Three-Party Quantum Self-Testing with a Proof by Diagrams

Spencer Breiner
NIST
spencer.breiner@nist.gov

Amir Kalev
Joint Center for Quantum Information and Computer Science (QuICS)
amirk@umd.edu

Carl A. Miller
NIST
Joint Center for Quantum Information and Computer Science (QuICS)
camiller@umd.edu

Quantum self-testing addresses the following question: is it possible to verify the existence of a multipartite state even when one's measurement devices are completely untrusted? This problem has seen abundant activity in the last few years, particularly with the advent of parallel self-testing (i.e., testing several copies of a state at once), which has applications not only to quantum cryptography but also quantum computing. In this work we give the first error-tolerant parallel self-test in a three-party (rather than two-party) scenario, by showing that an arbitrary number of copies of the GHZ state can be self-tested. In order to handle the additional complexity of a three-party setting, we use a diagrammatic proof based on categorical quantum mechanics, rather than a typical symbolic proof. The diagrammatic approach allows for manipulations of the complicated tensor networks that arise in the proof, and gives a demonstration of the importance of picture-languages in quantum information.

1 Introduction

Quantum rigidity has its origins in quantum key distribution, which is one of the original problems in quantum cryptography. In the 1980's Bennett and Brassard proposed a protocol for secret key distribution across an untrusted public quantum channel [3]. A version of the Bennett-Brassard protocol can be expressed as follows: Alice prepares N EPR pairs, and shares the second half of these pairs with Bob through the untrusted public channel. Alice and Bob then perform random measurements on the resulting state, and check the result to verify that indeed their shared state approximates N EPR pairs. If these tests succeed, Alice and Bob then use other coordinated measurement results as the basis for their shared key. Underlying the proof of security for the Bennett-Brassard protocol is the idea that if a shared 2-qubit state approximates the behavior of a Bell state under certain measurements, then the state itself must itself approximate a Bell state.

If we wish to deepen the security, we can ask: what if Alice's and Bob's measurement devices are also not trusted? Can we prove security at a level that guards against possible exploitation of defects in their measurement devices? This leads the question of quantum rigidity: is it possible to completely verify the behavior of n untrusted quantum measurement devices, based only on statistical observation of their measurement outputs, and without any prior knowledge of the state they contain?

We say that a n-player cooperative game is *rigid* if an optimal score at that game guarantees that the players must have used a particular state and particular measurements. We say that a state is *self-testing* if its existence can be guaranteed by such a game. Early results on this topic focused on self-testing the 2-qubit Bell state [31, 19, 24]. Since then a plethora of results on other games and other states have appeared. The majority of works have focused on the bipartite case, and there are a smaller number of works that address n-partite states for $n \geq 3$ [25, 21, 38, 37, 29, 14].

More recently, it has been observed that rigid games exist that self-test not only one copy of a bipartite state, but several copies at once. Such games are a resource not only for cryptography, but also for

Submitted to:
QPL 2018

quantum computation: these games can be manipulated to force untrusted devices to perform measurements on copies of the Bell state which carry out complex circuits. This idea originated in [32] and has seen variants and improvements since then [21, 26, 11]. For such applications, it is important that the result include an error term which is (at most) bounded by some polynomial function of the number of copies of the state.[1]

It is noteworthy that all results proved so far for error-tolerant self-testing of several copies of a state at once (that is, parallel self-testing) apply to bipartite states only [22, 23, 13, 26, 27, 28, 5, 32, 12, 8, 10, 9]. There is a general multipartite self-testing result in [36] which can be applied to the parallel case, but it is not error-tolerant and no explicit game is given. Complexity of proofs is a factor in establishing new results in this direction: while it would be natural to extrapolate existing parallelization techniques to prove self-tests for n-partite states, the proofs for the bipartite case are already difficult, and we can expect that the same proofs for $n \geq 3$ are more so. Yet, if this is an obstacle it is one worth overcoming, since multi-partite states are an important resource in cryptography. For example, a much-cited paper in 1999 [15] proved that secret sharing is possible using several copies of the GHZ state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, in analogy to the use of Bell states in the original QKD protocol [3].

In this work, we give the first proof of an error-tolerant parallel *tripartite* self-test. Specifically, we prove that a certain class of 3-player games self-test N copies of the GHZ state, for any $N \geq 1$, with an error term that grows polynomially with N. To accomplish this we introduce, for the first time, the graphical language of categorical quantum mechanics into the topic of rigidity. As we will discuss below, the use of graphical languages is a critical feature of the proof — games involving more than 2 players involve complicated tensor networks, which are not easily expressed symbolically. Our result thus demonstrates the power and importance of visual formal reasoning in quantum information processing.

1.1 Categorical quantum mechanics

Category theory is a branch of abstract mathematics which studies systems of interacting processes. In Categorical Quantum Mechanics (CQM), categories (specifically *symmetric monoidal categories*) are used to represent and analyze the interaction of quantum states and processes.

Inspired by methods from computer science, CQM introduces a explicit distinction between traditional quantum semantics in Hilbert spaces and the syntax of quantum protocols and algorithms. In particular, symmetric monoidal categories support a diagrammatic formal syntax called *string diagrams*, which provide an intuitive yet rigorous means for defining and analyzing quantum processes, in place of the more traditional bra-ket notation. This expressive notation helps to clarify definitions and proofs, making them easier to read and understand, and encourages the use of equational (rather than calculational) reasoning.

The origins of CQM's graphical methods can be found in Penrose's tensor diagrams [30], although earlier graphical languages from physics (Feynman diagrams) and computer science (process charts) can be interpreted in these terms. Later, Joyal and Street [16] used category theory and topology to formalize these intuitive structures. More recently, the works of Selinger [33, 34] and Coecke, et al. [1, 7] have substantially tightened the connection between categorical methods and quantum information, in particular developing diagrammatic approaches positive maps and quantum-classical interaction, respectively. A thorough and self-contained introduction to this line of research can be found in the recent textbook [6].

[1] This condition allows the computations to be performed in polynomial time. The works [26, 11] go further, and prove an error term that is independent of the number of copies of the state.

For a brief review of categorical quantum mechanics and the syntax of string diagrams used in our proofs, see Appendix A.

1.2 Statement of main result

In the three-player GHZ game, a referee chooses a random bit string $xyz \in \{0,1\}^3$ such that $x \oplus y \oplus z$=0, and distributes x, y, z to the three players (Alice, Bob, Charlie) respectively, who return numbers $a, b, c \in \{-1, 1\}$ respectively. The game is won if

$$abc \quad = \quad (-1)^{\neg(x \vee y \vee z)}. \tag{1}$$

(In other words, the game is won if the parity of the outputs is even and $xyz \neq 000$, or the parity of the outputs is odd and $xyz = 000$.) It is easy to prove that this game has no classical winning strategy. On the other hand, if Alice, Bob, and Charlie share the 3-qubit state

$$|G\rangle \quad = \quad \frac{1}{2\sqrt{2}} \quad \sum_{r+s+t \leq 1} |rst\rangle - \sum_{r+s+t \geq 2} |rst\rangle \Bigg) \Bigg(\tag{2}$$

and obtain their outputs by either performing an X-measurement $\{|+\rangle\langle+|, |-\rangle\langle-|\}$ on input 0 or the Z-measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on input 1, they win perfectly. This is known to be the only optimal strategy (up to local changes of basis) and therefore the GHZ game is rigid [20]. (An equivalent strategy, which is more conventional, is to use the state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and X- and Y-measurements to win the GHZ game. We will use the state $|G\rangle$ instead for compatibility with previous work on rigidity. Note that $|G\rangle$ is equivalent under local unitary transformations to $|GHZ\rangle$.)

To extend this game to a self-test for the $|G\rangle^{\otimes N}$ state, we use a game modeled after [5]. The game requires the players to simulate playing the GHZ game N times. We give input to the rth player in the form of a pair (U_r, f_r) where $\{1, 2, \ldots, N\} \supseteq U_r \xrightarrow{f_r} \{0,1\}$ is a partial function assigning an "input" value for some subset of the game's "rounds" $1, \ldots, N$. The output given by such a player is a function $g_r \colon U_r \to \{0,1\}$ assigning a bit-valued "output" to each round. The game is won if the GHZ condition (1) is satisfied on all the rounds in $U_1 \cap U_2 \cap U_3$ for which the input string was even-parity.

Fortunately, it is not necessary to query the players on all possible subsets $U_r \subseteq \{0, 1, \ldots, N\}$ (which would involve an exponential number of inputs) — it is only necessary to query them on one- and two-element subsets. This yields the game $\overline{GHZ}_N$, which is formally defined in Figure 1 below. Our main result is the following. (See Proposition 10 below for a formal statement.)

Theorem 1. *The game $\overline{GHZ}_N$ is a self-test for the state $|G\rangle^{\otimes N}$, with error term $\mathcal{O}(N^4\sqrt{\varepsilon})$.*

In other words, if three devices succeed at the game $\overline{GHZ}_N$ with probability $1-\varepsilon$, then the devices must contain a state that approximates the state $|G\rangle^{\otimes N}$ up to an error term of $\mathcal{O}(N^4\sqrt{\varepsilon})$. The proof proceeds by assuming that the players have such a high-performing strategy, and then using the measurements from that strategy to map their state isometrically to a state that is approximately of the form $|G\rangle \otimes L'$, where L' is some arbitrary tripartite "junk" state. This approach is a graphical translation of the method of many previous works on rigidity (in particular, [21] and our previous paper [17]).

1.3 Related works and further directions

In previous works on quantum rigidity, pictures are often used as an aid to a proof, but not as a proof itself. The only other rigidity paper that we know of which used rigorous graphical methods is the recent

Participants: Player 1 (Alice), Player 2 (Bob), Player 3 (Charlie), and a Referee
Parameter: $N \geq 1$ (the number of rounds)

1. The referee chooses a number $r \in \{0,1,2,3\}$ and a two distinct elements $i, j \in \{1,2,\ldots,N\}$ uniformly at random.
2. If $r = 0$, then the referee sets $U_1 = U_2 = U_3 = \{i\}$. Otherwise, he sets $U_r = \{i, j\}$ and sets each the other variables U_k (for $k \neq r$) to be equal to $\{i\}$.
3. The referee chooses values for $f_1(i), f_2(i), f_3(i) \in \{0,1\}$ uniformly at random under the constraint that $f_1(i) \oplus f_2(i) \oplus f_3(i) = 0$. Also, if $r > 0$, the referee chooses $f_r(j) \in \{0,1\}$ at random.
4. The referee sends each pair (U_i, f_i) to the ith player, respectively, who returns a function $g_i \colon U_i \to \{-1,1\}$.
5. The game is won if

$$g_1(i)g_2(i)g_3(i) \quad = \quad (-1)^{\neg(f_1(i) \vee f_2(i) \vee f_3(i))}. \tag{3}$$

Figure 1: The augmented GHZ game ($\overline{GHZ}_N$).

paper [12] which successfully used the concept of a group picture to prove rigidity for a new class of 2-player games. Group pictures are visual proofs of equations between elements of a finitely presented group. In the context of rigidity, group pictures construct approximate relations between products of sequences of operators, and as such they are a useful general tool for proving rigidity of 2-player games. An interesting further direction is to try to merge the formalism of [12] with the one given here in order to address general n-player games.

