Non-local Quantum Systems with Infinite Entanglement

by

Li Liu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Computer Science (Quantum Information)

Waterloo, Ontario, Canada, 2022

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Miguel Navascues Group Leader, Institute for Quantum Optics and Quantum Information – Vienna
Supervisor(s):	Richard Cleve Professor, IQC, University of Waterloo
Internal Member:	John Watrous Professor, IQC, University of Waterloo Shalev Ben-David Assistant Professor, IQC, University of Waterloo
Internal-External Member:	Vern Paulsen Professor, IQC, University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

- In Chapter 4, I give explicit definitions that build upon the C*-model to describe quantum systems that can be applied in topics of quantum information theory such as embezzlement of entanglement.
- In Chapter 5, I give a characterization of linear system game in infinite dimensions under the commuting operator model [4].
- In Chapter 6, I describe a protocol for performing perfect embezzlement of entanglement in the commuting operator and C*-model, as well as the impossibility of an exact protocol in the tensor product model [26].
- In Chapter 7, I describe a protocol for performing self-embezzlement in the commuting operator model and C*-model, and the impossibility of approximate self-embezzlement in the tensor product model [7].

.

Abstract

The study of quantum entanglement under quantum information has mostly been done in the mathematical model of tensor product of Hilbert spaces. In infinite dimensions, this model cannot capture all cases of non-local systems, and a more general model needs to be adopted; the most commonly used model here is the commuting operator model. We introduce another model, the C*-model, to describe non-local quantum systems in infinite dimensions. Instead of using Hilbert spaces to describe the states of a quantum system, a C*-algebra is used to describe the operators of a quantum system. The combination of two local quantum systems under this model is achieved by taking the tensor product of the two C*-algebras. The C*-model can be converted into the commuting operator model using the GNS representation theorem [13, 29], and it is a generalization of the tensor product of the Hilbert spaces model.

One of the applications of infinite dimensional entanglement is the so-called linear system games. Linear system games are non-local games derived from linear systems of equations. We show that a linear system game has a perfect commuting operator strategy if and only if the equations have a potentially infinite-dimensional operator solution, and this is related to the properties of the representations of a certain group called the solution group of the system of equations. This understanding of linear system games is used as the foundation for the work in [30] in which the author showed significant progress toward Tsirelson's problem[31].

Another application of infinite entanglement is the problem of embezzlement and self-embezzlement. Embezzlement is the task of locally creating an EPR pair using a shared state without changing the shared state; whereas self-embezzlement is the task of creating a copy of a shared entangled state locally without changing the

original shared state. These tasks can be achieved if there exist infinitely many EPR pairs in the shared state, and thus would require a stronger model such as the commuting operator model to be used. We show the protocol for embezzlement and self-embezzlement using both the commuting operator model and the C*-model. An interesting property of embezzlement and self-embezzlement is that under the tensor product of the Hilbert spaces model, embezzlement is impossible to achieve, and self-embezzlement is impossible to approximate. These two problems show that the C*-model is indeed more powerful than the tensor product of the Hilbert spaces model in handling infinite-dimensional quantum systems.

Acknowledgements

I would like to express my sincere gratitude towards my supervisor Richard Cleve, for his continuous support during the long journey of my Ph.D. study. His patience, motivation, and immense knowledge have guided me through all my research projects and the strenuous thesis writing process. Without his support, it would have been impossible to reach what I achieved in my studies.

I would also like to thank Prof. Vern Paulsen, for going above and beyond in patiently answering all the questions I had during my research and thesis writing, and for having extremely helpful discussions on my research projects. I thank William Slofstra for being an encouraging mentor in the collaboration of our co-authored paper. I appreciate all the efforts from my defence committee member, John Watrous, Shalev Ben-David, and Miguel Navascues for carefully going through my thesis and pointing out the typos and mistakes I had.

Finally, I would like to thank my parents for supporting me during the most difficult times of my thesis writing, and my roommate Weiliang Chen for being a great friend and being there with me during my entire Ph.D. study.

Dedication

To my parents

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Quantum mechanics, Quantum Information, and entanglement

Quantum mechanics studies the law of physics at the microscopic level. At the subatomic level, particles are no longer simply particles — they also behave like waves. The concept that matter is both continuous (wave-like) and discrete (particle-like) seems to be intuitively contradictory, and yet the wave-particle duality has been confirmed by countless experimental scrutiny over the past century. The oddity of quantum mechanics does not stop there. The wave-like property of particles allows them to superimpose on top of each other, sometimes causing two particles to cancel out each other at certain points due to the interference of their waveforms. Entanglement allows two particles to hold some shared information about each other so that even when they are spatially separated, measuring one particle in any coordinate system can determine the measurement outcome of the other particle in the same coordinate

system. The idea that the action on a particle will affect another particle arbitrarily distant apart seems to violate the principle of relativity. Einstein himself, even though his paper on the photoelectric effect puts him as one of the founders, was skeptical about quantum mechanics. His famous paper with Podolsky and Rosen on the EPR paradox [11] is an attempt to formalize this discrepancy mathematically. It was not clear to physicists at the time what exactly the issue was regarding entanglement.

In modern times, the study of quantum information looks at quantum mechanics from the angle of information theory. Instead of describing quantum mechanics based on physical systems, quantum information uses the abstract notation of qubits as the basic description of a quantum state. A pure qubit is described by a unit vector in $\mathbb{C}^2$. Similar to a classical bit that has a binary value between 0 and 1, a qubit can be expressed in terms of basis element $|0\rangle$ and $|1\rangle$ in $\mathbb{C}^2$. Using the Dirac notation for quantum states, the description of qubits contains no physical information, such as the position and momentum of a particle, about the underlying quantum system, and can be viewed as a purely mathematical object.

Multiple qubits are defined in terms of the tensor product of $\mathbb{C}^2$'s. The computational basis state of n qubits is typically expressed in terms of n-bit binary strings in the ket notation. It is not necessary to have a direct connection between the abstract n qubits and the corresponding physical system. An n-qubit state could be n particles with spins, or a single particle with 2^n energy levels, or something else entirely, although the n particle system is a more common interpretation. The Bell states, studied by J. S. Bell to refute the EPR paradox [3], are four maximally entangled two-qubit quantum state states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$, $\frac{|10\rangle-|01\rangle}{\sqrt{2}}$, and $\frac{|10\rangle+|01\rangle}{\sqrt{2}}$. They are typically considered as entangled states between two parties, which in turn implies that there is somehow a physical separation between the underlying physical object

behind the two qubits. Nevertheless, the type of physical object behind a Bell state is not important in quantum information, and the mathematical abstraction gives a clearer picture in explaining the EPR paradox.

We focus our discussion on the mathematical descriptions of non-local quantum systems in quantum information. There are different models describing non-locality. The most common model is the tensor-product model, which is extremely useful in cases where the dimension of the quantum system is finite. In infinite dimensions, the commuting operator model has been adopted by quantum field theory to describe localized systems. With models having their own strengths and shortcomings, we introduce a less commonly studied C*-model which acts as an in-between model.

1.2 The tensor product model and its shortcomings

Typically, when non-local systems are studied in quantum information, the default mathematical framework that is used to describe the system is the tensor product of Hilbert spaces. For a bipartite system between Alice and Bob, each of their quantum systems is usually a Hilbert space, $\mathcal{H}_A$ and $\mathcal{H}_B$, and the combined system is $\mathcal{H}_A \otimes \mathcal{H}_B$. Alice and Bob can have their quantum states and operators on their individual subsystems, and the overall system can be described by taking their tensor product.

For finite-dimensional quantum systems, the tensor product model describes the system accurately. It can be natural to assume that by simply taking the limit from finite to infinite dimensions, the tensor product model can also be used to describe infinite dimensional non-local quantum systems. After all, if Alice's quantum system can be described by an infinite dimensional Hilbert space, and so can Bob's quantum

system, it would make sense to take the tensor product of the two Hilbert spaces to describe the combined system.

However, such intuition is unfortunately insufficient to describe infinite dimensional non-local quantum systems. It may be surprising to many that the simple idea of having infinitely many Bell states shared between Alice and Bob cannot be described by taking the infinite tensor product of Bell states. In fact, as long as Alice and Bob are using the tensor product model, they are not able to share infinitely many Bell states. One may think that infinitely many Bell states can be achieved by taking the limit of $n \to \infty$ for n pairs of Bell states. However, this approach does not make sense mathematically, because for different n, the dimension of the Hilbert space for the state to be in is different, and as a result, there is no meaningful distance between n copies of Bell states and $n+1$ copies of Bell states. There is no such limit because the Hilbert spaces for different states are not comparable. One way to circumvent this issue is to start with infinite-dimensional Hilbert space, and a n-copy Bell states is a state with n copies Bell states in the first $2n$ qubits and $|00\rangle$ in the rest of the qubits. This allows the meaningful comparison between n and $n+1$ copies of Bell states, and one may think that the limit of $n \to \infty$ would make sense in this case. However, the issue here is different. The Hilbert space in this case is a space with all but finitely many qubits being $|00\rangle$ (or in other words, all the vectors in this Hilbert space must have infinitely many $|00\rangle$ at the end). By taking $n \to \infty$, the resulting state will not have infinitely trailing $|00\rangle$, and as a result, does not lie in the Hilbert space defined earlier. In spite of these failed approaches, there is a more fundamental reason behind why infinitely many Bell states cannot exist in a tensor product model that is somewhat technical. It relies on the analysis of the Schmidt coefficient of the state, which will be discussed later.

1.3 The commuting operator model

Despite the shortcomings in the mathematical modelling discussed earlier, the idea of having infinitely many Bell states is an intuitive one. In fact, there is a more general model of locality that has been used in quantum field theory to handle infinite-dimensional quantum systems, the commuting operator model, that can be used to describe infinitely many Bell states. The commuting operator model, different from the tensor product model, considers localities in a different way. Instead of having individual quantum subsystems tensor products together, the commuting operator model has only one Hilbert space that encompasses all of its subsystems. The notion of locality lies not in the structure of the Hilbert space itself, but in the structure of the operators on the Hilbert space. For example, consider a system with Alice and Bob's local systems in the commuting operator model. Alice and Bob share a single Hilbert space $\mathcal{H}$, and what makes Alice's local system "separated" from Bob's local system is that all of Alice's operators must mutually commute with all of Bob's operators. The rationale behind this commutivity requirement is the following. If a state is shared between Alice and Bob who are far apart, and they each apply some local operation to the state without any communication, the final resulting state should be the same regardless of whether Alice or Bob applied their operations first. Since there is only one Hilbert space for the entire system, any operator A Alice can perform must commute with any operator B Bob can perform, in other words, they must satisfy $AB = BA$. This is a generalization of the tensor product model since, in the tensor product model, Alice's operator will be of the form $A \otimes \mathcal{I}$ and Bob's operator will be of the form $\mathcal{I} \otimes B$ and those two operators always commute.

Since the locality of a commuting operator model depends on the sets of the local

operators, it is the structure of the operators that give rise to different local "parts" of the quantum system under the same Hilbert space. With the same Hilbert space, and the same quantum state, different sets of local operators could imply very different "ownership" of the state. An extreme example would be Alice's operators are all the bounded operators on the Hilbert space, and Bob's set of local operators will be forced to contain only the trivial identity operator. This is analogous to Alice having access to the entire quantum system leaving Bob with nothing in his hand. In another case, Alice and Bob could have some non-trivial mutually commuting sets of operators, and there exists another set of operators that mutually commute with both Alice's and Bob's operators. In this case, Alice's and Bob's quantum systems combined are not the entire quantum system described by the Hilbert space, and there could potentially be a third party with local quantum systems separated from Alice and Bob.

In the commuting operator model, it is difficult to single out part of a quantum state that "belongs" to a quantum subsystem, because everything is described under the same Hilbert space. Although the definition of the separable and entangled state exists in the commuting operator model, it is less clear where the boundaries are between different local systems. In the discussion of non-local quantum systems, it is often desirable to be able to think about different local systems separately and combine them or isolate out parts of the system. While the commuting operator model provides a powerful mathematical tool for handling infinite-dimensional quantum systems, the single Hilbert space makes it difficult to consider different local systems individually. For example, consider Alice and Bob having two identical quantum systems in their local lab, and share some entangled state between them. Under the commuting operator model, since Alice and Bob's systems both rely on the same Hilbert space, they have two individual sets of operators. To express that their local

systems are identical, there needs to be some equivalence relationship between Alice and Bob's operators. Furthermore, the idea that Alice and Bob share two copies of the same state would be tricky to define because there is only one single Hilbert space and the state cannot be split into two different parts. These issues can be addressed properly with careful definitions. However, the fact that such a simple concept would require extra effort in the basic definitions may raise the question of how approachable the commuting operator model is in discussing more complex problems.

1.4 The C*-model

Wanting the power of the commuting operator model in handling infinite-dimensional quantum systems, as well as the clarity of having a tensor product to describe local systems, a different model, which we call the C*-model will be discussed. The C*-model is a mathematical model that can use the tensor product as a separator for different local quantum systems, can be used to handle some of the infinite-dimensional cases the tensor-product model fails to, and can be mapped into the commuting operator model through a standard conversion. Instead of using Hilbert spaces as the fundamental building blocks for quantum systems, the C*-model uses C*-algebras. There is no inherent Hilbert space in the C*-model, and quantum states are simply functions that map operators in the C*-algebras into numbers. This may sound like a foreign and even arbitrary idea to those who are used to considering quantum states as vectors or density operators, but it is in fact very closely related to the conventional model. When taking measurements of a quantum state, the standard way is to take the trace of the product of the density operator and the measurement operator. This mapping from operators to scalars is abstracted in the definition of an *abstract*

state on a C*-algebra. In the C*-model, a state is defined by its measurement outcomes with respect to measurement operators, just like how a density operator can be viewed as a probabilistic mixture of different measurement outcomes. Without going into the details, the quantum operators in the C*-model are defined similarly to the quantum operators in the conventional Hilbert space model. Having different local quantum systems is equivalent to having different C*-algebras, and combining them is a matter of taking the tensor product (with some technicality here) of the C*-algebras. In a way, the C*-model can be made to "look like" the tensor product model in describing non-local quantum systems, and have similar properties when manipulated.

The benefit of the C*-model is that it can correctly capture some infinite dimensional cases that the tensor product model fails to capture, such as having infinitely many Bell states. It can be converted into the commuting operator model if one prefers the more standard notations for quantum mechanics. In a way, it can be viewed as an in-between model between the tensor product and commuting operator model.

1.5 Applications of the Models in Quantum Information

A natural question following the discussion of these more general models of locality is when they are useful in quantum information. The quantum state with infinitely many Bell states is an example of a useful state that cannot be achieved by the tensor product model but can be defined in the commuting operator model and the

C*-model. A few places where this particular state is useful include in the non-local game of linear system games, as well as the protocol of embezzlement and self-embezzlement. In these cases, the ability to define the infinitely many Bell states allows these applications to achieve something that could not be achieved using the tensor product model.

1.5.1 Non-Local Games

A non-local game is a set of rules involving multiple (typically two) players and a referee. In the two-player (Alice and Bob) case, the players are physically separated and not allowed to communicate once the game starts. The referee sends each player some classical input string from a set of inputs at random, and each player must reply with a classical output string. The outcome of the game is determined by a predefined payout metric, and the players win if their output strings satisfy the metric requirement of the income strings they received.

A simple example of a non-local game is when Alice and Bob each receive a single bit $a, b \in \{0, 1\}$, and output a single bit $s, t \in \{0, 1\}$, and they win if and only if $a \cdot b = s \oplus t$. This game is called the CHSH game and it has the surprising property that if Alice and Bob share a maximally entangled state, they can win the game with a probability of around 85%; whereas if they only share classical information, their maximal winning probability is mere 75%. There are also non-local games where Alice and Bob can win the game with certainty (probability 1) if they share entanglement but without entanglement, their chance of winning is strictly lower. The details of the games will be discussed later.

An interesting property of non-local games like the CHSH game is the existence

of a gap between classical and quantum winning probability. Even though the input and output strings of non-local games are of finite length, there are non-local games that require infinite-dimensional quantum states to perform optimally. With infinite-dimensional quantum systems, the question comes to whether it is under the tensor product model or the commuting operator model. It turns out that whether there is a gap between the optimal game-winning probability of the tensor product and the commuting operator model is directly related to Connes' Embedding Conjecture in mathematics [12, 16, 22]. The Connes' Embedding Conjecture was recently shown to be false by some very complex protocols developed using quantum information theory.[15]

A simpler example of non-local games demonstrating the power of the commuting operator model over the tensor product model is the linear system games. In linear system games, the questions and answers for the game come from a set of (binary) linear systems of equations. Without entanglement, Alice and Bob can only win the game with certainty if the set of linear systems of equations has a satisfying assignment of binary numbers to each of the variables. With entanglement, the players can win the game with probability 1 if there is an assignment of linear operators satisfying a variation of the original linear system of equations. The use of operators allows more general strategies between the players. One property of the linear system games is that the dimension of the operator solution does not need to be finite. When the dimension of the operator solution is finite, there exists a tensor product strategy for the players to win the game with probability 1. However, if the dimension of the operator solution is infinite, a commuting operator solution is needed to achieve winning probability 1.

1.5.2 Embezzlement and Self-Embezzlement

Another example where the commuting operator model as well as the C*-model, outperforms the tensor product model is the protocol of embezzlement and self-embezzlement. Embezzlement is based on the idea that if Alice and Bob share an infinite amount of entanglement (resource state), they should be able to locally retrieve a Bell state out of their resource state without changing it. Self-embezzlement is similar to embezzlement except instead of a single Bell state, Alice and Bob want to extract a copy of their resource state.

Even though infinitely many Bell state cannot be defined in the tensor product model, with some clever design of the resource state in finite dimensions, embezzlement can be achieved approximately when Alice and Bob extracts a Bell state and end up with a state that is close to the resource state [8]. The larger the dimension of the resource state, the closer the resulting state of Alice and Bob is to the resource state, and the approximation can be achieved for arbitrary precision. However, it can be shown that as long as Alice and Bob are under the tensor product model, perfect embezzlement is not possible. In other words, one cannot simply take a limit to make the resource state infinite-dimensional and get rid of the approximation.

To achieve embezzlement exactly, the commuting operator model (or the C*-model) can be used. The resource state contains infinite copies of Bell states, and Alice and Bob can swap out a Bell state while keeping the resource state intact.

Self-embezzlement is embezzlement with a twist. Alice and Bob's goal is to locally turn one copy of the resource state into two copies of the same state. The resource state can be any state (including finite-dimensional states) as long as it has at least as much entanglement as a single Bell state. The interesting aspect of self-embezzlement

is that it can be achieved exactly using the commuting operator model, whereas if Alice and Bob are restricted to the tensor product model, they cannot get the resulting state to approximate two copies of the resource state more than some constant strictly below 1.

Chapter 2

Quantum Mechanics and The Hilbert Space Model

2.1 Mathematical models for Quantum Mechanics

This section will briefly discuss the commonly used mathematical model for quantum mechanics.

2.1.1 Quantum states

One of the main aspects of quantum mechanics is that quantum states are described using wave functions. A wave function is a complex function over some domains such that it forms a probability density distribution. For example, consider a quantum state consisting of a particle in one-dimensional space with location $x \in \mathbb{R}$. The wave function $\psi(x)$ for this particle is a function indicating the probability density of being

at location x: $\int_{x_b}^{x_a} |\psi(x)|^2 dx$ gives out the probability that the particle is between location x_a and x_b. The particle exists somewhere along the x axis, and therefore

$$\int_{-\infty}^{\infty} |\psi(x)|^2 dx = 1. \tag{2.1.1}$$

In Dirac's notation, a quantum state can be described by a vector in the Dirac notation $|\psi\rangle$ in a Hilbert space $\mathcal{H}$ where $\langle\psi|\,\psi\rangle = 1$.

On the surface, the two definitions of quantum states appear very different from each other. The wave function $\psi(x)$ is a concrete description of the location of a particle, whereas $|\psi\rangle$ is an abstract vector that might appear to have little correspondence with the physical quantum system. It turns out that these two models are equivalent. For two wave functions $\psi(x)$ and $\phi(x)$, define the inner product between the two functions to be

$$\langle\phi|\,\psi\rangle = \int_{-\infty}^{\infty} \phi^*(x)\psi(x)dx. \tag{2.1.2}$$

With this inner product, an orthonormal basis can be defined for the wave functions. This orthonormal basis can then be further extended into a Hilbert space.

2.1.2 Observables on quantum states

Observables are physical properties of a system that can be measured. Examples of observables in classical mechanics include a physical system's position, momentum, and energy. In quantum mechanics, observables are Hermitian linear operators acting on the quantum states, and every observable in classical mechanics has a counterpart in quantum mechanics.

Given an observable $\hat{O}$, the possible measurement outcomes are the eigenvalues of $\hat{O}$. Let $\hat{O} = \sum \lambda_n |n\rangle \langle n|$ be the eigendecomposition of $\hat{O}$, and a measurement outcome

of λ_n indicates that the system is in state $|n\rangle$. Given a state $|\psi\rangle$, the expected value of $|\psi\rangle$ on observable $\hat{O}$ is $\langle\psi|\,\hat{O}\,|\psi\rangle$.

A typical example of observable is the Hamiltonian, which indicates the energy of a given system. Let $\hat{H}$ be a Hamiltonian describing a quantum system with a particle in a one-dimensional axis x. Let's further assume that the number of eigenstates of $\hat{H}$ is countable. Let $|n\rangle$ be the eigenstates of $\hat{H}$, satisfying $\hat{H}\,|n\rangle = E_n\,|n\rangle$, where the E_n's are sorted in ascending order. E_n is the system's energy level, with E_0 indicating the lowest energy any state in this system could have. A quantum state can be written as $|\psi\rangle = \sum |n\rangle\,\langle n|\,\psi\rangle$, where $\langle n|\,\psi\rangle = \int \langle n|\,x\rangle\,\langle x|\,\psi\rangle dx$, and $\{|n\rangle\}$ form a basis of the Hilbert space $|\psi\rangle$ is in.

2.1.3 Dynamics

Quantum states evolve in time according to the time-dependent Schrodinger's equation

$$\hat{H}\,|\psi\rangle = i\hbar\frac{\partial}{\partial t}\,|\psi\rangle\,, \tag{2.1.3}$$

where $\hat{H}$ is Hermitian. We adopt the hat notation for operators commonly used by physicists here in a discussion related to quantum mechanics.

As an operator, the time-evolution of a quantum system is $\hat{U}(t) = e^{-i\hat{H}t}$ such that a state $|\psi(t)\rangle = \hat{U}(t)\,|\psi(0)\rangle$ where $|\psi(0)\rangle$ is the quantum state of the system at time 0 and $|\psi(t)\rangle$ is the evolved quantum state at time t. If $|\psi\rangle$ is an eigenstate of $\hat{H}$ with eigenvalue E, $\hat{U}(t)\,|\psi\rangle = e^{-iEt}\,|\psi\rangle$.

The conceptualization that quantum states evolve over time, whereas observables remain unchanged, is called Schrodinger's picture. In contrast, according to Heisen-

berg's picture, quantum states are fixed, and evolution happens on the observables. An observable $\hat{O}$ at time t is described by $\hat{O}(t) = \hat{U}^*(t)\hat{O}\hat{U}(t)$, where $\hat{U}(t)$ is the same evolution unitary operator mentioned earlier. These two pictures are equivalent to each other mathematically. At time t, performing observable $\hat{O}$ on a state $|\psi\rangle$ gives

$$\langle\psi(t)|\,\hat{O}\,|\psi(t)\rangle = \langle\psi|\,\hat{U}^*(t)\hat{O}\hat{U}(t)\,|\psi\rangle = \langle\psi|\,\hat{O}(t)\,|\psi\rangle\,, \tag{2.1.4}$$

where both the Schrödinger's picture and Heisenberg's picture will give rise to the same measurement outcome.

2.2 Hilbert Space Model and Quantum Information

In quantum information theory, considering the physical interpretation of wave function behind a quantum state is rare, as they contain physical information of the quantum system. Quantum information treats quantum states as abstract units of information, and as a result, it is not concerned about the physical interpretation behind the abstraction. Whether a state in $|0\rangle$ corresponds to the location, energy, spin, or polarization of a particle is irrelevant, and only key concepts from quantum mechanics, such as observables and unitaries, are adopted.

2.2.1 Hilbert Spaces

This section discusses the Hilbert space model of quantum mechanics, as well as some basic elements of quantum information. The Hilbert space model is the mathematical model used to describe systems in quantum information, and we start with a review of Hilbert spaces and their properties.

Definition 2.1. *A* Hilbert space $\mathcal{H}$ *is a complex or real inner product space that is complete in metric space under the norm induced by the inner product.*

An inner product space is a vector space V over a field F with an inner product $\langle \cdot, \cdot \rangle \colon V \times V \to F$ satisfying the following: for all $x, y, z \in V$, $\alpha \in F$,

- $\langle x, y \rangle = \overline{\langle y, x \rangle}$,
- $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$ and $\langle x + z, y \rangle = \langle x, y \rangle + \langle z, y \rangle$,
- $\langle x, x \rangle \geq 0$ and $\langle x, x \rangle = 0$ if and only if $x = 0$.

Inner product spaces have a norm, $\| \cdot \| : V \to F$ defined by

$$\|x\| = \sqrt{\langle x, x \rangle}. \tag{2.2.1}$$

The distance function induced by the inner product $d \colon V \times V \to \mathbb{F}$ is defined as

$$d(x, y) = \|x - y\|. \tag{2.2.2}$$

Complete under a norm $\| \cdot \|$ in metric space means that every Cauchy sequence converges. :et $\{x_i\}_{i \in \mathbb{N}}$ be a sequence containing elements of V. Then $\{x_i\}_{i \in \mathbb{N}}$ is a Cauchy sequence if it satisfies for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $i, j > N$, $\|x_i - x_j\| < \epsilon$. Converging means that for all Cauchy sequences $\{x_i\}_{i \in \mathbb{N}} \subseteq V$, $\lim_{i \to \infty} x_i$ exists and $\lim_{i \to \infty} \in V$.

Given two Hilbert spaces $\mathcal{H}_1$, $\mathcal{H}_2$, it is possible to consider the composition of the two spaces in two ways, the direct sum and the tensor product.

Definition 2.2. *The* direct sum *of two Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$ is a Hilbert space denoted by $\mathcal{H}_1 \oplus \mathcal{H}_2$ where for any $a, c \in \mathcal{H}_1$, $b, d \in \mathcal{H}_2$,*

$$\langle a \oplus b, c \oplus d \rangle = \langle a, c \rangle_{\mathcal{H}_1} + \langle b, d \rangle_{\mathcal{H}_2}. \tag{2.2.3}$$

The addition rule for the direct sum is, for $a, c \in \mathcal{H}_1, b, d \in \mathcal{H}_2, \lambda \in \mathbb{C}$,

$$(a \oplus b) + \lambda(c \oplus d) = (a + \lambda c) \oplus (b + \lambda d). \tag{2.2.4}$$

Definition 2.3. *The* tensor product *of two Hilbert spaces $\mathcal{H}_1$, $\mathcal{H}_2$, is a Hilbert space denoted by $\mathcal{H}_1 \otimes \mathcal{H}_2$ where for any $a, c \in \mathcal{H}_1$, $b, d \in \mathcal{H}_2$,*

$$\langle a \otimes b, c \otimes d \rangle = \langle a, c \rangle_{\mathcal{H}_1} \langle b, d \rangle_{\mathcal{H}_2}. \tag{2.2.5}$$

The addition rule for the tensor product is, for $a, b \in \mathcal{H}_1, b, d \in \mathcal{H}_2, \lambda, \gamma \in \mathbb{C}$,

$$(a + \lambda b) \otimes (c + \gamma d) = (a \otimes c) + \gamma(a \otimes d) + \lambda(b \otimes c) + \lambda\gamma(b \otimes d). \tag{2.2.6}$$

For finite dimensional Hilbert spaces, if $\mathcal{H}_1$ has dimension m and $\mathcal{H}_2$ has dimension n, then the dimension of $\mathcal{H}_1 \oplus \mathcal{H}_2$ is $m + n$, whereas the dimension for $\mathcal{H}_1 \otimes \mathcal{H}_2$ is mn.

A linear operator on a Hilbert space $\mathcal{H}$ is a mapping $\mathcal{H} \to \mathcal{H}$ that is also linear. For finite-dimensional Hilbert spaces, they can be expressed in terms of finite square matrices. In quantum mechanics, most of the operators in discussion are linear. We will review some properties of linear operators commonly used in quantum mechanics.

Definition 2.4. *The norm $\|\cdot\|$ of a linear operator $O : \mathcal{H} \to \mathcal{H}$ is defined as*

$$\|O\| = \sup\{\|Ox\| \mid x \in \mathcal{H}, \|x\| = 1\}. \tag{2.2.7}$$

The norm of an operator in $\mathcal{H}$ depends on the inner product used to define $\mathcal{H}$. More properties of operators can be defined with the definition of the operator norm. Note that not all operators have a finite norm.

Definition 2.5. *A linear operator $O\colon \mathcal{H} \to \mathcal{H}$ is* bounded *if $\|O\| < \infty$. The set of all bounded linear operators in $\mathcal{H}$ is denoted by $\mathbb{B}(\mathcal{H})$.*

All finite-dimensional operators are bounded.

Definition 2.6. *An operator $A \in \mathbb{B}(\mathcal{H})$ is* self-adjoint *if $A = A^*$* [1]

Definition 2.7. *An operator $P \in \mathbb{B}(\mathcal{H})$ is an* orthogonal projection *if $P = P^* = P^2$.*

Definition 2.8. *An operator $P \in \mathbb{B}(\mathcal{H})$ is called a* positive *operator, denoted by $P \geq 0$, if for all $x \in \mathcal{H}$, it holds that $\langle x, Px\rangle \geq 0$.*

Let $P \in \mathbb{B}(\mathcal{H})$ be an orthogonal projection. Then the space $\mathcal{H}' = \{Px \mid x \in \mathcal{H}\}$ is a subspace of $\mathcal{H}$, and P is the projector onto $\mathcal{H}'$. P is used to convert the elements of $\mathcal{H}$ to elements of $\mathcal{H}'$ as well as to convert the linear operators in $\mathbb{B}(\mathcal{H})$ to $\mathbb{B}(\mathcal{H}')$.

Definition 2.9. *Let $\mathcal{H}$ be a Hilbert space and $\mathcal{H}'$ be a subspace of $\mathcal{H}$. Let P be the projection onto $\mathcal{H}'$. The* projection of operator $\cdot|_{\mathcal{H}'} : \mathbb{B}(\mathcal{H}) \to \mathbb{B}(\mathcal{H}')$ *is defined as*

$$A|_{\mathcal{H}'} = PAP \tag{2.2.8}$$

for all $A \in \mathcal{H}$.

Given an operator $B \in \mathbb{B}(\mathcal{H})$, its range $\mathrm{Ran}(B)$ is the set of vectors it can map to

$$\mathrm{Ran}(B) = \{x \in \mathcal{H} \mid \exists y \in \mathcal{H} \text{ s.t. } x = By\}. \tag{2.2.9}$$

[1] While physicists prefer to use the notation $A^\dagger$ to denote the conjugate transpose, we adopt the mathematician's notation of A^* in this thesis.

If the dimension of $\mathrm{Ran}(B)$ is finite, then B is said to have a finite rank.

An operator is compact if its image of the unit ball is compact. Equivalently,

Definition 2.10. *An operator $K \in \mathbb{B}(\mathcal{H})$ is* compact *if there exists a family $\{A_i\}_{i\in\mathbb{N}}$ of finite rank operators such that $\lim_{n\to\infty} \|K - A_n\| = 0$. The set of all compact operators is denoted by $\mathcal{K}(\mathcal{H})$.*

Next, we look at an important class of operators that are closely related to the evolution of quantum systems, namely the unitary, isometry, and co-isometry.

Definition 2.11. *A* unitary *$U \in \mathbb{B}(\mathcal{H})$ where $UU^* = U^*U = \mathcal{I}$.*

Similar to unitary is the definition of isometry.

Definition 2.12. *An operator $W \in \mathbb{B}(\mathcal{H})$ is an* isometry *if $W^*W = \mathcal{I}$; $W \in \mathbb{B}(\mathcal{H})$ is a* co-isometry *if $WW^* = \mathcal{I}$.*

A unitary is an operator that is both an isometry and a co-isometry.

Definition 2.13. *An operator $W \in \mathbb{B}(\mathcal{H})$ is a* partial isometry *if there exists some $P \in \mathbb{B}(\mathcal{H})$ where P is an orthogonal projection such that $W^*W = P$.*

It is also possible to define isometry and co-isometry on operators mapping from one Hilbert space to a different Hilbert space. For $W\colon \mathcal{H}_1 \to \mathcal{H}_2$, isometry means $W^*W = \mathcal{I}_2$, and co-isometry means $WW^* = \mathcal{I}_1$.

Next, we will define trace in infinite dimensions. Unlike in finite dimensions, the trace cannot be defined in general on all bounded operators in a Hilbert space. We will need to first define the class of operators where a trace can be taken, called the trace class.

Definition 2.14. *Let $\mathcal{H}$ be a Hilbert space and $T \in \mathbb{B}(\mathcal{H})$, let $s_1, s_2, \cdots$ be the singular values of T. T is in trace class if*

$$\|T\|_1 = \sum_i |s_i| < \infty. \tag{2.2.10}$$

We denote the set of trace class by $TC(\mathcal{H}) = \{T \in \mathbb{B}(\mathcal{H}) : \|T\|_1 < \infty\}$.

The trace class of $\mathcal{H}$ is spanned by the density operators in $\mathcal{H}$.

For any $T \in TC(\mathcal{H})$, the sum of the singular value converges and is the trace of T.

Definition 2.15. *The* trace $\mathrm{Tr}\colon TC(\mathcal{H}) \to \mathbb{C}$ *is a map defined in terms of an orthonormal basis $\{e_i\}$ of $\mathcal{H}$, where for any $A \in TC(\mathcal{H})$,*

$$\mathrm{Tr}(A) = \sum_i \langle Ae_i, e_i \rangle. \tag{2.2.11}$$

The sum is independent of the choice of the basis $\{e_i\}$

The trace operator satisfies $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for all $A, B \in TC(\mathcal{H})$.

For finite-dimensional operators, the trace is simply the sum of all the diagonal elements.

Closely related to trace is the definition of partial trace. Given an operator that acts on the tensor product of Hilbert spaces, it is possible to map it to an operator only acting on a subspace of the original space.

Definition 2.16. *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hilbert spaces. The* partial trace *of $\mathcal{H}_1 \otimes \mathcal{H}_2$ on $\mathcal{H}_2$ is a map $\mathrm{Tr}_{\mathcal{H}_2} : TC(\mathcal{H}_1 \otimes \mathcal{H}_2) \to \mathbb{B}(\mathcal{H}_1)$ where for any $a \in TC(\mathcal{H}_1 \otimes \mathcal{H}_2)$, we write $a = \sum_{i,j} \alpha_{ij} a_{1i} \otimes a_{2j}$,*

$$\mathrm{Tr}_{\mathcal{H}_2}(a) = \sum_{i,j} \alpha_{ij} \mathrm{Tr}(a_{2j}) a_{1i}. \tag{2.2.12}$$

The Hilbert space $\mathcal{H}_2$, in this case, is called being traced out from operator a.

2.2.2 Quantum States

In this section, we look at the basic properties of quantum systems described by Hilbert spaces. Let Q denote a quantum system, and $\mathcal{H}$ be the Hilbert space modelling Q.

We start by defining the quantum states as density operators.

Definition 2.17. *A state in* Q *is described by* $\rho \in \mathbb{B}(\mathcal{H})$*, satisfying* $\rho \geq 0$ *and* $\mathrm{Tr}(\rho) = 1$*. The set of all quantum states is denoted by* $\mathcal{D}(\mathcal{H})$*.*

$\mathcal{D}$ is also called the set of density operators.

Definition 2.18. *A quantum state* $\rho \in \mathcal{D}(\mathcal{H})$ *is pure if and only if there exists* $|\psi\rangle \in \mathcal{H}$ *such that* $\rho = |\psi\rangle\langle\psi|$*. If a state is not pure, it is called mixed.*

By linearity, a probabilistic mixture of density operators is also a density operator.

Let $\{p_i\}$ be a probability distribution and $\rho_i \in \mathcal{D}(\mathcal{H})$, then $\sum_i p_i \rho_i \in \mathcal{D}(\mathcal{H})$.

The set of density operators is a convex set, with the extremal points being the pure states.

In the case of pure states, it is common to use $|\psi\rangle$ instead of $|\psi\rangle\langle\psi|$ to denote a quantum state.

In quantum information, it is common to break down the basis of a Hilbert space into tensor products of $\mathbb{C}^2$'s, so that the states are manipulated at the "bit-wise" level called qubits. A qubit is simply a state $|\psi\rangle \in \mathbb{C}^2$ with orthonormal basis $\{|0\rangle, |1\rangle\}$ or explicitly, $\{\binom{1}{0}, \binom{0}{1}\}$.

The computational basis of multiple qubits is usually expressed in a string of $\{0, 1\}$ with the tensor product omitted. For example, for a Hilbert space with 2 qubits, the computational basis is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

2.2.3 Operations on Quantum States

There are different types of operations that can be performed on a quantum state.

The basic operators that can change quantum states are the unitary operators. Unitary operators in a Hilbert space maps one set of orthonormal basis in the Hilbert space to another set of orthonormal basis. Let $\mathcal{H}$ be a Hilbert space, and let $U \in \mathbb{B}(\mathcal{H})$ be unitary. Then there exists two sets of orthonormal basis $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ of $\mathcal{H}$ such that $U = \sum_i |f_i\rangle \langle e_i|$. A unitary can also be seen as a rotation of quantum states where the angle between states is preserved. Let $|\psi\rangle, |\phi\rangle \in \mathcal{H}$, so that $U|\phi\rangle$ and $U|\psi\rangle$ are the states after evolution U. Then $\langle\psi|\,\phi\rangle = \langle\psi|\,U^*U\,|\phi\rangle$. A unitary applied to a density operator ρ is the conjugation of U to ρ, $U\rho U^*$.

For single-qubit, the unitaries are 2 by 2 matrices that can be expressed in terms of linear combination of the Pauli matrices, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\mathcal{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, because they form the basis of $\mathbb{B}(\mathbb{C}^2)$. Note that the Pauli matrices themselves are also unitaries.

There are also non-unitary evolutions to quantum states. The most general form of the evolution is called channels, or CPTP (completely positive trace-preserving) maps.

Definition 2.19. *A quantum* channel *is a linear map* $\Phi : \mathbb{B}(\mathcal{H}) \to \mathbb{B}(\mathcal{H})$ *that satisfy the following two conditions.*

1. *For any Hilbert space* $\mathcal{H}_1$ *and* $P \in \mathbb{B}(\mathcal{H} \otimes \mathcal{H}_1)$, $P \geq 0 \implies (\Phi \otimes I)(P) \geq 0$.

2. *For all* $O \in \mathbb{B}(\mathcal{H})$, $\mathrm{Tr}(O) = \mathrm{Tr}(\Phi(O))$.

The first condition is the completely positive condition. It ensures that applying the channel to part of a state still gives a positive operator. The second condition is the trace-preserving condition that makes sure applying the channel to a quantum state still results in a state.

It turns out that any channel Φ can be expressed in terms of some set of operators called the Kraus operators, $\{A_i\} \subseteq \mathbb{B}(\mathcal{H})$ with $\sum_i A_i^* A_i = \mathcal{I}$, such that for any $O \in \mathbb{B}(\mathcal{H})$,

$$\Phi(O) = \sum_i A_i O A_i^*. \tag{2.2.13}$$

The Stinespring dilation theorem states that for any completely positive map $\Phi : \mathbb{B}(\mathcal{H}) \to \mathbb{B}(\mathcal{H})$, there exists a Hilbert space $\mathcal{K}$ and a unital $*$-homomorphism $\pi : \mathbb{B}(\mathcal{H}) \to \mathbb{B}(\mathcal{K})$ and $V : \mathcal{H} \to \mathcal{K}$ such that $\Phi(a) = V^* \pi(a) V$ for all $a \in \mathcal{H}$.

Moreover, for a mixed state $\rho \in \mathcal{D}(\mathcal{H})$, there exists a Hilbert space $\mathcal{K} = \mathcal{H} \otimes \mathcal{H}'$ and a state $|\psi\rangle \in \mathcal{K}$ such that $\mathrm{Tr}_{\mathcal{H}'}(|\psi\rangle\langle\psi|) = \rho$. $|\psi\rangle$ is called the purification of ρ. Let $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, then $|\psi\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle \otimes |e_i\rangle$, where $\{|e_i\rangle\} \subseteq \mathcal{H}'$ is an orthonormal set, is the purification of ρ.

Measurement operators are operations that can be performed on quantum states to get an outcome. A pure state $|\psi\rangle$ is a linear combination of basis elements $\{e_i\}$ of the Hilbert space, $|\psi\rangle = \sum_i \alpha_i |e_i\rangle$ where $\alpha_i \in \mathbb{C}$ and a measurement in the orthonormal basis $\{e_i\}$ can give rise to outcome i with probability $|\alpha_i|^2$, which can be interpreted as the state $|\psi\rangle$ has a probability of $|\alpha_i|^2$ to be in the state $|e_i\rangle$ after measurement.

