Constant gap between conventional strategies and those based on C*-dynamics for self-embezzlement

Richard Cleve[1], Benoît Collins[2], Li Liu[1], and Vern Paulsen[3]

[1]Institute for Quantum Computing and Cheriton School of Computer Science, University of Waterloo, Canada.
[2]Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan.
[3]Institute for Quantum Computing and Department of Pure Mathematics, University of Waterloo, Canada.

We consider a bipartite transformation that we call *self-embezzlement* and use it to prove a constant gap between the capabilities of two models of quantum information: the conventional model, where bipartite systems are represented by tensor products of Hilbert spaces; and a natural model of quantum information processing for abstract states on C*-algebras, where joint systems are represented by tensor products of C*-algebras. We call this the *C*-circuit* model and show that it is a special case of the commuting-operator model (in that it can be translated into such a model). For the conventional model, we show that there exists a constant $\epsilon_0 > 0$ such that self-embezzlement cannot be achieved with precision parameter less than ϵ_0 (i.e., the fidelity cannot be greater than $1 - \epsilon_0$); whereas, in the C*-circuit model—as well as in a commuting-operator model—the precision can be 0 (i.e., fidelity 1).

Self-embezzlement is not a non-local game, hence our results do not impact the celebrated Connes Embedding conjecture. Instead, the significance of these results is to exhibit a reasonably natural quantum information processing problem for which there is a constant gap between the capabilities of the conventional Hilbert space model and the commuting-operator or C*-circuit model.

1 Introduction and summary

In the conventional model of quantum information, separate quantum systems are represented by Hilbert spaces and joint systems are represented by their tensor products. Localized dynamics and measurements are operations on the Hilbert spaces of the subsystems.

This model—that we refer to here as the *conventional* model—is not fully general. In a more general *commuting-operator* model, there is one global Hilbert space and the localized dynamics and measurements act on that space with the requirement that certain operators on separate subsystems commute. In 2017, Slofstra [20] showed that there are *non-local correlations* that can be attained in the commuting-operator model that cannot be obtained in the conventional model. It remains an open question whether every commuting-operator

Richard Cleve: cleve@uwaterloo.ca
Benoît Collins: collins@math.kyoto-u.ac.jp
Li Liu: 147liu@uwaterloo.ca
Vern Paulsen: vpaulsen@uwaterloo.ca

correlation can be approximated to arbitrary precision by a conventional correlation. This question is equivalent to that of the celebrated *Connes embedding conjecture* [5, 8, 14].

We consider a broader scenario than non-local correlations, and prove that there is a task that can be performed in the commuting-operator model (as well as a model of quantum information processing for abstract states on C*-algebras) that has the property that it cannot even be approximated to arbitrary precision in the conventional model.

Our task is a variant of *embezzlement*, which was introduced by van Dam and Hayden in [3]. Embezzlement is a mapping where, by local operations, an entangled state ψ is used catalytically to create some other entangled state ϕ with high fidelity. An ϵ-precision embezzlement scheme for state ϕ using catalyst ψ with precision parameter ϵ is a set of local operations that map $\psi \otimes (|0\rangle \otimes |0\rangle)$ to $\psi \otimes \phi$ within fidelity $1 - \epsilon$. The case where $\epsilon = 0$ corresponds to exact embezzlement. In the conventional model, any entangled state ϕ can be embezzled with precision arbitrarily close to 0 but not exactly (even if the Hilbert spaces of the individual systems are allowed to be infinite dimensional and ψ has infinite entanglement entropy); however, in a commuting-operator model, states can be embezzled exactly [2].

Embezzlement cannot be directly tested experimentally the way non-local correlations can, because the parties can utilize concealed entanglement. Nevertheless, non-local correlations based on the *idea* of embezzlement have been discovered that can approximated to arbitrary precision ϵ in the conventional model, but where the amount of entanglement required is $\Omega(1/\epsilon)$ [7] (see also the earlier related results [16, 12]).

Our new result concerns a task that we call *self-embezzlement* and which is remarkable because it can be achieved exactly in the commuting-operator model, whereas *it cannot even be approximated to arbitrary precision* in the conventional model. In self-embezzlement, a second copy of the catalyst state is embezzled. That is, by local operations, state $\psi \otimes (|0\rangle \otimes |0\rangle)$ is mapped to $\psi \otimes \psi$ within fidelity $1 - \epsilon$. Here, we don't have a specific target state; rather, we allow the catalyst to be any pure state that is non-trivially entangled in the sense that it can be used to approximately attain the maximal violation of the CHSH inequality [1] (i.e., by a factor of $\sqrt{2} - \epsilon$). Our main results, stated informally, are:

Theorem 1.1. *There exists an $\epsilon_0 > 0$ such that, in the conventional model, approximate self-embezzlement to precision ϵ_0 is impossible.*

Theorem 1.2. *In the commuting-operator model, exact self-embezzlement is possible.*

We do not know whether there are non-local correlations based on the idea of self-embezzlement that exhibit a gap between the two models and make no claim of any consequences regarding the Connes conjecture. Instead, the significance of these results is to exhibit a reasonably natural quantum information processing problem for which there is a constant gap between the conventional model and the commuting-operator model. (See [13] for another example of a constant-gap separation between the conventional and commuting-operator model—for the task of steering.)

An additional contribution of this work is the proposal and development of a natural model of information processing for abstract states on C*-algebras, that we call the *C*-circuit* model, where the reversible gates are (suitably localized) $*$-automorphisms (see Appendix A for a brief review of the definitions of *C*-algebra*, *abstract state*, and *$*$-automorphism*). In fact, our exact self-embezzlement protocol is expressed in the C*-circuit model and can be converted into a commuting-operator model by applying the GNS Theorem [6, 19] to a suitable crossed product of our C*-algebra. Thus, Theorem 1.2 is a corollary of:

Theorem 1.3. *In the C*-circuit model, exact self-embezzlement is possible.*

Theorem 1.3 is similar to something pointed out by Keyl *et al.* in [11], where they refer to a "maximally entangled state of infinite entanglement" that is said to be (in comment "ME 8" of section 5.A) "unitarily isomorphic to two copies of itself". It is important for this to be with respect to some notion of local operations, and our definition and construction in terms of C*-circuits is a way of putting this intuition into a rigorous framework.

It is noteworthy that the construction in Theorem 1.3 uses the so-called CAR algebra (an acronym of "canonical anti-commutation relations"), a particular C*-algebra that is *hyperfinite*, which is a property that permits it to be built up in a natural way from finite-dimensional C*-algebras. It is known that no constant gap can be obtained for non-local correlations with a hyperfinite C*-algebra [18]. That is, for any hyperfinite C*-algebras, $\mathcal{A}$ and $\mathcal{B}$, the non-local correlations attainable with the corresponding C*-circuit model are limit points of non-local correlations attainable in the conventional model. The proof of this uses the fact that, for hyperfinite C*-algebras, $\mathcal{A} \otimes_{\max} \mathcal{B} = \mathcal{A} \otimes_{\min} \mathcal{B}$. A consequence of this is that no constant gap between the conventional model and the C*-circuit model for non-local correlations can be obtained by a simple black-box reduction to our self-embezzlement transformation.

Returning to the separation between models in [20], this can also be expressed as a difference between the C*-circuit model and the conventional (circuit) model, albeit not by a constant-gap. In that case the C*-algebras involved in the construction do not appear to be hyperfinite (rather, they are a star-crossed product of the CAR algebra with a group action).

In summary, we obtain a constant-gap separation in capability between the C*-circuit model (with the CAR algebra) and the conventional model for a natural problem. We believe that the C*-circuit model is a natural model for capturing the capabilities of quantum information processing for infinite-dimensional systems represented as abstract states on C*-algebras, and that its capabilities merit further investigation.

2 Definitions

2.1 The conventional model and the C*-circuit model

The *quantum circuit* model is the underlying paradigm in which almost all quantum computations and protocols are expressed.

In the *conventional* circuit model, *registers* are represented by Hilbert spaces and *compound registers*[1] are represented by tensor products of Hilbert spaces. The *states* of a register are the density operators on its Hilbert space. The states of (possibly compound) registers can be transformed by a series of reversible *gates*, which are unitary operations on the associated Hilbert spaces; and also they can be *measured* by POVMs (positive-operator valued measures) on the Hilbert spaces.

The *C*-circuit* model is a natural analogue of the conventional model for abstract states on C*-algebras[2]. In the C*-circuit model, *registers* are represented by C*-algebras and *compound registers* are represented by tensor products of C*-algebras. The *states* of a register are the unital positive linear functionals on its C*-algebra. The states of (possibly compound) registers can be transformed by a series of reversible *gates*, which are

[1] We are using the terminology for registers in [22] (including compound registers).

[2] See Appendix A for definitions and some basic properties of C*-algebras and abstract states on them.

