Correlations and Security — genuinely multipartite nonlocality and free-energy cryptography

Doctoral Dissertation submitted to the
Faculty of Informatics of the Università della Svizzera italiana
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

presented by
Xavier Coiteux-Roy

under the supervision of
Stefan Wolf

September 2022

Dissertation Committee

Prof. Jonathan Barrett	Wolfson College, UK
Dr. Charles H. Bennett	IBM T.J. Watson, USA
Prof. Antonio Carzaniga	USI, Switzerland
Prof. Olaf Schenk	USI, Switzerland
Prof. Stefan Wolf	USI, Switzerland

Dissertation accepted on 21 September 2022

Research Advisor	PhD Program Directors
Stefan Wolf	**Stefan Wolf and Walter Binder**

I certify that except where due acknowledgement has been given, the work presented in this thesis is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; and the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program.

Xavier Coiteux-Roy
Lugano, 21 September 2022

À mes parents, Hélène et Claude

Abstract

An important takeaway of Bell's famous theorem is that the notion of information is intrinsically dependent on its physics. To expose this idea, I first analyze a colourful game, the Red-Green-Blue no-signalling game, which is a strikingly simple and instructive illustration of Bell nonlocality and of its underlying framework of Local Operation and Shared Randomness (LOSR). I then extend the setting to more parties in a network, and approach the natural question of how to define nonlocality that is genuinely tripartite. I use the inflation method to devise a thought experiment demonstrating in a device-independent way that the quantum states GHZ and W are genuinely tripartite nonlocal. I also show that this statement can be generalized to more parties in order to reach the conclusion that "there are correlations in Nature that are genuinely N-partite nonlocal, for any N". This claim has been recently verified by three independent experimental teams, up to $N = 4$.

Turning towards another fundamental theory of physics, I examine the cryptographic possibilities offered by the second law of thermodynamics. I find that unconditionally secure cryptography is, in principle, possible in a model where the only limited resource is free energy. More precisely, I build proof-of-principle protocols for secret-key establishment and multi-party computation that are secure against adversaries whose bound in free energy is exponentially larger than the amount required by the honest players. While impractical, the model probes the limits of reversible computing and gives rise to an "almost-no-cloning" theorem that is reminiscent but different from the quantum no-cloning theorem.

Acknowledgements

I am certainly not able to express properly how thankful I am to everyone that contributed to all of my learnings and *expériences*... Let me try briefly.

I am first deeply ingrained to Stefan, my advisor, for his very holistic support. For the inspiration. For his teachings. For sharing his excellence in oration and in writing. For the Dada creativity: *Bref, grazie caro, für alles*.

Then, many thanks to all members of my dissertation committee for their time and interest. Thanks also to the *Decanato*'s office, whose support always made my life easier. I am happy to acknowledge the Fonds de recherche du Québec - Nature et technologie (FRQNT) and the Swiss National Science Foundation (SNSF) for the financial support.

I want to specially thank my co-author Claude Crépeau for setting me on a path that led, after many surprises, to the Chapter 1 of this thesis. I am also very grateful to my co-authors Marc-Olivier Renou and Elie Wolfe, for making me discover the world of causal inflation, the foundation of that Chapter 1. I thank Gilles Brassard and Pierre McKenzie for listening carefully to my research and leading me towards branching programs. I would also like to thank Alberto Montina for sharing his thorough mathematical knowledge and for his help regarding everything optimization. I acknowledge William Schober, Charles-Alexandre Bédard, and Marc-Olivier Renou for welcome feedback on earlier drafts of my thesis.

I am also highly grateful to Charles for helping me understand the value of a good Popperian epistemology (he will know how much that means). I furthermore thank Maélia, Valérie and Charles, for always welcoming me with open arms in their wonderful, spiralling family.

Thanks Sophie for teaching me about constructor theory, but above all, for all the laughs. Grazie Cecilia for our blog project, and for the practice in Italian. Thank you Arne for introducing me to vim, tikz, git — and lead climbing. Thank

you Bart and Boris for the fun collaboration. Thank you Libor and Robert for the warm welcome in Munich. Danke Kathrin for entertaining my learning of German. Many thanks, Ämin, Carla, Geoffroy, Manuel, Pauli, Philippe, and Veronika, for discussions that have changed my world view.

I thank warmly Manuel and Tayo — we have learned so much together during those countless times in the mountains.

Shoutout to the colourful Gandriese community for all the good times: Ardil, Aldo, Aryan, Barbara, Chimgee, Cecilia, Chiara, Dimos, Giulio, Julien, Lisa, Lisa, Malek, Muriel, Raffaele, Ricardo, et Seif.

Lastly, I thank sincerely my family, for being with me throughout this journey and its unforeseen detours.

Contents

Prologue

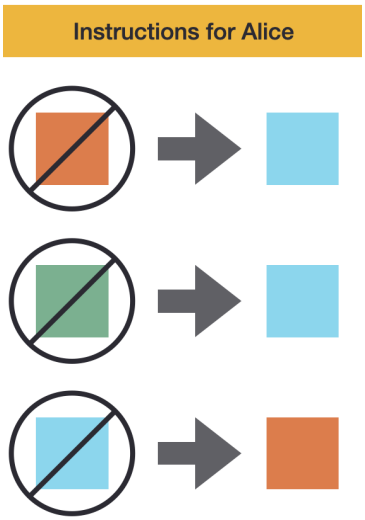
Quantum mechanics has the folkloric reputation of being incomprehensible. This is mainly because quantum mechanics is a radical departure from previous physical theories. The latest manifestation of this departure is Bell nonlocality: The fact that quantum mechanics transcends the class of local hidden-variable models that we would have once thought sufficient to explain (albeit in a very reductionist way) all of the observable world. Maybe surprisingly, the demonstration of this counter-intuitive property, the violation of Bell inequalities, can now be concisely illustrated through the modern concept of nonlocal game. Let us present the idea with the following thought experiment (the RGB no-signalling game) imagined by Claude Crépeau and of which I have found the quantum solution ([CRC19]).

The colourful story of nonlocality

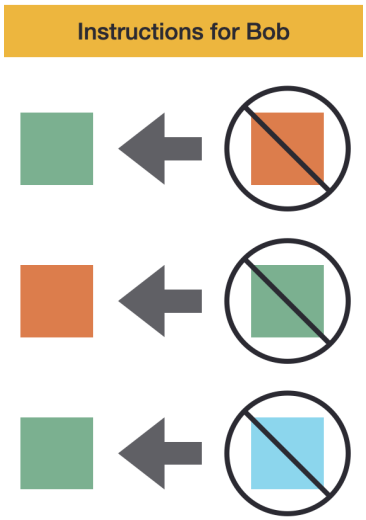
> *Alice and Bob are two actors in a strange game. They start with a choice of three colours (Red, Green, Blue), and are forbidden one colour each (the choice is from their point of view completely random). Alice and Bob each answer one of their remaining two colours, and win if those answers are different; otherwise, if they are the same, they lose.*
>
> *And there is one more crucial detail — Alice and Bob are on two different planets, and because there is a limit to the speed of light, which applies to any type of information transmission, communication between them is impossible, or rather, it is too slow to be useful; if Alice were to send Bob a message, it would arrive to Bob long after the game is over.*

A) “Classical” models

Before the advent of quantum mechanics, in accordance with classical ways of thinking, which posited *by default* that local hidden variables were the only sensible fundamental models, the behaviour of Alice and Bob would have been tentatively modelled by a set of deterministic instructions such as the ones illustrated in Fig. 1a and Fig. 1b. Those instructions assign a definite answer to each possible question [1].



(a) An example of a local hidden-variable model for Alice.



(b) An example of a local hidden-variable model for Bob.

Figure 1. When following a local hidden-variable model, Alice and Bob separately prepare answers for each question they could receive.

The Bell inequality of the RGB game

Let us compute the Bell inequality of the RGB game, that is, let us prove that Alice and Bob can only win with probability up to 8/9 by following a classical model such as the one described above.

Proof. An important remark is that since each colour can be forbidden, there

[1] A slightly more general class of local hidden-variable models would be to allow the players to draw a deterministic model at random from a set of many deterministic models, but we skip over such probabilistic models because picking a strategy at random is never better than choosing the best strategy (the argument is called convexity).

will always be at least 2 different colours in the set of Alice's possible answers (above, it is Blue and Red) and at least 2 different colours in the set of Bob possible answers (above, it is Green and Red) .

It then follows that since there are only 3 different colours in total (Red, Green, Blue), those 2 different colours of Alice cannot be both different from the 2 different colours of Bob. One must appear as a possible answer in both sets of instructions (above, it is Red, which is answered by both players if Alice is asked not-Blue while Bob is asked not-Green).

Hence, because at least one pair of Alice–Bob questions leads to a loss, and because all 9 pairs of questions are equally probable, no local hidden-variable strategy can win with probability more than 8/9. The model illustrated in Fig. 1a and Fig. 1b does achieve 8/9; it is, therefore, optimal. □

Of course, an instructive way to assimilate the limits of such classical strategy is to actually play the game.

B) Quantum models

The relevance of the RGB game comes when we can experimentally observe that Alice and Bob win with probability more than 8/9, because it means that Alice and Bob are doing something that escapes the traditional intuition. As a matter of fact, it is possible for Alice and Bob to win up to probability 11/12 by building devices that exploit the quantum-mechanical phenomenon called entanglement (see Fig 2, and the explanation below). And it is not because Alice and Bob cheat through hidden communication or through prior knowledge of the forbidden colours — the nature of quantum information itself is what steps beyond the classical boundary; it cannot be captured by the so-called classical models.

The explicit quantum strategy

The better-than-classical quantum strategy which wins with probability 11/12 is the following. We use the quantum-information formalism (braket notation) on the Bloch sphere.

Alice and Bob share a singlet state $|\psi^-\rangle_{AB}$. They use the same measurement strategy[2]. According to their own input colour, Alice and Bob choose their mea-

[2]This comes in contrast with the quantum strategy for the CHSH game, which is asymetric in

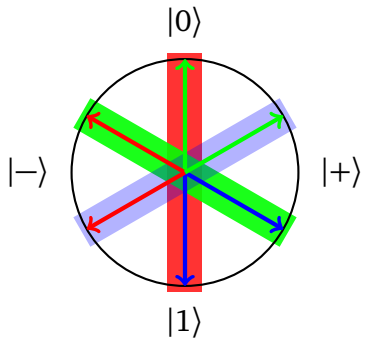


Figure 2. For those familiar with the Bloch sphere, the above figure illustrates Alice and Bob's best quantum strategy: Making the represented projective measurement (interestingly, it is the same) on their respective half of a maximally entangled pair of qubits. The choice of basis (rectangle) depends on their own input colour. Their output is the colour of the measured arrow.

surement from the following list:

$$\Pi_{\text{Red}} = |0\rangle\langle 0|\,, \Pi_{\text{Green}} = \left|v^+\right\rangle\!\left\langle v^+\right|, \Pi_{\text{Blue}} = \left|v^-\right\rangle\!\left\langle v^-\right|\,, \tag{1}$$

where

$$\left|v^\pm\right\rangle = \frac{1}{2}|0\rangle \pm \frac{\sqrt{3}}{2}|1\rangle\ . \tag{2}$$

These 3 projectors are located in the same plane equidistantly (like the Mercedes-Benz logo). The colour names can be permutated freely as long as Alice and Bob do the same projection for the same colour.

If the output of their measurement is positive, they output the colour that comes after their input colour in the cycle *RGB*. Otherwise, they output the previous colour. They never output their own input colour as it leads to a sure loss.

For example, if Alice's input is Green and she measures a positive result when applying the projector Π_{Green}, then $a = G$ and $x = G+1 = B$ (the colour addition is modulo 3). Figure 2 explains the protocol graphically.

Proof. We prove that this quantum strategy only loses with probability $1/12$. We first need to introduce some notation: $a, b \in \{\text{Red}, \text{Green}, \text{Blue}\}$ are the inputs to Alice and Bob, respectively, and $x, y \in \{\text{previous}, \text{next}\}$ are their outputs. The notation refers to the relation with the input colour in reference to the cyclic

Alice and Bob.

order (Red→Green→Blue→Red). For example, on the input $a =$ Red, the output $x =$ previous means Blue. Alice and Bob lose in the following cases:

$$\begin{array}{lll} x = y & \text{if } a = b\,, & \\ x = \text{previous} \wedge y = \text{next} & \text{if } a \text{ (immediately) precedes } b\,, & \text{(all losing cases)} \\ x = \text{next} \wedge y = \text{previous} & \text{if } a \text{ (immediately) follows } b\,. & \end{array}$$

The probability of error E only depends on the relation between a and b and is given by

$$E_{a=b} = \mathrm{tr}\Big(\big|\psi^-\big\rangle\!\big\langle\psi^-\big|_{AB} \cdot \big((\Pi_a \otimes \Pi_b) + (\Pi_a^\perp \otimes \Pi_b^\perp)\big)\Big) = 0\,, \tag{3}$$

$$E_{a \text{ precedes } b} = \mathrm{tr}\Big(\big|\psi^-\big\rangle\!\big\langle\psi^-\big|_{AB} \cdot (\Pi_a^\perp \otimes \Pi_b)\Big) = \frac{1}{8}\,, \tag{4}$$

$$E_{a \text{ follows } b} = \mathrm{tr}\Big(\big|\psi^-\big\rangle\!\big\langle\psi^-\big|_{AB} \cdot (\Pi_a \otimes \Pi_b^\perp)\Big) = \frac{1}{8}\,. \tag{5}$$

And the winning probability of this quantum strategy is (with uniformly random inputs):

$$P_Q(\text{win}) = 1 - \frac{3E_{a=b} + 3E_{a \text{ precedes } b} + 3E_{a \text{ follows } b}}{9} = \frac{11}{12}\,. \tag{6}$$

The game is therefore won with probability 11/12 using this quantum strategy. □

In Appendix A figures the complete and rigorous analysis of the RGB game, in which I also prove, using semi-definite programming, that the quantum strategy presented above is optimal. 11/12 is, therefore, the Tsirelson bound of the RGB game. Interestingly, this Tsirelson bound is rational (Tsirelson bounds are usually irrational numbers. For example, for the CHSH game, the optimal quantum strategy wins with probability $\frac{2+\sqrt{2}}{4}$.)

Takeaway of this introduction

The simplicity of the RGB game formulation, the clarity of its Bell inequality, the rationality of its Tsirelson bound, and the symmetry of its best quantum solution all make it an excellent pedagogical tool to learn the basic concepts of Bell nonlocality and to familiarize oneself with quantum measurements on the Bloch sphere.

C) Structure of this thesis

This thesis investigates the nature of information. It focuses on two ideas: network nonlocality (quantum mechanics of information) and reversible computing (thermodynamics of information).

As it is my epistemological conviction that too many initial details hinder comprehension, I have tried to incorporate multiple levels of explanations in my thesis, starting from high-level content (which I aspire one day to turn into blog posts) and progressing to standard article format, with most of the dry technical details only in the appendices. I hope that such incremental structure helps the reader to better understand the content.

- The present prologue introduced the concept of Bell nonlocality through the RGB no-signalling game, which rigorous analysis figures in Appendix A.
- The first chapter — Correlations — is the logical continuation of the prologue. In that chapter, I extend the concept of Bell nonlocality to causal networks of many players. After a gentle introduction of the inflation method, I exhibit a thought experiment on the $|\mathrm{GHZ}\rangle$ quantum state whose conclusion is that “Nature’s nonlocality cannot be merely bipartite." This statement that constrains the set of physical models that could one day replace quantum mechanics, and it has now been verified experimentally. In Appendix B, I generalize the proof to more parties (concluding from measurements on $|\mathrm{GHZ}_N\rangle$ that “Nature’s nonlocality is boundlessly multipartite nonlocal") and give the proof that the $|\mathrm{W}\rangle$ quantum state also exhibits genuinely tripartite nonlocality.
- The second chapter — Security — is self-contained. It explores the cryptographic consequences of perfect reversible computing and of the second law of thermodynamics. I offer protocols for two of the main tasks of cryptography — namely, secret key establishment and secure two-party computation — that are information-theoretically secure against adversaries that are bounded in free energy.
- I conclude with an epilogue containing some remarks, open questions, and comments about the present research.

Chapter 1

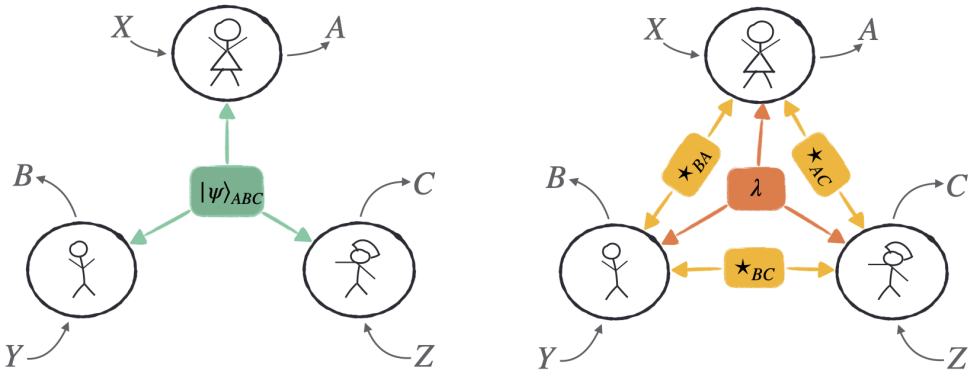
Correlations

- Section 1.1 describes the principles around network nonlocality and Section 1.2 the inflation method. They aim to be accessible.
- Section 1.3 ([CRWR21b]) is work with Marc-Olivier Renou and Elie Wolfe. It explains the main result — the prediction by quantum theory of genuinely tripartite nonlocality — in a concise manner.
- Appendix B ([CRWR21a]), also with Marc-Olivier Renou and Elie Wolfe, handles the technical details, and extends the result to more states and more parties: "Nature is boundlessly multipartite nonlocal."
- Section 1.4 refers to recent experimental demonstrations of these results.

1.1 Network nonlocality

In the prologue, the RGB two-player game highlighted the distinction between shared randomness and quantum entanglement. Network nonlocality is a generalization of that basic scenario. Formally, a causal network is represented by a directed acyclic graph (DAG) whose nodes are players (Section 1.1.1) and resources of different kinds (Section 1.1.2), and whose edges pair the resources to the players (Section 1.1.3).

One of the main topics studied in this thesis — genuinely tripartite nonlocality — is the contrast of the two causal scenarios illustrated in Figure 1.1 (whose meaning we clarify in the next sections). Further, simpler examples of causal network are drawn in Figure 1.2 and Figure 1.3a.



(a) Tripartite quantum resource.

(b) Triangle scenario with arbitrary no-signalling resources plus shared randomness.

Figure 1.1. We prove in Section 1.3 ([CRWR21b]) that some behaviours $P(ABC|XYZ)$ possible in the network on the left are not compatible with the network on the right.

1.1.1 Players

Players are nodes representing deterministic devices that take a classical input (the questions) and produce a classical output (the answers) by performing local operations (LO) on certain resources. The allowed set of local operations depend on the type of resources and theory considered (see below).

Players are probed in a *device-independent* manner, meaning that the only quantity of interest is the (classical) conditional probability distribution over all players, which represents their input–output relation (their behaviour).

1.1.2 Resources

This thesis is concerned with three types of resources and their associated local operations.

i. Shared randomness (SR — also called local hidden variables or classical resources) and post-processing.

ii. Quantum entanglement and quantum channels (completely positive maps).

iii. Wildcard resources in any causal theory — these are unspecified resources that obey the device-replication condition (see below) and the no-signalling

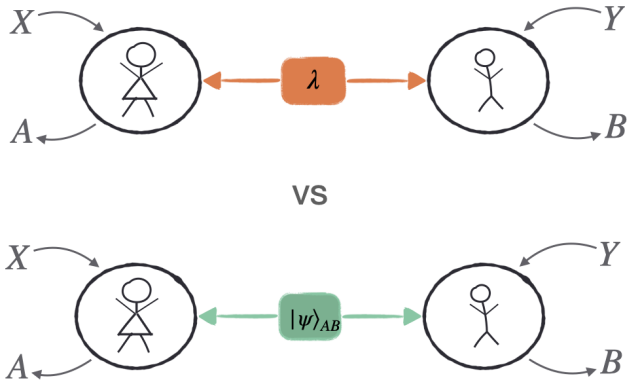


Figure 1.2. For example, in the RGB game presented in the prologue, the quantum players perform local operations corresponding to quantum measurements on a shared maximally entangled state (bottom), while the local-hidden-variable players are restricted to post-processing of shared randomness (top). By analyzing the conditional probability distribution $P(AB|XY)$ of their respective answers (now A, B) given their respective questions (now X, Y), one concludes that certain input–output behaviours are possible in the first scenario but not in the second — they violate a Bell inequality.

principle (also below): They can be, for example, quantum entangled states, nonlocal boxes (such as the Popescu-Rohrlich box), or any kind of resources described by some generalized probabilistic theory (GPT) and which could, for example, allow for local operations that generalize entangled measurements.

1.1.3 Causal relations

Those different flavours of players and resources are also studied in the bipartite case. The novelty of network nonlocality is to restrict the causal relations between players and resources: Not all players are connected to all resources — some pairs are assumed to be independent. For example, in the triangle scenario plus shared randomness (featured in Figure 1.1b), the shared randomness is common to all players, but the unspecified no-signalling resources are shared only by pairs of players (no tripartite “nonlocal” resource is allowed).

1.2 The inflation method

Inflation is central to the study of network nonlocality. Inflation is a thought experiment that relies on imagining multiple copies of the players and resources, connected in various manners. Its interest comes from the fact that the existence of a behaviour in the inflated scenarios allows us to constrain the set of distributions in the original causal scenario. We first describe how these inflated scenarios are constructed (Section 1.2.1). Then we describe the core rules to derive constraints from inflated scenarios (Section 1.2.2) and give a simple example of a proof made through inflation (Section 1.2.3). At last, we explain how inflation can be taken as fundamental (Section 1.2.4).

1.2.1 Types of inflation

Since inflation is based on the duplication of players and resources, it relies on the following assumption.

Device-replication principle

Identical independent copies of any players and of any resources can exist.

Note the weakness of this assumption; the principle does not, for example, contradict the quantum no-cloning principle because it does not require that the actual copying of unknown states be possible. For instance, a $(|00\rangle + |11\rangle)/\sqrt{2}$ state can be obtained in quantum mechanics by a device (a laser + a crystal) exploiting spontaneous parametric down-conversion (SPDC). A duplicate of the device would consist of another, identical laser plus another, identical crystal.

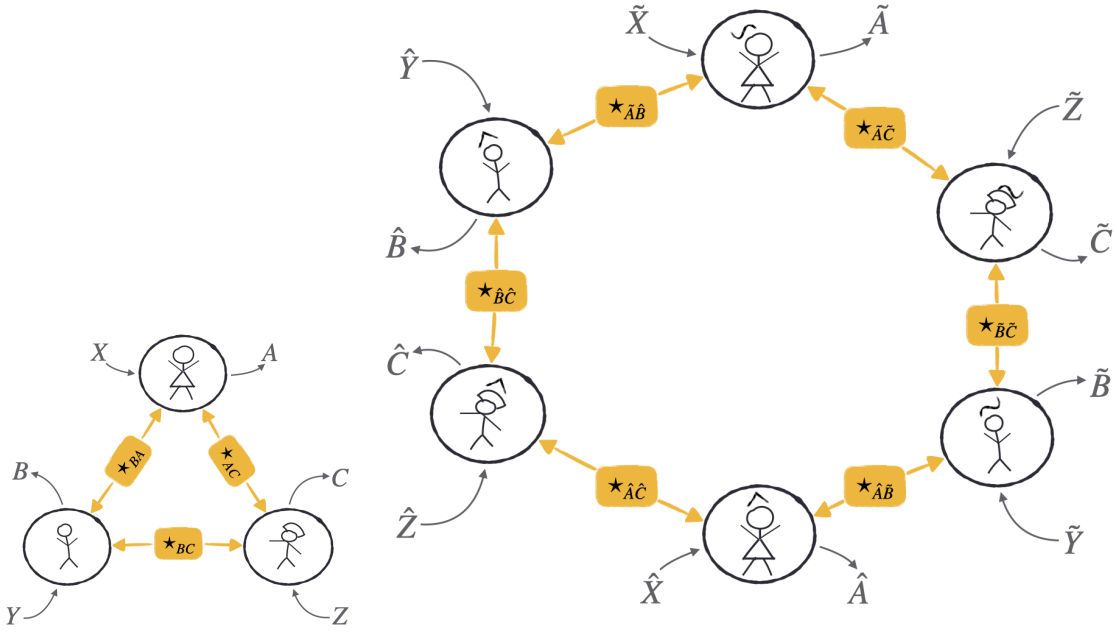
There are three different flavours of inflation, depending on how the resources are copied.

1 *Non-fanout inflation* allows fewer inflation possibilities than fanout inflation. In the k^{th}-level inflation, there are exactly k copies of each player and of each resource, and they are connected so as to be locally undistinguishable from the original connections. The global structure, however, need not be identical to k copies of the original scenario. The wheel in Figure 1.3b is an example of non-fanout inflation. Note how each resource is connected to the two players corresponding to her "type", and each player is connected to two resources of the appropriate "type".

2 *Fanout inflation* is more permissive in its cloning: it allows clones of a same

player to be connected to the same instance of a resource. This can only be applied to classical resources (shared randomness) because nonlocal resources cannot be in general copied in this way (for example, copying half of a maximally entangled state would allow to signal faster than light). Pure fanout inflation is not used in this work.

3 *Mixed inflation* is the mixed use of fanout inflation for the (classical) shared randomness and non-fanout inflation for the additional (non-classical) resources. Mixed inflation is applied in Section 1.3 to the triangle scenario with shared randomness (Figure 1.1b).



(a) The triangle scenario without shared randomness.

(b) The wheel — a possible second-order non-fanout inflation of the triangle scenario.

Figure 1.3. Illustrative example considered in Section 1.2.3.

1.2.2 The principles of inflation

Besides from device replication, inflation relies on two major principles [CDP11; GBC+20; CRWR21a].

Causality I (independence principle)

If two players do not share a common resource, they exhibit statistically independent behaviours.

Causality II (no-signalling principle)

If two (sub)groups of players and resources from the original or inflated scenarios are isomorphic to each other, they exhibit identical behaviours.

We illustrate their use in the next section.

Note that in the context of the LOSR framework, where all players share a common random variable λ, the independence principle and the no-signalling principle apply individually for each value λ_i of the shared randomness.

1.2.3 Inflation as a proof method

We give an example of how inflation can be used as a proof technique to rule out causal models.

Example (3-way coin flip). We use as an example the causal structure of the triangle network without shared randomness, represented in Figure 1.3a.

We then use the second-level inflation of Figure 1.3b to show that the 3-way coin flip, $\frac{1}{2}[000]+\frac{1}{2}[111]$, is a distribution that is incompatible with that causal structure.

$$P(A{=}B{=}C{=}0) = P(A{=}B{=}C{=}1) = 1/2\,. \qquad \text{(3-way coin flip)}$$

The result was first proven in [HLP14].

Proof. We assume by contradiction that $\frac{1}{2}[000]+\frac{1}{2}[111]$ can be realized by the causal scenario of Figure 1.3a.

On one hand, we have by no-signalling that

$$\begin{aligned} P(\tilde{A}{=}\hat{B}) = P(A{=}B) &= 1\,, && \text{(no-signalling)}\\ P(\hat{B}{=}\hat{C}) = P(B{=}C) &= 1\,, && \text{(no-signalling)}\\ \implies P(\tilde{A}{=}\hat{C}) &= 1\,. && \text{(transitivity)} \end{aligned}$$

On the other hand, we have by causality that

$$P(\tilde{A},\hat{C}) = P(\tilde{A}) \cdot P(\hat{C}) \,, \implies P(\tilde{A}{=}\hat{C}) = 1/2 \,. \qquad \text{(independence)}$$

We conclude from this contradiction that the 3-way coin flip cannot be produced in the triangle scenario without shared randomness, in any causal theory generalizing quantum theory. □

1.2.4 Inflation as a foundation

In our works [CRWR21b; CRWR21a] (Section 1.3, Appendix B), our use of the inflation method goes beyond its use as a proof method: we use it as a definition of genuinely tripartite (and N-partite) nonlocality.

Definition 1 (LOSR genuinely tripartite nonlocality)**.** *A no-signalling*[1] *tripartite behaviour $P(ABC|XYZ)$ is genuinely tripartite nonlocal if and only if it is not compatible with all levels (an infinite hierarchy) of mixed inflation applied to the triangle scenario (Figure 1.1b).*

The necessity for a LOSR definition of genuinely tripartite nonlocality arose because previous definitions of the concept (namely, in [Sve87] and in [BBGP13]) were based on the local operations and classical communication framework (LOCC). A striking example of the inadequacy of this framework when doing causal analysis is the following.

Example (parallel hack). Consider the tripartite probability distribution $P_{ABC} = P_{AB_1} \cdot P_{B_2C}$ obtained by the parallel composition of a bipartite nonlocal distribution P_{AB_1} between Alice and Bob and of an independent bipartite nonlocal distribution P_{B_2C} between Bob and Charlie. This distribution P_{ABC} is genuinely multipartite nonlocal according to Svetlitchny's criterion. It is, however, clearly produced from bipartite-nonlocal resources.

Our redefinition solves this operational problem[2].

[1] A behaviour cannot signal to Alice if for every subset, $P(A|XYZ) = P(A|X)$. A behaviour is said to be no-signalling when this condition holds, *mutatis mutandis*, for all players and all coalitions of players. In [CRC19], we give an alternative, but equivalent, formulation of the class of no-signalling behaviours.

[2] A similar problem existed with the LOCC definition of genuinely multipartite *entanglement* [SU08], which implies, for example, that the 4-qubit state $|\psi^-\rangle_{AB} \otimes |\psi^-\rangle_{B'C}$ is genuinely tripartite entangled. A more operationally sound, LOSR definition was introduced in [NWRPK20] to remedy to the problem.

1.3 No bipartite-nonlocal causal theory can explain Nature's correlations ([CRWR21b])

The following is a full retranscription of my work ([CRWR21b]) with Marc-Olivier Renou and Elie Wolfe.

Abstract.— We show that some tripartite quantum correlations are inexplicable by any causal theory involving bipartite nonclassical common causes and unlimited shared randomness. This constitutes a device-independent proof that *Nature's nonlocality is fundamentally at least tripartite* in every conceivable physical theory — no matter how exotic. To formalize this claim we are compelled to substitute Svetlichny's historical definition of genuine tripartite nonlocality with a novel theory-agnostic definition tied to the framework of Local Operations and Shared Randomness (LOSR). A companion article [PRA. 104, 052207 (2021)] generalizes these concepts to any $N \geq 3$ number of parties, providing experimentally amenable device-independent inequality constraints along with quantum correlations violating them, thereby certifying that Nature's nonlocality must be *boundlessly* multipartite.

Introduction.— Nonlocality is one of the most common-sense challenging, but nevertheless well-established, properties of quantum physics [EPR35; Bel64]. Two or more parties measuring a shared entangled quantum state can obtain correlated outputs which resist explanation in terms of any local hidden-variable model. Understanding of the concept of nonlocality and of its manifestations has captivated the attention of hundreds of researchers spanning decades, see Ref. [BCP$^+$14] and references therein. Seminal milestones include the development of tasks inaccessible with only classical resources such as the CHSH game [CHSH69], celebrated experimental demonstrations [FC72; AGR81; TBZG98; H$^+$15; S$^+$15; G$^+$15; RBG$^+$17], and the device-independent certification of experimental apparatuses taken as black boxes [MY98; AGM06; ABG$^+$07; P$^+$10; RAF16].

The bipartite scenario is arguably the most studied. However, scenarios with more that two parties exhibit certain valuable features which are qualitatively distinct from those of the bipartite scenario. For instance, tripartite quantum scenarios can demonstrate a stronger version of Bell's theorem [GHSZ90]. More generally, the nonlocality of multipartite chains of bipartite Bell inequalities decays to zero as the number of party increases (the gap between the local and no-signalling bounds collapses), whereas genuinely multipartite Bell inequalities allow for *non*-decaying witnesses of nonlocality [WW01; CAF06; CCAA12].

Any bipartite scenario can be artificially lifted to a tripartite scenario by adding an extra spectating party [Pir05]. To exclude such uninteresting cases, it is critical to find an appropriate criterion for whether a setup in a tripartite scenario is *genuine*, *i.e.*, exploits possibilities not present in scenarios involving only two parties. One avenue to highlight tripartiteness is to focus on entanglement — the property of quantum states that enables nonlocal correlations. This is the proposal of Ref. [SFK+20] which relates nonlocality to the notion of tripartite entanglement formalized in Ref. [NWRPK20]. Such genuinely tripartite entanglement resists any explanation in terms of local operations applied to networks of bipartite quantum states.

This letter proposes instead a theory-agnostic avenue. We consider any causal description of Nature — including classical and quantum physics, and beyond — and ask the following fundamental question: *Could our physical world be comprised of merely bipartite nonlocal causal constituents?* That is, does there exist any description of quantum theory's operational predictions, perhaps very exotic, built upon bipartite nonclassical common causes? It is already well known that bipartite resources are not enough to reproduce all tripartite phenomena. For instance, perfect correlations between three parties cannot be obtained from bipartite resources, even in a theory-agnostic analysis [HLP14].[3] However, that result is predicated on the absence of shared randomness, which is arguably not realistic. Shared classical randomness can be obtained by pre-agreement on a common classical phenomenon to observe, or with preestablished shared randomness stored in local memories. It is also known that boxworld [Jan12], an alternative theory for correlations based on no-signalling boxes [Bar07], cannot reproduce all quantum correlations even when allowing for shared randomness [CR17; Bie20]. This result is restricted to a precise alternative to classical and quantum mechanics, and may not encompass all possible causal theories of correlations [CDP11; Chi14].

Accordingly, in this letter we focus on the (non)simulability of certain tripartite correlations in setups allowing for the local composition of any bipartite resources *with* global access to common shared randomness. We adopt a theory-agnostic perspective that applies to any causal theory [CDP11; Chi14] compatible with device replication [CRWR21a] — however exotic it might be. This includes the classical theory and quantum theory as specific causal theories, but also more generally any hypothetical Generalized Probabilistic Theory (GPT) such as boxworld [Jan12]. Our approach is closely related to the concept of network non-

[3] The proof is given in Section 1.2.3.

locality which has been extensively studied in the past decade [TPKLR21; Fri12; BGP10; RBB$^+$19; WPKG$^+$21].

It is natural to name *genuinely tripartite nonlocal* those correlations which resist explanation in terms of arising from bipartite resources and shared randomness. That denotation, however, conflicts with a historical term of art due to Svetlichny [Sve87]. We will explain why Svetlichny's definition is not suitable for causal analysis, leading us to propose an alternative definition (see Definition 2), which constitutes the main *conceptual* result of this letter.

Subsequently, we prove that $|\mathrm{GHZ}\rangle := (|000\rangle + |111\rangle)/\sqrt{2}$ is a resource that can manifest correlations which are genuinely tripartite nonlocal according to our novel definition. This is the subject of Proposition 3, the main *technical* result of this letter. The formal characterization of such correlations, along with our proof of the quantum realizability of such correlations, together constitute a profound implication: The operational predictions of the quantum theory preclude — in the strongest possible sense — any future description of Nature built upon bipartite common causes, regardless of how exotic or nonclassical they could be.

We conclude this letter by contrasting our no-go theorem with previous works aiming to exclude physical theories limited to 2-way nonclassical common causes. We also recognize the desideratum of certifying Nature's genuine multipartiteness without presupposing the operational validity of quantum theory, and accordingly discuss considerations for the experimental verification of our results.

Although this letter focuses mainly on the tripartite case for pedagogical simplicity, we note that all of our introduced concepts and most of our results are valid in the generalized multipartite case, beyond three parties. We develop the N-partite case in an extended version of this work [CRWR21a], which includes extending the result regarding the $|\mathrm{GHZ}\rangle$ state to any number of parties N (see Proposition 5) as well as a result regarding the resourcefulness of the $|\mathrm{W}\rangle := (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ state (see Proposition 4). These generalizations of our main results to any number of parties imply that, for any fixed k, any theory based on subjecting k-way multipartite resources to local operations cannot reproduce the operational predictions of quantum theory for $N{>}k$ spacelike-separated parties.