A type of general measurement operator is called the POVMs (positive operator-valued measurements).

Definition 2.20. *A POVM is a set of operator* $\{P_i\} \subseteq \mathbb{B}(\mathcal{H})$ *satisfying* $P_i \geq 0$ *for all* i *and* $\sum_i P_i = \mathcal{I}$.

If $P_i = P_i^2$ for all i, then $\{P_i\}$ are projective measurements.

Applying POVM $\{P_i\}$ on a state $\rho \in \mathcal{D}(\mathcal{H})$ will give rise to measurement outcome i with probability $\mathrm{Tr}(P_i\rho)$.

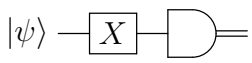
There are arguments on the interpretation of a state after measurement. Some would say a state collapses and is gone for good after a measurement is being performed, and others consider the state to change to a different state in accordance with the measurement operator. In particular, given some projective measurement $\{P_i\}$ and a state ρ, if the outcome of the measurement is i, then the state becomes

$$\rho' = \frac{P_i \rho P_i^*}{\mathrm{Tr}(P_i \rho P_i^*)}. \tag{2.2.14}$$

In quantum information, measurement outcomes tend to focus on which element of POVM it corresponds to, rather than the eigenvalue of an observable, as is the case in quantum mechanics.

2.2.4 Quantum Circuits

A useful tool to describe algorithms in quantum computing is the quantum circuit diagram. An algorithm usually consists of multiple steps of broken-down tasks. For quantum algorithms, even though all the steps can be combined into an all-encompassing



(a) $X|\psi\rangle$

(b) SWAP gate

(c) CNOT gate

Figure 2.1: Quantum circuit gates

unitary, a circuit diagram can be helpful in visualizing the logical flow of the algorithm in alignment with the broken-down steps. A quantum circuit diagram consists of lines that represent qubits, boxes that represent gates (or unitaries), and sometimes a special object that represents measurements (typically in the computational basis). The flow of the diagram is from left to right, so the left-most gate is applied to the qubits first.

For example, the following circuit diagram Fig 2.1a describes a single-qubit state $|\psi\rangle$ passing through a Pauli X gate, followed by a measurement operator. As a result, the state $X|\psi\rangle$ will be measured in the computational basis $\{|0\rangle, |1\rangle\}$.

There are other operations that can be described by the circuit diagram. For example, Fig 2.1b is a swap gate, which interchanges the two qubits. The corresponding unitary would be

$$U_{\text{SWAP}} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|. \tag{2.2.15}$$

Fig 2.1c shows a CNOT (controlled not) gate that flips the bit value of the second qubit if the first qubit is $|1\rangle$. The corresponding unitary is

$$U_{\text{CNOT}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|. \tag{2.2.16}$$

The swap gate can also be expressed in terms of three CNOT gates, as shown in Fig 2.2.

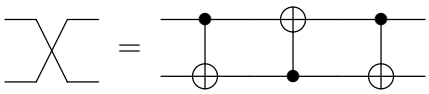


Figure 2.2: SWAP by CNOT

Quantum circuits can provide visual guidance to describe quantum algorithms with more clarity. An example is the quantum circuit for the 2-qubit quantum Fourier transform. A quantum Fourier transform (QFT) is the mapping of

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle \tag{2.2.17}$$

where $|j\rangle$ is a computational basis state and $\omega_N = e^{\frac{2\pi i}{N}}$

Example 2.1. Let U_{QFT2} be the unitary for 2-qubit quantum Fourier transform with the mapping

$$U_{\text{QFT2}} |j\rangle = \frac{1}{2} \sum_{k=0}^{3} i^{jk} |k\rangle . \tag{2.2.18}$$

Let $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ be the Hadarmard gate and $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ be the phase gate. Then the 2-qubit Fourier transform can be expressed as the following decomposition

$$U_{\text{QFT2}} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} = (\mathcal{I} \otimes H) U_{\text{SWAP}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} (H \otimes \mathcal{I}). \tag{2.2.19}$$

Using quantum circuits, U_{QFT2} can be expressed as

Note that in Equation 2.2.19, the deconstructed unitary multiplication will be applied to states from right to left, where the right-most unitary $(H \otimes \mathcal{I})$ is applied

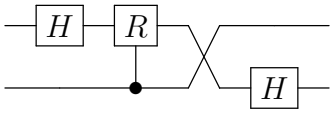


Figure 2.3: 2-qubit QFT circuit for U_{QFT2}

first. In contrast, the corresponding quantum circuit is drawn from left to right, so the left-most unitary $(H \otimes \mathcal{I})$ will be the first to apply to states.

Chapter 3

Locality under the Hilbert Space Models

Locality is a concept of a larger system consisting of smaller subsystems that are separated from (thus local to) each other, and any exchange of information between local systems is non-local.

Typically, when a quantum system Q is the composition of multiple subsystems, the subsystems are considered to be separated either physically or logically. For physically separated quantum systems, an entangled state is said to have non-local correlations between the two systems.

Einstein and others were skeptical about quantum mechanics [11] because quantum entanglement seems to be able to achieve something that is not classically possible. In the famous EPR paradox, the idea that a pair of entangled particles that are spatially separated could somehow "know" each other's spin if one of them is measured seems to be a violation of the no-signalling principle in relativity. To Einstein

et al., the so-called "spooky action at a distance" was a defect in the formulation of quantum mechanics, and with Bohm, they suggested that there must be some "hidden-variable" that contributes to the non-local effect brought by quantum entanglement.

Today we know that non-locality in quantum mechanics does not violate special relativity, but the problem remained open until Bell formulated his famous Bell's theorem in 1964. Bell's theorem essentially provides a concrete way to test for whether the world we live in is quantum mechanical or not in terms of the principle of locality.

There are two commonly used mathematical models describing multipartite quantum systems, the tensor product model and the commuting operator model. The commuting operator model is a generalization of the tensor product model, and with infinite dimensions, these two models can be shown to be equivalent. However, the precise relationship between these two models in infinite dimensions is not known in general. More discussions on this topic can be found in [31, 28, 16, 12].

3.1 Tensor Product Model for Multipartite Quantum Systems

When there are multiple local quantum systems, the typical way to describe them is to use a Hilbert space for each and every one of the local quantum systems and combine them by taking their tensor product. Given quantum systems $\{\mathsf{Q}_1, \mathsf{Q}_2, \cdots, \mathsf{Q}_n\}$, described by Hilbert spaces $\{\mathcal{H}_1, \cdots, \mathcal{H}_n\}$, the combined system is described by $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. The dimension of these Hilbert spaces can be finite, countably infinite, or uncountably infinite.

For example, let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Let an orthonormal basis of $\mathcal{H}_1$ be $\{|e_a\rangle\}_{a\in\Sigma_1}$ where Σ_1 is a set of indices that can potentially be uncountable. Similarly, let an orthonormal basis of $\mathcal{H}_2$ be $\{|f_b\rangle\}_{b\in\Sigma_2}$ where Σ_2 is a set of (potentially uncountable) indices. The tensor product of $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ has an orthonormal basis $\{|e_a\rangle \otimes |f_b\rangle\}_{a\in\Sigma_1, b\in\Sigma_2}$.

If each of the quantum systems Q_i has a state ρ_i defined in Section 2.18, then the corresponding combined state in Q is $\rho = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$. A state in the combined system Q, however, is not necessarily a direct composition of states from the subsystems.

Consider $\mathsf{Q} = (\mathsf{Q}_1, \mathsf{Q}_2)$ with Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

Definition 3.1. *A state $\rho \in \mathcal{D}(\mathcal{H}) = \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is a product state if there exist density operators $\rho_1 \in \mathcal{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathcal{D}(\mathcal{H}_2)$ such that*

$$\rho = \rho_1 \otimes \rho_2. \tag{3.1.1}$$

Definition 3.2. *A state $\rho \in \mathcal{D}(\mathcal{H}) = \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is separable if it is a probabilistic distribution of product states. In other words, there exists some probability distribution $\{p_i\}$ and density operators $\{\sigma_i\} \in \mathcal{D}(\mathcal{H}_1)$, $\{\gamma_i\} \in \mathcal{D}(\mathcal{H}_2)$ such that*

$$\rho = \sum_i p_i \sigma_i \otimes \gamma_i. \tag{3.1.2}$$

If ρ is not separable, it is entangled.

For pure states, the separability condition is more straightforward. Let $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be a state. Then $|\psi\rangle$ is separable if there exists $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$ such that $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.

One interesting property of states in uncountably infinite dimensional Hilbert spaces is that they can be expressed as a linear combination of countably many basis elements of the Hilbert space.

Theorem 3.1. *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state in which $\mathcal{H}$ has an orthonormal basis $\{|e_a\rangle\}_{a\in\Sigma}$ where Σ is an uncountable set. Then $|\psi\rangle$ can be written as a linear combination of countably many basis elements*

$$|\psi\rangle = \sum_{i\in\mathbb{N}} \alpha_a |e_a\rangle . \tag{3.1.3}$$

Proof. We can write $|\psi\rangle = \sum_a \alpha_a |e_a\rangle$ for some $\{\alpha_a\}_{a\in\Sigma}$. For $|\psi\rangle$ to be a state, we must have $\sum_a |\alpha_a|^2 = 1$. Since α_a's are square summable, only countably many of them can be non-zero. This can be shown by considering the sets $S_n := \{\alpha_a : \frac{1}{n+1} < |\alpha_a|^2 \leq \frac{1}{n}\}$ for $n \in \mathbb{N}$. $|S_n| \leq n$ because $|\alpha_a|^2$ sums to 1. Then the set of all non-zero of α_a is $\cup_n S_n$. The union of countably many finite-sized sets is countable. Therefore, $|\psi\rangle$ only has countably non-zero coefficients with respect to the orthonormal basis $\{e_a\} \subset \mathcal{H}$. □

Similarly, if a quantum state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is in the tensor product of two Hilbert spaces that have uncountable dimensions, it can be written in a Schmidt decomposition $|\psi\rangle = \sum_a \alpha_a |e_a\rangle \otimes |f_a\rangle$ for $\{|e_a\rangle\}$ and $\{|f_a\rangle\}$ being orthonormal basis for $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, and the number of non-zero coefficients α_a's must be countable. In other words, we can write $|\psi\rangle = \sum_{i\in\mathbb{N}} \alpha_i |e_i\rangle \otimes |f_i\rangle$.

3.1.1 Schmidt Decomposition in Infinite Dimensions

In infinite dimensions, the Schmidt Decomposition of quantum states across the tensor product of two arbitrary Hilbert spaces can be achieved similar to the Schmidt Decomposition in finite-dimensional spaces.

Theorem 3.2. *Let $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ where $\mathcal{H}_1$ and $\mathcal{H}_2$ are arbitrary (potentially uncountable) dimensional Hilbert spaces. Then there exists a decomposition of $|\psi\rangle$ such that*

$$|\psi\rangle = \sum_{i \in \mathbb{N}} x_i |u_i\rangle \otimes |v_i\rangle \tag{3.1.4}$$

where $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ are orthonormal sets in $\mathcal{H}_1$ and $\mathcal{H}_2$ and $x_i \geq 0$. Moreover, the coefficients $\{x_i\}$ are unique.

Proof. Let $\{|e_a\rangle : a \in \Sigma_a\}$,$\{|f_b\rangle : b \in \Sigma_b\}$ be the orthonormal basis of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. As a result of Theorem 3.1, $|\psi\rangle$ can be expressed in terms of countable linear combination $|\psi\rangle = \sum_{i,j} x_{i,j} |e_i\rangle \otimes |f_j\rangle$

Define $X = \sum_{i,j} x_{i,j} |i\rangle \langle j|$. Since $x_{i,j}$ comes from the coefficients of a quantum state $|\psi\rangle$, X is a compact operator in $\mathcal{H}$. We will show in Lemma 3.2.1 that X can be decomposed in terms of $X = UDV$ where $U = \sum_{i,j} u_{i,j} |i\rangle \langle j|$ is a partial isometry, $D = \sum_k d_k |k\rangle \langle k|$ is diagonal, and $V = \sum_{i,j} v_{i,j} |i\rangle \langle j|$ is unitary.

Moreover, write $U = \sum_{i,j} u_{i,j} |e_i\rangle \langle e_j|$, then $X = UDV = \sum_{i,j,k} u_{i,k} d_k v_{k,j} |i\rangle \langle j|$ which gives us $x_{i,j} = \sum_k u_{i,k} d_k v_{k,j}$.

The last step is to re-write $|\psi\rangle$ in terms of $|\psi\rangle = \sum_k d_k |u_k\rangle \otimes |v_k\rangle$ for some $|u_k\rangle$ and $|v_k\rangle$ that are orthonormal sets.

Let $|u_k\rangle = U |e_k\rangle = \sum_i u_{i,k} |e_i\rangle$. Since U is a partial isometry and $|e_k\rangle$ are orthonormal sets, $|u_k\rangle$ must be orthonormal. Let $\tilde{V} = \sum_{i,j} v_{i,j} |f_j\rangle \langle f_i|$. Since $V = \sum_{i,j} v_{i,j} |i\rangle \langle j|$ is a unitary, $\tilde{V}$ with the same coefficients and different orthonormal basis must also be a unitary. Let $|v_k\rangle = \tilde{V} |f_k\rangle = \sum_j v_{k,j} |f_j\rangle$, then $|v_k\rangle$ must be an

orthonormal set in $\mathcal{H}_2$. Finally, putting all of these together, we have

$$\begin{aligned} |\psi\rangle &= \sum_{i,j} x_{i,j} |i\rangle \otimes |f_j\rangle && (3.1.5) \\ &= \sum_{i,j} \sum_k u_{i,k} d_k v_{k,j} |i\rangle \otimes |f_j\rangle && (3.1.6) \\ &= \sum_k d_k \left(\sum_i u_{i,k} |i\rangle \right) \otimes \left(\sum_j v_{k,j} |f_j\rangle \right) && (3.1.7) \\ &= \sum_k d_k U |k\rangle \otimes \tilde{V} |f_k\rangle && (3.1.8) \\ &= \sum_k d_k |u_k\rangle \otimes |v_k\rangle . && (3.1.9) \end{aligned}$$

□

Lemma 3.2.1. *Let $\mathcal{H}$ be a Hilbert space and X be a compact operator in $X : \mathcal{H} \to \mathcal{H}$, then there exists a decomposition $X = UDV$ where U is a co-isometry, D is diagonal and V is unitary.*

Proof. Define $|X| = (X^*X)^{1/2}$, which is compact and positive. $|X|$, therefore, can be decomposed by its eigenvalues

$$|X| = V^* D V \tag{3.1.10}$$

where $V = \sum_{i,j} v_{i,j} |i\rangle \langle j|$ are unitaries and $D = \sum_k d_k |k\rangle \langle k|$ is diagonal. $\{d_k\}$ are the eigenvalues of $|X|$, and the singular values of X.

By the polar decomposition, there exists a partial isometry W such that $W|X| = X$. Let $U = WV^* = \sum_{i,j} u_{i,j} |i\rangle \langle j|$, so

$$X = W|X| = WV^*DV = UDV = \sum_{i,j,k} u_{i,k} d_k v_{k,j} |i\rangle \langle j| . \tag{3.1.11}$$

Since W is a partial isometry and V is a unitary, $U = WV^*$ is also a partial isometry.

□

3.2 Definitions and properties of the Commuting Operator Framework

The commuting operator framework uses a different notion of locality. This formalism is used in quantum field theory as a more general model for the tensor product framework. See [31, 28, 10, 16, 12] for more discussions.

In the commuting operator framework, there is an overall Hilbert space $\mathcal{H}$, and each local quantum systems $\mathsf{Q}_1, \cdots, \mathsf{Q}_n$ are described by different sets of operators $\mathbb{O}_1, \cdots, \mathbb{O}_n \subseteq \mathbb{B}(\mathcal{H})$ such that for all $X_i \in \mathbb{O}_i$, $X_i X_j = X_j X_i$ if $i \neq j$.

For simplicity, we consider bipartite systems between Alice and Bob, where Alice's set of operators is $\mathbf{A}$ and Bob's set of operators are $\mathbf{B}$. The definitions and properties can be extended into multipartite systems. We use bold font letters to denote local sets of operators.

3.2.1 Separability

Definition 3.3. *A pure quantum state $|\psi\rangle \in \mathcal{H}$ is a product state between $\mathbf{A}$ and $\mathbf{B}$ in the commuting operator model if and only if for all $A \in \mathbf{A}$, $B \in \mathbf{B}$,*

$$\langle\psi| AB |\psi\rangle = \langle\psi| A |\psi\rangle \langle\psi| B |\psi\rangle . \tag{3.2.1}$$

This is similar to the definition in the tensor product framework, where a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if and only if it can be written as $|\psi_A\rangle \otimes |\psi_B\rangle$, where for all $A \in \mathbb{B}(\mathcal{H}_A)$ and $B \in \mathbb{B}(\mathcal{H}_B)$,

$$(\langle\psi_A| \otimes \langle\psi_B|)(A \otimes B)(|\psi_A\rangle \otimes |\psi_B\rangle) = \langle\psi_A| A |\psi_A\rangle \langle\psi_B| B |\psi_B\rangle . \tag{3.2.2}$$

Similar to the definition in the tensor product framework, we start the definition of separable density matrices in the commuting operator model by first defining what product states are.

Definition 3.4. *A quantum state $\rho \in \mathcal{D}(\mathcal{H})$ is a product state between* $\mathbf{A}$ *and* $\mathbf{B}$ *in the commuting operator model if and only if for all $A \in \mathbf{A}$, $B \in \mathbf{B}$,*

$$\mathrm{Tr}(AB\rho) = \mathrm{Tr}(A\rho)\,\mathrm{Tr}(B\rho). \tag{3.2.3}$$

Definition 3.5. *A quantum state $\rho \in \mathcal{D}(\mathcal{H})$ is separable between* $\mathbf{A}$ *and* $\mathbf{B}$ *in the commuting operator model if and only if it is a probabilistic mixture of product states between* $\mathbf{A}$ *and* $\mathbf{B}$*.*

From the definition, separable pure states in the commuting operator model are also product states.

3.2.2 Partial state

In the commuting operator framework, there is only one Hilbert space, as a result, a state in this space has to be shared by Alice and Bob. Within the Hilbert space, the model for a state only belonging to Alice does not exist. Attempts to trace out a part of the state will change the structure of the Hilbert space. Instead, equivalent classes of states can be defined to describe states having the same part in Alice's local system (or Bob's).

Definition 3.6. *Two states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ are equivalent with respect to* $\mathbf{A}$ *in the commuting operator framework if for all $A \in \mathbf{A}$,*

$$\langle\psi_1| A |\psi_1\rangle = \langle\psi_2| A |\psi_2\rangle . \tag{3.2.4}$$

The equivalence relation is denoted by $|\psi_1\rangle \overset{\mathbf{A}}{\cong} |\psi_2\rangle$.

In other words, if two states are equivalent with respect to Alice, then all measurements on the two states performed by Alice will be the same.

Another way to look at the equivalence relation is to consider the bi-partite system with a commuting set of operators $\mathbf{A}$ and $\mathbf{B}$. If there is a unitary $U_B \in \mathbf{B}$ such that $|\psi_1\rangle = U_B |\psi_2\rangle$, then for any $A \in \mathbf{A}$,

$$\langle\psi_1| A |\psi_1\rangle = \langle\psi_2| U_B^* A U_B |\psi_2\rangle = \langle\psi_2| U_B^* U_B A |\psi_2\rangle = \langle\psi_2| A |\psi_2\rangle , \tag{3.2.5}$$

so $|\psi_1\rangle \overset{\mathbf{A}}{\cong} |\psi_2\rangle$. This means that if Bob can transform a state $|\psi_1\rangle$ to a state $|\psi_2\rangle$ using only local operations, then Alice's part of these two states must be equivalent to each other.

3.2.3 Comparing states between Alice and Bob

In the tensor product model, if Alice and Bob have the same Hilbert space $\mathcal{H}$, the overall Hilbert space is $\mathcal{H} \otimes \mathcal{H}$. They can each hold a copy of the same state $|\psi\rangle \in \mathcal{H}$, where the overall state is simply $|\psi\rangle \otimes |\psi\rangle$.

In the commuting operator model, with a single Hilbert space and two different sets of operators, comparing states between Alice and Bob requires a bit more work.

Definition 3.7. *In the commuting operator model, Alice and Bob have identical quantum systems if there exists an *-isomorphism between* $\mathbf{A}$ *and* $\mathbf{B}$.

It turns out that the *-isomorphism can be converted into conjugation by unitary.

Proposition 3.3. *Let $\mathbf{A}, \mathbf{B} \subseteq \mathbb{B}(\mathcal{H})$ be two commuting sets of operators. If there exists an *-isomorphism between $\mathbf{A}$ and $\mathbf{B}$, then there exists $\tilde{\mathbf{A}}, \tilde{\mathbf{B}} \subseteq \mathbb{B}(\mathcal{H}')$ that are *-isomorphic to $\mathbf{A}$ and $\mathbf{B}$, and some unitary $W \in \mathbb{B}(\mathcal{H}')$ such that for all $A \in \tilde{\mathbf{A}}$,*

$$WAW^* \in \tilde{\mathbf{B}}, \tag{3.2.6}$$

and for all $B \in \tilde{\mathbf{B}}$,

$$W^*BW \in \tilde{\mathbf{A}}. \tag{3.2.7}$$

Proof. Let $\mathcal{H}' = \mathcal{H} \oplus \mathcal{H}$, and let $\alpha : \mathbf{A} \to \mathbf{B}$ be the *-isomorphism. Define

$$\tilde{\mathbf{A}} := \left\{ \begin{pmatrix} a & 0 \\ 0 & \alpha(a) \end{pmatrix} : a \in \mathbf{A} \right\}, \quad \tilde{\mathbf{B}} := \left\{ \begin{pmatrix} b & 0 \\ 0 & \alpha^{-1}(b) \end{pmatrix} : b \in \mathbf{B} \right\}, \quad W = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}. \tag{3.2.8}$$

Then $\tilde{\mathbf{A}}$ is isomorphic to $\tilde{\mathbf{B}}$ with a unitary W that converts between them. □

With the above proposition, we can say without loss of generality that if $\mathbf{A}$, $\mathbf{B}$ are *-isomorphic to each other, there exists some unitary W that will convert between $\mathbf{A}$ and $\mathbf{B}$.

In other words, Alice and Bob's operators differ only by conjugation of some unitary W, and their elements have the same structure when performing addition, multiplication, and the $*$-operation. We sometimes write this as $W\mathbf{A}W^* = \mathbf{B}$.

With this, we can define in the commuting operator model the situation where Alice and Bob each hold a copy of the same state.

Definition 3.8. *Let $\mathbf{A}$ and $\mathbf{B}$ be two commuting sets of the operator such that $W\mathbf{A}W^* = \mathbf{B}$ for some unitary W. A state $|\psi\rangle$ is said to be the same under $\mathbf{A}$ and $\mathbf{B}$ if*

$$|\psi\rangle = W |\psi\rangle . \tag{3.2.9}$$

The definition is based on the idea that for any measurement operator in $\mathbf{A}$, conjugation by W will give a corresponding operator in $\mathbf{B}$, and if $|\psi\rangle = W|\psi\rangle$, the measurement outcome of the state will be the same for the matching measurement operators.

3.2.4 Combination of local quantum systems

When there commuting operator model is used to describe multiple local quantum systems, it still has one single Hilbert space, and each local quantum system is described by a set of operators that mutually commute with all the other sets of operators. Consider a multi-partite quantum systems $\{\mathsf{Q_1}, \mathsf{Q_2}, \cdots, \mathsf{Q_n}\}$. In the tensor product model, each of those quantum systems can be described using a Hilbert space $\{\mathcal{H}_1, \cdots, \mathcal{H}_n\}$, and the combination of any subset of the quantum system with indices $\{i_1, i_2, \cdots, i_m\} \subseteq \{1, 2, \cdots n\}$, $\{\mathsf{Q}_{i_1}, \mathsf{Q}_{i_2}, \cdots, \mathsf{Q}_{i_m}\}$, is simply described by the tensor product of their corresponding Hilbert space,

$$\mathcal{H}_{i_1} \otimes \mathcal{H}_{i_2} \otimes \cdots \otimes \mathcal{H}_{i_m}. \tag{3.2.10}$$

In the commuting operator model, with a single Hilbert space $\mathcal{H}$, the local quantum systems are described by multiple sets of bounded operators $\mathbf{B}_1, \cdots, \mathbf{B}_n \subseteq \mathbb{B}(\mathcal{H})$ where $\mathbf{B}_i$ and $\mathbf{B}_j$ mutually commute for all $i \neq j$. To describe the combined quantum system consisting of a subset of the local systems with indices $\{k_1, \cdots, k_m\}$, the corresponding operators $\{\mathbf{B}_{k_1}, \cdots, \mathbf{B}_{k_m}\}$ need to be combined. Unlike in the tensor product model where the combination process is simply taking the tensor product of the corresponding Hilbert spaces, in the commuting operator model, combining different sets of bounded operators is more than taking the superset of those operators.

The very first step is to put the sets together to form $\mathbf{B}_{k_1} \cup \cdots \cup \mathbf{B}_{k_m}$, and then take the completion of the new sets $\overline{\mathbf{B}_{k_1} \cup \cdots \cup \mathbf{B}_{k_m}}$ so that any linear combination of the elements in the set is covered. While one might be tempted to think that this is all the work that is required to combine the two quantum systems, this is not the end of the process yet.

The set of operators $\mathbf{B}_i$ for a local quantum system $\mathsf{Q_i}$ can be viewed as a C^*-algebra of the observables associated with measurements that can be performed to the quantum states in $\mathsf{Q_i}$. Combining two quantum systems $\mathsf{Q_i}, \mathsf{Q_j}$ should result in a set of operators that are local to $\mathsf{Q_i}$ and $\mathsf{Q_j}$ as general as possible, containing $\overline{\mathbf{B}_i \cup \mathbf{B}_j}$.

Let $\tilde{\mathsf{Q}} = \{\mathsf{Q_{k_1}}, \cdots, \mathsf{Q_{k_m}}\}$ be the set of quantum systems we are interested in. Let $\tilde{\mathbf{B}} = \overline{\mathbf{B}_{k_1} \cup \cdots \cup \mathbf{B}_{k_m}}$ be the C*-algebra associated with $\tilde{\mathsf{Q}}$. Let $U \in \mathbb{B}(\mathcal{H})$ be a unitary operator. U is in the set of operators for our quantum system of interest $\tilde{\mathsf{Q}}$ if the following two conditions are satisfied.

1. U does not change anything outside $\tilde{\mathsf{Q}}$; or U is *localized* to $\tilde{\mathsf{Q}}$. More specifically, for any $X \in \mathbb{B}(\mathcal{H})$ where X commutes with $\tilde{\mathbf{B}}$ (this includes all elements of $\mathbf{B}_j, j \notin \{k_1, \cdots, k_m\}$), conjugating X by U should not change X:

$$U^* X U = X. \tag{3.2.11}$$

2. If an operator is within $\tilde{\mathsf{Q}}$, U will not move it outside the set; or U *preserves* the C^*-algebra associated with $\tilde{\mathsf{Q}}$. More specifically, if an operator $X \in \tilde{\mathbf{B}}$, the operator resulting from conjugation by U is still in the same set,

$$U^* X U \in \tilde{\mathbf{B}}. \tag{3.2.12}$$

Conjugation by the unitary U to an operator in the Heisenberg's picture is equivalent to applying the unitary U to a quantum state in the Schrödinger's picture.

The first condition essentially dictates that U has to commute with any operators that are not within the subset. Equation 3.2.11 is equivalent to $UX = XU$ (by multiplying U from the left on both sides of the equation).

Condition 2 allows U to be something that is more general than simply the set $\overline{\mathbf{B}_{k_1} \cup \cdots \cup \mathbf{B}_{k_m}}$. U can mix elements across different subsets of operators that may not be achievable by linear combinations, as long as the end result remains in the overall subset of operators. An example of such a unitary U is shifting of infinite indices, and the details will be discussed in Chapter 6.

3.3 Non-local games and tests for locality

Non-local games are the extension of the idea that different notions of locality can result in different types of achievable correlations that can be tested. (The term "game" is in reference to games in game theory.) The simplest form of a non-local game involves a referee and two players, Alice and Bob. At the beginning of a game, the referee selects two inputs from a finite set $s, t \in \Sigma_{\text{in}}$ drawn according to some probability distribution p, and sends s to Alice, t to Bob. Alice and Bob are required to return some output from a finite set $a, b \in \Sigma_{\text{out}}$ to the referee. The referee then decides whether the players win based on some payoff function $f(a, b|s, t)$. Σ_{in}, p, and f are known to the players, and they could decide on their strategy together before the game starts. However, once the game starts, they are not allowed to communicate with each other and can only use their local resources to produce their output. The enforcement of no-communication is typically achieved by assuming the players are spatially separated and requesting the players to reply within a short time frame. Assuming the no-signalling principle in special relativity holds, there is not enough

time for them to communicate before sending their output to the referee.

3.3.1 Strategies Based on Different Notions of Locality

There are different types of restrictions on what Alice and Bob are allowed to share non-locally, based on the correlations Alice and Bob are allowed to share during the game. The most restrictive model is the classical model where Alice and Bob do not have any power beyond discussing strategies before the game starts, and possibly sharing some pre-determined classical random values during the game. The winning probability of the optimal strategy in the classical model is called the classical value of the game.

Relaxing the restrictions, we get the quantum mechanics model where Alice and Bob are allowed to share entangled qubits. The entanglement allows Alice and Bob to share correlations that are not available in the classical model and thus may give them more power in the game. Under this model, Alice and Bob's operators fall under two categories discussed earlier – the tensor product framework and the commuting operator framework. If Alice and Bob are restricted to tensor products of their individual operators, the winning probability of the optimal strategy is called the tensor-product value. If Alice and Bob are allowed to use commuting operators, the optimal winning probability is the commuting operator value.

The most relaxed restriction is when Alice and Bob may share any correlation as long as there is no faster than the speed of light communication (often called no signalling) involved. In this case, non-signalling forbids Alice from learning anything about Bob's input, so her output can only depend on her own input and cannot be correlated to Bob's input in any manner. More formally, it means that for any input

s Alice receives, the probability of her outputting a is the same for all the possible input t Bob receives, and vice versa for Bob.

To illustrate the point, consider the following game where the possible inputs and outputs are binary bits $\{0, 1\}$, and consider a fixed strategy for Alice and Bob. Let $P_{s,t,a,b}$ be the probability of Alice and Bob outputting (a, b) given input (s, t) for this particular strategy. When the value of an input or output is not specified, the symbol $*$ is used in the subscript. For example, the probability of Alice outputting $a = 1$ with input $s = 0$ is

$$P_{0,*,1,*} = \frac{1}{2}(P_{0,0,1,0} + P_{0,0,1,1} + P_{0,1,1,0} + P_{0,1,1,1}). \tag{3.3.1}$$

The factor of a half is in place because we assume Bob will receive input $t = 0$ or 1 with equal probability.

For any input (s, t) pair, the sum of all the probabilities of possible output $P_{s,t,*,*} = 1$.

The strategy is non-signalling if and only if for all Alice's input-output (a, s) pair,

$$P_{s,0,a,*} = P_{s,1,a,*}, \tag{3.3.2}$$

and for all Bob's input-output (b, t) pair

$$P_{0,t,*,b} = P_{1,t,*,b}. \tag{3.3.3}$$

Note that the non-signalling strategy only serves as an upper bound for what non-local strategies can achieve, and there is no currently no physical interpretation as to what kind of resources needs to be shared between Alice and Bob to achieve it. What we are more interested in are the classical and the quantum strategies which have physical consequences.

3.3.2 CHSH Game

The CHSH game is a non-local game with binary input and output. The referee selects $s, t \in \{0, 1\}$ uniformly at random independently. The players outputs $a, b \in \{0, 1\}$. They win the game if $a \oplus b = st$. In other words, $f(a, b|s, t) = \begin{cases} 1 & \text{if } a \oplus b = st \\ 0 & \text{otherwise} \end{cases}$.

If the players do not share quantum entanglement, they can only rely on shared information before the game starts. In this case, the optimal probability of winning the game is 75%, where they always output the same bit 0.

First, a deterministic strategy would be optimal because the winning probability of any probabilistic strategy is the convex combination of the winning probability of deterministic strategies, and cannot get larger than the best deterministic strategy.

While it is possible to enumerate all the deterministic strategies and find out the optimal one, it is easier to see that the all-zero output is indeed optimal. It is easy to see that the game cannot be won all the time. Let a_0, a_1, b_0, b_1 be Alice and Bob's output for different value of s and t. To win the game all the time, the following must be satisfied

$$a_0 \oplus b_0 = 0 \tag{3.3.4}$$

$$a_1 \oplus b_0 = 0 \tag{3.3.5}$$

$$a_0 \oplus b_1 = 0 \tag{3.3.6}$$

$$a_1 \oplus b_1 = 1. \tag{3.3.7}$$

By summing all the four equations, we get $0 = 1$ which is a contradiction. Therefore, Alice and Bob can't possibly win on all four possible inputs of (s, t). The next best outcome is for them to win on three inputs, which is the case they output 0 all the time. Thus outputting 0 is the optimal strategy and the winning probability is 3/4.

However, if the players are allowed to share entangled states, then by sharing a Bell state $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, they can achieve the optimal winning probability $\frac{1}{2} + \frac{1}{\sqrt{2}}$. When Alice receives input 0, she will measure her qubit of $|\psi\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$; and if Alice receives 1, she measure her qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$ where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If Bob receives input 0, he measures his qubit in $\{|a_0\rangle, |a_1\rangle\}$ basis where $|a_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and $|a_1\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$, and output i if his outcome is $|a_i\rangle$. If Bob receives 1, he measures in the basis $\{|b_0\rangle, |b_1\rangle\}$ where $|b_0\rangle = \cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle$ and $|b_1\rangle = \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$, and outputs i for output b_i.

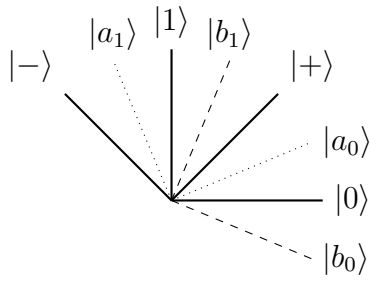


Figure 3.1: Measurements Associated with the CHSH game

Figure 3.1 shows the relative positioning of the basis where Alice's basis is in solid lines and Bob's basis is in dotted lines. It is easy to calculate the probability Alice and Bob's output matches any given input. For example, on input $(0, 0)$, the probability Alice and Bob output $(0, 0)$ is the probability of $|\psi\rangle$ projected onto $|0\rangle$ for Alice and $|a_0\rangle$ for Bob, which correlates to the angle between $|0\rangle$ and $|a_0\rangle$, which is $|\langle a_0|\, 0\rangle|^2 = \cos^2\frac{\pi}{8}$. Using the same argument, for any input other than $(1, 1)$, the winning outputs are $(0, 0)$ and $(1, 1)$, and the probability of Alice and Bob outputting the same bit is $\cos^2\frac{\pi}{8}$. If the input is $(1, 1)$, Alice and Bob's winning outputs are $(0, 1)$ and $(1, 0)$, and thus the winning probability relates to the angle between $\{|+\rangle, |b_1\rangle\}$,

and $\{|-\rangle, |b_0\rangle\}$, which is again $\cos^2 \frac{\pi}{8}$. The overall winning probability with this strategy is, therefore, $\cos^2 \frac{\pi}{8} = \frac{1}{2} + \frac{1}{\sqrt{2}}$. Tsirelson's inequality dictates that $\cos^2 \frac{\pi}{8}$ is indeed the maximum possible winning probability so the above strategy is optimal.

If the only limitation for the players is the non-signalling principle between spatially separated non-local parties, then this means the probability distribution of one player's output is independent of the other player's input. In term's of the CHSH game, this can be translated to the probability of Alice outputting 0 is the same for $t = 0$ and $t = 1$, and the probability of Bob outputting 0 is the same for $s = 0$ and $s = 1$. Under the non-signalling restriction, the best strategy would allow the players to win the game with probability 1.

$s\backslash t$		0		1	
$a\backslash b$		0	1	0	1
0	0	1/2	0	1/2	0
	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
	1	0	1/2	1/2	0

Table 3.1: Probability Output of CHSH Non-signalling Strategy

Table 3.1 shows a perfect non-signalling strategy for Alice and Bob. The first row and column are Alice and Bob's inputs, and the second row and column are Alice and Bob's outputs. The entries in the table are the probability of Alice and Bob producing the designated outputs given the corresponding inputs. For example, the probability of Alice and Bob outputting $(0, 0)$ given input $(0, 1)$ from the table is $1/2$. It is easy to see that all the non-zero entries in the table correspond to a winning

input-output combination. The strategy is non-signalling because Alice's probability of outputting 0 and 1 is the same for each of her inputs regardless of what Bob's output is.

By repeating the CHSH game, it is statistically possible to determine which version of the non-locality holds.

3.3.3 Binary Constraint System Games

A binary constraint system game [5] is a generalization of the CHSH game. It is a non-local game based on a system of binary linear equations (the constraints).

For the non-local game, Alice receives a mod-2 linear equation from the list of equations as constraints, and Bob receives a variable that appears in Alice's equation. Alice is required to output an assignment of all the variables in her equation, and Bob is required to output the assignment of the variable he receives. They win the game if Alice's assignment satisfies the equation and Bob's assignment matches with Alice's output of the variable. If the system of linear equations is not restricted to being binary, it is called linear system games. More discussions on linear system games will be made in Chapter 5.

In the case of the CHSH game, the linear equations are

$$a_1 \oplus a_2 = 0 \tag{3.3.8}$$

$$a_1 \oplus a_2 = 1. \tag{3.3.9}$$

Alice will receive one of the two equations (1 and 2) and Bob will receive one of the two variables (a_1 and a_2). Assuming Alice and Bob would like to have an optimal

strategy, Alice only needs to output the value for the first variable a_1. This is because the game is automatically lost if Alice's output does not satisfy the equation, and the value of a_2 is determined by the value of a_1. Table 3.2 shows all the possible input and output for the CHSH game and the outcome of the game (W for win and L for lose).

Input \ Output	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(1, 1)	W	L	L	W
(1, 2)	W	L	L	W
(2, 1)	W	L	L	W
(2, 2)	L	W	W	L

Table 3.2: Outcome for binary constraint version of CHSH

Input \ Output	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	W	L	L	W
(0, 1)	W	L	L	W
(1, 0)	W	L	L	W
(1, 1)	L	W	W	L

Table 3.3: Outcome for standard CHSH

Table 3.2 is essentially identical to the outcome table for the standard version of the CHSH game shown in Table 3.3, and therefore the binary constraint system version of the game is equivalent to the standard CHSH game.

In general, an equation in the linear system of equations may not contain all the variables in the system. As a result, Bob's input will depend on which equation Alice

gets. An interesting example of the binary linear system game is Mermin's Magic Square game.

3.3.4 Mermin's Magic Square Game

In the CHSH game, the 75% vs. 85% difference between classical and quantum strategies can be a little unsatisfactory to some. If two parties claim to share quantum entanglement, there is a more definitive way to prove that they are lying (assuming there are no errors in the qubits and measurements). The magic square game [24, 1, 6], based on Mermin's magic square [20, 19], gives an example where the optimal classical strategy has a winning probability of 17/18, whereas the optimal quantum strategy can win with certainty 1.

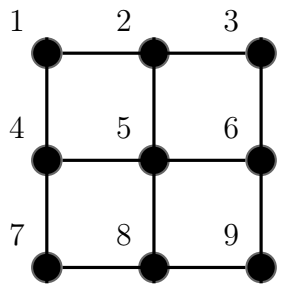


Figure 3.2: Mermin's Magic Square

A Mermin's magic square, as illustrated in Fig 3.2, has nine nodes, and six hyperedges with 3 nodes each. Each of the hyperedge e_i has a parity value of 0 or 1. The goal of the magic square is to assign binary value a_i to each node i, such that for the three nodes that share the same edge, the sum of the value of the nodes corresponds to the parity of the edge. In the original paper, all the horizontal edges have parity

0 and the vertical edges have parity 1.

$$\begin{aligned} a_1 \oplus a_2 \oplus a_3 &= 0 & a_1 \oplus a_4 \oplus a_5 &= 1 \\ a_4 \oplus a_5 \oplus a_6 &= 0 & a_2 \oplus a_5 \oplus a_8 &= 1 \\ a_7 \oplus a_8 \oplus a_9 &= 0 & a_3 \oplus a_6 \oplus a_9 &= 1. \end{aligned} \tag{3.3.10}$$

A slight modification to the magic square is to set the parity of all edges to 0 except for the edge with nodes 3, 6, and 9, where the parity is set to 1. This version of the magic square is equivalent to the original definition by flipping the value of a_7 and a_8. The new set of equations is

$$\begin{aligned} a_1 \oplus a_2 \oplus a_3 &= 0 \quad (e_1) & a_1 \oplus a_4 \oplus a_5 &= 0 \quad (e_4) \\ a_4 \oplus a_5 \oplus a_6 &= 0 \quad (e_2) & a_2 \oplus a_5 \oplus a_8 &= 0 \quad (e_5) \\ a_7 \oplus a_8 \oplus a_9 &= 0 \quad (e_3) & a_3 \oplus a_6 \oplus a_9 &= 1. \quad (e_6) \end{aligned} \tag{3.3.11}$$

We focus our discussion on this modified version of the magic square.