$*$-automorphisms of the associated C*-algebras; and also they can be *measured* by POVMs with elements from the C*-algebras.

The following table compares the conventional quantum circuit model and the C*-circuit model.

Conventional quantum circuit model	C*-circuit model ($\otimes_{\min}$ version)
Register R: associated Hilbert space $\mathcal{H}_{\mathsf{R}}$	Register R: associated C*-algebra $\mathcal{A}_{\mathsf{R}}$
Compound register $(\mathsf{R}_1, \mathsf{R}_2)$: $\mathcal{H}_{\mathsf{R}_1} \otimes \mathcal{H}_{\mathsf{R}_2}$	Compound register $(\mathsf{R}_1, \mathsf{R}_2)$: $\mathcal{A}_{\mathsf{R}_1} \otimes_{\min} \mathcal{A}_{\mathsf{R}_2}$
States of R: density operators on $\mathcal{H}_{\mathsf{R}}$	States of R: unital positive linear functionals on $\mathcal{A}_{\mathsf{R}}$
Dynamics of R: unitary operators on $\mathcal{H}_{\mathsf{R}}$	Dynamics of R: $*$-automorphisms of $\mathcal{A}_{\mathsf{R}}$
Measurements of R: POVMs on $\mathcal{H}_{\mathsf{R}}$	Measurements of R: POVMs with elements from $\mathcal{A}_{\mathsf{R}}$

Figure 1: Conventional quantum circuit model vs. C*-circuit model

The gates acting on a register are the reversible *dynamics* of the register and the $*$-automorphisms are the most general such operations that preserve the algebraic structure and norm of a register's C*-algebra (in analogy with unitary operations in the conventional model, which are the most general operations that preserve the algebraic structure and norm of a register's Hilbert space). Our framework resembles that of *C*-dynamical systems*, which are C*-algebras combined with sets of $*$-automorphisms acting on them[3]; however, in the C*-circuit model there are various localization conditions imposed on the dynamics (i.e., each gate acts on a subset of the registers).

The above definition is a basic model where the gates are reversible and where measurements produce classical outcomes but no residual (or "collapsed") quantum states. This model is complete in that channels and measurements that produce residual states can be defined in a Stinespring form (as $*$-automorphisms on a larger system). Kraus operators (that need not be elements of the C*-algebra) can also be defined, though we do not do that here.

2.2 Informal definition of self-embezzlement

Alice and Bob each have two quantum systems, call them A_1, A_2 and B_1, B_2 (respectively). In computer science terminology, we call these *registers*. First, we define exact self-embezzlement, followed be ϵ-approximate self-embezzlement.

Definition of *exact self-embezzlement*:

- There is some catalyst state ψ that satisfies a *nontriviality* condition that rules out product states and states close to product states. The condition is that ψ can be used to maximally violate the CHSH inequality by a factor of $\sqrt{2}$. The catalyst state ψ is allowed to be any pure state that satisfies this property.

- The *initial* joint state of Alice and Bob's respective first registers (A_1 and B_1) is the catalyst ψ. The initial joint state of their respective second registers (A_2 and B_2) is some product state, such as $\phi_A \otimes \phi_B$. So the initial state of $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$ is $\psi \otimes (\phi_A \otimes \phi_B)$.

[3]More precisely, a *C*-dynamical system* is a triple of the form $(\mathcal{R}, G, \alpha)$, where $\mathcal{R}$ is a C*-algebra, G is a locally compact group, and α is a continuous action of G on the $*$-automorphisms of $\mathcal{R}$.

- Alice and Bob are each allowed to perform operations that are local to their registers. For Alice, this is the compound register $(\mathsf{A}_1, \mathsf{A}_2)$. For Bob, this is the compound register $(\mathsf{B}_1, \mathsf{B}_2)$.
- The *final* state of $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$ (after they apply their local operations) is $\psi \otimes \psi$. (That is, $(\mathsf{A}_1, \mathsf{B}_1)$ is in state ψ and $(\mathsf{A}_2, \mathsf{B}_2)$ is in state ψ.)

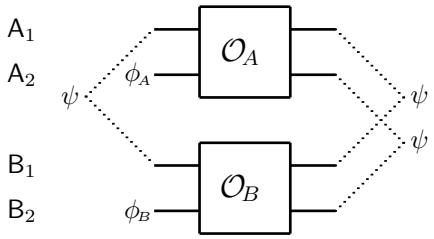

Figure 2: Circuit diagram for self-embezzlement. In the conventional model, $\mathcal{O}_A$ and $\mathcal{O}_B$ are unitary operators acting on registers $(\mathsf{A}_1, \mathsf{A}_2)$ and $(\mathsf{B}_1, \mathsf{B}_2)$, respectively. In the C*-circuit model, $\mathcal{O}_A$ and $\mathcal{O}_B$ are $*$-automorphisms acting on $\mathcal{A}_1 \otimes_{\min} \mathcal{A}_2$ and $\mathcal{B}_1 \otimes_{\min} \mathcal{B}_2$ (the C*-algebras associated with $(\mathsf{A}_1, \mathsf{A}_2)$ and $(\mathsf{B}_1, \mathsf{B}_2)$), respectively.

Next we define *ϵ-approximate self-embezzlement* as the following relaxation of the above. First of all, the violation of CHSH need only be by a factor of $\sqrt{2} - \epsilon$ (as opposed to the maximum violation of $\sqrt{2}$). Second, when Alice and Bob apply their local operations to the initial state $\psi \otimes (\phi_A \otimes \phi_B)$, they need only obtain an approximation of the state $\psi \otimes \psi$ within fidelity $1 - \epsilon$.

In the next two subsections, we present precise definitions of approximate self-embezzlement (to match the results in section 3) and exact self-embezzlement (to match the results in section 4).

2.3 Definition of approximate self-embezzlement in the conventional model

Define an *ϵ-precision self-embezzling scheme* to be a tuple $(\mathcal{H}_A, \mathcal{H}_B, \psi, \phi_A, \phi_B, U_A, U_B)$, where:

1. $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces. (Alice has two registers, which we call A_1 and A_2, associated with $\mathcal{H}_A$, and Bob has two registers, which we call B_1 and B_2, associated with $\mathcal{H}_B$.)
2. ψ is a normalized vector in $\mathcal{H}_A \otimes \mathcal{H}_B$ such that state ψ can be used to violate the CHSH inequality by factor $\sqrt{2} - \epsilon$. We call ψ the *catalyst*.
3. ϕ_A and ϕ_B are normalized vectors in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively (with no restriction).
4. U_A is a unitary operation on $\mathcal{H}_A \otimes \mathcal{H}_A$ and U_B is a unitary operator on $\mathcal{H}_B \otimes \mathcal{H}_B$. Applying $U_A \otimes U_B$ to system $((\mathsf{A}_1, \mathsf{A}_2), (\mathsf{B}_1, \mathsf{B}_2))$ has the following property: in the context of system $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$, it maps state $\psi \otimes (\phi_A \otimes \phi_B)$ to state $\psi \otimes \psi$ within fidelity $1 - \epsilon$.

2.4 Definition of exact self-embezzlement in the C*-circuit model

Define an *self-embezzling scheme* to be a tuple of the form $(\mathcal{A}, \mathcal{B}, \psi, \phi_A, \phi_B, \alpha_A, \alpha_B)$, where:

1. $\mathcal{A}$ and $\mathcal{B}$ are C*-algebras. (Alice has two registers, which we call A_1 and A_2, associated with $\mathcal{A}$, and Bob has two registers, which we call B_1 and B_2, associated with $\mathcal{B}$.)

2. $\psi : \mathcal{A} \otimes_{\min} \mathcal{B} \to \mathbb{C}$ can be any pure state which has the property that ψ can be used to maximally violate the CHSH inequality[4] (by factor $\sqrt{2}$). We call ψ the *catalyst*.

3. $\phi_A : \mathcal{A} \to \mathbb{C}$ and $\phi_B : \mathcal{B} \to \mathbb{C}$ are states (with no restriction).

4. α_A is a $*$-automorphism on $\mathcal{A} \otimes_{\min} \mathcal{A}$ and α_B is a $*$-automorphism on $\mathcal{B} \otimes_{\min} \mathcal{B}$.

5. Applying $\alpha_A \otimes \alpha_B$ to system $(\mathsf{A}_1, \mathsf{A}_2, \mathsf{B}_1, \mathsf{B}_2)$ has the following property: in the context of system $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$, it maps state $\psi \otimes (\phi_A \otimes \phi_B)$ to state $\psi \otimes \psi$.

3 There exists $\epsilon_0 > 0$ such that, in the conventional model, self-embezzlement with precision $\leq \epsilon_0$ is impossible

3.1 The case of unitary operations

Without loss of generality, a pure catalyst state is of the form

$$\psi = \sum_{k=1}^{\infty} \lambda_k |k\rangle \otimes |k\rangle, \tag{1}$$

where $\lambda_1 \geq \lambda_2 \geq \cdots$ and $\sum_k |\lambda_k|^2 = 1$, and the initial states of ϕ_A and ϕ_B are $|1\rangle$.

