Graphical Methods in Device-Independent Quantum Cryptography

Spencer Breiner,[1] Carl A. Miller,[1,2] and Neil J. Ross[2]

[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

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 as least as far as Penrose's use of diagrams [32]. During the last decade of the twentieth century, rigorous methods for graphical reasoning in monoidal categories were developed by Joyal, Street, and others [23, 36]. 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 [41], quantum error correction [8], and beyond [10]. 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 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 [11, 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 [14, 22, 13], 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. (One important example is [9], which has a focus similar to the current paper. See also [26, 31, 38, 21]).

[1]See Section 12.6 of [30] for an introduction.

One of the recent major achievements of quantum cryptography is the development of *device-independent* security proofs [27]. 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. Our goal is to provide a graphical framework for device-independent security proofs.

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 [15, 33, 40, 34, 20, 17, 29, 28, 19, 5, 7]. 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 [3] for a gentle introduction to this topic and [37] for a discussion of possible implementation.

Recent work [17, 9, 29] 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 achieve an arbitrary amount of randomness generation from a fixed 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 fairly compact proof of this extension (based on [9, 29]) using a graphical language. Explicitly, we prove graphically that any secure protocol for linear randomness expansion implies a secure protocol for unbounded randomness expansion.

A great benefit of graphical proofs is they are also highly amenable to computer verification. The Globular proof assistant software [6] carries out category-theoretic proofs, using diagrams that are easily compatible with [11, 12]. 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 [1].

This extended abstract is organized as follows. In Section 2 we formalize a language for dealing with quantum processes, building on [11, 12] 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.

1.1 Recent work

A new preprint [24] addresses a different problem in the graphical setting (device-dependent quantum key distribution) and gives a security proof that improves on previous graphical security proofs. The early technical material in this paper and in [24] (which were written independently) develop some similar concepts. In particular, our notion of approximation of processes (denoted $=_\epsilon$) is essentially the same as theirs. We expect that there will be a useful synergy between the two papers.

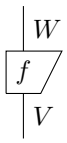
2 Fundamentals

In this section, we briefly review useful techniques and concepts. 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 symmetric purification. For further details the reader is encouraged to consult [11, 12] for categorical quantum mechanics and [42] for notions of distance relevant to quantum information theory.

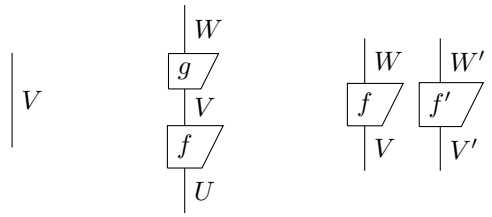
2.1 The graphical language of categorical quantum mechanics

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 a space of dimension n for every non-negative integer n. We sometimes refer to the elements of O as *types*

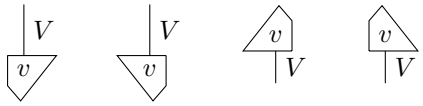
or *registers*. We say that f is a *process of type* $V \to W$ if f is a linear operator $V \to W$. It is represented by a box labelled f whose input and output wires are labelled with the types V and W as follows.



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).

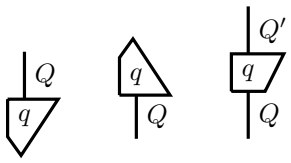


Note that two processes can be vertically composed only if their types are compatible. A process with no input wires is a *state*. A state v of type V should be interpreted as a vector in V and is represented by the first diagram below. The conjugate, transpose, and conjugate-transpose (i.e., adjoint)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



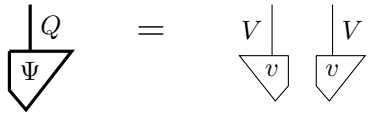
A process with no output wires is called an *effect*. A process with no input and no output is a *number*. Because they will play an important role below, we introduce special notations for the *uniform vector* $(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n})$ in a space V of dimension n (which we represent by the gray node on the left below) and for real numbers $r \in [0, 1]$ (which we represent by the diamond on the right below).

The diagrams introduced so far are *classical*. A *quantum* type or 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 diagrams below.