Another equivalent form of the magic square is to change the nodes to take the value $(-1)^{a_i}$ instead of a_i, and the equation for the edges are multiplications of the variables, equaling to -1 to the power of the parity of the edges. This gives us a different set of equations from Eq 3.3.11,

$$\begin{aligned} a_1 \cdot a_2 \cdot a_3 &= 1 & a_1 \cdot a_4 \cdot a_5 &= 1 \\ a_4 \cdot a_5 \cdot a_6 &= 1 & a_2 \cdot a_5 \cdot a_8 &= 1 \\ a_7 \cdot a_8 \cdot a_9 &= 1 & a_3 \cdot a_6 \cdot a_9 &= -1. \end{aligned} \tag{3.3.12}$$

It is easy to see that there is no assignment of the nodes that can satisfy all the parity of the edges at the same time. Since $a_i^2 = 1$ for all a_i, multiplying all the edges together will give us a contradiction of $1 = -1$.

However, if the a_i's are allowed to be matrices A_i's, there is a satisfying assignment for the following systems of equations.

$$\begin{aligned} A_1 \cdot A_2 \cdot A_3 &= \mathcal{I} & A_1 \cdot A_4 \cdot A_5 &= \mathcal{I} \\ A_4 \cdot A_5 \cdot A_6 &= \mathcal{I} & A_2 \cdot A_5 \cdot A_8 &= \mathcal{I} \\ A_7 \cdot A_8 \cdot A_9 &= \mathcal{I} & A_3 \cdot A_6 \cdot A_9 &= -\mathcal{I}. \end{aligned} \tag{3.3.13}$$

In order for a matrix assignment to make sense, the following two conditions must be met.

1. $A_i^2 = \mathcal{I}$ for all i. This is in line with the fact that $a_i^2 = 1$ for all i.
2. If node i and j appear in the same edge, $A_i A_j = A_j A_i$. This commutivity condition serves two purposes. First, in Equation 3.3.12, the order of a_i does not matter; and second, mutually commuting observables in quantum mechanics can be measured simultaneously.

The following is an assignment of binary observables that satisfy the above conditions

$$\begin{aligned} A_1 &= \mathcal{I}_2 X & A_2 &= X\mathcal{I}_2 & A_3 &= XX \\ A_4 &= Y\mathcal{I}_2 & A_5 &= \mathcal{I}_2 Y & A_6 &= YY \\ A_7 &= YX & A_8 &= XY & A_9 &= ZZ. \end{aligned} \tag{3.3.14}$$

where $\mathcal{I}_2, X, Y, Z$ are the 2×2 Pauli matrices and we omitted the $\otimes$ between each pair of operators. (i.e. $\mathcal{I}_2 X$ is shorthand for $\mathcal{I}_2 \otimes X$ etc.)

The set of equations in Mermin's magic square can be used to form a binary constraint system game. In this particular game, Alice and Bob are given Equation 3.3.11 from Mermin's magic square. At the start of the game, Alice is given a random number from 1 to 6, where each number corresponds to one equation (e_i) in

Equation 3.3.11; and Bob is given a random number from 1 to 9, where each number corresponds to one variable a_1 to a_9; the variable Bob receives must appear in Alice's equation. Alice is required to output 3 bits that assign a binary value to each variable in the equation she receives, and Bob is required to output 1 bit which is the assignment of the variable he receives. The players win the game if Alice's output satisfies the linear equation she receives, and Bob's assignment of the variable is the same as Alice's assignment of the same variable.

For example, if Alice's input is 2, the equation she receives is $a_4 \oplus a_5 \oplus a_6 = 0$, and she will need to assign value to variable a_4, a_5, and a_6 as her output. Bob in this case may receive input from $\{4, 5, 6\}$. If Bob receives 5, he will need to assign a bit value to a_5 as his output. If Alice's assignment is $0, 1, 1$, then Bob's output must be 1 to win the game.

If Alice's assignment does not satisfy the equation, the game is lost right away. Therefore, it is reasonable to consider in the setting of optimal strategy that Alice always satisfies her assignment. This means that she only needs to output the first two bits, and the third bit is automatically determined by the parity of the equation.

If Alice and Bob are not allowed to share any entanglement, a deterministic strategy would be optimal because the winning probability of any probabilistic strategy is the convex combination of the winning probability of deterministic strategies, and cannot get larger than the best deterministic strategy. It turns out that the best strategy for them is to always output 0 for all inputs. In this case, they will win on all the inputs except when Alice receives 6 and Bob receives 9.

If Alice and Bob are allowed to share entanglement, there exists a strategy where they can win the game with certainty. To begin the game, Alice and Bob shares two

pairs of maximally entangled qubits in Bell state, $|\psi\rangle = \frac{1}{2}\sum_{j=0}^{3} |j\rangle \otimes |j\rangle$. To output the value of variable a_i, Alice applies measurements A_i defined in Equation 3.3.14 her part of the shared state, and Bob applies measurement A_i^T to his part of the shared state. Alice and Bob's outcome of the same measurement will be the same because

$$\langle\psi| A_i \otimes A_i^T |\psi\rangle = \langle\psi| A_i A_i \otimes \mathcal{I} |\psi\rangle = \langle\psi |\psi\rangle = 1. \tag{3.3.15}$$

Note that all the A_i's are binary observables with eigenvalue ± 1, and while Alice is required to perform two measurements, her two observables commute with each other, meaning the measurements could be performed simultaneously without affecting the outcome of each other.

In [2], Arkhipov showed that a generalization of Mermin's magic square game to a special type of binary constraint system game where each variable appears in exactly two constraints, there exists a polynomial time algorithm to determine if a perfect entangled strategy exists.

Chapter 4

The C*-model

The use of operator algebras to describe quantum systems has been studied before, notably by von Neumann. However, in quantum information theory, quantum systems have been studied mainly under the Hilbert space model. In particular, the notion of local quantum systems is typically described using the tensor product of Hilbert spaces, or sometimes a single Hilbert space with commuting sets of operators. We want to introduce the operator algebra approach to describe (potentially infinitely many) qubits. In particular, we consider the formulation of quantum information theory using C*-algebras.

4.1 Basic Systems in C*-model

For readers who are not familiar with operator theory, we start by introducing the basic definitions of C*-algebras. They can be seen as an abstraction of complex square matrices, or generalization of linear operators on Hilbert spaces. In general,

the calligraphic font for capital letters, such as $\mathcal{A}, \mathcal{B}$, etc., are used to denote C*-algebras, except $\mathcal{H}$ for Hilbert spaces, and $\mathcal{I}$ for the identity element.

4.1.1 Definition of a C*-algebra

Definition 4.1. *A C*-algebra $\mathcal{A}$ is a normed associative algebra over the field of complex numbers with operator $\cdot^*\colon \mathcal{A} \to \mathcal{A}$, such that for all $a, b \in \mathcal{A}$ and $\alpha \in \mathbb{C}$,*

- $(a^*)^* = a$,
- $(ab)^* = b^* a^*$,
- $(\alpha a + b)^* = \bar{\alpha} a^* + b^*$,
- $\|a\|^2 = \|aa^*\|$,
- $\|ab\| \leq \|a\|\|b\|$,

and the algebra is complete under its norm.

The set of bounded operators on a Hilbert space is an example of a concrete C*-algebra.

Example 4.1. Let $\mathcal{H} = \mathbb{C}^n$. The set of bounded operators on $\mathcal{H}$, which are all the $n \times n$ complex matrices, forms a C*-algebra $\mathcal{M}_n$. The $*$ operator on $\mathcal{M}_n$ is the adjoint of the matrices, and the norm $\|\cdot\|$ on $\mathcal{M}_n$ is the operator norm on the matrices, defined by

$$\|M\|^2 = \sup_{|\psi\rangle \in \mathcal{H}, \||\psi\rangle\|=1} \langle\psi| MM^* |\psi\rangle \tag{4.1.1}$$

for any $M \in \mathcal{M}_n$.

4.1.2 Basic Properties of C*-Algebras

Here we discuss some basic properties of C*-algebras that are useful for describing quantum systems. Many of these concepts can be found in the books by Pederson [25] and Davidson [9].

Definition 4.2. *A C*-algebra is unital if and only if it contains the multiplicative identity $\mathcal{I}$, and $\mathcal{I} = \mathcal{I}^*$.*

Since the identity operator is essential in quantum information, we require all our C*-algebras to be unital. This requirement can be easily satisfied since any non-unital C*-algebra has a unique conversion to an unital C*-algebra that contains the original C*-algebra.

Proposition 4.1. *Let $\mathcal{A}$ be a non-unital C*-algebra. Then there exists an unital C*-algebra that contains $\mathcal{A}$ isometrically as a subalgebra.*

Proof. Let $\mathcal{A}^+ := \mathcal{A} \oplus \mathbb{C}$ be an algebra. Any $a \in \mathcal{A}$ can be mapped to $a \oplus 0 \in \mathcal{A}^+$. The product rule for $a \oplus \lambda, b \oplus \gamma \in \mathcal{A}^+$ is the following

$$(a \oplus \lambda) \cdot (b \oplus \gamma) = (ab + \lambda b + \gamma a) \oplus \lambda\gamma. \tag{4.1.2}$$

Therefore, the multiplicative identity element in $\mathcal{A}^+$ is $0 \oplus 1$.

For any $a \oplus \lambda \in \mathcal{A}^+$, we define the following as the norm:

$$\|a \oplus \lambda\| = \sup_{b \in \mathcal{A}, \|b\|_A \leq 1} \|ab + \lambda b\|. \tag{4.1.3}$$

[1] With the above norm defined, we obtain unital C*-algebra containing $\mathcal{A}$. □

[1] In [25], it is proven that $\|a \oplus 0\| = \|a\|$

With the above result in mind, all the C*-algebras for the C*-model are unital unless specified otherwise.

Next, we introduce a few definitions that are useful for quantum information.

Definition 4.3. *Let $\mathcal{A}$ be a C*-algebra. $p \in \mathcal{A}$ is* positive*, denoted by $p \geq 0$ if and only if there exists some $x \in \mathcal{A}$ such that $p = xx^*$.*

Definition 4.4. *Let $\mathcal{A}$ be a C*-algebra. $p \in \mathcal{A}$ is a* projection *if and only if $p \geq 0$ and $p = p^2$.*

Definition 4.5. *Let $\mathcal{A}$ be a C*-algebra. $u \in \mathcal{A}$ is a* unitary *if and only if $uu^* = u^*u = \mathcal{I}$.*

Definition 4.6. *Let $\mathcal{A}$, $\mathcal{B}$ be two C*-algebras. A linear map $\pi : \mathcal{A} \to \mathcal{B}$ is a $*$-homomorphism if and only if for all $x, y \in \mathcal{A}$,*

$$\pi(x)^* = \pi(x^*), \tag{4.1.4}$$

$$\pi(xy) = \pi(x)\pi(y). \tag{4.1.5}$$

If a *-homomorphism π preserves the identity element, it is called unital *-homomorphism. We are primarily interested in the unital *-homomorphism, so the *-homomorphisms we discuss later are all unital.

A special case of $*$-homomorphism is $*$-isomorphism.

Definition 4.7. *Let $\mathcal{A}, \mathcal{B}$ be two C*-algebras. A linear map $\pi : \mathcal{A} \to \mathcal{B}$ is a $*$-isomorphism if and only if it is a $*$-homomorphism and is invertible.*

Similar to $*$-isomorphism is the definition of $*$-automorphism.

Definition 4.8. *Let $\mathcal{A}$ be a C*-algebra. The map $\alpha : \mathcal{A} \to \mathcal{A}$ is a $*$-automorphism if α is a $*$-homomorphism and is invertible. $Aut^*(\mathcal{A})$ denotes the set of all $*$-automorphisms on $\mathcal{A}$.*

α is called a inner $*$-automorphism if there exists some unitary $u \in \mathcal{A}$ such that for all $a \in \mathcal{A}$, $\alpha(a) = uau^{-1}$. The set of all inner $*$-automorphisms on $\mathcal{A}$ is denoted as $Inn^*(\mathcal{A})$.

$Out^*(\mathcal{A}) := Aut^*(\mathcal{A}) \backslash Inn^*(\mathcal{A})$ is the set of all outer $*$-automorphisms on $\mathcal{A}$.

For some C*-algebras, all $*$-automorphisms are inner $*$-automorphisms. We will discuss more about such C*-algebras in Theorem 4.2.

4.1.3 States and Measurements in the C*-model

While our goal is to use C*-algebras to describe quantum systems, we are not inventing new definitions for quantum mechanics. In particular, the C*-model is an abstraction of the typical Hilbert space model and can be easily converted back to the Hilbert space model.

We start with defining states and measurement operators in the C*-model.

Definition 4.9. *Given a C*-algebra $\mathcal{A}$, a map $\phi : \mathcal{A} \to \mathbb{C}$ is positive, denoted by $\phi \geq 0$, if and only if for all $x \in \mathcal{A}$, $x \geq 0 \implies \phi(x) \geq 0$.*

With the above definition of positive operators, we can now define states in the C*-model.

Definition 4.10 (States)**.** *Given a C*-algebra $\mathcal{A}$ that describes a quantum system Q, a state s is a positive linear map $s : \mathcal{A} \to \mathbb{C}$ satisfying $s(\mathcal{I}) = 1$.*

The states in the C*model are also called the abstract states. These abstract states are simply an abstraction of the states in the Hilbert space model.

We define a special type of state that corresponds to the maximally mixed states in the Hilbert space model.

Definition 4.11 (Tracial states)**.** *Given a C*-algebra $\mathcal{A}$, an abstract state $\tau : \mathcal{A} \to \mathbb{C}$ is tracial if for all $a, b \in \mathcal{A}$, $\tau(ab) = \tau(ba)$.*

The term tracial is referring to the fact that τ has the same cyclic property as a trace. For the C*-algebra of $n \times n$ complex matrices, $\mathcal{M}_n(\mathbb{C})$, a tracial state τ correspond to the ordinary trace scaled by $\frac{1}{n}$ (so that identity is mapped to 1), Tr_n. The state can also be seen as $s(x) = \mathrm{Tr}(\rho_n x)$ where ρ_n is the density operator corresponding to the maximally mixed state in $\mathcal{M}_n$.

A general finite dimensional C*-algebra is a direct sum of matrix algebras, $\mathcal{M} = \bigoplus_{k=1}^{m} M_{n_k}$ for some m. A tracial state on $\mathcal{M}$ is then a weighted sum on Tr_{n_k}:

$$\tau(A_1 \oplus \cdots \oplus A_m) = w_1 \,\mathrm{Tr}_{n_1}(A_1) + \cdots + w_m \,\mathrm{Tr}_{n_m}(A_m), \tag{4.1.6}$$

where $w_1 + \cdots + w_m = 1$ is a weighted probability distribution.

Consider the C*-model where the C*-algebra $\mathcal{A}$ is the set of bounded operators on a Hilbert space $\mathcal{H}$. A state $s : \mathcal{A} \to \mathbb{C}$ can be defined in terms of either a pure state $|\psi\rangle \in \mathcal{H} : \| |\psi\rangle \|^2 = 1$ as $s(X) = \langle\psi| X |\psi\rangle$, or a density operator[2] $\rho \in \mathbb{B}(\mathcal{H}) : \rho \geq 0, \mathrm{Tr}(\rho) = 1$ as $s(X) = \mathrm{Tr}(\rho X)$. In fact, the Hilbert space model can be seen as a representation of the C*-model, as we will see in the discussion about the GNS construction later.

[2]A density operator ρ is a positive bounded operator that has trace 1. While not every bounded operator has a trace, we only consider operators with a trace here.

The most general form of measurement operator in the Hilbert space model is the positive operator-valued measure or POVM. We define the measurement operators in the C*-model in a similar manner.

Definition 4.12 (Measurements)**.** *Let $\mathcal{A}$ be a C*-algebra describing a quantum system* Q*. Let Σ be an alphabet. $\{E_i\}_{i\in\Sigma} \subset \mathcal{A}$ is a POVM in $\mathcal{A}$ if for all i, $E_i \geq 0$, and $\sum_i E_i = \mathcal{I}$.*

The set of POVMs of $\mathcal{A}$ gives all the measurement operators for Q. We discuss the details of measurements in a later section.

4.1.4 Evolution in the C*-model

The Hilbert space model is typically considered under Schrödinger's picture, where the evolution of the system is based on the evolution of states. However, in the C*-model, while it is possible to consider the evolution of states, it is more natural to use Heisenberg's picture, where the evolution acts on the operators.

Definition 4.13 (Evolution)**.** *Let $\mathcal{A}$ be a C*-algebra describing a quantum system* Q*. Then, the set of evolution on* Q *is the set of $*$-automorphisms in $\mathcal{A}$.*

Given a state $s : \mathcal{A} \to \mathbb{C}$, and a $*$-automorphism $\alpha : \mathcal{A} \to \mathcal{A}$, the evolved state $s' : \mathcal{A} \to \mathbb{C}$ is defined as

$$s'(a) = s(\alpha(a)). \tag{4.1.7}$$

We check that s' is indeed a state. Because $*$-automorphisms preserve the multiplicative identity, $s'(\mathcal{I}) = s(\mathcal{I}) = 1$; moreover, $\alpha(a) \geq 0 \iff a \geq 0$ so s' is positive.

We note that some automorphisms are inner, but not all of them can be described this way. Nevertheless, we can use common techniques from quantum information to show that, as a weaker version of the Skolem-Noether theorem, all $*$-automorphisms on full finite-dimensional matrices are inner.

Theorem 4.2. *Let $\mathcal{M}_n = \mathbb{C}^n \otimes \mathbb{C}^n$ be the set of all $n \times n$ complex matrices. Let $\alpha : \mathcal{M}_n \to \mathcal{M}_n$ be a $*$-automorphism. There exists a unitary $U \in \mathcal{M}_n$ such that for all $X \in \mathcal{M}_n$,*

$$\alpha(X) = UXU^*. \tag{4.1.8}$$

Proof. Let $\mathcal{H}$ be a n-dimensional Hilbert space so $\mathbb{B}(\mathcal{H}) = \mathcal{M}_n$. Let $\{|i\rangle\}$ be the computational basis of $\mathcal{H}$. We will show that for all i, there exists a state $|\psi_i\rangle \in \mathcal{H}$ where $\alpha(|i\rangle\langle i|) = |\psi_i\rangle\langle\psi_i|$. Let $U = \sum_{i=0}^{n-1} |\psi_i\rangle\langle i|$, then U is a unitary and $\alpha(X) = UXU^*$ for all $X \in \mathcal{M}_n$

We start by proving $\mathrm{Tr}(X) = \mathrm{Tr}(\alpha(X))$. Let $E_{i,j} = |i\rangle\langle j|$ for $i, j \in \{1, \cdots, n\}$. If $i \neq j$, for any k,

$$\mathrm{Tr}(\alpha(E_{i,j})) = \mathrm{Tr}(\alpha(E_{i,k})\alpha(E_{k,j})) = \mathrm{Tr}(\alpha(E_{k,j})\alpha(E_{i,k})) = \mathrm{Tr}(\alpha(E_{k,j}E_{i,k})) = 0. \tag{4.1.9}$$

The diagonal entries are all equal: for any i, j,

$$\mathrm{Tr}(\alpha(E_{i,i})) = \mathrm{Tr}(\alpha(E_{i,j}E_{j,i})) = \mathrm{Tr}(\alpha(E_{j,i}E_{i,j})) = \mathrm{Tr}(\alpha(E_{j,j})). \tag{4.1.10}$$

Furthermore, we know that $\mathrm{Tr}(\alpha(\mathcal{I})) = \mathrm{Tr}(\mathcal{I}) = n$, which gives us $\mathrm{Tr}(\alpha(E_{i,i})) = 1$.

Let $x_{i,j} = \langle i| X |j\rangle$ be the (i,j)-th entry of X, then

$$\mathrm{Tr}(\alpha(X)) = \mathrm{Tr}(\alpha(\sum_{i,j} x_{i,j}E_{i,j})) = \sum_{i,j} x_{i,j}\,\mathrm{Tr}(\alpha(E_{i,j})) = \sum_i x_{i,i} = \mathrm{Tr}(X). \tag{4.1.11}$$

Let $\rho_i = \alpha(E_{i,i})$. ρ_i is a density operator: $\rho_i = \rho_i^* \rho_i$ so $\rho_i \geq 0$, and $\mathrm{Tr}(\rho_i) = 1$

Since $\rho_i^2 = \rho_i$, ρ_i is a pure state. Let $|\psi_i\rangle \in \mathcal{H}$ be a state such that $\rho_i = |\psi_i\rangle \langle\psi_i|$ ($|\psi_i\rangle$ is unique up to a phase and can be found explicitly).

The set $\{|\psi_i\rangle\}_{i\in\{1,\cdots,n\}}$ forms an orthonormal basis: for $i \neq j$,

$$|\langle\psi_i|\psi_j\rangle|^2 = \mathrm{Tr}(\rho_i\rho_j) = \mathrm{Tr}(\alpha(E_{i,i}E_{j,j})) = 0.$$

Next we show that we can write $\alpha(E_{ij}) = |\psi_i\rangle\langle\psi_j|$. Since $\{|\psi_i\rangle\}$ form a basis, we can write $\alpha(E_{ij}) = \sum_{k,l} \beta_{k,l} |\psi_k\rangle\langle\psi_l|$ for some $\beta_{k,l}$. ($\beta_{i,i} = 1$) Then

$$\alpha(E_{ij}) = \alpha(E_{ii}E_{ij}E_{jj}) = |\psi_i\rangle\langle\psi_i|\alpha(E_{ij})|\psi_j\rangle\langle\psi_j| = \beta_{i,j}|\psi_i\rangle\langle\psi_j|.$$

We also know that $\alpha(E_{ij}E_{ij}^*) = \alpha(E_{ii})$ so $|\beta_{i,j}|^2 = 1$. Recall that $|\psi_i\rangle$ is unique up to a phase. We redefine $\{|\psi_i\rangle\}_{i\geq 2}$ by incorporating the phase $\beta_{i,j}$ in the following sense.

$$\alpha(E_{1,j}) = |\psi_1\rangle\langle\psi_j|.$$

Then all the phases vanish and we get

$$\alpha(E_{ij}) = \alpha(E_{i1}E_{1j}) = |\psi_i\rangle\langle\psi_j|.$$

The operator U, defined by $U := \sum_i |\psi_i\rangle\langle i|$ is therefore a unitary. To show that U is the correct unitary for the $*$-automorphism, we show that $X = U^*\alpha(X)U$ entrywise. For all i, j,

$$\langle i|U^*\alpha(X)U|j\rangle = \langle\psi_i|\alpha(X)|\psi_j\rangle = \mathrm{Tr}(\alpha(X)|\psi_j\rangle\langle\psi_i|) = \mathrm{Tr}(\alpha(X)\alpha(E_{j,i})) \quad (4.1.12)$$

$$= \mathrm{Tr}(\alpha(XE_{j,i})) = \mathrm{Tr}(XE_{j,i}) = \langle i|X|j\rangle = x_{i,j}. \quad (4.1.13)$$

This concludes the proof that there exists a unitary $U \in \mathcal{M}_n$ satisfying $\alpha(X) = UXU^*$ for all X. □

With measurements, states, and evolution defined, the C*-model can be used to describe the basic aspects of quantum systems.

4.1.5 Paulis as Example of an Abstract C*-algebra

We give an example of an abstractly defined C*-algebra that corresponds to very familiar objects: the 2×2 Pauli Matrices.

Example 4.2. Consider the C*-algebra $\mathcal{P}$ formed by linear combinations of $\{X, Y, Z, \mathcal{I}\}$, satisfying

- $X = X^*$, $Y = Y^*$, and $Z = Z^*$,
- $X^2 = Y^2 = Z^2 = \mathcal{I}$,
- $XY = -iZ$.

From the above relations, one can also deduce that any of the two $\{X, Y, Z\}$ anti-commute:

$$YX = (XY)^* = (-iZ)^* = iZ = -XY \tag{4.1.14}$$

$$XZ = X(iXY) = iY = -(iY)^* = -(XZ)^* = -ZX \tag{4.1.15}$$

$$ZY = (iXY)Y = iX = -(iX)^* = -(ZY)^* = -YZ. \tag{4.1.16}$$

For any $a \in \mathcal{P}$, one can write $a = a_0\mathcal{I} + a_1X + a_2Y + a_3Z$ for some $a_i \in \mathbb{C}$. To finish the definition, let the norm of a be

$$\|a\| = |a_0| + \sqrt{|a_1|^2 + |a_2|^2 + |a_3|^2}. \tag{4.1.17}$$

As one might have already noticed, while $\mathcal{P}$ is defined abstractly, it has a very familiar faithful representation: the set of bounded operators acting on a single qubit, where X, Y, and Z are represented by single-qubit Pauli matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ respectively. The norm on $\mathcal{P}$ is equivalent to the operator norm on 2×2 matrices.

By considering $\mathcal{P}$ as the abstraction of 2×2 matrices, one can consider any abstract state s on $\mathcal{P}$ as the abstraction of some one qubit states $|\psi\rangle$. For $a \in \mathcal{P}$, let M_a be the 2×2 matrix representing a with the aforementioned Pauli representation. Then, for any one qubit state $|\psi\rangle$, the corresponding abstract state s_ψ is defined as $s : \mathcal{P} \to \mathbb{C}$,

$$s_\psi(a) = \langle\psi| M_a |\psi\rangle . \tag{4.1.18}$$

Since $\mathcal{I}, X, Y$ and Z form the basis of $\mathcal{P}$, by linearity, to define a state s, it is sufficient to define it over its action on X, Y, and Z ($s(\mathcal{I}) = 1$ is always fixed). For example, the state s_0 corresponding to $|0\rangle$ is defined by

$$s_0(X) = \langle 0| X |0\rangle = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = 0 \tag{4.1.19}$$

$$s_0(Y) = \langle 0| Y |0\rangle = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = 0 \tag{4.1.20}$$

$$s_0(Z) = \langle 0| Z |0\rangle = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = 1. \tag{4.1.21}$$

By Theorem 4.2, all the $*$-automorphisms on $\mathcal{P}$ are inner-automorphisms, and therefore can be expressed in terms of conjugation by unitaries $u \in \mathcal{P}$, $uu^* = u^*u = \mathcal{I}$. These unitaries are precisely the set of unitary evolutions on one-qubit systems.

4.2 Combination of local systems in C*-model

The next part of this section focuses on defining the combination of local quantum systems using the C*-model, which is also the motivation for considering the C*-model.

4.2.1 Tensor product of C*-algebras

Under the tensor product of the Hilbert spaces model, combining two local quantum systems can be achieved by taking the tensor product of the corresponding Hilbert spaces.

Let Q be a quantum system consisting of local subsystems $\{\mathsf{Q}_1, \cdots, \mathsf{Q}_n\}$, and write $\mathsf{Q} = \{\mathsf{Q}_1, \cdots, \mathsf{Q}_n\}$. The model used to describe Q needs a method to combine the subsystems in a natural way. In particular, the following conditions should be satisfied.

1. Each local system Q_i can be described individually.
2. Any subset of the local systems $S \subseteq \{1, \cdots n\}$ can be combined to form a larger quantum system $\mathsf{Q}_S = \{\mathsf{Q}_i\}_{i \in S}$
3. If $S, T \subseteq \{1, \cdots, n\}$ and $S \cap T = \emptyset$, then combining Q_S with Q_T gives $\mathsf{Q}_{S \cup T}$.

The above rules ensure that the local systems can be combined to form a larger quantum system in a consistent manner.

In the Hilbert space model, the tensor product framework achieves the above conditions by defining the combination of two local systems as the tensor product

of their corresponding Hilbert spaces. Under the commuting operator framework, the Hilbert spaces remain unchanged, and combining two subsystems is achieved by combining the set of operators of the two systems and taking the closure.

In the C*-model, we define the combination of two local systems using the tensor product of their corresponding C*-algebras.

Definition 4.14 (Combination of local systems)**.** *Let $\mathcal{A}_1, \mathcal{A}_2$ be the C*-algebra for two local quantum systems Q_1, Q_2. The C*-algebra for the quantum system combining Q_1 and Q_2 is $\mathcal{A}_1 \otimes \mathcal{A}_2$.*

To understand the above definition, we need to take a closer look at what the tensor product of C*-algebra means exactly. Let $\mathcal{A}$, $\mathcal{B}$ be two C*-algebras. Let $\mathcal{A} \otimes \mathcal{B}$ be their algebraic tensor product: for any $x = \sum_i a_i \otimes b_i$ and $y = \sum_j c_j \otimes d_j$,

$$xy = \sum_{i,j} a_i c_j \otimes b_i d_j \tag{4.2.1}$$

and

$$x^* = \sum_i a_i^* \otimes b_i^*. \tag{4.2.2}$$

$\mathcal{A} \otimes \mathcal{B}$ is a *-algebra. In order to make it into a C*-algebra, a norm needs to be defined so that $\mathcal{A} \otimes \mathcal{B}$ can be completed in the norm.

Definition 4.15 (Min and Max Norm)**.** *Let $x \in \mathcal{A} \otimes \mathcal{B}$. Then $\|x\|_{\max}$ and $\|x\|_{\min}$ are defined as the following:*

$$\|x\|_{\max} = \sup\{\|\pi(x)\| \colon \pi \colon \mathcal{A} \otimes \mathcal{B} \to \mathbb{B}(\mathcal{H}) \text{ is a *-homomorpihsm}\}. \tag{4.2.3}$$

*Let $\pi_1 \colon \mathcal{A} \to \mathbb{B}(\mathcal{H})$ and $\pi_2 \colon \mathcal{B} \to \mathbb{B}(\mathcal{H})$ be *-homomorphisms. Define $\pi_1 \otimes \pi_2 \colon \mathcal{A} \otimes$*

$\mathcal{B} \to \mathbb{B}(\mathcal{H} \otimes \mathcal{H})$, *to be* $(\pi_1 \otimes \pi_2)(a \otimes b) = \pi_1(a) \otimes \pi_2(b)$. *Then,*

$$\|x\|_{\min} = \sup\{\|(\pi_1 \otimes \pi_2)(x)\| : \pi_1 : \mathcal{A} \to \mathbb{B}(\mathcal{H}), \pi_2 : \mathcal{B} \to \mathbb{B}(\mathcal{H}) \text{ are } *\text{-homomorphisms}\}. \tag{4.2.4}$$

Any C*-norm on $\mathcal{A} \otimes \mathcal{B}$ lies in between these two norms, and therefore the name min and max norm. With the two norms defined, we can now define the min and max tensor product of C*-algebras.

Definition 4.16 (Min and Max tensor product)**.** *The completion of* $\mathcal{A} \otimes \mathcal{B}$ *by the norm* $\|x\|_{\min}$ *is a C*-algebra denoted by* $\mathcal{A} \otimes_{\min} \mathcal{B}$*, and the completion of* $\mathcal{A} \otimes \mathcal{B}$ *by the norm* $\|x\|_{\max}$ *is denoted by* $\mathcal{A} \otimes_{\max} \mathcal{B}$*.*

In some cases, the min and max tensor products of C*-algebras are identical. In general, they may not be equal. As a result, in our definition of the combined local systems, we often do not specify which tensor product to use, so that it can be determined case by case based on the application.

Moreover, while the min tensor product of C*-algebras is defined by the norm of the tensor product of two *-homomorphisms, its representation might not be a tensor product of operators on two Hilbert spaces. We will discuss this more in detail in Chapter 6.

4.2.2 Combined States and Entanglement

One of the advantages of the tensor product framework over the commuting operator framework is that given a state on a combined system, the state of each subsystem can be found easily by taking the partial trace to trace out the other subsystems. In

the C*-model, the state on a subsystem can be defined in a similar fashion using the partial trace.

Definition 4.17 (Partial trace on states)**.** *Let $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, and $s : \mathcal{A} \to \mathbb{C}$ be a state. Taking partial trace on s to trace out $\mathcal{A}_2$ results in a state $s_1 : \mathcal{A}_1 \to \mathbb{C}$ defined by*

$$s_1(a_1) = s(a_1 \otimes \mathcal{I}). \tag{4.2.5}$$

We also denote the partial trace as $\mathrm{Tr}_{\mathcal{A}_2} : (\mathcal{A}_1 \otimes \mathcal{A}_2 \to \mathbb{C}) \to (\mathcal{A}_1 \to \mathbb{C})$, so

$$(\mathrm{Tr}_{\mathcal{A}_2}(s))(a_1) = s_1(a_1). \tag{4.2.6}$$

Given local states on two local systems, it is easy to combine the two states into a state in the larger system by taking the tensor product between them.

Definition 4.18 (Tensor product of states)**.** *Let $s_1 : \mathcal{A}_1 \to \mathbb{C}$ and $s_2 : \mathcal{A}_2 \to \mathbb{C}$ be two abstract states. Then the combined state $s_1 \otimes s_2 : \mathcal{A}_1 \otimes A_2 \to \mathbb{C}$ is defined as*

$$(s_1 \otimes s_2)(a_1 \otimes a_2) = s_1(a_1)s_2(a_2) \tag{4.2.7}$$

for all $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$.

If $s : \mathcal{A}_1 \otimes \mathcal{A}_2 \to \mathbb{C}$ can be written as $s = s_1 \otimes s_2$, then s is a product state.

The above definition is in fact a state on any $\mathcal{A}_1 \otimes \mathcal{A}_2$. It is trivial that $s(1) = (s_1 \otimes s_2)(1 \otimes 1) = 1$. We show that s is indeed positive. Let $\mathcal{H}_1, |\psi\rangle_1, \pi_1 : \mathcal{A}_1 \to \mathbb{B}(\mathcal{H}_1)$ be the GNS representation[3] of $\mathcal{A}_1$ and s_1, $\mathcal{H}_2, |\psi_2\rangle, \pi_2 : \mathcal{A}_2 \to \mathbb{B}(\mathcal{H}_2)$ be the GNS representation of $\mathcal{A}_2$ and s_2. Then $\mathcal{H}_1 \otimes \mathcal{H}_2$, $\pi = \pi_1 \otimes \pi_2$, and $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ forms a

[3]We defer the discussion of GNS representation theorem to Section 4.3.2.

representation of $\mathcal{A}_1 \otimes \mathcal{A}_2$ and s where $s(a) = \langle\psi| \pi(a) |\psi\rangle$ for all $a \in \mathcal{A}_1 \otimes \mathcal{A}_2$. Since $*$-homomorphism preserves positivity, for any $a \geq 0$, $\pi(a) \geq 0$ so $s(a) = \langle\psi| \pi(a) |\psi\rangle \geq 0$.

We only need to define the state on all operators of the form $a_1 \otimes a_2$, since the value of the state on all the other operators can be determined based on linearity and continuity.

Having defined product states, it is possible to define separable states in a way that is similar to separable states in the tensor product framework.

Definition 4.19 (Separable states)**.** *Let $s : \mathcal{A}_1 \otimes \mathcal{A}_2 \to \mathbb{C}$ be a state. s is a separable state if and only if s can be written as a convex combination of product states.*

$$s = \sum_i p_i (r_i \otimes t_i), \tag{4.2.8}$$

where $\{p_i\}$ is a probability distribution, $r_i : \mathcal{A}_1 \to \mathbb{C}$ and $t_i : \mathcal{A}_2 \to \mathbb{C}$ are states.

Entanglement can also be defined.

Definition 4.20 (Entangled states)**.** *Let $s : \mathcal{A}_1 \otimes \mathcal{A}_2 \to \mathbb{C}$ be a state. s is entangled if and only if s is not separable.*

While it is easy to define what entangled states are, it is not clear what is the best way to measure the amount of entanglement a state has, since in many cases, an abstract state can have an infinite amount of entanglement. Nevertheless, it is possible to define whether a state is maximally entangled.

Definition 4.21 (Maximally entangled states)**.** *A state $s : \mathcal{A}_1 \otimes \mathcal{A}_2 \to \mathbb{C}$ is called maximally entangled if s is pure, and $\mathrm{Tr}_{\mathcal{A}_1}(s)$ and $\mathrm{Tr}_{\mathcal{A}_2}(s)$ are tracial.*

Note that the set of states is a convex set. A state is called pure if it is an extreme point of this set. We defer the discussions on the details of pure states to a later section because it involves using the GNS construction which has not been introduced yet.

This definition of a maximally entangled state is compatible with the definition of maximally entangled states in the tensor product model. In the tensor product model, a state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is maximally entangled if its Schmidt coefficients are the same over all Schmidt basis. In other words, if we trace out $\mathcal{H}_i$ from $|\psi\rangle$, we will end up with a maximally mixed state, which corresponds to the tracial state in the C*-model.

4.2.3 Local Evolutions and Measurements

Having defined states on the tensor product of C*-algebras, we now consider what local operators and measurements are in the C*model. In particular, given some quantum systems $\{\mathsf{Q}_1, \cdots \mathsf{Q}_n\}$ described by C*-algebras $\{\mathcal{A}_1, \cdots, \mathcal{A}_n\}$, how to describe local measurements and evolutions on a subset of the quantum systems. Recall that in the commuting operator model, defining local operators relative to local quantum systems was not a straightforward task. It turns out that, fortunately, the definitions in the C*-model are relatively simple.

The overall combined C*-algebra is $\mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_n$. For a single quantum system Q_i, the local evolution on Q_i is simply the set of evolution on $\mathcal{A}_i$ and identity on all other C*-algebras. In other words, it is the set of $*$-automorphisms $\alpha_i : \mathcal{A}_i \to \mathcal{A}_i$ tensor product with identity: $\mathcal{I}_1 \otimes \cdots \otimes \alpha_i \otimes \cdots \otimes \mathcal{I}_n$. Similarly, the local measurement on Q_i is simply the measurement operators on $\mathcal{A}_i$ tensor product with identity everywhere

else.

For a subset of local systems, we take the tensor product of their corresponding C*-algebra as the C*-algebra of the combined system and use the corresponding local evolution operators and measurements on the combined C*-algebra. For example, the local system containing Q_1 and Q_2 is described by $\mathcal{A}_{1,2} = \mathcal{A}_1 \otimes \mathcal{A}_2$. The local evolutions are therefore the $*$-automorphisms on $\mathcal{A}_{1,2}$.

4.3 Equivalences between the Hilbert space and C*-model

As mentioned in the previous section, the C*-model is an abstraction of the Hilbert space model. This section will discuss the correspondences between the two models.

It turns out that the two models can be converted to each other in a standard manner.

4.3.1 Hilbert Space to C*-Model

The Hilbert space model and the C*-model are equivalent in the sense that they can be converted to each other to describe the same quantum system. The conversion from the Hilbert space model to the C*-model is straightforward.

Theorem 4.3. *Given a Hilbert space $\mathcal{H}$, there exists a C*-algebra $\mathcal{A}$, and a $*$-isomorphism $\pi : \mathbb{B}(\mathcal{H}) \to \mathcal{A}$ such that for all $M \in \mathbb{B}(\mathcal{H})$, for all unit vector $|\psi\rangle \in \mathcal{H}$, there exists a state $s : \mathcal{A} \to \mathbb{B}$ where $\langle\psi| M |\psi\rangle = s(\pi(M))$.*

Proof. The proof is straightforward. Define $\mathcal{A} = \mathbb{B}(\mathcal{H})$, and for each $|\psi\rangle \in \mathcal{H}$, $a \in \mathbb{B}(\mathcal{H})$, define $s_{|\psi\rangle}(a) = \langle\psi| a |\psi\rangle$. □

The above conversion will map any Hilbert space model into the C*-model. However, for combined systems such as the commuting operator model, the converted C*-algebra will not have the structure of the localized tensor product. It turns out that the commuting operator model can be converted into the max tensor product of C*-model in the following sense.

Theorem 4.4. *Let $\mathcal{H}$ be a Hilbert space and $\mathbf{A}, \mathbf{B}$ be two mutually commuting sets of operators that are algebraically closed under the operator norm. Then there exists two C*-algebras $\mathcal{A}, \mathcal{B}$ with a $*$-homomorphism $\pi : \mathcal{A} \otimes_{\max} \mathcal{B} \to \mathbb{B}(\mathcal{H})$ where for all $a \in \mathbf{A}, b \in \mathbf{B}$, $\pi(a \otimes \mathcal{I}) \in \mathbf{A}$ and $\pi(\mathcal{I} \otimes b) \in \mathbf{B}$.*

Proof. Let $\mathcal{A}, \mathcal{B}$ be the C*-algebra of the presentation of $\mathbf{A}$ and $\mathbf{B}$. Then $\mathcal{A} \otimes_{\max} \mathcal{B}$ is a C*-algebra where $\mathcal{A} \otimes \mathcal{I}$ and $\mathcal{I} \otimes \mathcal{B}$ is also a presentation of $\mathbf{A}$ and $\mathbf{B}$. This gives a $*$-homomorphism π that maps the presentation $\mathcal{A} \otimes \mathcal{I}$ and $\mathcal{I} \otimes \mathcal{B}$ to the representation $\mathbf{A}$ and $\mathbf{B}$.

