Graphical Methods in Device-Independent Quantum Cryptography

Spencer Breiner, Carl A. Miller, and Neil J. Ross

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, NS B3H 4R2, Canada

Abstract

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 recent result from device-independent quantum cryptography: any linear randomness expansion protocol can be converted into an unbounded randomness expansion protocol. We give a graphical exposition of a proof of this result and implement parts 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 [35]. During the last decade of the twentieth century, rigorous methods for graphical reasoning in monoidal categories were developed by Joyal, Street, and others [25, 38]. When Abramsky and Coecke proposed monoidal categories as an alternative foundation for quantum physics [2], 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 [2] to quantum algorithms [41], quantum error correction [7], and beyond [9, 12]. 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 [1], 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 — both for accessibility and for mathematical rigor — if proofs themselves could be expressed as pictures. For this reason, the field of quantum cryptography can benefit from the abstract methods of categorical quantum mechanics [10, 12].

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 [13, 14, 24], although these are not yet at the level of security that has been proved through non-graphical means. Meanwhile, the literature has a number

---

1 See Section 12.6 of [33] for an introduction.
of formal treatments of cryptography that are not primarily based on graphical reasoning. (One important example is [8], which has a focus similar to the current paper. See also [23, 28, 34, 39].)

One of the recent major achievements of quantum cryptography is the development of device-independent security proofs [29]. 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 [3, 5, 15, 17, 18, 20, 30, 31, 36, 37, 40]. 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 [1] for a gentle introduction to this topic and [32] for a discussion of a possible implementation.

Recent work [8, 17, 31] showed an extension: 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. Proving the security of this extension is not easy (indeed, the paper containing the first proof [16] was 36 pages long). Here, we give a proof of this extension (based on [8, 31]) 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 also highly amenable to computer verification. The Globular proof assistant software [4] carries out category-theoretic proofs, using diagrams that are easily compatible with [10, 11]. 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 [22].

This paper is organized as follows. In Section 2 we formalize a language for dealing with quantum processes, building on [10, 11] and adding some new elements. 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.

We note that the recent preprint [26] also addresses graphical proofs of quantum cryptography with a different focus (device-dependent quantum key distribution). The graphical concepts in the present paper and in [26] were developed independently, and we expect that there will be a useful synergy between the two papers.

### 1.1 Our contributions

The picture-language in this paper is based primarily on [10, 11]. We have added some new elements in order to enable quantum cryptographic proofs. Here are some of the additions:

1. **Diagrams versus sets.** Whereas a diagram in the language of [10, 11] represents a quantum process, we have 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. **Approximation.** We use the symbol $\approx_{\epsilon}$ to denote that the state represented by one diagram is approximately equal to the state represented by another. This allows proofs via chains of approximations. (This feature was also independently used in [26].)

3. **Duplication of states.** We define the “duplication” of a classical-quantum state (see subsection 2.3), a convenient shorthand which encompasses both copying of classical states and purification of quantum states.
4. **A graphical formalization of device-independence.** We give a graphical formalization of what it means precisely for a protocol to be device-independent (subsection 3.2).

## 2 Fundamentals

In this section, we cover useful graphical techniques and concepts, building on [10][11]. 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 [10][11] or the more recent [12] for categorical quantum mechanics, and [42] for notions of distance relevant to quantum information theory.

### 2.1 The graphical language of categorical quantum mechanics

Throughout, \( O \) denotes a collection of finite-dimensional Hilbert spaces, each with a fixed orthonormal basis. We assume that \( O \) is closed under tensor products (i.e., if \( V, W \in O \) then \( V \otimes W \in O \)) and that \( O \) contains the space \( \mathbb{C}^n \) for every non-negative integer \( n \). We sometimes refer to the elements of \( O \) as *types* or *registers*. We say that \( f \) is a *process of type* \( V \to W \) if \( f \) is a linear operator whose domain is \( V \) and whose range is \( W \). It is represented by a box labelled \( f \) whose input and output wires are labelled with the types \( V \) and \( W \) as follows.

\[
\begin{array}{c}
W \\
\downarrow f \\
V \\
\end{array}
\]  

(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).