The initial state of $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$ is

$$\psi_{\text{initial}} = \psi \otimes (\phi_A \otimes \phi_B) = \left(\sum_{k=1}^{\infty} \lambda_k |k\rangle \otimes |k\rangle \right) \otimes \Big(|1\rangle \otimes |1\rangle \Big). \tag{2}$$

In a purported self-embezzlement scheme, Alice applies a local unitary U_A on register $(\mathsf{A}_1, \mathsf{A}_2)$ and Bob U_B on register $(\mathsf{B}_1, \mathsf{B}_2)$. We shall bound the fidelity between $(U_A \otimes U_B)\psi_{\text{initial}}$ and

$$\psi_{\text{target}} = \psi \otimes \psi = \left(\sum_{j=1}^{\infty} \lambda_j |j\rangle \otimes |j\rangle \right) \otimes \left(\sum_{k=1}^{\infty} \lambda_k |k\rangle \otimes |k\rangle \right). \tag{3}$$

Theorem 3.1. *There exists a constant $\epsilon_0 > 0$ such that, for any ψ that is $(\sqrt{2} - \epsilon_0)$-CHSH violating, for any local unitary operations U_A and U_B, the trace distance between $(U_A \otimes U_B)\psi_{\text{initial}}$ and ψ_{target} is at least $\frac{2}{9}$.*

Proof. If ψ can be used to violate the CHSH inequality by a factor of $\sqrt{2} - \epsilon$ then, by the rigidity results in [17], there exist local unitary operations that map ψ within distance $O(\sqrt{\epsilon})$ from a state of the form $(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle) \otimes \psi'$. This implies that the largest Schmidt coefficient of ψ satisfies $\lambda_1 \leq \frac{1}{\sqrt{2}} + O(\sqrt{\epsilon})$. Set $\epsilon_0 > 0$ to be sufficiently small[5] so that $\lambda_1 \leq \sqrt{2/3}$.

Using the fact that $\lambda_1 \leq \sqrt{2/3}$, we shall show that, for any local unitaries U_A and U_B, the trace distance between $(U_A \otimes U_B)\psi_{\text{initial}}$ and ψ_{target} is at least $\frac{2}{9}$.

[4] CHSH in the framework where Alice is allowed to perform POVM measurements with elements in $\mathcal{A}$, and similarly for Bob with $\mathcal{B}$.

[5] Using the bounds in [10], it can be calculated that it suffices to set $\epsilon_0 \leq \frac{1}{50}$.

Expressed as states on $((\mathsf{A}_1,\mathsf{A}_2),(\mathsf{B}_1,\mathsf{B}_2))$, the initial state and target states are

$$\psi_{\text{initial}} = \sum_{j=1}^{\infty}\sum_{k=1}^{\infty} \lambda_j \delta_{k,1} \Big(|j\rangle \otimes |k\rangle\Big) \otimes \Big(|j\rangle \otimes |k\rangle\Big) \tag{4}$$

$$\psi_{\text{target}} = \sum_{j=1}^{\infty}\sum_{k=1}^{\infty} \lambda_j \lambda_k \Big(|j\rangle \otimes |k\rangle\Big) \otimes \Big(|j\rangle \otimes |k\rangle\Big), \tag{5}$$

where $\delta_{i,j}$ is the Kronecker-delta function.

By Lemma 1 in [21], the fidelity is maximized when the Schmidt-basis states are the same and the Schmidt coefficients are lined up in terms of magnitude (i.e., largest with largest, second largest with the second largest, etc.). Thus, we need only consider unitary operations U_A and U_B that each apply a permutation of the basis states $\{|j\rangle \otimes |k\rangle\}_{j,k}$ (U_A on register $(\mathsf{A}_1,\mathsf{A}_2)$ and U_B the same permutation on register $(\mathsf{B}_1,\mathsf{B}_2)$).

To analyze this, we first consider a related statement about probability distributions. Let $p = (p_1, p_2, \dots)$ be a probability distribution on $\mathbb{N}$ (possibly of finite support) and assume that $p_1 \geq p_2 \geq \dots$. We consider how close a rearrangement of the probabilities in p can be to $p \otimes p$. A rearrangement can be defined as a bijection $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where πp is the probability distribution on $\mathbb{N} \times \mathbb{N}$ defined as $(\pi p)(j,k) = p_{\pi(j,k)}$.

Recall that the *variation distance* between distributions p and q is defined as $\frac{1}{2}\|p - q\|_1 = \frac{1}{2}\sum_k |p_k - q_k|$.

Lemma 3.2. *If $p_1 \leq \frac{2}{3}$ and $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is any bijection then the variation distance between πp and $p \otimes p$ is at least $2/9$.*

Proof (of Lemma 3.2). Define $m = \max\{m \in \mathbb{N} : p_1 + \dots + p_m \leq \frac{2}{3}\}$ and $S = \{1, \dots, m\}$. Then

$$\frac{1}{3} < p(S) \leq \frac{2}{3}. \tag{6}$$

The first inequality follows because, if $p_1 + \dots + p_m \leq \frac{1}{3}$ then $p_{m+1} \leq \frac{1}{3}$, so $p_1 + \dots + p_{m+1} \leq \frac{2}{3}$.

Define $\mu = p(S)$. Consider the set T, defined as the m largest components of $p \otimes p$. We next show that $p(T) \leq \mu^2$. To see why this is so, note that

$$(p \otimes p)(\{1, \dots, m\} \times \{1, \dots, m\}) = (p_1 + p_2 + \dots + p_m)(p_1 + p_2 + \dots + p_m) = \mu^2 \tag{7}$$

and also that it is straightforward to show that

$$T \subseteq \{(j,k) \in \mathbb{N} \times \mathbb{N} : j + k \leq m + 1\} \subseteq \{1, \dots, m\} \times \{1, \dots, m\}. \tag{8}$$

This is because, if $(j', k') \notin \{(j,k) \in \mathbb{N} \times \mathbb{N} : j + k \leq m + 1\}$ then there are at least $j'k' - 1$ elements of T that are larger than $p_{j'} p_{k'}$.

Therefore, the variation distance between the m largest components of $p \otimes p$ and πp is at least $\frac{1}{2}(\mu - \mu^2) = \frac{1}{2}\mu(1 - \mu) \geq \frac{1}{2}(\frac{2}{3})(\frac{1}{3}) = \frac{1}{9}$. It follows that the variation distance between (all components of) $p \otimes p$ and πp is at least $\frac{1}{2}(\mu - \mu^2) + \frac{1}{2}((1 - \mu^2) - (1 - \mu)) = \frac{2}{9}$. This completes the proof of Lemma 3.2. □

Returning to the proof of Theorem 3.1, Lemma 3.2 implies that if U_A and U_B are permutations of the basis states of ψ_{initial} then one particular way of distinguishing between $(U_A \otimes U_B)\psi_{\text{initial}}$ and ψ_{target} (based on first measuring the state in the computational basis) distinguishes with probability at least $\frac{2}{9}$. This implies that the trace distance between $(U_A \otimes U_B)\psi_{\text{initial}}$ and ψ_{target} is at least $\frac{2}{9}$. This completes the proof of Theorem 3.1. □

Corollary 3.3. *There exists a constant $\epsilon_0 > 0$ such that, for any ψ that is $(\sqrt{2}-\epsilon_0)$-violating, for any local unitary operations U_A and U_B, the fidelity between $(U_A \otimes U_B)\psi_{\text{initial}}$ and ψ_{target} is at most $\sqrt{1-(2/9)^2} < 0.974996 < 39/40$.*

3.2 The case of channels

It turns out that even if Alice and Bob are allowed to use channels (completely positive trace preserving maps) instead of unitaries, they are still not able to perform approximate self-embezzlement. More formally, using the same notation as the previous subsection, and let $\mathcal{N}_A$ be a channel on $(\mathsf{A}_1, \mathsf{A}_2)$, $\mathcal{N}_B$ be a channel on $(\mathsf{B}_1, \mathsf{B}_2)$, we have

Lemma 3.4. *If ψ is a $(\sqrt{2}-\epsilon_0)$-CHSH violating state for some constant $\epsilon_0 > 0$, then there exist some threshold $\epsilon > 0$, where no local channels $\mathcal{N}_A$ and $\mathcal{N}_B$ can achieve*

$$\langle \psi_{\text{target}}, \mathcal{N}_A \otimes \mathcal{N}_B(\psi_{\text{initial}}\psi^*_{\text{initial}})\psi_{\text{target}} \rangle > 1-\epsilon. \tag{9}$$

Proof. The proof is by contradiction. Let U_A and U_B be the Stinespring form of $\mathcal{N}_A$ and $\mathcal{N}_B$, and call the registers holding the extra qubits from Stinespring dilation P_1 and P_2. Let $\psi'_{\text{initial}} = \psi_{\text{initial}} \otimes |0\rangle \otimes |0\rangle$ be ψ_{initial} extended to P_1 and P_2 with $|0\rangle$, such that tracing out P_1 and P_2 on $U_A \otimes U_B \psi'_{\text{initial}}$ gives us $\mathcal{N}_A \otimes \mathcal{N}_B(\psi_{\text{initial}}\psi^*_{\text{initial}})$. Let $\psi_{\text{final}} = U_A \otimes U_B \psi'_{\text{initial}}$. If Eq. (9) holds, then

$$\langle \psi_{\text{target}}, \text{Tr}_{\mathsf{P}_1,\mathsf{P}_2}(\psi_{\text{final}}\psi^*_{\text{final}})\psi_{\text{target}} \rangle > 1-\epsilon \tag{10}$$

We show that since the partial trace of ψ_{final} is close to ψ_{target}, there exists a state ϕ in register $(\mathsf{P}_1, \mathsf{P}_2)$ such that $|\langle \psi_{\text{final}}, (\phi \otimes \psi_{\text{target}}) \rangle|^2 > 1-2\epsilon$ with the following proposition.

