Computational Complexity in Entanglement Transformations

by

Eric A. Chitambar

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Physics)
in The University of Michigan
2010

Doctoral Committee:

Professor Yaoyun Shi, Chair
Professor Luming Duan
Professor James D. Wells
Professor Kim A. Winick
Lecturer Carl A. Miller

The following is certified E.A.T.S. material. Even quantum mechanics attracts the occasional demon.

ACKNOWLEDGEMENTS

Over the past four years I have been privileged to work with some of the nicest and brightest thinkers in the world, and this dissertation cannot begin without properly acknowledging these individuals. I would first like to thank my advisor Yaoyun Shi for introducing me to this subject and helping me to think like a theoretical scientist. It has been a pleasure working with him and I am gracious for all his support.

I thank my collaborator and friend Runyao Duan for inviting me to visit Beijing as well as bestowing guidance throughout my graduate studies. I would also like to express gratitude to Andreas Winter for providing warm hospitality overseas and sharing his expertise on the various problems I have studied.

I have been fortunate to have fruitful discussions with Jon Allcock, Michael Bremner, Lin Chen, Toby Cubitt, Luming Duan, Aram Harrow, Richard Jozsa, Tom Lawson, Richard Low, Will Matthews, Carl Miller, Ashley Montanaro, James Wells, Kim Winick, Yu Xin and Nengkun Yu. In addition to the shared "shop talk," it has been a delight getting to know them all personally.

As Ann Arbor has been my home base throughout the past five years, I extend local love to all my roommates, friends and colleagues here, as well as Luke at Fish Doctor's for all the discounted African Cichlids, Senate at Noggins for mastering the one-fade, and Kroger Plus Memberships. In addition, I am indebted to the intangible supports of Jack Bauer, the now-discontinued 24 g protein Lean Pocket,

Meadow Soprano, Richard Swinburne, and Norma Jean's third album, track three. I also thank my lovely girlfriend for not letting Alice and Bob off the hook so easily.

Last but not least, I thank my mother for explaining the correct use of gerund phrases and my father for teaching me about the square-root of a number. In more ways than one, I would not be here today without you both.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS . . . . **ii**

LIST OF FIGURES . . . . **vi**

ABSTRACT . . . . **vii**

CHAPTER

I. Introduction 1

II. Preliminary Material 10

2.1 Complexity Theory 10
2.2 Quantum Information 18
2.2.1 Basic Formalism 18
2.2.2 Entanglement Measures and LOCC Operations 20
2.2.3 Entanglement Partial Ordering 24

III. Bipartite Transformations 26

3.1 Overview of Known Results 27
3.2 Optimizing One-Way Transformations 30
3.3 Deciding Unitary Equivalence Between Sets of States 32
3.3.1 The Algorithm 36

IV. Multipartite to Bipartite Transformations 39

4.1 Multipartite to Bipartite Entanglement Transformations and Polynomial Identity Testing 40
4.2 Multipartite Transformations with One-Way Classical Communication and the Geometric Measure of Entanglement 47

V. Tripartite Transformations 51

5.1 Overview of Known Results 51
5.2 Equivalence in $2 \otimes m \otimes n$ Systems 53
5.2.1 Matrix Pencils 56
5.2.2 Connection to $2 \otimes m \otimes n$ Pure States 58
5.2.3 Equivalence Algorithm 64
5.2.4 The State Kronecker Canonical Form 66
5.2.5 All Tripartite Systems with a Finite SLOCC Equivalence Partitioning 67

5.2.6 Non-Invertible Transformations 72
5.3 Tripartite Transformations, Tensor Rank and Matrix Multiplication 77
5.4 The Tensor Rank of Symmetric States and $|W\rangle^{\otimes n}$ 85

VI. Conclusion 91

BIBLIOGRAPHY **94**

LIST OF FIGURES

Figure

2.1 Possible relationships between complexity classes with arrows indicating problem reductions: problem (3) solves (2) solves (1). (a) P⊂BPP, P≠NP, (b) P⊂BPP, P≠NP, and (c) P=BPP, P≠NP. 17

5.1 Complete Hierarchy of SLOCC Equivalence Classes; Arrows Indicate a Non-invertible Transformation. 75

ABSTRACT

Computational Complexity in Entanglement Transformations

by

Eric A. Chitambar

Chair: Yaoyun Shi

In physics, systems having three parts are typically much more difficult to analyze than those having just two. Even in classical mechanics, predicting the motion of three interacting celestial bodies remains an insurmountable challenge while the analogous two-body problem has an elementary solution. It is as if just by adding a third party, a fundamental change occurs in the structure of the problem that renders it unsolvable.

In this thesis, we demonstrate how such an effect is likewise present in the theory of quantum entanglement. In fact, the complexity differences between two-party and three-party entanglement become quite conspicuous when comparing the difficulty in deciding what state changes are possible for these systems when no additional entanglement is consumed in the transformation process. We examine this entanglement transformation question and its variants in the language of computational complexity theory, a powerful subject that formalizes the concept of problem difficulty.