\[
\begin{array}{c}
W \\
\downarrow g \\
V \\
\downarrow f \\
U \\
\end{array} \quad \begin{array}{c}
W \\
\downarrow f \\
V \\
\downarrow f' \\
V' \\
\end{array}
\]  

(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 below. The conjugate, transpose, and conjugate-transpose (i.e., adjoint) of \( v \) are also depicted below (second, third, and fourth diagram respectively).

\[
\begin{array}{c}
V \\
\downarrow v \\
\end{array} \quad \begin{array}{c}
V \\
\downarrow v \\
V \\
\end{array} \quad \begin{array}{c}
V \\
\downarrow v \\
V \\
\end{array} \quad \begin{array}{c}
V \\
\downarrow v \\
\end{array}
\]  

(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 simply by a diamond with a label on it indicating its value.

A *spider* is a process drawn as follows,

\[
\begin{array}{c}
w \\
\downarrow w \\
\end{array}
\]  

(4)
The diagram (4) denotes the vector $\sum e \otimes e \otimes e \in W \otimes W \otimes W$, where the sum is taken over the standard basis of $W$. Because they will play an important role below, we will also introduce the uniform vector, which is denoted by a gray node:

\[
\begin{array}{c}
\text{\bigtriangleup} \\
1/ \text{dim } W
\end{array}
\]

Thus, the diagram on the left side of (5) denotes the vector $(1/ \text{dim } W) \sum e \otimes e \otimes e \in W \otimes W \otimes W$.

A quantum type, or quantum register, is an element $Q$ of $O$ 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 respective diagrams below.

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

A mixed quantum state of $Q$ is a state of the form $\sum_i v_i \otimes \bar{v_i}$ 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.

A linear map $Q \to \mathbb{C}$ is a quantum effect if it maps all states to the interval $[0, 1]$ — that is, if whenever $\Psi$ is a quantum state of $Q$,

\[
\begin{array}{c}
\text{\bigtriangleup} \\
\beta
\end{array}
\]

\[
\in \quad [0, 1].
\]

(In the more conventional framework, 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 $w \mapsto \langle w, \sum_i e_i \otimes e_i \rangle$, where $\{e_i\}$ denotes the standard basis of $Q$, is denoted by

\[
\text{\bigtriangleup}
\]

A causal quantum process $\Sigma$ from a register $Q$ to another register $R$ is a linear homomorphism such that for any state $\Psi$ of $Q \otimes Q$, the diagram below represents a state. (In the conventional framework, causal quantum processes correspond to completely positive trace-preserving maps.)
A **stochastic** quantum process is one that satisfies the same condition, with the weaker requirement that the diagram above is a subnormalized quantum state. Unless otherwise specified, the phrase word “quantum process” refers to a stochastic quantum process.

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

$$\psi = \Psi$$  \hfill (11)

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

If $\Psi$ is a state of $QR$, we denote the partial trace over $R$ as follows:

$$\Psi_{QR}$$  \hfill (12)

If $C$ is a register, then a **classical state** is a vector $v \in C$ of the form $v = \sum_i p_i e_i$, where $\{e_i\}$ denotes the standard basis of $C$ and $\{p_i\}_i$ is a probability distribution. If $Q$ is a quantum register, then a **classical-quantum state** of $CQ$ is a state of the form $\sum_i p_i e_i \otimes v_i$, 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 $\sum_i e_i e_i^* \otimes \Phi_i$, where each $\Phi_i$ is a process on $Q$.

A diagram in which every element is specified as an explicit linear map is itself a linear map (obtained by composition and tensor product). A diagram in which some elements are unlabelled denotes a set of linear maps. For example, the diagram

$$Q \quad \Downarrow \quad R$$  \hfill (13)

denotes the set of all (normalized mixed) states of $Q$. A single unlabelled wire denotes the set of all identity functions $\{Id_V : V \rightarrow V \mid V \in O\}$. In general, a diagram denotes the set of all processes that can be expressed in the form shown in the diagram.

We will use the picture element $\Diamond$ to denote an arbitrary element of $[0, 1]$.

### 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. (This metric is half of the diamond norm distance — see [42] for further details).