It is easy to see that since $\mathcal{A} \otimes \mathcal{I}$ commutes with $\mathcal{I} \otimes \mathcal{B}$, $\pi(\mathcal{A} \otimes \mathcal{I})$ commutes with $\pi(\mathcal{I} \otimes \mathcal{B})$, which match with the fact that $\mathbf{A}$ commutes with $\mathbf{B}$. □

The max tensor product is required here because there is a single $*$-homomorphism π maps $\mathcal{A} \otimes_{\max} \mathcal{B}$ to a single $\mathbb{B}(\mathcal{H})$.

4.3.2 C* to Hilbert Space: The GNS Construction

While going from Hilbert space to abstract C*-algebra is straightforward, the converse is less obvious. To convert abstract C*-algebras to operators on Hilbert spaces, we

invoke the Gelfand-Naimark-Segal (GNS) theorem.

Theorem 4.5 (Gelfand-Naimark-Segal)**.** *Let $\mathcal{A}$ be an abstract C*-algebra. Then there is a Hilbert space $\mathcal{H}$ and a map $\pi : \mathcal{A} \to \mathbb{B}(\mathcal{H})$ such that*

- *π is a $*$-homomorphism,*
- *$\|\pi(x)\| = \|x\|$ for all $x \in \mathcal{A}$.*

Moreover, if $\mathcal{A}$ is unital, then it is possible to arrange that $\pi(1) = \mathcal{I}_{\mathcal{H}}$.

The two conditions above ensure that $\pi(\mathcal{A})$ is a C*-algebra of operators. If a state is defined, the GNS representation theorem on states will give a representation of the state in addition to the Hilbert space and $*$-homomorphism.

Theorem 4.6 (GNS State Representation Theorem)**.** *Let $\mathcal{A}$ be a C*-algebra, and $s : \mathcal{A} \to \mathbb{C}$ be a state. Then there exists a Hilbert space $\mathcal{H}$, a $*$-homomorphism $\pi : \mathcal{A} \to \mathbb{B}(\mathcal{H})$, and a unit vector $|\psi\rangle \in \mathcal{H}$ such that for all $a \in \mathcal{A}$, $s(a) = \langle\psi| \pi(a) |\psi\rangle$. Moreover, $\{\pi(\mathcal{A}) |\psi\rangle\}$ is dense in $\mathcal{H}$.*

Proof. Let $\mathcal{A}_s := \{a \in \mathcal{A}, s(a^*a) = 0\}$. $\mathcal{A}_s$ is a left ideal of $\mathcal{A}$. We define the quotient space of $\mathcal{A}$ by $\mathcal{A}_s$ as $\tilde{\mathcal{A}} = \mathcal{A}/\mathcal{A}_s$. Elements of $\tilde{\mathcal{A}}$ are of the form $a + I$ where I is from the left ideal $\mathcal{A}_s$ of $\mathcal{A}$.

Elements of $\tilde{\mathcal{A}}$ form a vector space, and to get a Hilbert space, we define the following inner product to take the norm of the vectors in:

$$\langle a + I, b + I\rangle = s(a^*b), \quad \forall a, b \in \mathcal{A}. \tag{4.3.1}$$

Let $\mathcal{H}$ be the Hilbert space formed by elements of $\tilde{\mathcal{A}}$ completed by the inner product defined above.

Define the $*$-homomorphism $\pi : \mathcal{A} \to \mathbb{B}(\mathcal{H})$ as

$$\pi(a)(b + I) = ab + I, \tag{4.3.2}$$

and let $|\psi\rangle = 1 + I = \mathcal{I} \in \tilde{\mathcal{A}}$. (The identity element exists because we only consider unital C*-algebras. There are walk-arounds for non-unital C*-algebras which we will omit the details here.) Then we have what we desired:

$$\langle\psi| \pi(a) |\psi\rangle = s(\mathcal{I}a\mathcal{I}) = s(a). \tag{4.3.3}$$

It is also clear that since $|\psi\rangle = \mathcal{I}$, $\pi(a) |\psi\rangle = a + I$ so $\pi(\mathcal{A}) |\psi\rangle$ gives every element of $\tilde{\mathcal{A}}$, which is dense in $\mathcal{H}$. □

The above equivalence relations between the two model means that they have measurements and states that can give the same measurement outcomes. The missing part is the equivalence between the evolutions in the two models. We consider the evolution in the Hilbert space model to be unitaries on the Hilbert space since any channel has a Stinespring form that is unitary in a larger Hilbert space.

Since conjugation by unitary in a C*-algebra is a$*$-automorphism, the conversion from unitary in the Hilbert space to $*$-automorphism on the corresponding C*-algebra is trivial.

Let $\mathcal{H}$ be a Hilbert space, $\mathcal{A}$ be a C*-algebra, and $\pi : \mathbb{B}(\mathcal{H}) \to \mathcal{A}$ be a $*$-isomorphism. For all unitary $U \in \mathbb{B}(\mathcal{H})$, $UU^* = U^*U = \mathcal{I}$, the corresponding $*$-automorphism $\alpha_U : \mathcal{A} \to \mathcal{A}$ is $\alpha_U(\pi(X)) = \pi(UXU^*)$.

While all conjugation by unitaries is $*$-automorphisms, the converse is not necessarily true. Let $\alpha : \mathcal{A} \to \mathcal{A}$ be a $*$-automorphism that cannot be expressed in terms of $\alpha(a) = uau^*$, where $u \in \mathcal{A}$ is a unitary. In order to convert α into a unitary in

the Hilbert space model, the C*-algebra needs to be extended before performing the GNS construction. More details of this extension can be found in the book of [25] in the chapter that discusses cross products.

Proposition 4.7. *Assume $u \notin \mathcal{A}$. Let $\mathcal{A}_\alpha$ be the C*-algebra that contains $\mathcal{A}$ as a subalgebra and is generated by $\mathcal{A}$ and one extra element u, such that $\alpha(a) = uau^*$ for all $a \in \mathcal{A}$, and $uu^* = u^*u = \mathcal{I}$. Then for all $b \in \mathcal{A}_\alpha$, there exists some $a_i \in \mathcal{A}$, $n_i \in \mathbb{Z}$, and $\beta_i \in \mathbb{C}$ such that $b = \sum_i \beta_i a_i u^{n_i}$.*

Proof. We start by showing that the left multiplication of u or u^* to an element of $\mathcal{A}$ is equal to the right multiplication of u or u^* of another element of $\mathcal{A}$.

For any $x \in \mathcal{A}$, $ux = yu$ where $y = uxu^* = \alpha(x) \in \mathcal{A}$, and similarly, $u^*x = y^*u^*$ where $y^* = u^*xu = \alpha(x)^* \in \mathcal{A}$.

Since $\mathcal{A}_\alpha$ is the extension of $\mathcal{A}$ with u, any element $b \in \mathcal{A}$ can be written as a product of some sequence of u, u^*, and some $a \in \mathcal{A}$. By the property shown above, all the u and u^* in b can be moved to the right to give the expression of the form $b = au^n$ for some $n \in \mathbb{Z}$. (Since u is unitary, $u^{-1} = u^*$.) □

Before applying GNS on the extended C*-algebra $\mathcal{A}_\alpha$, we need to extend the state $s : \mathcal{A} \to \mathbb{C}$ to act on the extended algebra $s_\alpha : \mathcal{A}_\alpha \to \mathbb{C}$. The extension exists by Hahn Banach theorem, and in many cases, it is possible to simply define the extension as $s_\alpha(au^n) = 0$ for $a \in \mathcal{A}$, $n \neq 0$. This type of extension is called the canonical extension, and in general, there are many other possible extensions given by the Hahn-Banach theorem. We provide the statement of the Hahn Banach theorem below and omit the proof.

Theorem 4.8 (Hahn-Banach extension theorem)**.** *Let X be a normed linear space over $\mathbb{F}$, let $Y \subseteq X$ be a subspace, and let $f : Y \to \mathbb{F}$ be a bounded linear functional. Then there exists an extension $g : X \to \mathbb{F}$ that is also a bounded linear functional and satisfies $\|g\| = \|f\|$.*

Applying the GNS construction on $\mathcal{A}_\alpha$ and s_α gives a Hilbert space $\mathcal{H}$, a state $|\psi\rangle \in \mathcal{H}$, and a $*$-homomorphism $\pi : \mathcal{A}_\alpha \to \mathbb{B}(\mathcal{H})$ such that $s(a) = \langle\psi| \pi(a) |\psi\rangle$ for all $a \in \mathcal{A}_\alpha$.

We note that by Hahn-Banach theorem, when s is extended to s_α on $\mathcal{A}_\alpha$, s_α is also a state because the extension preserves the norm where $\|s_\alpha\| = 1$ and $s_\alpha(\mathcal{I}) = 1$ are still satisfied.[4]

If there are more than one $*$-automorphisms used that cannot be expressed in terms of conjugation by unitaries in $\mathcal{A}$, then $\mathcal{A}_\alpha$ needs to be the extension of $\mathcal{A}$ that includes the unitaries for each of the $*$-automorphisms.

So far, the equivalence between the C*-model and the Hilbert space model is based on some abstract state s. As a result, only a subset of the states in the C*-algebra has their corresponding states in the Hilbert space model. More precisely, we call these states the set of states affiliated with s.

Definition 4.22. *Given a C*-algebra $\mathcal{A}$, and a state $s : \mathcal{A} \to \mathbb{C}$, a state s' is called affiliated with s if and only if there exists $u \in \mathcal{A}$ such that for all $a \in \mathcal{A}$, $s'(a) = s(uau^*)$.*

Given a C*-algebra, not all states are affiliated with each other. If we want the equivalence relation to hold for all states in the C*-algebra, a more general version of

[4] It is shown in [9] and [23] that if $s(\mathcal{I}) = 1$ then $\|s\| = 1$ if and only if $s \geq 0$.

the GNS construction can be used. In particular, given a C*-algebra $\mathcal{A}$, if two states $s, t : \mathcal{A} \to \mathbb{C}$ are not affiliated with each other, it is possible to apply GNS on s and on t separately to get two Hilbert spaces $\mathcal{H}_s$ and $\mathcal{H}_t$, and define the overall Hilbert space to be $\mathcal{H} = \mathcal{H}_s \oplus \mathcal{H}_t$.[5] For $a \in \mathcal{A}$, the corresponding operator in the Hilbert space is then $\pi(a) = \pi_s(a) \oplus \pi_t(a)$, where π_s and π_t are the $*$-homomorphisms from the individual GNS constructions with state s and t. In general, one could apply the GNS construction on a C*-algebra $\mathcal{A}$ directly without any states by taking the direct sum of the Hilbert space from applying GNS on all the states that are not affiliated with each other. The resulting Hilbert space model will be equivalent to the C*-model on all possible states.

In general, there can be uncountably many states that are not affiliated with each other, so if we consider the Hilbert space that arises from applying GNS to encompass all possible states, the dimension of the Hilbert space has to be uncountable.

4.3.3 Tensor product of C*-algebra to commuting operators

As we have shown, while the C*-model can appear to be more powerful than the Hilbert space model, the two models are in fact equivalent and can be transformed into each other. However, as we will see below, when it comes to describing local quantum systems, the C*-model has a little more structure than the commonly used commuting operator model in infinite dimensions.

Given two local quantum systems Q_1 and Q_2, the combined system Q can be de-

[5] If the two states are affiliated with each other, this construction still works, but it is also possible to perform GNS on one state and get the other state in the same Hilbert space with a unitary transformation.

scribed under the tensor product of the Hilbert space model, the commuting operator model, and the tensor product of C*-model. We show that the tensor product of the Hilbert space model is a special case of the tensor product of C*-model, which is, in turn, a special case of the commuting operator model.

Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ be the Hilbert space consisting of two local quantum subsystems Q_1 described by $\mathcal{H}_1$ and Q_2 described by $\mathcal{H}_2$. Let $\mathcal{A}_1 = \mathbb{B}(\mathcal{H}_1)$ and $\mathcal{A}_2 = \mathbb{B}(\mathcal{H}_2)$. Then $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ is the C*-algebra that can be used to describes the same quantum systems under the C*-model: For each $|\psi\rangle \in \mathcal{H}$, define $s_{|\psi\rangle} : \mathcal{A} \to \mathbb{C}$ as $s_{|\psi\rangle}(X) = \langle\psi| X |\psi\rangle$.

Proposition 4.9. *Let $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ be the C*-algebra describing two local quantum systems Q_1 and Q_2. Then there exists a commuting operator model with Hilbert space $\mathcal{H}$, two sets of mutually commuting operators $\mathbf{B}_1$, $\mathbf{B}_2 \subseteq \mathbb{B}(\mathcal{H})$ that can be used to describe the same quantum system as the C*-model.*

Proof. Apply the GNS construction on $\mathcal{A}$ gives a Hilbert space $\mathcal{H}$, and a $*$-homomorphism $\pi : \mathcal{A} \to \mathbb{B}(\mathcal{H})$. Define $\mathbf{B}_1 = \{\pi(a_1 \otimes \mathcal{I}) : a_1 \in \mathcal{A}_1\}$, and $\mathbf{B}_2 = \{\pi(\mathcal{I} \otimes a_2) : a_2 \in \mathcal{A}_2\}$. Then by definition, elements of $\mathbf{B}_1$ commute with every element of $\mathbf{B}_2$. For any state $s : \mathcal{A} \to \mathbb{C}$, the GNS also gives a state $|\psi_s\rangle \in \mathcal{H}$ such that $s(a) = \langle\psi_s| \pi(a) |\psi_s\rangle$ for all $a \in \mathcal{A}$. □

One of the key properties of this relation is that since the GNS construction is applied to the overall C*-algebra, the $*$-homomorphism does not necessarily have the tensor product structure. As a result, the resulting operators could only preserve the commutativity between them.

4.4 More Properties of C*-Model in Quantum Information

Equipped with the GNS theorem, we are able to discuss more properties of the C*-model that are useful for quantum information theory.

4.4.1 More about States

Given a quantum state, it is natural to ask whether the state is pure or not. In the Hilbert space model, a pure state is an extreme point on a convex set of states. The pureness of an abstract state is defined similarly.

Definition 4.23 (Pure states)**.** *A state $s : \mathcal{A} \to \mathbb{C}$ is pure if it cannot be expressed as a convex combination of other states.*

While the above is a natural definition of pure states, it is not a very practical one: given a state s, it is not clear how one could use the above definition to figure out whether the state is pure or not. Alternatively,

Corollary 4.1. *Let $\mathcal{A}$ be a C*-algebra and $s : \mathcal{A} \to \mathbb{C}$ be a state. Let $\mathcal{H}_s, |\psi\rangle \in \mathcal{H}_s, \pi_s : \mathcal{A} \to \mathbb{B}(\mathcal{H}_s)$ be the GNS representation of $\mathcal{A}$ and s. Then s is pure if and only if $\pi_s(\mathcal{A})' = \mathbb{C} \cdot \mathcal{I}_{\mathcal{H}_s}$.*

Note that the commuton $\prime$ symbol means that $\mathcal{A}' = \{T \in \mathbb{B}(\mathcal{H}_s), aT = Ta,\ \forall a \in \mathcal{A}\}$.

Proof. If $\pi_s(\mathcal{A})' \neq \mathbb{C} \otimes \mathcal{I}_{\mathcal{H}_s}$, then there exists a projection $P \in \pi_s(\mathcal{A})\prime$ that is neither 0 or $\mathcal{I}_{\mathcal{H}_s}$. Let $|\psi_1\rangle = P|\psi\rangle$, and $|\psi_2\rangle = (\mathcal{I} - P)|\psi\rangle$. By the GNS representation

theorem, $\{\pi_s(\mathcal{A})\,|\psi\rangle\}$ is dense in $\mathcal{H}_s$, so $|\psi_1\rangle = 0$ or $|\psi_2\rangle = 0$ would mean $P = 0$ or $P = \mathcal{I}_{\mathcal{H}_s}$.

Let $t_i = \| \, |\psi_i\rangle \, \|^2$, and let

$$\begin{aligned} s_1(a) &= t_1^{-1} \langle\psi| P\pi_s(a)P \,|\psi\rangle = t_1^{-1} \langle\psi_1| \, \pi_s(a) \, |\psi_1\rangle \,, \\ s_2(a) &= t_2^{-1} \langle\psi| \, (\mathcal{I} - P)\pi_s(a)(\mathcal{I} - P) \, |\psi\rangle = t_2^{-1} \langle\psi_2| \, \pi_s(a) \, |\psi_2\rangle \,. \end{aligned} \tag{4.4.1}$$

Then we can write $s(a) = t_1 s_1(a) + t_2 s_2(a)$, which is not a pure state.

Next we show that if s is mixed, then $\pi_s(\mathcal{A})' \neq \mathbb{C} \cdot \mathcal{I}$. Instead of showing the full proof which can be found in [25], we omit some of the details of the proof and use some results directly from [25] our proof.

For simplicity, consider $s = t_1 s_1 + t_2 s_2$ where $t_1, t_2 > 0, t_1 + t_2 = 1$ and s_1, s_2 are different pure states. The proof can be easily extended to $s = \sum_i t_i s_i$. Consider the GNS representation $\{\pi_1, \mathcal{H}_1, |\psi_1\rangle\}$ for $\mathcal{A}$ and s_1, and $\{\pi_2, \mathcal{H}_2, |\psi_2\rangle\}$ for $\mathcal{A}$ and s_2. Let $\mathcal{H}_s := \mathcal{H}_1 \oplus \mathcal{H}_2$, $\pi_s : \mathcal{A} \to \mathcal{H}_s$ where $\pi_s(a) = \pi_1(a) \oplus \pi_2(a)$, and $|\psi\rangle = \sqrt{t_1} \, |\psi_1\rangle \oplus \sqrt{t_2} \, |\psi_2\rangle$. Then $\mathcal{H}_s, \pi_s, |\psi\rangle$ is a representation of $\mathcal{A}, s$, because

$$s(a) = \langle\psi| \, \pi_s(a) \, |\psi\rangle = t_1 \langle\psi_1| \, \pi_1(a) \, |\psi_1\rangle + t_2 \langle\psi_2| \, \pi_2(a) \, |\psi_2\rangle = t_1 s_1(a) + t_2 s_2(a). \tag{4.4.2}$$

We use the following results from [25] to show that $\{\pi_s, \mathcal{H}_s, |\psi\rangle\}$ is indeed a GNS representation of $\mathcal{A}, s$.

Lemma 4.9.1 ([25]). *Let $\mathcal{A}$ be a C^*-algebra and $s_1, s_2 : \mathcal{A} \to \mathbb{C}$ be two different pure states. Let $\{\pi_1, \mathcal{H}_1, |\psi_1\rangle\}$ and $\{\pi_2, \mathcal{H}_2, |\psi_2\rangle\}$ be the GNS representation of $\mathcal{A}, s_1$ and $\mathcal{A}, us_2$. Let $s = t_1 s_1 + t_2 s_2$ where $t_1, t_2 \geq 0$, $t_1 + t_2 = 1$, be a mixed state. Then $\{\pi_1 \oplus \pi_2, \mathcal{H}_1 \oplus \mathcal{H}_2, \sqrt{t_1} \, |\psi_1\rangle \oplus \sqrt{t_2} \, |\psi_2\rangle\}$ is a GNS representation of $\mathcal{A}, s$.*

Let P be the projection from $\mathcal{H}_s$ to $\mathcal{H}_1$ so $P \, |\psi\rangle = \sqrt{t_1} \, |\psi_1\rangle \oplus 0$. Then for all

$a \in \mathcal{A}$,

$$P\pi_s(a)\left|\psi\right\rangle = \sqrt{t_1}\pi_1(a)\left|\psi_1\right\rangle \oplus 0 = \pi_s(a)P\left|\psi\right\rangle, \tag{4.4.3}$$

which means $P \in \pi_s(\mathcal{A})'$. Since $P \neq 0$ or $\mathcal{I}_{\mathcal{H}_s}$, this gives us $\pi_s(\mathcal{A})' \neq \mathbb{C} \cdot \mathcal{I}_{\mathcal{H}_s}$. □

In the Hilbert space model, sometimes it is possible to project a state from a larger Hilbert space to a subspace. When this is done, the projected state is re-normalized. We describe what it means to project a state in the C*-model.

Definition 4.24 (Projection of states)**.** *Let $p \in \mathcal{A}$ be a projection, and let $A_p = p\mathcal{A}p := \{pap : a \in \mathcal{A}\}$. Let $\mathcal{A}_p$ be the C*-algebra generated by A_p. The projection of $s : \mathcal{A} \to \mathbb{C}$ to $s_p : \mathcal{A}_p \to \mathbb{C}$ is defined as*

$$s_p(a_p) = \begin{cases} \frac{s(a_p)}{s(p)} & s(p) \neq 0 \\ 0 & s(p) = 0 \end{cases} \tag{4.4.4}$$

for all $a_p \in \mathcal{A}_p$.

Note that in $\mathcal{A}_p = p\mathcal{A}p$, the identity element is $\mathcal{I}_{\mathcal{A}_p} = p \in \mathcal{A}$, which differs from the identity element $\mathcal{I} \in \mathcal{A}$. As a result, the re-normalization of state s' is necessary to ensure $s_p(p) = 1$.

From the Hahn-Banach theorem, given a state $s : \mathcal{A} \to \mathbb{C}$ where $\mathcal{A}$ is a subalgebra of $\mathcal{A}_p$, there exists a state $s' : \mathcal{A}' \to \mathbb{C}$ such that $s_p(a) = s(a)$ for all $a \in \mathcal{A}$. Moreover, this extension is unique. So given a projected state, it is always possible to extend it to a state acting on a larger C*-algebra.

A longstanding philosophical question regarding quantum mechanics is what happens to the quantum system after an observer performs a measurement. Do measurements change the system and cause the quantum state to collapse, or does it

cause the observer to jump into one of the many multi-worlds? While we do not plan on dwelling on the different interpretations of quantum mechanics, it is natural to consider the state of a quantum system (or universe) after performing some measurements. Under the Hilbert space model, one can describe the residual state based on the outcome of the Kraus operators for the measurement given.

Under the Hilbert space model, given a set of Krauss operators $\{E_1, \cdots, E_n\}$ where $\sum_i E_i^* E_i = \mathcal{I}$, it can be used to perform a measurement with outcome $\{1, \cdots, n\}$ on the density operator ρ of a state. The probability of obtaining outcome i is $\mathrm{Tr}(E_i \rho E_i^*)$, and the residual state σ_i is

$$\sigma_i = \frac{E_i \rho E_i^*}{\mathrm{Tr}(E_i \rho E_i^*)}. \tag{4.4.5}$$

Let $\mathcal{A}$ be a C*-algebra. Let $M = \{M_1, \cdots, M_n\} \subset \mathcal{A}$ be a set of operators that satisfy $\sum_i M_i^* M_i = \mathcal{I}$. Applying M as a measurement on abstract state $s : \mathcal{A} \to \mathbb{C}$ will yield outcome i with probability $s(M_i M_i^*)$, and the residual state $s_i : \mathcal{A} \to \mathbb{C}$ is

$$s_i(x) = \frac{s(M_i^* x M_i)}{s(M_i M_i^*)}. \tag{4.4.6}$$

It is easy to verify that s_i's are in fact abstract states. $s_i(\mathcal{I}) = \frac{s(M_i M_i^*)}{s(M_i M_i^*)} = 1$, assuming the probability of obtaining outcome i is not zero. s_i is positive because for any $x \geq 0$, $M_i x M_i^* \geq 0$ so $s_i(x) \geq 0$.

4.4.2 Norms of Operators

There are many similarities between the Hilbert space model and the C*-model for quantum information. One of the interesting relations is between the operator norm of an operator in the Hilbert space model and the norm of an element of the C*-algebra.

Recall that in the Hilbert space model, given a Hilbert space $\mathcal{H}$, the operator norm of $X \in \mathbb{B}(\mathcal{H})$ can be expressed as

$$\|X\|^2 = \sup_{|\psi\rangle \in \mathcal{H}, \||\psi\rangle\|=1} \langle\psi| X^* X |\psi\rangle .$$

While the norm for a C*-algebra can appear more abstract, using the notion of abstract state, it can be expressed in a similar form.

Theorem 4.10. *Let $\mathcal{A}$ be a C*-algebra, and $a \in \mathcal{A}$. Let $S := \{s : \mathcal{A} \to \mathbb{C} \colon s \geq 0, s(\mathcal{I}) = 1\}$ be the set of all abstract states.*

$$\|a\|^2 = \sup_{s \in S} s(aa^*).$$

Proof. For $a \in \mathcal{A}$, $\|a\| \leq r \iff r^2\mathcal{I} - aa^* \geq 0$. Therefore, for any $s \in S$, $s(r^2\mathcal{I} - aa^*) \geq 0$, which in turn gives $s(aa^*) \leq r^2$ for any $r \geq \|a\|$. Therefore, we have $s(aa^*) \leq \|a\|^2$.

At the same time, it is known that if $x \in \mathcal{A}$ is positive, then there exists a state $s_x : \mathcal{A} \to \mathbb{C}$ such that $s_x(x) = \|x\|$. A sketch of the proof of the above statement is the following. Consider the sub-algebra of $\mathcal{A}$ generated by $\mathcal{I}$ and x. Let s be a state on this sub-algebra defined by $s(x) = \|x\|$. Then there exists an extension of s to $\mathcal{A}$ by the Hanh-Banach Theorem.

Since aa^* is Hermitian, there exists a state such that $s(aa^*) = \|aa^*\| = \|a\|^2$. □

4.5 Example: CAR-Algebra

An example of a natural C*-algebra for quantum information is the CAR algebra (canonical anticommutation relation). Intuitively, it is the algebra of finite Paulis acting on infinitely many qubits.

Recall in Example 4.2, $\mathcal{P}$ is a C*-algebra that is the abstraction of operators on single-qubit systems. We define the CAR algebra in a similar spirit, using relations similar to what was used to define $\mathcal{P}$.

4.5.1 Definition of CAR-Algebra

We consider the following algebra over $\mathbb{C}$ generated by elements $X_i, Z_i, i \in \mathbb{N}$ satisfying

1. $X_i^2 = Z_i^2 = \mathcal{I}$ for all i,
2. $X_i^* = X_i$, $Z_i^* = Z_i$ for all i,
3. $X_i Z_i + Z_i X_i = 0$ for all i,
4. $X_i Z_j = Z_j X_i$, $X_i X_j = X_j X_i$, $Z_i Z_j = Z_j Z_i$ for all $i \neq j$.

For a set S, let $\mathrm{C}^*(S)$ denote the C*-algebra generated by $\{s, s^* : s \in S\}$.

We start by considering $\mathrm{C}^*(\{X_i, Z_i\})$ for some particular i.

From the previous restrictions, we have

$$(X_i Z_i)^2 = X_i Z_i X_i Z_i = -X_i^2 Z_i^2 = -\mathcal{I}. \tag{4.5.1}$$

Let $Y_i = -iX_i Z_i$ so that $Y_i^2 = \mathcal{I}$, then

$$C^*(\{X_i, Z_i\}) = \mathrm{span}\{X_i, Z_i, Y_i, \mathcal{I}\} \simeq \mathbb{M}_2, \tag{4.5.2}$$

where $X_i \simeq \sigma_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y_i \simeq \sigma_2 = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$, $Z_i \simeq \sigma_3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\mathcal{I} \simeq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ are the Pauli matrices as the basis for $\mathbb{M}_2$. Alternatively, we can write the basis elements as $X_i^j Z_i^k$ for $j, k \in \{0, 1\}$.

From Relation 4., for any $i \neq j$, $\mathrm{C}^*(\{X_i, Z_i\})$ commutes with $\mathrm{C}^*(\{X_j, Z_j\})$. So $\mathrm{C}^*(\{X_i, Z_i, X_j, Z_j\}) \simeq \mathbb{M}_4$ with basis $X_i^k Z_i^l X_j^s Z_j^t = X_i^k X_j^s Z_i^l Z_j^t$ for $k, l, s, t \in \{0, 1\}$.

In general, $\mathrm{C}^*(\{X_i, Z_i : 1 \leq i \leq n\}) \simeq \mathbb{M}_{2^n}$, and has basis

$$\prod_{i=1}^{n} X_i^{a(i)} Z_i^{b(i)} = \prod_{i=1}^{n} X_i^{a(i)} \prod_{j=1}^{n} Z_j^{b(j)} \tag{4.5.3}$$

for all functions a, b that maps $\{1, 2, \cdots, n\}$ into $\{0, 1\}$.

Instead of functions, we can also see a, b as binary strings of length n, the i-th element of the string is $a(i)$ and $b(i)$. This allows us to write the basis of $\mathrm{C}^*(\{X_i, Z_i : 1 \leq i \leq n\})$ as $X^a Z^b$ where $a, b \in \{0, 1\}^n$ and

$$X^a = \prod_{i=1}^{n} X_i^{a(i)}, \; Z^b = \prod_{i=1}^{n} Z_i^{b(i)}. \tag{4.5.4}$$

At index i, $X^a Z^b$ is $X_i^{a(i)} Z_i^{b(i)}$ which is isomorphic to the Pauli matrix $\sigma_1^{a(i)} \sigma_3^{b(i)}$. It can be interpreted as a quantum system with n qubits, where operator $X^a Z^b$ corresponds to Pauli operator $\sigma_1^{a(i)} \sigma_3^{b(i)}$ acting on qubit i for each $1 \leq i \leq n$. For example, let $n = 4$ and $a = 0110$, then X^a can be represented as $\sigma_1^0 \otimes \sigma_1^1 \otimes \sigma_1^1 \otimes \sigma_1^0 = \mathcal{I} \otimes \sigma_1 \otimes \sigma_1 \otimes \mathcal{I}$ which is Pauli σ_1 acting on qubit 2 and 3.

Let $\mathcal{C}_n = \mathrm{C}^*(\{X_i, Z_i : 1 \leq i \leq n\})$. Any $x \in \mathcal{C}_n$ can be represented by a $2^n \times 2^n$ matrix M. Let $\|x\| = \|M\|$ be the operator norm of the representation of x. We define the CAR algebra as

$$\mathcal{C} = \overline{\bigcup_{n=1}^{\infty} \mathcal{C}_n}. \tag{4.5.5}$$

$\mathcal{C}$ has a basis $X^a Z^b$ for $a, b \in \{0, 1\}^*$ where all but finitely many $a(i), b(i)$ are 0. Similar to Example 4.2, we defined the X_i and Z_i in a way that they each can be represented by the 2×2 Pauli matrices. It can be interpreted that X_i and Z_i

are infinite-dimensional operators with indices, where at index i, they are the 2×2 Pauli X and Z, and at all other indices, they act as identity. Each of X^a and Z^b can be seen as a product of $X_i^{a_i}$ and $Z_i^{b_i}$. For example, let $a = 01100\cdots$ (where the infinitely many trailing 0's are omitted), then similar to the previous example, X^a can be represented as $\mathcal{I} \otimes \sigma_1 \otimes \sigma_1 \otimes \mathcal{I} \otimes \mathcal{I} \cdots$.

We also note that the above is not the standard way to define CAR algebra. [9] provides an example of how the CAR algebra is typically defined. Although the definitions may appear very different, they share the same underlying structure that is fundamental to the CAR algebra, which is having finite weight elements on infinitely many copies of $\mathbb{M}_2$. The definition of CAR algebra as finite weight Pauli matrices makes it more accessible to quantum information.

In later chapters, with abuse of notation, we will use X, Y, Z at times to denote the 2×2 Pauli matrices instead of $\sigma_1, \sigma_2, \sigma_3$.

4.5.2 Application of the CAR-Algebra

One property of the CAR algebra is that $\mathcal{C} \otimes_{\max} \mathcal{C} = \mathcal{C} \otimes_{\min} \mathcal{C}$, due to the fact that $\mathcal{C}$ is nuclear. More discussions on this can be found in [9, 25].

Consider a quantum system with countably infinitely many qubits. To model it under the Hilbert space model, it is natural to consider a countably infinite dimensional Hilbert space, which would have a basis equivalent to $\{|0\rangle, |1\rangle, |2\rangle, \cdots\}$. Let $\mathcal{H}_0$ be a countably infinite Hilbert space with basis $\{|0\rangle, |1\rangle, |01\rangle, |11\rangle, \cdots\}$. Each bit in the basis describes the state of the corresponding qubit in the quantum system. For example, $|0\rangle \equiv |0\rangle^{\otimes\infty}$ is the state where all the qubits are in state $|0\rangle$, and $|01\rangle \equiv |0\rangle \otimes |1\rangle \otimes |0\rangle^{\otimes\infty}$ is the state where the second qubit is in state $|1\rangle$, and all

other qubits are in state $|0\rangle$. Under this model, every element of the basis has the property that only finitely many bits are non-zero, and as a result, all but finitely many qubits of the corresponding basis state are in state $|0\rangle$.

While $\mathcal{H}_0$ is a natural Hilbert space to describe the quantum system with infinitely many qubits, it has its limitations. By construction, its basis states must only have finitely many qubits in $|1\rangle$. Therefore, a quantum state where all qubits are in $|1\rangle$, $|1\rangle^{\otimes\infty}$, is not in $\mathcal{H}_0$. In order to allow states with infinitely many $|1\rangle$ at the end to be part of this Hilbert space model, $\mathcal{H}_0$ needs to be extended. Let $\mathcal{H}_1$ be the Hilbert space with basis $\{|1\rangle^{\otimes\infty}, |0\rangle\otimes|1\rangle^{\otimes\infty}, |10\rangle\otimes|1\rangle^{\otimes\infty}, \cdots\}$ describing the quantum system where all but finitely many qubits are in state $|1\rangle$. Then $\mathcal{H} = \mathcal{H}_0 \oplus \mathcal{H}_1$ is a Hilbert space that can describe quantum states that end with both infinitely many $|0\rangle$'s and infinitely many $|1\rangle$'s.

However, there are still many quantum states $\mathcal{H}$ cannot describe. For example, the state where all qubits are in $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|+\rangle^{\otimes\infty}$, or the state with alternating $|0\rangle$ and $|1\rangle$, $|01\rangle^{\otimes\infty}$, are not in $\mathcal{H}$. In general, there is no countable Hilbert space that can fully describe all possible quantum states with countably infinitely many qubits. (Simply consider states that correspond to the binary form of different real numbers between 0 and 1 – they are mutually orthogonal, and therefore form an uncountable basis.)

An alternative way to describe the quantum system with infinitely many qubits is by using the CAR algebra in the C*-model. Let $\mathcal{C}$ be a CAR algebra. To describe a state in the system, a corresponding abstract state $s : \mathcal{C} \to \mathbb{C}$ can be defined by specifying its action on all elements of $\mathcal{C}$. Since states are linear, only elements of the form $X^a Z^b$, where $a, b \in \{0,1\}^*$ are binary strings, need to be specified.

For example, consider the state where all the qubits are in $|0\rangle$. The corresponding abstract state is

$$s(X^a Z^b) = \prod_{i=0}^{\infty} \langle 0| X^{a_i} Z^{b_i} |0\rangle , \tag{4.5.6}$$

where a_i, b_i are the bit value of a and b at index i. Similarly, if the state has $|1\rangle$ at qubit j and $|0\rangle$ everywhere else, then it can be defined as

$$s(X^a Z^b) = \prod_{i \neq j} \langle 0| X^{a_i} Z^{b_i} |0\rangle \langle 1| X^{a_j} Z^{a_j} |1\rangle . \tag{4.5.7}$$

Under this system, a quantum state can be defined as long as its action on any finite weight Pauli $X^a Z^b$ can be specified.

Another useful state the CAR-algebra can help defining is the infinite tensor product of Bell states, $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. We will see in a later Chapter that such a state does not exist under the tensor product of the Hilbert space model. Using the CAR-algebra, we define the state $s : \mathcal{C} \otimes \mathcal{C} \to \mathbb{C}$ to be

$$s(X^a Z^b \otimes X^c Z^d) = \prod_{i=0}^{\infty} \langle \psi| X^{a_i} Z^{b_i} \otimes X^{c_i} Z^{d_i} |\psi\rangle . \tag{4.5.8}$$

s is properly defined and has the property that at each index i, it acts exactly like the Bell state. [18] describessuch astate as an example of the notion of an "infinitely entangled state". are

Chapter 5

Linear System Games

A linear system game is a specific type of non-local game based on a linear system of equations. Mermin's magic square game, as described in Section 3.3.4, is a particular example of a linear system game.

5.1 Binary Linear System Games

Consider the binary linear system of equation $Mx = b$ where $M \in \mathbb{Z}_2^{m \times n}$, and $b \in \mathbb{Z}_2^m$. If there exists a vector $X \in \mathbb{Z}_2^n$ such that $Mx = b$, then x is a solution to this linear system. This linear system $Mx = b$ contains n variables, $x_1, \cdots, x_n$, and m equations of the form $M_{i,1}x_1 + \cdots + M_{i,n}x_n = b_i$. With the binary system, some of the coefficients can be zero, so each equation i might only contain a subset of the variables.

Recall that in the case of Mermin's magic square game, the linear set of equations

are

$$\begin{aligned} a_1 + a_2 + a_3 &= 0 \qquad a_1 + a_4 + a_5 = 0 \\ a_4 + a_5 + a_6 &= 0 \qquad a_2 + a_5 + a_8 = 0 \\ a_7 + a_8 + a_9 &= 0 \qquad a_3 + a_6 + a_9 = 1. \end{aligned} \tag{5.1.1}$$

A binary linear system game based on $Mx = b$ is a non-local game with the following rules. As inputs, Alice receives one linear equation from the system, and Bob receives one variable contained in the same equation (with a non-zero coefficient). Without communication, Alice must output an assignment to all the variables in her equation, and Bob must output an assignment for his variable. To win the game, Alice's assignment must satisfy the linear equation given to her, and Bob's output must match Alice's assignment on the common variable. A classical strategy is a strategy in which Alice and Bob do not share any entanglement, and an entangled quantum strategy is a strategy where Alice and Bob share an entangled quantum state $|\psi\rangle$. If the state $|\psi\rangle$ is a bipartite state in a tensor product of Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$, the strategy is called the entangled strategy in the tensor product model. A perfect strategy is a strategy where the players can win with probability 1.

Interestingly, there exist games with perfect entangled quantum strategies, but no perfect classical strategies. Mermin's magic square is an example of such a game. It is easy to summarize the condition for the existence of a perfect classical strategy.

Theorem 5.1. *A binary linear system game based on $Mx = b$ has a perfect classical strategy if and only if the system of equations has a solution.*

Proof. If there exists a solution x such that $Mx = b$, Alice and Bob can always output the assignment of variables from x to win the game.

To show the converse, it is important to note that using probabilistic strategies does not improve the probability of winning, because the winning probability of a probabilistic strategy is a convex combination of the winning probability of deterministic strategies. For a deterministic strategy, Alice and Bob must decide on their output for each possible input before the start of the game. Therefore the value for each x_i must be fixed. In order to win with certainty, Alice must use the same assignment, and x_i must satisfy every equation in the linear system. In other words, the assignment of x in the deterministic strategy must be a solution to the linear system. □

The condition for the existence of perfect entangled quantum strategies, however, is not as simple. As a starting point, we consider the perfect entangled strategy under the tensor product model.

5.2 Tensor-product model

Cleve and Mittal [5] investigated binary linear system games as an extension of Mermin's magic square game under the tensor product model. A binary linear system of the form $Mx = b$ can be written in multiplicative form, where a vector $x \in \{\pm 1\}^n$ satisfies equation l if and only if

$$x_1^{M_{l,1}} x_2^{M_{l,2}} \cdots x_n^{M_{l,n}} = (-1)^{b_l}. \tag{5.2.1}$$

Alternatively, let

$$V_l = \{k_1, k_2, \cdots, k_r\} = \{1 \leq k \leq n : M_{l,k} = 1\} \tag{5.2.2}$$

be the set of indices of variables in equation l, and equation l can be expressed as

$$x_{k_1} x_{k_2} \cdots x_{k_r} = (-1)^{b_l}. \tag{5.2.3}$$

In order for a binary linear system game to have a perfect entangled strategy in the tensor product model, [5] showed that a finite-dimensional operator solution, which is a generalization of binary solutions, to the linear system must exist.

Definition 5.1. *An operator solution to a binary linear system $Mx = b$ is a sequence of bounded self-adjoint operators $A_1, \cdots, A_n$ on a Hilbert space $\mathcal{H}$ such that*

1. *$A_i^2 = \mathcal{I}$ for all $i \leq i \leq n$.*
2. *If x_i and x_j appear in the same equation, then $A_i A_j = A_j A_i$ (local compatibility).*
3. *For each equation of the form $x_{k_1} x_{k_2} \cdots x_{k_r} = (-1)^{b_l}$,*

$$A_{k_1} A_{k_2} \cdots A_{k_r} = (-\mathcal{I})^{b_l} \tag{5.2.4}$$

(constraint satisfaction).