A natural next step is to explore cryptographic applications. Since GHZ states form the basis for the secret-sharing scheme of [15], it may be useful to see if the game $\overline{GHZ}_N$ can be used to create a new protocol for 3-party secret sharing using untrusted quantum devices.

2 Preliminaries

2.1 The augmented GHZ game

The game $\overline{GHZ}_N$ that we will use to self-test the state $|G\rangle^{\otimes N}$ from equation (2) is given in Figure 1. In this game, each player is requested to give outputs for either one or two round numbers (chosen from the set $\{1,2,\ldots,N\}$) given inputs for each round number. Both the inputs and the players' outputs are expressed as partial functions on the set $\{1,2,\ldots,N\}$. This game is modeled after [5].

The variable r determines the type of input given to each player. Note that in the case $r = 0$, there are $4N$ possible input combinations that the referee could give to the players (since there are N possible values for i, and 4 possible values for $(f_1(i), f_2(i), f_3(i))$) and for each of the values, $r = 1,2,3$, there are $8N(N-1)$ possible input combinations. Each valid input combination occurs with probability $\Omega(1/N^2)$.

We wish to describe the set of all possible quantum behaviors by the players Alice, Bob, and Charlie in $\overline{GHZ}_N$. In the definition that follows, we use the term *reflection* to mean an observable with values in $\{\pm 1\}$ (in other words, a Hermitian operator whose square is the identity). A *quantum strategy* for the game $\overline{GHZ_N}$ game consists of the following data.

1. A unit vector $L \in A \otimes B \otimes C$, where A, B, C are finite-dimensional Hilbert spaces.
2. For each $i \in \{1, 2, \ldots, N\}$, $b \in \{0, 1\}$, and $W \in \{A, B, C\}$, a reflection
$$R^W_{i \to b} \tag{4}$$
on W.
3. For each $i, j \in \{1, 2, \ldots, N\}$, $b, c \in \{0, 1\}$, and $W \in \{A, B, C\}$, two *commuting* reflections
$$R^W_{i \to b | j \to c} \quad \text{and} \quad R^W_{j \to c | i \to b} \tag{5}$$
on W.

The spaces A, B, C denote the registers possessed by Alice, Bob, and Charlie, respectively. The vector L denotes the initial state that they share before the game begins. The reflections $R^W_{i \to b}$ describe their behavior on singleton rounds (specifically, on a singleton round the player measures his or her register W along the eigenspaces of $R^W_{i \to b}$, and reports either $+1$ or -1 for round i, appropriately). The reflections $R^W_{i \to b | j \to c}, R^W_{j \to c | i \to b}$ describe their behavior on non-singleton rounds (specifically, if the input to a player is the function $[i \to b, j \to c]$, then they measure along the eigenspaces of $R^W_{i \to b | j \to c}$ to obtain their output for round i and measure along the eigenspaces of $R^W_{j \to c | i \to b}$ to determine their output for round j). Note that since the reflections in (5) represent measurements that are carried out simultaneously by one of the players, we assume that these two reflections commute. (This assumption will be critical in our proof).

For any reflection Z and unit vector ψ on a finite-dimensional Hilbert space Q, if we measure ψ with Z then the probability of obtaining an output of -1 is precisely

$$[1 - \operatorname{Tr}(Z \psi \psi^*)]/2 \quad = \quad \| Z\psi - \psi \|^2 / 4 \tag{6}$$

We can use this fact to express the losing probabilities achieved by the players in terms of their strategy. If $r = 0$ and the players are queried for round i with inputs x, y, z, then their losing probability is precisely

$$\left\| R^A_{i \to x} R^B_{i \to y} R^C_{i \to z} L + (-1)^{x \vee y \vee z} L \right\|^2 / 4. \tag{7}$$

If Alice is queried for round i with input x and round j with input x', and Bob and Charlie are queried for round i with inputs y, z respectively, then the losing probability is

$$\left\| R^A_{i \to x | j \to x'} R^B_{i \to y} R^C_{i \to z} L + (-1)^{x \vee y \vee z} L \right\|^2 / 4. \tag{8}$$

Similar expressions hold for the case where Bob or Charlie is the party that receives two queries.

Note that the game $\overline{GHZ_N}$ is entirely symmetric between the three players Alice, Bob and Charlie. This means that, given any strategy $\left(L, \left\{R^W_{i \to b} \right. , \left\{R^W_{i \to b | j \to c}\right\}\right)$ for $\overline{GHZ_N}$, we can produce five additional strategies by choosing a nontrivial permutation $\sigma \colon \{1, 2, 3\} \to \{1, 2, 3\}$ and giving the pth players' subsystem and measurement strategy to the $\sigma(p)$th player, for each $p \in \{1, 2, 3\}$. We will make use of this symmetry in the proof that follows.

2.2 Approximation chains

We make the following definition (see similar notation in [18, 4]). If $F,G\colon A \to B$ are linear maps, then

$$F \underset{\delta}{=} G \tag{9}$$

denotes the inequality $\|F-G\|_2 \leq \mathscr{O}(\delta)$, where $\|\cdot\|_2$ denotes the Frobenius norm and $\mathscr{O}$ denotes asymptotic big-O notation. (If F and G are vectors, then $\|F-G\|_2$ is simply the Euclidean distance $\|F-G\|$.)

We will use this notation especially in the case where F and G are processes represented by diagrams. Note that this relation is transitive: if $F \underset{\delta}{=} G$ and $G \underset{\delta}{=} H$, then $F \underset{\delta}{=} H$. Note also that if $J\colon B \to C$ is a linear map whose operator norm satisfies $\|J\|_\infty \leq \alpha$, then $F \underset{\delta}{=} G \Longrightarrow J \circ F \underset{\delta\alpha}{=} J \circ G$.

3 Rigidity of the augmented GHZ game

Throughout this section, suppose that

$$\Big(L, \big\{R^A_{i\to a} \;, \big\{R^B_{i\to b} \;, \big\{R^C_{i\to c} \;, \Big\{R^A_{i\to a|j\to a'}\Big\}, \Big\{R^B_{i\to b|j\to b'}\Big\}, \Big\{R^C_{i\to c|j\to c'}\Big\}\Big)\Bigg(\tag{10}$$

is a quantum strategy for the $\overline{GHZ}_N$ game which wins with probability $1-\varepsilon$. It is helpful to introduce some redundant notation for this strategy: for any $W \in \{A,B,C\}$ and $i \in \{1,2,\ldots,N\}$ let

$$X'_{W,i} = R^W_{i\mapsto 0}, \tag{11}$$
$$Z'_{W,i} = R^W_{i\mapsto 1}, \tag{12}$$

The reason for this notation is that we intend to show that the operators $R^W_{i\mapsto 1}, R^W_{i\mapsto 1}$ approximate the behavior of the X and Z measurements in the optimal GHZ strategy (see the beginning of subsection 1.2). Similarly, let $X'_{W,i|j\to 1} = R^W_{i\to 0|j\to 1}$ and $Z'_{W,j|i\to 0} = R^W_{j\to 1|i\to 0}$.

We will drop the subscript W from this notation when it is clear from the context.

3.1 Initial steps

Our first goal is to prove approximate commutativity and anticommutativity relations for the operators $X'_{W,i}, Z'_{W,i}$.

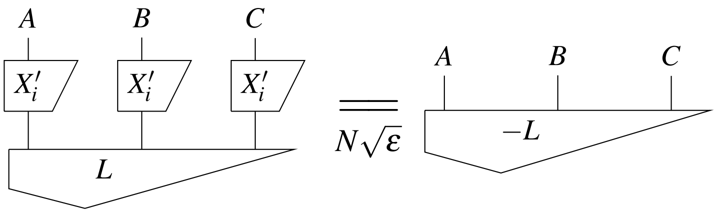
Since the losing probability for our chosen strategy is ε, and each input string occurs with probability $\Omega(N^2)$, we can conclude that the probability of losing on any particular input combination is $\mathscr{O}(N^2\varepsilon)$. By the discussion of expressions (7) and (8) above, we therefore have the following for any $i \in \{1,2,\ldots,N\}$:

$$\begin{aligned}
\left\|(I + X'_{A,i}X'_{B,i}X'_{C,i})|L\rangle\right\|^2 &\Bigg(\leq \mathscr{O}(N^2\varepsilon),\\
\left\|(I - Z'_{A,i}Z'_{B,i}X'_{C,i})|L\rangle\right\|^2 &\Bigg(\leq \mathscr{O}(N^2\varepsilon),\\
\left\|(I - X'_{A,i}Z'_{B,i}Z'_{C,i})|L\rangle\right\|^2 &\Bigg(\leq \mathscr{O}(N^2\varepsilon),\\
\left\|(I - Z'_{A,i}X'_{B,i}Z'_{C,i})|L\rangle\right\|^2 &\Bigg(\leq \mathscr{O}(N^2\varepsilon),
\end{aligned} \tag{13}$$

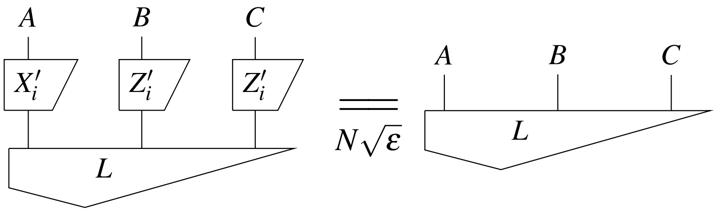
Additionally, if we take any of the four inequalities above, and replace any one of the operators $X'_{W,i}$ with $X'_{W,i|j\to t}$, where $j \neq i$ and $t \in \{0,1\}$, the inequality remains true, and likewise if we replace any $Z'_{W,i}$ with $Z'_{W,i|j\to t}$, the inequality remains true.