Since deciding feasibility of a specified bipartite transformation is relatively easy, this task belongs to the complexity class P. On the other hand, for tripartite systems, we find the problem to be NP-Hard, meaning that its solution is at least as hard as the solution to some of the most difficult problems humans have encountered. One can then rigorously defend the assertion that a fundamental complexity difference exists between bipartite and tripartite entanglement since unlike the former, the full range of forms realizable by the latter is incalculable (assuming P$\neq$ NP). However, similar to the three-body celestial problem, when one examines a special subclass of the problem - invertible transformations on systems having at least one qubit subsystem - we prove that the problem can be solved efficiently.

As a hybrid of the two questions, we find that the question of tripartite to bipartite transformations can be solved by an efficient randomized algorithm. Our results are obtained by encoding well-studied computational problems such as polynomial identity testing and tensor rank into questions of entanglement transformation. In this way, entanglement theory provides a physical manifestation of some of the most puzzling and abstract classical computation questions.

CHAPTER I

Introduction

Quantum Mechanics and the Theory of Computation Unite

In addition to its flawless experimental success, one of the most remarkable aspects of quantum mechanics is its strong mathematical foundation. Although much of the theory was understood before his time, von Neumann was the first to give the assertions of quantum mechanics a precise mathematical formulation in the 1930s [108]. Subsequent work has axiomatized quantum mechanics to the point that, of the foundational disagreements that remain, the primary issues typically involve interpreting what these axioms imply about the nature of our universe. While such philosophical debates are indeed important, the pragmatic physicist can brush them aside and be content with a theory whose laws have yet to be challenged by experimental data.

However, even the pragmatic physicist cannot rest too contently since there still is a practical matter of how easily these laws enable one to compute whether or not a given physical process is possible. Upon the construction of quantum theory, and especially after von Neumann's mathematical formulation, any field dealing with objects on the atomic scale was faced with a new variety of algebraic problems alien to classical mechanics. On the one hand, many quantum calculations could be performed with relative ease, thus allowing for various theoretical predictions to be tested. But on the other, a large number of the important questions or calculations encountered, especially those concerning atomic structure and molecular interactions, proved quite formidable to answer or compute.

Nevertheless, the subject continued to advance, and perhaps the most exciting application of quantum mechanics today is the relatively new field of quantum information science. As an interdisciplinary subject cutting across physics, computer science, engineering, and mathematics, quantum information science is devoted to the study and construction of devices that use quantum mechanical phenomenon to process information. Whereas the operation of modern computers is limited by the classical laws of physics, the action of quantum computers is constrained only by the much broader laws of quantum mechanics. Not surprisingly, the computationally difficult problems that lurk in the structure of quantum mechanics also emerge in the problems of quantum information. Researchers have exerted much effort in trying to solve these difficult problems in full generality but often have worked around them by restricting their attention to simpler classes of problems.

This paradigm of response to difficult problems is common to nearly all fields of science. One typically either tackles the problem directly, finds a suitable and easier alternative to the problem, or perhaps applies a mixture of the tactics. However, in recent years, an alternative course of action is proving to be quite informative and useful. Instead of seeking the solution to a given problem, one asks the question *how difficult is this problem to solve?* This involves a fundamental shift in the way problems are approached as the emphasis is placed not on particular solutions, but rather on the manner in which one arrives at these solutions.

The notion of problem difficulty is made precise in the branch of computer science known as computational complexity theory, a subject that studies the minimum amount of resources required to solve computation problems by rigorously defining notions like algorithm, computation time, and computation space. Like quantum information science, it is a relatively new field with all major results discovered within the last forty years. One crowning achievement is the classification of problems into two types of complexity: those problems that can be solved in a polynomial amount of computation time (P), and those problems that allow for a solution to be verified in a polynomial amount of time (NP); here "polynomial amount" means that the amount scales as some polynomial function of the input size. Whether the two complexity classes are equivalent, i.e. whether P=NP, is one the greatest open questions in all of theoretical science and actually worth a million dollars [1]. If P≠NP as many computer scientists suspect, then a large number of important problems belonging to the class of NP cannot be realistically solved on modern computers [49].

In this thesis, we will observe many connections between quantum information and complexity theory, but it is on the issue of solving NP problems that quantum information has garnered the most attention from computer scientists. In 1994, Peter Shor published an algorithm that uses a quantum computer to find the prime factors of an integer N in a time of order $\log N$, which is incredible considering the best known algorithm for classical computers does the job in a time *exponential* in $(\log N)^{1/3}$ [93]. This quantum speed-up has two major consequences: first, many important encryption schemes - such as the RSA method used by the government and commercial institutions to securely transmit information - become decipherable if one is able to factor large numbers. It is precisely because no efficient factoring algorithm is known on modern computers that the RSA scheme is currently so secure. However, through Shor's result and the use of a quantum computer, it now becomes possible to break RSA encryption using realistic amounts of resources and thus potentially undermine the secure transmission of important information. A second and perhaps deeper consequence of Shor's algorithm is that if no polynomial-time classical algorithm exists for factoring numbers, then quantum computers are fundamentally

[1] http://www.claymath.org/millennium

more powerful than classical computers. This means that any complete theory of computation must ultimately be a quantum theory of computation. In fact, there is an even newer area of research called *quantum computation complexity theory* that examines the resources required on a quantum computer to solve a particular problem [109]. Beyond Shor's algorithm, other examples of quantum speed-ups include Grover's algorithm for list-searching and the general estimation of any NP minimization problem by a technique known as adiabatic quantum computing [55, 43]. However, because these results only compare upper bounds between classical and quantum computation, the extent to which quantum computers can actually outperform their classical counterpart is still unknown [10].