Proposition 3.5. *Let $\psi \in \mathcal{H}$ and $\phi \in \mathcal{H}' \otimes \mathcal{H}$, where*

$$\langle \psi, \text{Tr}_{\mathcal{H}'}(\phi\phi^*)\psi \rangle > 1-\epsilon. \tag{11}$$

Then there exists $\psi_0 \in \mathcal{H}'$ such that

$$|\langle \phi, (\psi_0 \otimes \psi) \rangle|^2 > 1-2\epsilon \tag{12}$$

Proof. Let $\phi = \sum_i \sqrt{p_i} i \otimes |v_i\rangle$ be a Schmidt decomposition of ϕ across $\mathcal{H}'$ and $\mathcal{H}$, where $|i\rangle \in \mathcal{H}'$. Then we have

$$\sum_i p_i \langle \psi, v_i \rangle \langle v_i, \psi \rangle > 1-\epsilon. \tag{13}$$

Without loss of generality, assume $|v_0\rangle$ is the state closest to ψ, so that $|\langle \psi, v_0 \rangle|^2 > 1-\epsilon$. Since $\{|v_i\rangle\}$'s are orthonormal to each other, $\sum_{i\neq 0} |\langle \psi, v_i \rangle|^2 < \epsilon$. We use this to get a bound on p_0:

$$1-\epsilon < p_0 |\langle \phi, v_0 \rangle|^2 + \sum_{i>0} p_i |\langle \psi, v_i \rangle|^2 \leq p_0 + (1-p_0)\epsilon = p_0(1-\epsilon) + \epsilon, \tag{14}$$

therefore $p_0 > \frac{1-2\epsilon}{1-\epsilon}$. Now let $\psi_0 = |0\rangle$, then $|\langle \phi, (\psi_0 \otimes \psi) \rangle|^2 = p_0 \langle v_0, \psi \rangle > 1-2\epsilon$. □

Returning to the proof of Lemma 3.4, since U_A and U_B are local unitary operations for Alice and Bob, the Schmidt coefficients of ψ_{final} are the same as the Schmidt coefficeint of ψ_{initial}, which are $\{\lambda_1, \lambda_2, \dots\}$. Let $\{\gamma_1, \gamma_2, \dots\}$ be the Schmidt coefficients of ϕ across register P_1 and P_2. Then the Schmidt coefficient of $\phi \otimes \psi_{\text{target}}$ across Alice and Bob's registers are $\{\lambda_i \lambda_j \gamma_k\}_{i,j,k}$.

Since, for each k, $0 \leq \gamma_k \leq 1$, the largest m entries of $\{\lambda_i \lambda_j \gamma_k\}_{i,j,k}$ must be less or equal to the largest m entries of $\{\lambda_i \lambda_j\}_{i,j}$ for any $m > 0$. Following the same the proof of Lemma 3.2, if ψ is $(\sqrt{2}-\epsilon_0)$-violating for some constant $\epsilon_0 > 0$, it is not possible to have the fidelity between ψ_{final} and $\phi \otimes \psi_{\text{target}}$ be $1-2\epsilon$ for arbitrary $\epsilon > 0$. □

4 In C*-circuit model, exact self-embezzlement is achievable

4.1 The CAR algebra

The C*-algebra used is the so-called CAR algebra (where CAR is an abbreviation of "canonical anti-commutation relations"). (See [4, 15] for more background information.)

To define the CAR algebra, we can start with the infinite tensor products of Pauli operators of finite weight, where the Pauli operators are $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $XZ = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and the weight of such an infinite tensor product is the number of instances of X, Z, or XZ. For example, $I \otimes X \otimes (XZ) \otimes I \otimes Z \otimes I \otimes I \otimes \cdots$ has weight 3. We can denote each such operator as $X^a Z^b$, where $a, b \in \{0,1\}^*$, where it is understood that each string is padded on the right with an infinite sequence of 0s. Thus, $X^a Z^b = (X^{a_1} \otimes X^{a_2} \otimes \cdots)(Z^{b_1} \otimes Z^{b_2} \otimes \cdots)$. The above example is $X^a Z^b$, where $a = 011 \equiv 011000\ldots$ and $b = 00101 \equiv 00101000\ldots$. Define the set of generators $G = \{X^a Z^b : a, b \in \{0,1\}^*\}$ and $\mathbb{C}G$ to be the set of all (finite) linear combinations[6] of elements of G. $\mathbb{C}G$ is closed under multiplication and is a $*$-algebra. (Note that $\{\pm X^a Z^b : a, b \in \{0,1\}^*\} \subset \mathbb{C}G$ is a multiplicative group that we can think of as an infinite version of the Pauli group; however, G itself is not closed under multiplication.)

For each element $A \in \mathbb{C}G$, there is an $m \in \mathbb{N}$ and $M \in \mathbb{C}^{2^m \times 2^m}$ such that $A = M \otimes I \otimes I \otimes \cdots$. Define a norm on $\mathbb{C}G$ as $\|A\| = \|M\|$ (i.e., the spectral norm of M as an operator on $\mathbb{C}^{2^m}$). The CAR algebra is the completion of $\mathbb{C}G$ with respect to this norm.

4.1.1 Notation for the CAR algebra and some of its basic properties

Henceforth we denote the CAR algebra by $\mathcal{R}$.

Also, since $\mathcal{R} \otimes_{\min} \mathcal{R} = \mathcal{R} \otimes_{\max} \mathcal{R}$ (a consequence of $\mathcal{R}$ being hyperfinite [4]), we can unambiguously refer to the C*-algebraic tensor product as $\mathcal{R} \otimes \mathcal{R}$.

Note that, in the aforementioned description of the elements of the generating set G as $X^a Z^b$, we have used $\mathbb{N}$ as the index set for the bits of $a = a_1 a_2 \ldots$ and $b = b_1 b_2 \ldots$; however, any countably infinite set may be used. It is sometimes convenient to use $\mathbb{Z}$ as the index set, which corresponds to thinking of the infinite tensor products of Paulis as *two-way infinite* strings. (An alternative way of thinking about the equivalence between using $\mathbb{N}$ and $\mathbb{Z}$ as the index sets in the specification of the generators of $\mathcal{R}$ is as a $*$-isomorphism between $\mathcal{R}$ and $\mathcal{R} \otimes \mathcal{R}$, where the index set can be $\{0, 1, 2, \ldots\}$ for the first copy of $\mathcal{R}$ and $\{-1, -2, \ldots\}$ for the second copy.)

An example of a $*$-*automorphism* $\alpha : \mathcal{R} \to \mathcal{R}$ is conjugation by some unitary $u \in \mathcal{R}$ (where unitary means $uu^* = u^*u = I$). That is, $\alpha_u(a) = u^* a u$. These are called *inner* automorphisms. Automorphisms that are not inner are called *outer* automorphisms. An example of an outer automorphism is the bilateral-shift operation that maps $X^a Z^b$ (where $a, b : \mathbb{Z} \to \{0,1\}$) to $X^{a'} Z^{b'}$, where $a'_j = a_{j+1}$ and $b'_j = b_{j+1}$. Note that *any* permutation of the index set corresponds to a $*$-automorphism.