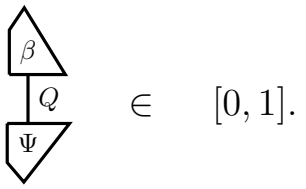


Quantum states correspond to density matrices. A quantum state v is *pure* if it is of the form $v \otimes \overline{v}$ with

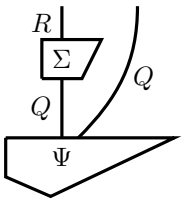
$\|v\| = 1$. Graphically, a quantum state is pure if it satisfies the diagrammatic equality below.



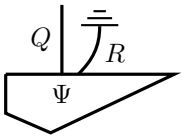
A *mixed* quantum state of Q is an element of the form $\sum_i v_i \otimes \overline{v_i}$ satisfying $\sum_i \|v_i\|^2 = 1$. A *subnormalized mixed state* is only required to satisfy $\sum_i \|v_i\|^2 \leq 1$. Unless otherwise specified, the word "state" refers to a normalized mixed state. In what follows, we always assume that quantum effects correspond to positive semidefinite operators with operator norm ≤ 1. That is, if β is a quantum effect and Ψ is any compatible quantum state then



A process Σ from a register Q to another register R is a linear homomorphism such that for any state Ψ of $Q \otimes Q$, the diagram below represents a state. That is, processes correspond to completely positive trace-preserving maps.



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



A diagram in which every element is labelled denotes a linear map. A diagram in which some elements are unlabelled denotes a *set* of linear maps. For example, the diagram

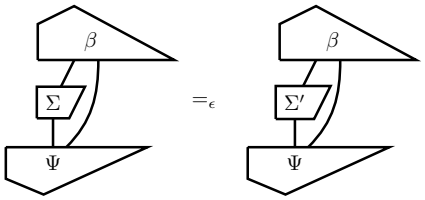
denotes the set of all (normalized mixed) states of Q. A single unlabelled wire denotes the set of all identity functions $\{Id_V : V \to V \mid V \in O\}$. In general, a diagram denotes the set of all processes that can be expressed in the form shown in the diagram.

We will use the picture element $\diamondsuit$ 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 introduce a relation between diagrams which captures the appropriate metric (half of the diamond norm, see [42] for further details).

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



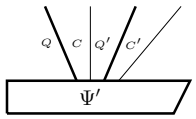
If we restrict the processes Σ and Σ' to be states (i.e., to have no inputs) then $\Sigma =_\epsilon \Sigma'$ if Σ and Σ' differ by no more than 2ϵ in trace distance. It can be verified that the notion of approximation defined above satisfies the triangle inequality: if $\Sigma =_\epsilon \Sigma'$ and $\Sigma' =_\delta \Sigma''$, then $\Sigma =_{\epsilon+\delta} \Sigma''$. Next we generalize the notion of distance between processes to a notion of distance between *sets* of processes. (The reader can compare the next definition to the notion of approximation in [26], which is similar.)

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 $A \subseteq_\epsilon B$.*

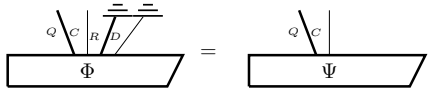
Note that the symbol $=_\epsilon$ is used to denote a relation between numbers, a relation between processes, and a relation between sets of processes. However, it will always be clear from the context whether numbers, processes, or sets of processes are being compared so that no ambiguity should arise from this slight abuse of notation.

2.3 Symmetric purification

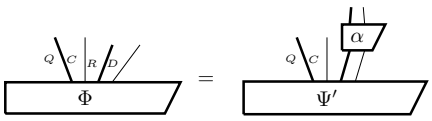
If Ψ is a state of classical-quantum register CQ, then a *symmetric purification* of Ψ is a state



where Ψ' is invariant under swapping the input wires $C \leftrightarrow C', Q \leftrightarrow Q'$, and is such that for any state Φ satisfying



there exists a process α satisfying



The symmetric purification exists and is unique – an expression is given by equation (8) of Appendix A.

If Ψ is a quantum state on a register Q, then the symmetric purification is a purification (in the traditional sense) of Ψ. If Ψ is a classical state on a register C, then the symmetric purification of Ψ simply results from copying the value of C into an additional register.[2]

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

[2]This is a small abuse of terminology, since the purification of a classical state is not itself "pure" in the standard sense. We are using the term "purification" here because the symmetric purification of a classical-quantum state has properties analogous to a purification of a quantum state.