**Definition 2.1.** If $c, d, \text{ and } \epsilon$ are real numbers, we write $c =_\epsilon d$ if $|c - d| \leq \epsilon$. Now let $\Sigma$ and $\Sigma'$ be two processes of the same type. We write $\Sigma =_\epsilon \Sigma'$ if for all states $\Psi$ and effects $\beta$,

$$\beta \quad \Downarrow \quad \Sigma \quad =_\epsilon \quad \beta \quad \Downarrow \quad \Sigma'$$  \hfill (14)
Note that the above definition remains equivalent if the phrase “for all states \( \Psi \)” is replaced by “for all pure states \( \Psi \).”

If we restrict the processes \( \Sigma \) and \( \Sigma' \) to be states (i.e., to have no inputs) then \( \Sigma =_\epsilon \Sigma' \) if \( \Sigma \) and \( \Sigma' \) differ by no more than \( 2\epsilon \) in trace distance. It can be verified that the notion of approximation defined above satisfies the triangle inequality: if \( \Sigma =_\epsilon \Sigma' \) and \( \Sigma' =_\epsilon \Sigma'' \), then \( \Sigma =_\epsilon \Sigma'' \). Next we 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 [28].)

**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 \( A \subseteq_\epsilon B \).

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, which is closely related to the notion of purification of quantum states (see section 2.5 of [33]).

If \( \Psi \) is a subnormalized classical-quantum state of a quantum register \( CQ \), then we can write \( \Psi = \sum_{ijk} \psi_{ij}^k e_k \otimes f_i \otimes f_j \), where the sum is taken over the standard basis vectors \( \{e_k\} \) for \( C \) and \( \{f_i \otimes f_j\} \) for \( Q \). The matrices \( M_k := [\psi_{ij}^k]_{ij} \) are then positive semidefinite. We can alternatively express \( \Psi \) as

\[
\Psi_{CQ} = P_{CQ} CQ (15)
\]

where \( P \) is the linear map defined by

\[
P(e_k \otimes f_i \otimes f_j) = e_k \otimes \sqrt{M_k} f_i \otimes \sqrt{M_k} f_j.
\]

Then, the *canonical duplicate state* of \( \Psi \) is given by

\[
\Psi'_{CQ} := P_{CQ} CQ (17)
\]

(See equation (48) in the appendix for an expression for this state in a more conventional form.) Note that

\[
\Psi' = \Psi (18)
\]

More generally, a state \( \Psi'' \) of \( CQQC \) is a *duplicate state* (or simply *duplication*) of \( \Psi \) if (18) holds (with \( \Psi' \) replaced by \( \Psi'' \)) and \( \Psi'' \) has the form \( \Psi'' = \sum_i e_i \otimes \psi_i \otimes e_i \), where each \( \psi_i \) is a pure subnormalized state of \( QQ \).
Duplicate states have the following universality property: for any subnormalized classical-quantum state $\Phi$ of $CQRD$, where $R$ is a quantum register and $D$ is a classical register, such that

\[ \Phi = CQ^R D \Psi \tag{19} \]

there exists a causal process $\alpha$ from $QC$ to $RD$ satisfying

\[ \Phi = CQ^R D \Psi' \tag{20} \]

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

**Proposition 2.3.** If $\Psi, \Phi$ are subnormalized states that satisfy $\Psi = \epsilon \Phi$, and $\Psi', \Phi'$ denote their respective canonical duplicate states, then $\Psi' = \sqrt{\epsilon} \Phi'$. \[ \square \]

The next corollary will be useful in later proofs.

