Graphical Methods in Device-Independent Quantum Cryptography

Spencer Breiner,[1] Carl A. Miller,[1,2] and Neil J. Ross[2,3]
[1]National Institute of Standards and Technology (NIST)
Gaithersburg, MD 20899, USA
[2]Joint Center for Quantum Information and Computer Science (QuICS)
University of Maryland, College Park, MD 20742, USA
[3]Department of Mathematics and Statistics
Dalhousie University, Halifax, NS B3H 4R2, Canada

We introduce a framework for graphical security proofs in device-independent quantum cryptography using the methods of categorical quantum mechanics. We are optimistic that this approach will make some of the highly complex proofs in quantum cryptography more accessible, facilitate the discovery of new proofs, and enable automated proof verification. As an example of our framework, we reprove a previous result from device-independent quantum cryptography: any linear randomness expansion protocol can be converted into an unbounded randomness expansion protocol. We give a graphical proof of this result, and implement part of it in the Globular proof assistant.

1 Introduction

Graphical methods have long been used in the study of physics and computation. In physics, this can be traced back at least as far as Penrose's use of diagrams [1]. During the last decade of the twentieth century, rigorous methods for graphical reasoning in monoidal categories were developed by Joyal, Street, and others [2, 3]. When Abramsky and Coecke proposed monoidal categories as an alternative foundation for quantum physics [4], they were able to draw from these technical developments to introduce an elaborate graphical language for reasoning about quantum mechanical concepts. Since then, the use of rigorous graphical methods has been extended widely, ranging from foundations [4] to quantum algorithms [5], quantum error correction [6], and beyond [7, 8]. The great success of graphical methods in the quantum sciences is largely due to their ability to deal with elaborate concepts in a simple way. This is especially true when compared to the standard methods involving linear operators acting on Hilbert space.

Quantum cryptography, the study of cryptographic protocols that are based on quantum mechanical principles (see Section 12.6 of [9] for an introduction) is an ideal candidate for graphical analysis. Indeed, proofs in quantum cryptography are often long and complicated even when the central idea of the proof is relatively clear. Pictures are regularly used as a conceptual aid in discussions of quantum cryptography, but it would be beneficial for both accessibility and rigor if proofs themselves could be expressed as pictures. For this reason, we believe that the field of quantum cryptography can benefit from the abstract methods of categorical quantum mechanics [8].

To our knowledge the use of graphical methods to formalize quantum cryptography is fairly new, although the literature provides some useful beginnings. Graphical security proofs for quantum key distribution (one of the original problems in the field) have been presented in [10–12], although these are not yet at the level of security that has been proved through non-graphical means. Meanwhile, the literature has a number of formal treatments of cryptography that are not primarily based on graphical reasoning. An important

example is [13], which has a focus similar to the current paper. See also [14–17].

One of the recent major achievements of quantum cryptography is the development of *device-independent* security proofs [18]. In such proofs, not only the adversary but also the quantum devices are untrusted, and allowed to exhibit uncharacterized behavior. Protocols in this field always include a classical test of the quantum devices which lead to a "succeed" or "abort" event at the end of the protocol, and we must prove that if the protocol "succeeds," then the desired cryptographic task has been securely carried out. Device-independence is a desirable level of security for quantum cryptography (in particular because it accounts for arbitrary noise or imperfection in the quantum hardware) and it will be our focus in this paper.

As a specific problem to study, we consider *device-independent randomness expansion*. Research over the last decade has led to a proof that random numbers can be generated with devices that are completely untrusted [13, 19–30]. Precisely, two untrusted quantum devices, together with a perfectly random seed of length N, can be manipulated by a classical user to generate a perfectly random output of size $f(N) > N$ with negligible error. See [31] for a gentle introduction to this topic and [32] for a discussion of a possible implementation.

Going further, it has been proved that one can take two copies of such a randomness expansion protocol (using different pairs of devices for each copy) and cross-feed them to produce an *arbitrarily large* quantity of random bits from a fixed-length seed [13, 23, 28]. Proving that randomness expansion can be extended in this way is not easy (indeed, the paper containing the first proof of unbounded expansion [33] was 34 pages long). Here, we give a proof of this extension (based on [13, 28]) using a graphical language. Explicitly, we prove that any secure protocol for linear randomness expansion implies a secure protocol for unbounded randomness expansion. The proof is based on formal graphical reasoning and is fairly compact.

A great benefit of graphical proofs is they are amenable to computer verification. The Globular proof assistant software [34] carries out category-theoretic proofs, using diagrams that are easily compatible with graphical languages for quantum mechanics. To further demonstrate the utility of our work we implemented the proof of unbounded randomness expansion in Globular. The proof is available as a video at [35].

This paper is organized as follows. In Section 2 we formalize a language to deal with quantum processes, building on the diagrammatic language given [36, 37]. Section 3 provides the formal basis for quantum cryptographic protocols that are based on untrusted devices. In Section 4 we give the proof that linear randomness expansion implies unbounded randomness expansion, and comment on our use of computer-assisted proof software. We conclude and discuss future work in Section 5.

The recent paper [38] also addresses graphical proofs of quantum cryptography, albeit with a different focus (device-dependent quantum key distribution). The graphical concepts in the present paper and in [38] were developed independently, and we expect that there will be a useful synergy between the two papers.

1.1 Our contributions

The graphical language used in this paper is based primarily on [36, 37]. We added new elements to enable quantum cryptographic proofs. Here are some of the additions:

1. **Diagrams for sets of processes.** Whereas a diagram in the language of [36, 37] represents a quantum process, we expanded this to allow diagrams with uncharacterized elements to represent *sets* of processes. This is especially useful in the device-independent context for expressing security statements (see Definition 2.2).

2. **Approximations.** We use the symbol $=_\epsilon$ when the state represented by one diagram is approximately equal to the state represented by another. This allows proofs via chains of approximations. A similar feature was independently used in [38].

3. **Duplication of states.** We define the "duplication" of a classical-quantum state (see Section 2.3), a convenient shorthand which subsumes both the copying of classical states and the purification of quantum states.

4. **A graphical formalization of device-independence.** We give a graphical formalization of what it means for a protocol to be device-independent (Section 3.2).

2 Fundamentals

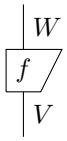
In this section, we cover useful graphical techniques and concepts, building on [36, 37]. First, we describe the graphical language of categorical quantum mechanics. Next, we introduce a notion of distance between diagrams. Finally, we define the process of duplicating states. For further details the reader is encouraged to consult [36, 37] or the more recent [8] for categorical quantum mechanics, and [39] for notions of distance relevant to quantum information theory.

2.1 The graphical language of categorical quantum mechanics

Throughout, $\mathcal{O}$ denotes a collection of finite-dimensional Hilbert spaces, each with a fixed orthonormal basis. We use Dirac notation when it is convenient: for any $V \in \mathcal{O}$, we denote the fixed orthonormal basis by $\{|1\rangle_V, |2\rangle_V, \ldots\}$ (with the subscript V typically dropped). For any $v \in V$, the expression $|v\rangle$ is simply another way of writing the vector v, and $\langle v|$ denotes the dual of v.

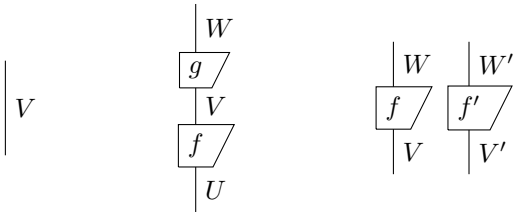
We assume that $\mathcal{O}$ is closed under tensor products (i.e., if $V, W \in \mathcal{O}$ then $V \otimes W = VW \in \mathcal{O}$) and contains the space $\mathbb{C}^n$ for every non-negative integer n. We sometimes refer to the elements of $\mathcal{O}$ as *types* or *registers*. The elements of $\mathcal{O}$ are the objects of the category in which our graphical reasoning takes place. We refer the reader to [8] for further details. To simplify the notation in our diagrams, we sometimes write N to represent the N-bit quantum register $\mathbb{C}^{2^N}$.

We say that f is a *process of type* $V \to W$ if f is a linear operator whose domain is V and whose codomain is W. It is represented by a box labeled f whose input and output wires are labeled with the types V and W as follows.



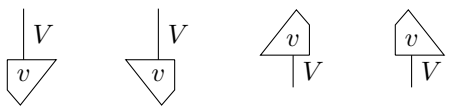
(1)

Note that diagrams are read from bottom to top. The identity operator is a process represented by a box-less diagram (below, left). The composition and tensor product of processes are respectively represented by the vertical and horizontal composition of diagrams (below, center and right).



(2)

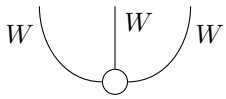
Note that two processes can be vertically composed only if their types are compatible. A process with no input wires is a *state*. A state v of type V should be interpreted as a vector in V and is represented by the first diagram on the left below. The conjugate, transpose, and conjugate-transpose (i.e., adjoint) of v are also depicted below (second, third, and fourth diagram respectively).



(3)

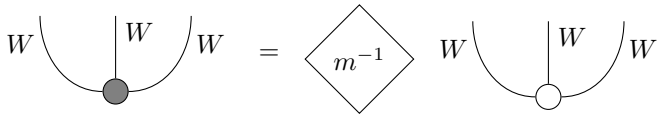
A process with no output wires is called an *effect*. A process with no input and no output is a *number*, and is represented by a diamond whose label indicates its value.