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

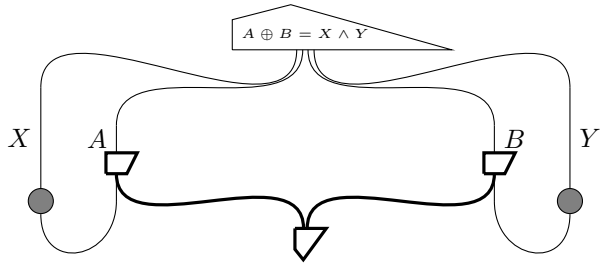
Note that, by the definition of symmetric purification, it suffices in Definition 2.1 to let Ψ vary over symmetric purification states.

3 Untrusted quantum processes

An *untrusted quantum protocol* 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.



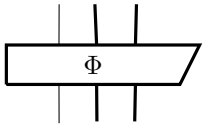
The effect at the top denotes the map $\left(\mathbb{C}^2\right)^{\otimes 4} \to \mathbb{C}$ representing the Boolean function $(A, X, Y, B) \mapsto (A \oplus B = X \wedge Y)$. This game is a building block for the randomness expansion results that we will consider in section 4.

3.2 Device-independent quantum protocols

Now we are ready to formalize the notion of a protocol in the device-independent setting. We need to specify exactly which operations are possible for the classical user. (Our treatment can be compared to the non-graphical formalization of device-independent protocols in section 4 of [9].)

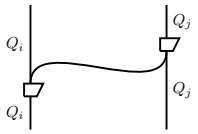
For simplicity our definition is for a 2-device protocol, but it could easily be generalized to an N-device protocol.

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



where Φ is constructed from the following subdiagrams.

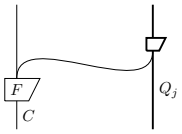
1. ***Communication between devices.*** *An untrusted process transferring information (one way) from one of the two quantum registers to the other:*



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

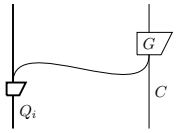
3. ***Failure.*** *The value of the classical register C is checked to see if it lies in a chosen subset S; if it does not, the protocol aborts.*[3]

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



   Here, F denotes a (trusted) deterministic function.

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



Device-independent protocols are sets of linear operators. Device-independent protocols can be composed (i.e. 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

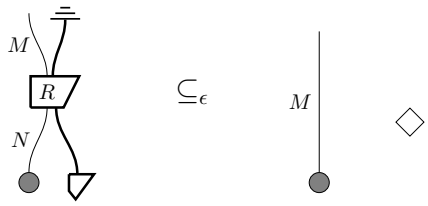
4.1 Linear randomness expansion

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 [29] for an example). For the purposes of our discussions here, we need only to assert that secure randomness expansion protocols exist.

[3] Mathematically, this process is the map $\sum p_i c_i \mapsto \sum_{c_i \in S} p_i c_i$.

A simple way to assert security for a 2-device randomness expansion protocol R is to say that when the protocol succeeds, its classical output by itself is approximately uniform, i.e.,

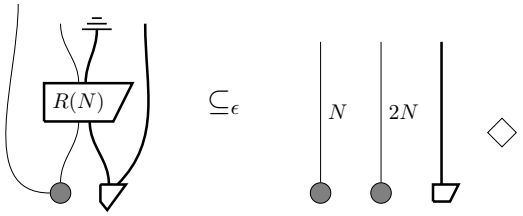


(1)

(Here we have compressed the two device states of R into a single thick wire, and we are using the labels M and N to specify the dimensions of the classical wires.) 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 $\epsilon = \epsilon(N) \in 2^{-\Omega(N)}$, such that the following holds.*

1. ***Soundness.***



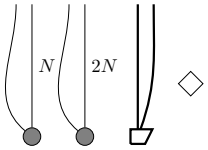
(2)

2. ***Completeness.***

(3)