We can translate the inequalities above into graphical form.

Proposition 2. *The following inequalities hold.*



(14)

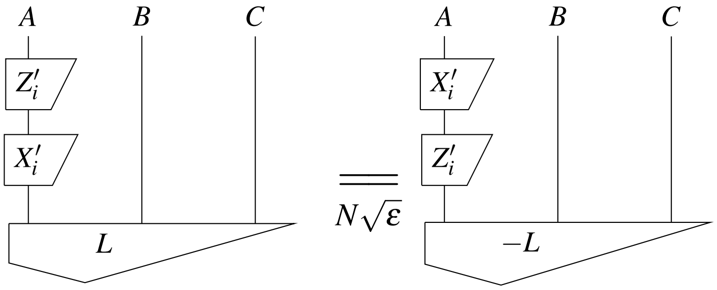


(15)

And, inequality (15) also holds for any permutation of the letters A,B,C.

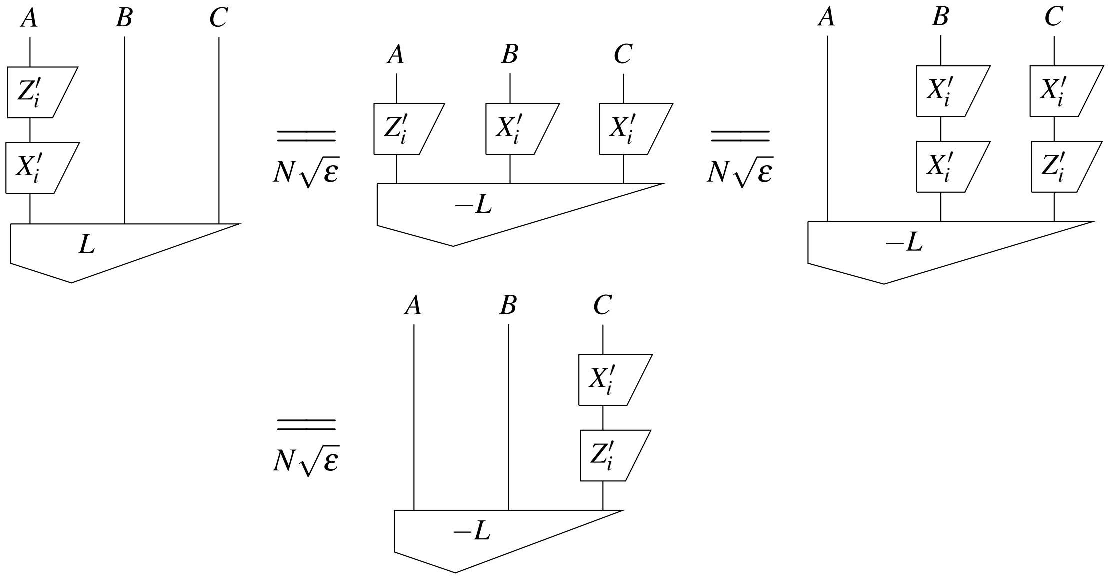
We will use Proposition 2 to prove the following assertion.

Proposition 3 (Approximate anti-commutativity)**.** *For any i, the following inequality holds:*



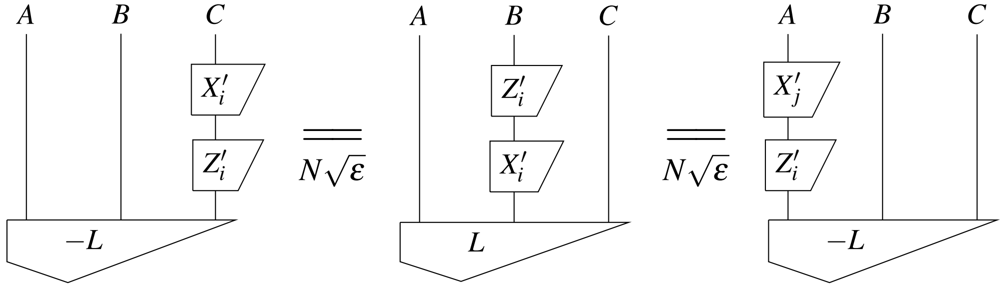
(16)

Proof. Repeatedly applying Proposition 2,



(17)

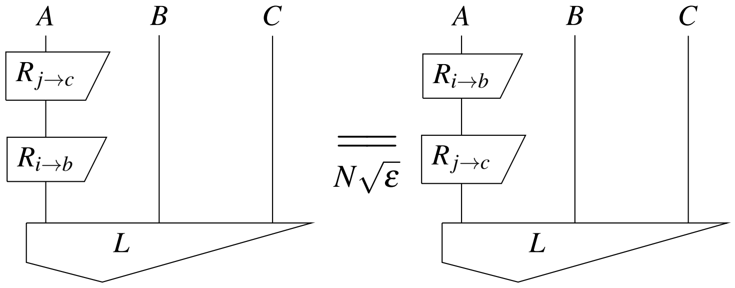
(Here we have used the fact that all of the unitary maps in these diagrams are self-inverse.) Applying the same steps symmetrically across the wires A,B,C,



(18)

as desired. □

Proposition 4 (Approximate commutativity)**.** *The following equation holds for any distinct* $i,j \in \{1,2,\dots,N\}$ *and any bits* $b,c \in \{0,1\}$*:*



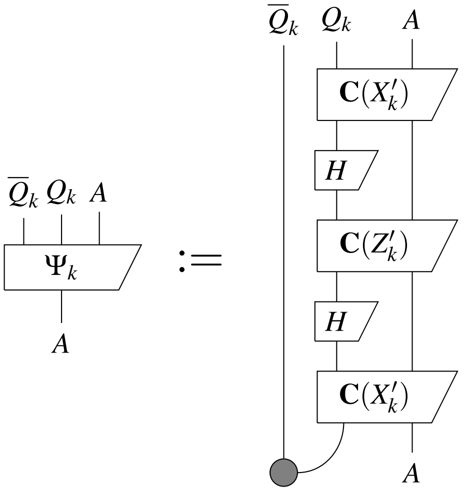
The proof of Proposition 4 is given in appendix C, and is based on the fact that the related reflections $R_{i\to b|j\to c}$ and $R_{j\to c|i\to b}$ commute.

3.2 Isometries

Next we define the local isometries which will relate the state L to the ideal state $|GHZ\rangle^{\otimes N}$. Roughly speaking, for each $k \in \{1,2,\ldots,N\}$ and $W \in \{A,B,C\}$, we will construct an isometry $\Psi_{W,k}$ which approximately "locates" a qubit with the ith players' system, and swaps it out onto a qubit register $Q \cong \mathbb{C}^2$. We then apply these isometries in order, for $1,2,\ldots,N$, the system W. We will use approximate commutativity to show that the different isometries $\Psi_{W,k}$ do not interfere much with one another when applied in sequence. Our approach borrows from previous works on rigidity and uses similar notation to that of the non-graphical rigidity proof in our previous paper [17].

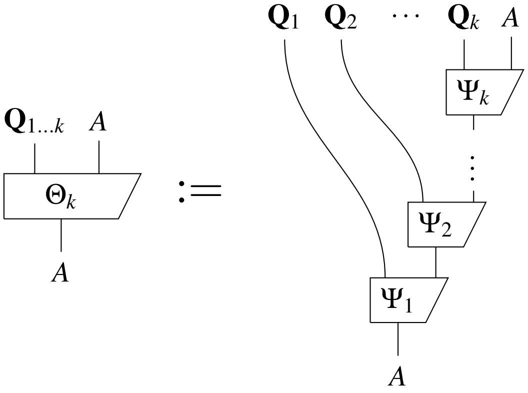
In the following, we use controlled unitary gates, $\mathbf{C}(U)$, which are defined and discussed in Appendix B. Let $H\colon \mathbb{C}^2 \to \mathbb{C}^2$ denote the Hadamard gate $[|0\rangle \mapsto |+\rangle, |1\rangle \mapsto |-\rangle]$. We define isometries $\Psi_{A,k}$ on the system A which involve preparing a Bell state (denoted by a gray node) and then performing an approximate "swap" procedure between one half of the Bell state and A. (This is based on [21].) Then we define an isometry $\Theta_{A,k}$ on A which chains together the swapping maps $\Psi_{A,1},\ldots,\Psi_{A,k}$.

Definition 5 (Swapping maps). *For each $k \in \{1,2,\ldots,N\}$, let Q_k and $\overline{Q}_k$ denote qubit registers, and define an isometry $\Psi_{A,k}$ as follows (suppressing the label A when it is not necessary):*



(19)

Let $\mathbf{Q}_k = \overline{Q}_k \otimes Q_k$ and $\mathbf{Q}_{1\ldots k} = \mathbf{Q}_1 \otimes \cdots \otimes \mathbf{Q}_k$. Define an isometry $\Theta_{k,A}$ by



(20)

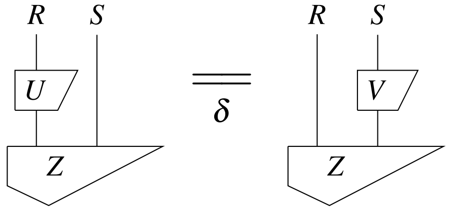
Let $Q_{N+1},\ldots,Q_{3N},\overline{Q}_{N+1},\ldots,\overline{Q}_{3N}$ be qubit registers, and define $\Psi_{B,k}$ analogously as an isometry from B to $B\otimes\overline{Q}_{N+k}\otimes Q_{N+k}$. Define $\Psi_{C,k}$ analogously as an isometry from C to $C\otimes\overline{Q}_{2N+k}\otimes Q_{2N+k}$. Define composite maps $\Theta_{B,k}$ and $\Theta_{C,k}$ similarly in terms of $\Psi_{B,k}$ and $\Psi_{C,k}$.

3.3 Commutativity properties

We now investigate some approximate (anti-)commutativity relationships between the Pauli operators on Q, the reflection strategies for A, B and C, and the isometries defined in the last section.

We begin with the following definition and lemma, which are crucial.