The first condition enforces that the A_i's are binary observables. The term local compatibility in the second condition comes from quantum mechanics, where two observables commute if and only if they are compatible in the sense that they can be measured simultaneously. The local compatibility condition also matches the fact that in the original linear system, all variables appearing in the same linear equation can be placed in any order. The third condition simply forces the operators to multiply in the same way that satisfies the original constraint.

Theorem 5.2. *A binary linear system game based on $Mx = b$ has a perfect entangled strategy in the tensor product model if and only if there exists a finite-dimensional operator solution to the linear system.*

The proof of this result can be found in the original paper [5] by Cleve and Mittal and is outside the scope of our discussion. In [5], it was required that the Hilbert space must be separable. However, this condition can be dropped because any entangled state $|\psi\rangle$ in a Hilbert space $\mathcal{H}$ can be expressed in terms of a countable linear combination of some orthonormal basis elements $|e_i\rangle \otimes |f_j\rangle$, namely

$$|\psi\rangle = \sum_{i,j} \alpha_{i,j} |e_i\rangle \otimes |f_j\rangle \,. \tag{5.2.5}$$

5.3 Commuting operator strategy and solution group

Now consider the commuting operator strategy where the entanglement shared by Alice and Bob, $|\psi\rangle$, is in a joint Hilbert space $\mathcal{H}$. Alice's and Bob's measurements are observables on $\mathcal{H}$, with the restriction that all of Alice's observables commute with Bob's observables. More specifically, using the V_l defined in Eq 5.2.2, we have the following definition.

Definition 5.2. *Let $Mx = b$ be an $m \times n$ binary linear system. A commuting operator strategy for the non-local game associated to $Mx = b$ consists of a Hilbert space $\mathcal{H}$, a state $|\psi\rangle \in \mathcal{H}$, and two collections of self-adjoint operators on H, $\{A_i^{(l)} : 1 \leq l \leq m, i \in V_l\}$ and $\{B_j : i \leq j \leq n\}$, such that*

(a) $(A_i^{(l)})^2 = B_j^2 = \mathcal{I}$ *for all* $1 \leq l \leq m$, $i \in V_l$, *and* $i \leq j \leq n$

(b) $A_i^{(l)} B_j = B_j A_i^{(l)}$ *for all* $1 \leq l \leq m$, $i \in V_l$, *and* $1 \leq j \leq n$.

(c) $A_i^{(l)} A_j^{(l)} = A_j^{(l)} A_i^{(l)}$ *for all* $i \leq l \leq m$ *and* $i, j \in V_l$ *(local compatibility).*

Different commuting operator strategies will give Alice and Bob different probabilities of winning the binary linear system game. A commuting operator strategy is perfect if it can be used to win the binary linear system game with probability 1. As one may recall, this requires Alice and Bob's output for the same variable to be identical, and Alice's outputs have to satisfy the constraint she is given. We give the mathematical conditions for a perfect commuting operator strategy later in Proposition 5.4.

It turns out that for a perfect commuting operator strategy to exist, the binary linear system game must have an operator solution. Unlike the case with perfect tensor product strategies, the operator solution here may be infinite-dimensional.

To prove that the existence of a perfect commuting operator strategy is equivalent to having operator solutions, we define an intermediary object called the solution group.

Definition 5.3. *The solution group of a binary linear system* $Mx = b$ *is the group* Γ *generated by* $g_1, \cdots g_n$ *and* J *satisfying the following relations (where* e *is the group identity):*

1. $g_i^2 = e$ *for all* $1 \leq i \leq n$ *(g_i's are involutions).*
2. *If* x_i *and* x_j *appear in the same equation, then* $g_i g_j = g_j g_i$ *(local compatibility).*
3. *For each equation of the form* $x_{k_1} x_{k_2} \cdots x_{k_r} = (-1)^{b_l}$*, the generators satisfy*

$$g_{k_1} g_{k_2} \cdots g_{k_r} = J^{b_l} \tag{5.3.1}$$

(constraint satisfaction).

4. $g_i J = J g_i$ *for all* $i \leq i \leq n$, *and* $J^2 = e$ *(*J *commutes with each generator).*

Apart from the inclusion of the object J, the definition of the solution group appears almost identical to that of the operator solution defined in Definition 5.1. In fact, they are closely related.

Theorem 5.3. *Let* $Mx = b$ *be a binary linear system. Then the followings are equivalent:*

1. *There exists a perfect commuting operator strategy for the non-local game associated with* $Mx = b$.
2. *There exists an operator solution for* $Mx = b$
3. *The solution group for* $Mx = b$ *has the property that* $J \neq e$.

The third condition enforces J in the solution group to be a non-trivial element that commutes with the rest of the group, and since $J^2 = e$, J behaves as the identity multiplied by the scalar -1.

5.4 Proof of Equivalences

To prove Theorem 5.3, we start by considering the conditions for a commuting operator strategy to be perfect.

Proposition 5.4. *A commuting operator strategy* $\left(\mathcal{H}, |\psi\rangle, \left\{A_i^{(l)}\right\}, \{B_j\}\right)$ *is perfect if and only if*

1. $A_i^{(l)} |\psi\rangle = B_i |\psi\rangle$ *for all* $1 \leq l \leq m$ *and* $i \in V_l$ *(consistency between Alice and Bob) and*

2. $\prod_{i \in V_l} A_i^{(l)} |\psi\rangle = (-1)^{b_l} |\psi\rangle$ *for all* $1 \leq l \leq m$ *(constraint satisfaction).*

Proof. In order for Alice's and Bob's outputs to be consistent,

$$\langle\psi| A_i^{(l)} B_i |\psi\rangle = 1 \tag{5.4.1}$$

for all $1 \leq l \leq m$ and $i \in V_l$. Since $A_i^{(l)}$ and B_j are unitary operators, their product is also unitary. Given that $|\psi\rangle$ is a unit vector, Eq 5.4.1 is equivalent to

$$A_i^{(l)} B_j |\psi\rangle = |\psi\rangle . \tag{5.4.2}$$

Since $(A_i^{(l)})^2 = \mathcal{I}$, by left-multiplying $A_i^{(l)}$ on both sides, Eq 5.4.2 becomes the condition in Part 1. of the proposition. Similarly, in order for Alice's assignment to satisfy equation l,

$$\langle\psi| (-1)^{b_l} \prod_{i \in V_l} A_i^{(l)} |\psi\rangle = 1. \tag{5.4.3}$$

Using the same argument that $(-1)^{b_l} \prod_{i \in V_l} A_i^{(l)}$ is unitary, Eq 5.4.3 becomes the condition in Part 2. of the proposition. □

The next step is to show that a perfect commuting operator strategy can be turned into an operator solution for the linear system.

Lemma 5.4.1. *Let* $\left(\mathcal{H}, |\psi\rangle, \left\{A_i^{(l)}\right\}, \{B_j\}\right)$ *be a perfect commuting operator strategy for* $Mx = b$*. Then there exist some* $Q_1, \cdots, Q_n \in \mathbb{B}(\mathcal{H})$ *that form an operator solution for* $Mx = b$*.*

The idea of the Lemma is to project Alice's operators onto a smaller subspace. Recall the definition of the projection onto a subspace, $\cdot|_{\mathcal{H}}$.

Definition 5.4 (Def 2.9)**.** *The operator $\cdot|_{\mathcal{H}_0}$ is the projection from $\mathbb{B}(\mathcal{H})$ to a subspace $\mathbb{B}(\mathcal{H}_0)$. Let P be the projection from $\mathcal{H}$ to $\mathcal{H}_0$, and $A \in \mathbb{B}(\mathcal{H})$, then*

$$A|_{\mathcal{H}_0} = PAP. \tag{5.4.4}$$

Let $\mathcal{A}$ be the unital algebra generated by $\{A_i^{(l)}\}$, and $\mathcal{A}|\psi\rangle = \{A|\psi\rangle : A \in \mathcal{A}\}$. Let $\mathcal{H}_0 = \overline{\mathcal{A}|\psi\rangle}$, and $Q_i := A_i^{(l)}|_{\mathcal{H}_0}$ for some l with $i \in V_l$. We show that the Q_i's defined this way form an operator solution.

The above lemma can be verified by checking all the conditions in the definition of an operator solution are satisfied.

Proof of Lemma 5.4.1. Before starting the verification, we first show that Q_i is the same regardless of the choice of l.

Let $\mathcal{B}$ be the unital algebra generated by $\{B_j\}$. Given a perfect commuting operator strategy, by Proposition 5.4, $A_i^{(l)}|\psi\rangle = B_i|\psi\rangle$ for all l where $i \in V_l$. Therefore, for every $A \in \mathcal{A}$, there exists $B \in \mathcal{B}$ such that $A|\psi\rangle = B|\psi\rangle$. This means that $\mathcal{A}|\psi\rangle = \mathcal{B}|\psi\rangle$ and $\mathcal{H}_0 = \overline{\mathcal{B}|\psi\rangle}$. Let $A, A' \in \mathcal{A}$ such that $A|\psi\rangle = A'|\psi\rangle$. Then for all $B \in \mathcal{B}$,

$$AB|\psi\rangle = BA|\psi\rangle = BA'|\psi\rangle = A'B|\psi\rangle. \tag{5.4.5}$$

Since $\overline{\mathcal{B}|\psi\rangle} = \mathcal{H}_0$, the above equation means that the action of A on any element of $\mathcal{H}_0$ is the same as the action of A' on any element of $\mathcal{H}_0$. Because A and A' are continuous, $A|_{\mathcal{H}_0}|\phi\rangle = A'|_{\mathcal{H}_0}|\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}_0$, and as a result $A|_{\mathcal{H}_0} = A'|_{\mathcal{H}_0}$. For perfect commuting operator strategy, $A_i^{(l)}|\psi\rangle = B_i|\psi\rangle = A_i^{(l')}|\psi\rangle$ for any $i \in V_l \cap V_{l'}$, which means $A_i^{(l)}|_{\mathcal{H}_0} = A_i^{(l')}|_{\mathcal{H}_0}$ so Q_i is uniquely defined for each i.

Next, we show that the $\cdot|_{\mathcal{H}_0}$ is a $*$-homomorphism on $\mathcal{A}$. Let P be the orthogonal projection from $\mathcal{H}$ to $\mathcal{H}_0$. Then for any $|\phi\rangle \in \mathcal{H}_0$, $P|\phi\rangle = |\phi\rangle$, and for all $A \in \mathcal{A}$,

$A|_{\mathcal{H}_0} = PAP$. Let $A, A' \in \mathcal{A}$. Then

$$A|_{\mathcal{H}_0} A'|_{\mathcal{H}_0} = PAPPA'P = PAPA'P = (APA')|_{\mathcal{H}_0}. \tag{5.4.6}$$

For any $|\phi\rangle \in \mathcal{H}_0$, $A' |\phi\rangle \in \mathcal{H}_0$ so $APA' |\phi\rangle = AP(A' |\phi\rangle) = AA' |\phi\rangle$ for all $|\phi\rangle \in \mathcal{H}$. This is equivalent to the homomorphism requirement

$$A|_{\mathcal{H}_0} A'|_{\mathcal{H}_0} = (APA')|_{\mathcal{H}_0} = (AA')|_{\mathcal{H}_0}. \tag{5.4.7}$$

The $*$ condition comes simply from the fact $P = P^*$:

$$(A|_{\mathcal{H}_0})^* = (PAP)^* = PA^*P = A^*|_{\mathcal{H}_0}. \tag{5.4.8}$$

Similarly, using the same argument, we can prove that $\cdot|_{\mathcal{H}_0}$ is a $*$-homomorphism on $\mathcal{B}$.

Moreover, we have that for any $A \in \mathcal{A}$, $A |\psi\rangle \in \mathcal{H}$ so

$$A|_{\mathcal{H}_0} |\psi\rangle = PAP |\psi\rangle = PA |\psi\rangle = A |\psi\rangle . \tag{5.4.9}$$

Similarly, for all $B \in \mathcal{B}$, $B|_{\mathcal{H}_0} |\psi\rangle = B |\psi\rangle$.

The first condition is to show that $Q_i^2 = \mathcal{I}$ for all i.

$$Q_i^2 = (A_i^{(l)}|_{\mathcal{H}_0})^2 = (A_i^{(l)})^2|_{\mathcal{H}_0} = \mathcal{I}. \tag{5.4.10}$$

The second condition requires $Q_i Q_j = Q_j Q_i$ if $i, j \in V_l$ for some l.

$$Q_i Q_j = A_i^{(l)}|_{\mathcal{H}_0} A_j^{(l)}|_{\mathcal{H}_0} = (A_i^{(l)} A_j^{(l)})|_{\mathcal{H}_0} = A_j^{(l)}|_{\mathcal{H}_0} A_i^{(l)}|_{\mathcal{H}_0} = Q_j Q_i. \tag{5.4.11}$$

The last condition is to show that Equation 5.2.4 is satisfied:

$$\prod_{i \in V_l} Q_i = (-1)^{b_l} \ \forall l. \tag{5.4.12}$$

To show this, we need to show that the projection $\cdot|_{\mathcal{H}_0}$ is a homomorphism on the algebra generated by both $\mathcal{A}$ and $\mathcal{B}$ combined. Let $A \in \mathcal{A}$ and $B \in \mathcal{B}$. To show that the projection is a homomorphism, it is necessary to have $(AB)|_{\mathcal{H}_0} = A|_{\mathcal{H}_0}B|_{\mathcal{H}_0}$.

$$A|_{\mathcal{H}_0}B|_{\mathcal{H}_0} = PAPPBP = PAPBP = (APB)|_{\mathcal{H}_0} \tag{5.4.13}$$

for any $|\phi\rangle \in \mathcal{H}_0$, $B|\phi\rangle \in \mathcal{H}_0$ so $PB|\phi\rangle = B|\phi\rangle$

$$PAPBP|\phi\rangle = PAB|\phi\rangle = PABP|\phi\rangle = (AB)|_{\mathcal{H}_0}|\phi\rangle\,. \tag{5.4.14}$$

This means $(AB)|_{\mathcal{H}_0} = A|_{\mathcal{H}_0}B|_{\mathcal{H}_0}$.

Next we show that $Q_iB|\psi\rangle = BQ_i|\psi\rangle$ for any $B \in \mathcal{B}$.

$$Q_iB|\psi\rangle = A_i^{(l)}|_{\mathcal{H}_0}B|_{\mathcal{H}_0}|\psi\rangle = B|_{\mathcal{H}_0}(Q_i|\psi\rangle) = BQ_i|\psi\rangle\,. \tag{5.4.15}$$

Since any state in $\mathcal{H}_0$ can be written as $B|\psi\rangle$ for some $B \in \mathcal{B}$,

$$\prod_{i\in V_l} Q_iB|\psi\rangle = B\prod_{i\in V_l} Q_i|\psi\rangle = B\prod_{i\in V_l} A_i^{(l)}|\psi\rangle = (-1)^{b_l}B|\psi\rangle\,, \tag{5.4.16}$$

and again by continuity, we have the constraint satisfaction condition

$$\prod_{i\in V_l} Q_i = (-1)^{b_l} \tag{5.4.17}$$

satisfied. □

Showing Condition 2 implies Condition 3 in Theorem 5.3 is relatively straightforward.

Lemma 5.4.2. *If $Mx = b$ has an operator solution, then $J \neq e$ in the solution group Γ of $Mx = b$*

Proof. Let $Q_1, \cdots, Q_n$ be an operator solution of $Mx = b$. Then the following mapping is a representation of Γ:

$$g_i \mapsto Q_i, \ 1 \leq i \leq n, \quad \text{and} \quad J \mapsto -\mathcal{I}. \tag{5.4.18}$$

In this representation, $J = -\mathcal{I} \neq \mathcal{I}$, which means $J \neq e$ in Γ. □

Having shown that Condition 1 implies Condition 2 (Lemma 5.4.1) and Condition 2 implies condition 3 (Lemma 5.4.2), the last step of the proof of Theorem 5.3 is to show that Condition 3 implies Condition 1.

Lemma 5.4.3. *If $Mx = b$ has a solution group Γ with $J \neq e$, then there exists a perfect commuting operator strategy for the associated binary linear system game.*

Proof. The goal here is to construct a Hilbert space, two sets of operators for Alice and Bob, and a state $|\psi\rangle$ that constitutes a perfect commuting operator strategy. Define a Hilbert space $\mathcal{H}$ to be

$$\mathcal{H} = \left\{ \sum_{g \in \Gamma} \alpha_g |g\rangle : \alpha_g \in \mathbb{C} \ \text{ such that } \ \sum_{g \in \Gamma} |\alpha_g|^2 < \infty \right\}. \tag{5.4.19}$$

$\mathcal{H}$ is the completion of the algebra of Γ, and $\{|g\rangle : g \in \Gamma\}$ form an orthonormal basis for $\mathcal{H}$. Let $L_g, R_g \in \mathbb{B}(\mathcal{H})$ where they are the left and right multiplication operators for g on $\mathcal{H}$. In other words,

$$L_g |h\rangle = |gh\rangle \quad \text{and} \quad R_g |h\rangle = |hg\rangle . \tag{5.4.20}$$

L_g and R_g are unitaries because they move the orthonormal basis elements around. Furthermore, for all $g, h \in \Gamma$, it is easy to see that

$$L_g R_h = R_h L_g, \ L_g L_h = L_{gh}, \quad R_g R_h = R_{hg}. \tag{5.4.21}$$

To get Alice and Bob's operators, let

$$A_i^{(l)} = L_{g_i} \text{ for all } 1 \leq l \leq m,\ i \in V_l, \tag{5.4.22}$$

and

$$B_j = R_{g_j} \text{ for all } 1 \leq j \leq n. \tag{5.4.23}$$

The state for the solution group is

$$|\psi\rangle = \frac{|e\rangle - |J\rangle}{\sqrt{2}}. \tag{5.4.24}$$

Because $J \neq e$, $|\psi\rangle$ is a well defined unit vector.

Now we show the above sets of operators and states will constitute a perfect commuting operator strategy. First, it needs to be a commuting operator strategy. For (a) in Definition 5.1,

$$(A_i^{(l)})^2 = L_{g_i}^2 = L_{g_i^2} = L_e = \mathcal{I} = R_{g_i}^2 = B_i^2. \tag{5.4.25}$$

To see (b),

$$A_i^{(l)} B_j = L_{g_i} R_{g_j} = R_{g_j} L_{g_i} = B_j A_i^{(l)}. \tag{5.4.26}$$

To show (c), we use the Condition 2 in Definition 5.3 that $g_i g_j = g_j g_i$ if $i, j \in V_l$ for some l:

$$A_i^{(l)} A_j^{(l)} = L_{g_i} L_{g_j} = L_{g_i g_j} = L_{g_j g_i} = A_j^{(l)} A_i^{(l)}. \tag{5.4.27}$$

To see that this commuting operator strategy is perfect, Proposition 5.4 needs to be satisfied. For Condition 1, we evoke $g_i J = J g_i$ for all i, so that

$$A_i^{(l)} |\psi\rangle = L_{g_i} \frac{|e\rangle - |J\rangle}{\sqrt{2}} = \frac{|g_i\rangle - |g_i J\rangle}{\sqrt{2}} = \frac{|g_i\rangle - |J g_i\rangle}{\sqrt{2}} = R_{g_i} |\psi\rangle = B_i |\psi\rangle . \tag{5.4.28}$$

For Condition 2,

$$\prod_{i \in V_l} A_i^{(l)} |\psi\rangle = \prod_{i \in V_l} L_{g_i} |\psi\rangle = L_{J^{b_l}} |\psi\rangle . \tag{5.4.29}$$

If $b_l = 0$,

$$L_{J^{b_l}} |\psi\rangle = L_e |\psi\rangle = |\psi\rangle , \tag{5.4.30}$$

and if $b_l = 1$,

$$L_{J^{b_l}} |\psi\rangle = L_J |\psi\rangle = \frac{|J\rangle - |e\rangle}{\sqrt{2}} = - |\psi\rangle . \tag{5.4.31}$$

This gives us $\prod_{i \in V_l} A_i^{(l)} |\psi\rangle = (-1)^{b_l} |\psi\rangle$ which finishes the proof of the equivalence relations. □

5.5 Discussion

The results here can be generalized to linear system games with linear systems over $\mathbb{Z}_n$ for any integer $n \geq 2$. Instead of outputting binary numbers, Alice and Bob will output each variable from $\mathbb{Z}_n$. The commuting operator strategy is based on a unitary U that is the principle n-th root of unity, $U^n = \mathcal{I}$, instead of $U^2 = \mathcal{I}$. Similarly, the solution group would require $g_i^n = e$ and $J^n = e$ instead of $g_i^2 = e$ and $J^2 = e$. The state for the commuting operator strategy $|\psi\rangle$ will be

$$|\psi\rangle = \frac{1}{\sqrt{p}} \sum_{i=0}^{n-1} e^{\frac{2\pi i}{n}} \left| J^i \right\rangle . \tag{5.5.1}$$

One interesting question regarding a perfect commuting operator protocol of a linear system game constructed from the solution group is how much entanglement the state $|\psi\rangle$ contains if the minimum dimension of the operator solution is infinite. Intuitively, the entanglement should be infinite, since otherwise, the protocol would be able to be converted into a finite-dimensional and therefore a tensor-product protocol. However, there is no clear method to calculate the amount of entanglement in the commuting operator model. It is not clear, that how the structure of the commuting

operators, which are left and right multiplications, in this case, give rise to meaningful entanglement in a state of the form $\frac{|e\rangle - |J\rangle}{\sqrt{2}}$. Typically, to show some state contains at least one set of Bell state, one only need to show that CHSH inequality can be maximally violated using this state. In this particular case, how to violate the CHSH inequality from this state is not immediately clear. Future work can be done on how to analyze and quantify the entanglement in the commuting operator framework.

Chapter 6

Embezzlement

Entanglement is a type of resource that is key to quantum communication. The Bell state, $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ has the largest amount of entanglement (in terms of entanglement entropy which we will discuss later) two qubits can ever hold. It is often called the maximally entangled state. What makes it extremely useful is that it gives out the same measurement outcome for any two compatible measurements performed on the individual qubits. Due to its versatility, the above Bell state is used in many quantum communication protocols.

In order to turn two separable qubits into an entangled pair, joint operators on both qubits must be applied. It is not possible to create entanglement with local operations.

Definition 6.1 (Entanglement entropy)**.** *Let $\mathcal{H}_1 \otimes \mathcal{H}_2$ be a finite-dimensional Hilbert space and $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ be a quantum state with a Schmidt decomposition $|\psi\rangle =$*

$\sum_i \alpha_i |u_i\rangle \otimes |v_i\rangle$. *The entanglement entropy of* $|\psi\rangle$ *is*

$$\mathcal{S}(|\psi\rangle) = -\sum_i |\alpha_i|^2 \log(|\alpha_i|^2). \tag{6.0.1}$$

Entanglement entropy is a measure of the amount of entanglement across a bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$. It is not possible to increase the entanglement entropy of a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ using local unitaries of the form $A \otimes B$ since such local operator cannot change the Schmidt coefficients of $|\psi\rangle$.

The discussion about entanglement and entanglement entropy is mostly on finite-dimensional systems. In an infinite-dimensional quantum system, however, there can be an infinite amount of entanglement present. The law of conservation of entanglement by local operations becomes less clear in this case since adding or subtracting a finite number from infinity still gives infinity. The idea here is born out of curiosity as to what will happen if one starts manipulating an infinite amount of entanglement using local operations. Is it possible to create some entanglement locally, if there is an infinite amount of entanglement at one's disposal? If it can be done, will the process be convoluted due to the subtleties in manipulating infinite-dimensional Hilbert spaces? Can infinite entanglement be modelled intuitively? The answers to all these questions are yes, as we will find in the study the protocol for embezzlement that "steals" finite entanglement from a resource state with infinite entanglement.

6.1 Embezzlement in tensor product model

Our first task is to tackle the problem of embezzlement of entanglement. The problem is studied in [26] where the commuting operator model for embezzlement is estab-

lished. We discuss the results in [26] as well as the C*-model for embezzlement in this thesis.

The original term "embezzlement" refers to stealing a tiny proportion from many large sums of money so that the thief ends up with a sizable profit whereas the change in the original accounts is unnoticeable. For example, if Eve could somehow take out 0.2 cents each from ten million bank accounts, she will up with $20000 without any of the account owners even noticing anything.

The embezzlement of entanglement has a similar spirit. If Alice and Bob share a large entangled state, can they use it to turn a pair of qubits in the product state into a Bell state (or some other entangled state with non-trivial entanglement entropy) using only local operations without making noticeable changes to the original state? More formally, under the tensor-product model,

Definition 6.2 (Embezzlement of entanglement (tensor product))**.** *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces owned by Alice and Bob, and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a shared state. Embezzlement of entanglement is a protocol where Alice and Bob each applies some local unitaries $U_A \in \mathcal{U}(\mathbb{C}^2 \otimes \mathcal{H}_A)$, $U_B \in \mathcal{U}(\mathcal{H}_B \otimes \mathbb{C}^2)$ to turn $|0\rangle \otimes |\psi\rangle \otimes |0\rangle$ into $\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle \otimes |0\rangle + |1\rangle \otimes |\psi\rangle \otimes |1\rangle)$.*

If the resulting state is $\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi'\rangle \otimes |0\rangle + |1\rangle \otimes |\psi'\rangle \otimes |1\rangle)$ instead, where $|\langle\psi|\psi'\rangle| \approx 1$, the protocol is called approximate embezzlement.

Approximate embezzlement was studied by [8]. The authors showed that approximate embezzlement could be achieved to arbitrary precision if the dimension of $\mathcal{H}_A$ and $\mathcal{H}_B$ can be arbitrarily large. In [14], the authors devised a non-local game based on the idea of embezzlement where the players can approximate embezzlement with precision ϵ if they share entanglement of the size $\Omega(\frac{1}{\epsilon})$.

Since larger dimensional Hilbert spaces lead to better approximation, a natural follow-up question is, if $\mathcal{H}_A$ and $\mathcal{H}_B$ are infinite-dimensional, can embezzlement be achieved exactly?

Theorem 6.1. *Embezzlement of entanglement is not possible under the tensor product model, regardless of the dimension of $\mathcal{H}_A$ and $\mathcal{H}_B$.*

The proof is simply based on the idea that local operations cannot change Schmidt coefficients.

Recall that backed in Chapter 3, we had Theorem 3.2 on Schmidt decomposition.

Theorem 6.2. *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces with arbitrary (potentially uncountable) dimensions, and let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite state. Then there exists a Schmidt decomposition*

$$|\psi\rangle = \sum_{i=0}^{\infty} s_i |u_i\rangle \otimes |v_i\rangle \tag{6.1.1}$$

where the number of non-zero Schmidt coefficients are countable.

Knowing that the Schmidt coefficients exist and are always countable, we can now finish off the proof of the no-go result. Let $|\psi\rangle = \sum_i s_i |u_i\rangle \otimes |v_i\rangle$ be a Schmidt decomposition of $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where s_i's are sorted in descending order.

The largest Schmidt coefficients of the starting state $|0\rangle \otimes |\psi\rangle \otimes |0\rangle$ is s_1; the largest Schmidt coefficients of the target state $\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle \otimes |0\rangle + |1\rangle \otimes |\psi\rangle \otimes |1\rangle)$ is $\frac{1}{\sqrt{2}} s_1$. Since local operations preserve Schmidt coefficients, the starting state cannot be converted into the target state locally. □

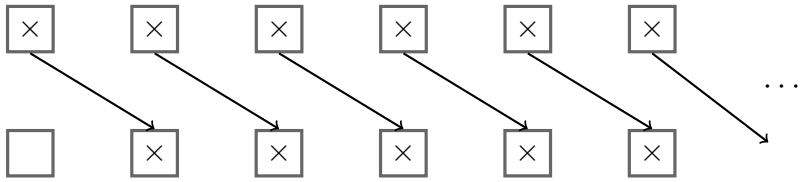


Figure 6.1: Hilbert Hotel

6.2 Perfect Embezzlement and the Hilbert Hotel

While perfect embezzlement is not possible in the tensor product model, there seems to be an intuitive way to achieve it with an infinite amount of entanglement. The idea behind this is the famous "Hilbert Hotel".

A Hilbert Hotel is an imaginary hotel with infinitely many rooms where all rooms are full. If a new guest arrives, the hotel manager can simply ask every guest to move to the next room adjacent to their original room, and the first room becomes available.

As for embezzlement, if there are infinitely many Bell states in a quantum system, is it possible to shift the state somehow so that one of the Bell states can be "swapped out" with a separable state while the rest of the state remains unchanged? In this case, since a separable state needs to be added and a Bell state needs to be removed without altering the original state, the original state must contain infinitely many Bell states and infinitely many separable states. Figure 6.2 describes such an imaginary protocol.

Let $|\psi\rangle$ be a state with infinitely many qubit pairs shared between Alice and Bob, indexed with integers from $-\infty$ to ∞ (each circle represents a qubit). The qubits on non-positive indices are in state $|00\rangle$ (disconnected circles on the left), and the qubit pairs on positive indices are Bell states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ shared across Alice and Bob

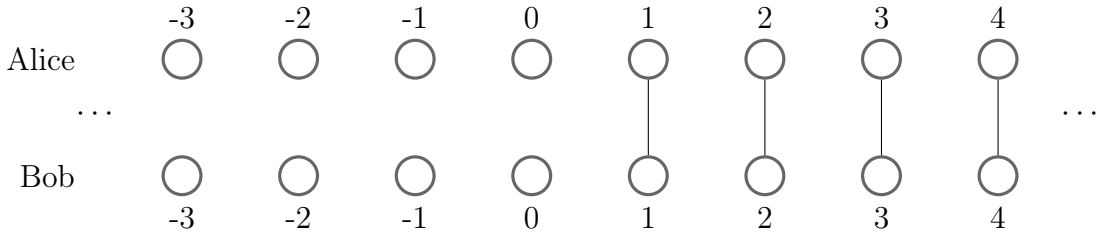


Figure 6.2: Starting State of Embezzlement

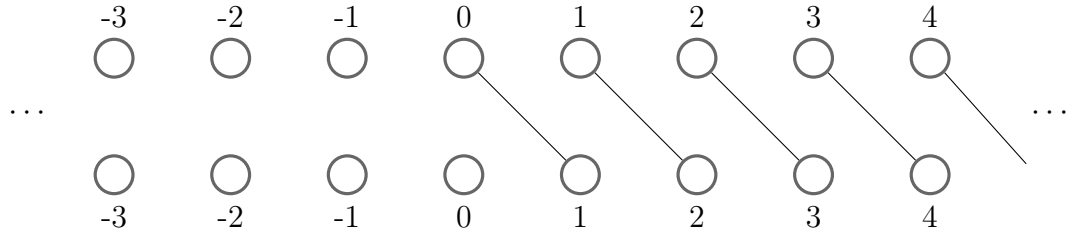


Figure 6.3: Left shift of Alice's Qubits by 1

(connected circles on the right).

To perform embezzlement, Alice and Bob shift all of their qubits from index i to $i-1$, so that the qubits at index 0 becomes a Bell state. Figure 6.3 shows the state of the qubits if Alice shifts her qubits before Bob does anything, and Figure 6.4 shows the states of the qubits when Bob shifts his qubits and Alcie does nothing. Figure 6.5 shows the final state when both Alice and Bob performed the left shift.

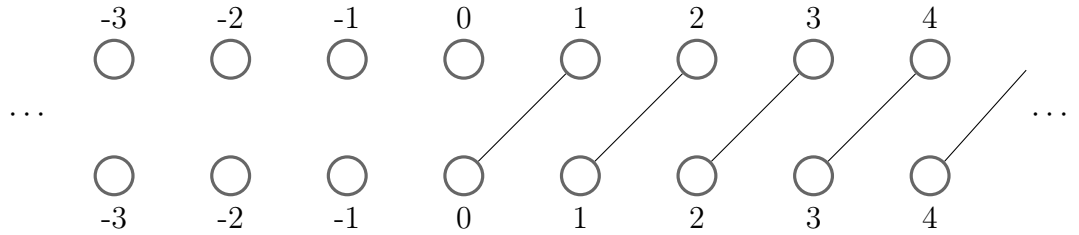


Figure 6.4: Left shift of Bob's Qubits by 1

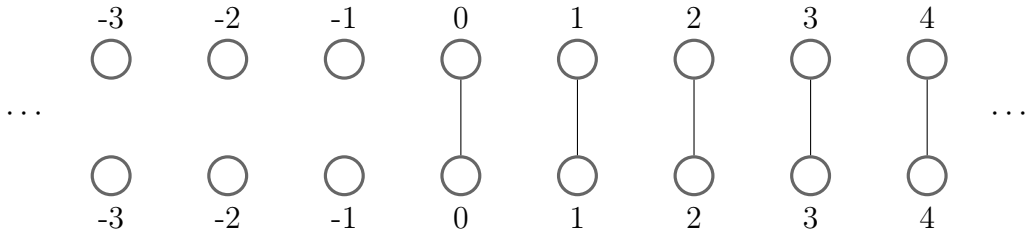


Figure 6.5: Leftshift of Both Alice and Bob's Qubits

Then, each of them swaps out their qubit at index 0 with an "outsider" qubit in $|0\rangle$, as shown in Figure 6.6

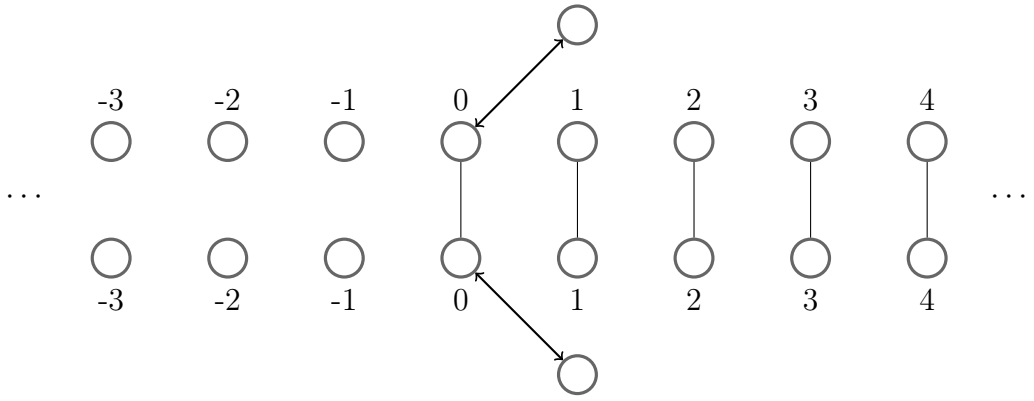


Figure 6.6: Swapping Out Qubits at Index 0

In the end, Alice and Bob end up with the original state $|\psi\rangle$ and a freshly swapped out extra Bell state. The final state is shown in Figure 6.7

While the above protocol makes sense intuitively, we know it cannot be converted into one that works in the tensor-product model due to the no-go theorem. If one attempts to translate it, the very first hurdle is that a state that contains infinitely many Bell states does not exist in the tensor product model. The Schmidt coefficients of n maximally entangled qubit pairs are all $\sqrt{2}^{-n}$, so the Schmidt coefficients of

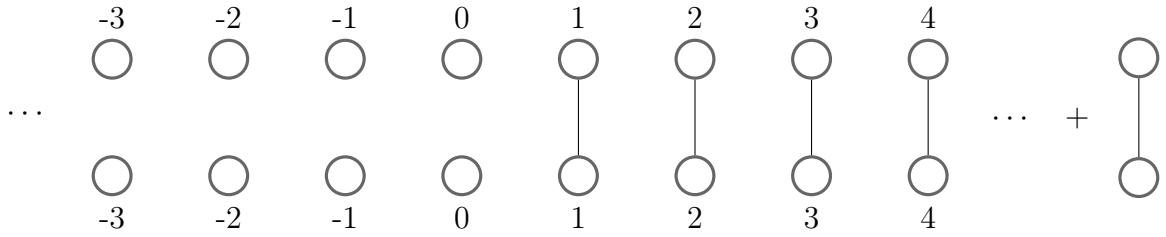


Figure 6.7: Final state of embezzlement

infinitely many Bell states must be all 0, and a state cannot have all 0 Schmidt coefficients.

6.3 Embezzlement in the Commuting Operator Model

The failure of embezzling with tensor product leads us to consider embezzlement in the more general commuting operator model. While Alice and Bob cannot share infinitely many Bell states in the tensor product model, there is no such restriction in the commuting operator model.

Definition 6.3 (Embezzlement in Commuting Operators)**.** *Consider a quantum system with $\mathcal{H}_A \otimes \mathcal{H} \otimes \mathcal{H}_B$ as its Hilbert space, where $\mathcal{H}$ is the Hilbert space shared between Alice and Bob, and $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ are Alice and Bob's private Hilbert space of one qubit. Let $\mathbf{A} \subseteq \mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H})$ be Alice's set of operators, and $\mathbf{B} \subseteq \mathbb{B}(\mathcal{H} \otimes \mathbb{C}^2)$ be Bob's set of local operators such that for all $A \in \mathbf{A}, B \in \mathbf{B}$,*

$$(A \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes B) = (\mathcal{I}_2 \otimes B)(A \otimes \mathcal{I}_2). \tag{6.3.1}$$

Embezzlement in the commuting operator model is a protocol with a starting state

$|\psi\rangle \in \mathcal{H}$, *and local unitaries* $A \in \mathbf{A}$, $B \in \mathbf{B}$ *such that*

$$(A \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes B)\,|0\rangle \otimes |\psi\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\psi\rangle \otimes |0\rangle + |1\rangle \otimes |\psi\rangle \otimes |1\rangle\right). \quad (6.3.2)$$

The conditions for Equation 6.3.1 can be illustrated by the quantum circuit diagram in Figure 6.8.

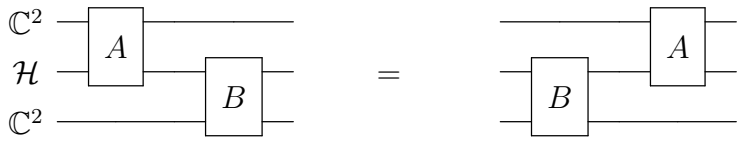


Figure 6.8: Operators That Commute for Embezzlement

The commuting operator protocol for embezzlement is illustrated by Figure 6.9.

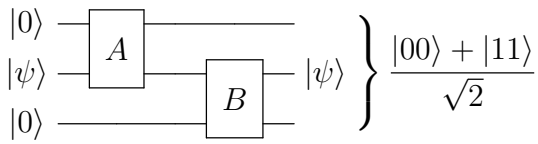


Figure 6.9: Commuting Operators Protocol for Embezzlement

Theorem 6.3. *Embezzlement in the commuting operator model can be achieved.*

We provide two proofs to the above theorem – a shorter existence proof based on C*-algebra and previous results from [8], and a longer constructive proof with the explicit protocol.

6.3.1 Existence of embezzlement protocol

The concept behind the existence proof of a perfect commuting operator strategy for embezzlement is the following. We first define an abstract C*-algebra that will capture the essence of Alice and Bob's commuting sets of operators for use for embezzlement. We then consider properties of abstract states on the C*-algebra that will allow the state and the C*-algebra can be converted into a commuting operator protocol for embezzlement. Finally, we show that such state exists by converting the result from about [8] approximate embezzlement into abstract states and taking the limit of those abstract states. In the framework set up by [8], a perfect embezzlement strategy cannot be achieved because the limit of their approximate embezzlement states does not exist. In the abstract state framework, the system is closed so the limiting state exists. By taking the abstraction, we convert an approximate tensor product strategy into an exact C*-algebra strategy, which in turn will can be converted into an exact commuting operator strategy.

We start by looking into defining an algebra we call $\mathcal{U}_2$ that behaves like 2×2 unitary over some algebras. To define $\mathcal{U}_2$, we need to get a good understanding of the structure of Alice and Bob's unitary operators. We first take a look at the breakdown of Alice's unitary operator $U \in \mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H})$.

$$U = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} = \sum_{i,j=0}^{1} |i\rangle \langle j| \otimes U_{ij}, \ U_{ij} \in \mathbb{B}(\mathcal{H}). \tag{6.3.3}$$

Since U is unitary, $UU^* = U^*U = \left(\begin{smallmatrix} \mathcal{I} & 0 \\ 0 & \mathcal{I} \end{smallmatrix}\right)$ so U_{ij} must satisfy the 8 constraints generated by

$$\begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \begin{pmatrix} U_{00}^* & U_{10}^* \\ U_{01}^* & U_{11}^* \end{pmatrix} = \begin{pmatrix} \mathcal{I} & 0 \\ 0 & \mathcal{I} \end{pmatrix} = \begin{pmatrix} U_{00}^* & U_{10}^* \\ U_{01}^* & U_{11}^* \end{pmatrix} \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}. \tag{6.3.4}$$

Similarly, Bob's unitary $V = \sum_{i,j=0}^{1} V_{ij} \otimes |i\rangle \langle j|$ needs to satisfy 8 similar constraints.

Moreover, in order for Alice and Bob's operators to commute,

$$(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) = (\mathcal{I}_2 \otimes V)(U \otimes \mathcal{I}_2). \tag{6.3.5}$$

Expanding the above equation to U_{ij} and V_{kl}, we get the following proposition.