A causally meaningful notion of genuine tripartite nonlocality.— We seek to distinguish those correlations which admit causal explanation in terms of bipartite nonclassical sources from correlations which resist any such causal explanation. Furthermore, in order to claim that Nature's nonlocality is necessarily tripartite

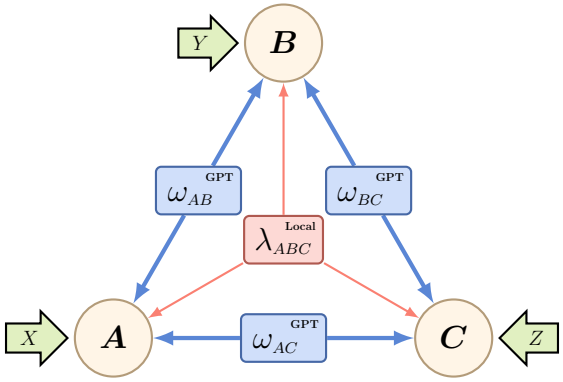


Figure 1.4. A tripartite distribution is genuinely tripartite nonlocal according to our definition if it cannot be realized by the above scenario, where the output of each player is determined by local operations (such as joint measurements) on 1) their input, 2) the 3-way randomness, and 3) 2-way GPT resources.

without *a priori* assuming the correctness of quantum causal explanations, we must be careful to apply the label "genuinely tripartite" only to those correlations which resist bipartite causal explanations in *any* physical theory.

One might ask if Svetlichny's historically accepted *definition* of genuine tripartite nonlocality [Sve87] is suitable for capturing such causal distinction. But no, it is easily hacked: the correlations obtained from CHSH violations in parallel between Alice and Bob as well as between Bob and Charlie fulfill Svetlichny's criterion for genuine tripartite nonlocality [CTPdV21]. Such correlations, however, are facially achievable in quantum theory restricted to bipartite states. What Svetlichny's definition *is* suitable for is as device-independent witness of genuine tripartite entanglement. Note that the traditional definition of genuine tripartite *entanglement* due to [SU01] is susceptible to precisely the same sort of hacking: A 4-qubit state composed of a singlet shared between Alice and Bob as well as a singlet shared between Bob and Charlie satisfies Seevinck's criterion for genuine tripartite entanglement, despite factorizing into bipartite constituents.

The reasons why the historical definitions of tripartiteness for both nonlocality and entanglement are ill-suited for causal analysis is because they were motivated by quantifying resourcefulness relative to Local Operations and Classical Communication (LOCC). When analysing Bell-inequality violations, however, we presume that the parties involved may be spacelike separated, which enforces the No-Signalling condition. When classical communication is forbidden, the only form of processing of nonclassical resources that remains is via Local Operations

and Shared Randomness (LOSR) [WSS+20; SFK+20; SZCG20].

Therefore, it is critical to employ the LOSR resource-theoretic framework instead of LOCC when quantifying the nonclassicality of a common cause in a Bell experiment. Ironically, Svetlichny's [Sve87] definition was specifically tailored to the task of witnessing *LOCC* tripartite entanglement, which is irreconcilably in tension with quantifying nonlocality, as nonlocality is only meaningfully studied in the *LOSR* paradigm.

A notion of genuine tripartiteness relative to LOSR entanglement has been formulated in Refs. [NWRPK20; SFK+20]. Ref. [SFK+20] seamlessly extends that notion to provide a definition of genuine tripartite *nonlocality* based on the concept of a correlation resisting explanation in terms of bipartite quantum states acted upon by LOSR. Our main conceptual contribution here is to provide an LOSR-motivated definition for genuine tripartite nonlocality that is theory-agnostic, in that it imagines that LOSR could be applied to *any* sort of bipartite nonclassical resource, not just quantum entanglement.

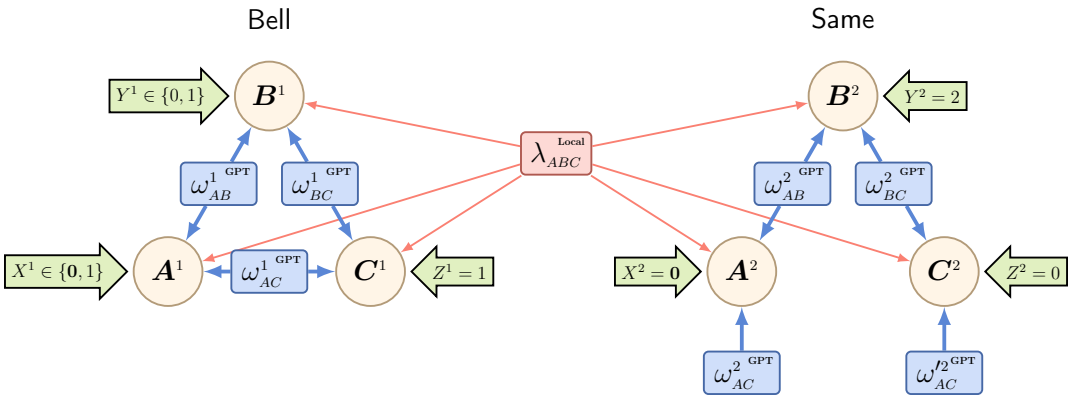


Figure 1.5. The inflation technique consists of duplicating and rearranging players, sources, and input distributions. Here we inflate the (non genuinely tripartite-nonlocal) triangle scenario of Figure 1.4 as to have the players play two parallel games (Bell and Same). It leads to a contradiction with the statistics of measurements on $|\mathsf{GHZ}\rangle$, and therefore to the conclusion that the $|\mathsf{GHZ}\rangle$ quantum state is a genuinely tripartite-nonlocal resource. The duplicated players constitute indistinguishable copies of the same abstract process, hence Alice, on input $X{=}\mathbf{0}$, could be playing either game (A_1 and A_2 must have the same behaviour). The only condition on the random inputs is that they be independent from all of the sources. The figure represents a cut of a larger inflation of order 3, consisting of a triangle and a hexagon.

We appeal to the GPT formalism to formally define local operations on "*any*" sort of bipartite nonclassical resource. In brief, we allow for any exotic physical theory that can extend (or restrict) the bipartite resource of quantum entanglement (including all nonsignalling nonlocal boxes such as the PR box [PR94]), and that can extend (or restrict) the process of combining subsystems via entangled joint quantum measurement [BGP10; BRGP12]. Quantum theory itself is merely one of an infinite spectrum of such hypothetical physical theories [CDP11; Chi14; SB09; SB10; Bar07; Jan12].

Definition 2 (Genuine LOSR tripartite nonlocality)**.** *A tripartite nonsignalling correlation P is said to be* genuinely LOSR tripartite nonlocal *if and only if it cannot be obtained by local operations over any 2-way GPT resources along with 3-way shared randomness between all parties. That is, P is said to be genuinely LOSR tripartite nonlocal when it cannot be realized via the abstract causal process depicted in Figure 1.4.*

Equipped with this new definition, let us now provide examples of quantum tripartite resources which are genuinely tripartite nonlocal. We also assume that *every* causal theory allow for device replication, i.e. one can make independent and identical copies of resources, to draw inferences from the nonfanout-inflation technique [WSF19] (see Ref. [CRWR21a] for an extended formal treatment of these ideas).

Genuinely tripartite nonlocal correlations exist in Nature.— We now prove that $|\mathrm{GHZ}\rangle := |000\rangle + |111\rangle/\sqrt{2}$ generates quantum correlations which are genuinely LOSR tripartite nonlocal. As in [CR17], the basic idea is to split the problem into two intertwined games, respectively detecting that some party's measurement must depend on both (1) some nonclassical resource, albeit possibly bipartite, and (2) some tripartite resource, albeit possibly classical. Performing well at both (1) *and* (2) would require dependence on a genuinely LOSR tripartite nonclassical (entangled) resource. More precisely, we introduce

(1) A bipartite nonlocal game (conditioned on the third's player output), which rewards nonclassical randomness.

This first task is the standard CHSH game between Alice and Bob, with the particularity that it is scored only when Charlie outputs $C{=}1$. The function to maximize is (the observables take value in $\{-1,+1\}$)

$$I_{\mathrm{Bell}}^{C_1=1} := \langle A_0B_0\rangle_{C_1=1} + \langle A_0B_1\rangle_{C_1=1} + \langle A_1B_0\rangle_{C_1=1} - \langle A_1B_1\rangle_{C_1=1}\,. \tag{1.1}$$

(2) A tripartite consistency game that rewards no-randomness or tripartite randomness.

Here, the players are asked to output the same result (which can take either of the two values ±1), and are scored according to the function

$$I_{\text{Same}} := \langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle \,. \tag{1.2}$$

Because $A_0 := A_{X=0}$ belongs to both games, on that input Alice is oblivious as to which of the two games she is partaking in. This prevents her from playing the two games separately; rather, her strategy for $X = 0$ must be optimized in respect to both games simultaneously. The impossibility of Alice decoupling the two games leads to our central argument:

"(1.1) + (1.2) rewards only genuinely tripartite nonlocality."

More precisely, in the $|\text{GHZ}\rangle$ case, we combine $I_{\text{Bell}}^{C_1=1}$ and I_{Same} into an inequality:

Proposition 3 (GHZ_3)**.** *In the absence of any 3-way nonclassical cause, if* $\langle C_1 \rangle = 0$*,*

$$I_{\text{Bell}}^{C_1=1} + 4 I_{\text{Same}} \leq 10 \,. \tag{1.3}$$

Measurements on the $|\text{GHZ}\rangle$ *quantum state can violate the above by reaching* $I_{\text{Bell}}^{C_1=1} + 4 I_{\text{Same}} = 2\sqrt{2}+8 > 10$*. The maximal GPT violation reaches the algebraic maximum of* 12*.*

For a better presentation, we focus on explaining why reaching the algebraic maximum of 12 leads to a contradiction. The quantified proof of Ineq. (1.3) is done in [CRWR21a], where we also explain how to remove the $\langle C_1 \rangle = 0$ assumption (this assumption is experimentally problematic).

Proof of equation (1.3)*, main ideas.* Let us assume by contradiction the existence of three black-box devices that satisfy the causal structure of the triangle scenario (Figure 1.4), but that can nevertheless reach the perfect scores $I_{\text{Bell}}^{C_1=1} = 4$ and $I_{\text{Same}} = 2$.

Inspired by inflation-technique ideas, we now imagine an inflated scenario where the devices and resources are duplicated and rearranged; see Figure 1.5. Note that the same instance of the shared randomness λ can be infinitely copied and hence be distributed to all parties, but that the (2-way) GPT resources cannot; it is possible, however, to have multiple independent instances of each of those resources by device replication. In our scenario, some of the 2-way resources

are inputted only to a single player; their second halves can be considered never measured.

First, on the left-hand side of the figure, the devices take the Bell test and inherit exactly the behaviour of the original devices (if we ignore the right-hand side of the inflated scenario, the left-hand side is precisely the original scenario).

An important property of Bell inequalities is that any violation implies true randomness [P$^+$10; BMP18]. In our case, A^1B^1 reaches the maximal algebraic violation of CHSH, which implies that A^1 (and also B^1) is totally unpredictable. Hence, in particular,

$$A^1_{X=0}C^2_{X=0} \text{ are perfectly uncorrelated.} \tag{1.4}$$

Second, on the right-hand side, the devices perform the Same test. As we do not know the inner workings of the black boxes, we cannot describe their whole tripartite joint behaviour. However, note that A^2B^2 and B^2C^2 inherit the joint statistics of their respective original counterparts, because they see the same environment. This means that they achieve perfect correlations at the Same test: $A^2_{X=0} = B^2_{X=0} = C^2_{X=0}$. Finally, from the structure of the graph, A^1C^2 and A^2C^2 also see the same environment and share the same statistics, so

$$A^1_{X=0}C^2_{X=0} \text{ are perfectly correlated.} \tag{1.5}$$

The contradiction between (1.4) and (1.5) ends our demonstration. In [CRWR21a] we explain how all the ingredients of this proof can be made quantitative to obtain the trade-off described by Eq. (1.3). □

Proof of violation. The quantum violation is achieved using $|\text{GHZ}\rangle$: On inputs corresponding to the Same game (XYZ=020), all players measure in the rectilinear basis. On input Z=1, Charlie measures his state in the Hadamard basis and obtains marginal $\langle C_1\rangle = 0$; when he obtains C_1=1 (corresponding to a measurement result $|+\rangle_C$), the state of Alice and Bob is steered towards the maximally entangled state $|\phi^+\rangle_{AB}$ and they can play the Bell game using the standard optimal strategy for CHSH.

Note that the maximal algebraic violation is achieved by the nonsignalling distribution $A_x{:=}(-1)^{r_0 \oplus r_1 \cdot x}$, $B_y{:=}(-1)^{r_0 \oplus x\cdot y}$, $C_z{:=}(-1)^{r_z}$, where r_0 and r_1 are uniformly random bits, and $\oplus$ denotes addition modulo 2. □

Generalization.— In [CRWR21a], we show how these ideas can be used to prove a similar result for the $|\text{W}\rangle := |001\rangle + |010\rangle + |100\rangle/\sqrt{3}$ state.

Proposition 4 (W)**.** *Appropriate measurements on the* $|\mathrm{W}\rangle$ *quantum state lead to genuinely LOSR-tripartite-nonlocal correlations.*

We also explain how to generalize our work to scenarios with arbitrary number of parties, in which $|\mathrm{GHZ}\rangle$ straightforwardly generalizes to an N-partite state $|\mathrm{GHZ}_N\rangle$. Indeed, our definition 2 can be generalized to the multipartite case [CRWR21a], introducing the concept of genuine LOSR multipartite nonlocality for which we have:

Proposition 5 (GHZ_N)**.** *For any N, genuinely LOSR N-multipartite nonlocal correlations can be obtained through appropriate measurements on the quantum state* $|\mathrm{GHZ}_N\rangle$.

Discussion.— We have proven that the correlations of $|\mathrm{GHZ}\rangle$ can only be obtained using genuinely LOSR-tripartite-nonlocal resources. Our work implies, under the (reasonable) hypothesis that quantum mechanics' predictions for local measurements over $|\mathrm{GHZ}\rangle$ are exact, that *Nature cannot be merely bipartite*. In [CRWR21a], our generalization implies that it cannot even be N-partite for any fixed N.

In our introduction, we intentionally kept the concept of *combining any exotic GPT bipartite resources*, together with tripartite shared randomness, vague. Let us now clarify it, based on the nonfanout-inflation technique [WSF19, Sec. 5.4], which is used in our proof (see also other related frameworks [HLP14; Chi14; CDP11; GBC$^+$20; BG21; BR21; Pir21]). It relies on two postulates. First, we admit the possibility of device replication: Any device distributing local resources, or locally operating resources, can be duplicated in independent copies, and one can reorder these replicated devices to form a new setup. Second, we admit causality. It implies that any two identical subsets of the initial or new setups must have the same behaviour (more than a consequence of causality, this can be seen as an operational definition of what is causality). Moreover, for any fixed value of the shared randomness, any marginal correlation of two disjoint subsets of a setup must factorize. With inflation, these two postulates provide the definition of *theory-agnostic correlations in networks*, which are all correlations P which do not lead, in any inflated scenario, to any contradiction. See Ref. [CRWR21a] for the formalized definition.

Let us conclude this letter with experimental considerations. In [CRWR21a], we relax our experimentally unrealistic constraint $\langle C_1\rangle = 0$ for inequality (1.3) to a generalized inequality valid for all C_1. Moreover, remark that for a mixture of the $|\mathrm{GHZ}_3\rangle$ state with white noise, of fidelity f, our inequality is vio-

lated for $f \gtrsim 93\%$. In [CRWR21a], we propose an algorithm based on inflation able to witnesses infeasibility down to $f \gtrsim 85\%$. This shows that an experimental proof that Nature is not merely bipartite is accessible to current technologies [HSH+14]. The experimental feasibility for larger N values is an open question [ZHW+15; ZBH+19].

1.4 Experiments

Genuinely tripartite nonlocality (as proposed theoretically in the previous section) has been experimentally demonstrated by three independent teams ([CRZ+22; MLYF22; HGJ+22]) by making measurements on the $|\text{GHZ}\rangle$ state.

In Appendix B, we make a similar claim about the quantum state $|\text{W}\rangle$ (it also exhibits genuinely tripartite nonlocality). At the time of this writing, it has not been experimentally tested.

In Appendix B, we also prove the stronger claim that "Nature is boundlessly multipartite nonlocal" by extending the thought experiment on $|\text{GHZ}\rangle$ to the generalized quantum states $|\text{GHZ}\rangle_N$. This has also been partially verified by the experiments in [CRZ+22] and [MLYF22], which confirm that $|\text{GHZ}\rangle_4$ exhibits genuinely 4-partite nonlocality.

Chapter 2

Security

This chapter is self-contained.

Key agreement and oblivious transfer from free-energy limitations ([CRW22])

Abstract. We propose one of the very few *constructive* consequences of the second law of thermodynamics. More specifically, we present protocols for secret-key establishment and multiparty computation the security of which is based fundamentally on Landauer's principle. The latter states that the erasure cost of each bit of information is at least $k_B T \ln 2$ (where k_B is Boltzmann's constant and T is the absolute temperature of the environment). Albeit impractical, our protocols explore the limits of reversible computation, and the only assumption about the adversary is her inability to access a quantity of free energy that is exponential in the one of the honest participants. Our results generalize to the quantum realm.

2.1 Introduction

2.1.1 Motivation

In the past decades, several attempts were made to achieve cryptographic security from physical properties of communication channels: Most prominently, of course, *quantum cryptography* [BB84; Eke91]; other systems made use of noise in

communication channels [Wyn75] or bounds on the memory space accessible by an adversary [Mau92]. These schemes have in common that no limit is assumed on the opponent's computational power: They are *information-theoretically secure*.

Our schemes for achieving confidentiality (key agreement or, more precisely, *key expansion*) as well as secure coöperation (multiparty computation, *i.e.*, *oblivious transfer*) rely solely on a bound on the accessible *free energy*[1] of an adversary. More specifically, we propose schemes the security of which follows from *Landauer's principle*, which is a quantification of *the second law of thermodynamics*: *In a closed system, "entropy" does not decrease* (roughly speaking).

Landauer's principle states that the *erasure of information* unavoidably costs free energy, the amount of which is proportional to the length of the string to be erased. On the "positive" side, the *converse* of the principle states that the all-0 string of length N has a free-energy value proportional to N. More precisely, the erasure cost and work value are both quantified by $k_{\mathrm{B}}\mathrm{T}\ln 2 \cdot N$, where k_{B} is *Boltzmann's constant* (in some sense the nexus between the micro- and macroscopic realms), and T is the absolute temperature of the environmental heat bath.

Our result can be seen as one episode in a series of results suggesting information-theoretic security to be, in principle, achievable under the assumption that *at least one in a list of physical theories*, such as quantum mechanics or special relativity, *is accurate*: We add to this list the second law of thermodynamics — to which not much glamour has been attached before.

2.1.2 Contributions

We base the "free-energy-bounded model" of information-theoretic cryptography upon the observation that the second law of thermodynamics has a cryptographically useful corollary: "Copying information has a fundamental cost in free energy." Bounding the free energy of an adversary forces them into picking parsimoniously what to copy, and that can be exploited in a reversible-computing context to ensure information-theoretic security. Our secret-key establishment protocol demonstrates how bounds in free energy can lead to cryptographic mechanisms similar to the ones used in quantum-key distribution and in the bounded-storage model, while our oblivious-transfer protocol exemplifies the novelty of our model.

[1] Free energy is "free" in the sense that it can be used to do work — it is not "entrapped" in a system.

This is an overview of our article: In Section 2.2, we review the subjects of information-theoretic cryptography and of reversible computing. In Section 2.3, we introduce, based on reversible computing, a novel model of computation and interaction that captures the consumption and the production of free energy in Turing machines. In Section 2.4, we establish some prerequisites: we prove a version of Landauer's principle in our framework, and construct a game that is basically equivalent to a thermodynamical "almost-no-cloning theorem," which we later use in our security proofs. In Sections 2.5 and 2.6, we offer protocols for *secret-key establishment* and *oblivious transfer*, respectively; their information-theoretical security is based fundamentally on Landauer's principle. It is assured against adversaries whose bound in free energy is exponential compared to the one of the honest players. While the present work focuses on classical information, we sketch in Section 2.7 how all our results generalize in presence of quantum adversaries.

2.2 State of the Art

2.2.1 Information-theoretic cryptography from physical assumptions

In parallel to the development of computationally secure cryptography — and somewhat in its shadow —, attempts were made to obtain in a provable fashion stronger, *information-theoretic security*, based not on the hardness of obtaining the (uniquely determined) message in question, but on the sheer lack of information. Hereby, the need for somehow "circumventing" Shannon's pessimistic theorem of perfect secrecy is met by some sort of *physical limitation*. The latter can come in the form of simple noise in a communication channel, a limitation on accessible memory, the uncertainty principle of quantum theory, or the non-signalling postulate of special relativity.

The first system of the kind, radically improving on the perfectly secret yet impractical *one-time pad*, has been *Aaron Wyner*'s wiretap channel [Wyn75]: Here, information-theoretic secret-key establishment becomes possible — under the assumption, however, that the legitimate parties already start with an advantage, more specifically, that the adversary only has access to a non-trivially degraded version of the recipient's pieces of information. A *broadcast scenario* was proposed by *Csiszár* and *Körner* [CK78] — where, again, an initial advantage in terms of information proximity or information quality was required by the legitimate partners *versus* the opponent. A breakthrough was marked by the work

of *Maurer* [Mau93], who showed that the need for such an initial advantage on the information level can be replaced by *interactivity* of communication: Maurer, in addition, conceptually simplified and generalized the model by separating the noisily correlated data generation from public yet authenticated communication, the latter being considered to be for free. The model shares its communication setting with both *public-key* as well as *quantum cryptography*. Maurer and Wolf [MW96] have shown that in the case of independent-channel access to a binary source, key agreement is in fact possible in principle in *all* non-trivial cases, *i.e.*, even when Eve starts with a massive initial advantage in information quality.

In the same model, it has also been shown that *multiparty computation* becomes possible, namely *bit commitment* and (the universal primitive of) *oblivious transfer* [CK88; Cré97]. More generally, oblivious transfer has also been achieved from *unfair* noisy channels, where the error behaviour is prone to be influenced in one way or another by the involved, distrusting parties willing to coöperate.

The *public-randomizer model* by Maurer [Mau92] has generally been recognized as the birth of the idea of "memory-bounded models," based on the fact that the *memory* an opponent or cheater (depending on the context) can access is limited. Specifically, Maurer assumes the wire-tapper can obtain a certain *fraction* of the physical bits. This was generalized to arbitrary *types* of information by *Dziembowski* and Maurer [DM02]. Analogously, also *oblivious transfer* has been shown achievable with a memory-bounded receiver [CCM98; DHRS04]. The main limitation to the memory-bounded model, for both secret-key establishment and multiparty computation, is that the memory advantage of the honest participants over the adversaries is at most quadratic [DM04].

The idea to use *quantum physics* for cryptographic ends dates back to *Wiesner*, who, for instance, proposed to use the uncertainty principle to realize unforgeable banknotes. His "conjugate coding" [Wie83] resembles oblivious transfer; the latter — even bit commitment, actually — we know now to be unachievable from quantum physics only [May97; LC98]. A breakthrough has been the now famous "BB84" protocol for key agreement by communication through a channel allowing for transmitting quantum bits, such as an optic fibre, plus a public yet authenticated classical channel [BB84].

A combination of the ideas described is the "bounded quantum-storage model" [DFSS08]: Whereas no quantum memory is needed at all for the honest players, a successful adversary can be shown to need more than $n/2$ of the communicated quantum bits. The framework has been unified and generalized to the "noisy"

model by *König*, *Wehner*, and *Wullschleger* [KWW12].

Very influential has been a proof-of-principle result by *Barrett, Hardy, and Kent* [BHK05]: The security in key agreement that stems from witnessing quantum correlations can be established regardless of the validity of quantum theory, only from the postulate of special relativity that there is *no superluminal signalling*. The authors combined *Ekert*'s [Eke91] idea to obtain secrecy from proximity to a pure state, guaranteed by *close-to-maximal violation of a "Bell inequality,"* with the role this same "nonlocality" plays in the argument that the outcomes of quantum measurements are, in fact, random and not predetermined: In the end, reasoning results that are totally *independent* of the completeness of quantum theory. Later, efficient realizations of the paradigm were presented [HRW; MPA11]. Conceptually, an interesting resulting statement is that information-theoretic key agreement is possible if *either quantum mechanics OR relativity theory* are complete and accurate "descriptions of nature." Another point of interest is that trust in the manufacturer is not even required: "device independence" [VV14].

Kent also demonstrated that bit commitment can be information-theoretically secure thanks to special relativity alone [Ken99]. On the other hand, oblivious transfer cannot be information-theoretically secure even when combining (without further assumptions) the laws of quantum mechanics and special relativity [Col07].

Now — the free-energy-bounded model:

We add to this list the novel *free-energy-bounded model*. Unlike the assumptions in memory-bounded models, thermodynamics does not in principle prohibit free-energy-bounded players from computing on memories of exponential size (in some security parameter), but it *does* prohibit those players from *erasing* a significant portion of such memories. If the players only have access to memories in *initial states of maximal entropy*, as is assumed in equilibrium in thermodynamics, the erasing restriction becomes a *copying* restriction (because one cannot copy without a blank memory to write the copy onto) and opens the way to a novel foundation of physics-based information-theoretic security that is different from the bounded-storage model.[2]

[2]In particular, the free-energy-bounded model offers fresh mechanisms, coming from reversible computing, to build information-theoretic protocols (e.g., our oblivious-transfer protocol). Another important difference is that in our protocols, the advantage of honesty in free-energy consumption is exponential in the security parameter, while in the bounded-storage model

2.2.2 Reversible computing

The cost of computation.

Security in cryptography relies on a cost discrepancy between honest and malicious actors. While fundamental thermodynamical limits to the cost of computation have been well-studied (for example, see [FDOR15] for a quantum-informational analysis and [BW19] for an algorithmic-information-theoretical analysis), they have never before[3] been considered as a means for cryptography — we address that.

The second law of thermodynamics.

The modern view of the second law of thermodynamics is due to *Ludwig Boltzmann*, who defined *the entropy of a macrostate* — roughly speaking, the natural logarithm of the number of microstates in the macrostate in question — and stated that the entropy of a closed system does not decrease with time. The second law has constantly been subject to discourse, confusion, and dispute; its most serious challenge was "*Maxwell's demon*" who apparently violates the law by adaptive acts, *i.e.*, by a sorting procedure. *Charles Bennett* [Ben87] explained that Maxwell's paradox actually disappears when the demon's internal state (its "brain") is taken into consideration. More specifically, *the erasure* of the stored information requires free energy that is then dissipated as heat to the environment. This is *Landauer's principle* [Lan61]; it did not only help to resolve the confusion around Maxwell's demon, but turned out to be an important manifestation of the second law with respect to information processing in its own right: Erasure of information — or, more generally, any logically irreversible computing step, has a thermodynamic cost. *Logical* irreversibility (information is lost) implies *thermodynamic* irreversibility (free energy is "burnt" to heat up the environment).

Landauer's principle.

Erasing n random bits requires to transform at least $n \cdot k_B T \ln 2$ J/K of free energy into heat, which is dissipated into the environment.

(which is not based on reversible computing but arguably more practical), it is polynomial.

[3] Let us mention the (questionable) conjecture in [HS03] that the heat-flow equation of thermodynamics is a computational one-way function.

Energy-neutral (thermodynamically reversible) computation.

Landauer's principle serves as a strong motivation to ask for the possibility whether computing can always be (made) *reversible*, *i.e.*, forced to not "forget" along the way any information about the past (previous computation). More specifically, can every Turing-computable function also be computed by a reversible Turing machine (the latter was introduced in [**?**]; see Chapter 5 of [**?**] for a more modern account)? In the early 1970s, *Charles Bennett* answered this question to the affirmative; the running time is also at most doubled, essentially — a very encouraging result [Ben73]: The imperative reversibility of microphysics can, at least in principle, be carried over to macrocomputing. Bennett's idea was that the reversible Turing machine would allocate part of its tape to maintain a history of its computation. While the latter needs to be gotten rid of in order to have the whole be "sustainable," that cannot be done by "crude" erasure of that history — all won would be lost again. It can, however, be done by *un-computing*: After copying the output, the reversible Turing machine reverts step by step the original computation, undoing its history tape in a "controlled" and reversible way until the output is computed back to the input. An idea similar to Bennett's elegant trick also works for circuits: Any irreversible circuit can be transformed into a reversible one, computing the same function, and having essentially only double depth.

All in all, this means that logical reversibility — which Landauer tells us to be a *necessary* condition for thermodynamic reversibility — can be achieved; remains the question whether it is also a *sufficient* condition for energy-neutral computation. The answer is *yes*, as exemplified by *Fredkin and Toffoli* [FT82] and their *Gedankenexperiment* of a "ballistic computer" which carries out its computations through elastic collisions between balls and balls, and balls and walls.

In the end, we get an optimistic picture for the future of computing: *Any computable function can be computed also without the transformation of free energy into heating of the environment*. (Clearly, a "loan" of free energy is necessary to start the computation, but no law of physics prevents its complete retrieval, alongside the result of the computation, when the latter concludes.)

Reversible computing.

Any logically reversible computation can be done at zero free-energy cost by a reversible Turing machine.

Reversible computing is at the core of our model.[4]

The energy value of redundancy.

The converse of Landauer's principle states that all physical representations of the all-0 string have work value. More generally, all redundant (i.e., compressible in a lossless fashion) strings have work value, which is essentially their length minus their best compression [Ben82]. A bound in free energy is therefore a bound on the redundancy of information; a principle we use in this work to construct cryptographic protocols.

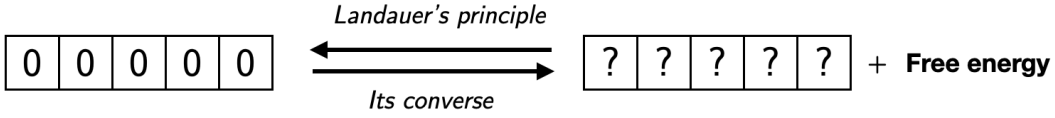


Figure 2.1. Given the existence of thermodynamical heat baths, there is a fundamental equivalence between free energy and redundancy (i.e., the absence of randomness).

The converse of Landauer's principle.

It is possible to extract an amount $n \cdot k_B T \ln 2$ of free energy from an environment by randomizing n blank bits.

In the light of Landauer's principle and of its converse, the all-0 string can be used as a proxy for free-energy (see Fig. 2.1). This allows us to abstract the thermodynamics completely from the model we present in Section 2.3, which is then formulated purely in terms of (logically reversible) Turing machines.

[4]Reversible computing is of paramount importance in the context of Moore's and Koomey's laws about the future of computation, because their continuation is threatened by physical walls and the most important one comes from thermodynamics (and not quantum mechanics). Reversible computing can in principle solve the problem completely by enabling computation without dissipation of heat.

2.3 Turing Machines with Polynomial Free-Energy Constraints

In the following, we have this classical[5] setting in mind: Alice, Bob, and Eve have their own secure labs, where they can store and manipulate exponentially long (in some security parameter ν) bit strings. Those strings start in uniformly random[6] states; we can think of them as the information about the specific microstate that describes the position and momentum of an exponential number of particles floating in their labs. We assume that technology is advanced enough to consider these exponentially long bit strings as static (even if the system starts in a random state, it does not get re-randomized at every time step), either because their evolution is tractable (it evolves according to the logically reversible laws of physics) or because the players can act on them quickly enough that it does not matter. The physical restriction on the honest and malicious players concerns their available free energy: For some security parameter ν, malicious players are bounded exponentially (more precisely, by 2^ν), while honest players need only an asymptotically $\mathcal{O}(\nu)$ amount. These bounds are constraining because any computation that is not logically reversible has a free-energy cost; a malicious agent cannot for example erase a $2 \cdot 2^\nu$-long segment of random information — by Landauer's principle, doing so would cost a quantity of free energy exceeding their free-energy bound. We formalize this computation model in Section 2.3.1.

Communicationwise, the players are allowed to broadcast $\mathcal{O}(\nu)$-length bit strings in the traditional sense using a public authenticated channel, or to transfer $\mathcal{O}(2^\nu)$-long bit strings through a private-but-insecure[7] SWAP channel, This channel, which swaps two bit strings at no energy cost, can also be substituted by an insecure *physical* channel. Both views are informationally equivalent, and are defined in Section 2.3.2.

In particular, our model differs from the bounded-storage model — both the players and the adversary have more power.

2.3.1 Computation model

The fundamental laws of physics are logically reversible. We hence base our formal notion of player (or adversary) on reversible Turing machines.

[5] The classical setting is used for all sections but Section 2.7, which approaches the quantum generalization.

[6] This randomness is motivated by the equipartition assumption of classical thermodynamics.

[7] By "insecure," we mean here that it is vulnerable to Eve-in-the-middle attacks.

Definition 6 (TTM)**.** *A* thermodynamical Turing machine *(TTM) is a logically reversible, deterministic, universal, prefix-free Turing machine with the following semi-infinite tapes:*

1 An input-only **instruction** tape.

2 An initially blank **computation** tape that must be returned blank when the machine halts.

3 An initially random **memory** tape.

4 An initially blank **free-energy** tape.

The **free-energy** tape of a TTM imitates a "reservoir" of free energy:

Definition 7 (consumption)**.** *The* free-energy input w_{in} *is quantified*[8]*, when the machine halts, by the distance, on the initially blank* ***free-energy*** *tape, between the extremity and the last cell with a* 1 *(after this cell, the tape contains only 0s).*

For example, if a machine always manages to return the **free-energy** tape as blank as it was — it uses no free energy and computes both logically and thermodynamically reversibly; if a machine writes, and leaves, some information on the first n cells of the initially blank **free-energy** tape, we say it *consumes* an amount $w_{\text{in}} = n$ of free-energy. (In this work we have set $k_{\text{B}}\text{T}\ln 2 := 1$.)

Our security proofs will rely on a concept we name **proof-of-work**.

Definition 8 (production)**.** *We say a TTM produces a* **proof-of-work** *of value* w_{out} *if it halts with a number* w_{out} *of* 0*s at the beginning of its (initially random)* ***memory*** *tape.*

We consider agents (TTMs) with bounds, in the security parameter ν, on the free-energy input.

Definition 9 (**BFE**)**.** *An* $f(\nu)$-**BFE** *agent — an agent who is* bounded in free energy by the function $f(\nu)$*, where* ν *is a security parameter — is modelled by a TTM that can only consume a quantity* $f(\nu)$ *of free energy.*

In other words, every time a $f(\nu)$-**BFE** agent reaches a halting state, the non-blank portion of its **free-energy** tape ends at a distance at most $f(\nu)$ from the extremity, by definition.

In our protocols, the honest players are asymptotically $\mathcal{O}(\nu)$-**BFE**, while the adversary is assumed exactly 2^{ν}-**BFE**. An important limitation of $f(\nu)$-**BFE** agents

[8] More precisely, it is bounded from below.

is given by the following theorem, to which the security of our protocols will be reduced.

Theorem 10. *For all $k > 0$, an $f(v)$-***BFE** *player cannot produce an $f(v) + k$ **proof-of-work**, except with probability 2^{-k}.*

The theorem is a consequence of the logical-reversibility characteristic imposed by the second law of thermodynamics. The proof is done in Section 2.4.2, based on Definitions 6 and 9 (*i.e.*, with no further references to thermodynamics).

2.3.2 Communication and reversible transfer

Our cryptographic model can be formalized further by integrating **BFE** parties into a multi-round interactive protocol that uses reversible computing. Let us, however, focus on how Alice and Bob can exchange information. There are of two distinct resources:

- Standard communication for messages of length $\mathcal{O}(v)$.
- Reversible transfer for longer messages, up to length $\mathcal{O}(2^v)$.

Standard communication.