Let W be a register. Then the diagram



(4)

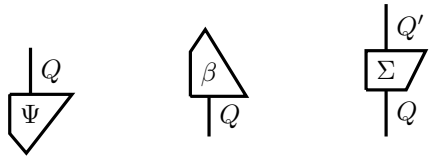
denotes the vector $\sum_{i=1}^{\dim W} |i\rangle \otimes |i\rangle \otimes |i\rangle \in W \otimes W \otimes W$ and is called a *spider*. Spiders can have an arbitrary number of outgoing wires (with all of the wires being of the same type, and the definition extending in the obvious way). Because they will play an important role below, we will also introduce the *uniform vector*, which is denoted by a gray node:



(5)

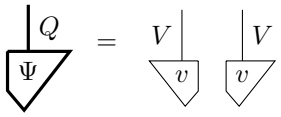
where $m = \dim W$. The diagram on the left-hand side of (5) denotes the vector $\frac{1}{m}\sum_{i=1}^{m} |i\rangle \otimes |i\rangle \otimes |i\rangle \in W \otimes W \otimes W$.

A *quantum* type, or quantum register, is an element Q of $\mathcal{O}$ of the form $Q = V \otimes V$. To graphically distinguish them for their classical counterparts, quantum states, effects, and processes are drawn with thick lines as in the diagrams below.



(6)

A *pure quantum state* Ψ is a state of the form $v \otimes \overline{v}$ with $\|v\| = 1$. Graphically, a quantum state is pure if it satisfies the diagrammatic equality below.



(7)

A *mixed quantum state* of Q is a state of the form $\sum_i v_i \otimes \overline{v_i}$ satisfying $\sum_i \|v_i\|^2 = 1$. A *subnormalized mixed state* is only required to satisfy $\sum_i \|v_i\|^2 \leq 1$. Unless otherwise specified, the word "state" refers to a normalized mixed state.

The above definition can be related to more conventional notation for quantum states (see, e.g., [39]) as follows. If

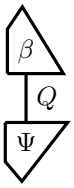
$$\sum_{ij} c_{ij} |i\rangle \langle j| \tag{8}$$

is a density operator on the vector space V which represents a quantum state in the conventional sense, then the corresponding quantum state in the notation that we are using is given by

$$\sum_{ij} c_{ij} |i\rangle \otimes |j\rangle \in V \otimes V. \tag{9}$$

The main difference between (8) and (9) is that (8) is a linear map from V to V, while (9) is simply an element of $Q = V \otimes V$.

A linear map $Q \to \mathbb{C}$ is a *quantum effect* if it maps all states to the interval $[0, 1]$. In other words, β is a quantum effect if



$\in [0, 1]$ (10)

for all quantum states Ψ of Q. Effects correspond to positive semidefinite operators on Q with operator norm less than or equal to one. The effect $Q \to \mathbb{C}$ given by $\sum_{ij} w_{ij} |ij\rangle \mapsto \sum_i w_{ii}$ is denoted by the diagram below

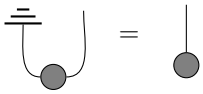
(11)

and corresponds to taking the trace of a linear operator. If V is a classical register then

(12)

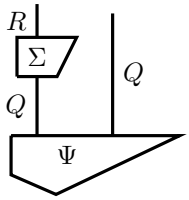
denotes the linear map $V \to \mathbb{C}$ given by $\sum_i v_i |i\rangle \mapsto \sum_i v_i$.

For use in later proofs, we note the obvious fact that uniform states absorb terminations, i.e.,



(13)

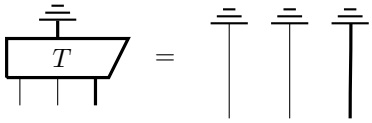
A *causal quantum process* Σ from a register Q to a register R is a linear homomorphism such that for any state Ψ of $Q \otimes Q$, the diagram below represents a state.



(14)

A *stochastic* quantum process is one that satisfies the same condition, with the weaker requirement that the diagram above is a subnormalized quantum state. Intuitively, a causal process is a process that always gives an outcome, while a stochastic process is a process that may sometimes "fail" and give no outcome (hence the trace of its output state may be smaller than the trace of its input state). Unless otherwise specified, the phrase "quantum process" refers to a stochastic quantum process.

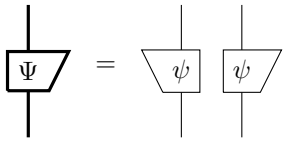
Diagrammatically, a process is causal if and only if the process of applying T and then discarding its output wires is equal to the process of merely discarding the input wires, e.g.,



(15)

Causal quantum processes correspond to completely positive trace-preserving maps in the conventional notation.

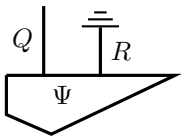
A *pure process* is a quantum process of the form



(16)

Note that pure processes map pure subnormalized states to pure subnormalized states.

If Ψ is a state of QR, then we can terminate one of its wires and obtain a state of Q:

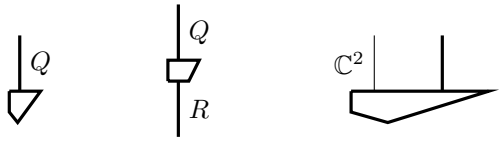


(17)

(This corresponds to taking a partial trace in the conventional framework.)

If C is a register, then a *classical* state is a vector $v \in C$ of the form $v = \sum_i p_i |i\rangle$, where $\{p_i\}_i$ is a probability distribution. If Q is a quantum register, then a *classical-quantum* state of CQ is a state of the form $\sum_i p_i |i\rangle \otimes v_i$, where $\{p_i\}_i$ is a probability distribution and each v_i is a normalized state of Q. A quantum process on CQ that is *controlled* by the classical register C is a process of the form $\sum_i |i\rangle\langle i| \otimes \Phi_i$, where each Φ_i is a process on Q.

In our context, it will be useful to represent *sets* of linear maps diagrammatically. A diagram in which every element is specified by an explicit linear map can itself be regarded a linear map (obtained by composition and tensor product). A diagram in which some elements are unspecified represents the set of all specifications of that form. For example, the following diagrams



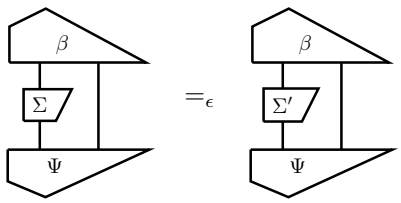
(18)

represent, respectively, the set of all (normalized, mixed) states on Q, the set of all stochastic quantum processes $R \to Q$, and the set of all classical-quantum states in which the classical register is $\mathbb{C}^2$ and the quantum register can be arbitrary. Notice that when a wire is unlabeled and otherwise unspecified, the quantification ranges over all (quantum or classical) registers. Similarly, the diagram $\diamond$ represents an arbitrary element of the interval $[0, 1]$.

2.2 Approximations

In what follows, we will need to be able to discuss the *distance* between certain processes. We therefore define a relation between diagrams which captures the appropriate metric (half of the diamond norm distance — see [39] for further details).

Definition 2.1. *If c, d, and ϵ are real numbers, we write $c =_\epsilon d$ if $|c - d| \leq \epsilon$. Let Σ and Σ' be two processes of the same type. Then, we write $\Sigma =_\epsilon \Sigma'$ if for all states Ψ and effects β,*



(19)

Note that the above definition remains equivalent if the phrase "for all states Ψ" is replaced by "for all pure states Ψ."

It follows from the definition that the notion of approximation defined above satisfies the triangle inequality (if $\Sigma =_\epsilon \Sigma'$ and $\Sigma' =_\delta \Sigma''$, then $\Sigma =_{\epsilon+\delta} \Sigma''$) and that it is preserved by composition (if $\Sigma =_\epsilon \Sigma'$, then $\Theta \circ \Sigma =_\epsilon \Theta \circ \Sigma'$ and $\Sigma \circ \Lambda = \Sigma' \circ \Lambda$ for all stochastic processes Θ, Λ of appropriate input and output

type). If we restrict the processes Σ and Σ' to be states (i.e., to have no inputs) then $\Sigma =_\epsilon \Sigma'$ if and only if Σ and Σ' differ by no more than 2ϵ in trace distance.

We now generalize the notion of distance between processes to a notion of distance between *sets* of processes. A similar notion of approximation appears in the non-graphical formalism of [15].

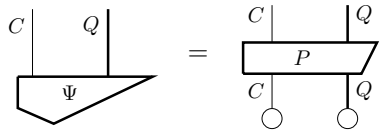
Definition 2.2. *Let A and B be two sets of processes, all of which have the same type. We write $A \subseteq_\epsilon B$ if for every $a \in A$, there exists $b \in B$ such that $a =_\epsilon b$. Moreover, we write $A =_\epsilon B$ if $B \subseteq_\epsilon A$ and $A \subseteq_\epsilon B$.*

These relations also satisfy a triangle inequality: if $A \subseteq_\epsilon B$ and $B \subseteq_\delta C$, then $A \subseteq_{\epsilon+\delta} C$. Note that the symbol $=_\epsilon$ is used to denote a relation between numbers, a relation between processes, and a relation between sets of processes. However, it will always be clear from the context whether numbers, processes, or sets of processes are being compared so that no ambiguity should arise from this slight abuse of notation.

2.3 Duplication

We now introduce the notion of *duplicate* states. Informally speaking, duplicating a classical-quantum state means copying its classical component and purifying its quantum component. See section 2.5 of [9] for a discussion of the notion of quantum state purification.