Entanglement Transformations and the Value of Complexity Theory

Very little more will be said concerning the differences between quantum and classical computers. Instead, this thesis aims to relate classical complexity theory to quantum information by investigating the inherent classical computation difficulty of some important questions encountered in quantum information, in particular those involving *quantum entanglement.* One of the most striking differences between multi-part classical and quantum systems is the ability of the latter to exist in so-called entangled states. Indeed, it was Einstein, Podalsky, and Rosen (EPR), who first argued for the incompleteness of quantum mechanics based on the bizarre non-local properties of an entangled state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ [41]. A fundamental project in quantum information is to continue EPR's train of thought by developing a richer understanding of quantum entanglement and pondering how this phenomenon might be useful in communication schemes.

For instance, the celebrated teleportation scheme discovered by Bennett *et al.* is one of the most powerful demonstrations of the feats entanglement can achieve [11]. In the protocol, a two-party system in the entangled state $|\Psi^-\rangle$ is shared between parties named

Alice and Bob. In some other local system of Alice's, she prepares an arbitrary state $|\theta\rangle$ and performs a joint measurement on this system and her half of the entangled system. She announces this measurement outcome to Bob in the form of classical information, i.e. tells him what she measured over the phone, and based on this result, Bob performs a certain operation on his half of the originally entangled system. It turns out that in the end, Bob's system will be exactly in the state $|\theta\rangle$. In total, the state $|\theta\rangle$ is "teleported" from Alice to Bob using a maximally entangled state $|\Psi^-\rangle$ and two bits of classical communication. The combination of shared entanglement and a means of classical communication is called a quantum channel since it provides the ability to transmit both classical and quantum information. In this case, the quantum channel is the state $|\Psi^-\rangle$ accompanied by the telephone line, and the quantum information communicated is the state $|\theta\rangle$.

A generalization of the previous scenario consists of some large quantum system shared among many parties. The individual parties can perform quantum manipulations only on their particular subsystem, but they can perhaps coordinate their actions by exchanging classical information. Quantum protocols of this sort are appropriately called **Local Operations and Classical Communication** (LOCC). During an LOCC protocol, the system undergoes a series of state changes which are often referred to as **entanglement transformations**. This term was first coined by Nielsen in his study of LOCC capabilities in bipartite systems [80]. Much research has been devoted to studying the range of entanglement transformations feasible by LOCC operations since they precisely identify the communication possibilities of a quantum channel [87]. As an example, imagine that Alice and Bob did not originally share the state $|\Psi^-\rangle$ but instead some other state $|\psi\rangle$. Further assume that in order to perform teleportation or perhaps some other task, it would be better if they started with the state $|\Psi^-\rangle$. The question then becomes whether the LOCC transformation of $|\psi\rangle$ into $|\Psi^-\rangle$, denoted as $|\psi\rangle \xrightarrow{\text{LOCC}} |\Phi^-\rangle$, is possible. In this thesis, we will study the computational complexity of this decision problem in general and many other variants of it.

The above examples demonstrate the importance that questions of entanglement convertibility have in quantum communication, but one may wonder whether any serious value is gained by analyzing the computational complexity of these problems. In fact, this speculation may explain the relative paucity in existent research committed to understanding the complexity of LOCC entanglement transformations. Below we provide two significant motivations for investigating the computational complexities of not only entanglement transformations, but any general problem in quantum information. First, quantum researchers gain a rigorous sense for the degree of difficulty that their problems represent, and thus have a guide for what type of questions are reasonable to ask. By determining the complexity class of a given problem, one knows exactly what sort of computational resources will solve it, or at least how it compares in difficulty to other famous and more studied problems. The important problem of quantum separability provides a fitting example of this [60]. While it is straightforward to determine whether some pure state is entangled, deciding whether a given mixed state is separable (i.e. not entangled) has been a major open problem throughout the past dozen years. However, in 2003, Gurvits proved the problem to be NP-Hard which means that it is at least as difficult to solve as all the problems in NP [56]. Prior to Gurvits' result, considerable effort had been spent trying to find a simple criterion for deciding separability. If researchers had originally approached the problem from a computational complexity perspective, they may have more quickly realized that their proposed goal was actually to prove P=NP. By first asking how difficult the problem is to solve, one can avoid frustrations and time loss on trying to find an easy solution when one may not even exist.