We consider that Alice and Bob have access to a *public authenticated* communication channel in the traditional sense: Alice broadcasts a message (making, therefore, inevitably many copies of its information content) and Bob receives it. Because Alice and Bob are $\mathcal{O}(v)$-**BFE**, this information-duplicating channel can only be used for messages of length $\mathcal{O}(v)$.

Reversible transfer.

To send states of length more than $\mathcal{O}(v)$, Alice and Bob have to resort to reversible computing. Reversible transfer differs from standard communication in the sense that, in order to implement the process at no free energy cost, the sender *must forget* the information content of the message they send. (They could, of course, preëmptively make a partial copy of that information, but copying is not free and is thus limited by the free energy assumption.) There are two different physical ways to picture such reversible transfer.

The first way is to implement, over a given distance, a reversible SWAP: In essence, this operation simply swaps two bit strings of equal length in a logically and thermodynamically reversible way — Alice gets Bob's string and Bob gets

Alice's string. Since we are only interested in the string that Alice (the sender) sends, Bob (the receiver) can input junk in exchange. The SWAP allows $\mathcal{O}(\nu)$-**BFE** players to transfer between themselves $\mathcal{O}(2^\nu)$ bits of information (without copying them).

The second way to implement reversible communication is to simply consider that Alice is sending the whole physical system encoding her string (*e.g.*, she puts a canister of gas with entropy 2^ν on a frictionless cart and pushes it toward Bob). For the cart as for the SWAP channel, since the information is never copied, it can be transferred from Alice to Bob at no thermodynamical cost. This is not dissimilar to how it is in practice cheaper to send hard drives directly by mail rather than to send their content through a cable.

These two pictures (the SWAP channel and the physical channel) are from an information point of view equivalent — we adopt the SWAP channel for this work.

2.4 Technical Preliminaries

We introduce some notation and introduce some of the techniques used later in the security proof of our main protocols.

2.4.1 Smooth min-entropy

Most of our formal propositions rely on the *variational distance*.

Definition 11. *The* variational distance *between two random variables X and Y is defined as*

$$\delta(X,Y) := \frac{1}{2}\sum_{i\in\mathcal{X}\cup\mathcal{Y}} |p(X=i)-p(Y=i)| \,. \tag{2.1}$$

It is operationally very useful because it characterizes the impossibility to distinguish between X and Y — using any physical experiment whatsoever. More precisely, given either X or Y with probability $1/2$, the optimal probability to correctly guess which one it is is $(1+\delta(X,Y))/2$.

Definition 12. *The* conditional min-entropy $H_\infty(X|Y)$ *is defined as*

$$H_\infty(X|Y) := -\log \sum_y P(Y=y)\max_x P(X=x|Y=y)\,. \tag{2.2}$$

It is the optimal probability of correctly guessing X given side information Y.

Smoothing entropies [RW04; RW05] is done to ignore events that are typically unlikely. We will typically use smoothing with a parameter $\epsilon = \mathbf{negl}(v)$. We denote by $\mathbf{negl}(v)$ the functions that are *negligible* in v, meaning asymptotically bounded from above by the inverse of every function that is polynomial in v.

Definition 13. *The* smooth conditional min-entropy $H^{\epsilon}_{\infty}(X|Y)$ *is defined as*

$$H^{\epsilon}_{\infty}(X|Y) := \max_{\omega\in\Omega \; s.t. \; P(\omega)\geq 1-\epsilon} \min_{y} \min_{x} (-\log P(X=x|Y=y,\omega)), \tag{2.3}$$

where Ω *is the set of all events.*

Smooth conditional min-entropy is used mainly for privacy amplification.

2.4.2 Proof of Theorem 10

We define and prove formally a version of Landauer's principle (Theorem 10), which is the claim in Section 2.3 that **BFE** players modelled as thermodynamical Turing machines cannot produce more free energy than they consume, except with exponentially vanishing probability. The theorem follows from the logical reversibility of a TTM — the existence of a thermodynamically free logically irreversible physical process would be a violation of the second law of thermodynamics. We introduce some algorithmic-information-theory notation along the way; a more exhaustive introduction is the excellent book by Li and Vitányi [LV$^+$08].

Theorem 14 (technical)**.** *Given infinite tapes* $\{x, y\}$*, a* $f(v)$-**BFE** *TTM* $U_p(x, y)$ *cannot produce a* $f(v) + k$ ***proof-of-work****, except with probability* 2^{-k}.

$\{p, x, y\}$ are, respectively, the representation of the **instruction**, **memory**, and (blank) **free-energy** tapes, at the beginning of the computation.

We start with the simpler case of assuming that all of these tapes are finite (but arbitrarily long), and then generalize our analysis to the infinite case.

The finite case.

Let $U_p(x, y)$ be a thermodynamical Turing machine as described in Definition 6: universal, prefix-free, deterministic and logically reversible. The program p is taken from the read-only **instruction** tape (which can be taken long but finite); the (initially random) **memory** tape starts in $x \in_R \{0,1\}^{\mathbf{len}(x)}$, with $\mathbf{len}(x)$ taken arbitrary but finite; the **free-energy tape** starts with blank content $y = 0^{\mathbf{len}(y)}$, where $\mathbf{len}(y)$ is also finite.

The logical-reversibility condition means $U_p(x,y) = U_p(x',y')$ if and only if $(x,y) = (x',y')$.

We use a counting argument. We consider the set S of all couples (x,y) of lengths fixed. There are $\#S = 2^{\mathbf{len}(x)}$ of them and they are all equally probable. We then consider the subset

$$S(w_{\text{in}}, w_{\text{out}}) \coloneqq \left\{ x,y \text{ s.t. } U_p(x,y) = \tilde{x},\tilde{y} \text{ with } \begin{cases} \tilde{x} = 0^{w_{\text{out}}} || * \\ \tilde{y} = * || \, 0^{\mathbf{len}(y)-w_{\text{in}}} \end{cases} \right\}, \quad (2.4)$$

where $*$ is an arbitrary padding string of appropriate length, and $||$ denotes a concatenation. Intuitively, w_{in} bounds the free-energy input and is the minimum number of bits that get randomized on the initially blank **free-energy** tape y; w_{out} bounds the free-energy output and is the maximum number of erased bits on the initially random **memory** tape x. (Those erased bits constitute the **proof-of-work**.)

Lemma 15.

$$\#S(w_{\text{in}}, w_{\text{out}}) \leq 2^{\mathbf{len}(x)-w_{\text{out}}+w_{\text{in}}}. \quad (2.5)$$

Proof. Because of logical reversibility, the input-couples $(x,y) \in S$ are at most[9] as numerous as the output-couples $(\tilde{x},\tilde{y})$ s.t. $\begin{cases} \tilde{x} = 0^{w_{\text{out}}} || * \\ \tilde{y} = * || \, 0^{\mathbf{len}(y)-w_{\text{in}}} \end{cases}$. We count the maximum number of such output-couples by summing the lengths of all "$*$ positions"; there are at most $2^{(\mathbf{len}(x)-w_{\text{out}})+w_{\text{in}}}$ of them. □

The probability of drawing at random such a couple (x,y) is therefore

$$P(x,y \in S(w_{\text{in}}, w_{\text{out}})) \leq \#S(w_{\text{in}}, w_{\text{out}})/\#S = 2^{w_{\text{in}}-w_{\text{out}}}. \quad (2.6)$$

Proposition 16. *Given finite* $\mathbf{len}(x)$ *and* $\mathbf{len}(y)$*, a* $f(v)$*-***BFE** *TTM* $U_p(x,y)$ *(therefore with free-energy input* $w_{\text{in}} = f(v)$*) is limited in its production of free energy* w_{out} *by*

$$\forall k > 0,\ P(w_{\text{out}} > w_{\text{in}} + k) \leq 2^{-k}. \quad (2.7)$$

[9] "At most" because not all programs halt and some output-couples might not be in the image of U_p.

The infinite case.

We now reduce the infinite case to the finite case that we just analyzed.

We take again a TTM. Let us consider $x \in_R \{0,1\}^\infty$, where each bit is perfectly random. Let us also set $y = 0^\infty$. Since p is fixed, it is enough to again consider it finite. The prefix-free condition implies that the behaviour of $U_p(x,y)$ is well defined even on infinite tapes because its programs[10] are self-delimited.

Definition 17. *Let*

$$\Omega_{U_p} := \sum_{\text{effective}(x) \text{ s.t. } U_p(x,y) \text{ halts}} 2^{-\textbf{len}(\text{effective}(x))} \tag{2.8}$$

be the halting probability *of* U_p *(*i.e*, Chaitin's constant [Cha75]), where the sum is over all self-delimited programs* $\text{effective}(x) \in \{0,1\}^*$ [11].

We also define its partial sum.

Definition 18.

$$\Omega_{U_p}(n) := \sum_{\text{effective}(x) \text{ s.t. } U_p(x,y) \text{ halts and } \textbf{len}(\text{effective}(x)) \leq n} 2^{-\textbf{len}(\text{effective}(x))}. \tag{2.9}$$

Note first that since $\Omega_{U_p}(n)$ is a monotonically increasing function that converges to Ω_{U_p}, it holds that

$$\forall \epsilon > 0, \exists N' \text{ s.t. } \Omega_{U_p} - \Omega_{U_p}(N') < \epsilon\,. \tag{2.10}$$

Definition 19. *Let* $\text{BB}_{U_p}(n)$ *be the* time-busy-beaver function*, which returns the maximum running time that a halting program* $\text{effective}(x)$ *of length* $\leq n$ *can take before halting.*

Observe that it implies that, for all halting programs of length $\leq n$, the infinite part of each tape that comes after the $(\text{BB}_{U_p}(n))^{\text{th}}$ bit is never read or modified by the TTM (moving there is by definition too long).

Proposition 20. *A TTM with infinite tapes* (x,y) *behaves with arbitrarily high probability exactly as if these infinite tapes were (extremely long but) finite:*
$\forall \epsilon > 0$*,* $\exists N$ *such that*

$$P\left(U_p(x,y) = \left(U_p(x_{[\leq N]}, y_{[\leq N]}) \;||\; (x_{[>N]}, y_{[>N]})\right)\right) \geq 1 - \epsilon\,, \tag{2.11}$$

where the subset notation is used to split $x = x_{[\leq N]} || x_{[>N]}$ *and* $y = y_{[\leq N]} || y_{[>N]}$.

[10] "Program" is taken here in the general sense and includes arguments p and x.

[11] We assume p to be fixed; by "program" we mean the random input x.

Proof. Taking Eq. 2.10 with $N := \mathrm{BB}_{U_p}(N')$, with the consideration about busy beaver above (any machine that halts affects only a finite amount of tape). □

Finally, Theorem 14 is obtained by combining Proposition 16 and Proposition 20, with $\epsilon \to 0$:

$$\forall k > 0,\, P\left(w_{\text{out}} > f(\nu) + k\right) \leq 2^{-k}, \tag{2.12}$$

where w_{out} is the value of the **proof-of-work**.

2.4.3 The exhaustive and sampled memory games

We detail here in a game format a reduction that we later use in our security proofs. Our memory games involve an adversary against a verifier. The adversary sends, using a reversible channel SWAP, an exponentially long string to the verifier, but is also asked to try to keep a copy of it; the verifier then interrogates the adversary about either all of that string (in the *exhaustive* variant), or about a random linear-size subset of it (in the *sampled* variant); we show that the adversary has limited advantage in guessing as compared to a trivial strategy, unless they made an accurate copy of the whole string of exponential length — a process that requires, in light of Landauer's principle, an exponential amount of either luck or free energy. We formalize this intuition, starting with the non-sampled version of the game.

Definition 21. *The* exhaustive $\binom{k\cdot 2^\nu}{k\cdot 2^\nu}$ memory game *is defined as follows for security parameters ν and k:*

1 The adversary isolates (by taking it from the environment of their lab for example) a system $X \in \mathscr{X} = \{0,1\}^{k\cdot 2^\nu}$. All the rest of their available information is modelled as E.

2 The adversary (modelled as a TTM) makes some computation on the systems X, E.

3 Through a noiseless reversible channel (*e.g.*, SWAP), the adversary sends X to the verifier.

4 The verifier provides the adversary a blank tape of length $k \cdot 2^\nu$, and asks the adversary to correctly print on it all of X.

Proposition 22. *For any 2^ν-***BFE** *adversary, the advantage at the exhaustive $\binom{k\cdot 2^\nu}{k\cdot 2^\nu}$ memory game, compared to a trivial coin-flip strategy, is bounded by*

$$H_\infty(X|E) \geq (k-1)2^\nu. \tag{2.13}$$

Proof. We reduce a violation of Theorem 1 (*i.e.*, Landauer's principle) to a large advantage at the exhaustive $\binom{k\cdot 2^v}{k\cdot 2^v}$ memory game. During the game, instead of sending X to the verifier, the adversary deviates and XORs onto X their best guess for X given side information E. If the adversary guesses correctly, it turns X into an all-0 string. This **proof-of-work** of length $k\cdot 2^v$ violates Theorem 1 if it is created with probability higher than $2^{-(k-1)2^v}$; therefore, it does not. □

The constraint also holds if the adversary is quizzed only on a random subset of positions.

Definition 23. *The* sampled $\binom{k\cdot 2^v}{t}$ memory game *is defined as follows for free-energy bound 2^v, security parameter k, and sample size t:*

1 The adversary isolates (by taking it from the environment of their lab for example) a system $X \in \mathscr{X} = \{0,1\}^{k\cdot 2^v}$. All the rest of their available information is modelled as E.

2 The adversary (modelled as a TTM) makes some computation on the systems X, E.

3 Through a noiseless reversible channel (*e.g.*, SWAP), the adversary sends X to the verifier.

4 The verifier chooses at random t *sample* positions $\subset \mathscr{X}$ and sends a description of these positions to the adversary, who must correctly guess $X_{[sample]}$.

Theorem 24. *For any 2^v-***BFE** *adversary, the advantage at the sampled $\binom{k\cdot 2^v}{t}$ memory game, compared to a trivial coin-flip strategy, is bounded, for all $\delta > 0$, by*

$$H_\infty^{\mathbf{negl}(t)}(X_{[sample]}|E) \geq \frac{t\cdot(k-1)}{k} - t\cdot\delta\,. \tag{2.14}$$

Proof. Lemma 6.2 in [Vad04] states that, under random sampling, the min-entropy per bit is with high probability approximately conserved. In our case, this implies that, for all $\delta > 0$,

$$H_\infty^{2^{-\Omega(t\delta^2\log^2\delta)}+2^{-\Omega(k2^v\delta)}}(X_{[sample]}|E) \geq \frac{t}{k\cdot 2^v} H_\infty(X|E) - t\cdot\delta\,, \tag{2.15}$$

given which Theorem 24 follows from Proposition 22. □

2.4.4 Universal hashing

Universal hashing is useful for both privacy amplification and authentication.

Definition 25 (2-universal hashing [CW79; WC81])**.** *Let $\mathscr{H}$ be a set of hash functions from $\{0,1\}^n \to \{0,1\}^m$. $\mathscr{H}$ is* 2-universal *if, given any distinct elements $x_1, x_2 \in \{0,1\}^n$ and any (not necessarily distinct) elements $y_1, y_2 \in \{0,1\}^m$, then*

$$\#\{h \in \mathscr{H} | y_1 = h(x_1) \wedge y_2 = h(x_2)\} = \#\mathscr{H}/2^{2m}\,. \tag{2.16}$$

Lemma 26 (Leftover hash lemma [BBR88; ILL89; HILL93; BBCM95])**.** *Let $h : \mathscr{S} \otimes \mathscr{X} \to \{0,1\}^m$ be a 2-universal hash function. If $H_\infty(X) \geq m + 2\epsilon$, then*

$$\delta\Big((h(S,X),S), U \otimes S\Big) \leq 2^{-\epsilon}\,. \tag{2.17}$$

S is a short uniformly random seed and X is the variable whose randomness is to be amplified. U is the uniform distribution of appropriate dimension. The symbol $\otimes$ is used to represent the joint probability of independent distributions.

2.5 Secret-Key Establishment

Secret-key establishment (SKE) is a fundamental primitive for two-way secure communication because it allows for a perfectly secure one-time-pad encryption between Alice and Bob about which Eve knows nothing (otherwise the protocol aborts).

2.5.1 Definitions (SKE)

Definition 27. *A secret-key-establishment scheme is* sound *if, at the end the protocol, Alice and Bob possess the same key with overwhelming probability in the security parameter η:*

$$P(K_A \neq K_B) \leq \mathbf{negl}(\eta)\,. \tag{2.18}$$

Definition 28. *A secret-key-establishment scheme is information-theoretically* secure *(*i.e.*, almost perfectly secret) if the key K_B is uniformly random even given all of the adversary's side information E, except with probability at most negligible in the security parameter ν:*

$$\delta\Big((K_B, E), U \otimes E\Big) \leq \mathbf{negl}(\nu)\,. \tag{2.19}$$

In what follows, the variables $(A,B) \in (\mathscr{A}, \mathscr{B})$ are strings from registers of length roughly $\mathscr{O}(\nu \log \nu)$, while $(X,Y) \in (\mathscr{X}, \mathscr{Y})$ denote strings from registers of length $\mathscr{O}(2^\nu)$.

2.5.2 Protocol (SKE)

Theorem 29. *The following secret-key-establishment protocol is information-theoretically sound and secure against any eavesdropper whose free energy is bounded by 2^ν. Alice and Bob need a quantity of free energy that is asymptotically $\mathcal{O}(\nu)$.*

Soundness is analyzed in Section 2.5.3, and security in Section 2.5.4.

Secret-key-establishment protocol:

1 Alice starts [a] with $X \in \mathcal{X} = \{0,1\}^{k\cdot 2^\nu}$ in a uniformly random state (extracted from the equidistributed environment of her lab). She draws uniformly at random a subset $\subset \{1,\dots,k\cdot 2^\nu\}$ of $s+t$ positions *rawkey* and copies $(rawkey, X_{[rawkey]}) \to A$ to her memory.
2 Alice sends $X \to Y$ to Bob using a reversible channel (*e.g.*, a SWAP channel); it is possibly intercepted by Eve.
3 Bob announces the receipt to Alice on an authenticated public channel. In case of no receipt, they abort.
4 Alice publishes the subset positions *rawkey* on the (noiseless) authenticated public channel so that Bob can select $Y_{[rawkey]} \to B$. Alice and Bob draw a *test* sub-subset of t bits that they sacrifice to estimate the error rate p_{error} between A and B.
5 If the estimated p_{error} is too large, they abort. Otherwise, Alice and Bob apply information reconciliation (detailed in Section 2.5.3) on the remaining s bits $A_{[\overline{test}]}$ and $B_{[\overline{test}]}$.
6 Alice and Bob apply privacy amplification (detailed in Section 2.5.4) and obtain a shared secret key of length $\approx ((k-1)/k - h_b(p_{\text{error}}))\cdot s$.

[a] The main parameters are
- ν, from the 2^ν bound in free energy of Eve;
- k, which determines the tolerated error rate between Alice and Bob;
- t, the number of test bits to estimate the above error rate;
- s, the length of the raw key (before processing).

$h_b(p) \coloneqq -p\log_2 p - (1-p)\log_2(1-p)$ is the *binary entropy*.

Note that for any fixed p_{error} (as long as it is not trivially $1/2$), Alice and Bob can choose a security parameter k for which the protocol will be secure for that value of p_{error}. That is unlike, for example, the BB84 quantum-key-distribution protocol, which only tolerates error rates less than $1/4$ (any more and Eve can intercept the whole quantum state).

The intuition.

Because she is 2^ν-bounded in free energy, Eve cannot copy to her memory the whole $k \cdot 2^\nu$-long string Y that she sends to Bob, on which Bob will later base the raw key. Alice circumvents this limitation by already knowing the raw-key positions at the moment she sends X (X becomes, after Eve's potential tampering, Y) and thus need not store more than an asymptotically $\mathcal{O}(\nu)$-long segment of the $k \cdot 2^\nu$-long string. As in quantum key distribution, Eve can force the protocol to abort.

2.5.3 Soundness analysis (SKE)

Parameter estimation.

We first estimate (using upper bounds) between Alice and Bob the global error rate p_{error} and the non-tested *rawkey* error rate $p_{\text{error}}^{\overline{test}}$. The former quantity is important for the privacy amplification analyzed in Section 2.5.4, while the second is needed to analyze information reconciliation.

Proposition 30. *Alice and Bob can accurately estimate the error rate p_{error} by sampling on the t test positions the error rate p_{error}^{test}:*

$$P\left(p_{\text{error}} \leq p_{\text{error}}^{test} + \epsilon\right) \geq 1 - e^{-2\epsilon^2 t}. \tag{2.20}$$

Proof. p_{error}^{test} is computed from the Hamming weight $\omega(\overline{A_{[test]} \oplus B_{[test]}}) = t(1 - p_{\text{error}}^{test})$. Chernoff's inequality bounds p_{error}. □

Proposition 31. *Alice and Bob can accurately estimate $p_{\text{error}}^{\overline{test}}$ from p_{error}^{test}:*

$$P\left(p_{\text{error}}^{\overline{test}} \leq p_{\text{error}}^{test} + \frac{s \cdot \epsilon}{s+t}\right) \geq 1 - e^{-2\epsilon^2 t}. \tag{2.21}$$

Proof. We insert $p_{\text{error}} = (s \cdot p_{\text{error}}^{\overline{test}} + t \cdot p_{\text{error}}^{test})/(s+t)$ in Eq. 2.20 and isolate $p_{\text{error}}^{\overline{test}}$. □

Information reconciliation (error correction).

Once they have a good estimate of $p_{\text{error}}^{\overline{test}}$, Alice and Bob achieve information reconciliation by applying error correction on that unused subset $\overline{test}$ of s bits.

Note that it is important that the established key be based on Bob's string, rather than on Alice's, because the reasoning (see the security analysis in Section 2.5.4) using the sampled memory game only directly bounds from above the mutual information between Bob and Eve, not the one between Alice and Eve.

Proposition 32. *For any non-trivial constant $p_{\text{error}}^{\overline{test}} \neq 1/2$, Alice and Bob can transform the samples $A_{[\overline{test}]}, B_{[\overline{test}]}$ into the (non-necessarily secret) keys K'_A, K'_B for which*

$$P\left(K'_A = K'_B\right) \geq 1 - \mathbf{negl}(\eta)\,. \tag{2.22}$$

They can do so with $w \approx h_b(p_{\text{error}}^{\overline{test}}) \cdot s$ (the exact value is given below) bits of authenticated public communication.

We present one standard construction to correct an arbitrary error rate on the s bits of *rawkey* that were not used during the parameter-estimation phase.

Asymptotically optimal protocol for information reconciliation [BS93]:

Let $w := \lceil s \cdot h_b(p_{\text{error}}^{\overline{test}} + \delta') + \eta \rceil$;

1 Bob picks at random a hash function $h : \{0,1\}^s \to \{0,1\}^w$ from a 2-universal family $\mathscr{H}$ and computes $h(B_{[\overline{test}]})$.

2 Bob communicates h and $h(B_{[\overline{test}]})$ to Alice, using the authenticated public channel.

3 Alice computes $\tilde{A}_{[\overline{test}]} := \underset{x \in \{0,1\}^{\mathbf{len}(s)}}{\operatorname{argmin}} \left(\omega(x, A_{[\overline{test}]}) | h(x) = h(B_{[\overline{test}]})\right)$.

Here, $\omega(\cdot,\cdot)$ is the Hamming distance; δ' determines efficiency and η is the security parameter.

Proof. We first count, in the uniform distribution, the smooth number of strings with length s that contains approximately $p_{\text{error}}^{\overline{test}}$: Let $M := \{x \in \{0,1\}^s \mid p_{\text{error}}^{\overline{test}} - \delta' \leq p_{\text{error}}^{\overline{test}}(x) \leq p_{\text{error}}^{\overline{test}} + \delta'\}$; from the asymptotic equipartition property, we have $\forall \delta' > 0$,

$$P\left(\#M \leq 2^{s \cdot h_b(p_{\text{error}}^{\overline{test}} + \delta')}\right) \geq 1 - 2^{-\Theta(\eta)}\,. \tag{2.23}$$

Because $\mathscr{H}$ is 2-universal, the probability of obtaining a correct hash from a non-correct candidate in M is bounded by 2^{-w}. By the union bound, the protocol is therefore sound except with probability at most $2^{-w} \cdot \#M$, which is $\mathbf{negl}(\eta)$. □

While the above ideal information reconciliation protocol is optimal, it offers no (known) efficient way (in the computational complexity sense) for Alice to decode Bob's codeword. While we are in this work only concerned with thermodynamic (rather than computational) efficiency, we refer to [BS93], or to the theory of Shannon-optimal efficient algebraic codes, such as convoluted codes, for asymptotically ideal information-reconciliation protocols that are also computationally efficient.

2.5.4 Security analysis (SKE)

If the protocol does not abort, Eve has negligible information about the key K_B at the end. This security resides on the fact that even if Eve intercepts X (which was sent from Alice to Bob) and replaces it with Y, she cannot keep roughly more than a fraction $1/k$ of the information about Y. Thus, since the key is based on Y, Eve has limited knowledge about it.

Formally, this can be analyzed with the sampled $\binom{k\cdot 2^{\nu}}{s}$ memory game in Section 2.4.3. Theorem 24 thereat guarantees a good starting point — Eve (who is 2^{ν}-**BFE**) must have limited information about Bob's raw key of length s:

$$\forall \delta > 0,\ H_{\infty}^{\mathbf{negl}(\nu)+\mathbf{negl}(s)}(Y_{\overline{[test]}} | E, rawkey, \overline{test}) = s \cdot \frac{k-1}{k} - s \cdot \delta\,. \tag{2.24}$$

The next step is to go from *low* information to *essentially no* information.

Privacy amplification.

Privacy amplification turns a long string about which the adversary has potentially some knowledge into a shorter one about which the adversary has essentially none.

In secret-key establishment, Eve's partial information can come from eavesdropping (and as shown, this quantity is roughly a fraction $1/k$) or from the public information leaked by the information reconciliation protocol, which is easily characterized.

Privacy amplification can be realized in an information-theoretically secure manner with 2-universal hashing (see Section 2.4.4).

Proposition 33. *After privacy amplification, K_B is approximately of length $\approx ((k-1)/k - h_b(p_{\text{error}})) \cdot s$, and Eve has essentially no knowledge about it.*

Proof. Let w quantify the number of bits about $B_{\overline{[test]}}$ exchanged publicly during the information-reconciliation (IR) protocol. We note that $H_{\infty}(K_B|E^{\text{preIR}}) \leq H_{\infty}(K_B|E^{\text{postIR}}) - w$, hence

$$\forall \delta > 0,\ H_{\infty}^{\mathbf{negl}(\nu)+\mathbf{negl}(s)}(K_B | E^{\text{postIR}}) = s \cdot \frac{k-1}{k} - s \cdot \delta - w\,. \tag{2.25}$$

Therefore, taking $m \coloneqq s \cdot \frac{k-1}{k} - s \cdot \delta - w - \epsilon$ guarantees after hashing (ϵ is the security parameter for the Leftover hash lemma; see Section 2.4.4) information-theoretic security on those remaining m bits. □

Note that for any fixed p_{error}, the parameters s and k can be selected as to make m a positive quantity when the protocol does not abort (as a result of too many errors). Also note that the parameters ν and s must not be too small.

2.6 1-out-of-2 Oblivious Transfer

Oblivious transfer (OT) is a cryptographic primitive that is universal for two-party computation [Rab81; Kil88]. It comes in many flavours, but they are all equivalent [Cré87]. We concern ourselves with 1-out-of-2 OT (or 1–2 OT). Informally: Alice sends two envelopes to Bob; Bob can open one to read the message in it, but he cannot open both; Alice cannot know which message Bob read. To have simple formal security definitions, we, however, concern ourselves with a variant of 1–2 OT where the choices are made uniformly at random by Alice and Bob.

2.6.1 Definitions (OT)

Definition 34. *A 1–2 OT protocol is perfectly* sound *if, when Alice and Bob are honest, the message $B(i)$ received by Bob is with certainty the message m_i sent by Alice, for a uniform choice of $i \in_R \{0,1\}$:*

$$P\left(B(i) = m_i\right) = 1\,. \tag{2.26}$$

Definition 35. *A 1–2 OT protocol is information-theoretically* secure-for-Alice *if Bob cannot learn something non-negligible about both of Alice's messages simultaneously: For any 2^ν-**BFE** Bob, $\exists$ random variable $j \in \{0,1\}$ such that*

$$\delta\Big((m_j, E_B), (U \otimes E_B)\Big) \leq \mathbf{negl}(\eta)\,. \tag{2.27}$$

E_B denotes all of (a potentially malicious) Bob's side information. And similarly for E_A in regards to Alice.

Definition 36. *A 1–2 OT protocol is information-theoretically* secure-for-Bob *if Alice cannot learn anything non-negligible about Bob's random choice $i \in_r \{0,1\}$: For any 2^ν-**BFE** Alice,*

$$\delta\Big((i, E_A), U \otimes E_A\Big) \leq \mathbf{negl}(\eta)\,. \tag{2.28}$$

An OT protocol is information-theoretically secure when it is information-theoretically secure for *both* Alice and Bob.

2.6.2 Protocol (OT)

Theorem 37. *The following 1–2 OT protocol is perfectly sound and information-theoretically secure against 2^{ν}-**BFE** adversaries. The free-energy requirement of the honest players is asymptotically $\mathcal{O}(\nu)$.*

The perfect soundness is straightforward. Security is analyzed in Section 2.6.3.

1–2 oblivious-transfer protocol:

(The variable η is a security parameter.)

1 Alice chooses random messages m_0 and m_1 of length n.
2 Alice starts with the exponentially long bit strings $X^{(0)}, X^{(1)} \in \mathscr{X} = \{0,1\}^{4\cdot 2^{\nu}}$ in uniformly random states. She picks a random subset $\subset \{1,\ldots,4\cdot 2^{\nu}\}$ of $n+\eta$ positions *raw* and stores $(raw, X^{(0)}_{[raw]}, X^{(1)}_{[raw]})$ in her memory.
3 Alice sends $(X^{(0)}, X^{(1)})$ to Bob using the reversible channel SWAP.
4 Bob chooses $i \in_R \{0,1\}$ and computes reversibly $(X^{(0)}, X^{(1)}) \to (X^{(i)}, X^{(0\oplus 1)})$, where we define $X^{(0\oplus 1)} := X^{(0)} \oplus X^{(1)}$. Then, Bob keeps $X^{(i)}$ and sends back $X^{(0\oplus 1)}$ reversibly to Alice using SWAP.
5 Alice receives $\tilde{X}^{(0\oplus 1)}$ and checks whether $\tilde{X}^{(0\oplus 1)}_{[raw]} = X^{(0\oplus 1)}_{[raw]}$. If they differ, Alice aborts.
6 Alice chooses at random a 2-universal hash function $h : \{0,1\}^{n+\eta} \to \{0,1\}^n$ and communicates $h, raw, m_0 \oplus h(X^{(0)}_{[raw]}), m_1 \oplus h(X^{(1)}_{[raw]})$ to Bob.
7 Bob computes the hash $h(X^{(i)}_{[raw]})$ and recovers m_i.

The intuition.

In addition to the previously exploited *impossibility to copy* exponential quantities of information without using corresponding quantities of free energy or violating Landauer's principle, the oblivious-transfer protocol makes use of another key feature of *reversible computing*: As long as Bob is in possession of $X^{(0\oplus 1)} := X^{(0)} \oplus X^{(1)}$, the maximally random variables $X^{(0)}$ and $X^{(1)}$ have conditionally exactly the *same* information content; but once $X^{(0\oplus 1)}$ is returned to Alice, $X^{(0)}$ and $X^{(1)}$ revert to being *uncorrelated*. In other words, although sending $X^{(0\oplus 1)}$ back to Alice forces Bob to *forget* information about the couple $X^{(0)}, X^{(1)}$ (enabling 1-out-of-2 transfer), it does not uniquely specify *which* information he forgot (Alice remains oblivious).

2.6.3 Security analysis (OT)

Security for Bob.

From Alice's point of view, Bob's behaviour (*i.e.*, sending $X^{(0\oplus1)}$ back to Alice) is identical whether he chooses message $i{=}0$ or message $i{=}1$; the scheme is therefore perfectly secure for Bob.

Security for Alice.

We prove that a malicious Bob cannot learn anything non-negligible about a second message as soon as he learns something non-negligible about a first message.

Proof. We pose without a loss of generality that ω is the event corresponding to "Bob learns something non-negligible about m_0." Because he is 2^ν-bounded in free energy, a malicious Bob's success at the sampled $\binom{4\cdot2^\nu}{n+\eta}$ memory game (on state $\tilde{X}^{(0\oplus1)}$ and sample *raw*) is bounded by Theorem 24:

$$\forall\delta>0,\ H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(\tilde{X}^{(0\oplus1)}_{[raw]}|E_B,\omega)\geq(n+\eta)/2-(n+\eta)\cdot\delta\,. \tag{2.29}$$

By subadditivity, we have

$$\begin{aligned}
&H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(\tilde{X}^{(0\oplus1)}_{[raw]}|E_B,\omega) && (2.30)\\
&\leq H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(X^{(0)}_{[raw]},X^{(1)}_{[raw]}|E_B,\omega) && (2.31)\\
&\leq H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(X^{(0)}_{[raw]}|E_B,\omega)+H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(X^{(1)}_{[raw]}|E_B,\omega)\,. && (2.32)
\end{aligned}$$

We apply the Leftover hash lemma (Lemma 26) with $\epsilon:=\eta/12-3n/8$. The two privacy-amplification steps succeed (except by the union bound with probability $\mathbf{negl}(\nu)+\mathbf{negl}(\eta)$) if, respectively,

$$\begin{aligned}
H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(X^{(0)}_{[raw]}|E_B,\omega)&\geq n/4+\eta/6\,, && (2.33)\\
H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(X^{(1)}_{[raw]}|E_B,\omega)&\geq n/4+\eta/6\,. && (2.34)
\end{aligned}$$

We assume by contradiction that they are both unsuccessful with non-negligible probability. It implies

$$H_\infty^{\mathbf{negl}(\nu)+\mathbf{negl}(\eta)}(\tilde{X}^{(0\oplus1)}_{[raw]}|E_B,\omega)<n/2+\eta/3\,, \tag{2.35}$$

which contradicts Eq. 2.29 for small $\delta\leq\eta/(6(n+\eta))$. □

2.7 From classical adversaries to quantum adversaries

Up to here, the notion of information that has been used — in the protocols for secret-key establishment and oblivious transfer, as well as in their analyses — is purely *classical*. But as scrutinised by thorough experiments (notably, the extensive serie of Bell experiments [FC72; ADR82; HBD+15; GVW+15; SMSC+15]), nature is *quantum-physical*. The aim of this section is to bring our work one step closer to the quantum realm. Namely, we investigate whether our (classical[12]) protocols are secure against quantum adversaries. We find that our SKE protocol (Section 2.5.2) is secure against a quantum Eve *as it is*. On the other hand, to retain security against a malicious quantum Alice, our OT protocol (Section 2.6.2) has to be slightly updated — the patched protocol presented below in Section 2.7.4 is quantum-safe but remains classical for honest players. Our work's conclusion, therefore, fully extends to the *quantum* world of Maxwell demons (given arbitrarily large but random environments): It is — on paper — information-theoretically cryptographically friendly.

2.7.1 The setting made quantum

Our model described in Section 2.3 is based on Alice, Bob, and Eve being classical computers with thermodynamical restrictions (we call them Thermodynamical Turing Machines) interacting through classical channels (a standard authenticated channel and a SWAP channel).

In a quantum setting, Alice, Bob, and Eve are upgraded to universal quantum computers [Deu85] and their communication channels can carry states in quantum superposition. A quantum computer cannot compute more than a classical computer could (given exponential computational time, a classical computer can simulate a quantum computer). Quantum computing cannot either be used to evade Landauer's principle [FDOR15]. As such, once all elements are properly defined, a quantum version of our Theorem 10 holds.