Proposition 6.4. *Let $U \in \mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H})$ and $V \in \mathbb{B}(\mathcal{H} \otimes \mathbb{C}^2)$, and write $U = \sum_{i,j=0}^{1} |i\rangle \langle j| \otimes U_{ij}$, $V = \sum_{k,l=0}^{1} V_{kl} \otimes |k\rangle \langle l|$. Then $(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) = (\mathcal{I}_2 \otimes V)(U \otimes \mathcal{I}_2)$ if and only if $U_{ij}V_{kl} = V_{kl}U_{ij}$.*

Proof. We prove the equivalences by expanding the terms in the unitaries.

$$\begin{aligned}(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) &= \left(\sum_{i,j} |i\rangle \langle j| \otimes U_{ij} \otimes \mathcal{I}_2\right)\left(\sum_{k,l} \mathcal{I}_2 \otimes V_{kl} \otimes |k\rangle \langle l|\right) \\ &= \sum_{i,j,k,l} |i\rangle \langle j| \otimes U_{ij}V_{kl} \otimes |k\rangle \langle l| .\end{aligned} \tag{6.3.6}$$

Similarly,

$$(\mathcal{I}_2 \otimes V)(U \otimes \mathcal{I}_2) = \sum_{i,j,k,l} |i\rangle \langle j| \otimes V_{kl}U_{ij} \otimes |k\rangle \langle l| . \tag{6.3.7}$$

Equating Equation 6.3.6 with Equation 6.3.7 gives us $U_{ij}V_{kl} = V_{kl}U_{ij}$ as desired. □

We note that for any $AB = BA$ where A is invertible, $A^{-1}B = BA^{-1}$. Since U is unitary, $U^{-1} = U^*$ so $(U^* \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) = (\mathcal{I}_2 \otimes V)(U^* \otimes \mathcal{I}_2)$. This gives us $U_{ij}^* V_{kl} = V_{kl} U_{ij}^*$ for all $i, j, k, l \in \{0, 1\}$. This property is called $\{U_{ij}\}$ and $\{V_{kl}\}$ *-commute.

Next we dfine an algebra that is the abstraction of U_{ij} where $U = (U_{ij})$ is unitary.

Let $\mathcal{U}_2$ be a $*$-algebra generated by 1 and u_{ij} for $i, j \in \{0, 1\}$ satisfying

$$\begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{pmatrix} \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}. \tag{6.3.8}$$

Then there exists a $*$-homomorphism $\pi : \mathcal{U}_2 \to \mathbb{B}(\mathcal{H})$, $\pi(u_{ij}) = U_{ij}$ where $\sum_{i,j=0}^{1} |i\rangle \langle j| \otimes U_{ij}$ is a unitary. $\mathcal{U}_2$ captures all unitaries that can be broken down into 2×2 blocks of operators on $\mathcal{H}$.

To make $\mathcal{U}_2$ a C*-algebra. a norm needs to be defined. For $x \in \mathcal{U}_2$, let

$$\|x\| = \sup \{\|\pi(x)\| : \pi \text{ is a *-homomorphism}\}. \tag{6.3.9}$$

This is the norm we adopt to take the completion in and make $\mathcal{U}_2$ a C*-algebra.

We want our abstract algebra to capture the commutivity between Alice and Bob's operator U and V, or by Proposition 6.4, U_{ij} and V_{kl} must commute. To do this, we consider the C*-algebra $\mathcal{U}_2 \otimes_{\max} \mathcal{U}_2$. There exists a $*$-homomorphism $\pi : \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{B}(\mathcal{H})$ where

$$\pi(u_{ij} \otimes 1) = U_{ij}, \ \pi(1 \otimes v_{ij}) = V_{ij}, \tag{6.3.10}$$

such that $U = (U_{ij})$ and $V = (V_{ij})$ are unitaries, $U_{ij}V_{kl} = V_{kl}U_{ij}$ for all $i, j, k, l \in \{0, 1\}$.

Remark 6.3.1. We note that the generators of $\mathcal{U}_2$, u_{ij} themselves are not unitaries, but the 2×2 matrix containing them $\left(\begin{smallmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{smallmatrix}\right)$ is a unitary. Moreover, $\mathcal{U}_2 \otimes \mathcal{U}_2$ are mapped to the decomposed version of Alice and Bob's operators, which act on $\mathbb{B}(\mathcal{H})$ instead of $\mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H})$ for Alice and $\mathbb{B}(\mathcal{H} \otimes \mathbb{C}^2)$ for Bob.

With $\mathcal{U}_2 \otimes \mathcal{U}_2$ defined, we are equipped with the tool to prove the existence of perfect commuting operator strategy for embezzlement.

Theorem 6.5. *A perfect commuting operator strategy for embezzlement exists if and only if there exists a state* $s\colon \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{C}$ *where the following four conditions are satisfied.*

- $s(u_{00} \otimes u_{00}) = \frac{1}{\sqrt{2}}$
- $s(u_{10} \otimes u_{00}) = 0$
- $s(u_{00} \otimes u_{10}) = 0$
- $s(u_{10} \otimes u_{10}) = \frac{1}{\sqrt{2}}$.

To prove the existence of a perfect commuting operator strategy, we only need to show the only if the direction of the above theorem. For completeness, we will include the other direction of the proof as well.

Proof. ($\Leftarrow$) Assume there exists a state s satisfying the four equations listed above. Applying the GNS construction on $\mathcal{U}_2 \otimes \mathcal{U}_2$ and s, we get a $*$-homomorphism $\pi\colon \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{B}(\mathcal{H})$ and a state $|\psi\rangle \in \mathcal{H}$ such that for all i, j,

$$\pi(u_{ij} \otimes 1) = U_{ij},\ \pi(1 \otimes u_{kl}) = V_{kl}, U_{ij}V_{kl} = V_{kl}U_{ij} \tag{6.3.11}$$

and

$$\langle\psi| U_{ij}V_{kl} |\psi\rangle = s(u_{ij} \otimes v_{kl}). \tag{6.3.12}$$

Let $U = \sum_{i,j=0}^{1} |i\rangle\langle j| \otimes U_{ij}$ and $V = \sum_{kl=0}^{1} V_{kl} \otimes |k\rangle\langle l|$, then $(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) = (\mathcal{I}_2 \otimes V)(U \otimes \mathcal{I}_2)$, and U, V are unitaries. Because $s(u_{00} \otimes u_{00}) = s(u_{10} \otimes u_{10}) = \frac{1}{\sqrt{2}}$,

$$\begin{aligned} 1 &= |\langle\psi| U_{00}V_{00} |\psi\rangle|^2 + |\langle\psi| U_{10}V_{10} |\psi\rangle|^2 \\ &\leq \|U_{00}V_{00} |\psi\rangle\|^2 + \|U_{10}V_{10} |\psi\rangle\|^2 \\ &\leq \|U_{00}V_{00} |\psi\rangle\|^2 + \|U_{10}V_{10} |\psi\rangle\|^2 + \|U_{10}V_{00} |\psi\rangle\|^2 + \|U_{00}V_{10} |\psi\rangle\|^2. \end{aligned} \tag{6.3.13}$$

We note that $\{U_{00}V_{00}, U_{10}V_{00}, U_{00}V_{10}, U_{10}V_{10}\}$ is the entry of the first columns of the unitary $(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V)$. Applying $(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V)$ to $|0\rangle |\psi\rangle |0\rangle$ gives us

$$\| U_{00}V_{00} |\psi\rangle \|^2 + \| U_{10}V_{10} |\psi\rangle \|^2 + \| U_{10}V_{00} |\psi\rangle \|^2 + \| U_{00}V_{10} |\psi\rangle \|^2 = 1. \tag{6.3.14}$$

Combining Equation 6.3.13 with Equation 6.3.14, we get

$$\| U_{10}V_{00} |\psi\rangle \| = \| U_{00}V_{10} |\psi\rangle \| = 0 \Rightarrow U_{10}V_{00} |\psi\rangle = U_{00}V_{10} |\psi\rangle = 0; \tag{6.3.15}$$

as well as

$$\| U_{00}V_{00} |\psi\rangle \| = \| U_{10}V_{10} |\psi\rangle \| = | \langle\psi| U_{00}V_{00} |\psi\rangle | = | \langle\psi| U_{10}V_{10} |\psi\rangle | = \frac{1}{\sqrt{2}}, \tag{6.3.16}$$

which gives us $U_{00}V_{00} |\psi\rangle = U_{10}V_{10} |\psi\rangle = \frac{1}{\sqrt{2}} |\psi\rangle$. Therefore,

$$\begin{aligned} (U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) |0\rangle |\psi\rangle |0\rangle &= \sum_{ij} |i\rangle \otimes U_{i0}V_{j0} |\psi\rangle \otimes |j\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle |\psi\rangle |0\rangle + |1\rangle |\psi\rangle |1\rangle), \end{aligned} \tag{6.3.17}$$

which is in line with the perfect embezzlement protocol.

($\Rightarrow$) Assume that there exista perfect commuting operator protocol with $U \in \mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H})$, $V \in \mathbb{B}(\mathcal{H} \otimes \mathbb{C}^2)$ and $|\psi\rangle \in \mathcal{H}$ so that

$$(U \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V) |0\rangle |\psi\rangle |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle |\psi\rangle |0\rangle + |1\rangle |\psi\rangle |1\rangle). \tag{6.3.18}$$

Decompose U and V into $U = \sum_{ij} |i\rangle \langle j| \otimes U_{ij}$ and $V = \sum_{ij} V_{ij} \otimes |i\rangle \langle j|$. Define a $*$-homomorphism $\pi : \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{B}(\mathcal{H})$ to be $\pi(u_{ij} \otimes 1) = U_{ij}$ and $\pi(1 \otimes u_{ij} = V_{ij}$, and state $s : \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{C}$ to be $s(u_{ij} \otimes v_{kl}) = \langle\psi| U_{ij}V_{kl} |\psi\rangle$. Then from Equation 6.3.18, we have

$$U_{00}V_{00} |\psi\rangle = U_{10}V_{10} |\psi\rangle = \frac{1}{\sqrt{2}} |\psi\rangle, \; U_{10}V_{00} |\psi\rangle = U_{00}V_{10} |\psi\rangle = 0, \tag{6.3.19}$$

which in turn gives us

$$s(u_{00} \otimes u_{00}) = s(u_{10} \otimes u_{10}) = \frac{1}{\sqrt{2}},\ s(u_{10} \otimes u_{00}) = s(u_{00} \otimes u_{10}) = 0. \tag{6.3.20}$$

□

To finish up the existence proof, we need to show the aforementioned state s indeed exists.

Theorem 6.6. *There exists a state $s : \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{C}$ that satisfies the four equations in Theorem 6.5, and as a result, a perfect commuting operator strategy for embezzlement exists.*

Proof. In [8], the authors showed that for any integer n, there exists an n-dimensinoal Hilbert space $\mathcal{H}_n$, a state $|\psi_n\rangle \in \mathcal{H}_n$, as well as unitary operators $U_n \in \mathbb{B}(\mathbb{C}^2 \otimes \mathcal{H}_n)$ and $V_n \in \mathbb{B}(\mathcal{H}_n \otimes \mathbb{C}^2)$. such that

$$\|(U_n \otimes \mathcal{I}_2)(\mathcal{I}_2 \otimes V_n)(|0\rangle\,|\psi_n\rangle\,|0\rangle) - \frac{1}{\sqrt{2}}(|0\rangle\,|\psi_n\rangle\,|0\rangle + |1\rangle\,|\psi_n\rangle\,|1\rangle)\| < \frac{1}{n}. \tag{6.3.21}$$

These operators induce $*$-homomorphisms $\pi_n \colon \mathcal{U}_2 \to \mathcal{U}_2 \to \mathbb{B}(\mathcal{H}_n)$ together with a state $s : \mathcal{U}_2 \otimes \mathcal{U}_2 \to \mathbb{C}^2$ defined as $s(x) = \langle\psi_n|\,\pi_n(x)\,|\psi_n\rangle$. The state s_n then satisfy

- $|s_n(u_{00} \otimes u_{00}) - \frac{1}{\sqrt{2}}| < \frac{1}{n}$
- $|s_n(u_{10} \otimes u_{00})| < \frac{1}{n}$
- $|s_n(u_{00} \otimes u_{10})| < \frac{1}{n}$
- $|s_n(u_{10} \otimes u_{10}) - \frac{1}{\sqrt{2}}| < \frac{1}{n}$

The sequence of state $\{s_n\}$ leads to a limit of these states $s = \lim_{n\to\infty} s_n$. The limiting state s exists because a C*-algebra, $\mathcal{U}_2 \otimes \mathcal{U}_2$ in our case, is compact in the weak *-topology[1]. Since s is the limit of $\{s_n\}$, it will satisfy the four conditions in Theorem 6.5. □

6.3.2 Construction of embezzlement protocol

Recall that the state for embezzlement from the Hilbert Hotel intuition consists of infinitely many $|00\rangle$ pairs and infinitely many Bell pairs. To model it in with a Hilbert space, we consider a countably infinite-dimensional Hilbert space where all but finitely many qubits are fixed.

To model infinitely many $|00\rangle$ qubit pairs, let $x, y \in \mathbb{N}_0$ be integers in binary, and x_i, y_i are the i-th binary digits of x and y. We express a basis state as $|\cdots x_2 x_1 x_0, \cdots y_2 y_1 y_0\rangle$, or as $|x, y\rangle$, where x_i and y_i are the state of the i-th qubit for Alice and Bob.

Next, consider the infinitely many Bell basis states, where all but finitely many qubit pairs are in $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Instead of using the computational basis, we use the Bell basis as shown in Table 6.1 for each of the qubit pairs.

More succinctly, a basis state $|ab\rangle$ in the Bell basis is

$$\frac{1}{\sqrt{2}}|0b\rangle + \frac{1}{\sqrt{2}}(-1)^a|1\bar{b}\rangle. \tag{6.3.22}$$

in the computational basis, where $\bar{b}$ is the negation of the bit value of b.

[1]Let $\mathbf{A}$ be a C*-algebra and $S(\mathbf{A})$ denote the set of all states on $\mathbf{A}$ Then $S(\mathbf{A})$ is a convex set and is closed under weak *-topology, meaning any net of sates $\{s_\lambda\}$ converges to a state s if and only if $\lim_\lambda |s_\lambda(a) - s(a)| = 0$ for all $a \in \mathbf{A}$

Bell Basis	Computational basis
$\|00\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$
$\|01\rangle$	$\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$
$\|10\rangle$	$\frac{1}{\sqrt{2}}\|01\rangle - \frac{1}{\sqrt{2}}\|10\rangle$
$\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$

Table 6.1: Bell to Computational Basis

Again, let $x, y \in \mathbb{N}_0$ be two binary integers, but this time with negative indices $i \in \mathbb{Z}^-$. We denote a basis state as $|0.x_{-1}x_{-2}x_{-3}\cdots, 0.y_{-1}y_{-2}y_{-3}\cdots\rangle$ where x_{-j} and y_{-j} represent the state of the qubit pair in position $-j$ for Alice and Bob in the Bell basis. For example, the state $|0.0, 0.0\rangle$ is a state where all qubit pairs are in the state $|00\rangle$ of the Bell basis, or $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ in the computational basis; and the state $|0.01, 0.10\rangle$ is a state where qubit pair in position -1 are in state $|10\rangle$ of the Bell basis, which is $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, and qubit pair in position -2 are in state $|01\rangle$ of the Bell basis, which is $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$.

By taking the tensor product of the two aforementioned Hilbert spaces, we get a countably infinite-dimensional Hilbert space where half of the states are in the computational basis, and the other half are in the Bell basis. It is convenient to denote an orthonormal basis of this combined Hilbert space as

$$|\cdots x_2x_1x_0 \cdot x_{-1}x_{-2}\cdots, \cdots y_2y_1y_0 \cdot y_{-1}y_{-2}\cdots\rangle, \tag{6.3.23}$$

where x and y are two-way infinite binary strings with all but finitely many bits set to 0. The non-negative indices are qubits in the computational basis, and the negative indices are qubits in the Bell basis, separated by the centred dot as a marker.

This gives a state with infinitely many $|01\rangle$ in the computational basis on the left (non-negative indices), and infinitely many $|00\rangle$ in the Bell basis on the right (negative indices). The centred dot $\cdot$ is used as an indicator to separate between the computational and Bell basis.

To achieve embezzlement, we need to define operators that mimic the action of shifting and swapping qubits on the Hilbert space.

6.3.3 Left-shift operations

We start by considering the left-shift operator where all the qubits are shifted to the left by 1. First, let L_1 be the simple shift operation that moves the digits of x and y:

$$L_1 \left|\cdots x_2 x_1 x_0 \cdot x_{-1} x_{-2} \cdots , \cdots y_2 y_1 y_0 \cdot y_{-1} y_{-2} \cdots \right\rangle \tag{6.3.24}$$

$$= \left|\cdots x_1 x_0 x_{-1} \cdot x_{-2} x_{-3} \cdots , \cdots y_1 y_0 y_{-1} \cdot y_{-2} y_{-3} \cdots \right\rangle . \tag{6.3.25}$$

L_1 is a unitary because it is a permutation of the basis states. However, L_1 does not implement the desired left shift because the qubits in position -1 are in the Bell basis, but the qubits in position 0 are in the computational basis. L_1 simply moved the bit value without performing a basis conversion. To properly perform a left shift, a basis conversion at position 0 must be done.

Let L_2 be the operator that converts the 0th qubit pair from Bell to computational basis:

$$L_2 \left|\cdots x_2 x_1 x_0 \cdot x_{-1} x_{-2} \cdots , \cdots y_2 y_1 y_0 \cdot y_{-1} y_{-2} \cdots \right\rangle \tag{6.3.26}$$

$$= \frac{1}{\sqrt{2}} \left|\cdots x_2 x_1 0 \cdot x_{-1} x_{-2} \cdots , \cdots y_2 y_1 y_0 \cdot y_{-1} y_{-2} \cdots \right\rangle \tag{6.3.27}$$

$$+ \frac{1}{\sqrt{2}} (-1)^{x_0} \left|\cdots x_2 x_1 1 \cdot x_{-1} x_{-2} \cdots , \cdots y_2 y_1 \bar{y_0} \cdot y_{-1} y_{-2} \cdots \right\rangle . \tag{6.3.28}$$

L_2 is a unitary because it is a direct sum of 4×4 unitaries. Lastly, define $L = L_2L_1$ to be the left-shift operator, which is also a unitary since both L_1 and L_2 are unitaries.

L is a unitary that maps $|0.0, 0.0\rangle$ to $\frac{1}{\sqrt{2}}|0.0, 0.0\rangle + \frac{1}{\sqrt{2}}|1.0, 1.0; \rangle$, which is the overall effect we would like to achieve using after *both* Alice and Bob performed their left shift in the Hilbert Hotel model. Ideally, we would like to decompose L into two local (aka commuting) left-shift operations for Alice and Bob. However, it turns out that the Hilbert space has to be enlarged to accommodate local left shifts.

As shown in Figure 6.3, when Alice shifts all her qubits to the left by one, and Bob's qubits are unchanged, the indices of the Bell basis become misaligned. Consider $i \in \mathbb{Z}^-$. Before the shift, qubits in x_i and y_i are in the Bell basis; however, after the shift, qubits x_i and y_{i+1} are in the Bell basis instead. The new states in the misaligned basis are not in the original Hilbert space, since they have infinitely many misaligned Bell states, and cannot be expressed in terms of linear combinations of the original basis states.

Moreover, if Alice can perform a local left shift, she should also be allowed to perform it arbitrarily many times, as well as its inverse. Each time Alice performs a local left (or right) shift without Bob, the offset for the misalignment of the Bell basis changes. For example, performing the local left-shift r times will put qubit x_i and y_{i+r} in the Bell basis for all $i \in \mathbb{Z}^-$. As a result, the Hilbert space must be enlarged to accommodate states with any offset value.

Let $\mathcal{H}$ be a Hilbert space with an orthonormal basis $|r, x, y\rangle$, where $r \in \mathbb{Z}$ is the offset value, and x, y are the same two-way infinite binary strings defined earlier. The state $|r, x, y\rangle$ can be interpreted as the following. x_i and y_i are qubit pairs in the aligned basis (computational or Bell depending on the value of i). However, since

there is an offset between the alignment of the physical qubits, while y_i is the state of the i-th qubit for Bob, x_i is the state of the $i-r$-th qubit for Alice.

Define Alice's left shift L_A as

$$L_A|r, x, y\rangle = |r+1, x, y\rangle\,. \tag{6.3.29}$$

We extend the overall left-shift operation L_0 to this new Hilbert space by performing L_0 on x and y and leaving the offset r unchanged.

Since L_A and L act on different components of the Hilbert space, they commute. This allows us to define Bob's local left shift as

$$L_B = LL_A^*. \tag{6.3.30}$$

Alice's left shift changes the offset of the alignment of the Bell basis from r to $r+1$, and when Bob performs a left shift, this offset gets reversed from $r+1$ to r (which is the action of L_A^*), and the pair of qubits at index 0 changes from the Bell basis to the computational basis (which is the action of L).

6.3.4 Swap operations

The next step is to define the local operators that can swap out Alice and Bob's 0-th qubit in $\mathcal{H}$ with their local qubits in $\mathcal{H}_A$ and $\mathcal{H}_B$, as shown in Figure 6.6. We need to create operators that satisfy the correct commuting relation with L_A and L_B.

Let S_B be Bob's local swap defined as the local unitary acting on $\mathcal{H} \otimes \mathcal{H}_B$:

$$S_B\,|r, x, \cdots y_1 y_0 \cdot y_{-1} \cdots\rangle \otimes |t\rangle = |r, x, \cdots y_1 t \cdot y_{-1} \cdots\rangle \otimes |y_0\rangle\,. \tag{6.3.31}$$

S_B is clearly a unitary and commutes with $L_A \otimes \mathcal{I}_2$ since they act on different components of $|r, x, y\rangle$.

The corresponding Alice's swap is, however, more complicated. We start by considering the same naïve swap as Bob's. Let $\tilde{S}_A$ be the following unitary

$$\tilde{S}_A |s\rangle \otimes |r, \cdots x_1 x_0 \cdot x_{-1} \cdots, y\rangle = |x_0\rangle \otimes |r, \cdots x_1 s \cdot x_{-1} \cdots, y\rangle . \tag{6.3.32}$$

Recall that r is the offset for Alice's left shift, and as a result, x_0 does not describe the 0-th qubit in Alice's system: the state of Alice's 0-th qubit is described by x_{-r}. Performing the naïve swap directly will swap out the wrong qubit. Moreover, $\tilde{S}_A$ does not commute with L_B. To correctly swap out Alice's qubit in position 0, we first define the controlled-L, denoted as C, acting on $\mathcal{H}$ as the following:

$$C |r, x, y\rangle = L^r |r, x, y\rangle . \tag{6.3.33}$$

C is a unitary since each L^r is unitary, and C is a direct sum of all L^r. Essentially, applying C to $|r, x, y\rangle$ re-aligns Alice's physical qubit location with the corresponding index of the state.

Define Alice's actual swap as

$$S_A = (\mathcal{I}_2 \otimes C^*)\tilde{S}_A(\mathcal{I}_2 \otimes C). \tag{6.3.34}$$

It is clear that S_A is unitary. The last step is to show that S_A commutes with S_B and L_B. Since the effect of S_A is localized to Alice's qubits and the effect of S_B is localized to Bob's qubits, S_A must commute with S_B.

Next, we consider a basis state $|s\rangle \otimes |r, x, y\rangle \in \mathcal{H}_A \otimes \mathcal{H}$. Since $\tilde{S}_A$ is independent

of the value of r, $\tilde{S}_A$ commutes with $\mathcal{I} \otimes L_A$,

$$S_A(\mathcal{I}_2 \otimes L_B)\,|s\rangle \otimes |r,x,y\rangle = (\mathcal{I}_2 \otimes C^*)\tilde{S}_A(\mathcal{I}_2 \otimes CL_B)\,|s\rangle \otimes |r,x,y\rangle \tag{6.3.35}$$

$$= (\mathcal{I}_2 \otimes C^*)\tilde{S}_A(\mathcal{I}_2 \otimes CL)\,|s\rangle \otimes |r-1,x,y\rangle \tag{6.3.36}$$

$$= (\mathcal{I}_2 \otimes L^{1-r})\tilde{S}_A(\mathcal{I}_2 \otimes L^r)\,|s\rangle \otimes |r-1,x,y\rangle \tag{6.3.37}$$

$$= (\mathcal{I}_2 \otimes L^{1-r})\tilde{S}_A(\mathcal{I}_2 \otimes L^r L_A^*)\,|s\rangle \otimes |r,x,y\rangle \tag{6.3.38}$$

$$= (\mathcal{I}_2 \otimes LL_A^*L^{-r})\tilde{S}_A(\mathcal{I}_2 \otimes L^r)\,|s\rangle \otimes |r,x,y\rangle \tag{6.3.39}$$

$$= (\mathcal{I}_2 \otimes L_BC^*)\tilde{S}_A(\mathcal{I}_2 \otimes C)\,|s\rangle \otimes |r,x,y\rangle \tag{6.3.40}$$

$$= (\mathcal{I}_2 \otimes L_B)S_A\,|s\rangle \otimes |r,x,y\rangle\,. \tag{6.3.41}$$

This shows that S_A commutes with $\mathcal{I}_2 \otimes L_B$, and as a result it is a valid operator for Alice.

6.3.5 The protocol

The last step is to put everything together to create the protocol for embezzlement. Alice and Bob start with the shared state $|0,0.0,0.0\rangle$, apply L_A and L_B, then swap out qubits in position 0 of $\mathcal{H}$ with $\mathcal{H}_A$ and $\mathcal{H}_B$ using S_A and S_B. Alice's operation is $U_A = S_AL_A$, and Bob's operation is $U_BS_BL_B$. U_A and U_B clearly commute, and the evolution of the state during the protocol is:

0. Initial state: $|0\rangle \otimes |0,0.0,0.0\rangle \otimes |0\rangle$
1. after L_AL_B: $|0\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0,0.0,0.0\rangle + \frac{1}{\sqrt{2}}\,|0,1.0,1.0\rangle\right) \otimes |0\rangle$
2. after S_AS_B: $\frac{1}{\sqrt{2}}\,|0\rangle \otimes |0,0.0,0.0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \otimes |0,0.0,0.0\rangle \otimes |1\rangle$

This completes the embezzlement protocol in the commuting operator framework.

On the surface, converting the state $|0\rangle \otimes |0, 0.0, 0.0\rangle \otimes |0\rangle$ to $\frac{1}{\sqrt{2}} |0\rangle \otimes |0, 0.0, 0.0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes |0, 0.0, 0.0\rangle \otimes |1\rangle$ might appear to be too simple and perhaps almost as if we are somehow "cheating". However, the carefully defined left shift L_A and L_B are performing all the necessary hard work behind the scene such as the basis transformation from the Bell to computational basis. This basis change is critical to embezzlement as it ensures that the state $|0, 0.0, 0.0\rangle$ is not a simple separable state, but a rather state with infinitely many Bell basis hidden in it.

6.4 Embezzlement in the C*-model

While the evolution of the state for the embezzlement protocol at the end was relatively simple, the construction of the states and operators was far less straightforward. Starting from a simple idea of shift and swap, one may even find the final construction overly convoluted. After all, the construction had to handle a direct sum of infinitely many infinite-dimensional Hilbert spaces arising from the local shift offset, changing between computational basis and Bell basis at the correct position, keeping track of the difference between the position of physical qubits and logical indices, as well as making sure that the correct commutation relation is satisfied. While we are not excluding the possibility that a simpler protocol for embezzlement may exist, the protocol above is a relatively straightforward reflection of the idea behind embezzlement based on the Hilbert Hotel's intuition. However, if we consider the C*-model, we can come up with a cleaner solution for embezzlement.

The work with the C*-model, we need first to find a reasonable definition for embezzlement. Recall that in the C*-model, Alice and Bob each own some C*-algebra,

and a shared state is an abstract state acting on the tensor product of the two C*-algebras.[2] To perform embezzlement, we first define the C*-algebra corresponding to the single-qubit state.

Let $\mathbb{M}_2 := \mathbb{B}(\mathbb{C}^2)$ be the algebra of 2×2 matrices, corresponding to single qubits. Let $s_0 : \mathbb{M}_2 \to \mathbb{C}$ be a state that corresponds to $|0\rangle$: for all $M \in \mathbb{M}_2$,

$$s_0(M) = \langle 0| M |0\rangle . \tag{6.4.1}$$

Define $s_{\text{bell}} : \mathbb{M}_2 \otimes \mathbb{M}_2 \to \mathbb{C}$ two be the two-qubit state corresponding to the Bell state: for any $M, N \in \mathbb{M}_2$,

$$s_{\text{bell}}(M \otimes N) = \frac{1}{2}[(\langle 00| + \langle 11|)M \otimes N(|00\rangle + |11\rangle)]. \tag{6.4.2}$$

Definition 6.4. *Embezzlement under the C*-model is a protocol with two C*-algebras $\mathcal{A}$ and $\mathcal{B}$, an abstract state $s : \mathcal{A} \otimes \mathcal{B} \to \mathbb{C}$, and *-automorphisms $\alpha_A : \mathbb{M}_2 \otimes \mathcal{A} \to \mathbb{M}_2 \otimes \mathcal{A}$, $\alpha_B : \mathbb{M}_2 \otimes \mathcal{B} \to \mathbb{M}_2 \otimes \mathcal{B}$,[3] such that for all $M, N \in \mathcal{M}_2$, $A \in \otimes\mathcal{A}$, $B \in \otimes\mathcal{B}$,*

$$(s_0 \otimes s_0 \otimes s)(\alpha_A \otimes \alpha_B(M \otimes N \otimes A \otimes B)) = s_{bell}(M \otimes N) \otimes s(A \otimes B). \tag{6.4.3}$$

Knowing that embezzlement can be achieved in the commuting operator model, it is not surprising that,

Theorem 6.7. *Embezzlement protocol can be achieved in the C*-model.*

[2] We will not get into the discussion of which tensor product should be used to define the protocol, since our protocol uses CAR-algebra as the local C*-algebras, and all the tensor product between CAR-algebras are the same. In the definition, $\otimes$ between two C*-algebras can be any tensor product.

[3] To simplify the expression, we let $\alpha_A \otimes \alpha_B$ act on $\mathbb{M}_2 \otimes \mathbb{M}_2 \otimes \mathcal{A} \otimes \mathcal{B}$ instead of $\mathbb{M}_2 \otimes \mathcal{A} \otimes \mathbb{M}_2 \otimes \mathcal{B}$ where the location of the center two C*-algebras are swapped. α_A acts on the first and third C*-algebra and α_B acts on the second and fourth C*-algebra in the tensor product.

6.4.1 The state

Recall that a CAR algebra $\mathcal{C}$ is a C*-algebra that consists of infinitely many Paulis with finite weight, and can be used to describe a quantum system with infinitely many qubits. Let $\mathcal{C}$ be a CAR algebra. Similar to the construction in the commuting operator framework, we first consider the state that corresponds to infinitely many $|00\rangle$ states and infinitely many Bell states.

Let $s_{00} : \mathcal{C} \otimes \mathcal{C} \to \mathbb{C}$ be an abstract state where for any $X^a Z^b, X^c Z^d \in \mathcal{C}$,

$$s_{|00\rangle}(X^a Z^b \otimes X^c Z^d) = \prod_{i=0}^{\infty} \langle 00| X^{a_i} Z^{b_i} \otimes X^{c_i} Z^{d_i} |00\rangle . \tag{6.4.4}$$

The two CAR algebras will be part of Alice and Bob's local C*-algebras.

Similarly, let $s_{|\psi\rangle} : \mathcal{C} \otimes \mathcal{C} \to \mathbb{C}$ be an abstract state where for any $X^a Z^b, X^c Z^d \in \mathcal{C}$,

$$s_{|\psi\rangle}(X^a Z^b \otimes X^c Z^d) = \prod_{i=0}^{\infty} \langle \psi| X^{a_i} Z^{b_i} \otimes X^{c_i} Z^{d_i} |\psi\rangle \tag{6.4.5}$$

where $|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Again, the first CAR algebra belongs to Alice and the second CAR algebra belongs to Bob.

To combine the two, consider the C*-algebra $\mathcal{A} = \mathcal{B} = \mathcal{C} \otimes \mathcal{C}$, which is also a CAR algebra. Consider $X^a Z^b \in \mathcal{A}$. For a and b, instead of using binary strings with natural numbers as indices, we use two-way infinite binary strings where its indices are integers. The non-negative indices are the qubits in the computational basis, and the negative indices are the qubits in the Bell basis. Let $s : \mathcal{A} \otimes \mathcal{B} \to \mathbb{C}$ be an abstract state where for any $X^a Z^b \in \mathcal{A}, X^c Z^d \in \mathcal{B}$,

$$s(X^a Z^b \otimes X^c Z^d) = \prod_{i=0}^{\infty} \langle 00| X^{a_i} Z^{b_i} \otimes X^{c_i} Z^{d_i} |00\rangle \prod_{i=-1}^{-\infty} \langle \psi| X^{a_i} Z^{b_i} \otimes X^{c_i} Z^{d_i} |\psi\rangle . \tag{6.4.6}$$

Essentially, s is $s_{|00\rangle} \otimes s_{|\psi\rangle}$ where the CAR algebras are rearranged in different order. We let $\mathcal{A}$ be Alice's C*-algebra and $\mathcal{B}$ be Bob's C*-algebra.

6.4.2 The local operators

The next step is to define the $*$-automorphisms that correspond to shifting and swapping out qubits.

The goal of the shift is to move the qubit pairs in the direction such that the qubit at index 0 converts from $|00\rangle$ to a Bell state. Based on the state s defined above, qubit i needs to be shifted to qubit $i+1$. Shifting the index of the qubit up by one is equivalent to shifting the index of the operators down by one.

Let Σ be the set of all two-way infinite (integer indices) binary strings with finitely many 1's. Let $\pi : \Sigma \to \Sigma$ be the following shift operation: for all $a \in \Sigma$, $\pi(a)_i = a_{i+1}$. Let $\alpha_\pi : \mathcal{A} \to \mathcal{A}$ be a linear map such that for all $X^a Z^b \in \mathcal{A}$,

$$\alpha_\pi(X^a Z^b) = X^{\pi(a)} X^{\pi(b)}. \tag{6.4.7}$$

It is not difficult to see that α_π is a $*$-automorphism. $*$ preservation: $\alpha_\pi(X^a Z^b)^* = X^{\pi(a)} X^{\pi(b)} = \alpha_\pi((X^a Z^b)^*)$; existence of inverse: $\alpha_\pi^{-1}(X^a Z^b) = X^{\pi^{-1}(a)} Z^{\pi^{-1}(b)}$ where $\pi^{-1}(a)_i = a_{i-1}$. To show that it is a homomorphism, we use the fact that α_π is a bit-wise operation.

Since X and Z anti-commute, $X^a Z^b = (-1)^{f(a,b)} Z^b X^a$. $f : \Sigma \times \Sigma \to \{0,1\}$ can be defined as $f(a,b) = \bigoplus_{i=0}^{\infty} a_i \wedge b_i$, where $\wedge$ and $\oplus$ are the binary operators AND

and XOR. It is clear that $f(a,b) = f(\pi(a), \pi(b))$ for all a, b. For $X^a Z^b, X^c Z^d \in \mathcal{C}$,

$$\alpha_\pi(X^a Z^b X^c Z^d) = (-1)^{f(b,c)} \alpha_\pi(X^{a\oplus c} Z^{b\oplus d}) \tag{6.4.8}$$

$$= (-1)^{f(\pi(b),\pi(c))} X^{\pi(a)} X^{\pi(c)} Z^{\pi(b)} Z^{\pi(d)} \tag{6.4.9}$$

$$= X^{\pi(a)} Z^{\pi(b)} X^{\pi(c)} Z^{\pi(d)} \tag{6.4.10}$$

$$= \alpha_\pi(X^a Z^b) \alpha_\pi(X^c Z^d). \tag{6.4.11}$$

α_π is the local shift operation for both Alice and Bob. ($\mathcal{A} = \mathcal{B}$ so α_π is also defined for Bob).

The swap operation is exactly as one might expect. We use a different a font a, b to denote single bits while a, b are infinite strings. Let $\alpha_{\text{swap}} : \mathbb{M}_2 \otimes \mathcal{A}$ be a linear map such that for any $X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^a Z^b \in \mathbb{M}_2 \otimes \mathcal{A}$, $\mathsf{a}, \mathsf{b} \in \{0,1\}$, $a, b \in \sigma$

$$\alpha_{\text{swap}}(X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^a Z^b) = X^{a_0} Z^{b_0} \otimes X^{a'} Z^{b'} \tag{6.4.12}$$

where

$$a'_0 = \mathsf{a},\ b'_0 = \mathsf{b} \text{ and } a'_i = a_i,\ b'_i = b_i \text{ for } i \neq 0. \tag{6.4.13}$$

It is clear that α_{swap} preserves $*$, and it is its own inverse. The proof for α_{swap} being a homomorphism is almost exactly the same as the proof for α_π:

$$\alpha_{\text{swap}}((X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^a Z^b)(X^{\mathsf{c}} Z^{\mathsf{d}} \otimes X^c Z^d)) \tag{6.4.14}$$

$$= (-1)^{\mathsf{b}\oplus\mathsf{c}\oplus f(b,c)} X^{a_0} X^{c_0} Z^{b_0} Z^{d_0} \otimes X^{a'} X^{c'} Z^{b'} Z^{d'} \tag{6.4.15}$$

$$= (-1)^{b_0\oplus c_0\oplus f(b',c')} X^{a_0} X^{c_0} Z^{b_0} Z^{d_0} \otimes X^{a'} X^{c'} Z^{b'} Z^{d'} \tag{6.4.16}$$

$$= X^{a_0} Z^{b_0} X^{c_0} Z^{d_0} \otimes X^{a'} Z^{b'} X^{c'} Z^{d'} \tag{6.4.17}$$

$$= \alpha_{\text{swap}}(X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^a Z^b) \alpha_{\text{swap}}(X^{\mathsf{c}} Z^{\mathsf{d}} \otimes X^c Z^d). \tag{6.4.18}$$

Again, α_{swap} is the local swap operation for Alice and Bob.

6.4.3 The protocol

Let $\alpha_A = \alpha_B = (\mathcal{I} \otimes \alpha_\pi) \circ \alpha_{\text{swap}}$. The last step is to show that the state s and the $*$-automorphisms indeed achieve embezzlement. We start by applying the $*$-automorphism on generators of the C*-algebra,

$$\alpha_A \otimes \alpha_B(X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^{\mathsf{c}} Z^{\mathsf{d}} \otimes X^a Z^b \otimes X^c Z^d) \tag{6.4.19}$$

$$= (\mathcal{I} \otimes \mathcal{I} \otimes \alpha_\pi \otimes \alpha_\pi)(\alpha_{\text{swap}} \otimes \alpha_{\text{swap}}(X^{\mathsf{a}} Z^{\mathsf{b}} \otimes X^{\mathsf{c}} Z^{\mathsf{d}} \otimes X^a Z^b \otimes X^c Z^d)) \tag{6.4.20}$$

$$= X^{a_0} Z^{b_0} \otimes X^{c_0} Z^{d_0} \otimes \alpha_\pi(X^{a'} Z^{b'}) \otimes \alpha_\pi(X^{c'} Z^{d'}) \tag{6.4.21}$$

$$= X^{a_0} Z^{b_0} \otimes X^{c_0} Z^{d_0} \otimes X^{\pi(a')} Z^{\pi(b')} \otimes X^{\pi(c')} Z^{\pi(d')}. \tag{6.4.22}$$

Finally by applying the state $s_0 \otimes s_0 \otimes s$ to the resulting element, we show that

embezzlement is indeed achieved:

$$s_0 \otimes s_0 \otimes s(X^{a_0}Z^{b_0} \otimes X^{c_0}Z^{d_0} \otimes X^{\pi(a')}Z^{\pi(b')} \otimes X^{\pi(c')}Z^{\pi(d')}) \tag{6.4.23}$$

$$= \langle 0| X^{a_0}Z^{b_0} |0\rangle \langle 0| X^{c_0}Z^{d_0} |0\rangle$$
$$\prod_{i=0}^{\infty} \langle 00| X^{a'_{i+1}}Z^{b'_{i+1}} \otimes X^{c'_{i+1}}Z^{d'_{i+1}} |00\rangle$$
$$\prod_{i=-1}^{-\infty} \langle \psi| X^{a'_{i+1}}Z^{b'_{i+1}} \otimes X^{c'_{i+1}}Z^{d'_{i+1}} |\psi\rangle \tag{6.4.24}$$

$$= \langle 0| X^{a_0}Z^{b_0} |0\rangle \langle 0| X^{c_0}Z^{d_0} |0\rangle \qquad \text{(Change of indices)}$$
$$\prod_{i=1}^{\infty} \langle 00| X^{a'_i}Z^{b'_i} \otimes X^{c'_i}Z^{d'_i} |00\rangle$$
$$\prod_{i=0}^{-\infty} \langle \psi| X^{a'_i}Z^{b'_i} \otimes X^{c'_i}Z^{d'_i} |\psi\rangle \tag{6.4.25}$$

$$= \langle 0| X^{a_0}Z^{b_0} |0\rangle \langle 0| X^{c_0}Z^{d_0} |0\rangle \qquad \text{(By Eq 6.4.13)}$$
$$\prod_{i=1}^{\infty} \langle 00| X^{a_i}Z^{b_i} \otimes X^{c_i}Z^{d_i} |00\rangle$$
$$\langle \psi| X^{\mathsf{a}}Z^{\mathsf{b}} \otimes X^{\mathsf{c}}Z^{\mathsf{d}} |\psi\rangle \prod_{i=-1}^{-\infty} \langle \psi| X^{a_i}Z^{b_i} \otimes X^{c_i}Z^{d_i} |\psi\rangle \tag{6.4.26}$$

$$= \prod_{i=0}^{\infty} \langle 00| X^{a_i}Z^{b_i} \otimes X^{c_i}Z^{d_i} |00\rangle \qquad \text{(Change of indices)}$$
$$\prod_{i=-1}^{-\infty} \langle \psi| X^{a_i}Z^{b_i} \otimes X^{c_i}Z^{d_i} |\psi\rangle \langle \psi| X^{\mathsf{a}}Z^{\mathsf{b}} \otimes X^{\mathsf{c}}Z^{\mathsf{d}} |\psi\rangle \tag{6.4.27}$$

$$= s_{\text{bell}} \otimes s(X^{\mathsf{a}}Z^{\mathsf{b}} \otimes X^{\mathsf{c}}Z^{\mathsf{d}} \otimes X^{a}Z^{b} \otimes X^{c}Z^{d}). \tag{6.4.28}$$

This shows that we indeed end up with a Bell state and a copy of the original state, which finishes our embezzlement protocol.