A second motivation for studying complexity issues in quantum information is that the analytic techniques used in one field can be applied to problems in the other. For instance, in the 1970s, Ja' Ja' used matrix pencil theory to obtain a polynomial-time algorithm for calculating the tensor rank of two bilinear forms [63]. As will be developed later in greater detail, a $2 \otimes m \otimes n$ tripartite quantum state can be represented as a pair of bilinear forms, and following Ja' Ja's lead, one can use matrix pencil theory to completely classify all forms of entanglement in such systems [25]. In the other direction, quantum information researchers have been quite clever in developing original tools for work in their own field. By establishing a broader connection with complexity theory, the techniques used in quantum information may find an application in other seemingly unrelated problems in computational theory. As an example, using properties of two common entropy measures in quantum information, Linden and coauthors were able to derive a limit on the transformation rate between certain tripartite states [73]. As we will see in Chapter V, this result places a lower bound on the so-called exponent of matrix multiplication, a quantity long sought after by computer scientists which quantifies the number of scalar multiplications required to multiply two square matrices.

We should note that the benefits gained by investigating quantum information from a computational complexity perspective can likewise be had by any other branch in theoretical science. For example, in the field of quantum chemistry, computational complexity issues have been shown to place limitations on the Density Function Theory (DFT) method for simulating systems of interacting electrons [89]. One can also equally consider the computational complexity of problems in *classical* physics, especially areas of statistical physics [84]. In part due to its youth, complexity theory has only begun to be appreciated by disciplines outside of computer science.

Outline of Thesis

With this background serving as motivation for the entire project, we now summarize the major results of this thesis. In fulfillment of our original goal, we have developed a quantitative comparison between the complexities in bipartite and multipartite entanglement transformations. From the work of Nielsen and subsequent researchers, the question of state convertibility for bipartite systems can be solved in deterministic polynomial-time, hence placing the problem in class P. Increasing the sophistication of the problem, we next consider transformations between different pairs of bipartite states under the same local unitary operation, as well as the single transformation of some N-party entangled state to one in which only two of the parties are entangled. It turns out that deciding feasibility in both these problems can be achieved by a randomized polynomial-time algorithm, thus earning it membership in the class BPP (to be defined in the next chapter). We then further increase the generality of the problem by allowing for both the initial and final states to be fully three-way entangled. This problem is found to be NP-Hard; not only is no polynomial-time algorithm (deterministic or randomized) known, but under the common belief in complexity theory that P≠NP, no such efficient algorithm exists. Hence, our results show that the transition from bipartite to tripartite systems is like the transition from P to NP-Hard. This can be taken as justification for the sentiment shared among researchers that tripartite entanglement is considerably more difficult to study than than its bipartite counterpart. In all cases, our results are obtained by showing entanglement transformations to be physical representations of some of the most well-studied problems in computer science.

At first, this may seem to place an insurmountable limitation on the abilities of quantum information science. If ever we are to design quantum communication devices, surely we will want to allow for more than just one-on-one communication such as “three-way calls” or simply general broadcasting scenarios. Does computational complexity then prohibit our ability to achieve such technologies like it does for DFT methods in quantum chemistry?

Not necessarily since it must be remembered that complexity analysis considers the worst-case scenarios, or the most difficult problems one would have to solve of a particular type. It may very well be the case that the multipartite entanglement transformations needed in mass communication schemes will not require us to make the more complex transformations.

We will arrive at the results over the course of six chapters. The first chapter provides a brief overview of some key ideas that we will borrow from complexity theory as well as an introduction to the basic elements of quantum information and entanglement theory. In Chapter III, we will discuss bipartite entanglement transformations and review the major known results. Original findings concerning bipartite LOCC protocols are also presented. Chapter IV considers the problem of distilling a bipartite pure state from some original N-party entangled state. Chapter V turns to the question of true tripartite conversions. Here, results will depend on the mathematical subjects of matrix pencil theory and tensor analysis. We provide a chart summarizing the major findings of our work in the concluding chapter.

CHAPTER II

Preliminary Material

In this chapter we provide a highly abbreviated discussion on both quantum information and computational complexity theory. We begin by reviewing basic subject matter in complexity theory. The concepts and definitions provided here will then be carried onto the next section where essential elements from quantum information theory will be quickly presented with a heavy emphasis placed on complexity issues. This chapter is by no means comprehensive and it is included just to provide the reader with enough background to appreciate the rest of the thesis. For a more thorough introduction to computational complexity theory we recommend Sipser [95], Garey and Johnson [49], and Arora and Barak [6]; while good primers for quantum information are the classics of Nielsen and Chung [81] and Kitaev [69].

2.1 Complexity Theory

The need for a theory of computation can be appreciated by anyone who has ever taken a math or physics course. Indeed, we have all had the experience of being stuck on a homework problem for hours (days?), frustrated to the point that the problem just seems "too difficult to solve." However, just when all hope has vanished, someone clever comes along and reveals a solution. You realize that the problem was actually not *that* difficult, and the apparent difficulty was really just a reflection of your short-sightedness. But what if there existed problems that not even the most clever individual could solve; what if there existed problems that were *intrinsically* difficult or even impossible to solve?