Definition 6. *Let R,S be registers and let $Z\in R\otimes S$ be a unit vector. If a unitary map $U:\ R\to R$ is such that there exists another unitary map $V:\ S\to S$ satisfying*



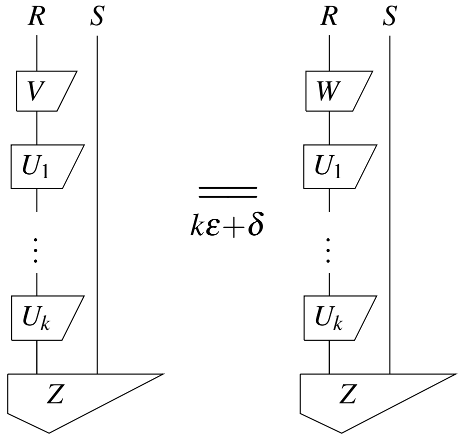
(21)

the we say that U can be pushed through Z with error term δ.

Lemma 7 (Push Lemma)**.** *Suppose that R,S are registers, $Z\in R\otimes S$ is a unit vector, and $V,W,U_1,U_2,\ldots,U_k$ are unitary operators on R such that*

1. *Each map U_i can be pushed through Z with error term ε, and*
2. *The approximate equality $(V\otimes I_S)L \underset{\delta}{=} (W\otimes I_S)L$ holds.*

Then,



(22)

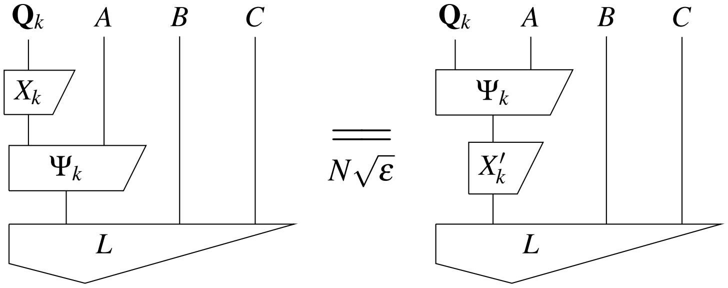
The Push Lemma follows from an easy inductive argument, and is given in the appendix. Note that by Proposition 2, for any k we have

$$X'_{A,k}L \underset{N\sqrt{\varepsilon}}{=} (-X'_{B,k}\otimes X'_{C,k})L \tag{23}$$

$$Z'_{A,k}L \underset{N\sqrt{\varepsilon}}{=} (Z'_{B,k}\otimes X'_{C,k})L, \tag{24}$$

and so all of the maps $X'_{\cdot,k}$ and $Z'_{\cdot k}$ can be pushed through L with error term $N\sqrt{\varepsilon}$. This fact underlies the proofs of the next two results, which are proved in the appendix using a combination of the Push Lemma, and the approximate commutativity and anti-commutativity properties of maps $X'_{\cdot k}$ and $Z'_{\cdot k}$.

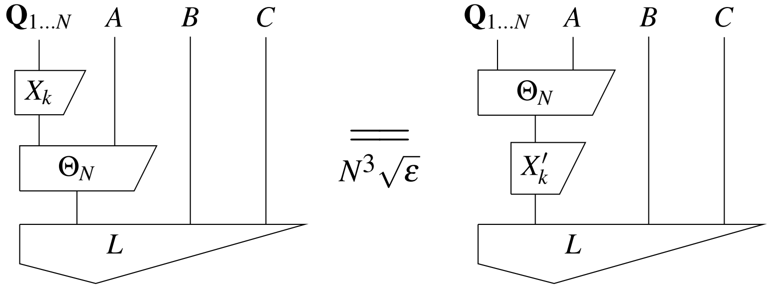
Proposition 8. *For $k \in \{1,2,\ldots,N\}$, let $X_{A,k}$ and $Z_{A,k}$ denote the Pauli operators on Q_k. Then,*



(25)

and similarly for Z'_k. Likewise, define $\{X_{B,k}, Z_{B,k}\}$ to be the Pauli operators on Q_{N+k} and define $\{X_{C,k}, Z_{C,k}\}$ to be the Pauli operators on Q_{2N+k}. Analogous statements hold for $\Psi_{k,B}$ and $\Psi_{k,C}$.

Proposition 9. *For any $k \in \{1,2,\ldots,N\}$,*



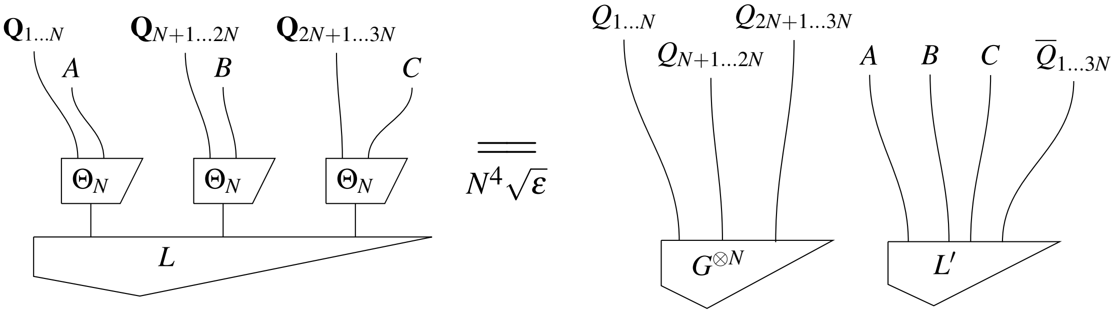
(26)

and similarly for Z'_k. Analogous statements hold for $\Theta_{B,k}$ and $\Theta_{C,k}$.

3.4 Rigidity

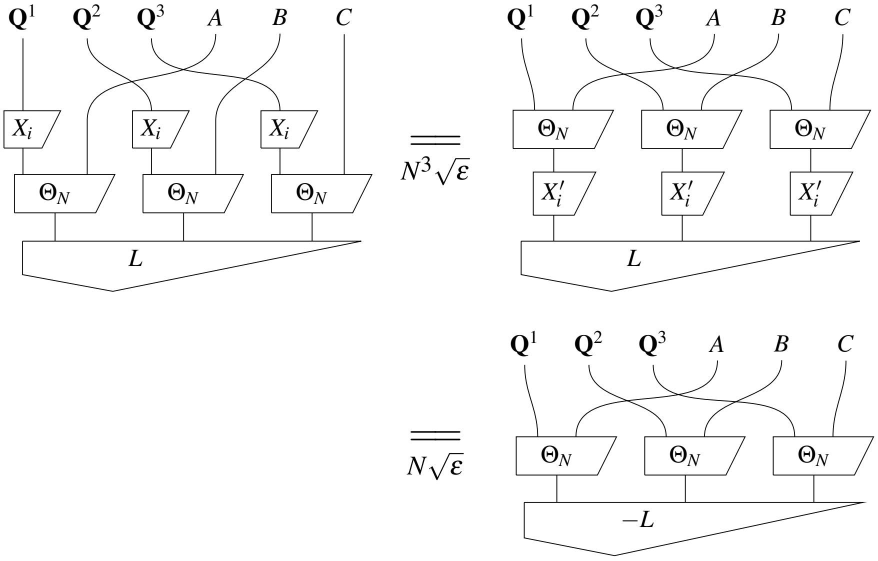
We are now ready to state and prove our main result.

Proposition 10 (Rigidity)**.** *Let $\Theta_{A,N}, \Theta_{B,N}, \Theta_{C,N}$ be the isometries from Definition 5. Then, there is some state L' on $A \otimes B \otimes C \otimes \overline{Q}_{1\ldots 3N}$ such that*



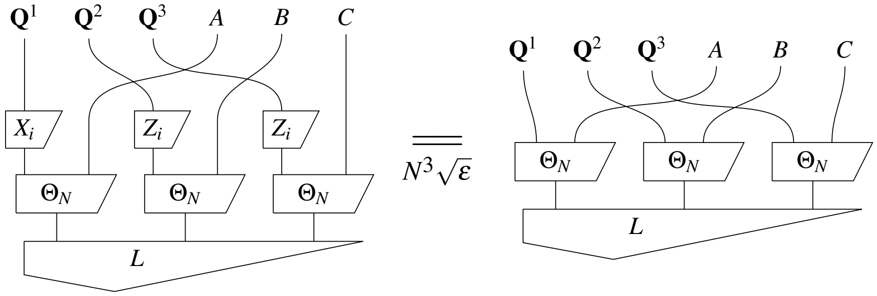
(27)

Proof. In the following, we write $\mathbf{Q}^1 := \mathbf{Q}_{1\ldots N}$, $\mathbf{Q}^2 := \mathbf{Q}_{(N+1)\ldots 2N}$ and $\mathbf{Q}^3 := \mathbf{Q}_{(2N+1)\ldots 3N}$ in order to conserve space. By application of Props. 2 and 9 we have,


$\mathbf{Q}^1$
$\mathbf{Q}^2$
$\mathbf{Q}^3$
A
B
C
X_i
Θ_N
L
$\overline{\overline{N^3\sqrt{\varepsilon}}}$
X_i'
$\overline{\overline{N\sqrt{\varepsilon}}}$
$-L$

(28)

(Here, X_i is used to denote the X-Pauli operator on either Q_i, Q_{N+i}, or Q_{2N+i} depending on which wire it is applied to.) Similarly we obtain that



(29)

where the last relation also holds for any permutation of the labels (X_i, Z_i, Z_i) on the left side of the equation.

The commuting reflection operators $X \otimes Z \otimes Z$, $Z \otimes X \otimes Z$, and $Z \otimes Z \otimes X$ on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ have a common orthonormal eigenbasis $G = G_0, G_1, \ldots, G_7$, in which G_0 is the only eigenvector that has eigenvalue $(+1)$ for all three operators. We can express $\Theta_A^N \otimes \Theta_B^N \otimes \Theta_c^N |L\rangle$ using this basis as

$$\Theta_A^N \otimes \Theta_B^N \otimes \Theta_c^N |L\rangle = \sum_{v_1,\cdots,v_N \in \{G_0,\ldots,G_7\}} |v_1\rangle \otimes \cdots \otimes |v_N\rangle \otimes |L'_{\mathbf{v}}\rangle. \tag{30}$$

where $L'_{\mathbf{v}} \in A \otimes B \otimes C \otimes \overline{Q}_{1\ldots 3N}$. For every term in the sum on the right except the one indexed by $G_0^{\otimes N}$, there is an operator of the form $X_{A,i} \otimes Z_{B,i} \otimes Z_{C,i}$, $Z_{A,i} \otimes X_{B,i} \otimes Z_{C,i}$, or $Z_{A,i} \otimes Z_{B,i} \otimes X_{C,i}$ which negates it. By equation (29) above, the total length of all the terms negated by any one particular gate of this form is $\mathscr{O}(N^3\sqrt{\varepsilon})$, and so the total length of all terms in (30) other than the $G_0^{\otimes N}$ term is $\mathscr{O}(N^4\sqrt{\varepsilon})$, as desired. □

We note that our proofs generalize in a straightforward manner to a proof of self-testing for an arbitrary number of copies of a k-GHZ state, for any integer $k > 3$. The graphical method seems generally well-suited to proving parallel self-testing for stabilizer states, including graph states [21]. We leave possible generalizations to future work.