Proposition 38 (Thm. 10 in the quantum realm (sketch))**.** *For all $k > 0$, a player modelled by a quantum computer with a bound $f(v)$ in free energy cannot erase more than $f(v) + k$ initially completely mixed qubits, except with probability 2^{-k}.*

The ability to send and receive quantum states does enable new possibilities for both honest and malicious agents — we investigate next how this affects the

[12] All classical operations can be viewed as quantum operations restricted to diagonal density matrices.

security of our previous SKE and OT protocols.

2.7.2 The quantum exhaustive and sampled memory games

We extend the proof method developed in Section 2.4.3 to the quantum world.

First, the bound on the success of an adversary at the exhaustive $\binom{k\cdot 2^\nu}{k\cdot 2^\nu}$ memory game (Proposition 22) is unaffected by the transition from classical to quantum information.

Proposition 39 (Prop. 22 with quantum side-information)**.** *For any quantum adversary with a bound 2^ν in free energy, the advantage at the exhaustive $\binom{k\cdot 2^\nu}{k\cdot 2^\nu}$ memory game, compared to a trivial coin-flip strategy, is bounded by*

$$H_\infty(X|E) \geq (k-1)2^\nu . \tag{2.36}$$

Proof. X is here still classical, but E represents side information that is possibly quantum. Since the operational meaning of conditional min-entropy is the same whether the side information is quantum or not [KRS09], the argument presented in Section 2.4.3 is unchanged. □

The next step is to sample from X (Theorem 24).

Proposition 40 (Thm. 24 with quantum side-information)**.** *For any quantum adversary with a bound 2^ν in free energy, the advantage at the sampled $\binom{k\cdot 2^\nu}{t}$ memory game, compared to a trivial coin-flip strategy, is bounded, for all $\delta > 0$, by*

$$H_\infty^{\mathbf{negl}(t)}(X_{[sample]}|E) \geq \frac{t\cdot(k-1)}{k} - t\cdot\delta . \tag{2.37}$$

Proof. The result by Vadhan [Vad04] that we used in the classical case has been generalized in presence of quantum side information by König and Renner in [KR11]. Apart from the exact parameter values hidden behind $\mathbf{negl}(t)$, our proof is, hence, unchanged by the addition of quantum side information. □

2.7.3 The classical SKE protocol is already quantum-resistant

The information-theoretical security of the SKE protocol from Section 2.5 depends uniquely on the one of privacy amplification and on Theorem 24.

Since in presence of quantum side information, universal-2 hashing (Lemma 26) remains a universally composably secure way of achieving privacy amplification [RK05; TSSR11], and that, as we just argued, so is the case of Theorem 24, the SKE scheme presented in Section 2.5.2 is secure against quantum adversaries.

Fundamentally different from standard quantum key distribution, the result is nevertheless an information-theoretically secure key distribution scheme for a quantum world in which entropy is exponentially cheaper than free energy.

2.7.4 A quantum-resistance patch for the OT protocol

Given that the above SKE protocol is quantum-resistant, and that the same argument applies to the security-for-Alice part of our oblivious-transfer protocol, it would be natural for our previously detailed scheme to be also quantum-resistant. But it is not: The security-for-Bob, which is trivial in the classical case (because $x+y = y+x$, see Fig. 2.2), can be broken by a malicious quantum Alice. The reason is that if Alice acts maliciously and sends the superposed quantum states $X^{(0)} = H|x\rangle$ and $Y^{(0)} = |y\rangle$ to Bob (for some random x and y), she can discriminate between the state sent back by Bob when he does $H|x\rangle \xrightarrow{\text{CNOT}} |y\rangle$ (to keep $X^{(0)}$) compared to when he does $|y\rangle \xrightarrow{\text{CNOT}} H|x\rangle$ (to keep $Y^{(0)}$). This attack is illustrated in Fig. 2.3.

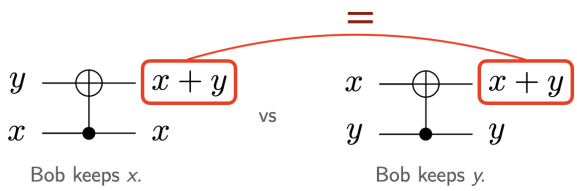


Figure 2.2. If Bob receives a classical state, the top state, $x + y$, that he will return to Alice during the OT protocol will be the same no matter whether he chooses to decrypt the first (left) or second message (right).

But there is a simple patch for this attack, or, in fact, for all quantum attacks by a malicious Alice. Alice's extra power comes from the fact she can send states in superposition, but Bob can in return preëmptively "classicize" the possibly quantum states $X^{(0)}$ and $X^{(1)}$ by CNOT-ing each bit to a different bit of the totally mixed environments π_0 and π_1. Given control of a large enough environment (of dimension $2^{\mathbf{len}(X^{(0)})+\mathbf{len}(X^{(1)})}$), Bob can do so at no free energy cost. The resulting state, when traced over that environment, is then undistinguishable from a (possibly noisy) state sent by a malicious-but-classical Alice. Even if misbehaviour

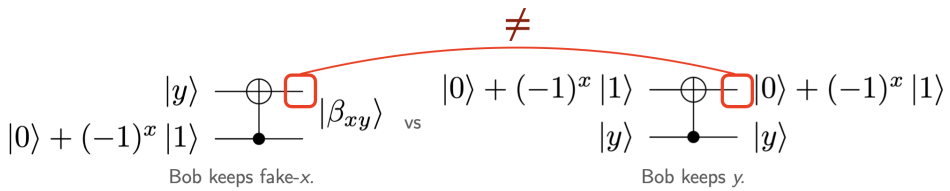


Figure 2.3. A malicious Alice can send to Bob one of the quantum states in the Hadamard basis. In that case, the upper state sent back to Alice by an honest Bob will be $|+\rangle$ or $|-\rangle$ if he wants to keep the first message, but half of one of the four Bell states $\{|\beta_{xy}\rangle\}_{xy}$ if he wants to keep the second message. Since Alice can distinguish between those two cases, the OT scheme is not secure for Bob. Below, we explain how Bob can prevent this quantum attack.

from Alice's part might affect the protocol's correctness (which is allowed for a malicious Alice), it leaves the perfect security intact: a quantum Alice can still not gain any information about Bob's choice.

Quantum-safe 1–2 oblivious-transfer protocol

Steps 1–3 and 5–7 are the same as in the previous classical protocol. Step 4 is changed to

4'. Bob chooses $i \in \{0,1\}$ and computes reversibly

$$(X^{(0)}, X^{(1)}, \pi_0, \pi_1) \to (X^{(i)}, X^{(0\oplus 1)}, \pi_0 \oplus X^{(1)}, \pi_1 \oplus X^{(2)}),$$

where π_0 and π_1 are completely mixed states of appropriate size taken from Bob's environment, and where we define $X^{(0\oplus 1)} := X^{(0)} \oplus X^{(1)}$. Then, Bob keeps everything but $X^{(0\oplus 1)}$, which he sends back (thermodynamically reversibly) to Alice using SWAP.

The above step reduces the security for Bob in the quantum case to the one of the classical case. The updated protocol does not require the honest players to make any quantum operations *per se*.

2.8 Concluding remarks

We propose a *free-energy-bounded* model of cryptography, in which we have derived information-theoretically secure protocols for secret-key establishment and oblivious transfer.

Even if the rationale behind its security is totally different: Our secret-key-establishment protocol is similar to standard quantum key distribution. Our oblivious-transfer protocol, on the other hand, is novel in itself: The mechanism that allows Alice to check that Bob honestly forgets information is proper to reversible computing.

Our schemes are not practical at this point: Current technology is still far from computing with memories that are large enough for Landauer's principle to become the main obstacle (it is worth noting that Boltzmann's constant, which we have in this work conveniently set to $k_B := 1/T$, is in fact $\approx 1.38 \cdot 10^{-23} JK^{-1}$); and whereas no laws of physics forbid it, implementing reversible computation on such states is for now science fiction. Our result is rather to be seen as part of the quest of distinguishing what physical phenomena allow for realizing cryptographic functionalities in principle, and which do not. In this spirit, our protocols add another element to the longer and longer list of physical laws from which cryptographic security *can* directly be derived: We can now claim that information-theoretic key agreement is theoretically possible as soon as one of the fundamental limits conjectured by *either* quantum theory *or* special relativity *or the second law of thermodynamics* is correct. Concerning the novel appearance of a thermodynamic law in this list, we remark first that according to *Albert Einstein*, thermodynamics is the only physical theory that will survive future development in Physics. Second, the second law is rather pessimistic in nature, and to see it being linked to a constructive application is refreshing. We are, in fact, not aware of many uses, besides our protocols, of the law. In summary, we can say, somewhat ironically: *One small step for cryptography — one giant leap for the second law.*

Epilogue

Bell's theorem is a profound result. Similarly to how Gödel's incompleteness theorem affected the field of mathematics and ended the programme of making mathematics mechanistic, the violation of Bell inequalities revealed[13] the emptiness of the reductionist programme of explaining physics, and by extension, all of science, through hidden variables. It launched the quest towards new information models, highlighting the importance of scientific creativity. It is fascinating that we pose and solve problems today, whose sense, not so long ago, was completely obfuscated, or simply did not even exist.

Yet, after almost 90 years of progress, quantum nonlocality is still frequently misunderstood. From the outset, even the name itself stems from a misconception — nonlocality can arise from local–realist processes, as explained by the parallel-lives model ([BRR13]). With irony, we could blame the second law of thermodynamics: when scientific knowledge piles up, without purposeful intervention, it grows more chaotic. In today's academia, this work, of simplification, of capturing of the essence, of tracing out the superfluous and the contingent, is undervalued. It is in that context my honour to have worked with Claude Crépeau on the RGB no-signalling game — to have contributed in illustrating quantum nonlocality in a pedagogical way. The analysis in the prologue is equivalent in its conclusion to Bell's theorem and to Tsirelson's bound. I believe the game should be taught alongside the CHSH game, in most introductory classes to quantum computing.

One lesson from the violation of Bell inequalities (such as exhibited in the RGB game) is that it is hard to make predictions about future scientific theories. Physicists of the early-19th century could only see local hidden variables (ironically), they missed the richness of quantum information. Will we find, one day, correlations that are even more "nonlocal" than quantum entanglement? What will the

[13] Although I know some would disagree.

successor of quantum mechanics look like? The first question is an unfalsifiable statement; and the second calls for a prophecy. Yet formidably, we can tangibly approach *the spirit* of such interrogations, with post-Gödelian answers such as "If maximally nonlocal bipartite correlations were to exist, they would make communication complexity trivial ([VD13])", or, in our case, the experimental-metaphysics conclusion "If the predictions of quantum mechanics are correct (but possibly incomplete), there are no bounds to the multipartite character of nonlocality — any future causal theory needs to include N-partite nonlocal resources, for any N (Chapter 1)."

An interesting research direction, to close the "Correlations" part of this thesis, is to compare the concept of genuinely multipartite entanglement (GME) and the one of genuinely multipartite nonlocality (GMNL). Are all pure GME states GMNL? (It would be a counterpart to Gisin's theorem.) Can we find a GME mixed state that is not GMNL? (Some entangled mixed states do not violate any Bell inequalities.)

In Chapter 2, I approached cryptography. One central (anti-)dogma in cryptography, or in security in general, is that a system can never be simply said to *be* secure. It is always secure *in regard to some model* of adversary. The quest for unconditional security seems ill founded; even the one-time pad, which is the perfect encryption method, is insecure against Prof. X as he can read one's mind (Prof. Xavier is a fictional character in the X-Men franchise).

This has not prevented the fruitful growth of the field of information-theoretic cryptography, it merely oriented it towards finding the minimal sets of assumptions guaranteeing security. The strongest links in such sets are arguably the ones based on fundamental laws of physics, because their violation would imply a total re-imagination of our physical world. As such, quantum cryptography, and, more recently, device-independent cryptography and relativistic cryptography, offer strong promises of concrete security, even in a post-quantum world where quantum technologies are ubiquitous.

But the study of cryptography as a discipline of physics goes beyond the making of commercial cryptographic devices — the cryptography developed in Chapter 2 is certainly technologically unthinkable today — it has more as endeavour the goal of unveiling the "principles of cryptography." One of those principles is that cryptography thrives in the presence of constraints: Cryptography is impossible under conditions of available-to-all, perfect information. A celebrated example is quantum cryptography, born from the impossibility of cloning unknown quantum states. Chapter 2 is a new illustration of the intimate link between the abstract

notion of security and the physical notion of information, and also it offers a no-cloning theorem, or rather an effective "almost-no-cloning" theorem, from which the pessimism of the second law of thermodynamics can be, in principle, overthrown. A little sarcastically, we could call the concept introduced in Chapter 2 *pre-heat-death cryptography*.

In the inverse direction (in quantum mechanics, information always flows in both ways, because of phase kickback), studying the security of physics-based models is interesting for it turns cryptography into a lens for physics. Since details matter in cryptography — one modification can make or break a scheme — cryptography offers an angle to contrast the details and implications of different physical assumptions. I hope that by taking Maxwell's demon seriously (going as far as to propose cryptography built from it), I contributed in expanding the universe of "Thermodemonics" and its promises of extending thermodynamics beyond equilibrium.

Interestingly, my oblivious-transfer protocol (Section 2.6) is secure through the use of a 1-out-of-2 proof of erasure based on Landauer's principle. Proofs of erasure in quantum mechanics ([CRW19]) cannot be done in that 1-out-of-2 way. The reason is that while the (large but classical) variables $\{X, Y, X \oplus Y\}$ are simultaneously all well defined in a thermodynamical model, the quantum information $\{X, Z, XZ\}$ is not, because of Heisenberg's uncertainty principle (but not because of quantum no-cloning, they are in this case two distinct concepts). There is also a nuance regarding Landauer's erasure principle that was left open in the cryptographic analysis of Chapter 2: What would be the implications of the existence of a hypothetical device that can store N bits but out of which only 1 bit can be retrieved, and whose erasure cost is $k_{\mathrm{B}}\mathrm{T}\ln 2$?

At last, this thesis analyzed different facets of information — in Chapter 1 its quantum-mechanical nature, and in Chapter 2 its thermodynamical nature — as well as their links with cryptography. This analysis featured different frameworks and it would be interesting to unify their core concepts under a common abstract framework such as constructor theory. A constructor theory of cryptography.

Appendix A

The RGB no-signalling game ([CRC19], full version)

The following is the complete retranscription of my work ([CRC19]) with Claude Crépeau.

Abstract. Introducing the simplest of all No-Signalling Games: the RGB Game where two verifiers interrogate two provers, Alice and Bob, far enough from each other that communication between them is too slow to be possible. Each prover may be independently queried one of three possible colours: Red, Green or Blue. Let a be the colour announced to Alice and b be announced to Bob. To win the game they must reply colours x (resp. y) such that $a \neq x \neq y \neq b$.

This work focuses on this new game mainly as a pedagogical tool for its simplicity but also because it triggered us to introduce a new set of definitions for reductions among multi-party probability distributions and related *non-locality classes*. We show that a particular winning strategy for the RGB Game is equivalent to the PR-Box of Popescu-Rohrlich and thus No-Signalling. Moreover, we use this example to define No-Signalling in a new useful way, as the intersection of two natural classes of multi-party probability distributions called one-way signalling. We exhibit a quantum strategy able to beat the classical local maximum winning probability of 8/9 shifting it up to 11/12. Optimality of this quantum strategy is demonstrated using the standard tool of semidefinite programming.

A.1 The Game

Claude started this research trying to find the simplest example he could think of to illustrate multi-party distributions achievable via entanglement and No-Signalling in general. His interest started from the following question on Quora: "Could someone explain quantum entanglement to me like I'm 5 years old?" Jon Hudson [Hud18], a former Stanford QM student, had given an answer involving friends choosing to have pizza (or not) on the Moon and on Earth but he did not quite come up with a crisp No-Signalling situation. Claude cooked up the RGB example after reading Jon's answer.

The canonical examples in this area are the Magic Square Game [Mer90; Per90] and the so-called PR-box [PR94] of Popescu-Rohrlich, both of which require some basic notions of arithmetics to be introduced, or at least some basic logic as a common background. The purpose now is to present an example so simple that even a five year old would understand it!

The RGB game is as follows:

> " Two people, Alice and Bob, play a game with friends Albert and Boris. Alice and Albert are on the moon, while Bob and Boris stay on earth. Albert and Boris each independently picks at random a colour out of three possibilities: Red, Green or Blue, and locally tells it to Alice or Bob.
>
> Right away Alice and Bob choose a colour different from the one provided by their local counterpart. For instance, if Albert tells Green to Alice, she may choose Red or Blue, while if Boris tells Red to Bob, he may choose Blue or Green.
>
> Alice and Bob win the game if they never answer the same colour, either Red-Blue, Red-Green or Blue-Green in the example above. "

Figure 1 summarizes the input/output relation that Alice and Bob must satisfy. a is the colour given to Alice and b is the colour given to Bob. Their answers are x and y respectively. The condition they are trying to achieve is simply $a \neq x \neq y \neq b$.

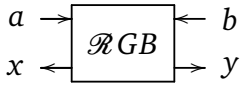


Figure A.1. The $\mathscr{R}GB$-box such that $a \neq x \neq y \neq b$

Such boxes are a standard way of representing the possible behaviours of Alice and Bob. Indeed we can think of this box as a channel precisely describing the distribution of x, y given fixed values of a, b. The box of Figure 1 does not specify the probabilities exactly and thus the name of the box is in calligraphic letters representing the set of all the distributions that satisfy the given conditions. There are many distinct ways of fulfilling the conditions of the game and many distributions that will win the game 100% of the time.

A.1.1 Winning Strategies

Let's first consider a deterministic strategy for Alice and Bob's behaviour as described by the box of Figure A.2.

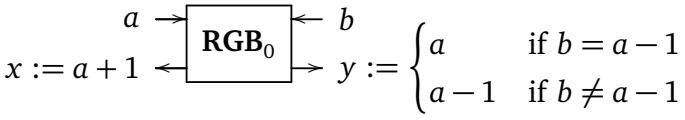


Figure A.2. A deterministic $\mathbf{RGB}_0$-box

In this example we assume the colours are labelled $0, 1$ or 2 and that arithmetic operations are performed modulo 3. When a and b are the same colour u it produces

$$a = u,\ x = u+1,\ y = u-1,\ b = u.$$

The values $u+1$ and $u-1$ are the other two colours, distinct from u. However, when a and b are the distinct colours u, v it produces either

$$a = u,\ x = u+1,\ y = u,\ b = v$$

when the third colour is $u+1 = v-1$ or

$$a = u,\ x = u+1,\ y = u-1,\ b = v$$

when the third colour is $u-1 = v+1$.

This deterministic strategy defines completely the probability distribution of the outputs x, y given a, b: $\Pr(x, y|a, b)$ is zero except when $x = a+1$ and $y = \begin{cases} a & \text{if } b = a-1 \\ a-1 & \text{if } b \neq a-1 \end{cases}$ in which case it is precisely one. Therefore we name this box $\mathbf{RGB}_0$ with bold characters because it precisely defines a unique probability distribution $P_{x,y|a,b}$. This box achieves the prescribed condition $a \neq x \neq y \neq b$ in a unique deterministic way for each a, b.

After complete examination of this condition one realizes that when $a = b$ is a single colour u the conditions can be satisfied in exactly two ways

$$a = u,\ x = u \pm 1,\ y = u \mp 1,\ b = u$$

whereas when a and b are distinct colours u, v the conditions can be satisfied in exactly three ways

$$a = u,\ x = v,\ y = u,\ b = v$$

$$a = u,\ x = u \pm 1,\ y = v \pm 1,\ b = v.$$

From this we conclude that out of the 9 possible a, b pairs, three of them ($a = b$) may have two solutions and six of them ($a \neq b$) may have three solutions. This yields a total of $2^3 3^6 = 18^3 = 5832$ distinct deterministic winning strategies. The above $\mathbf{RGB}_0$ strategy is only one of these.

We can completely parametrize all the winning strategies as a function of 15 real parameters $p_0, p_1, p_2, p_{01}, p_{02}, p_{10}, p_{12}, p_{20}, p_{21}, q_{01}, q_{02}, q_{10}, q_{12}, q_{20}, q_{21}$ in the interval $[0, 1]$ such that $p_{uv} + q_{uv} \leq 1$ as follows

$$P_{u+1,u-1|u,u} = p_u \text{ and } P_{u-1,u+1|u,u} = 1 - p_u, \text{ for } u \in \{0, 1, 2\} \tag{A.1}$$

$$P_{w,u|u,v} = p_{uv},\ P_{v,w|u,v} = q_{uv} \text{ and } P_{v,u|u,v} = 1 - p_{uv} - q_{uv}, \text{ for } \{u, v, w\} = \{0, 1, 2\}. \tag{A.2}$$

All the winning strategies to this game are among these probability distributions. They are all the valid convex combinations of the 5832 distinct deterministic winning strategies.

The deterministic strategy $\mathbf{RGB}_0$ of Figure A.2 is the special case

$$p_0 = p_1 = p_2 = p_{02} = p_{20} = q_{01} = q_{10} = q_{12} = q_{21} = 1$$

$$p_{01} = p_{10} = p_{12} = p_{21} = q_{02} = q_{20} = 0.$$

The rest of this paper is going to focus on exactly one of these strategies with a very remarkable property: it *does not require* Alice and Bob to signal to implement it (whereas all the others actually do). This strategy is going to be named $\mathbf{R}^{\mathbf{GR}}_{\mathbf{BG}}\mathbf{B}^1$ and is specified by the parameters

$$p_0 = p_1 = p_2 = p_{01} = p_{10} = p_{02} = p_{20} = p_{12} = p_{21} =$$

$$q_{01} = q_{10} = q_{02} = q_{20} = q_{12} = q_{21} = \frac{1}{2}.$$

Figure A.3. The $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$-box such that $a \neq x \neq y \neq b$, and $(x, y) \neq (b, a)$, uniformly among solutions

In Figure 3, $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$ is made precise by enforcing extra conditions on top of $a \neq x \neq y \neq b$. We force $P_{v,u|u,v} = 0$ by adding $(x, y) \neq (b, a)$. Uniformity finally imposes that all the remaining non-zero probabilities be exactly $\frac{1}{2}$.

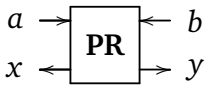


Figure A.4. The **PR**-box satisfying the CHSH condition, that $a \wedge b = x \oplus y$, uniformly among solutions

A.1.2 Our Results

The contributions of the paper are

1 Novel notion of reducibility among strategies

2 Novel definitions of basic notions such as locality, signalling, one-way signalling and no-signalling

3 A proof that our notion of no-signalling is equivalent to the generally accepted one

4 A proof of equivalence between $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$ and the well-known Popescu-Rohrlich Non-Local (yet No-Signalling) **PR**-box (see Figure 4). This Implies that $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$ is also complete for the set of No-Signalling (two-party) distributions

5 A proof that $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$ is the ONLY No-Signalling distribution winning the RGB game

6 A deterministic (and local) strategy with winning probability 8/9

7 A proof of optimality of this local strategy

8 Quantum strategy with winning probability 11/12

[1]The name is a reminder that this strategy has the feature that whenever a and b are distinct, $axyb$ is $abcb$ or $acab$ (c being the third colour) but never $abab$. $\mathbf{R}^{\mathbf{GR}}_{\overline{\mathbf{BG}}}\mathbf{B}$ is a combined string of types $a_{\overline{bc}}b$, $a^{\overline{ca}}b$.

9 A proof of optimality of this quantum strategy using semidefinite programming

10 Some related open problems

A.2 Definitions

In this section we solely focus on the two-party single-round games and strategies that are sufficient to discuss and analyze the strategies for the RGB game. Definitions and proofs for complete generalizations to multi-party multi-round games and strategies will appear in a forthcoming paper with co-authors Adel Magra and Nan Yang.

A.2.1 Strategies: Two-Party Channels

Games:

Let V be a predicate on $A \times B \times X \times Y$ (for some finite sets A, B, X, and Y) and let π be a probability distribution on $A \times B$. Then V and π define a (single-round) game G as follows: A pair of questions (a, b) is randomly chosen according to distribution π, and $a \in A$ is sent to Alice and $b \in B$ is sent to Bob. Alice must respond with an answer $x \in X$ and Bob with an answer $y \in Y$. Alice and Bob win if V evaluates to 1 on (a, b, x, y) and lose otherwise.

Strategies:

A strategy for Alice and Bob is simply a probability distribution $P_{(x,y|a,b)}$ describing exactly how they will answer (x, y) on every pair of questions (a, b). We now breakdown the set of all possible strategies for Alice and Bob according to their degree of *non-locality*.

Deterministic and Local Strategies:

A strategy $P_{(x,y|a,b)}$ is *deterministic* if there exists functions $f_A : A \to X, f_B : B \to Y$ such that

$$P_{(x,y|a,b)} = \begin{cases} 1 & \text{if } x = f_A(a) \text{ and } y = f_B(b) \\ 0 & \text{otherwise} \end{cases}.$$

A deterministic strategy corresponds to the situation where Alice and Bob agree on their individual actions before any knowledge of the values a, b is provided

to them. In this case they use only their own input to determine their individual output.

A strategy $P_{(x,y|a,b)}$ is *local* if there exists a finite set R, functions $f_A : A \times R \to X, f_B : B \times R \to Y$ and a probability distribution $\pi_r, r \in R$, such that

$$P_{(x,y|a,b)} = \sum_{r \in R : x = f_A(a,r) \text{ and } y = f_B(b,r)} \pi_r.$$

A local strategy corresponds to the situation where Alice and Bob agree on a deterministic strategy selected uniformly among $|R|$ such possibilities. The choice r of Alice and Bob's strategy, and the choice of inputs (a, b) provided to Alice and Bob are generally agreed to be statistically independent random variables.

A.2.2 Local Reducibility

We now turn to the notion of locally reducing a strategy to another, that is how Alice and Bob limited to local strategies but equipped with a particular (not necessarily local) strategy U' are able to achieve another particular (not necessarily local) strategy U. For this purpose we introduce a notion of distance between strategies in order to analyze strategies that are approaching each other asymptotically.

Several distances could be selected here as long as their meaning as it approaches zero are the same. In the definitions below, U, U' are strategies and $\mathscr{U}'$ is a finite set of strategies.

Definition 41. $|U, U'| = \sum_{a,b,x,y} |P_U(x, y|a, b) - P_{U'}(x, y|a, b)|$.

Definition 42. $|U, \mathscr{U}'| = \min_{U' \in \mathscr{U}'} |U, U'|$.

For natural integer n, we define the set $\mathrm{LOC}^n(U)$ of strategies that are local extensions (of order n) of U to be all the strategies Alice and Bob can achieve using local strategies where strategy U may be used up to n times as sub-routine calls[2].

Definition 43. *We say that U' Locally Reduces to U ($U' \leq_{\mathrm{LOC}} U$) iff* $\lim_{n \to \infty} |U', \mathrm{LOC}^n(U)| = 0$.

Definition 44. *We say that U' is Locally Equivalent to U ($U' =_{\mathrm{LOC}} U$) iff $U' \leq_{\mathrm{LOC}} U$ and $U \leq_{\mathrm{LOC}} U'$.*

[2]Done by selecting functions $f_A^0 : A \times R \to A$, $f_A^1 : A \times X \times R \to A, \ldots$, $f_A^{n-1} : A \times X^{n-1} \times R \to A$, $f_A^n : A \times X^n \times R \to X$ to determine the input of each sub-routine from input a and previous outputs.

Note: a similar notion of reducibility has been previously defined by Dupuis, Gisin, Hasidim, Méthot, and Pilpel [DGH+07] but without taking the limit to infinity. In their model they have previously showed that n instances of the PR-box modulo p cannot be used to replicate exactly the PR-box modulo q, for any distinct primes p, q. However, Forster and Wolf [FW11] have previously proved that **PR** is complete for No-Signalling distributions under a similar (asymptotic) definition.

A.2.3 Locality and Non-Locality

We now define the lowest of the non-locality classes $\mathbb{LOC}$. We could define it directly from the notion of local strategies as defined above, but for analogy with the other classes we later define, $\mathbb{LOC}$ is defined as all those strategies locally reducible to a *complete* strategy we call **ID** (see Figure A.5) for obvious reasons. Of course, any strategy is complete for this class.

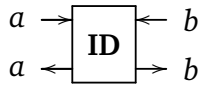


Figure A.5. The **ID**-box

Definition 45. $\mathbb{LOC} = \{U | U \leq_{\text{LOC}} \textbf{ID}\}$.

Note: $\mathbb{LOC}$ is the class of strategies that John Bell [Bel64] considered as classical hidden-variable theories and that he opposed to entanglement. It is also the class of strategies that BenOr, Goldwasser, Kilian and Wigderson [BOGKW19] chose to define classical Provers in Multi-Provers Interactive Proof Systems.

A.2.4 One-Way Signalling

We now turn to One-Way Signalling which allows communication from one side to the other. We name the directions arbitrarily Left and Right. We define **R**-$\mathbb{SIG}$ (resp. **L**-$\mathbb{SIG}$) as all those strategies locally reducible to a *complete* strategy we call **R-SIG** (see Figure A.6) (resp. **L-SIG** (see Figure A.7)). These classes are useful to define what it means for a strategy to *signal* as well as the notion of *No-Signalling* strategies.

Definition 46. **R**-$\mathbb{SIG} = \{U | U \leq_{\text{LOC}} \textbf{R-SIG}\}$.

Definition 47. *We say that U Right Signals (is* **R**-$\mathbb{SIG}$*-verbose*[3]*) iff* **R-SIG** $\leq_{\text{LOC}} U$.

Figure A.6. The **R-SIG**-box

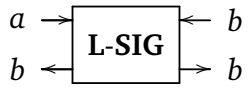


Figure A.7. The **L-SIG**-box

Definition 48. **L-**$\mathbb{SIG} = \{U | U \leq_{\text{LOC}} \textbf{L-SIG}\}$.

Definition 49. *We say that U Left Signals (is* **L-**$\mathbb{SIG}$*-verbose) iff* **L-SIG** $\leq_{\text{LOC}} U$.

Definition 50. *We say that U Signals iff U Right Signals or Left Signals.*

We prove a first result that is intuitively obvious. We show that the complete strategy **R-SIG** cannot be approximated in **L-**$\mathbb{SIG}$ and the other way around.

Theorem 51. **R-SIG** $\notin$ **L-**$\mathbb{SIG}$ *and* **L-SIG** $\notin$ **R-**$\mathbb{SIG}$.

Proof. Follows from a simple capacity argument. For all n, all the channels in LOC^n(**R-SIG**) have zero left-capacity, while **L-SIG** has non-zero left-capacity. And vice-versa. □

A.2.5 Signalling

We are now ready to define the largest of the non-locality classes named $\mathbb{SIG}$. Indeed every possible strategy is in $\mathbb{SIG}$.

Definition 52. $\mathbb{SIG} = \{U | U \leq_{\text{LOC}} \textbf{SIG}\}$.

Figure A.8. The **SIG**-box

Definition 53. *We say that U Fully Signals (is* $\mathbb{SIG}$*-verbose) iff U Right Signals and Left Signals.*

[3] We define the notion of $\mathbb{L}$-verbose in analogy to $\mathbb{NP}$-hard: it means "as verbose as any distribution in non-locality class $\mathbb{L}$". In consequence, a distribution U is $\mathbb{L}$-complete if $U \in \mathbb{L}$ and U is $\mathbb{L}$-verbose.

A.2.6 No-Signalling

We finally define the less intuitive non-locality class $\mathbb{NOSIG}$ in relation to classes defined above.

Definition 54. $\mathbb{NOSIG} = \mathbf{R}\text{-}\mathbb{SIG} \bigcap \mathbf{L}\text{-}\mathbb{SIG}$.

A similar characterization may be found in [AFLS15] Section 3 and [BFRW05] Corollary 3.5.

Theorem 55. *The above definition of* $\mathbb{NOSIG}$ *exactly coincides with the* traditional *notion of No-Signalling [BLM$^+$05a].*

Proof. If U is signalling then it is verbose for at least one of $\mathbf{R}\text{-}\mathbb{SIG}$ or $\mathbf{L}\text{-}\mathbb{SIG}$. Without loss of generality, assume it is verbose for $\mathbf{R}\text{-}\mathbb{SIG}$. Then by theorem 51, $U \notin \mathbf{L}\text{-}\mathbb{SIG}$, thus $U \notin \mathbf{R}\text{-}\mathbb{SIG} \bigcap \mathbf{L}\text{-}\mathbb{SIG}$.

If U is no-signalling then Alice's marginal distribution is independent from Bob's input b. Therefore, she can sample an output x according to her input a only as $P_{X|A=a}$ deduced from $P_{X,Y|A,B}$. Alice can now communicate a, x to Bob. Bob given a, b, x can select y according to the distribution $P_{Y|A=a,B=b,X=x}$ deduced from $P_{X,Y|A,B}$. The produced x, y will have distribution $P_{X,Y|A=a,B=b}$ as expected. This proves $U \in \mathbf{R}\text{-}\mathbb{SIG}$. Membership to $\mathbf{L}\text{-}\mathbb{SIG}$ is proven similarly. □

Figure A.9 shows the relation of these classes as well as the case obtained via quantum entanglement ($|\mathbb{LOC}\rangle$) as considered by Bell [Bel64] and via commuting-operators ($\mathbb{COMOP}$) as defined by Ito, Kobayashi, Preda, Sun, and Yao [IKP$^+$08].

Definition 56. *We say that U does not Signal iff U does not Right Signal nor Left Signal iff* $U \in \mathbb{NOSIG}$.

Theorem 57. *If* $U \in \mathbf{R}\text{-}\mathbb{SIG}$ *(or* $U \in \mathbf{L}\text{-}\mathbb{SIG}$*) and U is symmetric then U does not Signal.*

Proof. $U \in \mathbf{R}\text{-}\mathbb{SIG}$ and U is symmetric imply that $U \in \mathbf{L}\text{-}\mathbb{SIG}$ as well. Thus $U \in \mathbf{R}\text{-}\mathbb{SIG} \bigcap \mathbf{L}\text{-}\mathbb{SIG}$. □

Theorem 58. $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B} \in \mathbb{NOSIG}$.

Proof. $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B} \in \mathbf{R}\text{-}\mathbb{SIG}$ and $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$ is symmetric. □

Theorem 59. $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B} =_{\mathrm{LOC}} \mathbf{PR}$.

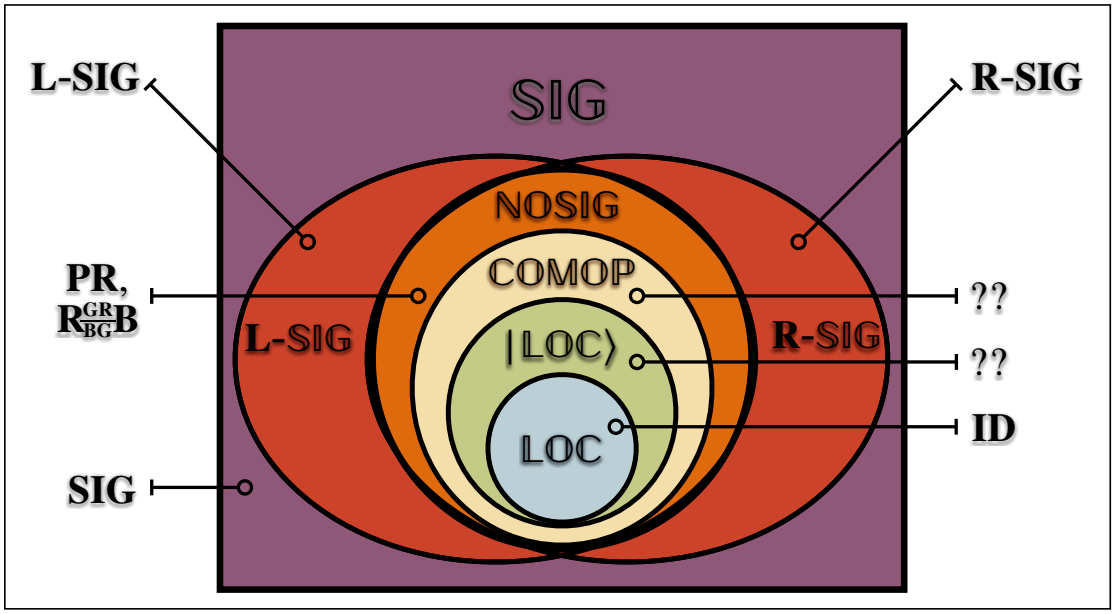


Figure A.9. Non-locality Hierarchy and complete (two-party) distributions in certain classes.