If Ψ is a subnormalized classical-quantum state of a register CQ, then we can write $\Psi = \sum_{ijk} \psi_{ij}^k |k\rangle \otimes |i\rangle \otimes |j\rangle \in C \otimes V \otimes V$, where $Q = V \otimes V$. The matrices $M_k := [\psi_{ij}^k]_{ij}$ are then positive semidefinite. We can alternatively express Ψ as

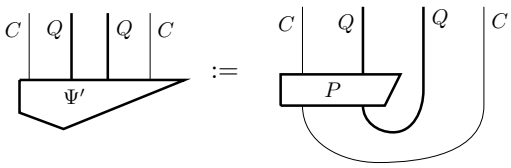


(20)

where P is the linear map defined by

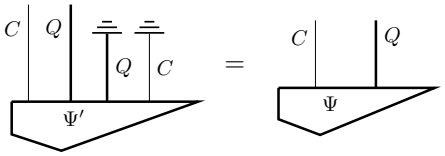
$$P(|k\rangle \otimes |i\rangle \otimes |j\rangle) = |k\rangle \otimes \sqrt{M_k}\,|i\rangle \otimes \overline{\sqrt{M_k}}\,|j\rangle\,. \tag{21}$$

Then, the *canonical duplicate state* of Ψ is given by



(22)

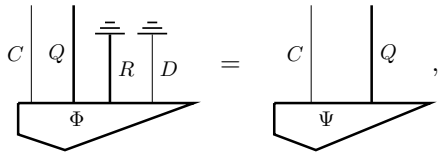
See equation (59) in the appendix for an expression for this state in conventional notation. Note that



(23)

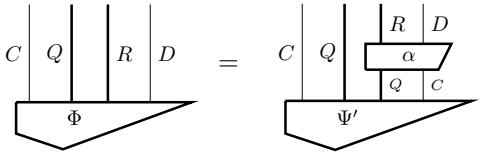
More generally, a state Ψ'' of $CQQC$ is a *duplicate state* (or simply *duplication*) of Ψ if (23) holds (with Ψ' replaced by Ψ'') and Ψ'' has the form $\Psi'' = \sum_i |i\rangle \otimes \psi_i \otimes |i\rangle$, where each ψ_i is a pure subnormalized state of QQ. Note that if $\psi = \sum_i p_i |i\rangle$ is a classical state (with no quantum component), then there is only one duplicate of ψ, and that is the "copied" state $\sum_i p_i |i\rangle \otimes |i\rangle$.

Duplicate states have the following universality property: for any subnormalized classical-quantum state Φ of $CQRD$, where R is a quantum register and D is a classical register, such that



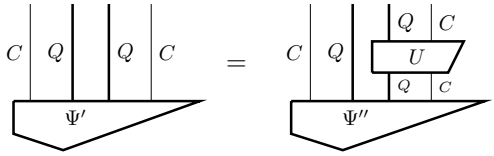
(24)

there exists a causal process α from QC to RD satisfying



(25)

Additionally, if Ψ' and Ψ'' are any two states of $CQQC$ that are both duplicate states of Ψ, then there exists a unitary operator U on QC, controlled by the register C, such that



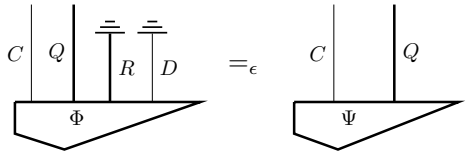
(26)

The following proposition follows from standard techniques and is proved in Appendix A.

Proposition 2.3. *If Ψ, Φ are subnormalized states that satisfy $\Psi =_\epsilon \Phi$, and Ψ', Φ' denote their respective canonical duplicate states, then $\Psi' =_{\sqrt{2\epsilon}} \Phi'$.* □

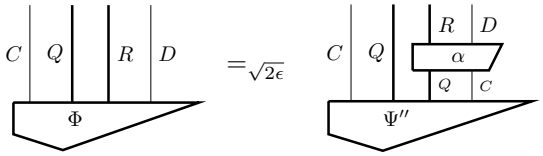
The next corollary will be useful in later proofs.

Corollary 2.4. *Suppose that*



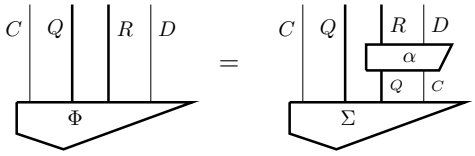
(27)

and let Ψ'' be a state on $CQQC$ that is a duplicate of Ψ. Then, there exists a causal process α from QC to RD satisfying



(28)

Proof. Let Ψ' denote the canonical duplicate state of Ψ. By the property noted in equation (26) above, it suffices to prove the desired relation (28) with Ψ'' replaced by Ψ'. By Proposition 2.3, the canonical duplicate state Σ of the state on the left side of (27) satisfies $\Sigma =_{\sqrt{2\epsilon}} \Psi'$. There is a causal process α from QC to RD such that



(29)

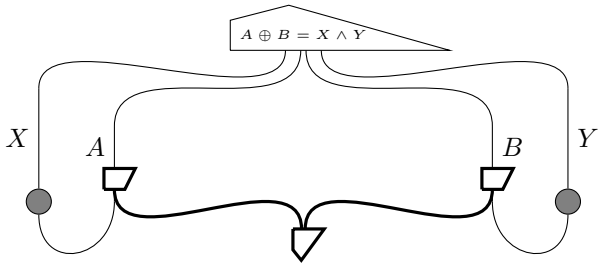
Applying the same process to Ψ' yields a state that is within distance $\sqrt{2\epsilon}$ from Φ. □

3 Untrusted quantum processes

An *untrusted quantum process* is represented by a diagram in which all of the quantum processes are unlabeled and all of the classical processes are labeled. We discuss an example of such processes and then give a definition of the more specific class of *device-independent quantum protocols*.

3.1 Example: Quantum strategies for nonlocal games

A nonlocal game is a game played by k parties ($k \geq 2$) in which the players are given random inputs $X_1, \ldots, X_k$ according to some fixed joint probability distribution. The players produce outputs $A_1, \ldots, A_k$ and these outputs are scored as $L(X_1, \ldots, X_k, A_1, \ldots, A_k)$, where L is a deterministic function that maps to $\{0, 1\}$. An example (the Clauser-Horne-Shimony-Holt game) is given below. The registers X, A, B, Y are classical bit registers (each isomorphic to $\mathbb{C}^2$).



(30)

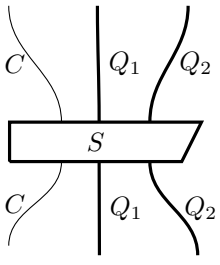
The effect at the top denotes the map $\mathbb{C}^{\{0,1\}^4} \to \mathbb{C}$ given by $(p_{xaby}) \mapsto \sum_{a \oplus b = x \wedge y} p_{xaby}$. This game is a common building block for device-independent protocols (including in particular the randomness expansion results that we will consider in section 4).

3.2 Device-independent quantum protocols

We are now ready to formalize the notion of a protocol in the device-independent setting. Historically, a quantum protocol is *device-independent* if all of its *quantum* processes are untrusted and uncharacterized (whereas strictly "classical" aspects, such as timing, non-communication, and computation, are still trusted). This definition can be traced back to early papers such as Mayers and Yao [18] and Ekert [40]. There is some room for interpretation as to exactly which quantum processes are allowed in device-independence, and we offer a specific formalism here. (Our treatment can be compared to the non-graphical formalization of device-independent protocols in section 4 of [13].)

For simplicity our definition is for a 2-device protocol, but it could easily be generalized to an N-device protocol.

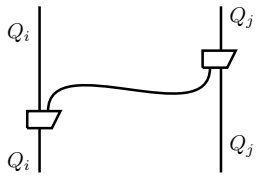
Definition 3.1. *A device-independent protocol with* 2 *quantum devices is a diagram of the form*



(31)

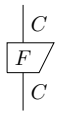
where S is constructed from the following subdiagrams.

1. ***Communication between devices.*** *An untrusted process transferring information (one way) from one of the two quantum registers to the other:*



(32)

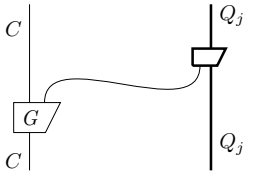
2. ***Deterministic classical functions.*** *A deterministic function is applied to the register C.*



(33)

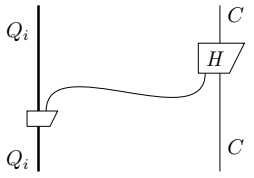
3. ***Failure.*** *The value of the classical register C is checked to see if it lies in a chosen subset S; if it does not, the protocol aborts. (Diagrammatically, this is the linear map from C to C given by $\sum_i p_i |i\rangle \mapsto \sum_{i\in S} p_i |i\rangle$.)*

4. ***Giving input to a device.*** *A deterministic function is applied to C and the result is given to one of the devices.*



(34)

5. ***Receiving input from a device.*** *Classical information is received from one of the devices.*



(35)

Note that every device-independent protocol has two representations: as a diagram (including some unlabeled elements) and as a set of processes from CQ_1Q_2 to CQ_1Q_2. We may use the label S to refer to either representation. Device-independent protocols can be composed (e.g., the output quantum states of one protocol can be given as inputs to another, which corresponds to re-using the devices from the first protocol in the second).

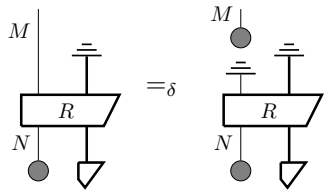
4 Randomness expansion

4.1 Linear randomness expansion

We can now phrase security results on device-independent randomness expansion [22] in terms of diagrams. A device-independent randomness expansion protocol accepts a seed and returns a larger output. Security results for such protocols consist of asserting that if the seed is uniformly random, then except with negligible

probability, the output is also uniformly random. The protocols that we consider for randomness expansion consist of iterating 2 untrusted devices many times, and sometimes at random playing a nonlocal game (such as the CHSH game) to test that the devices are behaving properly (see Figure 2 in [28]).