**Corollary 2.4.** Suppose that

\[ \Phi = \epsilon \Psi \tag{21} \]

Let $\Psi''$ be a state on $CQQC$ that is a duplicate of $\Psi$. Then, there exists a causal process $\alpha$ from $QC$ to $RD$ satisfying

\[ \Phi = \sqrt{2^{\epsilon}} \Psi'' \tag{22} \]

**Proof.** By the universality property noted above, it suffices to prove this with $\Psi''$ replaced by the canonical duplicate state $\Sigma$ of $\Psi$. By Proposition 2.3, the canonical duplicate state $\Sigma$ of the state on the left side of (21) satisfies $\Sigma = 2^{\epsilon} \Psi'$. There is a causal process $\alpha$ from $QC$ to $RD$ such that

\[ \Phi = \Sigma \tag{23} \]

Applying the same process to $\Psi'$ yields a state that is within distance $\sqrt{2^{\epsilon}}$ from $\Phi$. \[ \square \]

### 3 Untrusted quantum processes

An *untrusted quantum process* is represented by a diagram in which all of the quantum processes are unlabelled and all of the classical processes are labelled. 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 $k \geq 2$ parties in which the players are given random inputs $X_1, \ldots, X_k$, respectively, according to some fixed joint probability distribution, and they 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 $\mathbb{C}^2$).

\[
\begin{array}{c}
X \\
\downarrow \\
A \\
\downarrow \\
B \\
\downarrow \\
Y
\end{array}
\]

The effect at the top denotes the map $\mathbb{C}^{\{0,1\}^4} \rightarrow \mathbb{C}$ given by $(p_{xaby}) \mapsto \sum_a \delta_{b=x \wedge y} p_{xaby}$. 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

Now we are 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 [29] and Ekert [19]. 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 [8].)

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

\[
\begin{array}{c}
c \downarrow \\
S \downarrow \\
\downarrow \\
c \downarrow \\
q_1 \downarrow \\
q_2
\end{array}
\]

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:

\[
\begin{array}{c}
q_i \\
\downarrow \\
q_j
\end{array}
\]
2. **Deterministic classical functions.** A deterministic function is applied to the register $C$.

\[
\begin{array}{c}
C \\
\downarrow \\
\hat{F} \\
\downarrow \\
C
\end{array}
\] (27)

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 $\sum_i \lambda_i e_i \mapsto \sum_{c_i \in S} \lambda_i e_i$.)

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

\[
\begin{array}{c}
C \\
\downarrow \\
G \\
\downarrow \\
Q_i
\end{array}
\] (28)

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

\[
\begin{array}{c}
Q_i \\
\downarrow \\
\hat{R} \\
\downarrow \\
C
\end{array}
\] (29)

Note that every device-independent protocol has two representations: one is as a diagram (including some unlabelled elements) and the other is 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 [15] 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 [31] for an example). For the purposes of our discussions here, we need only to assert that secure randomness expansion protocols exist.

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.,

\[
\begin{array}{c}
M \\
\downarrow \\
R \\
\downarrow \\
N
\end{array} \quad = \delta
\] (30)
(Here we have 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 $\mathbb{C}^M$ and $\mathbb{C}^N$.) 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 $N$ and classical output dimension $2N$, and there exists a function $\delta = \delta(N) \in 2^{-\Omega(N)}$, such that the following hold.

1. **Soundness.**

\[
\subseteq_{\delta}
\]

2. **Completeness.**

\[
1 - \delta \in \subseteq \]

**Proof.** This is a special case of results from, e.g., section 2 of [31]. □

“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 $C$ 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 $\epsilon \in 2^{-\Omega(N)}$ such that for every integer $N \geq 1$,

---

2In [31], a protocol is presented which includes a parameter $q > 0$ such that the protocol obtains $\Omega(N)$ random bits from a seed of size $O(Nq \log q + \log^2 N)$, with error $O(2^{-\Omega(qN)})$. By taking $q$ to be some sufficiently small constant we obtain Theorem 4.1.
Proof. Let $\delta$ be as in Theorem 4.1, let $N$ be a positive integer, and let $r \in R(N)$. We have

\begin{equation}
\Gamma r^2 N = \delta \Gamma r (33)
\end{equation}

for any pure state $\Gamma$. We construct a duplication of the state on the right side of the above equation. The effect

\begin{equation}
X \mapsto (X, \sum_{ijk} \sigma_{ijk} e_i \otimes f_j \otimes f_k)\ (34)
\end{equation}

can be written as $X \mapsto \langle X, \sum_{ijk} \sigma_{ijk} e_i \otimes f_j \otimes f_k \rangle$ for some $\sigma_{ijk} \in \mathbb{C}$, where the matrices $\Sigma^i = [\sigma_{ijk}]_{jk}$ are positive semidefinite. Let

\begin{equation}
\Gamma b (35)
\end{equation}

denote the controlled pure process

\begin{equation}
X \mapsto \left( \sum_i e_i e_i^* \otimes \sqrt{\Sigma_i} \otimes \sqrt{\Sigma_i} \right) X \ (36)
\end{equation}