Proof. First we show how **PR** may be achieved from $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$, more precisely that $\mathbf{PR} \in \mathrm{LOC}^1(\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B})$. All arithmetic operations are performed modulo 3. Let $a' := f_A^1(a) := a$, and $b' := f_B^1(b) := 2b$. The possible pairs for (a', b') are therefore $(0,0),(0,2),(1,0),(1,2)$. Let $(x', y') \leftarrow \mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}(a', b')$. Let $x := f_A^2(a, x') := 2(x' - a + 1)$, and $y := f_B^2(b, y') := 2(y' - 2b + 1)$. We leave it as an exercice to check that (x, y) indeed satisfy the CHSH condition that $x \oplus y = a \wedge b$.

Secondly, we show how $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$ may be achieved from **PR**, more precisely that $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B} \in \mathrm{LOC}^2(\mathbf{PR})$. Again, all arithmetic operations are performed modulo 3[4]. The intuition in this case is that if $a = b$ then (x, y) should be either $(a+1, b-1)$ or $(a-1, b+1)$ at random. If $a \neq b$ then (x, y) should be either $(a+1, b+1)$ or $(a-1, b-1)$ at random. The following computations achieve precisely this using the identity $a = b$ iff $(\neg a' \oplus b') \wedge (\neg a'' \oplus b'')$, where a primed variable is the corresponding most significant bit and a double-primed variable is the corresponding the least significant bit.

The first pair of functions compute the negation of the most significant bit of their inputs: let $a' := f_A^1(a) := 1 - 2(a-1)a$, and $b' := f_B^1(b) := 1 - 2(b-1)b$. Let $(x', y') \leftarrow \mathbf{PR}(a', b')$.

[4]Therefore modulo 2 for the exponents according to Fermat's little theorem.

The second pair of functions compute the negation of the least significant bit of their inputs: let $a'' := f_A^2(a,x') := 1-2(a-1)(a+1)$, and $b'' := f_B^2(b,y') := 1-2(b-1)(b+1)$. Let $(x'',y'') \leftarrow \mathbf{PR}(a'',b'')$.

The third pair of functions compute $a \pm 1, b \pm 1$ according to the intuitive rule above: let $x := f_A^3(a,x',x'') := a + 2^{a_1 * a_2 + x' + x''}$, and $y := f_B^3(b,y',y'') := b + 2^{b_1 * b_2 + y' + y''}$. □

Corollary 59.1. $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$ *is* $\mathbb{NOSIG}$*-Complete.*

Proof. Since **PR** was previously proved $\mathbb{NOSIG}$-Complete by Forster and WolfÙ[FW11], then so is $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$. □

Theorem 60. $\mathbf{R}_{\mathbf{BG}}^{\mathbf{GR}}\mathbf{B}$ *is the ONLY strategy winning the RGB game that is also No-Signalling.*

Proof. Using the notation of Equations (A.1) – (A.2), for No-Signalling on Alice's side we need

$$P_{u+1,u-1|u,u} = p_u = P_{u+1,u-1|u,u+1} + P_{u+1,u|u,u+1} = 1 - p_{u\,u+1} = P_{u+1,u|u,u-1} = p_{u\,u-1}, 0 \le u \le 2$$

and symmetrically on Bob's side

$$P_{u-1,u+1|u,u} = 1 - p_u = P_{u-1,u+1|u+1,u} + P_{u,u+1|u+1,u} = 1 - q_{u+1\,u} = P_{u,u+1|u-1,u} = q_{u-1\,u}, 0 \le u \le 2.$$

Using all 6 sets of equalities we can get rid of all the variables but p_0, p_1, p_2 by setting

$$p_{u\,u-1} = q_{u+1\,u} = p_u \text{ and } p_{u\,u+1} = q_{u-1\,u} = 1 - p_u, 0 \le u \le 2.$$

It follows that

$$P_{u+1,u|u,u+1} = p_u + p_{u+1} - 1 = -P_{u,u+1|u+1,u}, 0 \le u \le 2$$

and since both $P_{u+1,u|u,u+1}$ and $P_{u,u+1|u+1,u}$ must be greater or equal to zero we conclude

$$P_{u+1,u|u,u+1} = P_{u,u+1|u+1,u} = 0 \text{ and } p_u = 1 - p_{u+1}, 0 \le u \le 2.$$

It results that $p_0 = 1 - p_1 = p_2 = 1 - p_0 = p_1 = 1 - p_2$ and thus

$$p_0 = p_1 = p_2 = p_{01} = p_{10} = p_{12} = p_{21} = p_{20} = p_{02} = q_{01} = q_{10} = q_{12} = q_{21} = q_{20} = q_{02} = 1/2$$

is the only solution as claimed. □

Theorem 61. *The maximum local winning probability $p^{\text{win}}_{\text{local}}$ to the RGB game is 8/9.*

Proof. Consider $f(R) = B$ and $f(G) = f(B) = R$ as well as $g(R) = g(B) = G$ and $g(G) = B$. By inspection of these functions we conclude $p^{\text{win}}_{\text{deterministic}} \geq 8/9$ because for all inputs a, b we have $f(a) \neq a$ and $g(b) \neq b$ and 8 out of 9 input pairs (a, b) are such that $f(a) \neq g(b)$. Since it is a well known fact that $p^{\text{win}}_{\text{local}} = p^{\text{win}}_{\text{deterministic}}$, it suffices to show that $p^{\text{win}}_{\text{deterministic}} \leq 8/9$ as well.

To prove this, consider any pair of functions f, g. To obtain $f(a) \neq a$ for all a, the image of f must contain at least 2 colours. Similarly for the image of g. Since both f and g can only take 3 values, their images must have a common colour. Therefore, there exists an a and a b such that $f(a) = g(b)$. We conclude $p^{\text{win}}_{\text{deterministic}} \leq 8/9$, and therefore $p^{\text{win}}_{\text{local}} = p^{\text{win}}_{\text{deterministic}} = 8/9$. □

Note: somewhat surprisingly Theorem 59 is not good enough to surpass $p^{\text{win}}_{\text{local}}$ in the quantum case. Since $\mathbf{R}^{\mathbf{GR}}_{\mathbf{BG}}\mathbf{B} \in \text{LOC}^2(\mathbf{PR})$ (and not in $\text{LOC}^1(\mathbf{PR})$), an optimal quantum approximation to a PR-box (known to succeed with probability $\frac{2+\sqrt{2}}{4}$) used instead of the perfect one only yields a $\frac{3}{4}$ approximation to an RGB-box.

A natural question is therefore to find a quantum strategy that is better than the local one.

A.3 A Better-than-Local Quantum Strategy

There is indeed a better-than-local quantum strategy which wins with probability 11/12:

Alice and Bob share a singlet state $|\psi^-\rangle_{AB}$. According to their own input colour, they choose their measurement from the following list:

$$\Pi_{\text{Red}} = |0\rangle\langle 0|, \Pi_{\text{Green}} = \left|v^+\right\rangle\!\left\langle v^+\right|, \Pi_{\text{Blue}} = \left|v^-\right\rangle\!\left\langle v^-\right|, \tag{A.3}$$

where

$$\left|v^\pm\right\rangle = \frac{1}{2}|0\rangle \pm \frac{\sqrt{3}}{2}|1\rangle . \tag{A.4}$$

These 3 projectors are located in the same plane equidistantly (like the Mercedes-Benz logo). The colour names can be permutated freely as long as Alice and Bob do the same projection for the same colour.

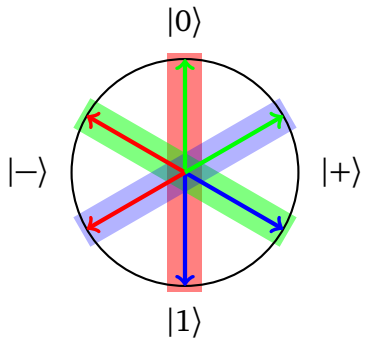


Figure A.10. Alice and Bob's best quantum strategy is to each make the above projective measurement on their half-singlet. The basis (rectangle) depends on their own input colour. Their output is the colour of the measured arrow.

If the output of their measurement is positive, they output the colour that comes after their input colour in the cycle RGB. Otherwise, they output the previous colour. They never output their own input colour as it leads to a sure loss.

For example, if Alice's input is Green and she measures a positive result when applying the projector Π_{Green}, then $a = G$ and $x = G+1 = B$ (the colour addition is modulo 3). Figure A.10 explains the protocol graphically.

A.3.1 Proof of Winning Probability

We look at the probability of losing as it is simpler. To simplify notation, we call directly $x = a-1 \leftrightarrow x = 0$ and $x = a+1 \leftrightarrow x = 1$ as well as $y = b-1 \leftrightarrow y = 0$ and $y = b+1 \leftrightarrow y = 1$. Alice and Bob lose in the following cases:

$$\begin{array}{ll} x = y & \text{if } b = a\,, \\ x = 0 \wedge y = 1 & \text{if } b = a+1 \mod 3\,, \\ x = 1 \wedge y = 0 & \text{if } b = a-1 \mod 3\,. \end{array} \qquad \text{(losing cases)}$$

The probability of error E only depends on the relation between a and b and is given by

$$E_{a=b} = \operatorname{tr}\left(\left|\psi^-\right\rangle\!\left\langle\psi^-\right|_{AB} \cdot \left((\Pi_a \otimes \Pi_b) + (\Pi_a^\perp \otimes \Pi_b^\perp)\right)\right) = 0\,, \tag{A.5}$$

$$E_{a+1=b} = \operatorname{tr}\left(\left|\psi^-\right\rangle\!\left\langle\psi^-\right|_{AB} \cdot (\Pi_a^\perp \otimes \Pi_b)\right) = \frac{1}{8}\,, \tag{A.6}$$

$$E_{a-1=b} = \operatorname{tr}\left(\left|\psi^-\right\rangle\!\left\langle\psi^-\right|_{AB} \cdot (\Pi_a \otimes \Pi_b^\perp)\right) = \frac{1}{8}\,. \tag{A.7}$$

And the winning probability of this quantum strategy is (with uniformly random inputs):

$$p(\text{win}) = 1 - \frac{3E_{a=b} + 3E_{a+1=b} + 3E_{a-1=b}}{9} = \frac{11}{12}. \tag{A.8}$$

The game is therefore won with probability 11/12 using this quantum strategy. □

A.4 The Bell Inequality Associated to the RGB Game

The above quantum strategy is optimal among quantum strategies. To prove it in Section A.5, we now analyze a Bell inequality associated to the RGB game. Bell game and Bell inequalities are equivalent formulations of the same phenomenon. We quickly recall how to translate from one paradigm to the other before defining the inequality and stating the corresponding bounds for quantum and No-Signalling strategies.

A.4.1 Bell Game vs Bell Inequality Notations

Up to now, we have analyzed the RGB game in the modern game context, meaning we treated strategies as probability distributions of the form $P_{x,y|a,b}$ and showed strategies in different non-locality classes (*i.e.*, local, quantum or No-Signalling) can achieve different win rates. To finetune our analysis, we excluded without losing generality the output colour that always lose (*i.e.*, $x = a$ and $y = b$) and treated the remaining outputs as binary (*i.e.*, $0 := u - 1$ and $1 := u + 1$). In the next subsections, we will use the notation $p_{(x,y|a,b)}$ for the individual conditional probabilities.

However, another way to see this problem is through Bell inequalities. Instead of looking at a game with binary outputs, one consider the properties of observables with values in $\{-1, 1\}$. An observable is simply a physical quantity one can decide to measure. In physics, Bell inequalities (*e.g.*, the CHSH inequality) are usually specified by a function of the expected correlations of different observables. This function defines a quantity to which classical mechanics (*i.e.*, local hidden-variable models) imposes a limit that can be broken using quantum mechanics. We remark that all of Alice's observables need to commute (meaning the order in which they are measured don't affect their results) with all of Bob's observable to respect the No-Signalling condition shared by $\mathbb{LOC}$, $|\mathbb{LOC}\rangle$ and $\mathbb{NOSIG}$.

The canonical example of a Bell inequality is the CHSH inequality. This Bell inequality also has a quantum limit: it is Tsirelson's bound. As we are about to see, there exists a similar bound for the RGB Bell-inequality.

The relevant point is that one can translate between the two formulations by expressing the conditional probabilities of the Bell game paradigm as expectancies of correlations in the Bell-inequality paradigm, and *vice versa*. We will in fact only need the following conversion equation:

$$p_{(x=y|a,b)} = \frac{1 + \langle A_a B_b \rangle}{2}, \tag{A.9}$$

where we noted $\langle A_a B_b \rangle$ the expected correlation between the measurement outcomes of Alice's observable A_a and Bob's observable B_b.

A.4.2 Intermediate Step: Rewriting the Probability of Winning as a Function of Expected Correlations

The following lemma will make the subsequent Bell-inequality formulation simple.

Lemma 62. *The probability of a given strategy distribution winning the game is given by*

$$p^{\text{win}} = \frac{1}{9} \sum_{u=0}^{2} 2 - p_{(x=y|u,u)} + \frac{p_{(x=y|u,u+1)}}{2} + \frac{p_{(x=y|u,u-1)}}{2}. \tag{A.10}$$

It depends only on the correlations between Alice's and Bob's outputs, not on their marginals.

Proof. By looking at the three losing cases above (see Section A.3), we obtain the probability of a distribution winning the game:

$$p^{\text{win}} = \frac{1}{9} \sum_{u=0}^{2} \left(3 - p_{(0,0|u,u)} - p_{(1,1|u,u)} - p_{(0,1|u,u+1)} - p_{(1,0|u,u-1)}\right).$$

(winning probability equation)

We rewrite it in terms of the marginals and correlations $\{p_{(x=0|a)}, p_{(y=0|b)}, p_{(x=y|a,b)}\}$. Here is how we can transform each term:

$$p_{(0,0|a,b)} = \frac{p_{(x=0|a)} + p_{(y=0|b)} + p_{(x=y|a,b)} - 1}{2}, \tag{A.11}$$

$$p_{(1,1|a,b)} = p_{(x=y|a,b)} - p_{(0,0|a,b)}, \tag{A.12}$$

$$p_{(0,1|a,b)} = p_{(x=0|a)} - p_{(0,0|a,b)}, \tag{A.13}$$

$$p_{(1,0|a,b)} = p_{(y=0|b)} - p_{(0,0|a,b)}. \tag{A.14}$$

Replacing them into the winning probability equation gives

$$p^{\text{win}} = \frac{1}{9}\sum_{u=0}^{2} 3 - p_{(0,0|u,u)} - p_{(1,1|u,u)} - p_{(0,1|u,u+1)} - p_{(1,0|u,u-1)} \tag{A.15}$$

$$= \frac{1}{9}\sum_{u=0}^{2} 3 - p_{(0,0|u,u)} - p_{(x=y|u,u)} + p_{(0,0|u,u)} - p_{(x=0|a=u)} + p_{(0,0|u,u+1)} - p_{(y=0|b=u-1)} + p_{(0,0|u,u-1)} \tag{A.16}$$

$$= \frac{1}{9}\sum_{u=1}^{2} 3 - p_{(x=y|u,u)} - p_{(x=0|a=u)} + \frac{p_{(x=0|a=u)} + p_{(y=0|b=u+1)} + p_{(x=y|u,u+1)} - 1}{2} - p_{(y=0|b=u-1)} + \frac{p_{(x=0|a=u)} + p_{(y=0|b=u-1)} + p_{(x=y|u,u-1)} - 1}{2} \tag{A.17}$$

$$= \frac{1}{9}\sum_{u=0}^{2} 2 - p_{(x=y|u,u)} + \frac{p_{(x=y|u,u+1)}}{2} + \frac{p_{(x=y|u,u-1)}}{2}. \qquad \square$$

A.4.3 The RGB Bell-Inequality

We show a new simple case of a Bell inequality which we call the RGB Bell-inequality. We define it by reformulating the bound on the local winning probability of the RGB game.

Proposition 63. *The following quantity is related to the RGB game:*

$$R := \left| \sum_{i=0}^{2} -2\langle A_i B_i\rangle + \langle A_i B_{i+1}\rangle + \langle A_i B_{i-1}\rangle \right|. \qquad \text{(RGB Bell-quantity)}$$

and allows us to express the RGB Bell-inequality:

$$R_{\text{local}} \leq 8\,. \qquad \text{(RGB Bell-inequality)}$$

Proof. We first rewrite the equation describing the probability of winning the RGB game into a Bell-inequality notation by taking Lemma 62 and making the simple substitution given in Eq. A.9. We obtain

$$p^{\text{win}} = \frac{1}{36}\sum_{i=0}^{2} 8 - 2\langle A_i B_i\rangle + \langle A_i B_{i+1}\rangle + \langle A_i B_{i-1}\rangle\,. \tag{A.18}$$

We then define the interesting part as the RGB Bell-inequality:

$$R := 36\cdot p^{\text{win}} - 24 = \left| \sum_{i=0}^{2} -2\langle A_i B_i\rangle + \langle A_i B_{i+1}\rangle + \langle A_i B_{i-1}\rangle \right|. \tag{A.19}$$

Finally, from Theorem 61 we have $p^{\text{win}}_{\text{local}} \leq \frac{8}{9}$, which by the last equation implies $R_{\text{local}} \leq 8$.

□

As we showed in Section A.3, quantum mechanics allows for better-than-local strategies, but we will soon show that there is also a limit to how good quantum strategies can be. In fact, the quantum strategy we described earlier is optimal.

Theorem 64. *The RGB Bell-inequality can be broken by quantum distributions, but there exists for the RGB game an analogue to Tsirelson's bound.*

$$R_{\text{quantum}} \leq 9\,. \qquad \text{(quantum bound)}$$

The inequality is tight.

Proof. The value $R_{\text{quantum}} = 9$ is possible. It follows directly from the quantum strategy achieving a win rate of $\frac{11}{12}$ (as described in Section A.3.) The proof one cannot do better is shown next in Section A.5. □

While quantum strategies cannot reach the trivial upper bound, No-Signalling strategies can.

Proposition 65. *No-Signalling physics (*i.e.*, access to* $\mathbf{R}^{\mathbf{GR}}_{\mathbf{BG}}\mathbf{B}$*) could break maximally the RGB Bell-inequality.*

$$R_{\text{No-Signalling}} \leq 12\,. \qquad \text{(trivial No-Signalling bound)}$$

The inequality is tight.

Proof. The value $R_{\text{No-Signalling}} = 12$ is possible by using the No-Signalling strategy described in Section 1 because it achieves a win rate of 1. The inequality is tight as all expected correlation terms are here bounded by $\{-1, 1\}$. □

A.5 Tsirelson's-like Bound and Proof of Optimality of the Quantum Strategy

We now prove the optimality of the quantum strategy described in Section A.3 by finding a Tsirelson's-like bound for the RGB Bell-inequality.

A.5.1 The Optimization Problem

We want to prove that for any $|\psi\rangle$, any $\{A_a\}$ and any $\{B_b\}$, the quantum limit for the RGB Bell-inequality holds:

$$R_{\text{quantum}} = \left| \sum_{u=0}^{2} -2 \langle A_u B_u \rangle + \langle A_u B_{u+1} \rangle + \langle A_u B_{u-1} \rangle \right| \leq 9 \,. \qquad \text{(quantum bound)}$$

We call the value associated to our known quantum strategy $R' = 9$ and the optimal value R^*.

A.5.2 Solving the Bell Inequality Using Semidefinite Programming

We closely follow Wehner's semidefinite programming technique [Weh06]. The idea is first to transform the Bell-inequality problem from the quantum realm to the real-vector space using a result by Tsirelson. Then we use semidefinite programming with Lagrangian duality. The key point is that the Lagrangian dual problem upper bounds the primal problem. So by guessing a solution to the dual problem which have the same value as R', we prove that R' is optimal.

A.5.3 A Bell Inequality as a Real Vector Problem

We will use an important theorem by Tsirelson[5] [Cir80].

Theorem 66 (Tsirelson)**.** *Let $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ be observables with eigenvalues in the interval $\{-1, 1\}$. Then for any state $|\psi\rangle \in \mathscr{A} \otimes \mathscr{B}$, there exist real unit vectors $\vec{x}_1, \ldots, \vec{x}_n, \vec{y}_1, \ldots, \vec{y}_n \in \mathbb{R}^{2n}$ such that for all $s, t \in \{1, \ldots, n\}$:*

$$\langle \psi | A_s \otimes B_t | \psi \rangle = \vec{x}_s \cdot \vec{y}_t \,. \tag{A.20}$$

Conversely, let $\vec{x}_s, \vec{y}_t \in \mathbb{R}^N$ be real unit vectors. Let $|\psi\rangle \in \mathscr{A} \otimes \mathscr{B}$ be any maximally entangled state where $\dim(\mathscr{A}) = \dim(\mathscr{B}) = 2^{\lceil N/2 \rceil}$. Then for all $s, t \in [n]$ there exist observables A_s on $\mathscr{A}$ and B_t on $\mathscr{B}$ with eigenvalues ± 1 such that

$$\vec{x}_s \cdot \vec{y}_t = \langle \psi | A_s \otimes B_t | \psi \rangle \,. \tag{A.21}$$

Applying it to our case, we reduce our Bell-inequality problem to maximizing the following real-vectorial expression:

[5] We write it as formulated in [Weh06], but fix a small mistake in the quantifiers order (it was correct in the original paper).

$$R = \sum_{i=0}^{2} -2\vec{x}_i \cdot \vec{y}_i + \vec{x}_i \cdot \vec{y}_{i+1} + \vec{x}_i \cdot \vec{y}_{i-1} \tag{A.22}$$

under the constraints $\forall i, ||\vec{x}_i|| = ||\vec{y}_i|| = 1$.

Proof of Quantum Optimality

A.5.4 The Primal Problem

We re-write the last statements in a matrix form.

$$G = \begin{pmatrix} \vec{x}_1 \\ \vec{x}_2 \\ \vec{x}_3 \\ \vec{y}_1 \\ \vec{y}_2 \\ \vec{y}_3 \end{pmatrix} \cdot \begin{pmatrix} \vec{x}_1 & \vec{x}_2 & \vec{x}_3 & \vec{y}_1 & \vec{y}_2 & \vec{y}_3 \end{pmatrix}. \tag{A.23}$$

We note G can have this form if and only if it is semidefinite positive and that its diagonal elements are equal to 1 because of the normalization constraints. We also define the matrix W in a way that $\frac{1}{2}\operatorname{tr} GW = R_G$ where R_G is the R defined in Eq. A.22 associated to this strategy G.

$$W = \begin{pmatrix} 0 & 0 & 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & 1 & -2 \\ -2 & 1 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 & 0 \\ 1 & 1 & -2 & 0 & 0 & 0 \end{pmatrix}. \tag{A.24}$$

Then the semidefinite optimization primal problem is

$$\text{maximize } \frac{1}{2}\operatorname{tr} GW \quad \text{subject to} \quad G \geq 0 \text{ and } \forall i, g_{ii} = 1\,. \qquad \text{(primal problem)}$$

The Primal Solution

The quantum strategy we found previously is associated with the value $R' = 9$. For the sake of completeness, we prove again here this value is achievable.

$$G' = \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} & -1 & \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & 1 & -\frac{1}{2} & \frac{1}{2} & -1 & \frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & 1 & \frac{1}{2} & \frac{1}{2} & -1 \\ -1 & \frac{1}{2} & \frac{1}{2} & 1 & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -1 & \frac{1}{2} & -\frac{1}{2} & 1 & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -1 & -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix}. \qquad \text{(primal solution)}$$

We check that $G' \geq 0$ by looking at its eigenvalues: they are indeed $\{3, 3, 0, 0, 0, 0\}$. G' is therefore a feasible solution whose primal value is 9.

A.5.5 The Dual Problem

We now turn to the dual problem with Lagrange multipliers. The idea is to pose an objective function $\mathscr{L}(G, \Lambda)$ which will be equal to R_G if G is a feasible solution (*i.e.*, G is semidefinite positive and all the normalization constraints are satisfied) and whose dual can be evaluated in a non-trivial way.

$$\mathscr{L}(G, \Lambda) = \frac{1}{2} \operatorname{tr} GW - \operatorname{tr} \Lambda (G - I_6), \qquad \text{(objective function)}$$

where Λ is the diagonal matrix of Lagrange multipliers $\{\lambda_1, \ldots, \lambda_6\}$. Note that $\mathscr{L}(G, \Lambda) = R_G$ for a valid solution because when the constraints are satistifed: $G - I_6 = \hat{0}$.

We can associate a dual function to the objective function:

$$\lambda(\Lambda) = \max_{G \text{ is feasible}} \mathscr{L}(G, \Lambda) = \max_{G \text{ is feasible}} \operatorname{tr} G(\frac{1}{2} W - \Lambda) + \operatorname{tr} \Lambda. \qquad \text{(dual function)}$$

The crucial fact about this dual function $\lambda(\Lambda)$ is that it upper bounds $\mathscr{L}(G, \Lambda)$, so for any feasible quantum strategy it also upper bounds R_G (and therefore R^*). This is because [BV04]:

$$\lambda(\Lambda) = \max_{G \text{ is feasible}} \mathscr{L}(G, \Lambda) \geq \mathscr{L}(G^*, \Lambda) = \mathscr{L}(G^*) = R^*. \qquad \text{(A.25)}$$

A.5.6 The Dual Solution

We simply exhibit one matrix Λ such that this upper bound $\lambda(\Lambda)$ is 9. Since we can reach it, then it will be tight.

We observe that $\lambda(\Lambda)$ evaluates to infinity if $-\frac{1}{2}W + \Lambda \not\geq 0$, and that otherwise, the G maximizing $\mathscr{L}(G, \Lambda)$ is the null matrix. This leads to the following dual problem:

$$\text{minimize}\,\mathrm{tr}\,\Lambda \quad \text{subject to} \quad -\frac{1}{2}W + \Lambda \geq 0\,. \qquad \text{(dual problem)}$$

We try the solution

$$\Lambda' = \frac{3}{2}I_6\,. \qquad \text{(dual solution)}$$

The eigenvalues of $-\frac{1}{2}W + \Lambda'$ are $\{3, 3, \frac{3}{2}, \frac{3}{2}, 0, 0\}$, confirming it is semidefinite positive and thus a feasible solution (it does not lead to the trivial bound). The associated dual value is 9 and confirms the optimality of our quantum solution.

A.6 Conclusion and Open Questions

We have defined a new game, the RGB Game, that is very simple and there exists a No-Signalling strategy winning it with probability one. In the sense we have defined, this strategy is equivalent to the winning strategy to the PR game. We showed the RGB game can be won with probabilities

$$p^{\text{win}}_{\text{local}} = \frac{8}{9}\,, \qquad p^{\text{win}}_{\text{quantum}} = \frac{11}{12}\,, \qquad p^{\text{win}}_{\text{No-Signalling}} = 1\,.$$

Our main open question is whether there exist $|\mathbb{LOC}\rangle$-complete and $\mathbb{COMOP}$-complete distributions. Another is to generalize our work to distributions over more than two parties.

Appendix B

Any physical theory of Nature must be boundlessly multipartite nonlocal ([CRWR21a])

The following is a full retranscription of my work ([CRWR21a]) with Marc-Olivier Renou and Elie Wolfe.

Abstract. We introduce the class of Genuinely Local Operation and Shared Randomness (LOSR) Multipartite Nonlocal correlations, that is, correlations between N parties that cannot be obtained from unlimited shared randomness supplemented by any composition of $(N-1)$-shared causal Generalized-Probabilistic-Theory (GPT) resources. We then show that noisy N-partite GHZ quantum states as well as the 3-partite W quantum state can produce such correlations. This proves, if the operational predictions of quantum theory are correct, that *Nature's nonlocality must be boundlessly multipartite* in any causal GPT. We develop a computational method which certifies that a noisy $N = 3$ GHZ quantum state with fidelity 85% satisfies this property, making an experimental demonstration of our results within reach. We motivate our definition and contrast it with pre-existing notions of genuine multipartite nonlocality. This work extends a more compact parallel letter [Phys. Rev. Lett. 127, 200401 (2021)] on the same subject and provides all the required technical proofs.

B.1 Introduction

Correlated events are ubiquitous. A fundamental objective of science is to understand the causal links between these events, behind correlations. Bell's seminal theorem [Bel64] demonstrated the failure of classical causal theories [Pea09] to reproduce the predictions of quantum theory. A natural interpretation of Bell's theorem is that the structural links between non-observed underlying variables (also called sources or resources) and observed variables (also called parties) in a network causal model are not sufficient to delimit all possible correlations that might be observed between them: the *physical nature* of the sources is also important [WSS$^+$20]. Indeed, even in a simple Bell scenario involving one source and several observed variables, a source producing quantum signals allows for "nonlocal" correlations that cannot be modelled classically [CHSH69]. Simply put, the correlations achievable with quantum common causes are richer than those achievable with purely classical sources.

The existence of nonclassical quantum correlations inspired the study of even more general causal theories, capable of explaining quantum correlations and even stronger-than-quantum correlations [PR94]. The explanatory power of such exotic theories is so strong that one might wonder if such a theory might describe all the correlations that may be observed in Nature while at the same time never exceeding some measure of complexity. In this article, we focus on the following question: Do there exist causal theories able to model all observable correlations based on *finite-size* nonclassical resources? More precisely, could Nature's correlations be explained by N-partite resources, for some finite N?

Unsurprisingly, even some *classical* correlations would be inexplicable in the absence of universal (N-way) shared randomness. In particular, no causal theory restricted to sharing bipartite resources of *any* physical nature could accommodate perfect correlations between three parties [H$^+$15] (We will show that this no-go result readily generalizes to N parties restricted to $(N-1)$-partite resources). Accordingly, the "No Shared Randomness" hypothesis is far too strong an assumption in general. Shared randomness is facially an accessible resource: Indeed, N parties can share randomness by simply agreeing on a common stochastic phenomenon to observe, such as the weather. Alternatively, pre-established high-entropy shared randomness can be stored indefinitely in local memories through the use of any number of digital technologies.

As such, in the following we consider shared randomness to always be accessible. We focus on the (non)simulability of certain N-partite correlations in scenarios

allowing for the local composition of $(N-1)$-shared *nonclassical* resources and Local Operations and Shared Randomness (LOSR) between N parties. N-partite correlations which *cannot* be simulated in such a scenario are hereafter deemed *genuinely LOSR multipartite nonlocal*.

Some causal theories of correlations generalizing quantum mechanics have already been introduced. In particular, *boxworld* is an alternative theory for correlations motivated by nonsignalling boxes [Jan12]. Although boxworld produces some correlations which are strictly *beyond* the scope of the predictions of quantum theory, it should also be noted that boxworld cannot reproduce *all* quantum correlations in scenarios with independent sources even when allowing for shared randomness [CR17; WC20; Bie20]. Here we aim to derive an argument in a theory-agnostic perspective, so that it be compatible with any causal theory. This includes classical; quantum; nonsignalling boxes; and, more generally, any hypothetical causal theory that can be defined in networks. In the following, we refer to such theories as causal Generalized Probabilistic Theories (GPT) in networks, or more shortly as GPTs. It is the role of these theories to define the resources, or states, emitted by each source, as well as the measurements made by each party. In our theory-agnostic approach, however, we do not refer to, nor rely on, any concrete formalism for GPTs; different ones [Bar07; SB10] can be used. Our unique requirements for the considered theory is to be causal, and to allow for device replication. (These requirements are formalized in Section B.2.) We call *theory-agnostic* any correlation which can be obtained from such causal theory (equivalent notions are already introduced in [HLP14; GBC$^+$20], see also related work [CDP11; Chi14; BG21; BR21; Pir21]). The present text extends a more compact parallel letter on the same subject [CRWR21b] and furnishes all the required technical proofs.

The question of the (non)simulability of certain N-partite correlations in setups allowing for the local composition of any $(N-1)$-shared GPT resources and N-shared randomness is intuitively clear. Nevertheless, it requires a technical definition of what are *genuinely LOSR N-multipartite nonlocal correlations — i.e.*, the correlations which can be obtained through such a process. In the following Section B.2, we base this definition on a causality principle and device replication, through the inflation paradigm. Then, in Section B.3 we prove that the N-partite quantum states $|\mathrm{GHZ}_N\rangle$ can create genuinely N-partite nonlocal correlations. This proves Theorem 70, the main result of this paper: Nature is not merely N-partite, for any N. Our result is noise tolerant. We also generalize this result to the tripartite state $|\mathrm{W}\rangle$. In Section B.4, we provide a linear-programming (LP) method to generate *certificates* of genuine multipartite nonlocality, based on

the inflation technique. We illustrate it over the $|\mathrm{GHZ}_3\rangle$ state, obtaining better noise-robust results accessible to current technologies. Such improvements illustrate the practical importance of this LP method for experimental realizations. Since there already exist several definitions of the concept of genuinely multipartite nonlocal correlations, we discuss in Section B.5 the adequacy of ours: an LOSR theory-agnostic framework which optimally accommodates an intuitive concept of genuinely multipartite nonlocal correlations. In particular, we compare our definition to the historically accepted notion due to Svetlichny [Sve87].

B.2 Definition of genuinely LOSR-multipartite-nonlocal correlations

In this section, we provide a definition of genuinely LOSR N-partite nonlocal correlations. Our approach is closely related to the concept of network nonlocality, which has been a subject of extensive study in the past decade [TPKLR21; Fri12; BGP10; RBB$^+$19]. By specializing to the case of $N = 3$, the definition herein will precisely formalize the more informal Definition 2 of Ref. [CRWR21b].

As prelude to defining genuine LOSR multipartite nonlocality, we first provide a definition of $(N-1)$-*partite LO theory-agnostic correlations*, that is, of correlations which can be obtained from causal GPT limited entirely to $(N-1)$-partite resources. Then, we extend it to a definition of $(N-1)$-*partite LOSR theory-agnostic correlations*, allowing for N-partite shared randomness in addition to $(N-1)$-partite GPT resources. Lastly, we define genuinely LOSR N-partite nonlocal correlations as the correlations that are *not* $(N-1)$-partite LOSR theory-agnostic.

Recall that standard Bell scenarios involve a single common cause accessible to all parties. In the absence of any particular physical restriction on the nature of that common cause the only *a priori* constraints over such theory-agnostic correlations in a Bell scenario are the No Signalling equalities [Bar07]. By contrast, in our case theory-agnostic correlations are restricted by nontrivial inequality constraints in addition to the equality constraints coming from No Signalling. We will show how these inequalities are consequences of the scenario being composed of several independent theory-agnostic sources available only to $N-1$ parties.

In the following, we base ourselves on a *causality principle* (formalized below, see also its definition in the framework of operational probabilistic theories [CDP11; Chi14]) that consists in accepting the causal structure of the scenario. We also assume that any device distributing a resource, or locally operating on resources,

can be replicated in independent copies which can be reordered to form a new setup. These two ingredients — causality and device replication — are all that are needed in order to draw inferences from the nonfanout-inflation technique [WSF19]; the latter also powers the analytic and computational results in this article.

B.2.1 Notations

Let us introduce $\mathscr{N}_N$, the N-partite network scenario in which every $N = \binom{N}{N-1}$ subset of $N-1$ parties is connected to an arbitrary causal GPT resource. Let $A_1, ..., A_N$ be its parties and $S_1, \ldots, S_N$ its sources, such that A_i is connected to every source except for S_i and similarly S_i is connected to every party except for A_i. For $N = 3$, this corresponds to the triangle network (*without* shared randomness).

Consider now a nonzero integer K. We call *K^{th}-order nonfanout inflation of $\mathscr{N}$* any network $\mathscr{I}$ composed out of K copies $S_i^1, \ldots, S_i^K$ of each source S_i and K copies $A_j^1, \ldots, A_j^K$ of each party A_j, such that the following inflation-compatibility rules are satisfied:

- In $\mathscr{I}$, any party A_j^k is connected to the same number and same types of sources as in $\mathscr{N}_N$,
- In $\mathscr{I}$, any source S_i^k connects the same number and same types of parties as in $\mathscr{N}_N$.