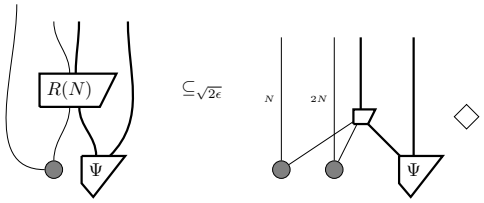
Proof. This is a special case of results from, e.g., section 2 of [29].[4] □

"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. We deduce a corollary of this result which will be more convenient for later proofs. First note that the symmetric purification of the diagram on the right of (2) has the form



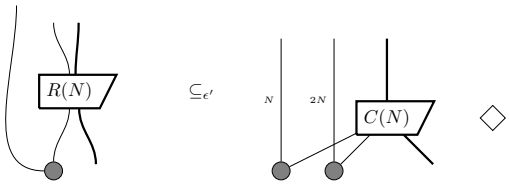
[4] In [29], a protocol is presented which includes a parameter $q > 0$ such that the protocol obtains $\Omega(N)$ random bits from a seed of size $O(Nq \log q + \log^2 N)$, with error $O(2^{-\Omega(qN)})$. By taking q to be some sufficiently small constant we obtain Theorem 4.1.

Therefore by Proposition 2.3, for any symmetric purification state Ψ,



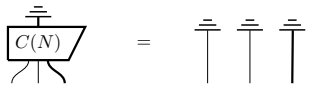
We then have the following corollary, which is expressed in terms of processes rather than in terms of states, and which will serve as a lemma in the proof of unbounded expansion.

Corollary 4.2 (**Spot-check lemma**). *There exists $\epsilon' \in 2^{-\Omega(N)}$ and sets of processes $C(1), C(2), \ldots$ such that*



4.2 Unbounded randomness expansion

Now we discuss a graphical proof of unbounded (rather than linear) randomness expansion. As a preface, note that if we were to assume Corollary 4.2 and we wish to prove linear randomness expansion, there is an easy (and easily generalized) way to do so. The correlation procedure $C(N)$ is completely positive and trace-preserving, which means that it is a *causal process* in the terminology of Kissinger [25]. Diagrammatically, this means that discarding the output of C is equivalent to simply discarding its inputs and never running the process at all:

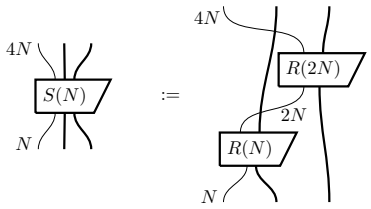


(4)

By combining this observation with the spot-check lemma, one can easily recover the statement of theorem 4.1.

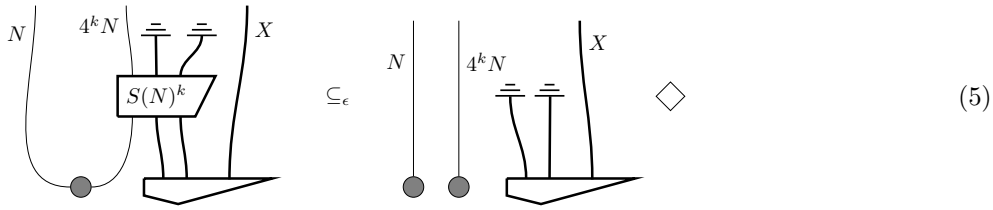
Next, we would like to apply the spot-checking protocol and lemma repeatedly, in order to obtain unbounded randomness expansion. Naívely stacking $R(N)$ operations atop one another does not work, but [17, 9, 29] observed that we can still obtain unbounded randomness via spot-check by employing a pair of devices and alternating which device is employed in the protocol. In effect, 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.

Formally, we iterate the following derived protocol $S(N)$:



By abuse of notation, we let $S(N)^k$ denote the iterated composition of $S(N), S(2N), \ldots, S(2^{k-1}N)$.