References

[1] Samson Abramsky & Bob Coecke (2004): *A categorical semantics of quantum protocols*. In: *Logic in computer science, 2004. Proceedings of the 19th Annual IEEE Symposium on*, IEEE, pp. 415–425.

[2] John Baez & Mike Stay (2010): *Physics, topology, logic and computation: a Rosetta Stone*. In: *New structures for physics*, Springer, pp. 95–172.

[3] Charles H Bennett & Gilles Brassard (2014): *Quantum cryptography: Public key distribution and coin tossing*. *Theor. Comput. Sci.* 560(P1), pp. 7–11.

[4] Spencer Breiner, Carl A Miller & Neil J Ross (2017): *Graphical Methods in Device-Independent Quantum Cryptography*. *arXiv preprint arXiv:1705.09213*.

[5] Rui Chao, Ben W Reichardt, Chris Sutherland & Thomas Vidick (2016): *Test for a large amount of entanglement, using few measurements*. *arXiv preprint arXiv:1610.00771*.

[6] Bob Coecke & Aleks Kissinger (2017): *Picturing quantum processes*. Cambridge University Press.

[7] Bob Coecke & Dusko Pavlovic (2006): *Quantum measurements without sums*. *arXiv preprint quant-ph/0608035*.

[8] Andrea Coladangelo (2017): *Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game*. *Quantum Information and Computation* 17(9-10), pp. 831–865.

[9] Andrea Coladangelo (2018): *A generalization of the CHSH inequality self-testing maximally entangled states of any local dimension*. *arXiv preprint arXiv:1803.05904*.

[10] Andrea Coladangelo, Koon Tong Goh & Valerio Scarani (2017): *All pure bipartite entangled states can be self-tested*. *Nature communications* 8, p. 15485.

[11] Andrea Coladangelo, Alex Grilo, Stacey Jeffery & Thomas Vidick (2017): *Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources*. *arXiv preprint arXiv:1708.07359*.

[12] Andrea Coladangelo & Jalex Stark (2017): *Robust self-testing for linear constraint system games*. *arXiv preprint arXiv:1709.09267*.

[13] Matthew Coudron & Anand Natarajan (2016): *The parallel-repeated magic square game is rigid*. *arXiv preprint arXiv:1609.06306*.

[14] Matteo Fadel (2017): *Self-testing Dicke states*.

[15] Mark Hillery, Vladimír Bužek & André Berthiaume (1999): *Quantum secret sharing*. *Physical Review A* 59(3), p. 1829.

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

[17] Amir Kalev & Carl A Miller (2017): *Rigidity of the magic pentagram game*. *Quantum Science and Technology* 3(1), p. 015002.

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

[19] Dominic Mayers & Andrew Yao (1998): *Quantum cryptography with imperfect apparatus*. In: *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, IEEE, pp. 503–509.

[20] Matthew McKague (2011): *Self-testing graph states*. In: *Conference on Quantum Computation, Communication, and Cryptography*, Springer, pp. 104–120.

[21] Matthew McKague (2016): *Interactive Proofs for BQP via Self-Tested Graph States*. *Theory of Computing* 12(3), pp. 1–42.

[22] Matthew McKague (2016): *Self-testing in parallel*. New Journal of Physics 18(4), p. 045013.

[23] Matthew McKague (2017): *Self-testing in parallel with CHSH*. Quantum 1, p. 1.

[24] Matthew McKague, Tzyh Haur Yang & Valerio Scarani (2012): *Robust self-testing of the singlet*. Journal of Physics A: Mathematical and Theoretical 45(45), p. 455304.

[25] Carl A. Miller & Yaoyun Shi (2013): *Optimal Robust Self-Testing by Binary Nonlocal XOR Games*. In: 8th Conference on the Theory of Quantum Computation, Communication and Cryptography, pp. 264–272.

[26] Anand Natarajan & Thomas Vidick (2017): *A Quantum Linearity Test for Robustly Verifying Entanglement*. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, ACM, New York, NY, USA, pp. 1003–1015, doi:10.1145/3055399.3055468. Available at `http://doi.acm.org/10.1145/3055399.3055468`.

[27] Anand Natarajan & Thomas Vidick (2018): *Low-degree testing for quantum states*. arXiv preprint arXiv:1801.03821.

[28] Dimiter Ostrev (2016): *The structure of nearly-optimal quantum strategies for the CHSH (n) XOR games*. Quantum Information & Computation 16(13-14), pp. 1191–1211.

[29] Károly F. Pál, Tamás Vértesi & Miguel Navascués (2014): *Device-independent tomography of multipartite quantum states*. Phys. Rev. A 90, p. 042340, doi:10.1103/PhysRevA.90.042340. Available at `https://link.aps.org/doi/10.1103/PhysRevA.90.042340`.

[30] Roger Penrose (1971): *Applications of negative dimensional tensors*. Combinatorial mathematics and its applications 1, pp. 221–244.

[31] Sandu Popescu & Daniel Rohrlich (1992): *Which states violate Bell's inequality maximally?* Physics Letters A 169(6), pp. 411–414.

[32] Ben W Reichardt, Falk Unger & Umesh Vazirani (2013): *Classical command of quantum systems*. Nature 496(7446), p. 456.

[33] Peter Selinger (2004): *Towards a quantum programming language*. Mathematical Structures in Computer Science 14(4), pp. 527–586.

[34] Peter Selinger (2007): *Dagger compact closed categories and completely positive maps*. Electronic Notes in Theoretical computer science 170, pp. 139–163.

[35] Peter Selinger (2010): *A survey of graphical languages for monoidal categories*. In: New structures for physics, Springer, pp. 289–355.

[36] Ivan Šupić, Andrea Coladangelo, Remigiusz Augusiak & Antonio Acín (2017): *A simple approach to self-testing multipartite entangled states*. ArXiv:1707.06534.

[37] Xingyao Wu (2016): *Self-Testing: Walking on the Boundary of the Quantum Set*. Ph.D. thesis, National University of Singapore.

[38] Xingyao Wu, Yu Cai, Tzyh Haur Yang, Huy Nguyen Le, Jean-Daniel Bancal & Valerio Scarani (2014): *Robust self-testing of the three-qubit W state*. Physical Review A 90(4), p. 042339.

Appendix A Categorical Quantum Mechanics

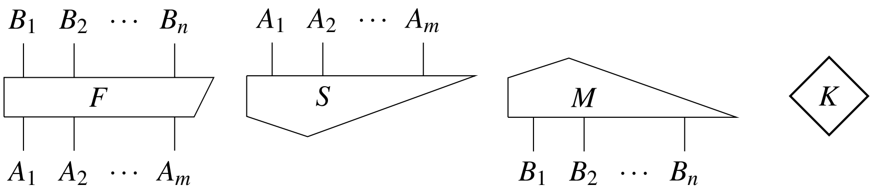
In this appendix we will briefly review some of the standard machinery of categorical quantum mechanics. For a thorough introduction to the topic, see [6].

A.1 Symmetric Monoidal Categories

The formal context for categorical quantum mechanics is that of *symmetric monoidal categories*. We develop the terminology in stages.

A *category* is a mathematical structure representing a universe of (possible) processes $F,G,H,\ldots$; each process has a typed input and output, often indicated by writing $F : A \to B$. The fundamental structure in a category is serial composition; whenever the output type of $F : A \to B$ matches the input type of $G : A \to C$, we may form a composite process $F \circ G : A \to C$.

A *monoidal* category generalizes the structure of an ordinary category to allows for multi-partite processes; here the fundamental object of study is a process $F : A_1 \otimes \ldots \otimes A_m \to B_1 \otimes \ldots \otimes B_n$, which is represented as a black box with m labeled inputs and n labeled outputs. (Either of the numbers m,n may be zero.) Diagramatically, we represent these classes as follows:

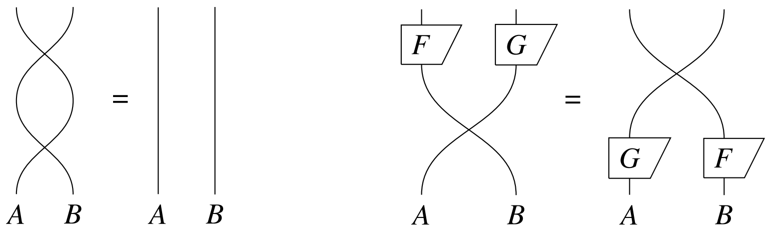

B_1 B_2 $\cdots$ B_n
F
A_1 A_2 $\cdots$ A_m
A_1 A_2 $\cdots$ A_m
S
M
B_1 B_2 $\cdots$ B_n
K

(31)

The categorical structure of serial composition is represented diagrammatically by matching the output wires of one process to the inputs of another, so long as the types match up. So, above, F can be pre-composed with S and post-composed with M to yield a scalar $M \circ F \circ S$ or, in Dirac notation, $\langle M|F|S\rangle$.

Along with multi-partite states and processes, monoidal structure also introduces an operation of parallel composition on processes: given $F : A \to B$ and $G : A' \to B'$, we can produce a parallel process $F \otimes G : A \otimes A' \to B \otimes B'$, depicted graphically by side-by-side juxtaposition. More generally, using parallel composition with identity processes (represented by bare wires), we can compose processes in which only some inputs and outputs match. Note that we will often suppress wire labels in complicated diagrams, as the labels are implicitly determined by the boxes they feed.