A slightly stronger question than this was first formally posed by the German mathematician David Hilbert at the beginning of the last century. Known as the *Entscheindungsproblem*, it asks whether there is "some general mechanical procedure which could, *in principle*, solve all the problems of mathematics [83]." In today's terminology, a "general mechanical procedure" for solving a problem is more commonly called an *algorithm*, and obviously to answer Hilbert's question, one must first be precise about the meaning of an algorithm. One thinker who was able to supply such a definition and resolve the *Entscheindungsproblem* was the English computer scientist Alan Turing. Turing's project was to first identify the elements essential to any procedure employed when solving a computation problem and then describe a machine that embodies exactly these elements and nothing more. The product of this abstraction is a **Turing machine**, which is a well-defined theoretical device that is able to solve a wide range of problems. In fact, the power of a Turing machine seems to be as great as possible, in the sense that if there exists *any* method for solving some computation problem, then the problem can be solved on a Turing Machine. This last assertion is known as the Church-Turing Thesis, and while it cannot be proven, its truth is nearly unanimously accepted. One can apply the Thesis by rigorously defining an **algorithm** as any set of instructions that is given to a Turing Machine to solve a particular problem. Remarkably, it turns out that there are well-posed problems that not even a Turing machine can solve. Hence, by the Church-Turing Thesis, there exists no means to solve these problems, and so the *Entscheindungsproblem* has a negative answer.

The work of Turing, Church and their contemporaries mark the birth of computer science. While this subject quickly expanded into diverse branches of research, one field of investigation has continued to study the question of problem difficulty under the name of **Computational Complexity Theory**. Turing's result can be seen as the first major result in this field. The type of problem that he asked to stump his own machine is called a decision problem since it has a "yes" or "no" answer. Any decision problem, like Turing's, that has no general solution is called **undecidable**. In addition to knowing whether a given problem is decidable, complexity theory also seeks to know the most efficient solution to the problem if one exists. The beauty of a Turing machine is that it makes rigorous the notions of computational time and space, although we will only consider time complexity here.

To demonstrate, let Σ denote some finite set of symbols and let Σ^* be the set of all finite strings of symbols from Σ. Assume we have some fixed encoding scheme such that any mathematical object we wish to discuss, whether it be numbers, graphs, vectors,...etc. can be encoded or approximately encoded by strings in Σ^*. For two sets $L_{\mathcal{D}}$ and I with $L_{\mathcal{D}} \subset I \subset \Sigma^*$, the **decision problem** $\mathcal{D}$ asks whether $x \in L_{\mathcal{D}}$ for some $x \in I$. The set I consists of elements called **instances**, and $L_{\mathcal{D}}$ is the **language** of problem $\mathcal{D}$. For example, I may be the group of males in the state of Michigan and L_D may be the group of males over six feet tall. Many other problems can also be modified into decision problem form. For instance, when maximizing or simply just calculating some function $f(x)$, one can ask: for a given $q \in \mathbb{Q}$, decide if $f(x) > q$. Throughout this thesis, whenever we speak of the complexity of some problem, we will mean the complexity of the problem when phrased as a decision problem.

By the Church-Turing thesis, $\mathcal{D}$ can be solved if and only if (iff) there exists a Turing machine that can solve it. What does it mean for a Turing machine to solve a problem? Answering this question will require a more detailed description of these theoretical objects. In short, a Turing machine M consists of some device that acts on elements $x \in \Sigma^*$ by manipulating its symbols one at a time according to some fixed set of instructions or algorithm A. Each symbol manipulation quantifies one time step in the operation of M, and M itself undergoes a state change at each time step. For every x input to M, the machine either halts in one of two final states Q_Y or Q_N after a finite number of time steps, or it never halts. If M halts, it outputs some $M(x) \in \Sigma^*$ and it is said to either accept or reject the input x depending on the whether the final state is Q_Y or Q_N respectively. Note that if M halts on every input, it is simply a function $M : \Sigma^* \to \Sigma^*$.

Let $t(n) : \mathbb{Z}^+ \to \mathbb{R}^+$ be any function. A Turing machine M has a **time complexity** of $O(t(n))$ if for any input of string size n, M halts after at most $O(t(n))$ computation steps. Now we can more formally state that a Turing machine M **solves** the problem $\mathcal{D}$ if M halts upon every input $x \in \Sigma^*$ and accepts x iff $x \in L_D$. *The difficulty of a problem can then be quantified in terms of the time complexity of the Turing machine that solves it.* We introduce the first major complexity category.

Definition 1. *The **complexity class P** consists of all decision problems that can be solved by a Turing machine having a time complexity of $O(p(n))$ where p is any polynomial function.*

For any problem in P, there exists a polynomial-time algorithm that solves it. As a general rule of thumb, decision problems belonging to the class P are those that can be solved efficiently [27]. Of course, efficiency here is measured relative to human time scales, and the idea is that a solution can be obtained in a manageable amount of time for those and only those problems in P, regardless of the input size. Famous examples include deciding whether some directed graph has a path connecting two nodes [95], whether a given integer is prime [4], and whether some semi-definite optimization program exceeds some given value [103].