There exist several nonfanout inflations of a given order. For instance, the case of the triangle ($N = 3$) admits two distinct inflations of order $K = 2$: one is two copies of the triangle, and the second is a hexagon. The case of the tetrahedron ($N = 4$) has six classes of inflations of order $K = 2$ (defined up to graph isomorphism, see Figure **??**). Our arguments will often be based on the correlations shared in a sub-network of some large inflation. We call such sub-network an inflation cut. In this paper, most of our figures represent inflation cuts. In the following, sub-network isomorphisms are of particular interest. A sub-network G of the network $\mathscr{N}$ or of its inflation $\mathscr{I}$ consists in a subgroup of parties with all the sources these parties are connected to.

We say that (G_1, G_2), two sub-networks of $(\mathscr{N}, \mathscr{I})$ or of $(\mathscr{I}, \mathscr{I})$, are *isomorphic* if they are isomorphic under the dropping of the indices of the parties and sources (because even if two copies of a same party or source have different indices, they are otherwise indistinguishable). A sub-network is defined by an *ordered* list of parties. The ordering means that a nontrivial isomorphism may exist between

two sub-networks of $\mathscr{I}$ even if both sub-networks refer to precisely the same *unordered* set of parties. Hence, an inflated network can be a sub-network of itself in a nontrivial way. See Figure B.1 for an illustration.

In the following, when R denotes a correlation — that is, a probability distribution of some outputs given some inputs — in some network $\mathscr{J}$, and if G denotes a sub-network of $\mathscr{J}$, then $R_{|G}$ represents the marginal distribution of R over the parties in G. If G_1, G_2 are two non-overlapping (that is, sharing no parties) sub-networks of $\mathscr{J}$, we write $G_1 \cup G_2$ the sub-network of $\mathscr{J}$ composed of the parties of G_1, G_2 and of the sources they are connected to. We write $R_{|G_1 \cup G_2} = R_{|G_1} \cdot R_{|G_2}$ to indicate that the marginal distribution can be factorized.

B.2.2 Genuinely LO-multipartite-nonlocal correlations

We now formalize our causality principle. It first leads to a definition of **LO** theory-agnostic correlations, which we then extend to **LOSR** theory-agnostic correlations in Section B.2.3.

Definition 67 ($(N-1)$-**LO** theory-agnostic correlation)**.** *Consider an N-partite nonsignalling correlation P. P is said to be an* $(N-1)$-LO theory-agnostic correlation *if, for every nonfanout inflation $\mathscr{I}$ of $\mathscr{N}_N$ (of any order), there exists a nonsignalling correlation Q of the parties in $\mathscr{I}$ such that:*

(C1) For all two (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{N}_N)$, if the two are isomorphic, then $Q_{|G_1} = P_{|G_2}$.

(C2) For all two (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{I})$, if the two are isomorphic, then $Q_{|G_1} = Q_{|G_2}$.

(C3) For all two non-overlapping (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{I})$, if the two have no sources in common, then $Q_{|G_1 \cup G_2} = Q_{|G_1} \cdot Q_{|G_2}$.

Note that $(C1)$ is a compatibility condition of Q with P, whereas $(C2)$ and $(C3)$ are self-consistency conditions of Q with itself.

Note that the set of correlations in $\mathscr{N}_N$ singled out by this definition has already been introduced in other works, under different names. In particular, it is the set of the generalized Markov correlations in $\mathscr{N}_N$, introduced in [HLP14]. It is also equivalent to the correlations restricted by the No Signalling and Independence principles of [GBC$^+$20]. There, $(C1)$ is seen as a consequence of an (extended) No Signalling principle, $(C3)$ is called the Independence principle, and $(C2)$ is implicit. In our paper, we view $(C1)$, $(C2)$, and $(C3)$ as consequences of causality.

More precisely, more than a consequence of causality, these three conditions can actually be seen as the *technical definition* of the intuitive notion of causality, once device replication is allowed.

Before introducing shared randomness, let us first remark that a random bit shared between three parties is not a 2-**LO** theory-agnostic correlation, as proven in [H$^+$15]. The proof can be easily extended to show that for any N, N-partite shared randomness is not an $(N-1)$-**LO** theory-agnostic correlation: see Figure B.2. As we justified, however, in our introduction, the concept of **LO** theory-agnostic correlation is not appropriate to discuss the simulability of Nature's correlations, as classical shared randomness is easily accessible. Hence, we now adapt this definition to take into account a shared source of classical randomness λ.

B.2.3 Genuinely LOSR-multipartite-nonlocal correlations

Consider an N-partite correlation P which is obtained from a physical process in a scenario involving arbitrary causal GPT resources distributed in $\mathscr{N}_N$, complemented by shared randomness. For any given randomness outcome λ_0, we obtain a distribution P_{λ_0}, which is a $(N-1)$-LO theory-agnostic correlation (note that, *a priori*, it does not have the same marginal as P). Writing $\mathrm{d}\mu(\lambda_0)$ the probability density of a given λ_0, P can then be written as $P = \int \mathrm{d}\mu(\lambda) P_\lambda$. This discussion motivates the following definition:

Definition 68 ($(N-1)$-**LOSR** theory-agnostic correlation)**.** *P is said to be an* $(N-1)$-LOSR theory-agnostic correlation *if it is a convex mixture of* $(N-1)$-LO *theory-agnostic correlations. More precisely, the latter implies that there exists a random variable λ of density $\mathrm{d}\mu(\lambda)$ such that $P = \int \mathrm{d}\mu(\lambda) P_\lambda$, and that for every any-order nonfanout inflation $\mathscr{I}$ of $\mathscr{N}_N$, there exists nonsignalling correlations Q_λ of the parties in $\mathscr{I}$ such that for all λ, Q_λ satisfies $(C1)$ with respect to P_λ, as well as $(C2)$ and $(C3)$ with respect to $\mathscr{I}$.*
Note that if we introduce $Q \coloneqq \int \mathrm{d}\mu(\lambda) Q_\lambda$, the above conditions imply that Q satisfies $(C1)$ with respect to P and that Q itself satisfies $(C2)$ via linearity of integration.

We can now define genuinely **LOSR**-multipartite-nonlocal correlations.

Definition 69 (Genuine **LOSR** multipartite nonlocality)**.** *An N-partite nonsignalling correlation P is said to be* genuinely LOSR multipartite nonlocal *if and only if it is not an $(N-1)$-LOSR theory-agnostic correlation.*

Note that Definition 68 and 69 are quite difficult to manipulate, in particular

because $(C3)$ is a nonlinear constraint. In Section B.4, we propose a relaxation of this set in which we drop this condition. There we show that a weaker — but more practical — notion of factorization survives, related to the De Finetti theorem.

B.3 $|\mathrm{GHZ}_N\rangle$ and $|\mathrm{W}\rangle$ create genuinely LOSR-multipartite-nonlocal correlations

In order to explore constraints on $(N-1)$-**LOSR** theory-agnostic correlations, we are required to move beyond the case of no-input networks. This is a consequence of the fact that in the presence of shared randomness *any* correlation is compatible with *every* no-input network. Consequently, hereafter we consider exclusively networks with inputs.

In the following Section B.3.1, we show that $|\mathrm{GHZ}_3\rangle$ can create genuinely 3-partite nonlocal correlations. We also prove a similar result for $|\mathrm{W}\rangle$ in Section B.3.3. Most importantly, we extend this first result in Section B.3.2 to show that $|\mathrm{GHZ}_N\rangle$ can create genuinely N-partite nonlocal correlations. This is the main result of this paper, which proves:

Theorem 70 (Nature is not merely N-partite)**.** *Under the hypothesis that quantum mechanics' predictions for local measurements over $|\mathrm{GHZ}_N\rangle$ are correct, Nature is not merely N-local. More precisely, there exist correlations which cannot be explained by any N-partite causal resources and shared randomness.*

Proof. This theorem is proven by Proposition 72 below. Note that this proof is noise tolerant. □

B.3.1 The $|\mathrm{GHZ}_3\rangle$ quantum state produces genuinely LOSR-tripartite-nonlocal correlations

In this section, we prove that the state $|\mathrm{GHZ}_3\rangle$ can produce genuinely LOSR-tripartite-nonlocal correlations. To this end, we first prove the following proposition, which states a constraint for all 2-LOSR theory-agnostic correlations. Then, we show that appropriate local measurements of $|\mathrm{GHZ}_3\rangle$ violate this constraint. It generalizes Proposition 3 of [CRWR21b] to any value of $\langle C_1\rangle$. This generalization is of particular interest from an experimental perspective.

Proposition 71 (GHZ_3, technical)**.** *In the absence of any 3-way nonclassical cause,*

$$I_{\mathrm{Bell}}^{C_1=1} + \frac{4I_{\mathrm{Same}}}{1+\langle C_1\rangle} \leq 6 + \frac{4-4\langle C_1\rangle}{1+\langle C_1\rangle}\,. \tag{P71}$$

Measurements on the $|\mathrm{GHZ}_3\rangle$ quantum state can violate the above by reaching $I_{\mathrm{Bell}}^{C_1=1} + \frac{4I_{\mathrm{Same}}}{1+\langle C_1\rangle} = 2\sqrt{2}+8 > 10$.

In the above, $I_{\mathrm{Bell}}^{C_1=1} \leq 4$ and $I_{\mathrm{Same}} \leq 2$ are respectively defined through the following two tasks:

i. The standard CHSH game between Alice and Bob, with the particularity that it is scored only when Charlie outputs $C{=}1$ (the observables take value in $\{-1,+1\}$):

$$\begin{aligned} I_{\mathrm{Bell}}^{C_1=1} \coloneqq \langle A_0B_0\rangle_{C_1=1} + \langle A_0B_1\rangle_{C_1=1} \\ + \langle A_1B_0\rangle_{C_1=1} - \langle A_1B_1\rangle_{C_1=1}\,. \end{aligned} \tag{B.1}$$

ii. A game whose goal is for all players to output the same result (*i.e.*, either all $+1$ or all -1):

$$I_{\mathrm{Same}} \coloneqq \langle A_0B_2\rangle + \langle B_2C_0\rangle\,. \tag{B.2}$$

Note that $A_0 \coloneqq A_{X=0}$ belongs to both games; Alice is oblivious on that input and thus she cannot adopt a different strategy for the first and second task. In the following, we first prove the inequality P71. Then, we show that the $|\mathrm{GHZ}_3\rangle$ state violates it.

Proof of Eq. (P71). The proof is based on the inflation argument illustrated in Figure B.4. There are four main steps to the proof:

First is the idea behind device-independent randomness certification: *True* randomness is a necessary condition to the violation of Bell inequalities — if a third party Charlie can guess Alice's input, then Alice and Bob can only win Bell's game with limited success (*i.e.*, Bell rewards nonclassical resources). This true randomness is quantified by Theorem 1 of Ref. [ADP$^+$14, Eq. (2)], which states in our case (note that the inequality remains valid when conditioned on $C_1^1 = 1$ because C^1 is space-time separated from $A^1B^1C^{21}$) that

[1]Note also that the original theorem in Ref. [ADP$^+$14, Eq. (2)] is formulated for (amongst others) the I_{BKP_2} Barrett-Kent-Pironio [BKP06] correlations of parameters $M{=}2$ and $d{=}2$, but they are equivalent (up to a relabelling symmetry) to the standard CHSH quantity.

$$I_{\mathrm{Bell}}^{C_1^1=1} \circ \{A^1B^1\} + 2\langle A_0^1 C_0^2\rangle_{C_1^1=1} \leq 4\,. \tag{B.3}$$

The $\circ$ notation is here used to specify that the $I_{\mathrm{Bell}}^{C_1^1=1}$ quantity is computed over the players Alice-1 and Bob-1, which are the players on the left-hand side of the inflated graph in Figure B.4 .

Second, we bound $\langle A_0^1 C_0^2\rangle_{C_1^1=1}$ with $\langle A_0^1 C_0^2\rangle$: For any two events $\{E_1, E_2\}$, the law of total probability implies the bound

$$P(E_1, E_2) = P(E_1) - P(E_1, \neg E_2)\,, \tag{B.4a}$$

$$\therefore \quad P(E_1|E_2) = \frac{P(E_1) - P(E_1, \neg E_2)}{P(E_2)} \geq \frac{P(E_1) - P(\neg E_2)}{P(E_2)}\,. \tag{B.4b}$$

($\neg E_2$ represents the negation of event E_2, so $P(E_2) = 1 - P(\neg E_2)$.) In our case, we apply the reasoning of Eq. (B.4b) to the probabilities $P(A_0^1 = C_0^2|C_1^1{=}1) = (1 + \langle A_0^2 C_0^2\rangle_{C_1^1=1})/2$ and $P(C_1^1 = \pm 1) = (1 \pm \langle C_1^1\rangle)/2$. It leads to the worst-case bound

$$\frac{1 + \langle A_0^1 C_0^2\rangle_{C_1^1=1}}{2} \geq \frac{\frac{1+\langle A_0^1 C_0^2\rangle}{2} - \frac{1-\langle C_1^1\rangle}{2}}{\frac{1+\langle C_1^1\rangle}{2}} \tag{B.5}$$

$$\iff \langle A_0^1 C_0^2\rangle_{C_1^1=1} \geq \frac{2\langle A_0^1 C_0^2\rangle + 2\langle C_1^1\rangle}{1 + \langle C_1^1\rangle} - 1\,. \tag{B.6}$$

We use Ineq. (B.6) to rewrite Ineq. (B.3),

$$I_{\mathrm{Bell}}^{C_1^1=1} \circ \{A^1B^1\} + \frac{4\langle A_0^1 C_0^2\rangle + 4\langle C_1^1\rangle}{1 + \langle C_1^1\rangle} \leq 6\,. \tag{B.7}$$

Third, we enter I_{Same} into the equation: We remark that $A_0^1 C_0^2 \sim A_0^2 C_0^2$ ($\sim$ denotes that the two joint distributions are similarly distributed). This can be seen by observing the inflation in Figure B.4: The view of the couple {Alice-1, Charlie-2} is exactly the same as the one of the couple {Alice-2, Charlie-2}; namely, the joint distributions of all their input resources are identical. One conclusion is hence that

$$\langle A_0^1 C_0^2\rangle = \langle A_0^2 C_0^2\rangle\,. \tag{B.8}$$

We then use an algebraic argument applied to inflation; we find from reformulating Ref. [NWRPK20, App. A, Eq. (3)] that

$$\langle A_0^2 C_0^2\rangle \geq \langle A_0^2 B_2^2\rangle + \langle B_2^2 C_0^2\rangle - 1 = I_{\mathrm{Same}} \circ \{A^2B^2C^2\} - 1\,. \tag{B.9}$$

We now link Ineq. (B.7) and Eq. (B.9), thanks to Ineq. (B.8), and obtain

$$I_{\mathrm{Bell}}^{C_1^1=1} \circ \{A^1B^1\} + \frac{4I_{\mathrm{Same}} \circ \{A^2B^2C^2\}}{1+\langle C_1^1\rangle} \leq 6 + \frac{4-4\langle C_1^1\rangle}{1+\langle C_1^1\rangle}\,. \tag{B.10}$$

At last, fourth, we apply the standard lemmas of the inflation technique to recognize that

$$A^1B^1C^1X^1Y^1Z^1 \sim ABCXYZ\,, \tag{B.11a}$$
$$A^2B^2X^2Y^2 \sim ABXY \text{ and } B^2C^2Y^2Z^2 \sim BCYZ\,, \tag{B.11b}$$

such that respectively

$$I_{\mathrm{Bell}}^{C_1^1=1} \circ \{A^1B^1\} = I_{\mathrm{Bell}}^{C_1=1} \text{ and } \langle C_1^1\rangle = \langle C_1\rangle\,, \tag{B.12a}$$
$$\text{and } I_{\mathrm{Same}} \circ \{A^2B^2C^2\} = I_{\mathrm{Same}}\,. \tag{B.12b}$$

As such, Eq. (B.10) — which applies to the specific inflated-scenario experiment of Figure B.4 — is transformed into the general statement of Proposition 71.

□

Proof of violation. The quantum violation is achieved using $|\mathrm{GHZ}\rangle$: On inputs corresponding to the Same game (XYZ=020), all players measure in the rectilinear basis. On input Z=1, Charlie measures his state in the Hadamard basis and obtains marginal $\langle C_1\rangle = 0$; when he obtains C_1=1 (corresponding to $|+\rangle_C$), the state of Alice and Bob is steered towards the maximally entangled state $|\phi^+\rangle_{AB}$ and they can play the Bell game using the standard optimal strategy for CHSH. □

B.3.2 The $|\mathrm{GHZ}_N\rangle$ quantum state produces genuinely LOSR N-multipartite nonlocal correlations

We now generalize Proposition 71 to all N-party scenarios in Eq. (P72) of the following proposition. The violation of this inequality by the $|\mathrm{GHZ}_N\rangle$ state (see below) provides the proof of Theorem 70 and of Proposition 5 of [CRWR21b].

Proposition 72. *In the absence of any N-way nonclassical common cause,*

$$I_{\mathrm{Bell}}^{\tilde{C}_1=1} + \frac{4I_{\mathrm{Same}_N}}{1+\langle \tilde{C}_1^1\rangle} \leq 6 + \frac{4(N-2)-4\langle \tilde{C}_1^1\rangle}{1+\langle \tilde{C}_1^1\rangle}\,, \tag{P72}$$

where the game scores $I_{\mathrm{Bell}}^{\tilde{C}_1=1}$ *and* I_{Same_N} *are defined below in* (B.13) *and* (B.14). *Measurements on the* $|\mathrm{GHZ}_N\rangle$ *quantum state can violate the above inequality.*

Proof of Eq. (P72). This is done by adding, to the two-player argument, extra players whose collective role is similar to Charlie's role in the three-player case. For this reason we name $\mathrm{Charlie}_{[i]}$ ($i \in \{1,\dots,N-2\}$) the players that are neither Alice nor Bob. In Figure B.5 we illustrate, for the 4-player case, the inflation scenario on which the following argument is based.

We start by defining the generalization of the two previous, three-player games. The game that necessitates nonclassical resources to be won maximally is

$$\begin{aligned} I_{\mathrm{Bell}}^{\tilde{C}_1=1} :=& \langle A_0B_0\rangle_{\tilde{C}_1=1} + \langle A_0B_1\rangle_{\tilde{C}_1=1} \\ &+ \langle A_1B_0\rangle_{\tilde{C}_1=1} - \langle A_1B_1\rangle_{\tilde{C}_1=1}\,, \end{aligned} \tag{B.13}$$

where the difference with the three-player game $I_{\mathrm{Bell}}^{C_1=1}$ is that $\tilde{C} := C_{1[1]}\cdot C_{1[2]}\cdot [\dots]\cdot C_{1[N-2]}$ is defined over the collective of Charlies (*i.e.*, $\tilde{C}_1{=}1$ indicates that all Charlie players had input 1 and an even number of them outputted -1); the game that favours no randomness or genuine tripartite resources (including classical shared randomness) is

$$\begin{aligned} I_{\mathrm{Same}_N} :=& \langle A_0B_2\rangle + \langle B_2C_{0[1]}\rangle + \langle C_{0[1]}C_{0[2]}\rangle \\ &+ [\dots] + \langle C_{0[N-3]}C_{0[N-2]}\rangle\,. \end{aligned} \tag{B.14}$$

The proof closely follows the one given in Section B.3.1 for three parties:

First, as in the three-player case, we use, *mutatis mutandis*, Theorem 1 of Ref. [ADP+14, Eq. (11)],

$$I_{\mathrm{Bell}}^{\tilde{C}_1^1=1} \circ \{A^1B^1\} + 2\langle A_0^1 C_{0[N-2]}^2\rangle_{\tilde{C}_1^1=1} \leq 4\,. \tag{B.15}$$

Second, we bound $\langle A_0^1 C_{0[N-2]}^2\rangle_{\tilde{C}_1^1=1}$ with $\langle A_0^1 C_{0[N-2]}^2\rangle$ and obtain (see Eqs.(B.4a)–(B.6))

$$\langle A_0^1 C_{0[N-2]}^2\rangle_{\tilde{C}_1^1=1} \geq \frac{2\langle A_0^1 C_{0[N-2]}^2\rangle + 2\langle \tilde{C}_1^1\rangle}{1+\langle \tilde{C}_1^1\rangle} - 1\,. \tag{B.16}$$

Therefore,

$$I_{\mathrm{Bell}}^{\tilde{C}_1^1=1} \circ \{A^1 B^1\} + \frac{4\langle A_0^1 C_{0[N-2]}^2\rangle + 4\langle \tilde{C}_1^1\rangle}{1+\langle \tilde{C}_1^1\rangle} \leq 6\,. \tag{B.17}$$

Third, we remark from the inflation technique that $A_0^1 C_{0[N-2]}^2 \sim A_0^2 C_{0[N-2]}^2$, so

$$\langle A_0^1 C_{0[N-2]}^2\rangle = \langle A_0^2 C_{0[N-2]}^2\rangle\,. \tag{B.18}$$

We find from applying the recursive algebraic argument of Ref. [NWRPK20, App. A, Eq. (27)] that

$$\begin{aligned}\langle A_0^2 C_{0[N-2]}^2\rangle \geq \langle A_0^2 B_2^2\rangle + \langle B_2^2 C_{0[1]}^2\rangle + \langle C_{0[1]}^2 C_{0[2]}^2\rangle \\ + [\dots] + \langle C_{0[N-3]}^2 C_{0[N-2]}^2\rangle - N + 2\,,\end{aligned} \tag{B.19}$$

or, equivalently,

$$\langle A_0^2 C_{0[N-2]}^2\rangle \geq I_{\mathrm{Same}} \circ \{A^2 B^2 C_{[0]}^2 \dots C_{[N-2]}^2\} - N + 2\,. \tag{B.20}$$

Combining the above (Eqs (B.17), (B.18) and (B.20)), we get

$$\begin{aligned} I_{\mathrm{Bell}}^{\tilde{C}_1^1=1} \circ \{A^1 B^1\} + \frac{4 I_{\mathrm{Same}_N} \circ \{A^2 B^2 C_{[0]}^2 \dots C_{[N-2]}^2\}}{1+\langle \tilde{C}_1^1\rangle} \\ \leq 6 + \frac{4(N-2) - 4\langle \tilde{C}_1^1\rangle}{1+\langle \tilde{C}_1^1\rangle}\,. \end{aligned} \tag{B.21}$$

At last, fourth, we recognize using the inflation technique that

$$I_{\mathrm{Bell}}^{\tilde{C}_1^1=1} \circ \{A^1 B^1\} = I_{\mathrm{Bell}}^{\tilde{C}_1=1}\,, \tag{B.22}$$

$$\langle \tilde{C}_1^1\rangle = \langle \tilde{C}_1\rangle\,, \tag{B.23}$$

$$I_{\mathrm{Same}_N} \circ \{A^2 B^2 C_{[1]}^2 \dots C_{[N-2]}^2\} = I_{\mathrm{Same}_N}\,; \tag{B.24}$$

we conclude the robust statement generalized to N parties:

$$I_{\mathrm{Bell}}^{\tilde{C}_1=1} + \frac{4 I_{\mathrm{Same}_N}}{1+\langle \tilde{C}_1^1\rangle} \leq 6 + \frac{4(N-2) - 4\langle \tilde{C}_1^1\rangle}{1+\langle \tilde{C}_1^1\rangle}\,. \tag{P72}$$

□

Proof of violation. Eq. (P72) admits a violation using measurements on the N-partite quantum state $|\mathrm{GHZ}_N\rangle := (|0_1 \dots 0_N\rangle + |1_1 \dots 1_N\rangle)/\sqrt{2}$. The strategy is straightforward — on inputs corresponding to the Same game, all players measure in the rectilinear basis; on inputs corresponding to the Bell game, the Charlie players measure in the Hadamard basis (if their product is positive, they have then successfully steered Alice and Bob to the maximally entangled state $|\phi^+\rangle_{AB}$), while Alice and Bob use optimal measurements for the standard Bell game, centred on Alice measuring in the rectilinear basis on input $X = 0$. The resulting value for the left-hand side of Eq. (P72) is then $2\sqrt{2} + 4(N-1)$, while the right-hand side is $4N-2$, hence smaller. This proves that $|\mathrm{GHZ}_N\rangle$ can produce correlations that are genuinely LOSR N-partite nonlocal. □

B.3.3 The $|\mathrm{W}\rangle$ quantum state produces genuinely LOSR-tripartite-nonlocal correlations

In this section, we prove that some measurements on $|\mathrm{W}\rangle$ lead to correlations that are LOSR genuinely tripartite nonlocal. We use a technique that is similar to the one that we use with $|\mathrm{GHZ}\rangle$: a multi-game format analyzed through inflation. It provides the proof of Proposition 4 of [CRWR21b]. As opposed to the previous examples, our proof is not noise tolerant.

Proposition 73 (W)**.** *In the absence of any 3-way nonclassical cause, there are quantum measurements on the quantum state* $|\mathrm{W}\rangle$ *that cannot be simulated exactly.*

The global construction rest on a fourth-order inflation (a triangle plus a third-order ring). In the rest of this section, we detail the proof by examining various relevant cuts.

Preliminaries

For ease of notation, in this section we take the convention to denote the binary outputs as $\{0, 1\}$ rather than as $\{\pm 1\}$.

BKP Inequalities.

The argument presented in the present section is based on the Barrett–Kent–Pironio correlations of parameter $d=2$ [BKP06], which are equivalent to the chained Bell inequalities of Refs. [Pea70; BC90] and can be defined

as

$$\begin{aligned} I_{\mathrm{BKP}_M} := P(A{=}B|X{=}1, Y{=}M) \\ + P(A{\neq}B|X{=}M, Y{=}M) \\ + \sum_{\substack{i\in\{1,\ldots,M-1\} \\ j\in\{0,1\}}} P(A{\neq}B|X{=}i+j, Y{=}i)\,. \end{aligned} \tag{B.25}$$

The inputs have values $X, Y \in \{1, \ldots, M\}$. All outputs are binary (*i.e.*, 0 or 1). The algebraic minimum is $I_{\mathrm{BKP}_M} = 0$ but local resources cannot reach less than 1.

The BKP inequalities concern two players, but as for the $|\mathrm{GHZ}\rangle$ case, we consider the lifted case where we condition on the outcome $C{=}0$ of a third, space-like separated player (the same local and algebraic minima then apply).

$$\begin{aligned} I^{C=0}_{\mathrm{BKP}_M} := P(A{=}B|X{=}1, Y{=}M, C{=}0) \\ + P(A{\neq}B|X{=}M, Y{=}M, C{=}0) \\ + \sum_{\substack{i\in\{1,\ldots,M-1\} \\ j\in\{0,1\}}} P(A{\neq}B|X{=}i+j, Y{=}i, C{=}0)\,. \end{aligned} \tag{B.26}$$

Key results concerning BKP correlations are that, in the asymptotic limit $M \to \infty$, the optimal violation allowed by a maximally entangled state $|\phi^+\rangle$ is the algebraic minimum $I^{C=0}_{\mathrm{BKP}_M} = 0$ [BKP06, Eq. (9)], while for all λ for which the output of Alice is completely determined given output C, the classical bound of $I_{\mathrm{BKP}_M} \geq 1$ applies (corollary of Theorem 1 in Ref. [ADP+14, Eq. (11)]).

A multi-game which can be won with perfect probability using a $|\mathrm{W}\rangle$-state quantum strategy. Similarly to the proof presented for the $|\mathrm{GHZ}\rangle$ case, the proof here also follows a multi-game format. Here we define three games which can all be won at the same time using a quantum strategy.

I On inputs $X \in \{1, \ldots, M\}, Y \in \{1, \ldots, M\}, Z{=}1$, the players are asked (in the asymptotic limit) to reach $\lim_{M\to\infty} I^{C=0}_{\mathrm{BKP}_M} = 0$, while having $P(C{=}0|Z{=}1) = 2/3$.

II A game identical to B.3.3 but with the roles of Alice and Charlie swapped.

III On inputs $XYZ{=}101$ the players must collectively output exactly one "1" and two "0"s (*i.e.*, $ABC \in \{001, 010, 100\}$).

An important fact is that on input $X{=}1$ (or $Z{=}1$), Alice (or Charlie) does not know which one of the three games she (or he) is playing.

The quantum strategy to win maximally all three games with the $|\mathrm{W}\rangle := (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ state is straightforward. On inputs $X = 1$, $Y = 0$ and $Z = 1$, the players measure in the rectilinear basis and by doing so always win the third game of outputting exactly one 1. On input $Z{=}1$, Charlie obtains 0 with probability $2/3$ and in that case the state at Alice–Bob is steered towards a maximally entangle state $|01\rangle + |10\rangle/\sqrt{2}$. Alice and Bob can then on inputs $X, Y \in \{1, \ldots, M\}$ apply the strategy described in Ref. [BKP06] to violate maximally the BKP inequality, achieving asymptotically $\lim_{M\to\infty} I^{AB|C=0}_{\mathrm{BKP}_M} \to 0$. The strategy is symmetric in Alice–Charlie and thus the players also violate the BKP inequality when the roles of Alice and Charlie are switched.

"Nonlocal sharing-of-the-one." Our proof relies on a concept that we call "nonlocal sharing-of-the-one." (Note that, without a loss of generality, we consider any private randomness as also part of Λ.)

Definition 74. *The* nonlocal–sharing-of-the-one indicators *are defined for distributions that simulate perfectly (on inputs $XYZ = 101$) the classical* W *distribution (*i.e.*, game (iii)); they are*

$$f^{\lambda}_{AB} := \begin{cases} 1 & \text{if } P(A{=}1|X{=}1, \Lambda{=}\lambda) > 0 \\ & \quad \text{AND } P(B{=}1|Y{=}0, \Lambda{=}\lambda) > 0\,, \\ 0 & \text{otherwise}\,, \end{cases} \tag{B.27}$$

$$f^{\lambda}_{BC} := \begin{cases} 1 & \text{if } P(B{=}1|Y{=}0, \Lambda{=}\lambda) > 0 \\ & \quad \text{AND } P(C{=}1|Z{=}1, \Lambda{=}\lambda) > 0\,, \\ 0 & \text{otherwise}\,, \end{cases} \tag{B.28}$$

$$f^{\lambda}_{AC} := \begin{cases} 1 & \text{if } P(A{=}1|X{=}1, \Lambda{=}\lambda) > 0 \\ & \quad \text{AND } P(C{=}1|Z{=}1, \Lambda{=}\lambda) > 0\,, \\ 0 & \text{otherwise}\,. \end{cases} \tag{B.29}$$

Intuitively f^{λ}_{AB}, for any fixed λ, is 0 if Alice or Bob (or both) automatically output "0" for that λ without considering the GPT sources (on inputs $X = 1$ and $Y = 0$). It equals 1 if both players need the result of manipulations involving GPT resources before ruling out the output "1." The two other indicators have a similar interpretation.

The proof by contradiction

We show that the players are not able to complete all three tasks perfectly using shared randomness and merely bipartite resources (while they were able to do so using measurements on the quantum state $|\mathrm{W}\rangle$). More precisely, in the triangle scenario (see Figure B.3) succeeding perfectly at all tasks implies two contradictory statements:

a. $\mathbb{E}_\lambda(f^\lambda_{AB} + f^\lambda_{BC}) \leq 1$.
b. $\mathbb{E}_\lambda(f^\lambda_{AB} + f^\lambda_{BC}) \geq 4/3$.

We prove those two contradictory statements in the subsections below.

Proof that winning perfectly Game B.3.3 implies $\mathbb{E}_\lambda(f^\lambda_{AB} + f^\lambda_{BC}) \leq 1$. We look exclusively at the third game and show that simulating perfectly the image of the classical W distribution in the LOSR framework with bipartite resources leads to the upper bound $\mathbb{E}_\lambda(f^\lambda_{AB} + f^\lambda_{BC}) \leq 1$. In fact, we prove a stronger statement:

Proposition 75 (Monogamy of the nonlocal one)**.** *In the triangle scenario (see Figure B.3), when sampling perfectly from the image* $\{001, 010, 100\}$*, the following bound must hold.*

$$f^\lambda_{AB} + f^\lambda_{BC} + f^\lambda_{AC} \leq 1\,. \tag{B.30}$$

In other words, for each instance λ of the shared randomness, at least one player disregards its GPT sources and deterministically outputs 0.

Proof. Each term in the sum is by definition either 0 or 1. We first prove that, for any value λ for which "sometimes Alice outputs 1; and sometimes Charlie outputs 1," then "one of them *will* output 1," hence Bob can never output 1 for this λ. In other terms, we prove:

$$\forall \lambda : \left\{ f^\lambda_{AC} = 1 \implies f^\lambda_{AB} = f^\lambda_{BC} = 0 \right\}. \tag{B.31}$$

Our proof use two inflated scenarios. It is a direct corollary of Lemma 77 (below), which uses Lemma 76 (also below). Then, the full proposition results from repeating the argument with permuted players (*e.g.*, by replacing ABC and inputs $XYZ{=}101$ with BAC and inputs $YXZ{=}100$). □

Lemma 76. *In the short-line inflation illustrated in Figure B.6,* $\forall \lambda$ *such that* $f^\lambda_{AC}{=}1$*,*

$$P(A^1C^1 \in \{01, 10\} | B^1B^2{=}00, Y^1Y^2{=}00, \Lambda{=}\lambda) = 1\,. \tag{B.32}$$

Proof. Consider λ such that $f_{AC}^{\lambda} = 1$. Remark first that we have $P(B{=}1|Y{=}0, \Lambda{=}\lambda) < 1$ because if Bob were to always output 1 for that λ, then to reproduce the image $\{001, 010, 100\}$ neither Alice nor Charlie could ever output 1 for that λ.

We use the line inflation depicted in Figure B.6, and we condition, given λ, on $B^1 = B^2 = 0$ (it has non-zero weight by the previous remark and because $B^1 \sim B \sim B^2$). In what follows, all probabilities are conditioned on the inputs $XYZ{=}101$; we omit them to ease notation.

From inflation, we have

$$\begin{aligned}\{A^1B^1\} &\sim \{AB\}\,,\\ \{B^2C^1\} &\sim \{BC\}\,,\\ \{A^1C^1\} &\sim \{AC\}\,.\end{aligned}$$

Because there is exactly one "1," we have both

$$\begin{aligned}P(A{=}1|BC{=}00) &= 1\,,\\ P(A{=}1|BC{=}01) &= 0\,.\end{aligned}$$

It also holds that

$$\begin{aligned}P(A{=}1|B{=}0) =& P(C{=}0|B{=}0)P(A{=}1|BC{=}00)\\ &+P(C{=}1|B{=}0)P(A{=}1|BC{=}01)\,.\end{aligned}$$

Taken all together, we obtain

$$P(A^1{=}1|B^1{=}0) + P(C^1{=}1|B^2{=}0) = 1\,.$$

Moreover, we have

$$\begin{aligned}1 =& P(A^1C^1{=}00|B^1B^2{=}00) + P(A^1C^1{=}01|B^1B^2{=}00)\\ &+ P(A^1C^1{=}10|B^1B^2{=}00) + P(A^1C^1{=}11|B^1B^2{=}00)\,.\end{aligned}$$

As the two middle terms are[2]

$$\begin{aligned}&P(A^1C^1{=}01|B^1B^2{=}00) + P(A^1C^1{=}10|B^1B^2{=}00)\\ =&P(C^1{=}1|B^1B^2{=}00) + P(A^1{=}1|B^1B^2{=}00)\\ =&P(C^1{=}1|B^2{=}0) + P(A^1{=}1|B^1{=}0)\\ =&1\,,\end{aligned}$$

[2]The second equality holds because B^1 and B^2C^2 are space-like separated, as well as B^2 and A^1B^1, and because $P(B^1{=}0|B^2{=}0) > 0$ and *vice versa* have non-zero probabilities.

we have that

$$P(A^1C^1{=}00|B^1B^2{=}00) = 0 = P(A^1C^1{=}11|B^1B^2{=}00)\,.$$

In conclusion, for any λ for which the conditioning on $B{=}0$ is possible (*e.g.*, all λs for which $f^{\lambda}_{AC} = 1$), we have

$$\begin{aligned} P(A^1C^1{=}00|B^1B^2{=}00, \Lambda = \lambda) = 0 \\ P(A^1C^1{=}11|B^1B^2{=}00, \Lambda = \lambda) = 0\,. \end{aligned}$$

Therefore Lemma 76 holds.