Then,

\begin{equation}
\Gamma b \ (37)
\end{equation}

is a duplication of the state

\begin{equation}
\Gamma r \ (38)
\end{equation}

Likewise, the state

\begin{equation}
\Gamma b \ (39)
\end{equation}
is a duplication of the state on the right side of (33). Therefore by Corollary 2.4 there is a causal process \( c \) such that

\[
\Gamma_r = \sqrt{2} \delta N^2 N_b \Gamma(40)
\]

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 the uniform state on \( \mathbb{C}^{2N} \). (This is similar to the use of “adjustment completeness error” in [31].)

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

\[
R(N) \in \zeta 2^{-N}(41)
\]

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

\[
\square 2N \in \delta \Gamma(42)
\]

The desired result follows, with \( \zeta = 2\delta \). \( \square \)

### 4.2 Unbounded randomness expansion

Now we discuss a graphical proof of unbounded (rather than linear) randomness expansion. We begin with the following elementary remarks.

**Remark 4.4** (Causality). A process \( T \) 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.,

\[
\square T = \square
\]

**Remark 4.5** (Deleting copies of uniform states). Uniform states absorb terminations, e.g.,

\[
\square = \square
\]
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, but [8, 17, 31] observed that we can still obtain unbounded randomness via spot-check 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 4.6.** For any integer $N \geq 1$, let $S(N)$ denote the set of processes given by

\[
S(N) := R(N) \circ R(2N) \circ \ldots \circ R(N)
\]

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

\[
S(M) \subseteq \epsilon' - 4M \leq C - \epsilon(M)
\]

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

**Proof.** We first use Definition 4.6 to expand the left-hand side of Equation (43) and then apply Lemma 4.2 to the occurrence of $R(M)$ in the resulting diagram.
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.

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

Lemma 4.8. For all integers $N, k \geq 1$, we have

\[
S_k(N) \subseteq \gamma N \subseteq \gamma (4kN - 1) 
\]

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

Proof. By induction on $k$. The case $k = 1$ follows from Lemma 4.7 by setting $M = N$. So suppose that $k > 1$. Then we can expand the left-hand side of Equation (44) and apply the induction hypothesis to obtain

\[
S(4^{k-1}N - 1) \subseteq \alpha N \subseteq \beta (4^{k-1}N - 1) 
\]

where $\alpha = \epsilon(M) + \epsilon(2M) + \ldots + \epsilon(2^{2k-1}M)$ and $\beta = \epsilon(2^{2k-2}M) + \epsilon(2^{2k-1}M)$. The desired result follows.
Theorem 4.9 (Soundness for Unbounded Expansion). There is a function $\lambda = \lambda(N) \in 2^{-\Omega(N)}$ such that for any $N, k \geq 1$,

\begin{equation}
\begin{aligned}
4^k N & \quad \underset{\text{S}_k(N)}{\Rightarrow} \quad X \\
\downarrow & \quad \downarrow \\
N & \quad \subseteq \lambda \\
& \quad X \quad \downarrow \quad \Box \\
4^k N & \quad \downarrow \\
\end{aligned}
\end{equation}

Proof. By Remark 4.5, we can add a terminated branch to the left-hand side of Equation (45) so that we can apply Lemma 4.8.

We next apply Remark 4.4 (causality) followed by Remark 4.5.

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 $\{0, 1, 2, \ldots, \}$

\begin{equation}
f \in 2^{-\Omega(N)} \implies \sum_{i=0}^{\infty} f(2^i N) \in 2^{-\Omega(N)}. \tag{46}
\end{equation}

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

Theorem 4.9 asserts soundness for $S_k(N)$. Completeness for $S_k(N)$ follows easily from Lemma 4.3 and fact (46) 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 (semi-)formal verification of our proof using the Globular proof assistant [4] for the case \( k = 2 \). The reader can find and explore the Globular proof at [21], and a video is available at [22]. The Globular proof assistant [4] provides a system for creating string diagrams 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. Proofs become three-dimensional diagrams, though we often think of them in as a “movie” of slices which traces through the diagrams of the proof.