Finally, a *symmetric* structure on a monoidal category allow for additional flexibility in how wires can be manipulated. A symmetry allows us to permute the ordering of strings, and is represented diagrammatically by crossing wires (called a *twist*). Formally, the twist is axiomatized terms of intuitive diagrammatic equations:



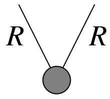
(32)

A.2 Quantum states and processes

To apply the above approach to quantum mechanics, we work within the category **Hilb** of finite-dimensional Hilbert spaces over $\mathbb{C}$. In this category, the types are finite-dimensional Hilbert spaces (i.e., vector spaces of $\mathbb{C}$ with semi-linear inner product) each equipped with a fixed orthonormal basis, and the processes are $\mathbb{C}$-linear maps between such vector spaces. For example, if $A_1,\ldots,A_m,B_1,\ldots,B_n$ are finite-dimensional Hilbert spaces, then the diagrams in display box (31) above represent, respectively, a linear map $F\colon A_1\otimes\ldots\otimes A_m\to B_1\otimes\ldots\otimes B_n$, a vector $S\in A_1\otimes\ldots\otimes A_m$, a linear map $M\colon B_1\otimes\ldots\otimes B_n\to\mathbb{C}$, and a scalar $K\in\mathbb{C}$. Serial composition of diagrams simply represents composition of functions — for example, the composition of S,F and M is simply the scalar $M(F(S))\in\mathbb{C}$. It is elementary to show this category is a symmetric monoidal category (with the tensor product as its monoidal operation).

For our purposes, a *state* is a vector in a Hilbert space (i.e., a process with no inputs) whose norm is equal to one. A *unitary process* $F\colon A\to B$ is a linear map that satisfies $FF^*=I_B$ and $F^*F=I_A$. (Also, a linear map $G\colon A\to B$ that satisfies the single condition $G^*G=I_A$ is called an *isometry*.) With these definitions, we will be able to express quantum states and processes as diagrams like the ones in (31) and (32) above.

We note that while symmetric monoidal categories are sufficient to handle the book-keeping needed in our proofs, it is only a fragment of the full CQM theory. Further development introduces compact closed structures (trace, transpose, state-process duality), dagger structures (adjoint, conjugate), Frobenius structures (orthonormal basis, classical-quantum interaction) and Hopf structures (complementary bases, ZX-calculus). For our purposes, we need only one additional visual definition, which is the *Bell state*. In this paper we use a gray node with two wires of the same type R,



(33)

to denote the unit vector

$$\left(\frac{1}{\sqrt{\dim R}}\right)\sum_e e\otimes e \quad \in \quad R\otimes R, \qquad (34)$$

where the sum is taken over the standard basis of R. If $R\cong\mathbb{C}^2$, we denote this state symbolically by Φ^+.

Appendix B Controlled Unitaries

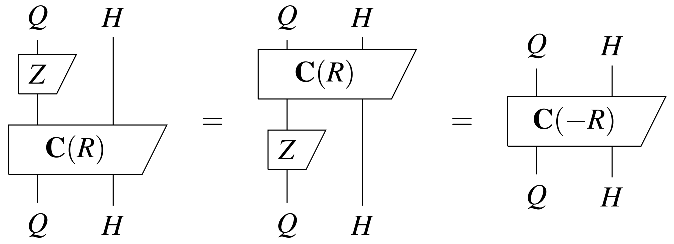
Our proof makes substantial uses of controlled unitary operations. This appendix collects key facts about controlled operations which will simplify our main proof.

Definition 11 (Controlled Unitary). *Let $Q\cong\mathbb{C}^2$ denote a qubit register with a fixed computational basis $\{|0\rangle,|1\rangle\}$, and suppose $U\colon H\to H$ is a unitary operation. The associated* controlled unitary $\mathbf{C}(U):Q\otimes H\to Q\otimes H$ *is defined by*

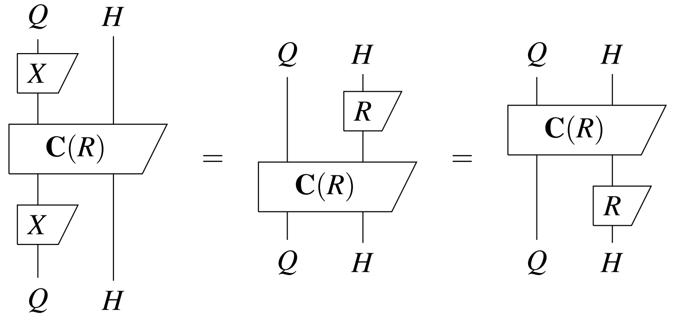
$$\mathbf{C}(U) \quad = \quad |0\rangle\langle 0|\otimes I_H+|1\rangle\langle 1|\otimes U. \qquad (35)$$

The next lemma describes some (anti-)commutativity properties between controlled unitaries and Pauli operators X and Z. The proofs follow directly from the definition.

Lemma 12. *For any reflection $R : H \to H$ we have the following equations*



(36)



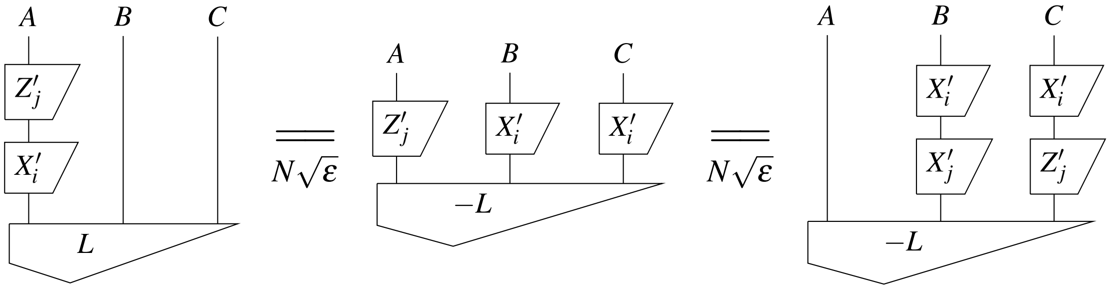
(37)

Appendix C Supporting Proofs

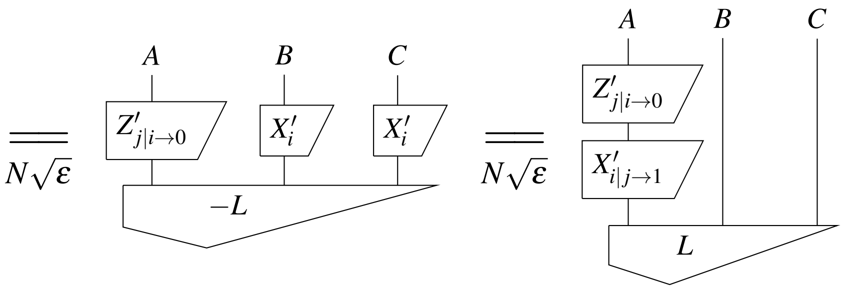
In this appendix we provide the proofs for propositions from the main text.

C.1 Proof of Proposition 4

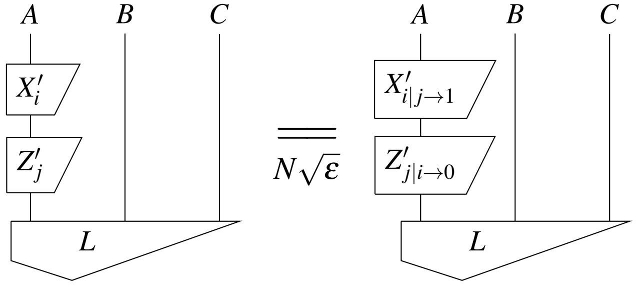
We give the proof for $b = 0, c = 1$; the other cases are analogous. Using inequalities (13) and their variants, we have


A
B
C
Z'_j
X'_i
L
$\overline{\overline{N\sqrt{\varepsilon}}}$
A
B
C
Z'_j
X'_i
X'_i
−L
$\overline{\overline{N\sqrt{\varepsilon}}}$
A
B
C
X'_i
X'_i
X'_j
Z'_j
−L

(38)



A similar sequence shows that

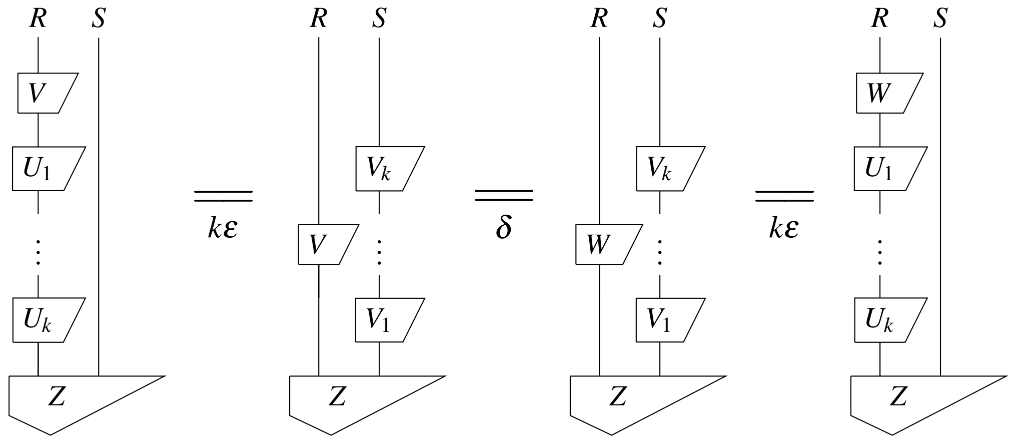


(39)

Since $X'_{A,i|j\to1} = R^A_{i\to0|j\to1}$ and $Z'_{A,j|i\to0} := R^A_{j\to1|i\to0}$ are assumed to commute, the result follows.