□

Lemma 77. *In the triangle scenario (see Fig B.3), when sampling perfectly from the image* $\{001, 010, 100\}$*,* $\forall\lambda$ *such that* $f^{\lambda}_{AC}{=}1$*,*

$$P(B{=}1|Y{=}0, \Lambda{=}\lambda) = 0\ . \tag{B.33}$$

Proof. We consider the slightly extended line inflation of Figure B.7. We again consider any λ for which $P(A{=}1|\lambda) > 0$[3] and $P(C{=}1|\lambda) > 0$ (*i.e.*, $f^{\lambda}_{AC}{=}1$). Note that $\{C^2A^2|\Lambda{=}\lambda\} \sim \{C^2|\Lambda{=}\lambda\}\{A^2|\Lambda{=}\lambda\}$ (*i.e.*, they are independent given λ). We use that opportunity to condition on $A^2 = 1 = C^2$. Because we are reproducing the image of the W distribution and because $\{A^2B^2\} \sim \{AB\}$ and $\{B^1C^2\} \sim \{BC\}$, we have

$$\begin{aligned} P(B^2{=}0|A^2{=}1) = 1\,, \\ P(B^1{=}0|C^2{=}1) = 1\,. \end{aligned}$$

By Lemma 76, we end up with

$$\begin{aligned} &P(A^1C^1 \in \{01, 10\}|A^2C^2{=}11, \Lambda{=}\lambda) \\ {=}&P(A^1C^1 \in \{01, 10\}|B^1B^2{=}00, \Lambda{=}\lambda) \\ {=}&1 \end{aligned}$$

for all λ. Finally, the inflation tells us that

$$\{A^1C^1|A^2C^2{=}11, \Lambda{=}\lambda\} \sim \{A^1C^1|\Lambda{=}\lambda\} \sim \{AC|\Lambda{=}\lambda\}\,.$$

Hence we can remove the conditioning on $A^2C^2{=}11$ and obtain that $1 = P(A^1C^1 \in \{01, 10\}|\Lambda{=}\lambda)$ (remember that we are assuming $f^{\lambda}_{AC}{=}1$). Eq. (B.33) follows. □

[3] The inputs $XYZ = 101$ are still omitted.

Proof that winning perfectly all games imply $\mathbb{E}_\lambda(f^\lambda_{AB}+f^\lambda_{BC})\geq 4/3$. We look at the first two games — violating BKP inequalities conditioned on C=0, or A=0, respectively — and prove a lower bound that contradicts the upper bound found in *a*.

Proposition 78. *In all nonsignalling LOSR GPT scenarios, if the players succeed perfectly at both Game B.3.3 and Game B.3.3, and also at Game B.3.3, then*

$$\mathbb{E}_\lambda(f^\lambda_{AB}+f^\lambda_{BC})\geq 4/3\,. \tag{B.34}$$

The proof follows from Corollary 79.1.

We start with a lemma.

Lemma 79. *If the players win perfectly Game B.3.3, then* $\forall\lambda$ *such that* $f^\lambda_{AB}=0$*,* $\forall M$*,*

$$I^{C=0}_{BKP_M}(\lambda)\geq 1\,. \tag{B.35}$$

Note that a similar statement holds when Alice and Charlie are switched.

Proof. On inputs $XYZ=101$: Given any λ, if $f^\lambda_{AB}=0$, at least either Alice or Bob outputs deterministically 0. If it is Alice, then her strategy for Game B.3.3 is local, and (pre-processing on C=0 or not) the local bound $I^{C=0}_{BKP_M}(\lambda)\geq 1$ applies. If it is Bob that always output 0 for that λ, then Alice must irremediably output 1 whenever $C=0$. Her strategy for Game B.3.3 is therefore also local in reference to Bob when conditioned on $C=0$, and the local bound $I^{C=0}_{BKP_M}(\lambda)\geq 1$ also applies. □

Corollary 79.1. *If the players win perfectly Game B.3.3 (*i.e.*,* $\lim_{M\to\infty} I^{C=0}_{BKP_M}=0$ *and* $P(C{=}0|Z{=}1)=2/3$*) and Game B.3.3,*

$$\mathbb{E}_\lambda(f^\lambda_{AB})\geq 2/3\,. \tag{B.36}$$

Note that the equivalent for Game B.3.3 (replacing Game B.3.3) holds, when Alice and Charlie are switched.

Proof. By contradiction from combining Lemma 79 and $\lim_{M\to\infty} I^{C=0}_{BKP_M}=0$, we have that $\forall\lambda$ such that $P(C{=}0|Z{=}1,\Lambda{=}\lambda)\neq 0$, $f^\lambda_{AB}=1$. To have $P(C{=}0|Z{=}1)=2/3$, the summed weight of these λs must be at least $2/3$. Therefore, $\mathbb{E}_\lambda(f^\lambda_{AB})\geq 2/3$. □

B.4 A computational method to prove the genuineness of LOSR multipartite nonlocality

In the previous section, we exhibited several genuinely LOSR-multipartite-nonlocal correlations. We proved that the quantum states $|\mathrm{GHZ}_N\rangle$ and $|\mathrm{W}\rangle$ can produce such correlations. We obtained some (limited) noise-tolerant results for the $|\mathrm{GHZ}_N\rangle$ state. In this section, we provide a linear-programming method to obtain certificates of genuine LOSR multipartite nonlocality based on the inflation technique. We show that this method improves the noise tolerance that we obtained in the previous section for $|\mathrm{GHZ}_3\rangle$. The improved noise tolerance makes within experimental reach a demonstration that Nature is not merely bipartite. This method consists in a hierarchy of linear-programming (LP) problems able to characterize a relaxation of the set of LOSR-theory-agnostic correlations.

We first introduce the set of *weakly* $(N-1)$-***LOSR*** *theory-agnostic correlations* which we then show can be freely strengthened, and from which we then define an explicit hierarchy.

Definition 80 (Weakly $(N-1)$-**LOSR** theory-agnostic correlation)**.** *Consider an N-partite nonsignalling correlation P. We say that P is a* Weakly $(N-1)$-LOSR theory-agnostic correlation *if for every any-order nonfanout inflation $\mathscr{I}$ of $\mathscr{N}_N$, there exists a nosignalling correlation Q of the party of $\mathscr{I}$ such that Q satisfies (C1) with respect to P, and (C2) with respect to $\mathscr{I}$.*

Note first that due to the comment at the end of Definition 68, the set of Weakly $(N-1)$-LOSR theory-agnostic correlations is clearly a relaxation of the set of $(N-1)$-LOSR theory-agnostic correlations.

One can readily anticipate an implementation in terms of linear programs (see Section B.4.2), as the conditions over Q are linear for any fixed inflation $\mathscr{I}$. In the following, using De Finetti's theorem, we first show that a looser version of the nonlinear condition $(C3)$ can be derived from the relaxed definition.

B.4.1 A free strengthening of the defining conditions for weakly $(N-1)$-LOSR theory-agnostic correlations

The following Proposition shows that a looser version of the nonlinear condition $(C3)$ is implied by Definition 80.

Proposition 81 (Weakly $(N-1)$-**LOSR** theory-agnostic correlation)**.** *Consider an N-partite nonsignalling correlation P. P is a* Weak $(N-1)$-LOSR theory-agnostic

correlation *if and only if, for every any-order nonfanout inflation $\mathscr{I}$ of $\mathscr{N}_N$, there exists a random variable λ of density $d\mu(\lambda)$ and nonsignalling correlation Q_λ such that, with $Q = \int \mathrm{d}\mu(\lambda) Q_\lambda$:*

1 *Q satisfies $(C1)$ with respect to P: for all two (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{N}_N)$, if the two are isomorphic, then $\int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1} = P_{|G_2}$.*

2 *Q satisfies $(C2)$ with respect to $\mathscr{I}$: for all two (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{I})$, if the two are isomorphic, then $\int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1} = \int \mathrm{d}\mu(\lambda) Q_{\lambda|G_2}$.*

3 *Q satisfies a loosening of $(C3)$ with respect to $\mathscr{I}$: For all two non-overlapping (G_1, G_2) sub-networks of $\mathscr{I}$, if the two have no sources in common, then $\int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1 \uplus G_2} = \int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1} \cdot Q_{\lambda|G_2}$.*

Remark that in Definitions 68, the conditions $(C1), (C2), (C3)$ were imposed for every fixed λ. This proposition replaces all these conditions by weaker versions in which one first integrate over λ before imposing the constraint.

Proof. Consider a P satisfying the proposition's conditions. Consider an inflation $\mathscr{I}$ of $\mathscr{N}_N$. We need to find a correlation Q of the parties in $\mathscr{I}$ which decomposes as $Q = \int \mathrm{d}\mu(\lambda) Q_\lambda$ such that the conditions 1., 2., 3. of the proposition are satisfied. For this, we introduce a larger (infinite) inflation $\mathscr{J} = \{\mathscr{I}_p\}_{p\in\mathrm{N}}$ of both $\mathscr{N}_N$ and $\mathscr{I}$, which consists of infinitely many independent copies of $\mathscr{I}$. As P satisfies the proposition's conditions, there exists a nonsignalling correlation $R = R_{|\{\mathscr{P}_p\}_{p\in\mathrm{N}}}$ over all the parties in $\mathscr{J}$ such that R satisfies 1. and 2..

Remark first that as 2. is satisfied, for any permutation σ of N, the inflation $\mathscr{J}^\sigma = \{\mathscr{I}_{\sigma(p)}\}_{p\in\mathrm{N}}$ which consists in a reordering of the copies of $\mathscr{I}$ is isomorphic to $\mathscr{J}$. Hence, R is invariant under any permutation σ of the parties: $R_{|\{\mathscr{P}_p\}_{p\in\mathrm{N}}} = R_{|\{\mathscr{P}_{\sigma(p)}\}_{p\in\mathrm{N}}}$. By the De Finetti theorem, this implies that R is a mixture of independent and identically distributed probability distributions over the $\{\mathscr{P}_p\}$:

$$R = \int d\mu(\lambda) (Q_\lambda)^{\otimes\infty} \tag{B.37}$$

We consider the marginal of R over $\mathscr{I}_0$, a sub-network of $\mathscr{J} = \{\mathscr{I}_p\}_{p\in\mathrm{N}}$, which can be written $Q = R_{|\mathscr{I}_0} = \int d\mu(\lambda) Q_\lambda$. Q can also be seen as a distribution over the parties of $\mathscr{I}$. As R satisfies 1. and 2., Q clearly satisfies 1. and 2.. Moreover, consider two sub-networks G_1, G_2 of $\mathscr{I}$ which have no sources in common. Then, there exist two ways to see the network (G_1, G_2) as a sub-network of $\mathscr{J}$:

- (G_1, G_2) is a sub-network of $\mathscr{I}_0$, hence of $\mathscr{J}$: we call it $G \subset \mathscr{I}_0 \subset \mathscr{J}$. Note that G can also be seen as a sub-network of $\mathscr{I}$.
- We can also see (G_1, G_2) as a sub-network of $\mathscr{I}_1 \times \mathscr{I}_2$ where $G_1 \subset \mathscr{I}_1$ and $G_2 \subset \mathscr{I}_2$. In this case (G_1, G_2) can be seen as a different sub-network of $\mathscr{J}$: we call it $G' \subset \mathscr{I}_1 \times \mathscr{I}_2 \subset \mathscr{J}$.

Remark that, as G_1, G_2 have no sources in common, the two sub-networks G and G' of $\mathscr{J}$ are isomorphic.

Then, we have $\int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1G_2} = Q_{|G} = R_{|G} = R_{|G'} = \int \mathrm{d}\mu(\lambda) Q_{\lambda|G_1} \cdot Q_{\lambda|G_2}$, where we used the fact that R satisfies 2. in the third equality and Eq. (B.37) in the fifth equality. □

B.4.2 A Linear Programming Hierarchy

Definition 80 leads to a natural algorithmic way to prove that a nonsignaling correlation P is not a weakly $(N-1)$-LOSR theory-agnostic correlation. As this notion is a relaxation, the success of the algorithm directly implies that P is not a $(N-1)$-LOSR theory-agnostic correlation, hence that P is genuinely LOSR N-partite nonlocal.

Our hierarchy is based on enumerating *all* K^{th}-order inflations $\mathscr{I}_1, ..., \mathscr{I}_{p_K}$ of $\mathscr{N}_N$, requiring a Q satisfying Definition 80 for each of them, but also imposing cross-inflation compatibility constraints, which would normally only show up at a higher-order inflation. Nevertheless, adding these extra constraints does not require any increase in the number of variables in the linear program, and hence it would be wasteful in practice not to include them.

Definition 82 (The K^{th}-order inflation test for evaluating if P might be a weakly $(N-1)$-LOSR theory-agnostic correlation)**.** *Consider an N-partite nonsignalling correlation P. Then, a necessary condition for P to be a weakly $(N-1)$-LOSR theory-agnostic correlation is that for every nonfanout inflation $\mathscr{I}$ of $\mathscr{N}_N$ (up to order K), there exists a nonsignalling correlation $Q^{(\mathscr{I})}$ of $N \times K$ parties such that:*

(C1) For all two (G_1, G_2) sub-networks of $(\mathscr{I}, \mathscr{N}_N)$, if the two are isomorphic, then $Q^{(\mathscr{I})}_{|G_1} = P_{|G_2}$.

(C2+) For all two (G_1, G_2) sub-networks of a pair of K^{th}-order inflations $(\mathscr{I}_1, \mathscr{I}_2)$, including but not limited to the special case $\mathscr{I}_1 = \mathscr{I}_2$, if G_1 and G_2 are isomorphic, then $Q^{(\mathscr{I}_1)}_{|G_1} = Q^{(\mathscr{I}_2)}_{|G_2}$.

This algorithm is a direct adaptation of the algorithms presented in the original papers on the inflation technique [WSF19; NW20], hence we only sketch it.

Algorithm 1 The K^{th}-order inflation test for evaluating if P might be a weakly $(N-1)$-LOSR theory-agnostic correlation

INPUT: *An N-partite nonsignalling correlation P and an integer K specifying the hierarchy order*
Enumerate all K^{th}-order inflations $\mathscr{I}_1, ..., \mathscr{I}_{p_K}$ of $\mathscr{N}_N$.
for $i = 1, \ldots, p_K$ **do**
    Find $A_1^{(i)}$, $B_1^{(i)}$ such that the linear-compatibility conditions $(C1)$ between the unknown correlation $Q^{(\mathscr{I}_i)}$ and the distribution P can be written as $A_1^{(i)} \cdot Q^{(\mathscr{I}_i)} = B_1^{(i)}$.
    for $j = i, \ldots, p_K$ **do**
        Find $A_2^{(i)}$, $A_3^{(j)}$ such that for every pair of isomorphic subgraphs of $\mathscr{I}_i$ and $\mathscr{I}_j$ the linear-compatibility conditions $(C2+)$ between the unknown marginal correlations $Q_{|G_1}^{(\mathscr{I}_1)}$ and $Q_{|G_2}^{(\mathscr{I}_2)}$ can be captured by constraints $A_2^{(i)} \cdot Q^{(\mathscr{I}_i)} = A_3^{(j)} \cdot Q^{(\mathscr{I}_j)}$.
    end for
end for
Solve the Linear Program (LP) regarding the existence of vectors $0 \leq Q^{(\mathscr{I}_1)}, ..., Q^{(\mathscr{I}_{p_K})} \leq 1$ such that
- for all $i \in \{1, \ldots, p_K\}$, each $Q^{(\mathscr{I}_i)}$ is a correlation;
- and for all $i \in \{1, \ldots, p_K\}$, the correlation satisfies $A_1^{(i)} \cdot Q^{(\mathscr{I}_i)} = B_1^{(i)}$;
- and for all $i, j \in \{1, \ldots, p_K\}$ such that $i \leq j$, the pairs of correlations satisfy $A_2^{(i)} \cdot Q^{(\mathscr{I}_i)} = A_3^{(j)} \cdot Q^{(\mathscr{I}_j)}$.

if LP is infeasible (*i.e.*, the constraints cannot be simultaneously satisfied) **then**
    Output "P is not a Weakly $(N-1)$-LOSR theory-agnostic Correlation."
end if

Details of the practical technicalities involved with formulating the appropriate A matrices and B vectors can be found in Ref. [WSF19]. Infeasibility of the LP indicates that P is not a weak $(N-1)$-LOSR theory-agnostic correlation, and hence that P is genuinely LOSR N-partite nonlocal.

Note that in finite time one can only ever test K^{th}-order inflations up to some finite K. Hence, in finite time, the algorithm cannot prove that P *is* a weakly $(N-1)$-LOSR theory-agnostic correlation (but it can prove it is *not*). In other words, this

algorithm is only useful in proving the genuine LOSR N-partite nonlocality of a distribution; happily, this is precisely our goal.

B.4.3 A better noise tolerance for $|\mathrm{GHZ}_3\rangle$

Our proposition 71 in Section B.3.1, which generalizes Proposition 3 of [CRWR21b], proves that the state $|\mathrm{GHZ}_3\rangle$ can produce genuinely LOSR-tripartite-nonlocal correlations. In this section, we focus on the noise tolerance of this claim: With a noisy source of $|\mathrm{GHZ}_3\rangle$ states, can one still observe genuinely LOSR-tripartite-nonlocal correlations? This question is of particular interest for experimental concerns.

For simplicity, we focus on the case of white noise, for a state measured with optimal measurements operators (the following can be generalized to other noise models). We consider a source emitting a mixture of $|\mathrm{GHZ}_3\rangle$ with the maximally mixed state,

$$\rho_p = p\,|\mathrm{GHZ}_3\rangle\langle\mathrm{GHZ}_3| + (1-p)\mathbb{1}/8\,, \tag{B.38}$$

and look for conditions on p ensuring that ρ_p can demonstrate genuinely LOSR-tripartite-nonlocal correlations. The fidelity of ρ_p with $|\mathrm{GHZ}_3\rangle$ is $f = \langle GHZ_3|\,\rho_p\,|\mathrm{GHZ}_3\rangle = (1+7p)/8$, *i.e.*, $p = (8f-1)/7$.

Remark first that Proposition 71 already allows to find a first noise-tolerant bound: with ρ_p, performing the same measurements as in the ideal protocol, $I_{Bell}^{C_1=1}[\rho_p] = p\cdot 2\sqrt{2}$, $I_{Same}[\rho_p] = p\cdot 2$ and $\langle C_1\rangle = 0$, hence (P71) is violated as long as $p\cdot(2\sqrt{2}+8) > 10$. Hence, we obtain a first proof of genuine LOSR tripartite nonlocality for $p \gtrsim 92\%$, corresponding to a fidelity $f \gtrsim 93\%$. This bound is experimentally challenging. For instance, recent experimental work could prove a violation of Mermin and Svetlichny inequalities with a three-photon $|\mathrm{GHZ}_3\rangle$ state of fidelity $\sim 86\%$ [HSH+14].

To improve the noise tolerance of our result, we implemented Algorithm 1 using Mathematica and evaluated it for the inflation test of order K=2. Considering again the correlation obtained by measuring ρ_p with the same measurements as in the ideal protocol of Proposition 71, we obtained a certificate of LOSR tripartite nonlocal genuiness for all state with $p > 2\sqrt{(2)} - 2 \approx 83\%$, *i.e.*, of fidelity $f \gtrsim 85\%$.

This improvement shows the importance of the computation approach for experimental proofs of the claim that Nature is not merely N-partite for low N (see [HSH+14; ZHW+15; ZBH+19; PPG+19] for experimental capabilities up to

$N = 6$). Considering higher order inflation tests may result in better noise-tolerant results. We also emphasize that Algorithm 1 can also be applied to the $|\text{GHZ}_N\rangle$ and $|\text{W}\rangle$ cases, possibly with alternative quantum measurements.

B.5 On LOCC vs LOSR and everything in between

B.5.1 A generalization of $(N-1)$-theory-agnostic correlations to k-theory-agnostic correlations

In Section B.2, we introduced Definition 68, namely $(N-1)$-LOSR theory-agnostic correlations, for describing the set of N-partite correlations that can be obtained by local composition with any GPT $(N-1)$-partite resources as well as as N-partite shared randomness.

Here we firstly note, in an informal way, that this definition can easily be altered to characterize instead the N-partite theory-agnostic correlations that can be obtained by allowing for shared randomness alongside GPT *k-partite resources*, for some $k < N$. To do this, one needs simply consider the N-party network scenario in which every subset of k parties is connected to an arbitrary causal GPT resource. One can then proceed, as before, by considering K^{th}-order nonfanout inflation of this network scenario.

B.5.2 Several definitions of genuine multipartite nonlocality

We defined as genuinely LOSR N-multipartite nonlocal the correlations which are not $(N-1)$-theory-agnostic. One can, however, consider a variety of related definitions of genuinely multipartite-nonlocal distributions, and of associated k—theory-agnostic correlations. Here we enumerate some of them, and discuss on how they interrelate to one another.

In the following, we consider various physical causal theories for correlations such as the classical, quantum and boxworld theories, or the signalling-boxes theory, which allows for signalling distributions. We consider the set of all k—partite *$\mathscr{R}$-like boxes*, that is, all correlations which can be obtained in a k—party scenario in a theory $\mathscr{R}$. We call $\boldsymbol{P}_{\mathscr{R}}^{\leq k}$ this set of correlations. Given $\mathscr{R}$, one can define a notion of LOCC nonclassicality as follows:

Definition 83 (Genuine LOCC-$\mathscr{R}$ tripartite nonlocality)**.** *A tripartite nonsignalling correlation P is said to be* LOCC-$\mathscr{R}$ tripartite producible *if P can be decomposed*

into a convex mixture of products of onepartite and bipartite $\mathscr{R}$-like boxes, i.e.*, correlations in $\boldsymbol{P}^{\leq 2}_{\mathscr{R}}$.*
A distribution which is not LOCC-$\mathscr{R}$ bipartite producible is said to be genuinely LOCC-$\mathscr{R}$ tripartite nonlocal.

In this definition, the term LOCC indicates that one is allowed to perform local operation over the *classical* inputs and output of $\mathscr{R}$-like boxes, such as post-processing or wiring. Local operations over the *physical states* in theory $\mathscr{R}$ are not allowed. In particular, when $\mathscr{R} \to \mathscr{Q}$ is quantum theory, entanglement swapping is not an allowed operation as it cannot be performed via local operation on some quantum measurement classical outputs.

This definition specializes to the standard Svetlichny notion of multipartite nonlocality (Definition 2 of [CRWR21b]) upon taking $\boldsymbol{P}^{\leq 2}_{\mathscr{R}}$ to be the set of all (onepartite and bipartite) correlations, including signalling correlations, *i.e.* , $\mathscr{R} \to \mathscr{S}\rangle\}$. One can also take $\mathscr{R} \to \mathscr{NS}$ to be the set of all (onepartite and bipartite) nonsignalling boxes, such as in Refs. [CGL15; BTF$^+$19]. Additional significant choices for $\mathscr{R}$ include the $\mathscr{R} \to \mathscr{Q}$ — obtaining $\boldsymbol{P}^{\leq 2}_{\mathscr{Q}}$, the set of all quantum (onepartite and bipartite) correlations — as well as $\mathscr{R} \to \mathscr{TOBL}$ — obtaining $\boldsymbol{P}^{\leq 2}_{\mathscr{TOBL}}$, the set of all (onelocal and bilocal) time-ordered (TOBL) correlations, see Refs. [GWAN12; BBGP13].

Ref. [CGL15] provides a quantitative generalization of these LOCC-centric definitions of multipartite nonlocality to more than three parties:

Definition 84 (LOCC-$\mathscr{R}$ minimal group size)**.** *An N-partite correlation P is said to be* LOCC-$\mathscr{R}$ k-partite producible *if P can be decomposed into a convex mixture of products of* at most *k-partite $\mathscr{R}$-like boxes,* i.e.*, correlations in $\boldsymbol{P}^{\leq k}_{\mathscr{R}}$.*
The LOCC-$\mathscr{R}$ minimal group size *of a correlation P is the smallest k such that P is LOCC-$\mathscr{R}$ k-partite producible.*

A plurality of definitions can similarly be encompassed within a spectrum of notions of LOSR multipartite nonlocality.

It is important to keep in mind that in the LOCC-$\mathscr{R}$ sub-definitions, one is limited to the type "$\mathscr{R}$ "*boxes*, producing the correlations $\boldsymbol{P}^{\leq k}_{\mathscr{R}}$, to find a convex decomposition of P. By contrast, in the following LOSR-$\mathscr{S}$ sub-definitions, one can use some family of k-way *sources* $\omega^{\leq k}_{\mathscr{S}}$ that are comprising the elementary constituents of a physical network.

For any class of type-$\mathscr{S}$ sources which can serve as nonclassical resources in a physical network we have:

Definition 85 (Genuine LOSR-$\mathscr{S}$ tripartite nonlocality)**.** *A tripartite nonsignalling correlation P is said to be* LOSR-$\mathscr{S}$ tripartite producible *if P can be obtained by local operations over any 2-way $\mathscr{S}$-type resources $\omega_{\mathscr{S}}^{\leq k}$ along with 3-way shared randomness between all parties.*
A distribution which is not LOSR-$\mathscr{S}$ tripartite producible is said to be genuinely LOSR-$\mathscr{S}$ tripartite nonlocal.

We define bipartite GPT states as the states which allow to recover our definition of genuinely LOSR-multipartite-nonlocal correlations for $N = 2$, that is, the states $\boldsymbol{\omega}_{\mathscr{G}\mathscr{P}\mathscr{T}}^{\leq 2}$ recovers Definition 69. Alternatively, one could take the 2-way resources to be the quantum states $\boldsymbol{\psi}_{\mathscr{Q}}^{\leq 2}$. This *quantum* causal notion of LOSR multipartite nonlocality is equivalent to the definition of 3-way nonlocality given in Ref. [SFK$^+$20]. One could also imagine explicit nonclassical theories distinct from quantum theory, such as explicit variants of the *boxworld* GPT [Jan12].

The multipartite generalization is as follows:

Definition 86 (LOSR-$\mathscr{S}$ minimal group size)**.** *An N-partite correlation P is said to be* LOSR-$\mathscr{S}$ k-partite producible *if P can be obtained via local operations acting on some network consisting of various k-way $\mathscr{S}$-type sources along with N-way classical randomness shared between all parties.*
The LOSR-$\mathscr{S}$ minimal group size *of a correlation P is the smallest k such that P is LOSR-$\mathscr{S}$ k-partite producible.*

B.5.3 Networks with sources distributing nonlocal boxes instead of entangled states

To assess LOSR multipartite nonlocality, we are imagining N-partite networks wherein every size k subset of parties shares a nonclassical source. Accordingly, every individual party is connected to $\binom{N-1}{k-1}$ distinct sources. (For the triangle we have N=3 and k=2, and every party is connected to two sources.)

This manuscript is concerned with GPT sources $\boldsymbol{\omega}_{\mathscr{G}\mathscr{P}\mathscr{T}}$, *i.e.*, sources which distribute GPT entanglement. We have also alluded to sources which distribute *quantum* entanglement $\boldsymbol{\psi}_{\mathscr{Q}}$. In all such cases, we are considering the sources themselves to be described as multipartite entangled *states*. One can, however, imagine a network in which the k-way sources connecting noncommunicating parties are taken to be *nonlocal boxes* instead of entangled states.

That is to say, in addition to possibly considering $\boldsymbol{\omega}_{\mathscr{G}\mathscr{P}\mathscr{T}}^{\leq k}$ and $\boldsymbol{\psi}_{\mathscr{Q}}^{\leq k}$ we can imagine to consider $\mathscr{S} \to \boldsymbol{P}_{\mathscr{N}\mathscr{S}}^{\leq k}$ (resp. $\mathscr{S} \to \boldsymbol{P}_{\mathscr{Q}}^{\leq k}$), that is to consider correlations in $\boldsymbol{P}_{\mathscr{N}\mathscr{S}}^{\leq k}$

(resp. $\boldsymbol{P}_{\mathscr{Q}}^{\leq k}$) as our sources.

When the sources in a network are themselves multipartite entangled states, then the local operations performed by a single party (say, Alice) are described by *entangled measurements* applied to Alice's subspaces within her $\binom{N-1}{k-1}$ connected sources. By contrast, when the sources in a network are themselves nonlocal boxes, then the local operations performed by Alice are described by *wirings* that she applies to her portions of the $\binom{N-1}{k-1}$ nonlocal boxes that she is connected to.

Entangled measurements are more general than wirings. Accordingly, the set of correlations realizable using a network of k-way quantum sources ($\boldsymbol{\psi}_{\mathscr{Q}}^{\leq k}$) includes the set of correlations realizable using a network of k-way quantum-correlation boxes ($\mathscr{S} \to \boldsymbol{P}_{\mathscr{Q}}^{\leq k}$).

It is worth emphasizing that the inclusion is *strict* however.

Proposition 87. *The set of tripartite correlations which are LOSR-producible using sources $\boldsymbol{\psi}_{\mathscr{Q}}^{\leq 2}$ is a strict superset of the tripartite correlations that are LOSR-producible using $\mathscr{S} \to \boldsymbol{P}_{\mathscr{Q}}^{\leq 2}$.*

Proof. The following proof makes use of the entanglement swapping, which is the paradigmatic advantage of sharing bipartite entanglement compared to sharing bipartite nonlocal correlations. The closest analog of entanglement swapping is nonlocal coupling [SB09; SB10], but nonlocality coupling is not possible in a paradigm where local operations on boxes are limited to classical wirings. Consider a tripartite correlation with two settings for Alice and Charlie and three settings for Bob, ($x \in \{0,1\}$, $y \in \{0,1,2\}$, $z \in \{0,1\}$). Alice and Charlie always measure according to mutually unbiased bases. Bob, however, will ignore the singlet shared with Charlie for his first two settings, choosing instead measurements which lead to maximal violation of the CHSH inequality with Alice. For Bob's third setting, he performs a Bell-state measurement on the two singlets, coarse graining the outcome of that measurement to be 0 if the postselected state on Alice and Charlie is the singlet, and 1 otherwise. This $\boldsymbol{\psi}_{\mathscr{Q}}^{\leq 2}$ based strategy produces a correlation of the form:

$$P(abc|xyz) = \begin{cases} \frac{2+(-1)^{a\oplus b\oplus xy}\sqrt{2}}{16} & y \in \{0,1\} \\ \frac{4-2(-1)^{b}+(-1)^{a\oplus b\oplus c\oplus xz}\sqrt{2}}{32} & y{=}2 \end{cases} \tag{B.39}$$

We now argue that this correlation is not LOSR-producible using $\mathscr{S} \to \boldsymbol{P}_{\mathscr{Q}}^{\leq 2}$. From the maximal CHSH-inequality violation between Alice and Bob achieved when $y \in \{0,1\}$, we conclude that the measurements performed by Alice cannot depend in any way on the source that she shares with Charlie. On the other hand,

we observe significant (maximal) CHSH-inequality violation between Alice and Charlie when we condition on $y{=}2$ and $b{=}0$. This Alice–Charlie nonlocality induced by postselection on Bob's measurement can *only* be explained by entanglement swapping, since we have eliminated the possibility that $P(abc|xyz)$ utilizes any Alice–Charlie source. □

Let us conclude this section with a conjecture. Remark first that the set of correlations realizable using a network of k-way GPT sources ($\boldsymbol{\omega}^{\leq k}_{\mathscr{G}\mathscr{P}\mathscr{T}}$) naturally includes the set of correlations realizable using a network of k-way nonsignalling boxes ($\mathscr{S} \to \boldsymbol{P}^{\leq k}_{\mathscr{N}\mathscr{S}}$). We conjecture that here too, the inclusion is strict.

Conjecture 1. *The set of tripartite correlation which are LOSR-producible using $\boldsymbol{\omega}^{\leq 2}_{\mathscr{G}\mathscr{P}\mathscr{T}}$ is a strict superset of the tripartite correlations that are LOSR-producible using $\mathscr{S} \to \boldsymbol{P}^{\leq 2}_{\mathscr{N}\mathscr{S}}$.*

Our conjecture is based on the extremal-class #4 of the set of extremal nonsignalling tripartite correlations, as enumerated in Ref. [PBS11]. These correlations are known to be incompatible with a triangle network of type $\mathscr{S} \to \boldsymbol{P}^{\leq 2}_{\mathscr{N}\mathscr{S}}$ per Ref. [Sca06, Sec. 5-A]. Hence it is sufficient to prove they are LOSR-producible using $\boldsymbol{\omega}^{\leq 2}_{\mathscr{G}\mathscr{P}\mathscr{T}}$, that is, that they are 2-LOSR theory-agnostic. We found evidence that the linear constraint given by all the triangle inflations cannot rule out these correlations, suggesting they are at least *weakly* 2-LOSR theory-agnostic correlations.

B.5.4 Comparing and contrasting LOCC and LOSR producibility

If a correlation P is in $\boldsymbol{P}^{\leq k}_{\mathscr{R}}$, *i.e.*, LOCC-$\mathscr{R}$ k-producible, then P is also LOSR-producible using $\mathscr{S} \to \boldsymbol{P}^{\leq k}_{\mathscr{R}}$. The LOSR network which realizes the LOCC-relevant convex decomposition utilizes the shared randomness as a switch variable. Accordingly, if P is genuinely LOSR-$\mathscr{G}\mathscr{P}\mathscr{T}$ multipartite nonlocal, then P is also certainly genuinely LOCC k-partite nonlocal relative to $\mathscr{R} \to \mathscr{N}\mathscr{S}$. From the well-known containment of $\boldsymbol{P}_{\mathscr{Q}} \subset \boldsymbol{P}_{\mathscr{N}\mathscr{S}}$, we further establish that if P is genuinely LOSR-$\mathscr{G}\mathscr{P}\mathscr{T}$ multipartite nonlocal, then P is also certainly genuinely LOCC k-partite nonlocal relative to $\mathscr{Q}$.

It is worth emphasizing that the implications about LOCC multipartite nonlocality from LOSR multipartite nonlocality run strictly *one way*. That is, there are correlations which are genuinely LOCC-$\mathscr{N}\mathscr{S}$ multipartite nonlocal which are *not* genuinely LOSR-$\mathscr{N}\mathscr{S}$ multipartite nonlocal. Perhaps the most famous example is the Svetlichny box; see Ref. [BLM$^+$05b, Fig. 5]. Another simple example is the parallel composition of two distinct bipartite Tsirelson boxes, one for Alice–Bob

and another for Bob–Charlie, as discussed in [CRWR21b]. The resulting tripartite correlation (involving a 2-bit setting variable and 2-bit outcome variable for Bob) is genuinely LOCC-$\mathscr{NS}$ multipartite nonlocal [CTPdV21], but, by construction, *not* genuinely LOSR-$\mathscr{NS}$ multipartite nonlocal.

It is also critical to recognize that *Svetlichny* genuine multipartite nonlocality is *not* implied by LOSR multipartite nonlocality. This is readily evident by noticing that inequality (P71) is strongly violated by nonsignalling correlations generated via causal models wherein a is allowed to functionally depend on b and y (hidden signalling from Bob to Alice). Consider the following fine-tuned (hidden signalling) local hidden-variable model (LHVM): Let λ indicate the value of the globally shared classical hidden random variable, such that λ is uniformly distributed amongst the dichotomous values $\{+1,-1\}$. Let $c{=}\lambda$ always, *i.e.*, for both $z \in \{0,1\}$; similarly, let $b{=}\lambda$ always, *i.e.*, for all cases $y \in \{0,1,2\}$. Finally, let Alice's outcome depend on y such that $a = b \times (-1)^{xy}$, an effect of which is that $a{=}b{=}c$ with unit probability for $y{=}2$.

For a further example, consider Box #8 in the set of extremal nonsignalling tripartite correlations as enumerated in Ref. [PBS11]. Such correlations are known to be LOCC-producible using correlations in $\boldsymbol{P}^{\leq 2}_{\mathscr{S}\rangle\}}$. Nevertheless, one can use nonfanout inflation to readily prove that such correlations are *not* LOSR-producible within triangle networks using sources of type $\boldsymbol{\omega}^{\leq 2}_{\mathscr{G}\mathscr{P}\mathscr{T}}$. As such, Box #8 is genuinely LOSR multipartite nonlocal yet not Svetlichny genuinely multipartite.