A simple way to assert security for a 2-device randomness expansion protocol R is to say that replacing the output with a true uniformly random state has a negligible effect, i.e.,

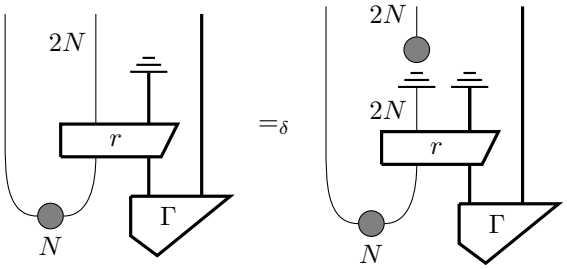


(36)

Above we compressed the two device states of R into a single thick wire, and we are using the labels M and N as a shorthand for $\mathbb{C}^{2^M}$ and $\mathbb{C}^{2^N}$. But it is preferable to have a stronger assertion: we wish to know that the output of the protocol is also approximately uniform when conditioned on the seed and on any quantum information entangled with the devices. The following theorem captures this stronger assertion.

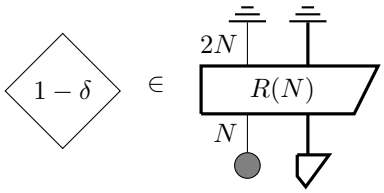
Theorem 4.1 (**Spot-check protocol**). *There exist device-independent protocols $R(1), R(2), R(3), \ldots$, where $R(N)$ has classical input dimension 2^N and classical output dimension 2^{2N}, and there exists a function $\delta = \delta(N) \in 2^{-\Omega(N)}$, such that the following hold.*

1. ***Soundness.*** *For any $r \in R(N)$ and any state Γ,*



(37)

2. ***Completeness.***



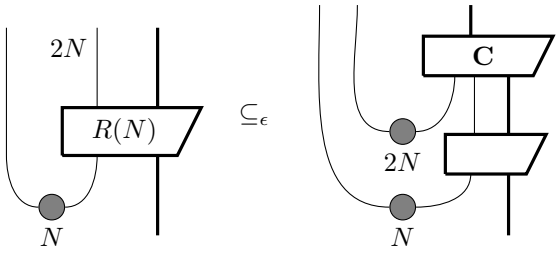
(38)

Proof. This follows from known results [20, 27, 28, 41]. See Appendix B for a formal explanation. □

"Soundness" asserts that the protocols $R(N)$ must either produce random numbers or fail. "Completeness" asserts that there exist processes which will make $R(N)$ succeed with probability approaching 1.

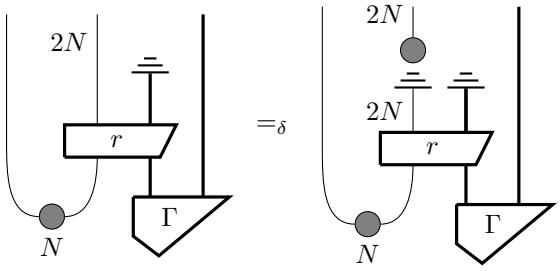
The following corollary will be a key step in our proof of unbounded randomness expansion. Whereas Theorem 4.1 assumes that the state of the devices is destroyed, the next lemma addresses the case where the device-state is preserved. In any diagram, let $\mathbf{C}$ denote the set of all causal processes (with input and output types as implied by the diagram).

Lemma 4.2 (Spot-Check Lemma)**.** *There exists $\epsilon = \epsilon(N) \in 2^{-\Omega(N)}$ such that for every integer $N \geq 1$,*



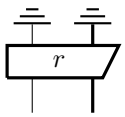
(39)

Proof. Let δ be as in Theorem 4.1, let N be a positive integer, and let $r \in R(N)$. We have



(40)

for any pure state Γ. We construct a duplication of the state on the right side of the above equation. Let $Q = V \otimes V$ denote the quantum register represented by the thick input wire received by the process r. The effect

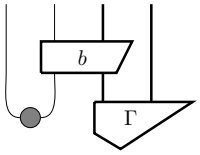


(41)

is an element in the dual of $\mathbb{C}^N \otimes V \otimes V$ which can be written as $\sum_{ijk} \sigma^i_{jk} \langle i| \otimes \langle j| \otimes \langle k|$, where the matrices $\Sigma^i = [\sigma^i_{jk}]_{jk}$ are positive semidefinite. Let $b : \mathbb{C}^N \otimes V \otimes V \to \mathbb{C}^N \otimes V \otimes V$ denote the controlled pure process

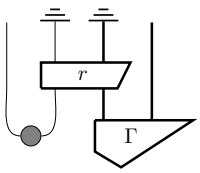
$$X \mapsto \left(\sum_i |i\rangle \langle i| \otimes \sqrt{\Sigma_i} \otimes \overline{\sqrt{\Sigma_i}} \right) X \tag{42}$$

Then, the state



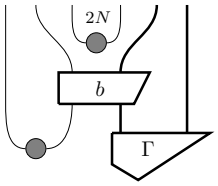
(43)

is a duplication of the state



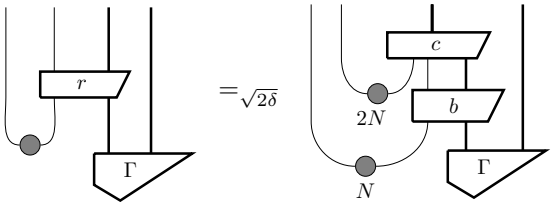
(44)

Likewise, the state



(45)

is a duplication of the state on the right side of (40). Therefore by Corollary 2.4, there is a causal process c such that

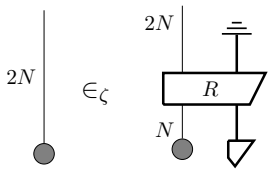


(46)

The desired result follows (with $\epsilon = \sqrt{2\delta}$). □

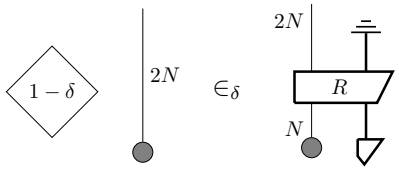
Additionally, we note the following alternative form of the completeness assertion for $R(N)$. The next lemma asserts that the set of all possible classical outputs of the spot-checking protocol must contain a state that is close to the (normalized) uniform state on $\mathbb{C}^{2^N}$. This is similar to the use of "adjustment completeness error" in [28].

Lemma 4.3. *There exists $\zeta(N) \in 2^{-\Omega(N)}$ such that*



(47)

Proof. Combining the soundness and completeness claims in Theorem 4.1, we have



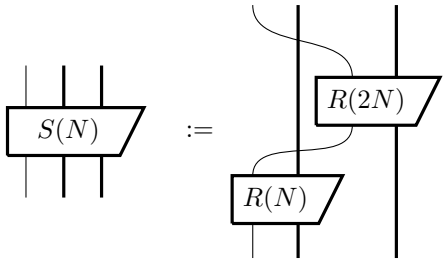
(48)

The desired result follows, with $\zeta = 2\delta$. □

4.2 Unbounded randomness expansion

Now we discuss a graphical proof of unbounded (rather than linear) randomness expansion. We would like to apply the spot-checking protocol and lemma repeatedly, in order to obtain unbounded randomness expansion. Naively stacking $R(N)$ operations atop one another does not work. Intuitively, this is because the results of subsection 4.1 only apply if the initial seed is independent of the state of the devices in the protocol $R(N)$. If we reuse devices in two successive iterations of the protocol, that independence assumption may not hold. However, it was observed in [13, 23, 28] that we can still obtain unbounded randomness by employing two pairs of devices and alternating which pair is employed in the protocol. In effect, one proves that the second application of the protocol wipes out any correlation with the first device, which may then be used in the third step to erase correlation with the second, and so on.

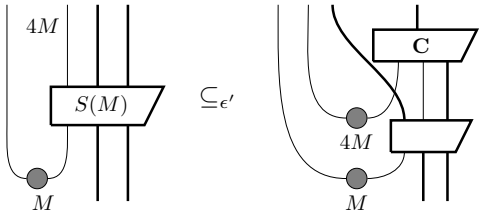
Definition 4.4. *For any integer $N \geq 1$, let $S(N)$ denote the set of processes given by*



where $R(N)$ denotes the process set from Theorem 4.1. Let $S_k(N)$ denote the composition $S(4^{k-1}N) \circ S(4^{k-2}N) \circ \ldots \circ S(N)$.

We prove the following lemma (which will be a building block for a later induction proof). For the remainder of this section, let $\epsilon = \epsilon(M)$ be the error function from Lemma 4.2.

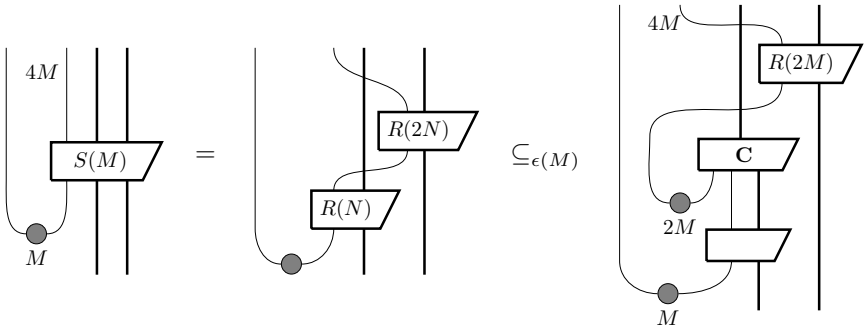
Lemma 4.5. *For every integer $M \geq 1$, we have*



(49)

where $\epsilon'(M) = \epsilon(M) + \epsilon(2M)$.