6.5 Comments on embezzlement

We showed that embezzlement cannot be achieved perfectly in the tensor product model, but can be achieved under the commuting operator and the C*-model. In the commuting operator model, the embezzlement protocol requires careful manipulation of the Hilbert spaces and the operators. As one might have noticed, Alice and Bob's full set of commuting operators was never defined. The only operator defined in the protocol is the shift and swap operators. There is no information on what Alice and Bob could perform as measurements on their joint Hilbert space. Since in the commuting operator framework, the notion of locality depends solely on the commuting sets of operators, the lack of fully defined commuting sets of operators makes the description of locality in this quantum system incomplete. One natural question is, given the missing information, is there actually an infinite amount of entanglement in the shared state between Alice and Bob? To put it more bluntly, is it possible that Alice and Bob (well, the author) cheated in this protocol? Luckily, even with incomplete information, this protocol achieved something that was not achievable with a finite amount of entanglement. In particular, the following restrictions made sure that an infinite amount of entanglement must exist in the protocol even with very few operators defined.

1. Alice and Bob need to convert a product state to a Bell state.
2. The only allowed operators are local unitaries
3. The shared state must remain unchanged after the protocol.

Condition 2 ensures that the total amount of entanglement between Alice and Bob cannot change, while Condition 1 and 3 forces the shared amount of entanglement

to increase by a constant amount. If the total amount of entanglement is finite, increasing it by a constant amount would violate Condition 2. Satisfying all three conditions at the same time ensures that the shared state must capture some form of infinite entanglement.

In contrast, the C*-model has a more complete description of the quantum system. The set of measurements operators Alice and Bob can perform on any state is defined by the CAR algebra. A lot of the work done to show how embezzlement works in the C*-model is to show that these local measurement operators are still well defined and behave as one would expect them to.

Moreover, as discussed earlier, in the commuting operator framework, the state $|0, 0.0, 0.0\rangle$ contains infinitely many Bell basis. This is not obvious by looking at the state itself and only becomes apparent when the left shift operators are applied. In the C*-model, the fact that the state s contains infinitely many Bell basis is clear from its definition.

The Hilbert space $\mathcal{H}$ in the commuting operator framework only accepts states that have a particular structure that can be expressed in terms of finite non-zero binary strings in the computational basis and the Bell basis and their shifted versions. A state that has infinitely many $|11\rangle$ on the left in the computational basis, for example, is not part of the Hilbert space. In the C*-model, in contrast, there is more freedom to what a state can be; the aforementioned state that was outside the Hilbert space in the commuting operator model can be easily defined in the C*-model. The only catch is that if multiple states are defined in the C*-model when converting it to the commuting operator model, the GNS construction may need to be applied to each state and the resulting Hilbert space will have to be a direct sum of all the Hilbert spaces arising from different states.

Chapter 7

Self-embezzlement

In essence, embezzlement of entanglement is a protocol that extracts a Bell state from a state containing infinitely many Bell states. It matches with the intuition that infinity plus one is still infinity. Naturally, one may wonder, since infinity plus infinity is also infinity, whether it is possible to create a protocol that turns infinitely many Bell states into two copies of the same state. This is answered by studying the problem of self-embezzlement [7]. Self-embezzlement has a very interesting property that while it is possible to come up with a protocol under the commuting operator and the C*-model, no protocol under the tensor product of the Hilbert space model exists to approximate it. This in turn shows a gap between the tensor product of the Hilbert space model and the commuting operator model. Another protocol with the similar property of a gap between the tensor product and the commuting operator model is the task of steering studied in [21].

7.1 Definitions of Self-embezzlement

Self-embezzlement is a variation of embezzlement. Instead of creating a single pair of Bell states locally using some resource state as a catalyst, the goal is to create a copy of the resource catalyst state using only local operations. In other words, self-embezzlement turns a state $|\psi\rangle \otimes |00\rangle$ into $|\psi\rangle \otimes |\psi\rangle$ with local operations. If $|\psi\rangle$ is a product state, self-embezzlement is trivial. Therefore, we require $|\psi\rangle$ to contain some non-trivial amount of entanglement for self-embezzlement. Informally, self-embezzlement must satisfy the following conditions.

1. Alice and Bob each have two quantum systems A_1, A_2, B_1, and B_2. $(\mathsf{A}_1, \mathsf{A}_2)$ is the joint local system for Alice and $(\mathsf{B}_1, \mathsf{B}_2)$ is the joint local system for Bob.

2. There is a resource (catalyst) state $|\psi\rangle$ on the joint system $(\mathsf{A}_1, \mathsf{B}_1)$, and $|\psi\rangle$ is non-trivially entangled. More specifically, $|\psi\rangle$ must be able to maximally violate the CHSH inequality by a factor of $\sqrt{2}$ across A_1 and B_1.

3. The initial state shared between Alice and Bob is $|\psi\rangle$ on $(\mathsf{A}_1, \mathsf{B}_1)$, some state $|\phi_A\rangle$ on A_2 and $|\phi_B\rangle$ on B_2. We denote this by $|\psi\rangle \otimes |\phi_A\rangle \otimes |\phi_B\rangle$

4. Alice and Bob are allowed to perform local operations on their local systems.

5. The final state after their local operations is $|\psi\rangle$ on $(\mathsf{A}_1, \mathsf{B}_1)$, and $|\psi\rangle$ on $(\mathsf{A}_2, \mathsf{B}_2)$, denoted by $|\psi\rangle \otimes |\psi\rangle$.

Approximate self-embezzlement is the same as above, except it allows $|\psi\rangle$ to violate the CHSH inequality by a factor $\sqrt{2}-\epsilon$, and the final state to be an approximation of $|\psi\rangle \otimes |\psi\rangle$ with fidelity $1 - \epsilon$.

Based on the above principles, we can define self-embezzlement in the conventional tensor product model, the commuting operator model, as well as the C*-model.

7.1.1 Tensor product model

We start by defining what self-embezzlement is in the tensor product mode.

Definition 7.1. *A self-embezzling scheme is a tuple of the form* $(\mathcal{H}_A, \mathcal{H}_B, |\psi\rangle, |\phi_A\rangle, |\phi_B\rangle, U_A, U_B)$ *where*

1. $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *are Hilbert spaces (for quantum system* A_i *and* B_i*,* $i \in \{1, 2\}$*).*
2. $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ *is a state (unit vector) that violates the CHSH inequality by factor* $\sqrt{2} - \epsilon$*.*
3. $|\phi_A\rangle \in \mathcal{H}_A$*,* $|\phi_B\rangle \in \mathcal{H}_B$ *are two quantum states.*
4. $U_A \in \mathbb{B}(\mathcal{H}_A \otimes \mathcal{H}_A)$ *is a unitary, and* $U_B \in \mathbb{B}(\mathcal{H}_B \otimes \mathcal{H}_B)$ *is a unitary.*
5. *Let* $\Pi(U_A \otimes U_B)$ *be the unitary* $U_A \otimes U_B$ *acting on* $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A \otimes \mathcal{H}_B$ *where the order of the center two Hilbert spaces are swapped.* [1]
6. *Applying* $\Pi(U_A \otimes U_B)$ *on* $|\psi\rangle \otimes |\phi_A\rangle \otimes |\phi_B\rangle$ *results in the state* $|\psi\rangle \otimes |\psi\rangle$*.*

If we change Condition 6 to the following, we have the definition of an ϵ-approximate self-embezzlement scheme.

6'. Applying $\Pi(U_A \otimes U_B)$ on $|\psi\rangle \otimes |\phi_A\rangle \otimes |\phi_B\rangle$ yields a state within fidelity $1 - \epsilon$ to $|\psi\rangle \otimes |\psi\rangle$.

[1] Π does not have any physical implication; it is only a notation to ensure that the unitaries are acting on the intended quantum systems.

7.1.2 C*-model

We can define self-embezzlement in the C*-model similar to the definition of it in the tensor product model.

Definition 7.2. *A self-embezzling scheme is 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 corresponding to (respective) quantum systems* A_i *and* B_i, $i \in \{1, 2\}$.

2. $\psi \colon \mathcal{A} \otimes_{\min} \mathcal{B} \to \mathbb{C}$ *is a pure abstract state that violates the CHSH inequality by factor* $\sqrt{2}$.

3. $\phi_A : \mathcal{A} \to \mathbb{C}$, $\phi_B : \mathcal{B} \to \mathbb{C}$ *are two pure abstract states.*

4. $\alpha_A : \mathcal{A} \otimes_{\min} \mathcal{A} \to \mathcal{A} \otimes_{\min} \mathcal{A}$ *and* $\alpha_B : \mathcal{B} \otimes_{\min} \mathcal{B} \to \mathcal{B} \otimes_{\min} \mathcal{B}$ *are two* $*$*-automorphisms.*[2]

5. *Let* $\Pi(\alpha_A \otimes \alpha_B)$ *be the* $*$*-automorphism applied on* $\mathcal{A} \otimes_{\min} \mathcal{B} \otimes_{\min} \mathcal{A} \otimes_{\min} \mathcal{B}$ *where the center two C*-algebras are swapped.*

6. *Applying* $\Pi(\alpha_A \otimes \alpha_B)$ *maps the state* $\psi \otimes \phi_A \otimes \phi_B$ *to* $\psi \otimes \psi$.

The main difference between the tensor product model and the C*-model, apart from the abstraction, is that the evolution operator of the state in the C*-model are local $*$-automorphisms instead of local unitaries.

[2]We choose to adopt the min tensor product in this definition to make the definition of self-embezzlement as restrictive as possible. This is not an issue since under the min tensor product, self-embezzlement is achievable.

7.1.3 Complications in the Commuting Operator Model

While the definition of self-embezzlement under the tensor product model and the C*-model have a lot of similarities, it is more involved to define self-embezzlement in the commuting operator model properly. There is only one Hilbert space $\mathcal{H}$ in the commuting operator model. To describe the four quantum systems $\mathsf{A}_1, \mathsf{A}_2, \mathsf{B}_1, \mathsf{B}_2$, there must be four corresponding set of operators that mutually commute, denoted by $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{B}_1$, $\mathbf{B}_2$.

In order for the final state $|\psi\rangle \otimes |\psi\rangle$ to make sense, $(\mathsf{A}_1, \mathsf{B}_1)$ must share the same structure as $(\mathsf{A}_2, \mathsf{B}_2)$ so that the state $|\psi\rangle$ can exist on both joint systems. In the previous two definitions, this was achieved using the same underlying mathematical model to describe the systems; $\mathcal{H}_A$ for both A_1 and A_2, $\mathcal{H}_B$ for both B_1 and B_2 for example.

In the commuting operator model, however, $\mathbf{A}_1$ and $\mathbf{A}_2$ are two individual sets of operators on $\mathcal{H}$ that mutually commute. So we need a way to express the fact that $\mathbf{A}_1$ and $\mathbf{A}_2$ share the same structure. (Of course, the same property must also apply to $\mathbf{B}_1$ and $\mathbf{B}_2$.)

Moreover, we need to consider how to define the allowed set of operators on joint systems, such as $(\mathsf{A}_1, \mathsf{A}_2)$, in the commuting operator framework.

To address the problem where $\mathbf{A}_1$ and $\mathbf{A}_2$ must share the same structure, we require $\mathbf{A}_1$ and $\mathbf{A}_2$ to be $*$-isomorphisms.

Define $S_A : \mathbf{A}_1 \to \mathbf{A}_2$ to be the $*$-isomorphism between $\mathbf{A}_1$ and $\mathbf{A}_2$, then $A_1 \in \mathbf{A}_1$ gets mapped to its equivalent $S_A(A_1) \in \mathbf{A}_2$. Similarly, we require $\mathbf{B}_1$ to be isomorphic to $\mathbf{B}_2$ with $*$-isomorphism $S_B : \mathbf{B}_1 \to \mathbf{B}_2$.

To properly define states for self-embezzlement, we need to consider the following properties of states in a commuting operator model. Some of these definitions are also discussed in Section 3.2.

Definition 7.3 (State with Bell Pair)**.** *Let* $\mathbf{A}, \mathbf{B} \in \mathbb{B}(\mathcal{H})$ *be two mutually commuting sets of operators. A state* $|\psi\rangle \in \mathcal{H}$ *is said to contain at least one maximally entangled pair of qubits over* $\mathbf{A}$ *and* $\mathbf{B}$ *if there exist operators in* $\mathbf{A}$ *and* $\mathbf{B}$ *on* $|\psi\rangle$ *such that the CHSH inequality can be maximally violated.*

The state $|\psi\rangle$ defined above contains the non-trivial amount of entanglement in the commuting operator framework.

Next, we consider what it means for two states $|\psi\rangle$ and $|\phi\rangle$ to contain the same partial state.

Definition 7.4 (two states containing the same partial state)**.** *Let* $\mathbf{A} \in \mathbb{B}(\mathcal{H})$ *be some set of bounded operators.* $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ *be states.* $|\psi\rangle$ *and* $|\phi\rangle$ *is said to contain the same state over* $\mathbf{A}$ *if for all* $A \in \mathbf{A}$*,* $\langle\psi| A |\psi\rangle = \langle\phi| A |\phi\rangle$*.*

The intuition behind the above definition is that, for all observables in $\mathbf{A}$, $|\psi\rangle$ and $|\phi\rangle$ will give the same measurement outcome, and therefore the part of the two states related to $\mathbf{A}$ are identical. In the tensor product and the C*-model, this property can be expressed in terms of the partial trace of the state.

The last missing piece of information we need is to define when a state contains two copies of the same state on two different sets of commuting operators.

Definition 7.5 (product state of two copies of the same partial state)**.** *Let* $\mathbf{A}, \mathbf{B} \in \mathbb{B}(\mathcal{H})$ *be two mutually commuting sets of operators that are *-isomorphic to each other*

with $*$-isomorphism $S : \mathbf{A} \to \mathbf{B}$. Let $|\psi\rangle \in \mathcal{H}$ be a state. Then $|\psi\rangle$ is said to contain the same state over $\mathbf{A}$ and $\mathbf{B}$ if for all $A \in \mathbf{A}$, $\langle\psi| A |\psi\rangle = \langle\psi| S(A) |\psi\rangle$

In order for a state to contain two copies of the same states, the underlying mathematical structures behind the two copies of the same state must be equivalent to each other. This forces $\mathbf{A}$ to be equivalent to $\mathbf{B}$, and the reason behind $\mathbf{A}$ being isomorphic to $\mathbf{B}$.

Next, we recall how to combine quantum systems $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ where $\mathsf{A}_1, \mathsf{A}_2$ are disjoint quantum systems in the commuting operator model. Let $\mathcal{H}$ be the Hilbert space describing A. We describe $\mathsf{A}_1, \mathsf{A}_2$ with C*-algebras $\mathbf{A}_1$, $\mathbf{A}_2 \in \mathbb{B}(\mathcal{H})$ be C*-algebras where $\mathbf{A}_1$ and $\mathbf{A}_2$ mutually commute. Consider $\mathbf{A} = \overline{\mathbf{A}_1 \cup \mathbf{A}_2}$, which is the C*-algebraic closure of $\mathbf{A}_1 \cup \mathbf{A}_2$. The set of allowed local operations on A is the set of operators that preserves the observables in A and does nothing to observables outside A. Mathematically, this means that

Definition 7.6. *$U \in \mathbb{B}(\mathcal{H})$ is a local operator on $\mathbf{A}$ if*

- *U does not change observables outside A: For any $\mathbf{B} \subseteq \mathbb{B}(\mathcal{H})$ where $\mathbf{B}$ mutually commutes with $\mathbf{A}$, for all $B \in \mathbf{B}$, $U^*BU = B$.* [3]
- *U preserves the observables in A: for all $A \in \mathbf{A}$, $U^*AU \in \mathbf{A}$.*

Note that this is the same definition we had in Chapter 3 in Equation 3.2.11 and Equation 3.2.12.

[3] Alternatively we could use for all B that commutes with $\mathbf{A}$ instead of $\mathbf{B}$. By using $\mathbf{B}$, we are emphasizing other local quantum systems instead of individual operators.

7.1.4 Definition in Commuting Operator Model

Now we can define self-embezzlement in the commuting operator model.

Definition 7.7. *A self-embezzling scheme in the commuting operator model is a tuple* $(\mathcal{H}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2, |\psi\rangle, |\phi\rangle, U, V)$*, on quantum system* $(\mathsf{A}_1, \mathsf{A}_2, \mathsf{B}_1, \mathsf{B}_2)$ *where*

1. $\mathcal{H}$ *is a Hilbert space, and* $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2 \subseteq \mathbb{B}(\mathcal{H})$ *are local set of operators for* A_1*,* A_2*,* B_1*,* B_2 *that mutually commute.*

2. *There exists *-isomorphisms* $S_A : \mathbf{A}_1 \to \mathbf{A}_2$ *and* $S_B : \mathbf{B}_1 \to \mathbf{B}_2$*.*

3. $|\psi\rangle$ *is a product state over three subsystems* $(\mathsf{A}_1, \mathsf{B}_1)$*,* A_2*, and* B_2*: for all* $X \in \overline{\mathbf{A}_1 \cup \mathbf{B}_1}$*,* $Y \in \mathbf{A}_2$*,* $Z \in \mathbf{B}_2$*,*

$$\langle\psi| XYZ |\psi\rangle = \langle\psi| X |\psi\rangle \langle\psi| Y |\psi\rangle \langle\psi| Z |\psi\rangle . \tag{7.1.1}$$

4. $|\psi\rangle$ *can be used to violate the CHSH inequality by factor* $\sqrt{2}$ *using operators from* $\mathbf{A}_1$ *and* $\mathbf{B}_1$*.*

5. $U, V \in \mathbb{B}(\mathcal{H})$ *are local unitaries to the systems* $(\mathsf{A}_1, \mathsf{A}_2)$ *and* $(\mathsf{B}_1, \mathsf{B}_2)$*.*

6. *The final state* $|\phi\rangle = UV |\psi\rangle$ *must contain two copies of the same state over* $(\mathsf{A}_1, \mathsf{B}_1)$ *and* $(\mathsf{A}_2, \mathsf{B}_2)$*; and* $|\phi\rangle$ *must contain the same entangled state in* $|\psi\rangle$ *over* $\mathsf{A}_1, \mathsf{B}_1$ *and* $\mathsf{A}_2, \mathsf{B}_2$*. For all* $X \in \mathbf{A}_1$*,* $Y \in \mathbf{B}_1$*,*

$$\langle\phi| XY |\phi\rangle = \langle\phi| S_A(X) S_B(Y) |\phi\rangle = \langle\psi| XY |\psi\rangle . \tag{7.1.2}$$

7.2 Impossibility under tensor product model

Recall that under the tensor product model, embezzlement cannot be achieved perfectly, but can be approximated to arbitrary precision. The existence proof of perfect embezzlement protocol in the commuting operator model relies on the fact that approximate embezzlement protocols exist. What makes self-embezzlement remarkable is that it can be achieved in the commuting operator model, but cannot be approximated to arbitrary precision in the tensor product model.

We start by showing that self-embezzlement is impossible to achieve under the tensor product model.

Theorem 7.1. *There exists an $\epsilon_0 > 0$ such that approximate self-embezzlement to precision ϵ_0 is impossible in the tensor product model.*

The proof for the no-go result, once again, relies on the analysis of Schmidt coefficients.

Without loss of generality, consider the Schmidt decomposition of the resource state $|\psi\rangle$ to be of the form

$$|\psi\rangle = \sum_{k=1}^{\infty} \lambda_k |k\rangle \otimes |k\rangle , \tag{7.2.1}$$

where λ_i's are arranged in descending order. The Schmidt coefficients of the initial state $|\psi\rangle \otimes |\phi_A\rangle \otimes |\phi_B\rangle$ is $\{\lambda_1, \lambda_2, \cdots\}$.

Self-embezzlement can be achieved if we can convert state

$$|00\rangle \otimes |\psi\rangle \equiv \sum_{k=1}^{\infty} \lambda_k |0\rangle |k\rangle \otimes |0\rangle |k\rangle \tag{7.2.2}$$

into the state

$$|\psi\rangle \otimes |\psi\rangle \equiv \sum_{k=1}^{\infty} \sum_{l=1}^{\infty} \lambda_k \lambda_l |k\rangle |l\rangle \otimes |k\rangle |l\rangle \tag{7.2.3}$$

using local operations.

The Schmidt coefficients for $|00\rangle \otimes |\psi\rangle$ are the same as the Schmidt coefficients of $|\psi\rangle$, $\{\lambda_1, \lambda_2 \cdots\}$. The Schmidt coefficients of $|\psi\rangle \otimes |\psi\rangle$ are $\{\lambda_1^2, \lambda_1\lambda_2, \lambda_1\lambda_2, \lambda_2^2 \cdots\}$.

Since the local operations in the tensor product framework preserve the Schmidt coefficients, the two sets of Schmidt coefficients need to be the same. However, the largest Schmidt coefficient of $|00\rangle \otimes |\psi\rangle$ is λ_1 and the largest Schmidt coefficient of $|\psi\rangle \otimes |\psi\rangle$ is λ_1^2. The two sets being equal implies $\lambda_1 = \lambda_1^2$, which gives us $\lambda_1 = 1$. With $\lambda_1 = 1$, $|\psi\rangle$ is a separable state and can be trivially self-embezzled.

If $|\psi\rangle$ contains any entanglement, $\lambda_1 < 1$, which means the two sets of Schmidt coefficients are different. Therefore, self-embezzlement is impossible.

7.2.1 Impossibility of approximation

It turns out that self-embezzlement is not only impossible to achieve under the tensor product framework but it also cannot even be approximated. To properly prove this, it is necessary to clarify what approximate self-embezzlement means.

Consider a starting state $|00\rangle \otimes |\psi\rangle$ in where $|00\rangle, |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. As discussed in the previous section, an exact self-embezzlement would use local operators on $\mathcal{H}_A \otimes \mathcal{H}_A$ and $\mathcal{H}_B \otimes \mathcal{H}_B$ to achieve the state $|\psi\rangle \otimes |\psi\rangle$, which is impossible. An approximate self-embezzlement scheme would require local operators to turn $|00\rangle \otimes |\psi\rangle$ into some state $|\varphi\rangle$, such that $|\varphi\rangle$ is very close to the target state $|\psi\rangle \otimes |\psi\rangle$. In particular, an ε-approximate self-embezzlement is achieved when $\| (\langle\psi| \otimes \langle\psi|) |\varphi\rangle \|^2 < 1 - \varepsilon$.

While exact self-embezzlement is impossible under the current tensor product framework, one might expect that perhaps using some clever tricks, ε-approximate self-embezzlement can be achieved for arbitrarily small $\varepsilon > 0$. In this case, even though one may not get perfect self-embezzlement, arbitrary approximation should give a "close enough" result.

However, unfortunately, it turns out that self-embezzlement cannot be approximated below some constant ε, even if the original state $|\psi\rangle$ only contains one EPR pair. The argument for it, again, lies in the Schmidt coefficients.

For any $|\psi\rangle = \sum_k \lambda_k |k\rangle \otimes |k\rangle$, define $|\psi_{\text{initial}}\rangle$ and $|\psi_{\text{target}}\rangle$ to be the states in Equation 7.2.2 and Equation 7.2.3,

$$|\psi_{\text{initial}}\rangle = \sum_i \lambda_i |i\rangle |0\rangle \otimes |i\rangle |0\rangle , \tag{7.2.4}$$

$$|\psi_{\text{targhet}}\rangle = \sum_i \sum_j \lambda_i \lambda_j |i\rangle |j\rangle \otimes |i\rangle |j\rangle , \tag{7.2.5}$$

and we consider the distance between $U \otimes V |\psi_{\text{initial}}\rangle$ and $|\psi_{\text{target}}\rangle$.

Theorem 7.2. *There exists ϵ_0 such that for any $|\psi\rangle$ that is $(\sqrt{2}-\epsilon_0)$-CHSH violating, for any local unitary U an V, the distance between $U \otimes V |\psi_{initial}\rangle$ and $|\psi_{target}\rangle$ is at least $\frac{2}{9}$.*

Proof. We start the proof with the rigidity results from [27] about Bell states. If a state $|\psi\rangle$ is $(\sqrt{2}-\epsilon)$-CHSH violating, then there exits local unitary acting on $|\psi\rangle$ such that it is within distance $\mathcal{O}(\sqrt{\epsilon})$ from a state of the form $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |\psi'\rangle$. This implies that the largest Schmidt coefficient of $|\psi\rangle$, $\lambda_1 \leq \frac{1}{\sqrt{2}} + \mathcal{O}(\sqrt{\epsilon})$. By using bounds in [17], it can be shown that by setting $\epsilon_0 = \frac{1}{50}$, $\lambda_1 \leq \sqrt{2/3}$.

With small enough λ_1 we can consider the minimum distance between $U \otimes V |\psi_{\text{initial}}\rangle$ and $|\psi_{\text{target}}\rangle$ by comparing their Schmidt-coefficients. Since local unitaries preserve

the Schmidt coefficients, $U \otimes V |\psi_{\text{initial}}\rangle$ has the same Schmidt coefficients as $|\psi_{\text{initial}}\rangle$. By Lemma 1 in [32], the fidelity between two states is maximized if the Schmidt bases are the same and the Schmidt coefficients are arranged in the same descending order. Since $|\psi_{\text{initial}}\rangle$ and $|\psi_{\text{final}}\rangle$ have the same Schmidt basis, the local unitaries U and V only need to re-arrange these Schmidt basis in $|\psi_{\text{initial}}\rangle$ as some permutation.

Instead of discussing $\{\lambda_i\}$ directly, we look at the probability distribution associated with $\{\lambda_i\}$: let $p = (\lambda_i^2)$ arranged in descending order. We consider the smallest variation distance between p and $p \otimes p$ up to any permutation. Recall that the variation distance between p and q, $\frac{1}{2}\|p - q\|_1 = \frac{1}{2}\sum_i |p_i - q_i|$. The variation distance is minimized when p and q are sorted in the same order. Let $q = \pi(p \otimes p)$ where π is the sorting function that outputs its input set elements in descending order.

Lemma 7.2.1. *Let p be a probability distribution and $q = \pi(p \otimes p)$ be the probability distribution defined above. If $p_1 \leq 2/3$, then the variation distance between p and q is at least $2/9$.*

Proof. Let $m = \max\{m \in \mathbb{N}, p_1 + \cdots + p_m \leq \frac{2}{3}\}$, and $S = \{1, \cdots, m\}$, and $p(S) = \sum_{i \in S} p_i$. Then

$$\frac{1}{3} < p(S) \leq \frac{2}{3}. \tag{7.2.6}$$

The first inequality arise from the fact that if $p(S) \leq \frac{1}{3}$, $p_{m+1} \leq \frac{1}{3}$ and $p_1 + \cdots + p_{m+1} \leq \frac{2}{3}$.

Now let $\mu = p(S)$. Next we show that $q(S) \leq \mu^2$. Recall that $q(S)$ is the sum of the m largest components of $p \otimes p$, which must be contained in the set

$$(p_1, \cdots, p_m) \otimes (p_1, \cdots, p_m) = (p_i p_j),\ 1 \leq i, j \leq m. \tag{7.2.7}$$

This containment is clear: if for some $k \leq m$, $q_k = p_i p_j$ where $i > m$, then $q_k \leq p_l p_j$ for all $l \leq m$ which means $k > m$.

Therefore, we have

$$q(S) \leq \sum_{i,j=1}^{m} p_i p_j = \mu^2, \tag{7.2.8}$$

and the variation distance for the m largest elements of p and q is

$$\frac{1}{2}\sum_{i=1}^{m} |p_i - q_i| \geq \frac{1}{2}\left|\sum_{i=1}^{m} p_i - \sum_{i=1}^{m} q_i\right| \geq \frac{1}{2}(\mu - \mu^2) = \frac{1}{2}\mu(1-\mu) \geq \frac{1}{2}\left(\frac{2}{3}\right)\left(\frac{1}{3}\right) = \frac{1}{9}. \tag{7.2.9}$$

Then the variation distance between p and q is at most

$$\frac{1}{2}(\mu - \mu^2) + \frac{1}{2}[(1-\mu^2) - (1-\mu)] = \mu - \mu^2 \geq \frac{2}{9}. \tag{7.2.10}$$

□

Back to the proof of the theorem, since $p = (\lambda_i)$, the variation distance between p and q is the same as the probability of distinguishing $(U \otimes V)\,|\psi_{\text{initial}}\rangle$ and $|\psi_{\text{target}}\rangle$ using measurements in the Schmidt basis. This implies that the trace distance between $(U \otimes V)\,|\psi_{\text{initial}}\rangle$ and $|\psi_{\text{target}}\rangle$ is at least $\frac{2}{9}$ which completes the proof. □

Corollary 7.1. *There exists a constant $\epsilon_0 > 0$ such that for any $|\psi\rangle$ that is $(\sqrt{2} - \epsilon_0)$-CHSH violating, for any local unitary operations U and V, the fidelity between $(U \otimes V)\,|\psi_{initial}\rangle$ and $|\psi_{target}\rangle$ is at most $\sqrt{1-(2/9)^2} < 0.974996 < 39/40$.*

7.3 Self-embezzlement in the Commuting operator model

Before getting into the technical details of a self-embezzling system in the commuting operators, we first take a look at the intuition behind how self-embezzlement would work.

7.3.1 Intuition

The idea behind self-embezzlement is similar to the idea of embezzlement. The resource state for Alice and Bob is the same resource state as embezzlement, where half of the infinite-dimensional state is maximally entangled and the other half a product state. The target state for self-embezzlement is simply a state with infinitely many copies of the same separable states as the ones in the resource state. Self-embezzlement is achieved by performing permutations qubits across the two states.

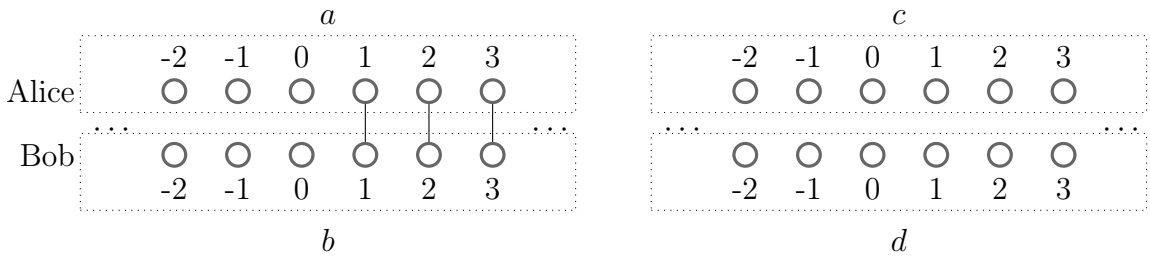


Figure 7.1: Self-embezzlement Starting State $|\psi\rangle$

As shown in Figure 7.1, the starting state $|\psi\rangle$ consists of four parts a, b, c, and d where a and c are Alice's qubits, b and d are Bob's qubits. We use a_i to denote the i-th qubit of a, b_i for the i-th qubit of b and so on. The part of the state over a and

b is the same as the state in the embezzlement protocol, where the two qubits joined by a line means the states are in the Bell basis. The part of the state over c and d is a simple separable state. To achieve self-embezzlement, Alice perform the following permutation $\sigma : \{0,1\} \times \mathbb{Z} \to \{0,1\} \times \mathbb{Z}$, where $(0,i)$ corresponds to a_i and $(1,i)$ corresponds to c_i, satisfying

$$\sigma(0,i) = \begin{cases} (0,2i) & i \geq 0 \\ (0,i) & i < 0 \end{cases}, \quad \sigma(1,i) = \begin{cases} (0,2i-1) & i > 0 \\ (1,\frac{i}{2}) & i \leq 0, i \text{ is even} \\ (1,\frac{-i+1}{2}) & i < 0, i \text{ is odd} \end{cases}. \tag{7.3.1}$$

We set a', c' to be the permuted qubits for Alice, where a'_i correspond to $\sigma(0,i)$ and c'_i correspondS to $\sigma(1,i)$. Then, we can write

$$a'_i = \begin{cases} a_{2i} & i \geq 0 \\ a_i & i < 0 \end{cases}, \quad c'_i = \begin{cases} a_{2i-1} & i > 0 \\ c_{\frac{i}{2}} & i \leq 0, i \text{ is even} \\ c_{\frac{-i+1}{2}} & i < 0, i \text{ is odd} \end{cases}. \tag{7.3.2}$$

This permutation σ can be visualized by Figure 7.2, where the positive indices of a get split into the positive indices of a' and c'; the indices of c are combined into the non-positive indices of c'. The grey area indicates the indices of qubits that are in the Bell basis. Bob performs the same permutation on his qubits over b and d.

With the above permutation, one copy of the entangled state is moved to two copies of the same state, as shown in Figure 7.3.

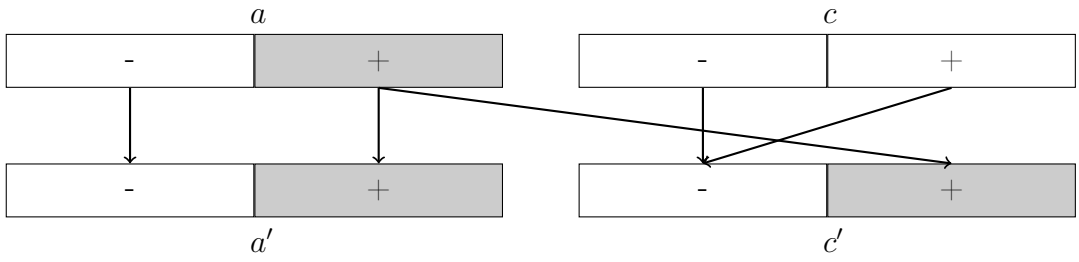


Figure 7.2: Permutation for Self-Embezzlement

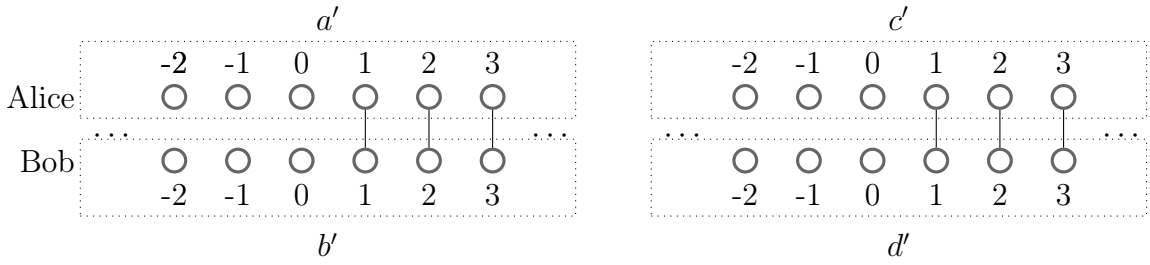


Figure 7.3: Self-embezzlement Resulting State $|\phi\rangle$

7.3.2 Base Hilbert Space

By formalizing the above intuition, self-embezzlement can be achieved in the commuting operator framework. We start with a Hilbert space $\mathcal{H}$ with basis states $|a, b, c, d\rangle$ of the form

$$|\cdots a_{-2}a_{-1}a_0.a_1a_2\cdots, \cdots b_{-2}b_{-1}b_0.b_1b_2\cdots, \cdots c_{-2}c_{-1}c_0.c_1c_2\cdots, \cdots d_{-2}d_{-1}d_0.d_1d_2\cdots\rangle \tag{7.3.3}$$

where a, b, c, d are binary strings with all but finitely many a_i, b_j, c_k, d_l are 0. The dot acts as an indicator of where the index 0 a_0, b_0, c_0, d_0 are in the doubly infinite string.

Let $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2 \in \mathbb{B}(\mathcal{H})$ be mutually commuting sets of operators, where $\mathbf{A}_1$ acts only on a, $\mathbf{A}_2$ acts only on c, $\mathbf{B}_1$ acts only on b, and $\mathbf{B}_2$ acts only on d. $\mathbf{A}_1$ is generated by linear combinations of finite-weight Paulis, so that for any $A_1 \in \mathbf{A}_1$,

A_1 only affects finitely many a_i's and acts as identity everywhere else, and a similar property holds for $\mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2$. We write the generators of the Paulis as P_a^i, P_b^j, P_c^k, P_d^l where $P_a^i \in \{X_a^i, Y_a^i, Z_a^i, \mathcal{I}_a^i\}$ is one of the four Paulis acting on qubit a_i and so on. $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2$ are in fact C*-algebras of operators that are closed under the operator norm.

When $i > 0$, the a_i and b_i are in the Bell basis, which is the same as the state defined in the embezzlement protocol. For $i > 0$, applying $P_a^i P_b^i$ to $|a, b, c, d\rangle$ is the same as applying $P_a P_b$ to $\frac{1}{\sqrt{2}} |0 b_i\rangle + \frac{1}{\sqrt{2}}(-1)^{a_i} \left|1\bar{b_i}\right\rangle$ and converting the state back to the Bell basis at a_i and b_i. For example, applying $X_a^i |a, b, c, d\rangle$ is the same as applying $X \otimes I$ to the Bell basis state of $|a_i b_i\rangle$, which gives us $X\mathcal{I}\left(\frac{1}{\sqrt{2}} |0 b_i\rangle + \frac{1}{\sqrt{2}}(-1)^{a_i} \left|1\bar{b_i}\right\rangle\right) = (-1)^{a_i} \frac{1}{\sqrt{2}} \left(\left|0\bar{b_i}\right\rangle + (-1)^{a_i} |1 b_i\rangle\right)$ which is $(-1)^{a_i} \left|a_i \bar{b_i}\right\rangle$ in the Bell basis. Therefore

$$X_a^i |a, b, c, d\rangle = (-1)^{a_i} \left|a, \cdots b_{i-1} \bar{b_i} b_{i+1} \cdots, c, d\right\rangle. \tag{7.3.4}$$

The rest of P_a^i and P_b^i for $i > 0$ can be defined in similarly, in line with the intuitions that they are the single-qubit Paulis acting on qubit a_i and b_i.

For $i \leq 0$, P_a^i and P_b^i are P_a and P_b applied directly to the state at location a_i and b_i. For example, $X |a_i\rangle = |\bar{a_i}\rangle$ so

$$X_a^i |a, b, c, d\rangle = |\cdots a_{i-1} \overline{a_i} a_{i+1} \cdots, b, c, d\rangle. \tag{7.3.5}$$

The action of the other P_a^i, P_b^i for $i \leq 0$ can be defined in a similar manner. Similarly, since c and d are in the computational basis, P_c^k and P_d^l applied directly to c_k and d_l similar to the definiton in Equation 7.3.5.

Next, we show that $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2$ are indeed mutually commuting sets of operators on $|a, b, c, d\rangle$, taking the Bell basis states into consideration. We note that only (a_i, b_i) are in the Bell basis for $i > 0$, so we only need to show that P_a^i, Q_b^i commutes

for $i > 0$. The intuition behind the commutivity is that P_a^i acts as $P \otimes \mathcal{I}$ and Q_b^i acts as $\mathcal{I} \otimes Q$ on the Bell basis state of $|a_i b_i\rangle$, and $P \otimes \mathcal{I}$ commutes with $\mathcal{I} \otimes Q$. Therefore the resulting P_a^i and P_b^i should commute on $|a, b, c, d\rangle$. The verification of this is tedious but straightforward. We give two examples here and leave out the rest.