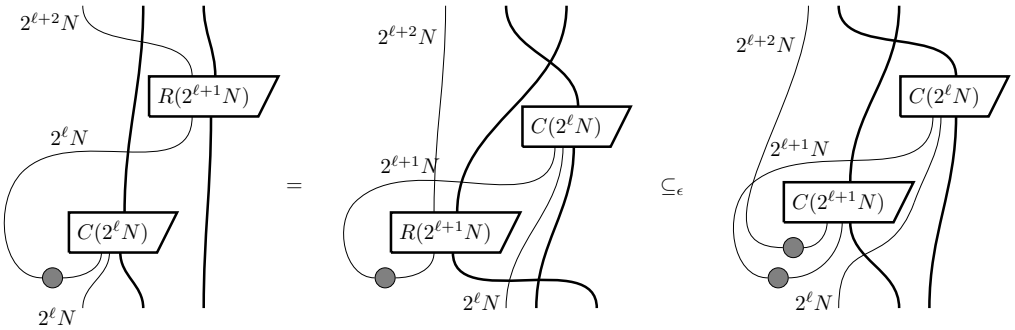
Theorem 4.3. *The spot-check protocol, together with two untrusted quantum devices, can be used to generate unbounded randomness from a uniformly random initial seed by applying the $S(N)$ protocol an arbitrary number of times and discarding the quantum devices at the end. More specifically, for fixed k, there exists a function $\epsilon \in 2^{-\Omega(N)}$ such that the following approximate inclusion holds:*



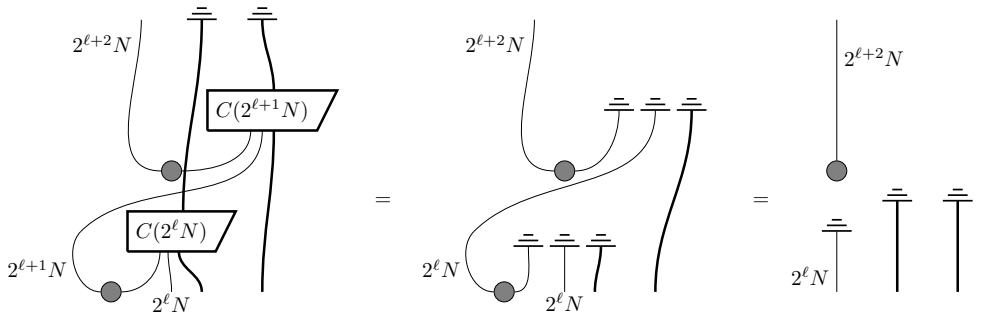
(5)

Proof. The principal difficulty in achieving unbounded randomness expansion is that the argument from causality requires a uniform input to $R(N)$ and a discarded output for $C(N)$, but here these are separated by additional layers of the $S(N)$ protocols. Our strategy is to first apply the spot-check lemma $2k$ times, working our way up from the bottom. Once we reach the top, we can then apply causality in order to complete the proof.

Since the input to overall protocol is uniformly random, it is clear that we can apply the spot-check lemma to the first application of $R(N)$. Now consider an intermediate step in the proof, as depicted below. By sliding boxes past wires and applying symmetry of the Bell state, we can move the application of R below that of C. In particular, the input to R is now uniformly random, so we can again apply the spot-check protocol. Finally, we slide boxes again so that the second application of C is above the first (not pictured).



Proceeding in this fashion, we can convert applications of $R(N)$ to applications of $C(N)$, one by one, until we reach the top of the diagram (5). At this point, we will have discarding operations immediately following the last two correlation protocols $C(2^{k-1}N)$ and $C(2^{k-1}N)$; applying causality disaggregates the inputs to these processes and leaves a free wire (i.e., a Bell state with both sides discarded). In particular, the so-called bone equation allows us to remove these unattached wires.



This again leaves two discards attached to the next layer of $C(N)$ operations; inductively, we eliminate all of them in this way. When we are done, all that is left is the right-hand side of (5), together with some additional free strings (those for even values of ℓ), which can again be removed, yielding the theorem.

The error terms accumulate (via the triangle inequality), but since

$$f \in 2^{-\Omega(N)} \implies \sum_{i=1}^{\infty} f(2^i N) \in 2^{-\Omega(N)} \tag{6}$$

the total error remains exponentially small in N. □

Theorem 4.3 asserts soundness for $S(N)^k$. Completeness for $S(N)^k$ follows easily from completeness for $R(N)$ and fact (6) 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 [6] for the case $k = 2$. The reader can find and explore the Globular proof at [2], and a video is available at [1]. The Globular proof assistant [6] 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 number of 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 (spot-check, correlation), and equations in dimension 3 (spot-check lemma, causality). 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 4.3. 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 4.3 for $k = 2$; the entire proof involved 212 steps.