4.2 The self-embezzlement scheme

We first define a state that can be intuitively thought of as a countably infinite tensor product of states of the form $\Psi = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$. It is impossible to express such a state as a vector in the tensor product of two Hilbert spaces (even if the Hilbert spaces are allowed to have uncountably infinite dimension; a proof of this is in [2], whose Appendix A

[6] This is well-defined because there are finitely many terms, each of which has all but finitely many factors of I.

shows that states in the tensor product of two Hilbert spaces have a Schmidt decomposition, with a countably number of Schmidt coefficients). However, as was essentially pointed out in [11], such a state *can* be defined as an abstract state $s_\Psi : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ such that

$$s_\Psi((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{j=-1}^{-\infty} \langle \Psi | (X^{a_j} Z^{b_j}) \otimes (X^{a'_j} Z^{b'_j}) | \Psi \rangle = \prod_{j=-1}^{-\infty} \delta_{a_j, a'_j} \delta_{b_j, b'_j}, \tag{15}$$

where δ is the Kronecker delta function (and, solely for convenience later on, we are using $-\mathbb{N} = \{-1, -2, \dots\}$ as the index set). In [11], such a state is described as an example of the notion of an "infinitely entangled state" and several of the properties of this state are explained. By Proposition A.6, the abstract state s_Ψ is a pure state.

We also define an abstract state $s_{00} : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ that corresponds to an infinite tensor product of $|00\rangle = |0\rangle \otimes |0\rangle$ states as

$$s_{00}((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{j=0}^{\infty} \langle 00 | (X^{a_j} Z^{b_j}) \otimes (X^{a'_j} Z^{b'_j}) | 00 \rangle = \prod_{j=0}^{\infty} (1 - a_j)(1 - a'_j). \tag{16}$$

We set the catalyst state, the initial state of $(\mathsf{A}_1, \mathsf{B}_1)$, to be the combination of s_{00} and s_Ψ, expressed as $\psi : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$, where

$$\psi((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{j=0}^{\infty} (1 - a_j)(1 - a'_j) \prod_{j=-1}^{-\infty} \delta_{a_j, a'_j} \delta_{b_j, b'_j}. \tag{17}$$

A schematic picture of ψ is illustrated in Figure 3.

We set the initial state of A_2 and of B_2 to each be $\phi : \mathcal{R} \to \mathbb{C}$, defined as

$$\phi(X^a Z^b) = \prod_{j=-\infty}^{\infty} \langle 0 | (X^{a_j} Z^{b_j}) | 0 \rangle = \prod_{j=-\infty}^{\infty} (1 - a_j). \tag{18}$$

Thus, the initial state of $(\mathsf{A}_2, \mathsf{B}_2)$ is the product state $(\phi \otimes \phi) : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$, where

$$(\phi \otimes \phi)((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{j=-\infty}^{\infty} \langle 00 | (X^{a_j} Z^{b_j} \otimes X^{a'_j} Z^{b'_j}) | 00 \rangle = \prod_{j=-\infty}^{\infty} (1 - a_j)(1 - a'_j). \tag{19}$$

A schematic picture of $\phi \otimes \phi$ is illustrated in Figure 4.

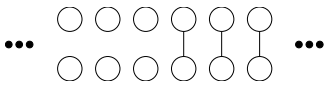

Figure 3: schematic of ψ, the initial state of $(\mathsf{A}_1, \mathsf{B}_1)$, with infinitely many $|00\rangle$ states on the left and infinitely many Ψ states on the right.

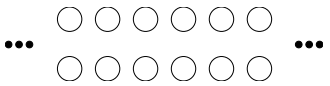

Figure 4: schematic of $\phi \otimes \phi$, the initial state of $(\mathsf{A}_2, \mathsf{B}_2)$, with infinitely many $|00\rangle$ states on the left and the right. This is a product state over $(\mathsf{A}_2, \mathsf{B}_2)$.

The self-embezzlement scheme is based on a $*$-automorphism $\alpha : \mathcal{R} \otimes \mathcal{R} \to \mathcal{R} \otimes \mathcal{R}$, where the same α is applied to $(\mathsf{A}_1, \mathsf{A}_2)$ as well as to $(\mathsf{B}_1, \mathsf{B}_2)$.

Intuitively, α moves infinitely many of the entangled pairs from $(\mathsf{A}_1, \mathsf{B}_1)$ to $(\mathsf{A}_2, \mathsf{B}_2)$ while preserving the entangled pairs in $(\mathsf{A}_1, \mathsf{B}_1)$. The $|00\rangle$ states are present so that this can be accomplished by a permutation of the qubits.

Formally, α permutes the generators of $\mathcal{R} \otimes \mathcal{R}$, which are each of the form $X^a Z^b \otimes X^c Z^d$. We define α as a reordering of the bits of (a, c) and of the bits of (b, d). Such a reordering

is a permutation on the index set. The index set of (a, c) is two copies of $\mathbb{Z}$, which can be denoted as $\mathbb{Z} \times \{1, 2\}$. Similarly, for the index set of (b, d). By a cardinality argument, there exists a bijection $p : \mathbb{Z} \times \{1, 2\} \to \mathbb{Z} \times \{1, 2\}$ such that

$$p(\{-1, -2, \dots\} \times \{1\}) = p(\{-1, -2, \dots\} \times \{1, 2\}). \tag{20}$$

We define $\alpha(X^a Z^b \otimes X^c Z^d) = X^{a'} Z^{b'} \otimes X^{c'} Z^{d'}$ where (a', c') is the permutation of the bits of (a, c) corresponding to p, and (b', d') is also the permutation of the bits of (b, d) corresponding to p. (This can be expressed as $(a', c')_\ell = (a, c)_{p(\ell)}$ and $(b', d')_\ell = (b, d)_{p(\ell)}$, for all $\ell \in \mathbb{Z} \times \{1, 2\}$.)

Since any permutation on the indices is a $*$-automorphism, α is a $*$-automorphism on $\mathcal{R} \otimes \mathcal{R}$. Also, α has been designed so that applying this α to $(\mathsf{A}_1, \mathsf{A}_2)$ and to $(\mathsf{B}_1, \mathsf{B}_2)$ transforms $\psi \otimes (\phi \otimes \phi)$ to $\psi \otimes \psi$.

5 Exact self-embezzlement in the commuting-operator model

The purpose of this section is to make the statement of Theorem 1.2 more precise.

We begin by sketching a definition of a multi-register commuting-operator framework. There is one Hilbert space $\mathcal{H}$ and, for registers $\mathsf{R}_1, \dots, \mathsf{R}_m$, there are corresponding algebras of observables, which are C*-algebras $\mathcal{A}_1, \dots, \mathcal{A}_m \subseteq B(\mathcal{H})$, with the requirement that, for each $j \neq k$, $\mathcal{A}_j$ and $\mathcal{A}_k$ commute. Intuitively, if Alice has register R_j in her lab then she can perform any POVM measurement with elements in $\mathcal{A}_j$. Moreover, for a compound register of the form $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$, the associated algebra of observables is defined as $\mathcal{A}_{(k_1,\dots,k_\ell)} = \overline{\mathcal{A}_{k_1} \cup \dots \cup \mathcal{A}_{k_\ell}}$ (where the bar denotes the C*-algebraic closure). If the global state of the system is $\psi \in \mathcal{H}$ then the state of register $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$ is $s : \mathcal{A}_{(k_1,\dots,k_\ell)} \to \mathbb{C}$ defined as $s(A) = \langle \psi, A\psi \rangle$ (for all $A \in \mathcal{A}_{(k_1,\dots,k_\ell)}$).

We can incorporate the reversible dynamics of a register in this model. Define a unitary $U \in B(\mathcal{H})$ to *act on register* $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$ if:

- U is *localized* to register $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$. Technically this is stated as, for all $j \notin \{k_1, \dots, k_\ell\}$ and $A \in \mathcal{A}_j$, $U^* A U = A$. (In other words, for all for all $j \notin \{k_1, \dots, k_\ell\}$, U centralizes $\mathcal{A}_j$.)
- U *preserves the C*-algebra of* $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$. Since applying U to a state is equivalent to conjugating the POVM elements of a subsequent measurement by U, this requirement is technically expressed as $U^* \mathcal{A}_{(k_1,\dots,k_\ell)} U = \mathcal{A}_{(k_1,\dots,k_\ell)}$. (In other words, U normalizes $\mathcal{A}_{(k_1,\dots,k_\ell)}$.)

Furthermore, in a scenario where there are multiple unitaries acting on distinct registers, we impose an additional requirement that they commute with each other. Thus, if U acts on register $(\mathsf{R}_{k_1}, \dots, \mathsf{R}_{k_\ell})$ and V acts on register $(\mathsf{R}_{j_1}, \dots, \mathsf{R}_{j_m})$, where $\{k_1, \dots, k_\ell\} \cap \{j_1, \dots, j_m\} = \emptyset$ then U and V commute.

5.1 Definition of self-embezzlement in the commuting operator model

There are four basic registers $\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2$ with respective C*-algebras $\mathcal{A}_1, \mathcal{B}_1, \mathcal{A}_2, \mathcal{B}_2 \subset B(\mathcal{H})$, where $\mathcal{H}$ is the underlying Hilbert space. There is an initial state $\psi \in \mathcal{H}$ and unitary operations U_A and U_B, in the reversible dynamics of registers of registers $(\mathsf{A}_1, \mathsf{A}_2)$ and $(\mathsf{B}_1, \mathsf{B}_2)$, respectively. The final state is $\psi' = U_A U_B \psi$.