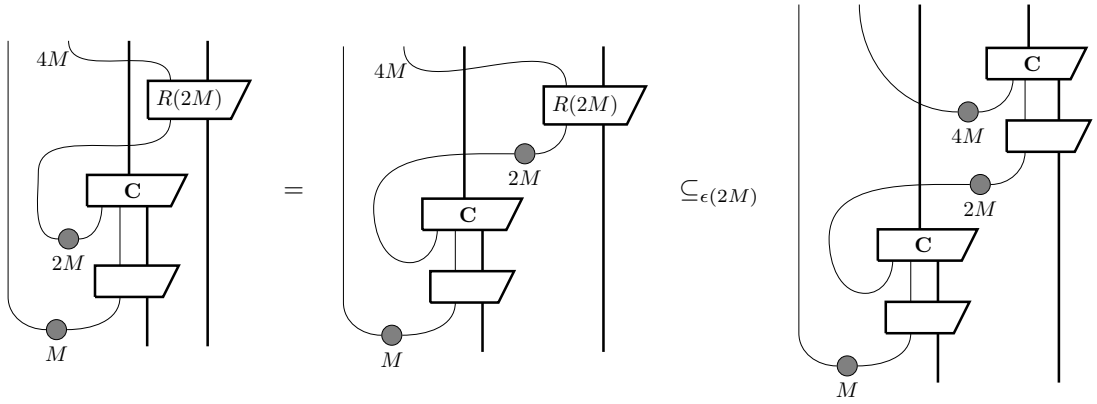
Proof. We first use Definition 4.4 to expand the left-hand side of Equation (49) and then apply Lemma 4.2 to the occurrence of $R(M)$ in the resulting diagram.



(50)

We can now move the spider of type $2M$ along its wire to place it below the occurrence of $R(2M)$ and apply

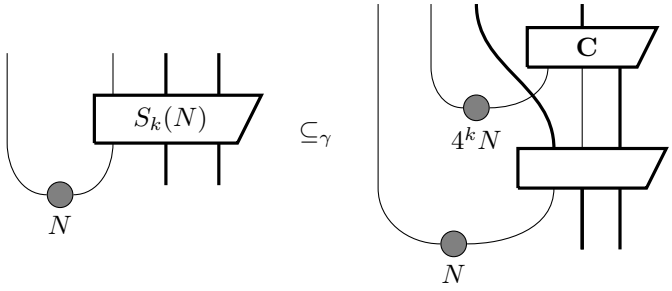
Lemma 4.2 again.



(51)

In the rightmost diagram above, the three lower boxes form a stochastic process, and this completes the proof. □

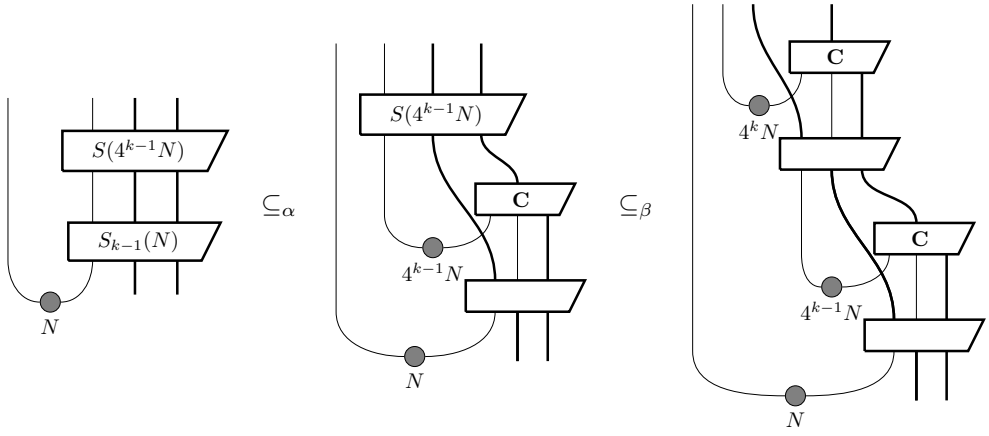
Lemma 4.6. *For all integers $N, k \geq 1$, we have*



(52)

where $\gamma = \gamma(N,k) = \sum_{i=0}^{2k-1} \epsilon(2^i N)$.

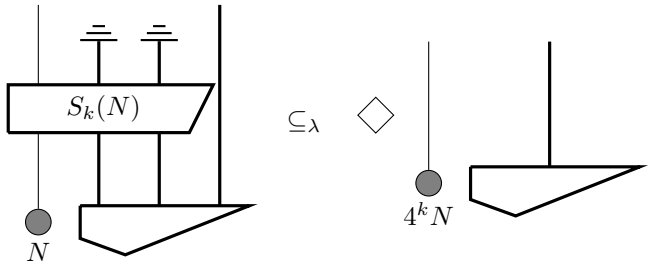
Proof. By induction on k. The case $k = 1$ follows from Lemma 4.5 by setting $M = N$. So suppose that $k > 1$. Then we can expand the left-hand side of Equation (52) and apply the induction hypothesis to obtain



(53)

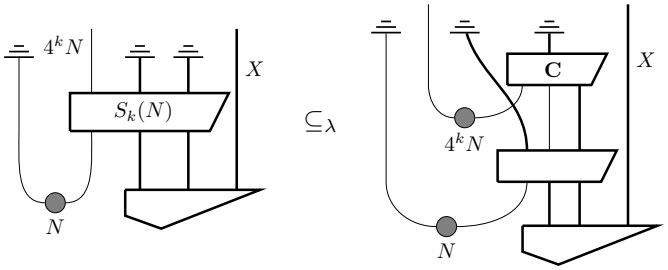
where $\alpha = \epsilon(M) + \epsilon(2M) + \ldots + \epsilon(2^{2k-3}M)$ and $\beta = \epsilon(2^{2k-2}M) + \epsilon(2^{2k-1}M)$. The desired result follows. □

Theorem 4.7 (Soundness for Unbounded Expansion)**.** *There is a function $\lambda = \lambda(N) \in 2^{-\Omega(N)}$ such that for any $N, k \geq 1$,*



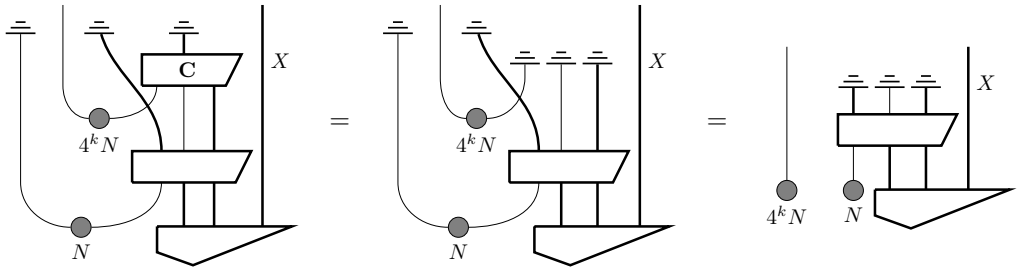
(54)

Proof. By the property noted in Equation (13), we can add a terminated branch to the left-hand side of Equation (54) so that we can apply Lemma 4.6.



(55)

We next apply causality (see the discussion of Equation (15)) followed by Equation (13).



(56)

The set of processes described by the rightmost diagram consist of a uniform state of dimension $4^k N$ together with a subnormalized state of X, as desired.

Let $\lambda(N) = \sum_{i=0}^{\infty} \epsilon(2^i N)$, which upper bounds the error term $\gamma(N, k)$. Note that for any nonnegative function f on the set $\{0, 1, 2, \dots, \}$

$$f \in 2^{-\Omega(N)} \implies \sum_{i=0}^{\infty} f(2^i N) \in 2^{-\Omega(N)}. \tag{57}$$

Thus $\lambda \in 2^{-\Omega(N)}$. This completes the proof. □

Theorem 4.7 asserts soundness for $S_k(N)$. Completeness for $S_k(N)$ follows from Lemma 4.3 and the implication (57) stated above.

4.3 Formalization

In addition to their intuitive appeal, the graphical structures of categorical quantum mechanics are amenable to computer formalization. In the long term, this will be critically important for managing the complexity

of medium- and large-scale security proofs. In this respect, computers can play a number of roles including validation and verification, copying and reuse, and proof search and discovery.

As part of our investigations, we have produced a computer-verified skeleton version of the main sequence of steps from our proof, for the case $k = 2$. We used the Globular proof assistant [34]. The reader can find and explore the proof object at [42], and a video of the diagrammatic moves involved in the proof is available at [35]. The Globular proof assistant provides a system for creating string diagram proofs, based on the perspective of higher-dimensional re-writing. In this project we used the system to prototype our arguments, and found the tool quite useful despite a few rough edges.

In Globular, one begins by declaring generators, atomic components which can be joined together into more complex diagrams. These generators come in several dimensions; strings in dimension 1 (classical, quantum), processes in dimension 2 (e.g., the spot-check protocols), and equations in dimension 3 (e.g., the spot-check lemma, the causality principle). More general protocols are complex two-dimensional diagrams. A proof becomes a three-dimensional diagram, though we often think of it as a "movie" whose frames are iterated slices of the 3-D diagram, tracing through the diagrammatic moves of the proof.

We used Globular to prototype the proof of Theorem 4.7. In particular, we used it to prototype and validate the general strategy of our proof in the case $k = 2$. Figure 1 shows part of the sequence of Globular diagrams in our proof of Theorem 4.7 for $k = 2$; the entire sequence involved 60 steps. (The sequence includes four applications of Lemma 4.2 followed by the final application of causality.)