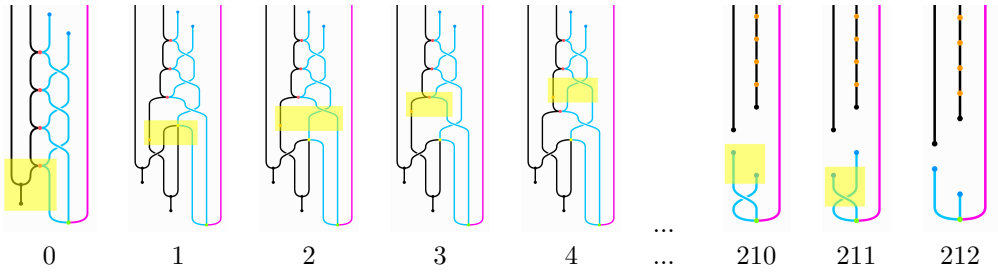


Figure 1: Steps in a Globular proof of theorem 4.3 for $k = 2$

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 (equation 4.2) and the final form of theorem 4.3. 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 (such as needing many individual steps to accomplish simple operations) limit its practical application. 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 4.2, and the other was the principle of *causality*. Causality is an elementary step in symbolic proofs for quantum information, but in 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 discussions that seeded this project. 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] Available at `http://www.umiacs.umd.edu/~camiller/GMQC/unbounded.avi`.

[2] Available at `http://globular.science/1704.003`.

[3] Scott Aaronson (2014): *Quantum Randomness. American Scientist* 102(4).

[4] Samson Abramsky & Bob Coecke (2004): *A categorical semantics of quantum protocols. CoRR* quant-ph/0402130. Preprint available from `arXiv:0402130`.

[5] Rotem Arnon-Friedman, Renato Renner & Thomas Vidick (2016): *Simple and tight device-independent security proofs.* ArXiv:1607.01797.

[6] Krzysztof Bar, Aleks Kissinger & Jamie Vicary (2016): *Globular: an online proof assistant for higher-dimensional rewriting.* Available from `arXiv:1612.01093`.

[7] Peter Bierhorst, Emanuel Knill, Scott Glancy, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam & Lynden K. Shalm (2017): *Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling.* ArXiv:1702.05178.

[8] Nicholas Chancellor, Aleks Kissinger, Stefan Zohren & Dominic Horsman (2016): *Coherent Parity Check Construction for Quantum Error Correction*. Available from `arXiv:1611.08012`.

[9] Kai-Min Chung, Yaoyun Shi & Xiaodi Wu (2014): *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions*. Available from `arXiv:1402.4797`.

[10] Bob Coecke (2016): *From quantum foundations via natural language meaning to a theory of everything*. Available from `arXiv:1602.07618`.

[11] Bob Coecke & Aleks Kissinger (2015): *Categorical Quantum Mechanics I: Causal Quantum Processes*. Available from `arXiv:1510.05468`.

[12] Bob Coecke & Aleks Kissinger (2016): *Categorical Quantum Mechanics II: Classical-Quantum Interaction*. Available from `arXiv:1605.08617`.

[13] Bob Coecke & Simon Perdrix (2010): *Environment and Classical Channels in Categorical Quantum Mechanics*, pp. 230–244. Springer Berlin Heidelberg, Berlin, Heidelberg, doi:`http://dx.doi.org/10.1007/978-3-642-15205-4_20`. Available at `http://dx.doi.org/10.1007/978-3-642-15205-4_20`.

[14] Bob Coecke, Quanlong Wang, Baoshan Wang, Yongjun Wang & Qiye Zhang (2011): *Graphical Calculus for Quantum Key Distribution (Extended Abstract)*. *Electron. Notes Theor. Comput. Sci.* 270(2), pp. 231–249. Available at `http://dx.doi.org/10.1016/j.entcs.2011.01.034`.

[15] Roger Colbeck (2007): *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. Ph.D. thesis, University of York, arXiv:0911.3814.