The following properties are relevant to being a self-embezzlement scheme:

1. The initial state ψ is a product state over the three registers $(\mathsf{A}_1, \mathsf{B}_1)$, A_2 and B_2. Technically, this can be expressed as, for all $X \in \overline{\mathcal{A}_1 \cup \mathcal{B}_1}$, $Y \in \mathcal{A}_2$, and $Z \in \mathcal{B}_2$,

$$\langle \psi, XYZ\psi \rangle = \langle \psi, X\psi \rangle \langle \psi, Y\psi \rangle \langle \psi, Z\psi \rangle. \tag{21}$$

2. Register $(\mathsf{A}_1, \mathsf{B}_1)$ incurs no net change when $U_A U_B$ is applied. Technically, for all $X \in \overline{\mathcal{A}_1 \cup \mathcal{B}_1}$,

$$\langle \psi, X\psi \rangle = \langle \psi', X\psi' \rangle. \tag{22}$$

3. For the final state ψ', the bipartite state of register $(\mathsf{A}_1, \mathsf{B}_1)$ is the same as the bipartite state of register $(\mathsf{A}_2, \mathsf{B}_2)$. Technically, there exist unitary operations $W_A, W_B \in B(\mathcal{H})$ acting on registers $(\mathsf{A}_1, \mathsf{A}_2), (\mathsf{B}_1, \mathsf{B}_2)$ (respectively) that map between the two registers. That is, $W_A^* \mathcal{A}_1 W_A = \mathcal{A}_2$ and $W_B^* \mathcal{B}_1 W_B = \mathcal{B}_2$. And, for all $X \in \mathcal{A}_1$ and $Y \in \mathcal{B}_1$

$$\langle \psi', XY\psi' \rangle = \langle \psi', (W_A^* X W_A)(W_B^* Y W_B)\psi' \rangle. \tag{23}$$

   Thus, for ψ', measurements of $(\mathsf{A}_1, \mathsf{B}_1)$ are equivalent to measurements of $(\mathsf{A}_2, \mathsf{B}_2)$, under the unitary transformation $W_A W_B$.

5.2 Converting from C*-circuit model to commuting-operator model

We begin with an exact embezzlement protocol in the C*-circuit model $(\mathcal{A}, \mathcal{B}, \psi, \phi_A, \phi_B, \alpha_A, \alpha_B)$ from section 4. The C*-algebra of the entire system $(\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2)$ is $\mathcal{C} = \mathcal{A} \otimes_{\min} \mathcal{B} \otimes_{\min} \mathcal{A} \otimes_{\min} \mathcal{B}$. Define the initial state $s : \mathcal{C} \to \mathbb{C}$ as

$$s(x \otimes y \otimes z) = \psi(x)\phi_A(y)\phi_B(z), \tag{24}$$

for $x \in \mathcal{A}_1 \otimes \mathcal{B}_1$, $y \in \mathcal{A}_2$, $z \in \mathcal{B}_2$.

The $*$-isomorphisms α_A and α_B are outer automorphisms of $\mathcal{C}$ of infinite order that commute with each other. Using the $*$-crossed construction [4], we can extend $\mathcal{C}$ to $\mathcal{C} \rtimes (\mathbb{Z} \times \mathbb{Z})$, where the $*$-crossed product is with respect to the group action generated by α_A and α_B. We can regard the crossed-product $\mathcal{C} \rtimes (\mathbb{Z} \times \mathbb{Z})$ as the C*-algebra generated by $\mathcal{C}$ together with two unitaries, u_A, u_B corresponding to the group elements $(1, 0)$ and $(0, 1)$, so that

$$u_A^*(a_1 \otimes b_1 \otimes a_2 \otimes b_2)u_A = a_1' \otimes b_1 \otimes a_2' \otimes b_2, \quad \text{where} \quad a_1' \otimes a_2' = \alpha_A(a_1 \otimes a_2), \tag{25}$$

and

$$u_B^*(a_1 \otimes b_1 \otimes a_2 \otimes b_2)u_B = a_1 \otimes b_1' \otimes a_2 \otimes b_2', \quad \text{where} \quad b_1' \otimes b_2' = \alpha_B(b_1 \otimes b_2). \tag{26}$$

From these equations one sees that u_A commutes with all elements of the form $I \otimes b_1 \otimes I \otimes b_2$ and, similarly, u_B commutes with all elements of the form $a_1 \otimes I \otimes a_2 \otimes I$.

The state s extends to $\mathcal{C} \rtimes (\mathbb{Z} \times \mathbb{Z})$ by setting s to 0 on all terms that contain a non-zero power of either u_A or u_B. To see that this is a well-defined state, one uses the usual representation of the reduced crossed-product.

By applying the GNS Representation Theorem [6, 19] to the state s, we obtain a Hilbert space $\mathcal{H}$, a unit vector $\eta \in \mathcal{H}$, and a unital $*$-homomorphism $\pi : \mathcal{C} \rtimes (\mathbb{Z} \times \mathbb{Z}) \to B(\mathcal{H})$ such that $s(c) = \langle \eta, \pi(c)\eta \rangle$ for all $c \in \mathcal{C}$.

Now we define

$$\mathcal{A}_1 = \pi(\mathcal{A} \otimes I \otimes I \otimes I) \tag{27}$$
$$\mathcal{A}_2 = \pi(I \otimes I \otimes \mathcal{A} \otimes I) \tag{28}$$
$$\mathcal{B}_1 = \pi(I \otimes \mathcal{B} \otimes I \otimes I) \tag{29}$$
$$\mathcal{B}_2 = \pi(I \otimes I \otimes I \otimes \mathcal{B}), \tag{30}$$

the initial state $\psi = \eta$, and

$$U_A = \pi(u_A) \tag{31}$$
$$U_B = \pi(u_B). \tag{32}$$

It is straightforward to check that conditions 1, 2, 3 in section 5.1 hold for $\mathcal{H}$, $\mathsf{A}_1, \mathsf{B}_1, \mathsf{A}_2, \mathsf{B}_2$, ψ, U_A, and U_B. To establish condition 3, we can set $W_A(u_A^k u_B^\ell(a_1 \otimes b_1 \otimes a_2 \otimes b_2)) = u_A^k u_B^\ell(a_2 \otimes b_1 \otimes a_1 \otimes b_2)$ and $W_B(u_A^k u_B^\ell(a_1 \otimes b_1 \otimes a_2 \otimes b_2)) = u_A^k u_B^\ell(a_1 \otimes b_2 \otimes a_2 \otimes b_1)$.

6 Acknowledgments

A substantial part of this paper was completed at l'Institut Henri Poincaré during their trimester "Analysis in Quantum Information Theory" in the fall of 2017. All authors met and collaborated there, and acknowledge its fruitful working environment. We thank Debbie Leung, Miguel Navascués (who informed us of Ref. [13]), William Slofstra, and Thomas Vidick (who informed us of Ref. [10]) for helpful comments. RC, VP, and LL acknowledge support by Canada's NSERC. BC acknowledges support by Kakenhi 15KK0162, 17H04823, 17K18734 and ANR-14CE25-0003-01.

References

[1] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, **23**(15):880–884, 1969.

[2] R. Cleve, L. Liu, and V. Paulsen. Perfect embezzlement of entanglement. *Journal of Mathematical Physics*, **58**:012204, 2017.

[3] W. van Dam and P. Hayden. Universal entanglement transformations without communication. *Physical Review A*, **67**(6):060302, 2003.

[4] K. R. Davidson. *C*-algebras by example*. American Mathematical Society, 1983.

[5] T. Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, **24**(5):1250012, 2012.

[6] I. M. Gelfand and M. A. Naimark. On the embedding of normed rings into the ring of operators in Hilbert space. *Matematiceskij sbornik*, **12**:197–213, 1943).

[7] Z. Ji, D. Leung, and T. Vidick. A three-player coherent state embezzlement game. Manuscript available at arXiv:1802.04926, 2018.

[8] M. Junge, M. Navascués, C. Palazuelos, D. Pérez-García, V. B. Scholz, and R. F. Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, **52**(1):012102, 2011.

[9] R. V. Kadison and J. R. Ringrose. *Fundamentals of the Theory of Operator Algebras, Volume II: Advanced Theory*. Academic Press, 1986.

[10] J. Kaniewski. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. *Physical Review Letters*, **117**(16):070402, 2016.

[11] M. Keyl, D. Schlingemann, and R. Werner. Infinitely entangled states. *Quantum Information and Computation* **3**(4):281–306, 2003.

[12] D. Leung, B. Toner, and J. Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. *Chicago Journal of Theoretical Computer Science*, **2013**:11, 2013.