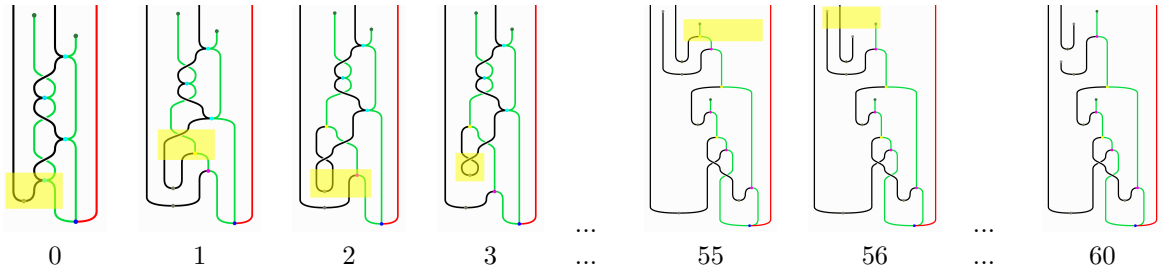


Figure 1: Steps in a Globular proof of Theorem 4.7 for $k = 2$

We found several significant benefits to building proofs in Globular. As diagrams become more complex, our ability to manipulate them with pen and paper is limited. Globular automates the management of diagrams, allowing for easy reuse and undo.

The proof assistant also "type-checks" the user, admitting only valid constructions and proof. This allows the user to explore the space of possible diagrams and proofs without accidentally introducing errors. This will be particularly important for learning because it permits a focus on concepts over calculation.

More generally, formalization serves to identify gaps in our reasoning. In this case, we first identified the graphical form of the spot-check lemma (Lemma 4.2) and the final form of Theorem 4.7. By trying to prove the theorem in Globular we first validated the back-and-forth approach described in the proof of our theorem, but also showed that it was insufficient to yield our desired result. This, in turn, helped to identify the role of causality in our argument.

Overall, we found the Globular proof assistant to be quite helpful in prototyping and managing our arguments, although some issues limit its practical application. For example, three steps are needed to pass from step 56 to step 60 (see above), despite the fact that the two diagrams are more-or-less identical. This problem reifies as diagrams become more complicated; in our proof, 19 steps of sliding operations were needed between the second and third applications of the spot-check protocol. Improvements to such tools, both in underlying computation and representation and in user interface would be valuable areas for future research.

5 Conclusion

Our graphical proof of unbounded expansion was based on two central steps: one was the application of the Spot-Check Lemma (Lemma 4.2), and the other was the principle of *causality*. Causality is an elementary step in symbolic proofs for quantum information, but in the case of our graphical proof it is an important manipulation.

We have used the tools of categorical quantum mechanics to give a streamlined proof that unbounded randomness expansion can be obtained via the spot-checking protocol. We hope to have convinced the reader of the usefulness and potential of graphical methods in quantum cryptography for proof exposition. Also, when graphical proofs are appropriately created, they open the door to automated proof-checking. Our experience using the Globular proof assistant can be seen as interesting case study in the usefulness of the software and we hope that our experience can motivate future work.

Our goal for later work is to develop a language for quantum cryptography that allows a wide range of expositions of old results and proofs of new results. Some proofs (including unbounded randomness expansion) seem easiest to understand in graphical form, while others (such as Proposition 2.3) may be most accessible as algebraic proofs. Thus, an ideal framework would allow easy translation back and forth between algebraic and graphical expositions.

Acknowledgements

We are greatly indebted to David Spivak for providing some of the original inspiration for this project and for helping us to get it started. CAM would also like to thank Brad Lackey for seminars at the University of Maryland that deepened his understanding of axiomatic quantum information. NJR is funded by the Department of Defense. This paper includes contributions from the U. S. National Institute of Standards and Technology, and is not subject to copyright in the United States.

References

[1] R. Penrose, in *Combinatorial Mathematics and its Applications*, edited by D. Welsh (Academic Press, New York, 1971) pp. 221–244.

[2] A. Joyal and R. Street, Advances in Mathematics **88**, 55 (1991).

[3] P. Selinger, "A Survey of Graphical Languages for Monoidal Categories," in *New Structures for Physics* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011) pp. 289–355.

[4] S. Abramsky and B. Coecke, in *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS 2004)* (2004) pp. 415–425.

[5] J. Vicary, in *Proceedings of the 28th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2013)* (2013) pp. 93–102.

[6] N. Chancellor, A. Kissinger, S. Zohren, and D. Horsman, "Coherent Parity Check Construction for Quantum Error Correction," (2016), available from `arXiv:1611.08012`.

[7] B. Coecke, "From Quantum Foundations via Natural Language Meaning to a Theory of Everything," (2016), available from `arXiv:1602.07618`.

[8] B. Coecke and A. Kissinger, *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning* (Cambridge University Press, 2017).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2002).

[10] B. Coecke and S. Perdrix, in *Computer Science Logic: 24th International Workshop, CSL 2010, 19th Annual Conference of the EACSL, Brno, Czech Republic, August 23-27, 2010. Proceedings* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 230–244, preprint available from `arXiv:1004.1598`.

[11] B. Coecke, Q. Wang, B. Wang, Y. Wang, and Q. Zhang, in *Proceedings of the 6th International Workshop on Quantum Physics and Logic (QPL 2009)* (2011) pp. 231 – 249.

[12] A. Hillebrand, in *Proceedings of the 8th International Workshop on Quantum Physics and Logic (QPL 2011)* (2012) pp. 103–121.
[13] K.-M. Chung, Y. Shi, and X. Wu, "Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions," (2014), available from arXiv:1402.4797.
[14] C. Heunen, Logical Methods in Computer Science **4**, 4 (2008).
[15] U. Maurer and R. Renner, in *Innovations in Computer Science* (Tsinghua University Press, 2011) pp. 1–21.
[16] D. Pavlovic, in *Categories and Types in Logic, Language, and Physics - Essays Dedicated to Jim Lambek on the Occasion of His 90th Birthday*, Vol. 8222 (2014).
[17] M. Stay and J. Vicary, Electronic Notes in Theoretical Computer Science **298**, 367 (2013), proceedings of the Twenty-ninth Conference on the Mathematical Foundations of Programming Semantics, MFPS XXIX.
[18] D. Mayers and A. Yao, in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)* (1998) pp. 503–509.
[19] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nature Communications **9**, 459 (2018).
[20] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and Tight Device-Independent Security Proofs," (2016), available from arXiv:1607.01797.
[21] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, "Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling," (2017), available from arXiv:1702.05178.
[22] R. Colbeck, "Quantum And Relativistic Protocols For Secure Multi-Party Computation," Ph.D. thesis, University of York (2007), available from arXiv:0911.3814.
[23] M. Coudron and H. Yuen, in *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, NY, USA, 2014) pp. 427–436.
[24] F. Dupuis, O. Fawzi, and R. Renner, "Entropy Accumulation," (2016), available from arXiv:1607.01796.
[25] S. Fehr, R. Gelles, and C. Schaffner, Physical Review A **87** (2011), 10.1103/PhysRevA.87.012335.
[26] E. Knill, Y. Zhang, and H. Fu, "Quantum probability estimation for randomness with quantum side information," (2018), arXiv:1806.04553.
[27] C. A. Miller and Y. Shi, SIAM Journal on Computing **46**, 1304 (2017).
[28] C. A. Miller and Y. Shi, Journal of the ACM **63**, 33:1 (2016).
[29] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A Manning, and C. Monroe, Nature **464**, 1021 (2010).
[30] S. Pironio and S. Massar, Physical Review A **87** (2011), 10.1103/PhysRevA.87.012336.
[31] S. Aaronson, American Scientist **102**, 266 (2014).
[32] National Institute of Standards and Technology (NIST), "Randomness Beacon Program," https://www.nist.gov/programs-projects/nist-randomness-beacon, accessed: 2019-02-01.
[33] M. Coudron and H. Yuen, "Infinite Randomness Expansion and Amplification with a Constant Number of Devices," (2013), preprint available from arXiv:1310.6755.
[34] K. Bar, A. Kissinger, and J. Vicary, Logical Methods in Computer Science **14** (2018).
[35] Globular, "Video," Available as ancillary material at arXiv:1705.09213 (2019), accessed: 2019-04-25.
[36] B. Coecke and A. Kissinger, "Categorical Quantum Mechanics I: Causal Quantum Processes," (2015), available from arXiv:1510.05468.
[37] B. Coecke and A. Kissinger, "Categorical Quantum Mechanics II: Classical-Quantum Interaction," (2016), available from arXiv:1605.08617.
[38] A. Kissinger, S. Tull, and B. Westerbaan, "Picture-perfect Quantum Key Distribution," (2017), available from arXiv:1704.08668.
[39] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).
[40] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[41] U. Vazirani and T. Vidick, in *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12 (ACM, New York, NY, USA, 2012) pp. 61–76.
[42] Globular, "Proof," http://globular.science/1904.001 (2019), accessed: 2019-04-25.
[43] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM Journal on Computing **41**, 915 (2012).
[44] F. Bonchi, P. Soboci'nski, and F. Zanasi, in *CONCUR 2014 - Concurrency Theory*, Lecture Notes in Computer Science, Vol. 8704 (2014) pp. 435–450.
[45] A. Kissinger and S. Uijlen, in *Proceedings of the 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2017)* (2017) pp. 1–12.