[16] Matthew Coudron & Henry Yuen (2013): *Infinite Randomness Expansion and Amplification with a Constant Number of Devices*. ArXiv:1310.6755.

[17] Matthew Coudron & Henry Yuen (2014): *Infinite Randomness Expansion with a Constant Number of Devices*. In: *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, ACM, New York, NY, USA, pp. 427–436. Preprint available from `arXiv:1310.6755`.

[18] Anindya De, Christopher Portmann, Thomas Vidick & Renato Renner (2012): *Trevisan's Extractor in the Presence of Quantum Side Information*. *SIAM Journal on Computing* 41(4), pp. 915–940. Preprint available from `arXiv:0912.5514`.

[19] Frederic Dupuis, Omar Fawzi & Renato Renner (2016): *Entropy accumulation*. ArXiv:1607.01796.

[20] Serge Fehr, Ran Gelles & Christian Schaffner (2013): *Security and composability of randomness expansion from Bell inequalities*. *Physical Review A* 87(1), p. 012335.

[21] Chris Heunen (2008): *Compactly Accessible Categories and Quantum Key Distribution*. *Logical Methods in Computer Science* 4(4).

[22] Anne Hillebrand (2011): *Superdense Coding with GHZ and Quantum Key Distribution with W in the ZX-calculus*. arXiv:1210.0650. In Proceedings 8th International Workshop on Quantum Physics and Logic.

[23] André Joyal & Ross Street (1991): *The geometry of tensor calculus, I*. *Advances in Mathematics* 88(1), pp. 55–112.

[24] Aleks Kissinger, Sean Tull & Bas Westerbaan (2017): *Picture-perfect Quantum Key Distribution*. ArXiv:1704.08668.

[25] Aleks Kissinger & Sander Uijlen (2017): *A categorical semantics for causal structure*. Available from `arXiv:1701.04732`.

[26] Ueli Maurer & Renato Renner (2011): *Abstract cryptography.* In: *Innovations in Computer Science*, Tsinghua University Press, pp. 1–21.

[27] D. Mayers & A. Yao (1998): *Quantum cryptography with imperfect apparatus.* In: *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pp. 503–509.

[28] Carl A. Miller & Yaoyun Shi (2015): *Universal security for randomness expansion from the spot-checking protocol.* Available from `arXiv:1411.6608`.

[29] Carl A. Miller & Yaoyun Shi (2016): *Robust Protocols for Securely Expanding Randomness and Distributing Keys Using Untrusted Quantum Devices.* *J. ACM* 63(4), pp. 33:1–33:63. Available at `http://doi.acm.org/10.1145/2885493`.

[30] Michael A. Nielsen & Isaac L. Chuang (2002): *Quantum Computation and Quantum Information.* Cambridge University Press, New York, NY, USA.

[31] Dusko Pavlovic (2014): *Chasing Diagrams in Cryptography.* In: *Categories and Types in Logic, Language, and Physics - Essays Dedicated to Jim Lambek on the Occasion of His 90th Birthday*, pp. 353–367. Preprint available from `arXiv:1401.6488`.

[32] Roger Penrose (1971): *Applications of negative dimensional tensors.* In D.J.A. Welsh, editor: *Combinatorial Mathematics and its Applications*, Academic Press, New York, pp. 221–244.

[33] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning et al. (2010): *Random numbers certified by Bell's theorem.* *Nature* 464(7291), pp. 1021–1024.

[34] Stefano Pironio & Serge Massar (2013): *Security of practical private randomness generation.* *Physical Review A* 87(1), p. 012336.

[35] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner & Björn Tackmann (2015): *Causal Boxes: Quantum Information-Processing Systems Closed under Composition.* ArXiv:1512.02240.

[36] P. Selinger (2011): *A Survey of Graphical Languages for Monoidal Categories*, pp. 289–355. Springer Berlin Heidelberg, Berlin, Heidelberg. Preprint available from `arXiv:0908.3347`.

[37] National Institute of Standards & Technology (NIST): *Randomness Beacon Program.* `https://www.nist.gov/programs-projects/nist-randomness-beacon`. Accessed: 2017-04-19.