One can imagine a more general Turing machine in which at each time step the specific symbolic manipulation is not determined by the instructions A. Instead, M randomly chooses one of many possible actions to perform according to some probability distribution. Then for each input $x \in \Sigma^*$, M will halt and output $y_i \in \Sigma^*$ with probability p_i for $1 \leq i \leq R$, or it will never halt with probability $1 - \sum_{i=1}^{R} p_i$. Here R indicates the number of possible branches the Turing machine can realize for the input x. As before, the halting state of M will always either be Q_Y or Q_N, and a Turing machine that behaves in this manner is called **probabilistic**. Its time complexity is $O(t(n))$ if for any input of string size n, M halts after at most $O(t(n))$ computation steps with probability one. Analogous to the deterministic case, M **solves a problem with error probability** ϵ iff M halts with probability one for all $x \in \Sigma^*$, and M halts in the accept (resp. reject) state with probability at least $1 - \epsilon$ when $x \in L_{\mathcal{D}}$ (resp. $x \notin L_{\mathcal{D}}$). Then we have

Definition 2. *The **complexity class BPP** (bounded-error probability polynomial time) consists of all decision problems that can be solved with error probability $\frac{1}{3}$ by a probabilistic Turing machine having a time complexity of $O(p(n))$ where p is any polynomial function.*

The error probability of $\frac{1}{3}$ is actually arbitrary since any algorithm can be repeated multiple times on the same input with a standard “majority wins” decision strategy used to reduce the error arbitrarily close to zero as long as $\epsilon < \frac{1}{2}$ [95]. BPP can be seen as a relaxation of the class P since the machine still makes a decision for every input within polynomial-time but now we allow for an ϵ decision error. However, it is still unclear how much more powerful computation becomes when using this relaxation, with an intriguing possibility being that $P = BPP$ [6]; we will return to this point in Chapter IV.

While no efficient solution may be known for some problem $\mathcal{D}$, there might exist easy proofs which demonstrate that x is a “yes” instance of $\mathcal{D}$ whenever $x \in L_{\mathcal{D}}$. For example, the Hamiltonian Path Problem asks whether for some directed graph there exists a path connecting one node to another passing through every node exactly once. While this problem has no known polynomial-time solution, if some graph x does possess such a path, then the path itself serves as an easy (here trivial) proof that $x \in L_{\mathcal{D}}$. In the language of Turing machines, a **polynomial verifier** for $\mathcal{D}$, is another Turing machine V with an associated polynomial p such that (i) for every $x \in L_{\mathcal{D}}$, there exists a $y \in \Sigma^*$ for which V accepts the concatenated input xy in a computation time $O(p(|x|))$, and (ii) V only accepts inputs of this form. For any xy accepted by V, y is called the **certificate** or proof for x. We thus arrive at another major complexity class.

Definition 3. *The **complexity class NP** consists of all decisions problems having a polynomial verifier.*

The letters NP stand for non-deterministic polynomial time and come from an alternative characterization of the class NP based on a non-deterministic Turing machine, a more abstract version of the probabilistic Turing machine described above. This connection will not be explored further, but it is a fundamental concept in complexity theory [95]. It should first be noted that P$\subset$ NP and it is a major open problem whether this inclusion is proper. Problems in NP that have no proven membership in P are some of the most well-studied problems in computer science. These include the Hamilton Path Problem, the Graph 3-Colorability Problem, and the solvability of a quadratic system over some finite field (see Ref. [49] for list of over 300 other problems). The mass amount of effort that has failed to discover efficient solutions to these problems supports the hypothesis that *no* polynomial-time solutions exist at all. Indeed, the belief held by most computer scientists is that there is something intrinsically different about these problems which prohibit them from being solved by more economical methods beyond brute-force.

The relationship between NP and BPP is also unknown. While it is speculated that BPP$\subseteq$NP, it is still possible that NP$\subset$BPP. In fact, the latter remains possible even if P=NP; see Fig. 2.1.

To prove that some problem belongs to a particular complexity class, the technique of reducibility is often employed. Reducibility allows one to show that some problem is no more difficult than another. Consider two problems $\mathcal{D}$ and $\mathcal{D}'$ with languages $L_{\mathcal{D}} \subset \Sigma^*$ and $L_{\mathcal{D}'} \subset \Sigma^*$ respectively. Recall that a polynomial-time Turing machine M can be regarded as a function $M : \Sigma^* \to \Sigma^*$. Then $\mathcal{D}$ is called **polynomial-time reducible** to $\mathcal{D}'$ if there exists a polynomial-time Turing machine M such that $x \in L_{\mathcal{D}}$ iff $M(x) \in L_{\mathcal{D}'}$. In this way, if there is some polynomial-time M' that solves $\mathcal{D}'$, the composition $M' \circ M$ is a polynomial-time Turing machine that solves $\mathcal{D}$. Hence solving $\mathcal{D}'$ means that at most an additional polynomial amount of resources is needed to solve $\mathcal{D}$. Conversely, if no polynomial-time algorithm solves $\mathcal{D}$, then no polynomial-time algorithm solves $\mathcal{D}'$. We introduce the following complexity definition.