[13] M. Navascués and D. Pérez-García. Quantum steering and spacelike separation. *Physical Review Letters*, **109**(16):160405, 2012.

[14] N. Ozawa. About the Connes embedding conjecture: Algebraic approaches. *Japanese Journal of Mathematics*, **8**(1):147–183, 2013.

[15] G. K. Pedersen. *C*-algebras and their automorphism groups*. Academic Press, 1979.

[16] O. Regev and T. Vidick. Quantum XOR games. In *Proceedings of IEEE Conference on Computational Complexity (CCC 2013)*, pages 144–155. IEEE, 2013.

[17] B. W. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, pages 321–322. ACM, 2013.

[18] V. B. Scholz and R. F. Werner. Tsirelson's problem. Manuscript available at arXiv:0812.4305, 2008.

[19] I. E. Segal. Irreducible representations of operator algebras. *Bulletin of the American Mathematical Society*, **53**:73–88, 1947.

[20] W. Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. Manuscript available at arXiv:1606.03140, 2016.

[21] G. Vidal, D. Jonathan, and M. A. Nielsen. Approximate transformations and robust manipulation of bipartite pure state entanglement. *Physical Review A*, **62**:012304, 2000.

[22] J. Watrous. *The theory of quantum information*. Cambridge University Press, 2018.

A Some basics of C*-algebras

In this appendix, we supply a few basics of the theory of C*-algebras.

Given a Hilbert space $\mathcal{H}$, by a *concrete C*-subalgebra* $\mathcal{A}$, we mean any subset of the bounded linear operators on $\mathcal{H}$, $B(\mathcal{H})$ that is a subalgebra, is a closed subset in the operator norm and has the property that if $A \in \mathcal{A}$, then its adjoint A^*(sometimes denoted $A^\dagger$) is also in $\mathcal{A}$. Such algebras also have an abstract characterisation.

Definition A.1. *Let $\mathcal{A}$ be an algebra over the complex numbers, with a norm $\|\cdot\|$ and a map, $a \to a^*$, satisfying $(a+b)^* = a^* + b^*$, $(\lambda a)^* = \overline{\lambda} a^*$, $\forall \lambda \in \mathbb{C}$ and $(ab)^* = b^* a^*$. Then $\mathcal{A}$ is called a* **C*-algebra** *provided:*

- *$\mathcal{A}$ is complete in the norm $\|\cdot\|$,*
- *$\|ab\| \leq \|a\|\|b\|$,*
- *$\|a^* a\| = \|a\|^2$.*

A C*-algebra is **unital** if it contains an identity element with respect to multiplication. Given two C*-algebras, $\mathcal{A}$ and $\mathcal{B}$ a linear map $\pi : \mathcal{A} \to \mathcal{B}$ is called a **$*$-homomorphism** provided that it is a homomorphism, i.e., $\pi(ab) = \pi(a)\pi(b)$, and $\pi(a^*) = \pi(a)^*$. A $*$-homomorphism that is one-to-one and onto is called a **$*$-isomorphism**, and a $*$-isomorphism from $\mathcal{A}$ to $\mathcal{A}$ is called a **$*$-automorphism**. A $*$-homomorphism is automatically contractive, and hence, a $*$-isomorphism is isometric.

By a **state** on a unital C*-algebra $\mathcal{A}$, we mean any complex linear functional $s : \mathcal{A} \to \mathbb{C}$ that satisfies $s(I) = 1$ and $s(a^*a) \geq 0$ for all $a \in \mathcal{A}$. (Intuitively, any such s defines the outcome probabilities of all possible POVM measurements: for a measurement element of the form b, where $0 \leq b \leq I$, $s(b)$ is the probability of outcome b.)

The celebrated **Gelfand-Naimark-Segal theorem** [6, 19] tells us that every abstract C*-algebra $\mathcal{A}$ is $*$-isomorphic to a concrete C*-subalgebra of $B(\mathcal{H})$ for some Hilbert space. The key element of this theorem is a result about states. Given a unital C*-algebra $\mathcal{A}$ and a state, $s : \mathcal{A} \to \mathbb{C}$, its **GNS representation** consists of a Hilbert space $\mathcal{H}_s$ and a $*$-homomorphism,

$$\pi_s : \mathcal{A} \to B(\mathcal{H}_s) \text{ and } \eta_s \in \mathcal{H}_s \text{ such that } s(a) = \langle \eta, \pi_s(a)\eta_s \rangle.$$

Conversely, given a $\pi : \mathcal{A} \to B(\mathcal{H})$ and unit vector η we obtain a state by setting $s(a) = \langle \eta, \pi(a)\eta \rangle$. We call this the *induced state*. The following identifies when a triple $(\pi, \mathcal{H}, \eta)$ is really the same as the GNS representation.

Given a representation $\pi : A \to B(\mathcal{H})$ a unit vector $\eta \in \mathcal{H}$ is called *cyclic* if the set of vectors $\{\pi(a)\eta : a \in \mathcal{A}\}$ is dense in $\mathcal{H}$.

Proposition A.2. *Let $\pi : \mathcal{A} \to B(\mathcal{H})$, let $\eta \in \mathcal{H}$ be a unit vector, let $s(a) = \langle \pi(a)\eta, \eta \rangle$ be the induced state and let $\pi_s : \mathcal{A} \to B(\mathcal{H}_s)$ and η_s be the GNS representation. If η is cyclic, then there is a unitary $U : \mathcal{H}_s \to \mathcal{H}$ with $U\eta_s = \eta$ such that $U^*\pi(a)U = \pi_s(a)$ for all a.*

Let $S(\mathcal{A})$ denote the set of all states on $\mathcal{A}$. This is a convex set and a state is *pure* if and only if it is an extreme point of this set.

Proposition A.3. *Let $s \in S(\mathcal{A})$. The following are equivalent:*

1. *s is pure,*
2. *if $f : \mathcal{A} \to \mathbb{C}$ is a positive linear functional such that $f(p) \leq s(p)$ for all $p \in \mathcal{A}^+$, then there is a constant $c \geq 0$ such that $f(a) = c\, s(a)$ for all a,*
3. *if $\pi_s : \mathcal{A} \to B(\mathcal{H}_s)$ is the GNS representation, then $\pi_s(\mathcal{H})' = \mathbb{C} \cdot I_{\mathcal{H}_s}$.*

Because these three statements are the same, some books use one of these other properties as the definition of pure. Combining the two results we see that:

Proposition A.4. *Let $\pi : \mathcal{A} \to B(\mathcal{H})$ be a representation and let $\eta \in \mathcal{H}$ be a cyclic vector. Then the induced state is pure if and only if $\pi(\mathcal{A})' = \mathbb{C} \cdot I_{\mathcal{H}}$.*

A.1 Tensor Products of C*-algebras

In this paper we needed some properties of tensor products of C*-algebras, especially in defining the CAR algebra and its properties. Here we provide a very brief explanation of some of these facts/ideas.

Let $\mathcal{A}$ and $\mathcal{B}$ be two unital C*-algebras, and let $\mathcal{A}\otimes\mathcal{B}$ be their algebraic tensor product. For $x=\sum_i a_i\otimes b_i$ and $y=\sum_j c_j\otimes d_j$ in $\mathcal{A}\otimes\mathcal{B}$ we set

$$xy=\sum_{i,j} a_ic_j\otimes b_id_j,$$

which defines a product, and we define *a *-map* by

$$x^*=\sum_i a_i^*\otimes b_i^*.$$

These two operations make $\mathcal{A}\otimes\mathcal{B}$ into a $*$-*algebra*.

Note that the *-subalgebra $\{a\otimes 1 : a\in\mathcal{A}\}$ can be identified with $\mathcal{A}$ and similarly, $\{1\otimes b : b\in\mathcal{B}\}$ can be identified with $\mathcal{B}$. Also $(a\otimes 1)(1\otimes b)=a\otimes b=(1\otimes b)(1\otimes a)$ so that these "copies" of $\mathcal{A}$ and $\mathcal{B}$ commute.

There are two important ways to give this $*$-algebra a norm. Once we have a norm, it can be completed to become a C*-algebra.

Given $x\in\mathcal{A}\otimes\mathcal{B}$ we set

$$\|x\|_{\max}=\sup\{\|\pi(x)\| :\ \pi:\mathcal{A}\otimes\mathcal{B}\to B(\mathcal{H}) \text{ is a unital } *\text{-homomorphism}\},$$

where the supremum is taken over all Hilbert spaces $\mathcal{H}$ and all unital $*$-homomorphisms, i.e., homomorphisms such that $\pi(x)^*=\pi(x^*)$. The completion of $\mathcal{A}\otimes\mathcal{B}$ in this norm is a C*-algebra denoted $\mathcal{A}\otimes_{\max}\mathcal{B}$.