C.2 Proof of Lemma 7

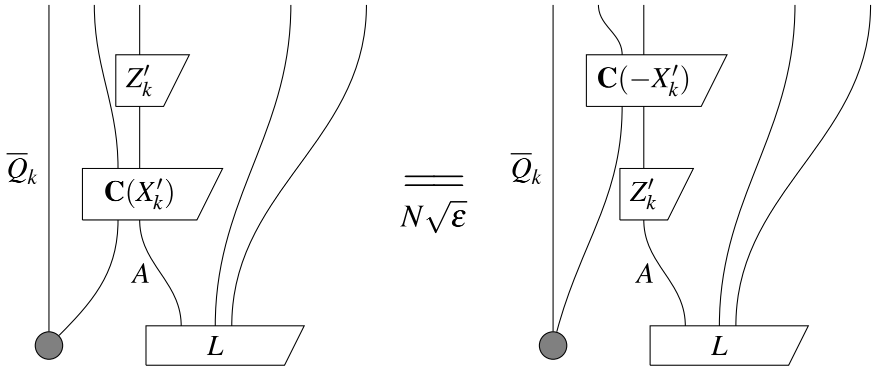
Applying the push condition inductively, we have the following for some unitary operators $V_1,\ldots,V_k$:



(40)

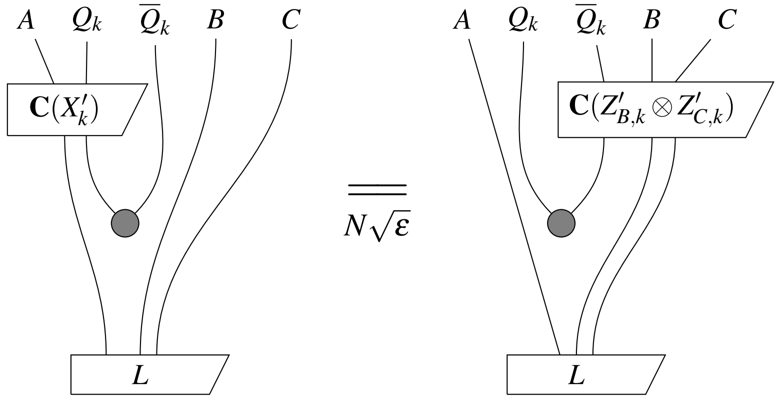
C.3 Proof of Proposition 8

We begin with two observations. First, the approximate anti-commutativity in Proposition 3 implies the following approximate anti-commutativity property for the controlled-X'_k gate (by superposition):



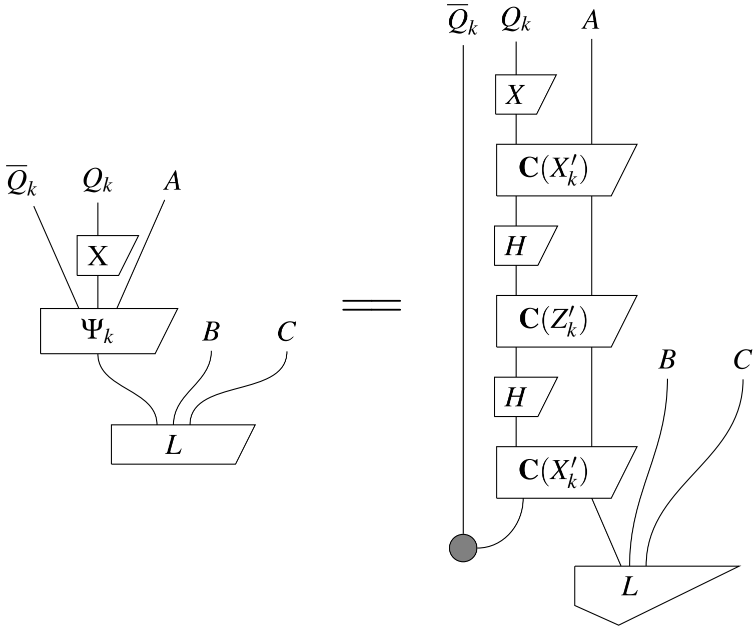
(41)

Secondly, the controlled operator $\mathbf{C}(X'_{A,k})$ on $Q_k \otimes A$ can be approximately pushed through the state $\Phi^+ \otimes L$ like so:

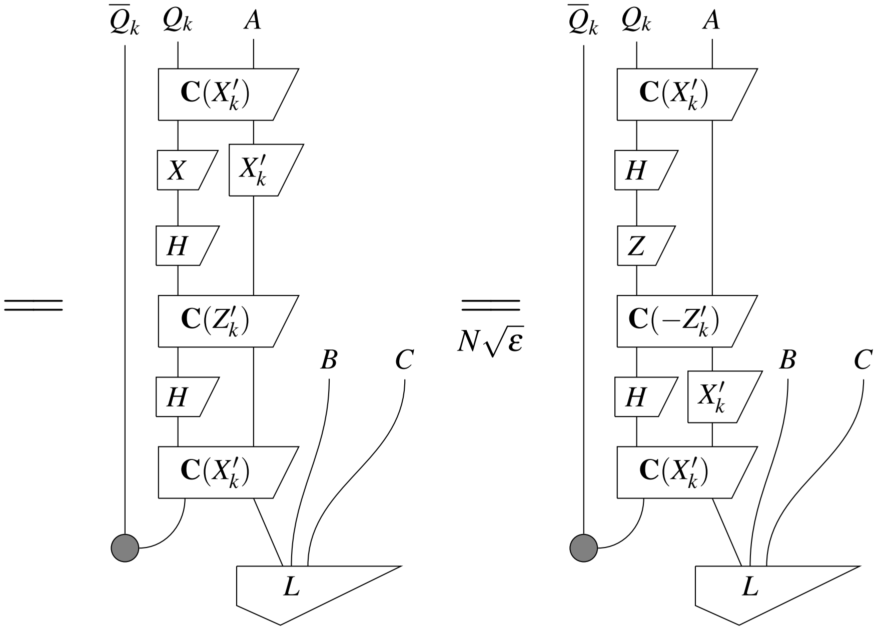


(42)

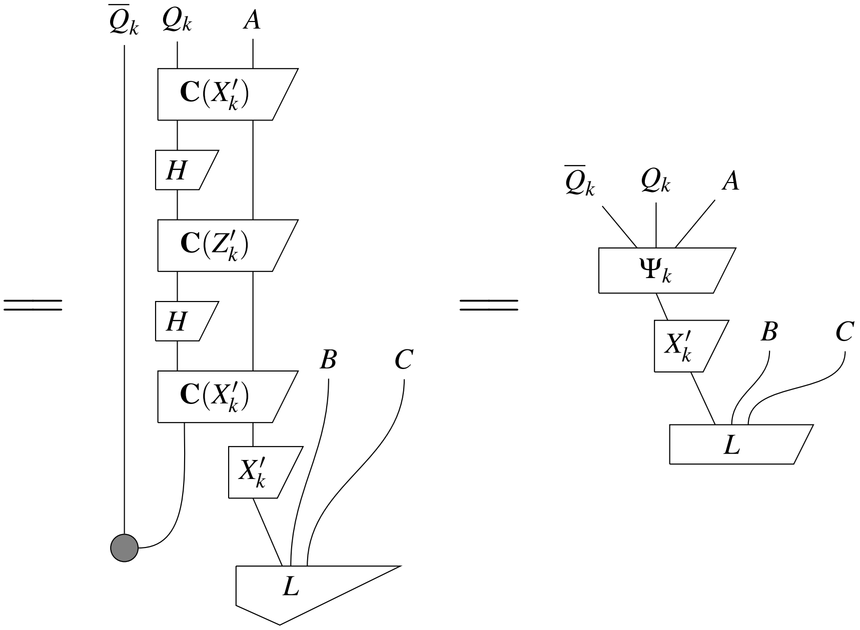
And similarly for $Z'_{A,k}$. The Hadamard operator $[H \otimes I_A]$ on $Q_k \otimes A$ can be exactly pushed through $\Phi^+ \otimes L$ (by merely applying H to $\overline{Q}_k$). This fact allows free application of the Push Lemma (Lemma 7). We have the following, in which we exploit approximate anti-commutativity, the Lemma 7, and the rules for controlled unitaries from Appendix B.



(43)

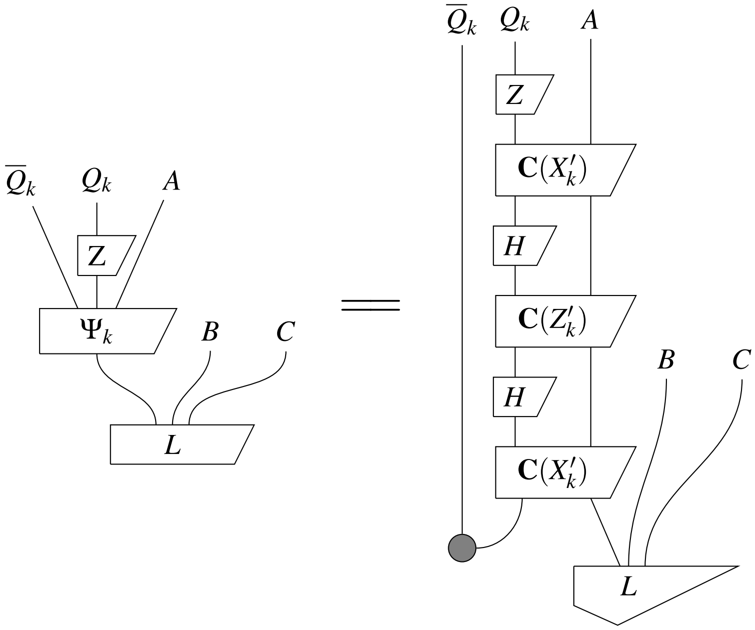


(44)



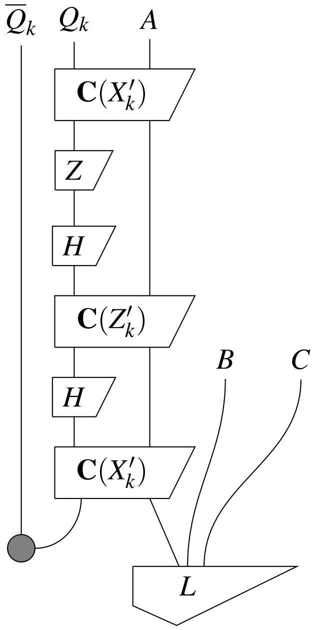
(45)

Similarly,

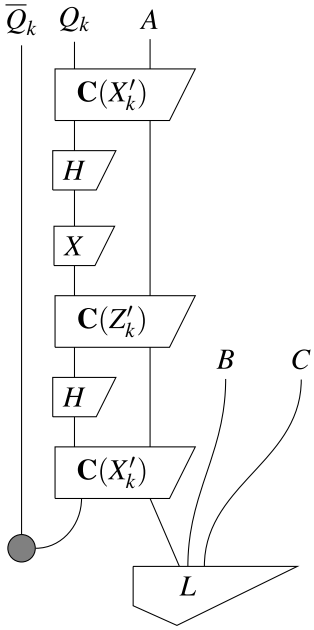


(46)