In this case, we used Globular to prototype the proof of Theorem 4.9. 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 4.9 for \( k = 2 \); the entire proof involved 66 steps.

![Figure 1: Steps in a Globular proof of theorem 4.9 for \( k = 2 \)](image)

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 4.9. 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 63 to step 66 (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, 24 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-checking 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 also 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 translation 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.

References

[1] S. Aaronson. Quantum Randomness. American Scientist, 102(4), Jul 2014.

[2] S. Abramsky and B. Coecke. A Categorical Semantics of Quantum Protocols. CoRR, quant-ph/0402130, 2004. Preprint available from [arXiv:0402130](http://arxiv.org/abs/quant-ph/0402130).

[3] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and Tight Device-Independent Security Proofs. Available from [arXiv:1607.01797](http://arxiv.org/abs/1607.01797), Jul 2016.

[4] K. Bar, A. Kissinger, and J. Vicary. Globular: an Online Proof Assistant for Higher-Dimensional Rewriting. Available from [arXiv:1612.01093](http://arxiv.org/abs/1612.01093), Dec 2016.

[5] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm. Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling. Available from [arXiv:1702.05178](http://arxiv.org/abs/1702.05178), 2017.

[6] F. Bonchi, P. Sobocinski, and F. Zanasi. A categorical semantics of signal flow graphs. In CONCUR 2014 - Concurrency Theory - 25th International Conference, CONCUR 2014, Rome, Italy, September 2-5, 2014. Proceedings, pages 435–450, 2014.

[7] N. Chancellor, A. Kissinger, S. Zohren, and D. Horsman. Coherent Parity Check Construction for Quantum Error Correction. Available from [arXiv:1611.08012](http://arxiv.org/abs/1611.08012), Nov 2016.

[8] K.-M. Chung, Y. Shi, and X. Wu. Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions. Available from [arXiv:1402.4797](http://arxiv.org/abs/1402.4797), Feb 2014.

[9] B. Coecke. From Quantum Foundations via Natural Language Meaning to a Theory of Everything. Available from [arXiv:1602.07618](http://arxiv.org/abs/1602.07618), Feb 2016.
[10] B. Coecke and A. Kissinger. Categorical Quantum Mechanics I: Causal Quantum Processes. Available from arXiv:1510.05468 Oct 2015.

[11] B. Coecke and A. Kissinger. Categorical Quantum Mechanics II: Classical-Quantum Interaction. Available from arXiv:1605.08617 May 2016.

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

[13] B. Coecke and S. Perdrix. Environment and Classical Channels in Categorical Quantum Mechanics, pages 230–244. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. Preprint available from arXiv:1004.1598.

[14] B. Coecke, Q. Wang, B. Wang, Y. Wang, and Q. Zhang. Graphical Calculus for Quantum Key Distribution (Extended Abstract). Electron. Notes Theor. Comput. Sci., 270(2):231–249, Feb. 2011.

[15] R. Colbeck. Quantum And Relativistic Protocols For Secure Multi-Party Computation. Ph.D. thesis, University of York, 2007. Preprint available from arXiv:0911.3814.

[16] M. Coudron and H. Yuen. Infinite Randomness Expansion and Amplification with a Constant Number of Devices. Preprint available from arXiv:1310.6755 Oct 2013.

[17] M. Coudron and H. Yuen. Infinite Randomness Expansion with a Constant Number of Devices. In Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing, STOC ’14, pages 427–436, New York, NY, USA, 2014. ACM. Preprint available from arXiv:1310.6755.

[18] F. Dupuis, O. Fawzi, and R. Renner. Entropy Accumulation. Available from arXiv:1607.01796 Jul 2016.

[19] A. K. Ekert. Quantum cryptography based on bell’s theorem. Phys. Rev. Lett., 67:661–663, Aug 1991.

[20] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. Physical Review A, 87(1):012335, 2013. Preprint available from arXiv:1111.6052.