Definition 4. *A problem $\mathcal{D}$ is called **NP-Hard** if every problem in NP is polynomial-time reducible to it.*

It is not at all obvious that such problems even exist. However, in his seminal paper, Cook provided examples of NP-Hard problems and since then many more have been discovered [29]. Even stronger, Cook proved the existence of NP-Hard problems that are themselves in NP. Such problems are called **NP-Complete**, and hence, to show that some problem is NP-Hard, it suffices to demonstrate that some NP-Complete problem is polynomial-time reducible to it.

By definition, if some problem is NP-Hard and P$\neq$NP, then there exists no polynomial-time algorithm for the problem. Therefore, since it is commonly believed that P$\neq$NP, proving a problem to be NP-Hard strongly suggests that it is intrinsically more complex than any other problem in P. Furthermore, even if P=NP, there still may not exist an efficient solution to the given NP-Hard problem. Twice in this thesis will we take problems previously known to be NP-Hard and polynomial-time reduce them to problems in entanglement theory. As a result, the proves the latter to be NP-Hard, thus strongly indicating their high-degree of intrinsic complexity. Possible relationships between the discussed complexity classes are provided in the following figure.

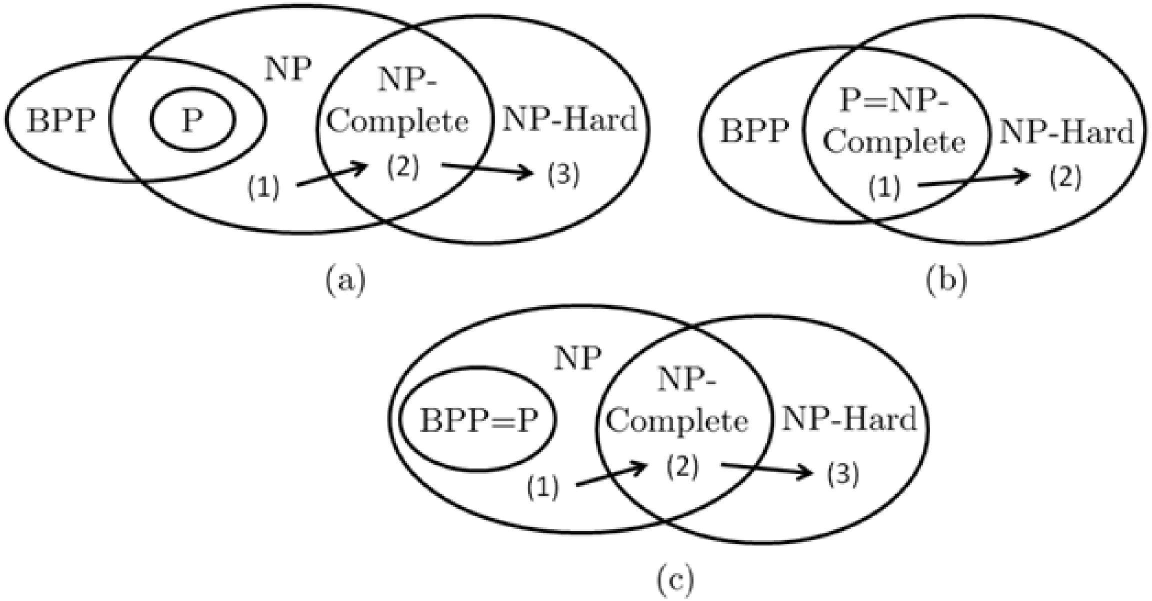

Figure 2.1: Possible relationships between complexity classes with arrows indicating problem reductions: problem (3) solves (2) solves (1). (a) P⊂BPP, P≠NP, (b) P⊂BPP, P≠NP, and (c) P=BPP, P≠NP.

It should be emphasized that when proving a problem to be in some complexity class, one does not need to provide a complete Turing machine algorithm. Instead, the algorithm just needs to be given in terms of arithmetic procedures that can be implemented on Turing machines with time complexities already known to be of some running time. This high-level description of an algorithm is how all major complexity results are proven and will be the approach we take in this thesis. The same holds true for proving reducibility of problems. Nevertheless, the language and proof techniques we will use always rest on the rigorous conceptual basis outlined in this chapter.

2.2 Quantum Information

2.2.1 Basic Formalism

The fundamental building block in quantum information is the **qubit** which, quite generally, is any physical system that can be observed in just two different states for some particular measurement. These states can be represented by the "kets" $|0\rangle$ and $|1\rangle$ and their complex linear span constitutes the **state space** of the system. Likewise, in N-dimensional systems, the kets $|0\rangle, ..., |N-1\rangle$ represent the observable states for some chosen measurement and are called a **computational basis** of state space. Any linear combination $|\psi\rangle = \sum_{i=0}^{n-1} c_i|i\rangle$ corresponds to a **pure state** of the system, and any convex combination, or classical ensemble, of pure states is called a **mixed state** with a linear operator representation $\rho = \sum_{i=1}^{k} p_i|\psi_i\rangle\langle\psi_i|$. The primary object of our investigation will be pure states, and consequently, much of the theory presented below will not be discussed in its full mixed state generality.