A Proof of Proposition 2.3

In this section we revert to standard notation for quantum systems. The state Ψ can be written as a density operator

$$\Psi = \sum_i |i\rangle\langle i| \otimes M_i, \tag{58}$$

where M_i are positive semidefinite operators on Q_1, with $Q = Q_1 \otimes Q_1$. Then, the duplicated state of Ψ is given by

$$\Psi' \quad = \quad \sum_i |i\rangle\langle i| \otimes |i\rangle\langle i| \otimes \left(\mathrm{Vec}\sqrt{M_i}\right)\left(\mathrm{Vec}\sqrt{M_i}\right)^*, \tag{59}$$

where the sum is taken over $i \in \{1, 2, \ldots, \dim(C)\}$, and where $\mathrm{Vec}(X)$ denotes the vector $\sum_{ij} x_{ij} |i\rangle \otimes |j\rangle$ for any $X = \sum_{ij} x_{ij} |i\rangle\langle j|$. If Φ is such that

$$\Psi =_\epsilon \Phi, \tag{60}$$

then

$$\|\Psi - \Phi\|_1 \leq 2\epsilon, \tag{61}$$

and therefore if we let

$$\Phi = \sum_i |i\rangle\langle i| \otimes M'_i, \tag{62}$$

we have

$$\sum_i \|M_i - M'_i\|_1 \leq 2\epsilon. \tag{63}$$

By Lemma 3.37 from [39], we have

$$\sum_i \left\|\sqrt{M_i} - \sqrt{M'_i}\right\|_2^2 \leq 2\epsilon. \tag{64}$$

For any i,

$$\begin{aligned}
&\left\|(\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^* - (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^*\right\|_1 && (65)\\
&\leq \left\|(\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^* - (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M'_i})^*\right\|_1 && (66)\\
&\quad + \left\|(\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M'_i})^* - (\mathrm{Vec}\sqrt{M'_i})(\mathrm{Vec}\sqrt{M'_i})^*\right\|_1 && (67)\\
&\leq \left\|\mathrm{Vec}\sqrt{M_i}\right\| \left\|\mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M'_i}\right\| + \left\|\mathrm{Vec}\sqrt{M'_i}\right\| \left\|\mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M'_i}\right\| && (68)
\end{aligned}$$

Therefore, applying the Cauchy-Schwartz inequality, the trace distance between the duplicated states of Φ and Ψ is upper bounded by

$$\sum_i \left(\left\| \mathrm{Vec}\sqrt{M_i} \right\| + \left\| \mathrm{Vec}\sqrt{M'_i} \right\| \right) \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M'_i} \right\| \tag{69}$$

$$\leq \sqrt{\left[\sum_i \left(\left\| \mathrm{Vec}\sqrt{M_i} \right\| + \left\| \mathrm{Vec}\sqrt{M'_i} \right\| \right)^2 \right] \left[\sum_i \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M'_i} \right\|^2 \right]} \tag{70}$$

$$\leq \sqrt{\left[\sum_i \left(2 \left\| \mathrm{Vec}\sqrt{M_i} \right\|^2 + 2 \left\| \mathrm{Vec}\sqrt{M'_i} \right\|^2 \right) \right] \left[\sum_i \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M'_i} \right\|^2 \right]} \tag{71}$$

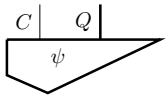
$$\leq \sqrt{4 \cdot 2\epsilon}, \tag{72}$$

as desired.

B Formal Justification of Theorem 4.1

Theorem 4.1 is a special case of known results on randomness expansion [20, 27, 28, 41]. In this appendix we demonstrate one way to derive Theorem 4.1.

We first define the conditional min-entropy of a classical-quantum state



(73)

where $Q = V \otimes V$, can be expressed in conventional form as an operator on $C \otimes V$:

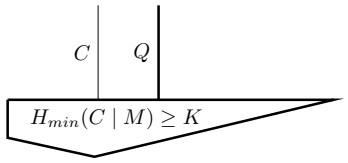
$$\Psi = \sum_i |i\rangle \langle i| \otimes M_i, \tag{74}$$

where each M_i is a positive semidefinite matrix on V. Then, the smooth min-entropy of C conditioned on V is given by

$$H_{min}(C \mid M)_\Psi = -\log \left[\min_{\sigma \geq M_i} \mathrm{Tr}(\sigma) \right], \tag{75}$$

where the minimum is taken over all Hermitian operators σ on Q that satisfy $\sigma \geq M_i$ for all i. (If Ψ is normalized, this quantity is the negative log of the optimal probability with which an adversary can guess the value of C given Q.)

Let



(76)

denote the set of all *sub*normalized classical-quantum states ψ of CQ satisfying

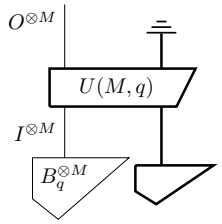
$$H_{min}(C \mid M)_\psi \geq K. \tag{77}$$

B.1 Achieving high min-entropy from a uniform seed

We will work with Protocol R_{gen} from Figure 2 in [27]. Fix the game G to be the CHSH game, and let the score threshold χ be equal to 0.85. Let T, A_1, A_2, X_1, X_2 denote classical bit registers, and let $I = (T, A_1, A_2)$ and $O = (X_1, X_2)$. For any real number q with $0 < q < 1$, let B_q denote the distribution on (T, A_1, A_2) given by

$$\mathbf{P}(t, a_1, a_2) = \begin{cases} q/4 & \text{if } t = 1 \\ (1-q) & \text{if } t = a_1 = a_2 = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{78}$$

(This is the distribution used in a single round of Protocol R_{gen} when the game G is the CHSH game.) The protocol R_{gen} can be expressed diagrammatically as follows.



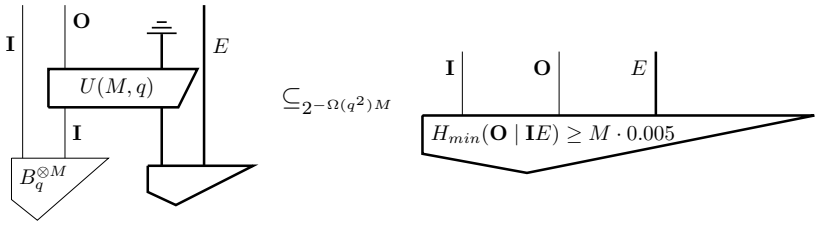
(79)

where $U(M, q)$ denotes the process described in steps $1 - 6$ in the device-independent Protocol R_{gen}.

Remark B.1. *The highest possible quantum winning probability for the CHSH game is* $\frac{1}{2} + \frac{\sqrt{2}}{4}$*, which is strictly greater than* $\chi = 0.85$*. Therefore, an honest quantum device employing the optimal strategy at each round will succeed at Protocol* R_{gen} *with probability* $1 - 2^{-\Omega(qN)}$*.*

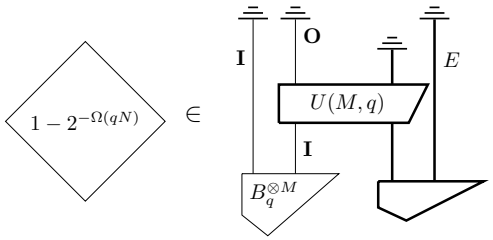
Applying Theorem 1.1 from [27] with $b := q$, and making use of formula (5.18) from [27], we obtain the following.

Theorem B.2. *There exist device-independent protocols* $\{U(M, q) \mid M \in \{1, 2, \ldots\}, 0 < q < 1\}$ *such that the following holds (soundness):*



(80)

where we have written $\mathbf{I}$ *and* $\mathbf{O}$ *for* $I^{\otimes M}$ *and* $O^{\otimes M}$ *respectively, and the following also holds (completeness):*



(81)

(The figure 0.005 in diagram (80) above is somewhat arbitrary – any figure that is less than $\pi(0.85 - 0.75) \approx 0.0096$ could be used in its place and the theorem statement would still hold true.)

Next we address the source distribution $B_q^{\otimes M}$. The following definition will be useful.

Definition B.3. *Let p be a subnormalized probability distribution on a finite set X, and let ℓ be an integer. Then, p is* 2^ℓ-rational *if $2^\ell p(x)$ is an integer for all x.*

Note that the condition above is equivalent to the condition that p can be expressed in the form $F(U_{2^\ell})$, where U is a uniform random variable on a set of size 2^ℓ and F is a deterministic process.

Proposition B.4. *For any $q \in (0, 1/4)$ and $M \in \{1, 2, \dots, \}$, there is a subnormalized probability distribution B on $\{0,1\}^{3M}$ such that*

1. *The distribution B is $2^{O(q \log(1/q) M)}$-rational, and*
2. *The statistical distance between B and $B_q^{\otimes M}$ is $2^{-\Omega(qM)}$.*

Proof. Let B' be the subnormalized probability distribution which assigns 0 to all sequences

$$((t^1, a_1^1, a_2^1), (t^2, a_1^2, a_2^2), \dots, (t^M, a_1^M, a_2^M)) \tag{82}$$

satisfying $\sum_{i=1}^M t^i > 2qM$, and assigns the same value as $B_q^{\otimes M}$ to all other sequences. Then, the statistical distance between B' and $B_q^{\otimes M}$ is precisely the probability that the sum $\sum_{i=1}^M t_i$ exceeds $2qM$. By elementary probability arguments, this probability is $2^{-\Omega(qM)}$. Additionally, the size of the support of B' is no more than $2^{H(2q)M} \cdot 2^{2qM} = 2^{O(q \log(1/q) M)}$. (Here, $H(t) = t \log(1/t) + (1-t)\log(1/(1-t))$ denotes the binary Shannon entropy function.)

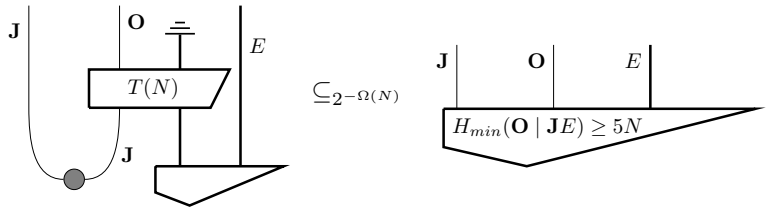
Let $t = \lceil qM + \log |\text{Supp } B'| \rceil$, and let B be the subnormalized probability distribution which assigns to each sequence $(\mathbf{t}, \mathbf{a}_1, \mathbf{a}_2)$ the value

$$2^{-t} \lfloor 2^t \mathbf{P}_{B'}(\mathbf{t}, \mathbf{a}_1, \mathbf{a}_2) \rfloor. \tag{83}$$

Then, the statistical distance between B and B' is no more than $2^{-t} |\text{Supp } B'| \leq 2^{-qM}$, and B is 2^t-rational. This implies the desired result. □

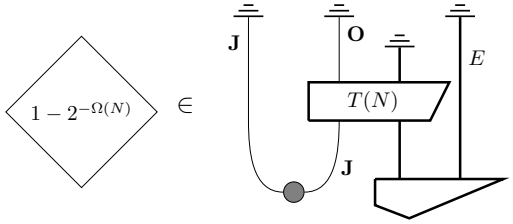
The previous proposition asserts that we can simulate the distribution $B_q^{\otimes M}$ up to error $2^{-\Omega(qM)}$ by applying a deterministic process to $O(q \log(1/q) M)$ uniformly random bits. When we fix $q \in (0, 1/4)$ to be sufficiently small so that the function the function represented by $O(q \log(1/q) M)$ in Proposition B.4 is upper bounded by $N := M/1000$ as $M \to \infty$, and also so that the function represented by $\Omega(q^2)$ in Theorem B.2 is positive, we obtain the following reformulation of Theorem B.2.

