finite number of uses of partially free sources.

We also comment on the implications of our result for experimental demonstrations of Bell-inequality violations. There are several potential loopholes in current experiments, leaving the door open for die-hards to reject certain philosophical implications. One such loophole that has received only minor attention in the literature is the so called free-choice loophole, which has been addressed in a recent experiment[22]. This loophole says that the supposedly free measurement settings were in fact correlated with the entanglement source (perhaps through some hidden system). In the aforementioned experiment, this is addressed by using random number generators, triggered at spacelike separation

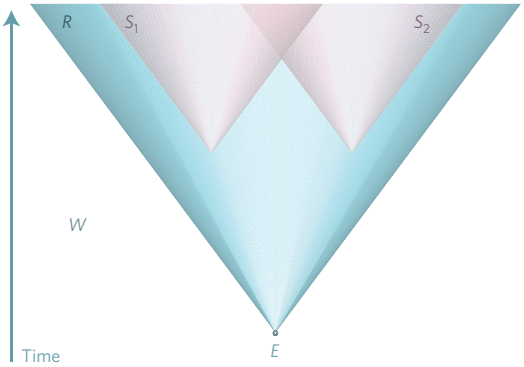


**Figure 2 | Typical causal structure of a protocol.** A randomness amplification protocol for generating a random bit $R$ may be initiated at a particular location and time represented by a spacetime point $E$. Depending on the protocol, information correlated to $R$ may be generated at various locations within the causal future of $E$, depicted by the blue region. Any point in this region may therefore potentially be in the causal future of $R$. The bit $R$ satisfies our definition of being free if it is uncorrelated with anything outside this region, indicated by the variable $W$. The protocol may invoke sources of random bits $S_1$ and $S_2$ at many locations. Technically, the only requirement on the causal structure is that the causal futures of each of these source bits (pink regions) lie in the blue region.

from the source of entangled pairs. However, as acknowledged in ref. 22, this leaves room for 'superdeterminism', because it is impossible to exclude the possibility that the random number generator and the source of entanglement are correlated through an extra hidden system.

Use of our result is also not able to close this loophole, and, as we can never rule out that the universe is deterministic, we do not see any way to completely close it. Nevertheless, our result complements existing work on the weakening of free choice in Bell experiments[5–9]: instead of having to assume that the entanglement source and the random number generator are completely uncorrelated, we would only need to assume that they are not strongly correlated. Furthermore, if our conjecture is true (that is, $\varepsilon$-free bits can be amplified for any $\varepsilon < 1/2$), then for certain Bell tests it would be sufficient to assume only that the source and the random number generator are not completely correlated.

In other scenarios in which the assumption of free choice is critical, generating such choices through our free-randomness amplification procedure would also enable stronger conclusions to be drawn. For example, within classical cryptography a wide range of cryptographic tasks that use perfect randomness are rendered impossible if the parties carrying them out have access only to imperfect randomness sources[23]. Our result shows that in a quantum setting this is not the case; any task that can be carried out securely using perfect randomness can also be carried out securely with access only to (sufficiently free) imperfect randomness.

## Methods

In this section we give more technical versions of our definitions and main results.

We consider a set $\Gamma$ that includes all random variables of interest in our set-up (Fig. 1) and equip $\Gamma$ with a causal structure (mathematically, this is a preorder relation between its elements). As explained in the main text, it is convenient (but not necessary) to think of the causal structure induced by relativistic spacetime.

**Definition.** Let $X \in \Gamma$ and let $\Gamma_X$ be the subset of random variables from $\Gamma$ that cannot be caused by $X$ (in particular, $\Gamma_X$ does not include $X$). Then $X$ is called $\varepsilon$-free if

$$D(P_{X|\Gamma_X=\gamma_X}, P_{\bar{X}}) \leq \varepsilon$$

for all $\gamma_X$, where $P_{\bar{X}}$ denotes the uniform distribution on $X$. $D(\cdot)$ denotes the variational distance, defined by $D(P_X, Q_X) := (1/2)\sum_x |P_X(x) - Q_X(x)|$. (Here and in the following we use lower case to denote particular instances of upper-case random variables.)

For our main claims, we use random variables $S_i \in \Gamma$ for $i = 1, 2, \ldots$ (these denote the random bits generated by an $\varepsilon$-free source) and $R \in \Gamma$ (the random bit generated by the protocol), where the causal structure can be arbitrary up to the following constraint: the causal future of $R$ includes the causal future of any $S_i$ (Fig. 2).

**Theorem 1.** There exists a protocol that takes as input $S_i$ and outputs $R$ such that the following statement holds under the assumptions NS and QT: if $S_i$ are $\varepsilon$-free, for any $\varepsilon < (\sqrt{2}-1)^2/2 \approx 0.086$, then $R$ is arbitrarily free, except with arbitrarily small probability.