B.6 Conclusion

In this paper, we focused on correlations that cannot be obtained from arbitrary $(N-1)$-partite causal GPT resources and N-shared randomness, for any fixed N, which we called *genuinely LOSR-multipartite-nonlocal correlations*. We proved that the (noisy) $|\mathrm{GHZ}_N\rangle$ states and the $|\mathrm{W}\rangle$ state can produce such correlations. This proves Theorem 70, the main result of this paper: *Nature is not merely N-partite, for any N*. As this definition relies on an infinite hierarchy of nonlinear existence problems involving linear- and nonlinear- equality constraints of factorization, it is hard to manipulate in practice. Using De Finetti's theorem, we obtained a nontrivial relaxation of the set of genuinely LOSR-multipartite-nonlocal correlations, which can be characterized by an infinite hierarchy of LP existence problems. We illustrated its usefulness by improving the noise tolerance of our analysis of $|\mathrm{GHZ}_3\rangle$, making an experimental proof accessible to current technologies. At last, we compared our introduced concept to already-existing definitions

of genuine multipartite nonlocality. We finish this paper with some comments and open questions.

Note that in our introduction, we argued that N-partite resource models of correlations should include classical shared randomness. This is motivated by the fact that, for instance, pre-established shared randomness can be stored in classical local memories. We now remark that more general forms of randomness can *a priori* be shared in the same way: For instance, pre-stored quantum states in quantum local memories can, in principle, also simulate a “live" shared random quantum source. Certainly such unlimited quantum local memories are fundamentally more technologically demanding. Nevertheless, we also want to appeal to more foundations arguments for why the storage of many-partite GPT resources should be treated as costly; see, for example, the resource theory of quantum memory developed in Ref. [RBL18]. The trade-off between nonclassical-memory capacity and the resource value of genuinely LOSR multipartite theory-agnostic correlations is a topic we highlight for future research.

The connections between our own definition of causal GPT in networks, which is based on the concepts of causality and device replication, and the standard GPT framework [SB09; SB10; Bar07; CDP11; Jan12] are also left for future work [Pir21].

Motivated by a desire to concretely formulate computational algorithms, we relaxed the set of LOSR theory-agnostic Correlations into the set of *weakly* LOSR theory-agnostic correlations. The question of the differences between these two sets remains open. It might be that a refined version of the argument based on De Finetti's theorem could prove that the two coincide. It might also be that our relaxation is strict and that there exists a correlation that is in the relaxed set without being in the original one. We expect that such approaches will allow to find better noise-tolerant results for practical experimental demonstrations that Nature is not merely genuinely LOSR N-partite nonlocal for low N [ZHW$^+$15; ZBH$^+$19; PPG$^+$19], and will allow to extend our analytical proofs to more quantum states, such as the generalization of the tripartite $|\mathrm{W}\rangle$ state.

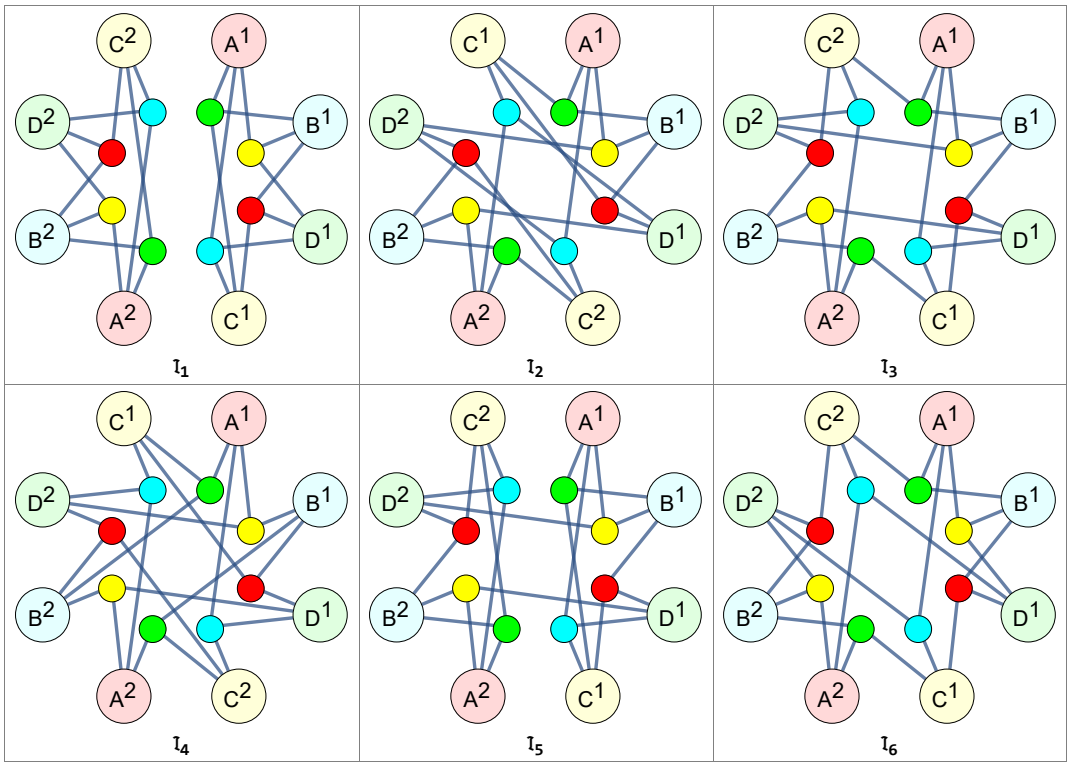


Figure B.1. All nonfanout inflations of order $K = 2$ for the tetrahedron network $\mathscr{N}_4$ (i.e., the network with four 3-way sources). $\mathscr{N}_4$ is composed of parties A (red), B (blue), C (yellow), D (green) and sources of colours (red, blue, green, yellow) such that each party is connected to each source except for the one of his own colour. We represent above the six non-isomorphic inflations $\mathscr{I}_1, ..., \mathscr{I}_6$ (which are of respective multiplicity $1, 3, 3, 1, 12, 12$). Let P be a nonsignalling correlation over A, B, C, D. For P to be a 3-LO theory-agnostic correlation, Definition 67 requires the existence of a correlation $Q^{(1)}, ..., Q^{(6)}$ for each inflated $\mathscr{I}_1, ..., \mathscr{I}_6$ such that $(C1)$, $(C2)$ and $(C3)$ are satisfied. For example:

(C1) implies that $Q^{(1)}{}_{|A^1B^1C^1D^1} = P$ and $Q^{(2)}{}_{|A^1D^2} = P_{|AD}$, but not that $Q^{(2)}{}_{|A^1B^1C^1D^1} = P$.

(C2) implies that every inflation is invariant under the exchange of all copy indices, *e.g.*, $Q_{|A^1,B^1,C^1,D^1,A^2,B^2,C^2,D^2} = Q_{|A^2,B^2,C^2,D^2,A^1,B^1,C^1,D^1}$.

(C3) implies that $Q^{(3)}{}_{|A^1B^1A^2B^2} = Q^{(3)}{}_{|A^1B^1} \cdot Q^{(3)}{}_{|A^2B^2}$.

Note that one can in principle also consider $\mathscr{J} = \mathscr{I}_1, ..., \mathscr{I}_6$, which is a valid inflation of $\mathscr{N}_4$ (but of order $K = 12$) and which implies the existence of a correlation Q of the parties over $\mathscr{J}$ that factorizes as the product $Q^{(1)} \cdot ... \cdot Q^{(6)}$ and satisfies the compatibility conditions imposed by $(C2)$: for instance, it implies $Q^{(3)}_{|A^1B^1C^1A^2B^2C^2} = Q^{(6)}_{|A^1B^1C^1A^2B^2C^2}$.

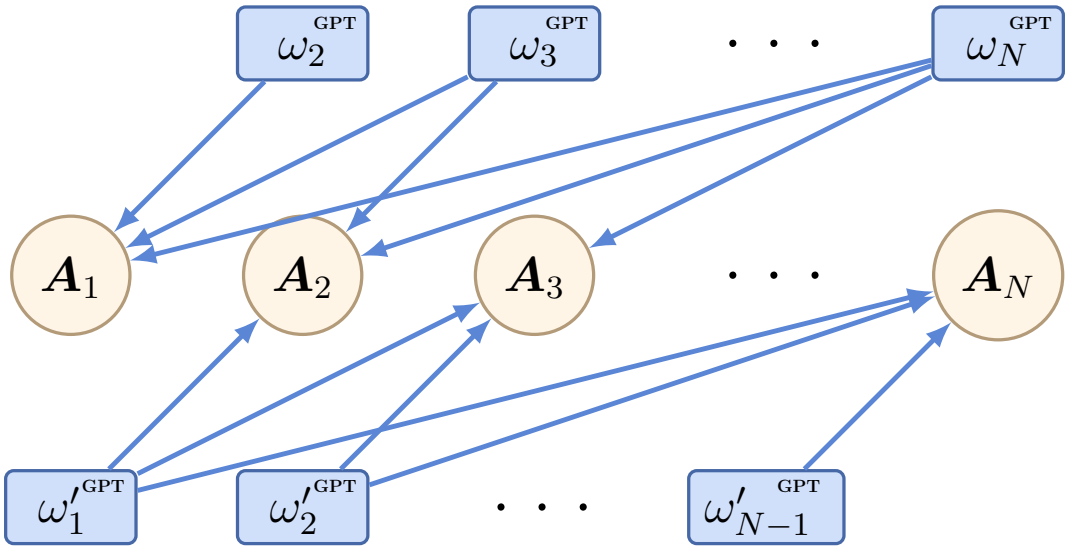


Figure B.2. In this inflation $\mathscr{I}$, each party A_i is connected to the original sources ω_j for $j > i$ and to the cloned sources ω'_j for $j < i$. Assume by contradiction that there exists an arbitrary setup, with some causal GPT, that allows us to simulate a shared random bit in $\mathscr{N}_N$. In $\mathscr{I}$, (C1) imposes that two consecutive parties A_j,A_{j+1} share an identical random bit. This implies that any chain of consecutive parties should all together share the same random bit. In particular, (A_1,A_N) share the same random bit, which is in contradiction with (C2) as they do not have any sources in common.

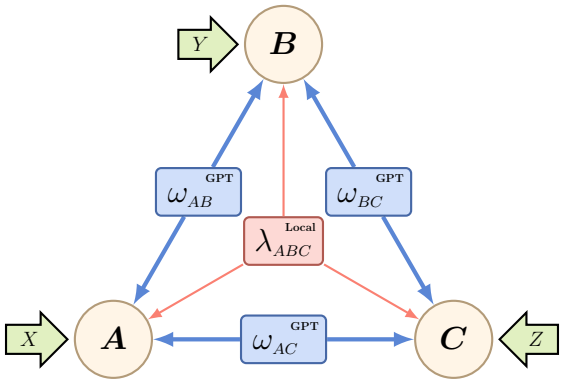


Figure B.3. A tripartite distribution is genuinely tripartite nonlocal according to our Definition 69 if it is not a 2–LOSR theory-agnostic correlation, that is if it cannot be realized by the above scenario, where the output of each player is determined by local operations (such as joint measurements) on 1) its input, 2) the 3-way randomness and 3) 2-way GPT resources.

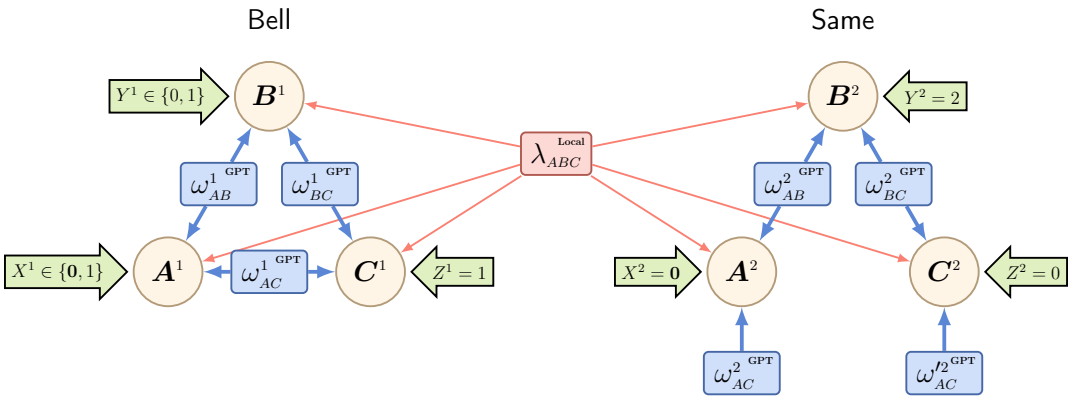


Figure B.4. The inflation technique consists of duplicating and rearranging players, sources, and input distributions. Here we inflate the (non genuinely tripartite-nonlocal) triangle scenario of Figure B.3 as to have the players play two parallel games (Bell and Same). It leads to a contradiction with the statistics of measurements on $|\mathsf{GHZ}\rangle$, and therefore to the conclusion that the $|\mathsf{GHZ}\rangle$ quantum state is a genuinely tripartite-nonlocal resource. The duplicated players are indistinguishable copies of the same abstract process, hence Alice, on input $X{=}\mathbf{0}$, could be playing either game (A_1 and A_2 must have the same behaviour). The only condition on the random inputs is that they be independent from all of the sources. The figure represents a cut of a larger inflation of order 3, consisting of a triangle and a hexagon (three parties of the hexagon are here fully ignored and only the input values relevant for the contradiction are featured).

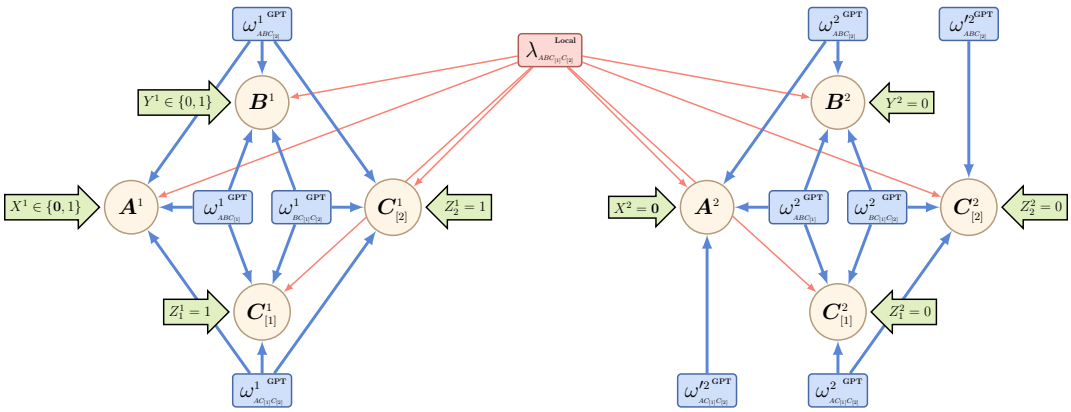


Figure B.5. This 4-party nonfanout inflation cut exposes that the quantum state $\left|\mathsf{GHZ}_4\right\rangle := (|0000\rangle + |1111\rangle)/\sqrt{2}$ is a genuinely 4-partite nonlocal resource.

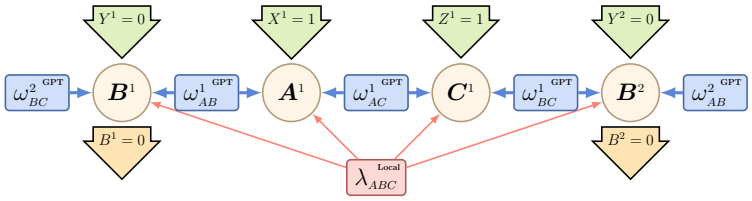


Figure B.6. Sufficient for Lemma 76, this line inflation is in fact a cut of the third-order ring inflation. Given λ, we condition on the output $B^1_\lambda = 0 = B^2_\lambda$ (whenever possible) and it imposes $A^1_\lambda C^1_\lambda \in \{01, 10\}$.

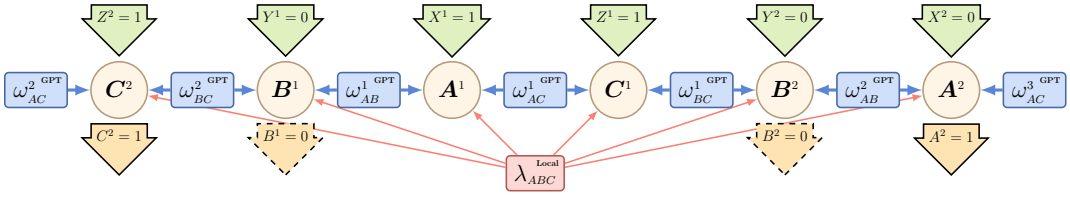


Figure B.7. Representing the second step of the proof of Proposition 75, this line inflation is in fact a cut of the third-order ring inflation. Given λ, we condition on the output $C^2_\lambda = 1 = A^2_\lambda$, which, to simulate without error a distribution in $\{001, 010, 100\}$, forces $B^1_\lambda = 0 = B^2_\lambda$.

Bibliography

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[ADP+14] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín. Elemental and tight monogamy relations in nonsignaling theories. *Phys. Rev. A*, 90:052323, Nov 2014.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804, 1982.

[AFLS15] Antonio Acín, Tobias Fritz, Anthony Leverrier, and Ana Belén Sainz. A combinatorial approach to nonlocality and contextuality. *Communications in Mathematical Physics*, 334(2):533–628, 2015.

[AGM06] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From Bell's Theorem to Secure Quantum Key Distribution. *Phys. Rev. Lett.*, 97(12):120405, Sep 2006.

[AGR81] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981.

[Bar07] Jonathan Barrett. Information processing in generalized probabilistic theories. *Phys. Rev. A*, 75:032304, Mar 2007.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, 1984*, pages 175–179, 1984.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[BBGP13] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. Definitions of multipartite nonlocality. *Phys. Rev. A*, 88:014102, Jul 2013.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[BC90] Samuel L. Braunstein and Carlton M. Caves. Wringing out better Bell inequalities. *Ann. Phys.*, 202(1):22–56, 1990.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014.

[Bel64] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[Ben73] Charles H. Bennett. Logical reversibility of computation. *IBM journal of Research and Development*, 17(6):525–532, 1973.

[Ben82] Charles H. Bennett. The thermodynamics of computation: a review. *International Journal of Theoretical Physics*, 21(12):905–940, 1982.

[Ben87] Charles H. Bennett. Demons, engines and the second law. *Scientific American*, 257(5):108–117, 1987.

[BFRW05] Howard Barnum, Christopher A Fuchs, Joseph M Renes, and Alexander Wilce. Influence-free states on compound quantum systems. *arXiv preprint quant-ph/0507108*, 2005.

[BG21] Jean-Daniel Bancal and Nicolas Gisin. Non-Local Boxes for Networks. *arXiv:2102.03597*, 2021.

[BGP10] C. Branciard, N. Gisin, and S. Pironio. Characterizing the Nonlocal Correlations Created via Entanglement Swapping. *Phys. Rev. Lett.*, 104:170401, Apr 2010.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[Bie20] Peter Bierhorst. Ruling out Bipartite Nonsignaling Nonlocal Models for Tripartite Correlations. *arXiv:2012.11132*, 2020.

[BKP06] Jonathan Barrett, Adrian Kent, and Stefano Pironio. Maximally Nonlocal and Monogamous Quantum Correlations. *Phys. Rev. Lett.*, 97:170409, Oct 2006.

[BLM+05a] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71(2):022101, 2005.

[BLM+05b] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71:022101, Feb 2005.

[BMP18] Cédric Bamps, Serge Massar, and Stefano Pironio. Device-independent randomness generation with sublinear shared quantum resources. *Quantum*, 2:86, August 2018.

[BOGKW19] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 373–410. 2019.

[BR21] Salman Beigi and Marc-Olivier Renou. Covariance Decomposition as a Universal Limit on Correlations in Networks. *arXiv:2103.14840*, 2021.

[BRGP12] Cyril Branciard, Denis Rosset, Nicolas Gisin, and Stefano Pironio. Bilocal versus nonbilocal correlations in entanglement-swapping experiments. *Phys. Rev. A*, 85(3):032119, 2012.

[BRR13] Gilles Brassard and Paul Raymond-Robichaud. Can free will emerge from determinism in quantum theory? In *Is science compatible with free will?*, pages 41–61. Springer, 2013.

[BS93] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, 1993.

[BTF+19] F. Baccari, J. Tura, M. Fadel, A. Aloy, J.-D. Bancal, N. Sangouard, M. Lewenstein, A. Acín, and R. Augusiak. Bell correlation depth in many-body systems. *Phys. Rev. A*, 100:022121, Aug 2019.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge University Press, 2004.

[BW19] Ämin Baumeler and Stefan Wolf. Free energy of a general computation. *Physical Review E*, 100(5):052115, 2019.

[CAF06] Kai Chen, Sergio Albeverio, and Shao-Ming Fei. Two-setting Bell inequalities for many qubits. *Phys. Rev. A*, 74:050101, Nov 2006.

[CCAA12] R. Chaves, D. Cavalcanti, L. Aolita, and A. Acín. Multipartite quantum nonlocality under local decoherence. *Phys. Rev. A*, 86:012108, Jul 2012.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 493–502. IEEE, 1998.

[CDP11] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Informational derivation of quantum theory. *Phys. Rev. A*, 84:012311, Jul 2011.

[CGL15] Florian John Curchod, Nicolas Gisin, and Yeong-Cherng Liang. Quantifying multipartite nonlocality via the size of the resource. *Phys. Rev. A*, 91:012121, Jan 2015.

[Cha75] Gregory J. Chaitin. A theory of program size formally identical to information theory. *Journal of the ACM (JACM)*, 22(3):329–340, 1975.

[Chi14] Giulio Chiribella. Dilation of states and processes in operational-probabilistic theories. *E. Proc. Theo. Comp. Sci.*, 172:1?14, Dec 2014.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[Cir80] Boris S. Cirel'son. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4(2):93–100, 1980.

[CK78] Imre Csiszár and Janos Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *FOCS*, volume 88, pages 42–52, 1988.

[Col07] Roger Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76(6):062308, 2007.

[CR17] R. Chao and B. W. Reichardt. Test to separate quantum theory from non-signaling theories. *arXiv:1706.02008*, June 2017.

[CRC19] Xavier Coiteux-Roy and Claude Crépeau. The RGB no-signalling game. In *14th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2019.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 350–354. Springer, 1987.

[Cré97] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 306–317. Springer, 1997.

[CRW19] Xavier Coiteux-Roy and Stefan Wolf. Proving erasure. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 832–836. IEEE, 2019.

[CRW22] Xavier Coiteux-Roy and Stefan Wolf. Key agreement and oblivious transfer from free-energy limitations, 2022.

[CRWR21a] Xavier Coiteux-Roy, Elie Wolfe, and Marc-Olivier Renou. Any physical theory of nature must be boundlessly multipartite nonlocal. *Physical Review A*, 104, Nov 2021.

[CRWR21b] Xavier Coiteux-Roy, Elie Wolfe, and Marc-Olivier Renou. No bipartite-nonlocal causal theory can explain nature's correlations. *Phys. Rev. Lett.*, 127, Nov 2021.

[CRZ+22] Huan Cao, Marc-Olivier Renou, Chao Zhang, Gaël Massé, Xavier Coiteux-Roy, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, and Elie Wolfe. Experimental demonstration that no tripartite-nonlocal causal theory explains nature's correlations. *arXiv preprint arXiv:2201.12754*, 2022.

[CTPdV21] Patricia Contreras-Tejada, Carlos Palazuelos, and Julio I. de Vicente. Genuine Multipartite Nonlocality Is Intrinsic to Quantum Networks. *Phys. Rev. Lett.*, 126:040501, Jan 2021.

[CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[Deu85] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[DFSS08] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[DGH+07] Frédéric Dupuis, Nicolas Gisin, Avinatan Hasidim, André Allan Méthot, and Haran Pilpel. No nonlocal box is universal. *Journal of mathematical physics*, 48(8):082107, 2007.

[DHRS04] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-round oblivious transfer in the bounded storage model. In *Theory of Cryptography Conference*, pages 446–472. Springer, 2004.

[DM02] Stefan Dziembowski and Ueli Maurer. Tight security proofs for the bounded-storage model. In *Proceedings of the thiry-fourth annual ACM Symposium on Theory of Computing*, pages 341–350, 2002.

[DM04] Stefan Dziembowski and Ueli Maurer. On generating the initial key in the bounded-storage model. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 126–137. Springer, 2004.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661, 1991.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[FC72] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14):938, 1972.

[FDOR15] Philippe Faist, Frédéric Dupuis, Jonathan Oppenheim, and Renato Renner. The minimal work cost of information processing. *Nature communications*, 6(1):1–8, 2015.

[Fri12] Tobias Fritz. Beyond Bell's theorem: correlation scenarios. *New J. Phys.*, 14(10):103001, 2012.

[FT82] Edward Fredkin and Tommaso Toffoli. Conservative logic. *International Journal of theoretical physics*, 21(3):219–253, 1982.

[FW11] Manuel Forster and Stefan Wolf. Bipartite units of nonlocality. *Physical Review A*, 84(4):042112, 2011.

[G+15] Marissa Giustina et al. Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[GBC+20] Nicolas Gisin, Jean-Daniel Bancal, Yu Cai, Patrick Remy, Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Sandu Popescu, and Nicolas Brunner. Constraints on nonlocality in networks from no-signaling and independence. *Nature Comm.*, 11(1):2378, May 2020.

[GHSZ90] Daniel M. Greenberger, Michael A. Horne, Abner Shimony, and Anton Zeilinger. Bell?s theorem without inequalities. *Am. J. Phys.*, 58(12):1131–1143, 1990.

[GVW+15] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Physical Review Letters*, 115(25):250401, 2015.

[GWAN12] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués. Operational Framework for Nonlocality. *Phys. Rev. Lett.*, 109:070401, Aug 2012.

[H+15] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[HBD+15] Bas Hensen, Hannes Bernien, Anaïs E Dréau, Andreas Reiserer, Norbert Kalb, Machiel S. Blok, Just Ruitenberg, Raymond FL. Vermeulen, Raymond N. Schouten, Carlos Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[HGJ+22] Liang Huang, Xue-Mei Gu, Yang-Fan Jiang, Dian Wu, Bing Bai, Ming-Cheng Chen, Qi-Chao Sun, Jun Zhang, Sixia Yu, Qiang Zhang, et al. Nature's nonlocality must be boundlessly multipartite: an experimental demonstration under strict locality condition. *arXiv preprint arXiv:2203.00889*, 2022.

[HILL93] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Construction of a pseudo-random generator from any one-way function. In *SIAM Journal on Computing*, 1993.

[HLP14] Joe Henson, Raymond Lal, and Matthew F. Pusey. Theory-independent limits on correlations from generalized Bayesian networks. *New J. Phys.*, 16(11):113043, 2014.

[HRW] Esther Hänggi, Renato Renner, and Stefan Wolf. Efficient device-independent quantum key distribution. *EUROCRYPT 2010*, pages 216–234.

[HS03] Norbert Hungerbühler and Michael Struwe. A one-way function from thermodynamics and applications to cryptography. *Elemente der Mathematik*, 58(2):49–64, 2003.

[HSH+14] Deny R. Hamel, Lynden K. Shalm, Hannes Hübel, Aaron J. Miller, Francesco Marsili, Varun B. Verma, Richard P. Mirin, Sae Woo Nam, Kevin J. Resch, and Thomas Jennewein. Direct generation of three-photon polarization entanglement. *Nature Photonics*, 8(10):801?807, Sep 2014.

[Hud18] J. Hudson. Could someone explain quantum entanglement to me like I'm 5 years old. Quora, May 2018. `https://www.quora.com/Could-someone-explain-quantum-entanglement-to-me-like-Im-5-years-old`.

[IKP+08] Tsuyoshi Ito, Hirotada Kobayashi, Daniel Preda, Xiaoming Sun, and Andrew C-C Yao. Generalized tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 187–198. IEEE, 2008.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM Symposium on Theory of Computing*, pages 12–24, 1989.

[Jan12] Peter Janotta. Generalizations of Boxworld. *Proc. Theo. Comp. Sci.*, 95:183?192, Oct 2012.

[Ken99] Adrian Kent. Unconditionally secure bit commitment. *Physical Review Letters*, 83(7):1447, 1999.

[Kil88] Joe Kilian. Founding crytpography on oblivious transfer. In *Proceedings of the twentieth annual ACM Symposium on Theory of Computing*, pages 20–31, 1988.

[KR11] Robert König and Renato Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory*, 57(7):4760–4787, 2011.

[KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347, 2009.

[KWW12] Robert König, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[Lan61] Rolf Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[LV+08] Ming Li, Paul Vitányi, et al. *An introduction to Kolmogorov complexity and its applications*, volume 3. Springer, 2008.

[Mau92] Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[Mau93] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414, 1997.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373, 1990.

[MLYF22] Ya-Li Mao, Zheng-Da Li, Sixia Yu, and Jingyun Fan. Test of genuine multipartite nonlocality in network. *arXiv preprint arXiv:2201.12753*, 2022.

[MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2(1):1–7, 2011.

[MW96] Ueli Maurer and Stefan Wolf. Towards characterizing when information-theoretic secret key agreement is possible. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 196–209. Springer, 1996.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proc. 39th Symposium on Foundations of Computer Science*, pages 503–509, 1998. (Cat. No.98CB36280).

[NW20] Miguel Navascués and Elie Wolfe. The Inflation Technique Completely Solves the Causal Compatibility Problem. *J. Caus. Inf.*, 8(1):70–91, September 2020.

[NWRPK20] Miguel Navascués, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens. Genuine Network Multipartite Entanglement. *Phys. Rev. Lett.*, 125:240505, Dec 2020.

[P+10] S. Pironio et al. Random numbers certified by Bell?s theorem. *Nature*, 464(7291):1021–1024, 2010.

[PBS11] Stefano Pironio, Jean-Daniel Bancal, and Valerio Scarani. Extremal correlations of the tripartite no-signaling polytope. *J. Phys. A*, 44(6):065303, 2011.

[Pea70] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970.

[Pea09] Judea Pearl. *Causality: Models, Reasoning, and Inference*. Cambridge University Press, 2009.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.

[Pir05] Stefano Pironio. Lifting Bell inequalities. *J. Math. Phys.*, 46(6):062112, 2005.

[Pir21] Stefano Pironio. In Preparation, 2021.

[PPG+19] Massimiliano Proietti, Alexander Pickston, Francesco Graffitti, Peter Barrow, Dmytro Kundys, Cyril Branciard, Martin Ringbauer, and Alessandro Fedrizzi. Experimental test of local observer independence. *Science Advances*, 5(9):eaaw9832, Sep 2019.

[PR94] S. Popescu and D. Rohrlich. Quantum Nonlocality as an Axiom. *Found. Phys.*, 24(3):379–385, 1994.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. *Technical Memo TR-81*, 1981.

[RAF16] Thomas Vidick Rotem Arnon-Friedman, Renato Renner. Simple and tight device-independent security proofs. *arXiv:1607.01797*, 2016.

[RBB+19] Marc-Olivier Renou, Elisa Bäumer, Sadra Boreiri, Nicolas Brunner, Nicolas Gisin, and Salman Beigi. Genuine Quantum Nonlocality in the Triangle Network. *Phys. Rev. Lett.*, 123:140401, Sep 2019.

[RBG+17] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes. *Phys. Rev. Lett.*, 119:010402, Jul 2017.

[RBL18] Denis Rosset, Francesco Buscemi, and Yeong-Cherng Liang. Resource Theory of Quantum Memories and Their Faithful Verification with Minimal Assumptions. *Phys. Rev. X*, 8:021033, May 2018.

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference*, pages 407–425. Springer, 2005.

[RW04] Renato Renner and Stefan Wolf. Smooth Rényi entropy and applications. In *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, page 233. IEEE, 2004.

[RW05] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *International conference on the theory and application of cryptology and information security*, pages 199–216. Springer, 2005.

[S+15] Lynden K. Shalm et al. Strong Loophole-Free Test of Local Realism. *Phys. Rev. Lett.*, 115:250402, 2015.

[SB09] Paul Skrzypczyk and Nicolas Brunner. Couplers for non-locality swapping. *New J. Phys.*, 11(7):073014, 2009.

[SB10] Anthony J. Short and Jonathan Barrett. Strong nonlocality: a trade-off between states and measurements. *New J. Phys.*, 12(3):033034, 2010.

[Sca06] Valerio Scarani. Feats, Features and Failures of the PR-box. In *AIP Conference Proceedings*. AIP, 2006.

[SFK+20] David Schmid, Thomas C. Fraser, Ravi Kunjwal, Ana Belen Sainz, Elie Wolfe, and Robert W. Spekkens. Understanding the interplay of

entanglement and nonlocality: motivating and developing a new branch of entanglement theory. *arXiv:2004.09194*, 2020.

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, et al. Strong loophole-free test of local realism. *Physical Review Letters*, 115(25):250402, 2015.

[SU01] Michael Seevinck and Jos Uffink. Sufficient conditions for three-particle entanglement and their tests in recent experiments. *Phys. Rev. A*, 65:012107, Dec 2001.

[SU08] Michael Seevinck and Jos Uffink. Partial separability and entanglement criteria for multiqubit quantum states. *Phys. Rev. A*, 78:032101, Sep 2008.

[Sve87] George Svetlichny. Distinguishing three-body from two-body nonseparability by a Bell-type inequality. *Phys. Rev. D*, 35:3066–3069, May 1987.

[SZCG20] Kuntal Sengupta, Rana Zibakhsh, Eric Chitambar, and Gilad Gour. Quantum Bell Nonlocality is Entanglement. *arXiv:2012.06918*, 2020.

[TBZG98] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell Inequalities by Photons More Than 10 km Apart. *Phys. Rev. Lett.*, 81:3563–3566, Oct 1998.

[TPKLR21] Armin Tavakoli, Alejandro Pozas-Kerstjens, Ming-Xing Luo, and Marc-Olivier Renou. Bell nonlocality in networks, 2021.

[TSSR11] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[Vad04] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004.

[VD13] Wim Van Dam. Implausible consequences of superstrong nonlocality. *Natural Computing*, 12(1):9–12, 2013.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113:140501, Sep 2014.

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[WC20] Mirjam Weilenmann and Roger Colbeck. Self-Testing of Physical Theories, or, Is Quantum Theory Optimal with Respect to Some Information-Processing Task? *Phys. Rev. Lett.*, 125:060406, Aug 2020.

[Weh06] Stephanie Wehner. Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities. *Physical Review A*, 73(2):022110, 2006.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[WPKG+21] Elie Wolfe, Alejandro Pozas-Kerstjens, Matan Grinberg, Denis Rosset, Antonio Acín, and Miguel Navascués. Quantum Inflation: A General Approach to Quantum Causal Compatibility. *Phys. Rev. X*, 11:021043, May 2021.

[WSF19] Elie Wolfe, Robert W. Spekkens, and Tobias Fritz. The Inflation Technique for Causal Inference with Latent Variables. *J. Causal Inference*, 7(2):0020, Sep 2019.

[WSS+20] Elie Wolfe, David Schmid, Ana Belén Sainz, Ravi Kunjwal, and Robert W. Spekkens. Quantifying Bell: the Resource Theory of Nonclassicality of Common-Cause Boxes. *Quantum*, 4:280, June 2020.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, Aug 2001.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[ZBH+19] Chao Zhang, Thomas R. Bromley, Yun-Feng Huang, Huan Cao, Wei-Min Lv, Bi-Heng Liu, Chuan-Feng Li, Guang-Can Guo, Marco Cianciaruso, and Gerardo Adesso. Demonstrating Quantum Coherence

and Metrology that is Resilient to Transversal Noise. *Phys. Rev. Lett.*, 123:180504, Nov 2019.

[ZHW+15] Chao Zhang, Yun-Feng Huang, Zhao Wang, Bi-Heng Liu, Chuan-Feng Li, and Guang-Can Guo. Experimental Greenberger-Horne-Zeilinger-Type Six-Photon Quantum Nonlocality. *Phys. Rev. Lett.*, 115:260402, Dec 2015.