Theorem B.5. *There exist device-independent protocols $T(1), T(2), T(3), \dots$ such that the following holds for any $N \in \{1, 2, \dots\}$:*



(84)

where the register **J** *has dimension 2^N and the register* **O** *has dimension 2^{1000N}. Also, the following soundness claim holds:*

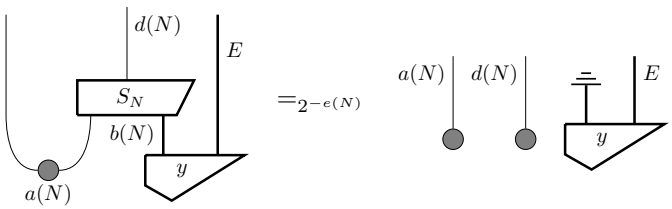


(85)

B.2 Randomness extraction

A randomness extractor converts a high min-entropy source into a near-uniformly random source, with the aid of a uniformly random seed. We will make use of a known construction (Trevisan's extractor).

Theorem B.6. *Let $a(N), b(N), c(N), d(N) \in \Theta(N)$ be functions and suppose that $(c(N) - d(N)) \in \Theta(N)$. Then, there exist deterministic processes $\{S_N \mid N \in \{1, 2, 3, \ldots\}\}$ and a function $e(N) \in \Theta(N)$ such the following relation holds*



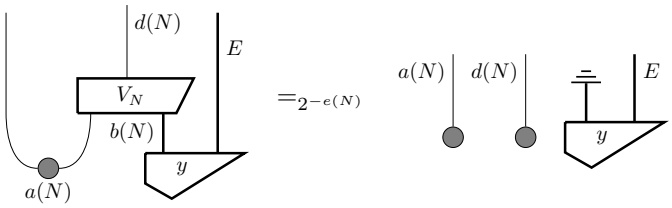
(86)

for any normalized state y whose min-entropy conditioned on E is at least $c(N)$.

Proof. This follows from Theorem 4.6, Lemma C.2, and Proposition C.5 in [43], letting $r = 1 + \delta$ and $\epsilon = 2^{-\delta N}$ where δ is a sufficiently small constant. □

We next assert that Theorem B.6 continues to hold when the phrase "normalized state" is replaced with "subnormalized state."

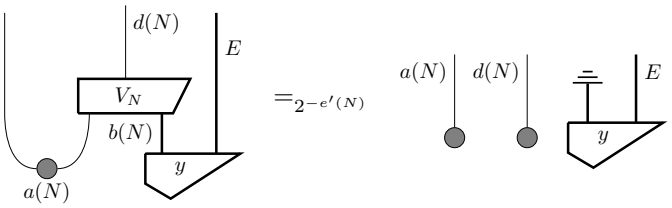
Corollary B.7. *Let $a(N), b(N), c(N), d(N) \in \Theta(N)$ be functions and suppose that $(c(N) - d(N)) \in \Theta(N)$. Then, there exist deterministic processes $\{V_N \mid N \in \{1, 2, 3, \ldots\}\}$ and a function $e(N) \in \Theta(N)$ such the following relation holds*



(87)

*for any **subnormalized** state y whose min-entropy conditioned on E is at least $c(N)$.*

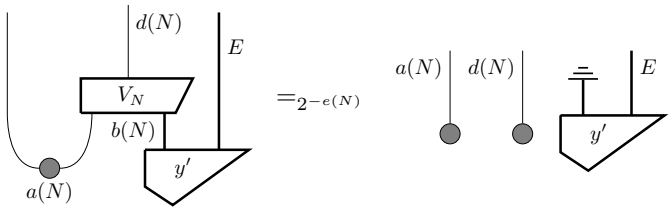
Proof. Choose a function $c'(N)$ such that $c'(N) - d(N) \in \Theta(N)$ and $c(N) - c'(N) \in \Theta(N)$. By Theorem B.6, there exists $e'(N) \in \Theta(N)$ and deterministic processes $\{V_N\}$ such that the following holds for any normalized state y whose min-entropy conditioned on E is at least $c'(N)$:



(88)

Let $e(N) \in \Theta(N)$ be a function that is less than or equal to both $(c(N) - c'(N))$ and $e'(N)/2$ for all N. Let y' be an arbitrary *sub*normalized state whose min-entropy conditioned on E is at least $c(N)$ (rather than $c'(N)$). If the trace of y' is at least $2^{-e(N)}$, then the next relation follows easily from the previous one (with

$y := y'/Tr(y'))$:

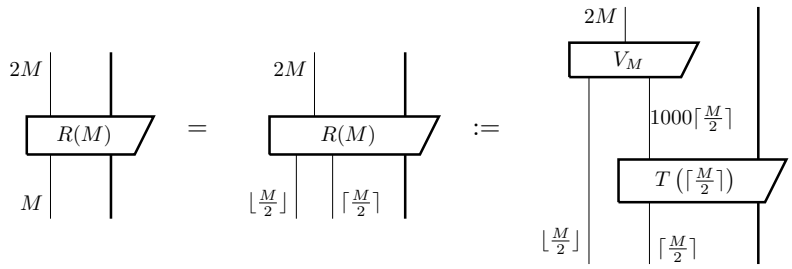


(89)

On the other hand, if the trace of y' is less than $2^{-e(N)}$, then both diagrams in relation (89) have trace less than $2^{-e(N)}$ and so the relation obviously holds. This completes the proof. □

B.3 Randomness expansion

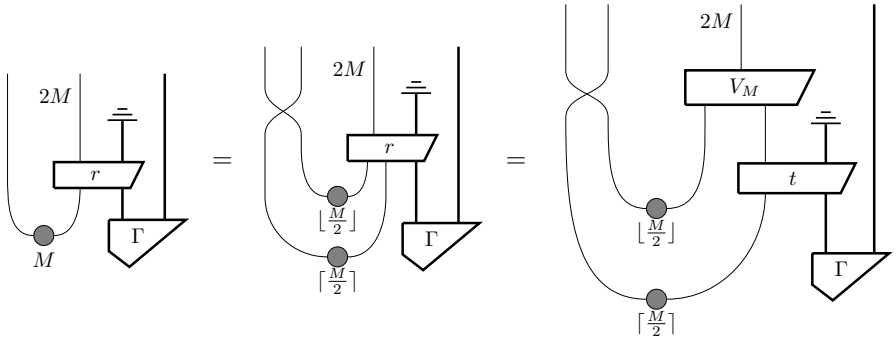
Now we combine the results of the previous two subsections to prove Theorem 4.1. For any positive integer M, let $T(M)$ denote the protocol defined in Theorem B.5. Define a device-independent protocol $R(M)$ by



(90)

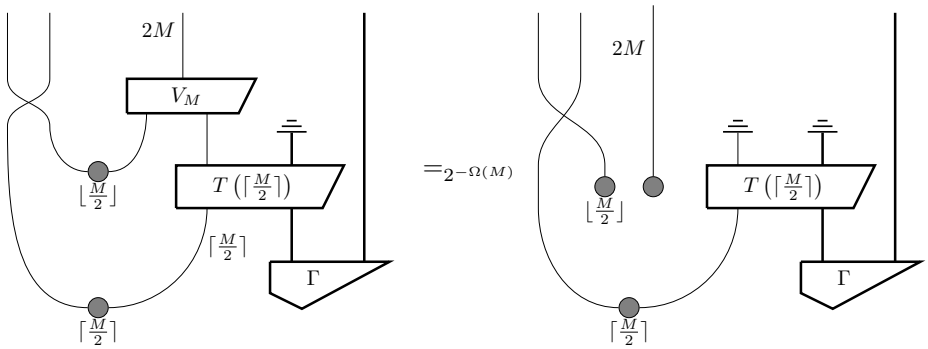
where V_M denotes the process defined in Corollary B.7, with $c(M) = \frac{5M}{2}$.

Then for any $r \in R(N)$ and normalized state Γ, there is some $t \in T(\lceil \frac{M}{2} \rceil)$ satisfying the following (the twist in the upper-left maintains the order of the original register M):



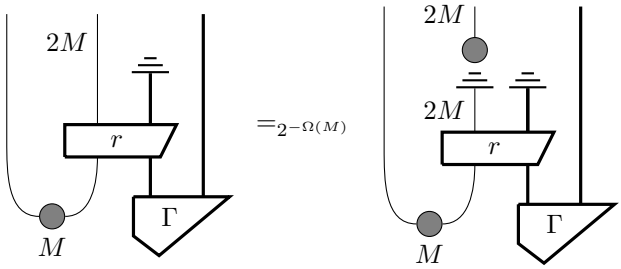
(91)

Now we can apply Theorem B.5 and Corollary B.7 to conclude that



(92)

from which it follows easily that



(93)

This implies the soundness claim in Theorem 4.1. The completeness claim in Theorem 4.1 follows easily from the completeness claim in Theorem B.5.