The proof relies on the bipartite set-up of Fig. 1. It is parameterized by an integer, $N$, corresponding to the number of measurement settings on each side. $A \in \{0, 2, \ldots, 2N-2\}$ and $B \in \{1, 3, \ldots, 2N-1\}$ correspond to the choices of measurements and $X \in \{+1, -1\}$ and $Y \in \{+1, -1\}$ are their respective outcomes. We introduce a measure of the strength of the resulting correlations by defining

$$I_N := P(X = Y|a_0, b_0) + \sum_{\substack{a,b \\ |a-b|=1}} P(X \neq Y|a, b)$$

where $a_0 = 0$, $b_0 = 2N-1$ and $P(X \neq Y|a, b)$ is the probability that the measurements give different outcomes for settings $A = a$, $B = b$. This quantity was originally introduced to study chained Bell correlations[10,11], and has found use in cryptography[13,24] and quantum foundations[12,25]. It turns out that all classical correlations (that is, those that can be reproduced from classical shared randomness) satisfy $I_N \geq 1$, whereas quantum correlations exist for which

$$I_N = 2N \sin^2 \frac{\pi}{4N} \tag{1}$$

which tends to zero in the limit of large $N$ (the state and measurements required to achieve this are given in Supplementary Information).

In the proof of Theorem 1, we use the following lemma about no-signalling distributions. This lemma bounds the independence of the output bits from the choices $A$ and $B$ as well as any values $W$. The bound is given in terms of the strength of quantum correlations, quantified using $I_N$, and how free the measurement settings are, quantified through

$$q_N(a, b) := \min_{\substack{a', b', w' \\ |a'-b'|=1}} \left[ \frac{P_{W|a'b'}(w')}{P_{W|ab}(w')} \right]$$

**Lemma 1.** If $P_{XY|ABw}$ is no-signalling for all $w$, and $q_N(a, b) > 0$, then

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{I_N}{2q_N(a, b)} \tag{2}$$

for all $a$ and $b$, where $P_{\bar{X}}$ denotes the uniform distribution on $X$.

The proof of this lemma is given in Supplementary Information.

**Proof of Theorem 1.** The protocol relies on the correlations introduced above, where the source bits $S_i$ are used to choose $A$ and $B$, and where $X$ is taken as the final output $R$. It remains to show that $R$ is arbitrarily free in the limit of large $N$. Let $W$ be any subset of $\Gamma$ that is not in the causal future of $R$, and therefore, by assumption, not in the causal future of the source bits $S_i$. Note that

$$q_N(a, b) = \min_{\substack{a', b', w' \\ |a'-b'|=1}} \left[ \frac{P_{AB|w'}(a', b')}{P_{AB|w'}(a, b)} \right]$$

in the case of uniform $P_{AB}$, which we can assume without loss of generality. For $N = 2^r$, the measurement settings, $A$ and $B$, can be picked using $r$ $\varepsilon$-free source bits, and hence $q_{2^r}(a, b) \geq ((1-2\varepsilon)/(1+2\varepsilon))^{2^r}$. Inserting this into equation (2) gives

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{I_{2^r}}{2} \left( \frac{1+2\varepsilon}{1-2\varepsilon} \right)^{2^r}$$

Substituting the value of $I_{2^r}$ obtainable in quantum theory (see equation (1)) gives

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq 2^r \left( \frac{1+2\varepsilon}{1-2\varepsilon} \right)^{2^r} \sin^2 \left( \frac{\pi}{2^{r+2}} \right)$$

Hence, using the bound $\sin x \leq x$ for $x \geq 0$, it follows that

$$D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab}) \leq \frac{\pi^2}{16} \left( \frac{1+2\varepsilon}{\sqrt{2}(1-2\varepsilon)} \right)^{2^r} =: \delta_{r,\varepsilon}$$

which tends to zero as $r$ tends to infinity provided $\varepsilon < (\sqrt{2}-1)^2/2$.

Note that $D(P_{XW|ab}, P_{\bar{X}} \times P_{W|ab})$ is equal to $\sum_w P_{W|ab}(w) D(P_{X|abw}, P_{\bar{X}})$, that is, the expectation over $W$ of the amount by which the output bits are free. Using

Markov's inequality, we have that $D(P_{X|abw}, P_{\bar{X}}) < \alpha$, except with probability at most $\delta_{r,\varepsilon}/\alpha$, for any $\alpha > 0$. Thus, taking $\alpha = \sqrt{\delta_{r,\varepsilon}}$, if the initial sources are $\varepsilon$-free for $\varepsilon < (\sqrt{2}-1)^2/2$, then, in the limit of large $r$, their outputs are $\sqrt{\delta_{r,\varepsilon}}$-free, except with probability $\sqrt{\delta_{r,\varepsilon}}$. The claim then follows because $\delta_{r,\varepsilon}$ can be made arbitrarily small by choosing a sufficiently large $r$.