[21] Globular. Proof. http://globular.science/1712.001v1 Accessed: 2018-01-04.

[22] Globular. Video. Available as ancillary material at arXiv:1705.09213 Accessed: 2018-01-04.

[23] C. Heunen. Compactly Accessible Categories and Quantum Key Distribution. Logical Methods in Computer Science, 4(4), 2008. Preprint available from arXiv:0811.2113.

[24] A. Hillebrand. Superdense Coding with GHZ and Quantum Key Distribution with W in the ZX-calculus. In Proceedings 8th International Workshop on Quantum Physics and Logic, 2011. Preprint available from arXiv:1210.0650.

[25] A. Joyal and R. Street. The Geometry of Tensor Calculus, I. Advances in Mathematics, 88(1):55–112, 1991.

[26] A. Kissinger, S. Tall, and B. Westerbaan. Picture-perfect Quantum Key Distribution. Available from arXiv:1704.08668 Apr 2017.

[27] A. Kissinger and S. Uijlen. A Categorical Semantics for Causal Structure. Available from arXiv:1701.04732 Jan 2017.

[28] U. Maurer and R. Renner. Abstract Cryptography. In Innovations in Computer Science, pages 1–21. Tsinghua University Press, 2011.
In this section we revert to standard notation for quantum systems. The state $\Psi$ can be written as a density operator
\begin{equation}
\Psi = \sum_i |c_i\rangle \langle c_i| \otimes M_i,
\end{equation}
where \( \{ c_i \} \) is the standard basis for \( c_i \) and \( M_i \) are positive semidefinite operators on \( Q_1 \), where \( Q = Q_1 \otimes Q_1 \). Then, the duplicated state of \( \Psi \) is given by

\[
\Psi' = \sum_i |c_i \rangle \langle c_i| \left( \text{Vec} \sqrt{M_i} \right) \left( \text{Vec} \sqrt{M_i} \right)^*,
\]

where \( \text{Vec}(X) \) denotes the vector \( \sum_{ij} x_{ij} |q_i \rangle|q_j \rangle \), where \( \{ q_i \} \) denotes the standard basis for \( Q_1 \) and \( X = \sum_{ij} x_{ij} |q_i \rangle|q_j \rangle \). If \( \Phi \) is such that \( \Psi = \epsilon \Phi \), then

\[
\| \Psi - \Phi \|_1 \leq 2\epsilon,
\]

and therefore if we let

\[
\Phi = \sum_i |c_i \rangle \langle c_i| \otimes M'_i,
\]

we have

\[
\sum_i \| M_i - M'_i \|_1 \leq 2\epsilon.
\]

By Lemma 3.37 from [42], we have

\[
\sum_i \| \sqrt{M_i} - \sqrt{M'_i} \|_2^2 \leq 2\epsilon.
\]

For any \( i \),

\[
\left\| (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* - (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* \right\|_1 \\
\leq \left\| (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* - (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* \right\|_1 \\
+ \left\| (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* - (\text{Vec} \sqrt{M_i})(\text{Vec} \sqrt{M_i})^* \right\|_1 \\
\leq \| \text{Vec} \sqrt{M_i} \| \| \text{Vec} \sqrt{M_i} \| + \| \text{Vec} \sqrt{M_i} \| \| \text{Vec} \sqrt{M_i} \|
\]

Therefore, applying the Cauchy-Schwartz inequality, the trace distance between the duplicated states of \( \Phi \) and \( \Psi \) is upper bounded by

\[
\sum_i \left( \| \text{Vec} \sqrt{M_i} \| + \| \text{Vec} \sqrt{M_i} \| \right) \| \text{Vec} \sqrt{M_i} - \text{Vec} \sqrt{M_i} \| \\
\leq \sqrt{\sum_i \left( \| \text{Vec} \sqrt{M_i} \| + \| \text{Vec} \sqrt{M_i} \| \right)^2} \left[ \sum_i \| \text{Vec} \sqrt{M_i} - \text{Vec} \sqrt{M_i} \|^2 \right] \\
\leq \sqrt{4 \cdot 2\epsilon},
\]

as desired.