[38] Mike Stay & Jamie Vicary (2013): *Bicategorical Semantics for Nondeterministic Computation.* *Electron. Notes Theor. Comput. Sci.* 298, pp. 367–382. Available at `http://dx.doi.org/10.1016/j.entcs.2013.09.022`.

[39] Marco Tomamichel (2016): *Quantum Information Processing with Finite Resources.* Springer International Publishing.

[40] Umesh Vazirani & Thomas Vidick (2012): *Certifiable quantum dice: or, true random number generation secure against quantum adversaries.* In: *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, ACM, pp. 61–76.

[41] Jamie Vicary (2013): *Topological Structure of Quantum Algorithms.* In: *28th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2013, New Orleans, LA, USA, June 25-28, 2013*, pp. 93–102. Available at `http://dx.doi.org/10.1109/LICS.2013.14`. Preprint available from `arXiv:1209.3917`.

[42] John Watrous: *Theory of Quantum Information.* Available at `https://cs.uwaterloo.ca/~watrous/TQI/`.

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

$$\Psi \quad = \quad \sum_i |c_i\rangle \langle c_i| \otimes M_i, \tag{7}$$

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 symmetric purification for Ψ is given by

$$\Psi \quad = \quad \sum_i |c_i\rangle \langle c_i| \, |c_i'\rangle \langle c_i'| \left(\mathrm{Vec}\sqrt{M_i}\right) \left(\mathrm{Vec}\sqrt{M_i}\right)^*, \tag{8}$$

where $\mathrm{Vec}(X)$ denotes the vector $\sum_{ij} x_{ij} |q_i q_j\rangle$, where $\{q_i\}$ denotes the standard basis for Q_1 and $X = \sum_{ij} x_{ij} |q_i\rangle \langle q_j|$. If Φ is such that

$$\Psi \quad =_\epsilon \quad \Phi, \tag{9}$$

then

$$\|\Psi - \Phi\|_1 \quad \leq \quad 2\epsilon, \tag{10}$$

and therefore if we let

$$\Phi \quad = \quad \sum_i |c_i\rangle \langle c_i| \otimes M_i', \tag{11}$$

we have

$$\sum_i \|M_i - M_i'\|_1 \quad \leq \quad 2\epsilon. \tag{12}$$

By Lemma 3.37 from [42], we have

$$\sum_i \left\| \sqrt{M_i} - \sqrt{M_i'} \right\|_2^2 \quad \leq \quad 2\epsilon. \tag{13}$$

For any i,

$$\begin{aligned}
& \left\| (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^* - (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^* \right\|_1 \\
\leq \quad & \left\| (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i})^* - (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i'})^* \right\|_1 + \left\| (\mathrm{Vec}\sqrt{M_i})(\mathrm{Vec}\sqrt{M_i'})^* - (\mathrm{Vec}\sqrt{M_i'})(\mathrm{Vec}\sqrt{M_i'})^* \right\|_1 \\
= \quad & \left\| \mathrm{Vec}\sqrt{M_i} \right\| \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M_i'} \right\| + \left\| \mathrm{Vec}\sqrt{M_i'} \right\| \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M_i'} \right\|
\end{aligned}$$

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

$$\begin{aligned}
& \sum_i \left(\left\| \mathrm{Vec}\sqrt{M_i} \right\| + \left\| \mathrm{Vec}\sqrt{M_i'} \right\| \right) \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M_i'} \right\| \\
\leq \quad & \sqrt{\left[\sum_i \left(\left\| \mathrm{Vec}\sqrt{M_i} \right\| + \left\| \mathrm{Vec}\sqrt{M_i'} \right\| \right)^2 \right] \left[\sum_i \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M_i'} \right\|^2 \right]} \\
\leq \quad & \sqrt{\left[\sum_i \left(2 \left\| \mathrm{Vec}\sqrt{M_i} \right\|^2 + 2 \left\| \mathrm{Vec}\sqrt{M_i'} \right\|^2 \right) \right] \left[\sum_i \left\| \mathrm{Vec}\sqrt{M_i} - \mathrm{Vec}\sqrt{M_i'} \right\|^2 \right]} \\
\leq \quad & \sqrt{4 \cdot 2\epsilon},
\end{aligned}$$

as desired.