In the second part of our main result, we show that assumption QT can be omitted.

**Theorem 2.** There exists a protocol that takes as input $S_i$ and outputs $R$ such that the following statement holds under assumption NS: if $S_i$ are $\varepsilon$-free, for any $\varepsilon < 0.058$, then $R$ is certified to be arbitrarily free, except with arbitrarily small probability.

We give a specific protocol that achieves this task and analyse it in Supplementary Information.

For completeness, we state our conjecture.

**Conjecture 1.** The restriction on $\varepsilon$ in Theorems 1 and 2 can be replaced by $\varepsilon < 1/2$.

It is likely that the alternative protocols required to prove the conjecture need to go beyond the bipartite set-up to succeed, as discussed in Supplementary Information.

Received 7 November 2011; accepted 23 March 2012; published online 6 May 2012

## References


1. Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics* Ch. 2 (Cambridge Univ. Press, 1987).
2. Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics* Ch. 12 (Cambridge Univ. Press, 1987).
3. De Finetti, B. La prévision: Ses lois logiques, ses sources subjectives. *Ann. de l'Inst. Henri Poincaré* **7,** 1–68 (1937).
4. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nature Phys.* **3,** 645–649 (2007).
5. Kofler, J., Paterek, T. & Brukner, C. Experimenter's freedom in Bell's theorem and quantum cryptography. *Phys. Rev. A* **73,** 022104 (2006).
6. Hall, M. J. W. Local deterministic model of singlet state correlations based on relaxing measurement independence. *Phys. Rev. Lett.* **105,** 250404 (2010).
7. Barrett, J. & Gisin, N. How much measurement independence is needed to demonstrate nonlocality? *Phys. Rev. Lett.* **106,** 100406 (2011).
8. Hall, M. J. W. Relaxed Bell inequalities and Kochen-Specker theorems. *Phys. Rev. A* **84,** 022102 (2011).
9. Lorenzo, A. D. Free will and quantum mechanics. Preprint at http://arxiv.org/abs/1105.1134 (2011).
10. Pearle, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2,** 1418–1425 (1970).
11. Braunstein, S. L. & Caves, C. M. Wringing out better Bell inequalities. *Ann. Phys.* **202,** 22–56 (1990).
12. Colbeck, R. & Renner, R. No extension of quantum theory can have improved predictive power. *Nature Commun.* **2,** 411 (2011).
13. Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
14. Conway, J. & Kochen, S. The free will theorem. *Found. Phys.* **36,** 1441–1473 (2006).
15. Conway, J. H. & Kochen, S. The strong free will theorem. *Notices AMS* **56,** 226–232 (2009).
16. Santha, M. & Vazirani, U. V. in *Proc. 25th IEEE Symposium on Foundations of Computer Science (FOCS-84)* 434–440 (IEEE Computer Society, 1984).
17. Colbeck, R. *Quantum and Relativistic Protocols For Secure Multi-Party Computation* PhD thesis, Univ. Cambridge (2007); available at http://arxiv.org/abs/0911.3814.
18. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).
19. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A* **44,** 095305 (2011).
20. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. Preprint at http://arxiv.org/abs/0912.5514 (2009).
21. Trevisan, L. Extractors and pseudorandom generators. *J. ACM* **48,** 860–879 (2001).
22. Scheidl, T. *et al.* Violation of local realism with freedom of choice. *Proc. Natl Acad. Sci. USA* **107,** 19708 (2010).
23. Dodis, Y., Ong, S. J., Prabhakaran, M. & Sahai, A. in *Proc. 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS-04)* 196–205 (Lecture Notes in Computer Science, IEEE Computer Society, 2004).
24. Barrett, J., Kent, A. & Pironio, S. Maximally non-local and monogamous quantum correlations. *Phys. Rev. Lett.* **97,** 170409 (2006).
25. Colbeck, R. & Renner, R. Hidden variable models for quantum theory cannot have any local part. *Phys. Rev. Lett.* **101,** 050403 (2008).


## Acknowledgements

We thank V. Galliard for useful discussions and L. del Rio for the figures. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. R.R. acknowledges support from the Swiss National Science Foundation (grant No 200020-135048, the National Centre of Competence in Research QSIT and the CHIST-ERA project DIQIP) and from the European Research Council (grant No 258932).

## Author contributions

Both authors contributed equally to this work.

## Additional information

The authors declare no competing financial interests. Supplementary information accompanies this paper on www.nature.com/naturephysics. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to R.C.