Consider X_a^i and Z_b^i for $i > 0$, then

$$X_a^i Z_b^i |a, b, c, d\rangle = (-1)^{a_i} |a, \cdots b_{i-1} b_i b_{i+1} \cdots, c, d\rangle = Z_b^i X_a^i |a, b, c, d\rangle . \tag{7.3.6}$$

For X_a^i and X_b^i with $i > 0$, we have

$$\begin{aligned} X_a^i X_b^i |a, b, c, d\rangle &= (-1)^{\overline{a_i}} (-1)^{b_i} \left|\cdots a_{i-1} \overline{a_i} a_{i+1} \cdots, \cdots b_{i-1} \overline{b_i} b_{i+1} \cdots, c, d\right\rangle \\ &= (-1)^{a_i} (-1)^{\overline{b_i}} \left|\cdots a_{i-1} \overline{a_i} a_{i+1} \cdots, \cdots b_{i-1} \overline{b_i} b_{i+1} \cdots, c, d\right\rangle \\ &= X_b^i X_a^i |a, b, c, d\rangle . \end{aligned} \tag{7.3.7}$$

The rest of the cases apply in a similar manner and we omit the details.

Moreover, there exist $*$-isomorphisms $S_A : \mathbf{A}_1 \to \mathbf{A}_2$ and $S_B : \mathbf{B}_1 \to \mathbf{B}_2$ where $S_A(P_a^i) = P_c^i$ and $S_B(P_b^j) = P_d^j$.

As suggested in Figure 7.1, any basis state of $|e\rangle \in \mathcal{H}$ has a very special property that is it is a product state across different i and j in the following sense. For all $i \neq j$,

$$\langle e| P_a^i P_a^j P_b^i P_b^j |e\rangle = \langle e| P_a^i P_b^i |e\rangle \langle e| P_a^j P_b^j |e\rangle , \tag{7.3.8}$$

and similarly,

$$\langle e| P_c^i P_c^j P_d^i P_d^j |e\rangle = \langle e| P_c^i P_d^i |e\rangle \langle e| P_c^j P_d^j |e\rangle . \tag{7.3.9}$$

If we consider the C*-algebra $\mathcal{P}_i$ and $\mathcal{P}_j$ generated by linear combinatinos of $P_a^i P_b^i$ and $P_a^j P_b^j$, it is easy to show that by linearity, $|e\rangle$ is a product state across $\mathcal{P}_i$ and $\mathcal{P}_j$.

7.3.3 Permutation and Its Aftermath

We define Alice's operator U to be a unitary that performs the permutation shown in Equation 7.3.2. U only acts on a and c. Ideally, we want to be able to claim that $U|a, b, c, d\rangle = |a', b, c', d\rangle$ where a' and c' are defined by Equation 7.3.2. However, the result of correctly applying U to $|a, b, c, d\rangle$ is a rather obscure state that can be visualized in Figure 7.4.

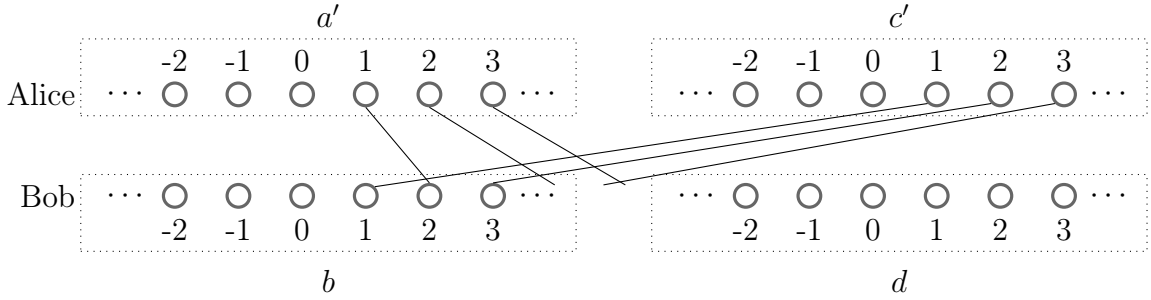


Figure 7.4: State after Alice's Permutation

The state in Figure 7.4, is not exactly $|a', b, c', d\rangle$. This is because $|a', b, c', d\rangle$ is the result of a simple permutation that only moves the value of the qubits around without changing the basis of the system so a'_i and b_i are in the Bell basis. The state we want to achieve with the correct permutation has a Bell basis between a'_i and b'_i instead.

Similar to in embezzlement where a left shift causes the state to become orthogonal to all states in the original Hilbert space, this permutation results in a state that is orthogonal to all elements of $\mathcal{H}$, and cannot be expressed in terms of a linear combination of elements in $\mathcal{H}$.

Moreover, the target state $|\phi\rangle$ shown in Figure 7.3 is also not in $\mathcal{H}$. To accommodate these states, we include two more elements in the basic state. Let p be the

number of times Alice performs permutation in Equation 7.3.2, and q be the number of times Bob performs his part of the permutation, then the corresponding basis state will be $|p, q, a, b, c, d\rangle$. This expands the Hilbert space $\mathcal{H}$ to a larger Hilbert space containing $p, q \in \mathbb{Z}$, and we will use this larger Hilbert space for the commuting operator protocol. Let U be Alice's operator for her permutation and V be Bob's operator for performing his permutation. Then we have

$$U\,|p, q, a, b, c, d\rangle = |p+1, q, a', b, c', d\rangle\,, \tag{7.3.10}$$

$$V\,|p, q, a, b, c, d\rangle = |p, q+1, a, b', c, d'\rangle\,. \tag{7.3.11}$$

Clearly, U and V commute. Therefore applying U and V together will give us $UV\,|0, 0, a, b, c, d\rangle = |1, 1, a', b', c', d'\rangle$. For example, let $a = b = c = d = 1.1$ then $a' = b = 1.0$, $c = d = 11.1$ as per Equation 7.3.2 and Figure 7.4 so

$$\begin{aligned} &UV\,|0, 0, \cdots 01.10 \cdots, \cdots 01.10 \cdots, \cdots 01.10 \cdots, \cdots 01.10 \cdots\rangle \\ &\quad = |1, 1, \cdots 01.0 \cdots, \cdots 01.0 \cdots, \cdots 011.10 \cdots, \cdots 011.10 \cdots\rangle\,. \end{aligned} \tag{7.3.12}$$

Now we need to define how to extend the operator from $\mathbf{A}_1, \mathbf{A}_2, \mathbf{B}_1, \mathbf{B}_2$ to act on the new Hilbert space with basis of the form $|p, q, a, b, c, d\rangle$. We start by setting the base case on $|0, 0, a, b, c, d\rangle$ where no permutation has been performed by Alice or Bob. $P_a^i\ P_b^j\ P_c^k$ and P_d^l should act exactly the same as they would before on $|a, b, c, d\rangle$, ignoring the first two zero elements.

We now give an example of how $P_a^i\ P_b^j\ P_c^k$ and P_d^l act on $|p, q, a, b, c, d\rangle$ by considering the action of X_a^i and X_c^i to $|1, 0, a', b, c', d\rangle$ on $i > 0$ where the qubits are entangled and basis changes are required.

Consider the σ defined in Equation 7.3.1 where $\sigma(i, j) = (k, l)$, define $\sigma(i, j)[0] = k$

and $\sigma(i,j)[1] = l$.[4] Let $i > 0$. Because $\sigma(0,i)[0] = 0$, we have $a'_i = a_{\sigma(0,i)[1]}$. This means $(a'_i, b_{\sigma(0,i)[1]})$ are in the Bell basis, and X^i_a to $|1,0,a',b,c',d\rangle$ is

$$X^i_a |1,0,a',b,c',d\rangle = (-1)^{a'_i} \left|1,0,a',\cdots b_{\sigma(0,i)[1]-1}\overline{b_{\sigma(0,i)[1]}}b_{\sigma(0,i)[1]+1}\cdots,c',d\right\rangle. \quad (7.3.13)$$

Since $\sigma(1,i)[0] = 0$, $c'_i = a_{\sigma(1,i)[1]}$ so c'_i is in the Bell basis with $b_{\sigma(1,i)[1]}$. Applying X^i_c to $|1,0,a',b,c',d\rangle$ is

$$X^i_c |1,0,a',b,c',d\rangle = (-1)^{c'_i} \left|1,0,a',\cdots b_{\sigma(1,i)[1]-1}\overline{b_{\sigma(1,i)[1]}}b_{\sigma(1,i)[1]+1}\cdots,c',d\right\rangle. \quad (7.3.14)$$

The other Paulis can be applied in a similar manner by considering their action on the correct corresponding qubits. For different values of p and q, the Bell basis is between qubits after the corresponding permutations. Applying the $P^i_a, P^j_b, P^l_c, P^k_d$ to $|p,q,a,b,c,d\rangle$ thus must take into account the correct permutation that is done by (p,q).

More formally, we define the operators $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{B}_1$, $\mathbf{B}_2$ as we enlarge them to act on the new Hilbert space. Because the permutation changed the location of the computational basis and the Bell basis, we need the operators to act correctly on the new location. Alice's operators are $\mathbf{A}_1$ and $\mathbf{A}_2$, which are C*-algebra of operators, so we can take the combined set of operators as $\overline{\mathbf{A}_1 \cup \mathbf{A}_2}$ where the bar means it is the C*-algebraic closure, and similarly Bob's combined set of operators as $\overline{\mathbf{B}_1 \cup \mathbf{B}_2}$. Define a $*$-automorphisms $\pi_A \colon \overline{\mathbf{A}_1 \cup \mathbf{A}_2} \to \overline{\mathbf{A}_1 \cup \mathbf{A}_2}$ to be the following: for $P^i_a \in \mathbf{A}_1$,

[4] This is similar to the notation of the array access in computer science, where [0] accesses the first element k of the tuple (k,l) and [1] accesses the second element l of the tuple.

$P_c^j \in \mathbf{A}_2$,

$$\pi_A(P_a^i) = \begin{cases} P_a^i & i \leq 0 \\ P_a^{2i} & i > 0 \end{cases} \text{ and } \pi_A(P_c^j) = \begin{cases} P_a^{2i-1} & i > 0 \\ P_c^{i/2} & i \leq 0 \text{ is even} \\ P_c^{(i-1)/2} & i \geq 0 \text{ is odd} \end{cases}. \tag{7.3.15}$$

π_A essentially performs the permutation in Equation 7.3.2 on Alice's operators. We define $\pi_B : \overline{\mathbf{B}_1 \cup \mathbf{B}_2} \to \overline{\mathbf{B}_1 \cup \mathbf{B}_2}$ in a similar manner for Bob. For $A \in \overline{\mathbf{A}_1 \cup \mathbf{A}_2}$,

$$A \left|p, q, a, b, c, d\right\rangle := U^p V^q \pi_A^p(A) U^{-p} V^{-q} \left|p, q, a, b, c, d\right\rangle. \tag{7.3.16}$$

The idea is to move $|p, q, a, b, c, d\rangle$ back to some $\left|0, 0, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}\right\rangle$ so that the operators acting on these states are already defined; apply the operator on the permuted qubits, and perform bring the state back to the form $|p, q, a, b, c, d\rangle$. And similarly, for $B \in \overline{\mathbf{B}_1 \cup \mathbf{B}_2}$,

$$B \left|p, q, a, b, c, d\right\rangle := U^p V^q \pi_B^q(B) U^{-p} V^{-q} \left|p, q, a, b, c, d\right\rangle. \tag{7.3.17}$$

We note that U commutes with all $B \in \overline{\mathbf{B}_1 \cup \mathbf{B}_2}$ because

$$\begin{aligned} BU \left|p, q, a, b, c, d\right\rangle &= B \left|p+1, q, a', b, c', d\right\rangle \\ &= U^{p+1} V^q \pi_B^q(B) V^{-q} U^{-p-1} \left|p+1, q, a', b, c', d\right\rangle \\ &= U^{p+1} V^q \pi_B^q(B) V^{-q} U^{-p} \left|p, q, a, b, c, d\right\rangle \\ &= UB \left|p, q, a, b, c, d\right\rangle. \end{aligned} \tag{7.3.18}$$

Similarly, V commutes with all $A \in \overline{\mathbf{A}_1 \cup \mathbf{A}_2}$. Moreover, $AB = BA$ because

$$\begin{aligned} AB\left|p,q,a,b,c,d\right\rangle &= U^pV^q\pi_A^p(A)U^{-p}V^{-q}U^pV^q\pi_B^p(B)U^{-p}V^{-q}\left|p,q,a,b,c,d\right\rangle \\ &= U^pV^q\pi_A^p(A)\pi_B^q(B)U^{-p}V^{-q}\left|p,q,a,b,c,d\right\rangle \\ &= U^pV^q\pi_A^p(A)\pi_B^q(B)\left|0,0,\tilde{a},\tilde{b},\tilde{c},\tilde{d}\right\rangle \\ &= U^pV^q\pi_B^q(B)\pi_A^p(A)\left|0,0,\tilde{a},\tilde{b},\tilde{c},\tilde{d}\right\rangle \\ &= U^pV^q\pi_B^q(B)\pi_A^p(A)U^{-p}V^{-q}\left|p,q,a,b,c,d\right\rangle \\ &= BA\left|p,q,a,b,c,d\right\rangle, \end{aligned} \tag{7.3.19}$$

where $\{\tilde{a},\tilde{c}\}$ is applying the inverse of Alice's permutaiton to $\{a,c\}$ in Equation 7.3.2 p times, and $\{\tilde{b},\tilde{d}\}$ is the inverse of Bob's permutation applied q times to $\{b,d\}$.

Let $\left|\psi\right\rangle = \left|0,0,0,0,0,0\right\rangle$, where the $\left|0\right\rangle$ for a,b,c,d are means all of a_i, b_j, c_k, d_l are 0, and we completely defined a protocol for self-embezzlement in the commuting operator framework.

7.3.4 Verification of Protocol

The final step is to verify that the $\mathcal{H}$, $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{B}_1$, $\mathbf{B}_2$, $\left|\psi\right\rangle$, U, V defined above satisfy the definition of a perfect commuting operator protocol for self-embezzlement.

Condition 1 to 5 in Definition 7.7 are either satisfied by definition or are trivial to show. We focus our attention on Condition 6, which requires $\left|\phi\right\rangle = UV\left|\psi\right\rangle = \left|1,1,0,0,0,0\right\rangle$ to satisfy for any $A_1 \in \mathbf{A}_1$, $B_1 \in \mathbf{B}_1$,

$$\left\langle\phi\right| A_1B_1\left|\phi\right\rangle = \left\langle\phi\right| S_A(A_1)S_B(B_1)\left|\phi\right\rangle = \left\langle\psi\right| A_1B_1\left|\psi\right\rangle. \tag{7.3.20}$$

Since $\left|\psi\right\rangle = \left|0,0,0,0,0,0\right\rangle$ is a basis state, recall that $\left|\psi\right\rangle$ is a product state across different i an j in the sense that for all $i \neq j$, $\left\langle\psi\right| P_a^iP_a^jP_b^iP_b^j\left|\psi\right\rangle = \left\langle\psi\right| P_a^iP_b^i\left|\psi\right\rangle\left\langle\psi\right| P_a^jP_b^j\left|\psi\right\rangle$.

$|\phi\rangle$ is a permutation of the bits of $|\psi\rangle$ where Alice and Bob perform the same permutation. Therefore, $|\phi\rangle$ also satisfies the same property. This means we only need to verify Equation 7.3.20 on $P_a^i P_b^i$ for all i.

Assume $i \leq 0$. Then $\pi_A(P_a^i) = P_a^i$ and $\pi_B(P_b^i) = P_b^i$, and $S_A(P_a^i) = P_c^i$, $S_B(P_B^i) = P_d^i$. We get

$$\begin{aligned}\langle\phi| P_a^i P_b^i |\phi\rangle &= \langle 1,1,0,0,0,0| UV\pi_A(P_a^i)\pi_B(P_b^i)U^{-1}V^{-1} |1,1,0,0,0,0\rangle \\ &= \langle 0,0,0,0,0,0| P_a^i P_b^i |0,0,0,0,0,0\rangle \\ &= \langle\psi| P_a^i P_b^i |\psi\rangle .\end{aligned} \tag{7.3.21}$$

And if i is even,

$$\begin{aligned}\langle\phi| S_A(P_a^i)S_B(P_b^i) |\phi\rangle &= \langle 1,1,0,0,0,0| UV\pi_A(P_c^i)\pi_B(P_d^i)U^{-1}V^{-1} |1,1,0,0,0,0\rangle \\ &= \langle\psi| P_c^{i/2} P_d^{i/2} |\psi\rangle .\end{aligned} \tag{7.3.22}$$

Recall that $|\psi\rangle$ at location $c^{i/2}d^{i/2}$ has the same value as $|\psi\rangle$ at location $a_i b_i$, which is $|00\rangle$ in the computational basis. Therefore, $\langle\psi| P_c^{i/2} P_d^{i/2} |\psi\rangle = \langle\psi| P_a^i P_b^i |\psi\rangle$. Similarly, if i is odd, $\langle\phi| S_A(P_a^i)S_B(P_b^i) |\phi\rangle = \langle\psi| P_a^i P_b^i |\psi\rangle$.

If $i > 0$, $\pi_A(P_a^i) = P_a^{2i}$ and $\pi_A(P_c^i) = P_a^{2i-1}$, which gives us

$$\begin{aligned}\langle\phi| P_a^i P_b^i |\phi\rangle &= \langle 1,1,0,0,0,0| UV\pi_A(P_a^i)\pi_B(P_b^i)U^{-1}V^{-1} |1,1,0,0,0,0\rangle \\ &= \langle\psi| P_a^{2i} P_b^{2i} |\psi\rangle ,\end{aligned} \tag{7.3.23}$$

and

$$\begin{aligned}\langle\phi| S_A(P_a^i)S_B(P_b^i) |\phi\rangle &= \langle 1,1,0,0,0,0| UV\pi_A(P_c^i)\pi_B(P_d^i)U^{-1}V^{-1} |1,1,0,0,0,0\rangle \\ &= \langle\psi| P_a^{2i-1} P_b^{2i-1} |\psi\rangle .\end{aligned} \tag{7.3.24}$$

$|\psi\rangle$ at $a_{2i}b_{2i}$ and $a_{2i-1}b_{2i-1}$ are $|00\rangle$ in the Bell basis, which is the same as $|\psi\rangle$ at a_ib_i. Therefore, we have

$$\langle\psi| P_a^{2i}P_b^{2i} |\psi\rangle = \langle\psi| P_a^{2i-1}P_b^{2i-1} |\psi\rangle = \langle\psi| P_a^iP_b^i |\psi\rangle . \tag{7.3.25}$$

7.4 Self-embezzlement in the C*-model

We start with a recollection of the CAR algebra. Recall that a CAR algebra is a C*-algebra where its basis elements are consisting of finite weight Paulis of the form X^aZ^b for $a, b \in \{0,1\}^*$. We use $\mathcal{R}$ to denote a CAR algebra. Recall that $\mathcal{R} \otimes_{\min} \mathcal{R} = \mathcal{R} \otimes_{\max} \mathcal{R}$, so we simply use $\mathcal{R} \otimes \mathcal{R}$ for this tensor product.

While a typical $\mathcal{R}$ has X^aZ^b as a basis where a and b are one-way infinite strings, we could map $\mathcal{R}$ to $\mathcal{R} \otimes \mathcal{R}$ via a *-isomorphism so a and b become two-way infinite strings. Next, we consider $*$-automorphisms on $\mathcal{R}$. An inner *-automorphism on $\mathcal{R}$ can be expressed in terms of an unitary $u \in \mathcal{R}$ where $\alpha_u(a) = u^*au$ is the *-automorphism $\mathcal{R} \to \mathcal{R}$. A $*$-automorphism that cannot be expressed in this manner is called an outer *-automorphism and an example of this is a bilateral shift that maps X^aZ^b to $X^{a'}Z^{b'}$ where $a'_i = a_{i+1}$ and $b'_i = b_{i+1}$.

The C*-algebra we will use for self-embezzlement is $\mathcal{R}\otimes\mathcal{R}\otimes\mathcal{R}\otimes\mathcal{R}$ where the first and third copy of $\mathcal{R}$ corresponds to Alice's local system A_1, A_2, and the second and fourth copy of $\mathcal{R}$ correspond to Bob's local system of B_1, B_2. The intuition behind self-embezzlement under the C*-model is the same as the one behind the commuting operator model, where Alice and Bob perform an appropriate permutation across their states to double the entangled state.

7.4.1 The State

We note that since the basis of $\mathcal{R}$ is $X^a Z^b$, the basis of $\mathcal{R} \otimes \mathcal{R}$ is $X^a Z^b \otimes X^c Z^d$ where a, b, c, d are two-way infinite strings. By linearity and continuity, to define a state on $\mathcal{R} \otimes \mathcal{R}$, we only need to define it on all the basis elements.

We start by considering the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and a state with infinitely many copies of $|\Psi\rangle$. We know from the previous discussions that such a state does not exist in the tensor product framework. However, such a state can be expressed as an abstract state in the C*-model. Let $s_\Psi : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ be an abstract state with infinitely many copies of $|\Psi\rangle$ in the positive indices state such that

$$s_\Psi((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{i=1}^{\infty} \langle\Psi| (X^{a_i} Z^{b_i}) \otimes (X^{a'_i} Z^{b'_i}) |\Psi\rangle . \tag{7.4.1}$$

From previous chapters, we know that for a maximally entangled state $|\Psi\rangle$, and $A, B \in \mathbb{B}(\mathbb{C}^2)$, $\langle\Psi| A \otimes B |\Psi\rangle = \langle\Psi| \mathcal{I} \otimes BA^T |\Psi\rangle$. This gives us

$$\begin{aligned} \langle\Psi| (X^{a_i} Z^{b_i}) \otimes (X^{a'_i} Z^{b'_i}) |\Psi\rangle &= \langle\Psi| \mathcal{I} \otimes X^{a'_i} Z^{b'_i} Z^{b_i} X^{a_i} |\Psi\rangle \\ &= (-1)^{a_i(b_i \oplus b'_i)} \langle\Psi| \mathcal{I} \otimes X^{a_i \oplus a'_i} Z^{b_i \oplus b'_i} |\Psi\rangle . \end{aligned} \tag{7.4.2}$$

Furthermore, it is easy to show $\langle\Psi| \mathcal{I} \otimes X |\Psi\rangle = \langle\Psi| \mathcal{I} \otimes Z |\Psi\rangle = \langle\Psi| \mathcal{I} \otimes XZ |\Psi\rangle = 0$. This allows us to write

$$s_\Psi((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{i=1}^{\infty} \delta_{a_i a'_i} \delta_{b_i b'_i}, \tag{7.4.3}$$

where $\delta_{i,j} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$ is the Kronecker delta function.

Similarly, we define $s_{00} : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ as the abstract state corresponding to the

infinitely tensor product of $|00\rangle$ in the non-positive indices:

$$s_{00}((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{i=0}^{-\infty} \langle 00| X^{a_i} Z^{b_i} \otimes X^{a'_i} Z^{b'_i} |00\rangle = \prod_{i=0}^{-\infty} (1 - a_i)(1 - a'_i). \quad (7.4.4)$$

Combing the two states, we define the catalyst state of self-embezzlement $\psi : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ to be

$$\psi((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{i=1}^{\infty} \delta_{a_i a'_i} \delta_{b_i b'_i} \prod_{i=0}^{-\infty} (1 - a_i)(1 - a'_i). \quad (7.4.5)$$

For the state we want to copy ψ onto, we first define $\phi : \mathcal{R} \to \mathbb{C}$ to be

$$\phi(X^a Z^b) = \prod_{i=-\infty}^{\infty} \langle 0| X^{a_i} Z^{b_i} |0\rangle = \prod_{i=-\infty}^{\infty} (1 - a_i), \quad (7.4.6)$$

and Alice and Bob each have one copy of this state, so the combined state $\phi \otimes \phi : \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ is

$$(\phi \otimes \phi)((X^a Z^b) \otimes (X^{a'} Z^{b'})) = \prod_{i=-\infty}^{\infty} (1 - a_i)(1 - a'_i). \quad (7.4.7)$$

The initial state for self-embezzlement in the C*-model is therefore

$$\psi \otimes \phi \otimes \phi : \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \to \mathbb{C} \quad (7.4.8)$$

where ψ is over A_1 and B_1, $\phi \otimes \phi$ is over A_2 and B_2.

7.4.2 The Permutation

We now consider the local operation on $\mathsf{A}_1, \mathsf{A}_2$ and $\mathsf{B}_1, \mathsf{B}_2$. To achieve self-embezzlement, we perform a permutation that maps the positive indices of A_1 to the positive indices of A_1 and A_2. With this permutation, the entangled Bell basis is mapped from the positive indices of A_1 to the positive indices of $\mathsf{A}_1, \mathsf{A}_2$ and therefore becomes two copies

of the original entangled state. To reduce clutter, instead of writing $X^a Z^b$ as basis elements for $\mathcal{R}$, we use the notation P_α, $\alpha \in \{a, b, c, d\}$, where $P_\alpha^i = X^{a_i} Z^{b_i}$ is a single bit Pauli at index i. Then the basis of $\mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R}$ can be expressed in terms of $P_a \otimes P_b \otimes P_c \otimes P_d$ where P_a is a finite weight Pauli on the CAR algebra of A_1, and P_b is on B_1, P_c is on A_2, and P_d is on B_2. This notation is similar to what we used in the commuting operator framework of self-embezzlement, except P_a, P_b, P_c, P_d are in a tensor product here whereas in the commuting operator model they are mutually commuting operators.

We define the following maps from (a, c) to (a', c') that corresponds to a permutation of the indices of (a, c).

$$a'_i = \begin{cases} a_i & i \leq 0 \\ a_{\frac{i}{2}} & i > 0 \text{ is even} \\ c_{\frac{i+1}{2}} & i > 0 \text{ is odd} \end{cases}, \qquad c'_i = \begin{cases} c_{2i} & i \leq 0 \\ c_{-2i+1} & i > 0 \end{cases}, \tag{7.4.9}$$

and similarly, from (b, d) to (b', d')

$$b'_i = \begin{cases} b_i & i \leq 0 \\ b_{\frac{i}{2}} & i > 0 \text{ is even} \\ d_{\frac{i+1}{2}} & i > 0 \text{ is odd} \end{cases}, \qquad d'_i = \begin{cases} d_{2i} & i \leq 0 \\ d_{-2i+1} & i > 0 \end{cases}. \tag{7.4.10}$$

We note that this is the reverse of the permutation in Equation 7.3.2 used for the commuting operator model. This is because in the commuting operator model the permutation is performed on the quantum state, whereas in the C*-model the permutation is performed on the operators.

Define $\alpha_A : \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \to \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R}$ as Alice's *-automorphism for her

permutation where

$$\alpha_A(P_a \otimes P_b \otimes P_c \otimes P_d) = P_{a'} \otimes P_b \otimes P_{c'} \otimes P_d. \tag{7.4.11}$$

α_A is local to A_1 and A_2 because it is invariant over the second and fourth CAR algebra.

Similarly, we define $\alpha_B : \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \to \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R}$ to be Bob's *-automorphism for the permutation where

$$\alpha_B(P_a \otimes P_b \otimes P_c \otimes P_d) = P_a \otimes P_{b'} \otimes P_c \otimes P_{d'}. \tag{7.4.12}$$

The combined *-automorphism is $\alpha = (\alpha_A \circ \alpha_B)$ that maps $P_a \otimes P_b \otimes P_c \otimes P_d$ to $P_{a'} \otimes P_{b'} \otimes P_{c'} \otimes P_{d'}$, where a', b', c', d' are related to a, b, c, d according to Equation 7.4.9 and 7.4.10.

7.4.3 The Verification

We started with the state $\psi \otimes \phi \otimes \phi$ and applies the *-automorphism to it. The last step is to check that $s_{\text{final}} : \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \to \mathbb{C}$ defined by

$$s_{\text{final}}(x) := (\psi \otimes \phi \otimes \phi)(\alpha(x)) \tag{7.4.13}$$

is indeed $\psi \otimes \psi$.

Let $\mathcal{P}$ be the C*-algebra of single-qubit Paulis. Let $\Psi : \mathcal{P} \otimes \mathcal{P} \to \mathbb{C}$ be the state for all $P, Q \in \mathcal{P}$,

$$\Psi(P \otimes Q) = \langle \Psi | \, P \otimes Q \, | \Psi \rangle \,, \tag{7.4.14}$$

where $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the Bell state defined earlier. Let $\Phi : \mathcal{P} \to \mathbb{C}$ be the single qubit $|0\rangle$ state

$$\Phi(P) = \langle 0 | \, P \, | 0 \rangle \,. \tag{7.4.15}$$

We note that by definition of ψ and ϕ, for all $P_a \otimes P_b \otimes P_c \otimes P_d$,

$$(\psi\otimes\phi\otimes\phi)(P_a\otimes P_b\otimes P_c\otimes P_d) = \prod_{i=1}^{\infty} \Psi(P_a^i\otimes P_b^i) \prod_{i=0}^{-\infty}(\Phi\otimes\Phi)(P_a^i\otimes P_b^i) \prod_j \Phi(P_c^j) \prod_k \Phi(P_d^k). \tag{7.4.16}$$

So if we apply $\psi \otimes \phi \otimes \phi$ to $P_{a'} \otimes P_{b'} \otimes P_{c'} \otimes P_{d'}$, we get

$$\begin{aligned}
&(\psi \otimes \phi \otimes \phi)(P_{a'} \otimes P_{b'} \otimes P_{c'} \otimes P_{d'}) \\
&\qquad = \prod_{i=1}^{\infty} \Psi(P_{a'}^i \otimes P_{b'}^i) \prod_{i=0}^{-\infty}(\Phi \otimes \Phi)(P_{a'}^i \otimes P_{b'}^i) \prod_j \Phi(P_{c'}^j) \prod_k \Phi(P_{d'}^k) \\
&\qquad = \prod_{i\le 0} \phi \otimes \phi(P_a^i \otimes P_b^i) \prod_{\substack{i>0 \\ \text{even}}} \Psi(P_a^{i/2} \otimes P_b^{i/2}) \prod_{\substack{i>0 \\ \text{odd}}} \Psi(P_c^{\frac{i+1}{2}} \otimes P_d^{\frac{i+1}{2}}) \\
&\qquad\quad \prod_{i\le 0}(\Phi \otimes \Phi)(P_c^{2i} \otimes P_d^{2i}) \prod_{i>0}(\Phi \otimes \Phi)(P_c^{-2i+1} \otimes P_d^{-2i+1}) \\
&\qquad = \prod_{i\le 0}(\Phi \otimes \Phi)(P_a^i \otimes P_b^i) \prod_{i>0} \Psi(P_a^i \otimes P_b^i) \prod_{i>0} \Psi(P_c^i \otimes P_d^i) \\
&\qquad\quad \prod_{i\le 0}(\Phi \otimes \Phi)(P_c^i \otimes P_d^i) \\
&\qquad = \psi(P_a \otimes P_b)\psi(P_c \otimes P_d) \\
&\qquad = (\psi \otimes \psi)(P_a \otimes P_b \otimes P_c \otimes P_d).
\end{aligned} \tag{7.4.17}$$

Since any element of $\mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R}$ is a linear combination of $P_a \otimes P_b \otimes P_c \otimes P_d$, by linearity and continuity, $(\psi \otimes \phi \otimes \phi)(\alpha(x)) = (\psi \otimes \psi)(x)$ for all $x \in \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R} \otimes \mathcal{R}$. This completes the constructino of a C*-model strategy for self-embezzlement.

Chapter 8

Summary

The description of infinite dimensional entanglement in quantum information requires a mathematical model more powerful than the tensor product of the Hilbert spaces model. The typical model used is the commuting operator model, where the local operators mutually commute and act on the same single Hilbert space. It is a generalization of the tensor product of the Hilbert spaces model since any operator tensor identity commutes with the identity tensor of any operator. In the commuting operator model, the commutivity defines the structure of locality, and sometimes it may not be clear how to describe a local sub-system in this model. In the discussion of linear system games, we showed that a game has a commuting operator strategy if and only if there exists a potentially infinite-dimensional operator solution to the game through the solution group. The construction of the commuting operator strategy from the solution group gives rise to Alice's and Bob's operators that correspond to the left and right multiplications of the group elements. In this case, the locality of the operators comes from the commutivity of the left and right group multiplications.

It is not exactly clear, given a state under this set of commuting operators, what it means to talk about Alice's or Bob's part of the localized state. There is no underlying bipartite structure in these commuting operators, and analysis of entanglement, in this case, can be tricky.

We also showed the formulation of quantum information theory using C*-algebras instead of Hilbert spaces as the foundation. The C*-model can be adopted to describe infinite entanglement that cannot be described by the tensor product of Hilbert spaces, using the tensor product of C*-algebras. Unlike the commuting operator model that has one single Hilbert space and relies on the commutivity to describe locality, the tensor product of C*-algebras has a more intuitive bipartite (or multipartite for multiple local subsystems) structure in describing local quantum subsystems.

Table 8.1 summarizes some of the differences between the tensor product of Hilbert spaces, the commuting operators, and the C*-model for non-local quantum systems. The tensor product and the C*-model share a lot of similarities in terms of their structures on local quantum systems. The commuting operator model is the most general model because the C*-model can be converted into it using the GNS construction, but the conversion the other way is not as clear. However, the commuting operator model does not have a lot of those structures in the tensor product and C*-model. The tensor product is a special case of the commuting operator, and the C*-model is a generalization of the tensor product model. With the GNS representation theorem, it is possible to convert the C*-model to the commuting operator model. There are situations where the structure of the C*-model comes in handy in describing quantum systems that cannot be defined by the tensor product model intuitively.

[1]We omit the statement $\forall A \in \mathbf{A}, B \in \mathbf{B}$ in some of the entries where applicable

[2]There is technically no partial state in the commuting operator framework.$|\psi_1\rangle \overset{\mathbf{A}}{\cong} |\psi_2\rangle$ only

	Tensor Product	Commuting Operator[1]	C*-algebra
Operators on System (A, B)	$\mathbb{B}(\mathcal{H}_A) \otimes \mathbb{B}(\mathcal{H}_B)$	$\mathbf{A}, \mathbf{B} \subseteq \mathbb{B}(\mathcal{H})$ $[\mathbf{A}, \mathbf{B}] = 0$	$\mathcal{A} \otimes \mathcal{B}$
Product state	$\lvert\psi_A\rangle \otimes \lvert\psi_B\rangle$	$\lvert\psi\rangle$ $\langle\psi\rvert AB \lvert\psi\rangle = \langle\psi\rvert A \lvert\psi\rangle \langle\psi\rvert B \lvert\psi\rangle$	$s_A \otimes s_B$
Partial State on A	$\mathrm{Tr}_B(\lvert\psi\rangle \langle\psi\rvert)$	$\lvert\psi_1\rangle \overset{\mathbf{A}}{\cong} \lvert\psi_2\rangle$ [2]	$s_A(a) = s(a \otimes 1)$
Same Type of System for A, B	$\mathcal{H}_A = \mathcal{H}_B$	$S : \mathbf{A} \to \mathbf{B}$ S is $*$-isomorphism	$\mathcal{A} = \mathcal{B}$
Local Evolution on A	$U_A \otimes \mathcal{I}_B$	$U \in \mathbb{B}(\mathcal{H})$ $UBU^* = B$, $UAU^* \in \mathbf{A}$	$\alpha_A \otimes \mathcal{I}$ α_A $*$-automorphism

Table 8.1: Description of Local System under Different Models

In particular, we gave the example of embezzlement and self-embezzlement, where the commuting operator model for the protocols requires careful consideration of nitty-gritty details. In contrast, we can construct the C*-model protocol directly from intuition. Moreover, since both embezzlement and self-embezzlement are impossible to achieve in the tensor product of the Hilbert space model, it shows that the C*-model is more powerful in describing infinite-dimensional non-local systems than the tensor product of the Hilbert space model.

Using CAR-algebra, we can define quantum states that are intuitive but do not exist in the tensor product of the Hilbert space model, such as infinitely many Bell states. The interpretation of the CAR algebra as finite-weight Paulis acting on in-

shows that the part of the state related to $\mathbf{A}$ of $|\psi_1\rangle$ and $|\psi_2\rangle$ are the same.

finitely many qubits makes it easy to formalize intuitions on operations performed on infinitely many qubits, such as shift or permutation of the qubits. With the tensor product of CAR algebra, we can easily visualize the ownership of local quantum systems.

The CAR-algebra is only one example of what the C*-model can do. It is possible that other C*-algebras have applications in the intuitive description of some other quantum systems or problems. This thesis aims to serve as a stepping stone for more potential uses of the C*-model in quantum information theory.

References

[1] Padmanabhan K. Aravind. "Quantum mysteries revisited again". In: *American Journal of Physics* 72.10 (2004), pp. 1303–1307.

[2] Alex Arkhipov. "Extending and characterizing quantum magic games". In: *arXiv preprint arXiv:1209.3819* (2012).

[3] John S. Bell. "On the Einstein Podolsky Rosen Paradox". In: *Physics Physique Fizika* 1.3 (1964), p. 195.

[4] Richard Cleve, Li Liu, and William Slofstra. "Perfect commuting-operator strategies for linear system games". In: *Journal of Mathematical Physics* 58.1 (2017), p. 012202.

[5] Richard Cleve and Rajat Mittal. "Characterization of binary constraint system games". In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2014, pp. 320–331.

[6] Richard Cleve et al. "Consequences and limits of nonlocal strategies". In: *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* IEEE. 2004, pp. 236–249.

[7] Richard Cleve et al. "Constant gap between conventional strategies and those based on C*-dynamics for self-embezzlement". In: *arXiv preprint arXiv:1811.12575* (2018).

[8] Wim van Dam and Patrick Hayden. "Universal entanglement transformations without communication". In: *Physical Review A* 67.6 (2003), p. 060302.

[9] Kenneth R. Davidson. *C*-algebras by example*. Vol. 6. American Mathematical Soc., 1996.

[10] Andrew C. Doherty et al. "The quantum moment problem and bounds on entangled multi-prover games". In: *2008 23rd Annual IEEE Conference on Computational Complexity*. IEEE. 2008, pp. 199–210.

[11] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" In: *Physical review* 47.10 (1935), p. 777.

[12] Tobias Fritz. "Tsirelson's problem and Kirchberg's conjecture". In: *Reviews in Mathematical Physics* 24.05 (2012), p. 1250012.

[13] I. M. Gelfand and M. A. Naimark. "On the embedding of normed rings into the ring of operators in Hilbert space". In: *Matematiceskij sbornik* 12 (1943), pp. 197–213. URL: http://eudml.org/doc/65219.

[14] Zhengfeng Ji, Debbie Leung, and Thomas Vidick. "A three-player coherent state embezzlement game". In: *Quantum* 4 (2020), p. 349.

[15] Zhengfeng Ji et al. "MIP*=RE". In: *Communications of the ACM* 64.11 (2021), pp. 131–138.

[16] Marius Junge et al. "Connes' embedding problem and Tsirelson's problem". In: *Journal of Mathematical Physics* 52.1 (2011), p. 012102.

[17] Jędrzej Kaniewski. "Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities". In: *Physical review letters* 117.7 (2016), p. 070402.

[18] Debbie Leung, Ben Toner, and John Watrous. "Coherent state exchange in multi-prover quantum interactive proof systems". In: *Chicago Journal of Theoretical Computer Science* 11.2013 (2013), p. 1.

[19] N. David Mermin. "Hidden variables and the two theorems of John Bell". In: *Reviews of Modern Physics* 65.3 (1993), p. 803.

[20] N. David Mermin. "Simple unified form for the major no-hidden-variables theorems". In: *Physical review letters* 65.27 (1990), p. 3373.

[21] Miguel Navascués and David Pérez-Garcıa. "Quantum steering and spacelike separation". In: *Physical Review Letters* 109.16 (2012), p. 160405.

[22] Narutaka Ozawa. "About the Connes Embedding Conjecture : Algebraic approaches". In: *arXiv preprint arXiv:1212.1700* (2012).

[23] Vern Paulsen. *Completely bounded maps and operator algebras*. 78. Cambridge University Press, 2002.

[24] Vern I Paulsen et al. "Estimating quantum chromatic numbers". In: *Journal of Functional Analysis* 270.6 (2016), pp. 2188–2222.

[25] Gert K. Pedersen. *C*-Algebras and their Automorphism Groups*. Academic Press, 1979.

[26] R. Cleve, L. Liu, and V. Paulsen. "Perfect embezzlement of entanglement". In: *Journal of Mathematical Physics* 58 (2017). DOI: https://doi.org/10.1063/1.4974818.

[27] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games". In: *arXiv preprint arXiv:1209.0448* (2012).

[28] Volkher B. Scholz and Reinhard F. Werner. "Tsirelson's problem". In: *arXiv preprint arXiv:0812.4305* (2008).

[29] I. E. Segal. "Irreducible representations of operator algebras". In: *Bulletin of the American Mathematical Society* 53 (1947), pp. 73–88. DOI: https://doi.org/10.1090/S0002-9904-1947-08742-5.

[30] William Slofstra. "The set of quantum correlations is not closed". In: *Forum of Mathematics, Pi*. Vol. 7. Cambridge University Press. 2019.

[31] Boris S. Tsirelson. "Some results and problems on quantum Bell-type inequalities". In: *Hadronic Journal Supplement* 8.4 (1993), pp. 329–345.

[32] G. Vidal, D. Jonathan, and M.A. Nielsen. "Approximate transformations and robust manipulation of bipartite pure-state entanglement". In: *Physical Review A* 62.1 (2000), p. 012304.