Alternatively, if $\pi_1:\mathcal{A}\to B(\mathcal{H}_1)$ and $\pi_2:\mathcal{B}\to B(\mathcal{H}_2)$ are unital $*$-homomorphisms, then setting $\pi(a\otimes b)=\pi_1(a)\otimes\pi_2(b)\in B(\mathcal{H}_1\otimes\mathcal{H}_2)$ and extending linearly, defines a unital $*$-homomorphism from $\mathcal{A}\otimes\mathcal{B}$ into $B(\mathcal{H}_1\otimes\mathcal{H}_2)$ denoted by $\pi=\pi_1\otimes\pi_2$.

Given $x\in\mathcal{A}\otimes\mathcal{B}$ we set

$$\|x\|_{\min}=\sup\{\|\pi_1\otimes\pi_2(x)\| :\ \pi_1:\mathcal{A}\to B(\mathcal{H}_1),\ \pi_2:\mathcal{B}\to B(\mathcal{H}_2) \text{ are unital } *\text{-homomorphisms}\}.$$

The completion of $\mathcal{A}\otimes\mathcal{B}$ in this norm is a C*-algebra denoted $\mathcal{A}\otimes_{\min}\mathcal{B}$.

Some C*-algebras $\mathcal{A}$ have the property that for every C*-algebra $\mathcal{B}$ the min norm and the max norm on $\mathcal{A}\otimes\mathcal{B}$ are equal. Such algebras are called *nuclear*. For example, every matrix algebra is nuclear.

Once we have seen these definitions for pairs of algebras it is easy to see how to extend it to define a min and a max norm on the tensor product of any finite collection of C*-algebras. To extend these definitions to tensor products of infinitely many C*-algebras, one first defines the infinite algebraic tensor product of unital algebras to consist of elements that are formal infinite tensor products that are equal to the identity in all but finitely many components. This is the construction used to build the CAR algebra, which is known to be a nuclear C*-algebra.

A good source for the above material is [9].

Here is an application of these ideas.

Theorem A.5. *If $s_1:\mathcal{A}_1\to\mathbb{C}$ and $s_2:\mathcal{A}_2\to\mathbb{C}$ be pure states then the state $s_1\otimes s_2:\mathcal{A}_1\otimes_{\min}\mathcal{A}_2\to\mathbb{C}$ defined as*

$$s_1\otimes s_2(a\otimes b)=s_1(a)s_2(b) \tag{33}$$

is also pure.

Proof. Let $\pi_i : \mathcal{A}_i \to B(\mathcal{H}_i)$, and η_i be a GNS for $s_i, i = 1, 2$. Then we have that

$$s_1 \otimes s_2(a \otimes b) = \langle \pi_1(a) \otimes \pi_2(b)\eta_1 \otimes \eta_2, \eta_1 \otimes \eta_2 \rangle.$$

Given any vector in $u \in \mathcal{H}_1 \otimes \mathcal{H}_2$ it can be approximated by a finite sum $\sum_i h_i \otimes k_i$. But since η_i are both cyclic vectors, we can approximate $h_i \sim \pi_1(a_i)\eta_1$ and $k_i \sim \pi_2(b_i)\eta_2$. Thus,

$$u \sim \pi_1 \otimes \pi_2(\sum_j a_j \otimes b_j)(\eta_1 \otimes \eta_2).$$

This proves that $\pi_1 \otimes \pi_2$ is the GNS representation for $s_1 \otimes s_2$. So to show that it is pure we need to show that $(\pi_1 \otimes \pi_2(\mathcal{A}_1 \otimes \mathcal{A}_2))' = \mathbb{C} \cdot (I \otimes I)$.

We can use operator matrices to do this. If we fix a basis $\{f_j\}$ for $\mathcal{H}_2$, then we can identify

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \simeq \sum_j \mathcal{H}_1 \otimes f_j \simeq \oplus_j \mathcal{H}_1.$$

With respect to this identification every $X \in B(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is represented by a matrix, $X = (X_{i,j})$, with $X_{i,j} \in B(\mathcal{H}_1)$.

Note that $\pi_1 \otimes \pi_2(a \otimes 1)$ becomes the diagonal matrix whose diagonal entries are $\pi_1(a)$. Now for $X = (X_{i,j})$ in the commutant, we have

$$(X_{i,j}\pi_1(a)) = X(\pi_1 \otimes \pi_2(a \otimes I)) = (\pi_1 \otimes \pi_2(a \otimes 1))X = (\pi_1(a)X_{i,j}).$$

Thus, each $X_{i,j} \in \pi_1(\mathcal{A}_1)$ and since s_1 was pure, we have $X_{i,j} = \lambda_{i,j} I_{\mathcal{H}_1}$.

So $X = I_{\mathcal{H}_1} \otimes T$ where $T = (\lambda_{i,j})$ is its matrix representation with repsect to the onb $\{f_j\}$.

But now the fact that $X = I \otimes T$ commutes with every $I \otimes \pi_2(b)$ and the fact that s_2 is pure, implies that $T = \lambda I_{\mathcal{H}_2}$. □

The following results are good for showing that the states on the CAR algebra that we are interested in are pure.

Proposition A.6. *Let $M_{n_1} \subseteq M_{n_2} \subseteq \cdots \subseteq \mathcal{A}$ be matrix algebras with $\mathcal{A}$ equal to the closure of their union, let $s : \mathcal{A} \to \mathbb{C}$ be a state and let $s_k : M_{n_k} \to \mathbb{C}$ be its restriction. If s_k is pure for all k, then s is pure.*

Proof. We show that if s is not pure, then there exists a k so that s_k is not pure. If s is not pure, then there exist states $0 < t < 1$ and states ρ, σ on $\mathcal{A}$ such that $s = t\rho + (1-t)\sigma$ and $s \neq \rho$.

If we let ρ_k, σ_k be the restrictions to M_{n_k} then $s_k = t\rho_k + (1-t)\sigma_k$. So we need to show that for some k, $s_k \neq \rho_k$. But since $s \neq \rho$ there exists $a \in \mathcal{A}$ with $|s(a) - \rho(a)| = r > 0$. By density we can find a k and $a_k \in M_{n_k}$ with $\|a - a_k\| < r/2$. Then

$$|s(a_k) - \rho(a_k)| = |(s-\rho)(a_k - a) + (s-\rho)(a)| \geq |s(a) - \rho(a)| - |(s - \rho(a - a_k)| \geq r - 2\|a - a_k\| > 0,$$

hence $s_k \neq \rho_k$. □

As an application consider our state on the CAR algebra defined by taking an infinite tensor product of $(\mathbb{C}^2, \psi_k)$. At the k-th level this is the vector state induced by $\psi_1 \otimes \cdots \otimes \psi_k \in \mathbb{C}^{2^k}$ on $M_{2^k} = B(\mathbb{C}^{2^k})$. Since M_{2^k} contains all linear transformations on this vector space, the vector is cyclic so this is the GNS representation of the induced state. But since the commutant of $M_{2^k} = B(\mathbb{C}^{2^k})$ is trivial, this state is pure. Thus, since s_k is pure for all k, the induced state on the CAR algebra is pure.

A.2 Actions and crossed-products

Some of our constructions use the concept of the crossed-product of a C*-algebra by an action of a group, which we briefly outline below. A good source for this material is [15].

Given a C*-algebra $\mathcal{A}$ and a unitary $u \in \mathcal{A}$, the map $a \to u^* a u$ is a $*$-automorphism of $\mathcal{A}$, but generally, not every $*$-automorphism can be obtained in this fashion. However, given a collection of $*$-automorphisms of $\mathcal{A}$, there is always a C*-algebra $\mathcal{B}$, containing $\mathcal{A}$, such that each of these $*$-automorphism of $\mathcal{A}$ is given as conjugation by a unitary in $\mathcal{B}$. More precisely, let $Aut(\mathcal{A})$ denote the group of $*$-automorphisms of $\mathcal{A}$, let G be a (discrete) group, and let $\alpha : G \to Aut(\mathcal{A})$, be a homomorphism. Then there is a C*-algebra, denoted $\mathcal{A} \rtimes_\alpha G$ which is generated as an algebra by $\mathcal{A}$ and a set of unitaries, U_g, $g \in G$ with the properties that

- $\mathcal{A} \subseteq \mathcal{A} \rtimes_\alpha G$,
- $U_g^* a U_g = \alpha_g(a), \forall a \in \mathcal{A}, g \in G$,
- whenever $\mathcal{B}$ is a C*-algebra, $\pi : \mathcal{A} \to \mathcal{B}$ is a one-to-one $*$-homomorphism and there exist unitaries $V_g \in \mathcal{B}$ satisfying $V_g^* \pi(a) V_g = \pi(\alpha_g(a))$, then there is a $*$-homomorphism $\Pi : \mathcal{A} \rtimes_\alpha G \to \mathcal{B}$ with $\Pi(a) = \pi(a)$ for all $a \in \mathcal{A}$ and $\Pi(U_g) = V_g$, for all $g \in G$.