$=$

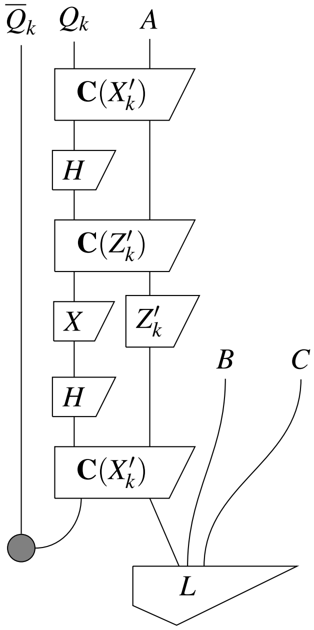

$\overline{Q}_k$
Q_k
A
$\mathbf{C}(X'_k)$
Z
H
$\mathbf{C}(Z'_k)$
H
$\mathbf{C}(X'_k)$
B
C
L

$=$

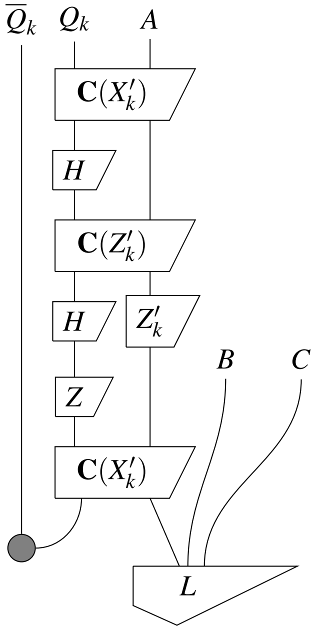

$\overline{Q}_k$
Q_k
A
$\mathbf{C}(X'_k)$
H
X
$\mathbf{C}(Z'_k)$
H
$\mathbf{C}(X'_k)$
B
C
L

(47)

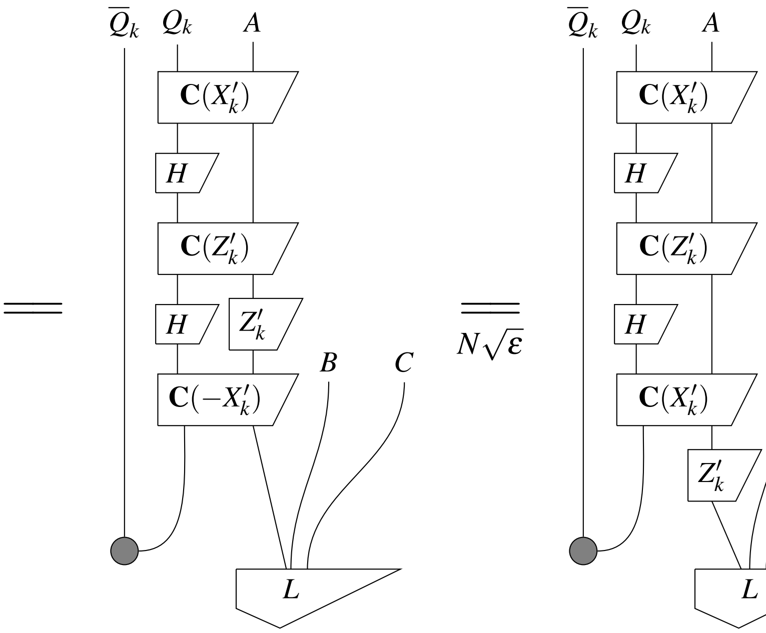
$=$


$\overline{Q}_k$
Q_k
A
$\mathbf{C}(X'_k)$
H
$\mathbf{C}(Z'_k)$
X
Z'_k
H
$\mathbf{C}(X'_k)$
B
C
L

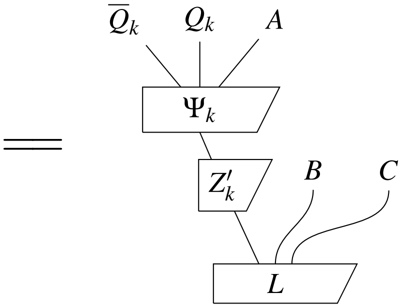
$=$


$\overline{Q}_k$
Q_k
A
$\mathbf{C}(X'_k)$
H
$\mathbf{C}(Z'_k)$
H
Z'_k
Z
$\mathbf{C}(X'_k)$
B
C
L

(48)



(49)



(50)

as desired. This completes the proof.

C.4 Proof of Proposition 9

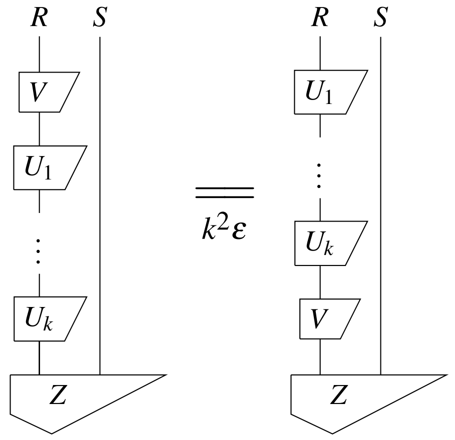
We begin with the following lemma. It is similar to the Push Lemma (Lemma 7) but it specifically addresses commutativity.

Lemma 13. *Suppose that R,S are registers, $Z \in R \otimes S$ is a unit vector, and $V, U_1, U_2, \ldots, U_k$ are unitary operators on R such that*

1. *Each map U_i can be pushed through Z with error term ε, and*

2. *The approximate equality $(VU_i \otimes I_S)L \underset{\varepsilon}{=} (U_iV \otimes I_S)L$ holds for all i.*

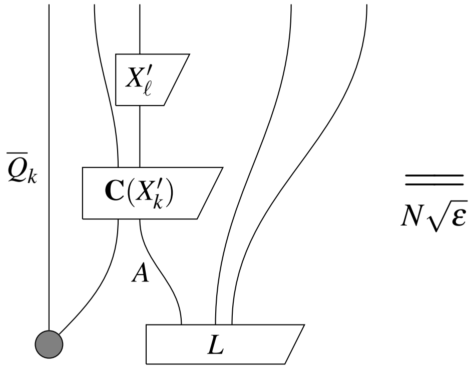
Then,



(51)

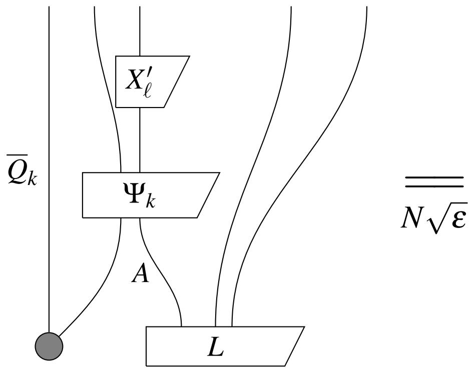
Proof. This follows easily by k applications of Lemma 7. □

By Proposition 4, for any $j \neq k$, we have



(52)

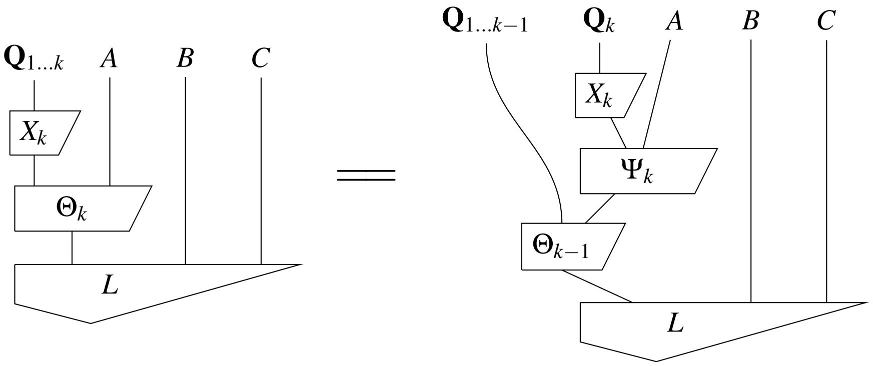
and the same holds with (X'_ℓ, X'_k) replaced by (X'_ℓ, Z'_k), (Z'_ℓ, X'_k), or (Z'_ℓ, Z'_k). Also, as noted at the beginning of section C.3, the gates that define $\Psi_{A,k}$ (see diagram (19) can each be pushed through L with error term $N\sqrt{\varepsilon}$. Therefore by Lemma 13,



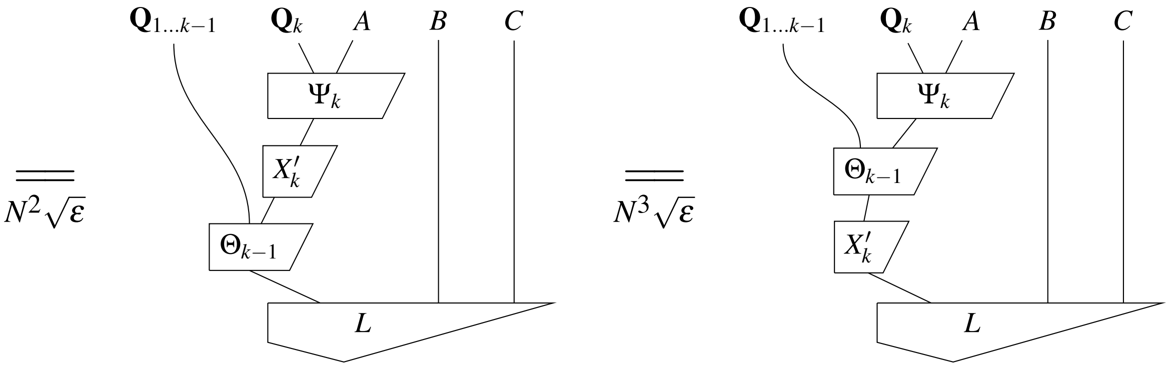
(53)

We therefore have the following, in which we first apply Proposition 8 with Lemma 7, and then apply

Lemma 13.



(54)


$\overline{\overline{N^2\sqrt{\varepsilon}}}$
$\mathbf{Q}_{1\ldots k-1}$
$\mathbf{Q}_k$
A
B
C
Ψ_k
X'_k
Θ_{k-1}
L
$\overline{\overline{N^3\sqrt{\varepsilon}}}$
$\mathbf{Q}_{1\ldots k-1}$
$\mathbf{Q}_k$
A
B
C
Ψ_k
Θ_{k-1}
X'_k
L

(55)

An analogous statement holds with X replaced by Z. Applying the isometries $\Psi_{k+1}, \ldots, \Psi_N$ in order now completes the proof.