When two or more systems are combined, their joint state space is described by the tensor product of the individual subspaces: $\mathbb{C}^{d_1} \otimes ... \otimes \mathbb{C}^{d_N}$ where d_i is the local dimension of system i. We will also denote this space as $d_1 \otimes ... \otimes d_N$. A state $|\psi\rangle \in d_1 \otimes ... \otimes d_N$ is called **separable**, or a product state, if it can be written a tensor product of vectors: $|\psi\rangle = |\alpha_1\rangle \otimes ... \otimes |\alpha_N\rangle$ for $|\alpha_i\rangle \in \mathbb{C}^{d_i}$. Otherwise, the state is said to be **entangled**. For mixed states, these definitions are generalized such that a state ρ is separable iff it can be represented as a convex combination of product states. If $\rho_{1...N}$ is some N-party state, the local state of the i^{th} party, denoted as ρ_i, is called a **reduced state** and is obtained by the partial trace over all but the i^{th} subsystem: $\rho_i = tr_{\bar{i}}(\rho_{1...N})$. We observe that a pure state $|\psi\rangle$ is separable iff $|\psi\rangle\langle\psi| = \rho_1 \otimes ... \otimes \rho_N$ where ρ_i is the i^{th} party reduced state of $|\psi\rangle$; consequently, pure state separability can be decided by checking whether each ρ_i is a rank one matrix. In stark contrast to this very simple computational task, it is NP-Hard to decide mixed state separability, even for bipartite states [56].

Typically, the term multipartite is reserved for describing systems with at least three or more subsystems. The primary reason for making such a distinction is that bipartite systems possess special properties not had by systems of more parties. In fact, the overarching theme of this thesis is how the unique structure of bipartite states affects questions on computational complexity. The major benefit in working with bipartite pure states is that they can be represented by scalar matrices. Letting $\{|i\rangle_A\}_{i=1...d_A}$ and $\{|i\rangle_B\}_{i=1...d_B}$ denote arbitrary bases for Alice and Bob's space respectively, any bipartite state $|\psi\rangle$ can be written as $|\psi\rangle = \sum_{i,j=1}^{d_A,d_B} c_{ij}|i\rangle_A|j\rangle_B$. Then $|\psi\rangle$ can be uniquely identified with a $d_B \times d_A$ matrix Ψ by $|\psi\rangle = (I \otimes \Psi)|\Phi_r\rangle$ where $|\Phi_r\rangle = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}|i\rangle_A|i\rangle_B$, $r = \min\{d_A, d_B\}$, and $[\Psi]_{ij} = c_{ij}$.

This matrix representation allows for a **Schmidt decomposition** of states, which essentially is a singular value decomposition on Ψ and is one of the most valuable tools in studying bipartite systems. Any bipartite state $|\psi\rangle$ can be expressed as $|\psi\rangle = \sum_{i=1}^{r}\lambda_i|\alpha_i\rangle|\beta_i\rangle$ where the $|\alpha_i\rangle$ and $|\beta_i\rangle$ are orthonormal bases for Alice and Bob's subsystems respectively, and the $\lambda_i > 0$ are called the **Schmidt coefficients** of $|\psi\rangle$. While there may exist some freedom in the choice of bases, the number r, called the **Schmidt rank**, is unique to the state $|\psi\rangle$ and is denoted by $Sch(\psi)$. Note that $Sch(\psi)$ is equal to the matrix rank of Ψ. One important feature of the Schmidt rank is that it is a multiplicative quantity; i.e. for two states $|\psi\rangle_{AB}$ and $|\phi\rangle_{AB}$, $Sch(|\psi\rangle_{AB} \otimes |\phi\rangle_{AB}) = Sch(\psi) \cdot Sch(\phi)$.

For multipartite states, the Schmidt decomposition has only a partial generalization. Any state $|\psi\rangle_{1...N}$ can always be expanded as a sum of product states by choosing some product state basis for the space $\mathbb{C}^{d_1} \otimes ... \otimes \mathbb{C}^{d_N}$. The tensor rank of a state $|\psi\rangle$, denoted as $rk(\psi)$ is the minimum number r such that there exists $|\phi_j\rangle_i \in \mathbb{C}^{d_i}$, $1 \leq j \leq r$ and

$$|\phi\rangle = \sum_{j=1}^{r}\bigotimes_{i=1}^{N}|\phi_j\rangle_i.$$

When $|\psi\rangle$ is bipartite, we have $Sch(\psi) = rk(\psi)$. Tensor rank provides another manner for characterizing entanglement since a multipartite state $|\psi\rangle$ is entangled iff $rk(\psi) > 1$. While, as noted above, it is fairly easy to decide if $rk(\psi) > 1$, determining its exact value has been proven by Haåstad to be NP-Hard [57]. Although separability and tensor rank are each NP-Hard questions, there does not seem to be a direct connection between the two.

2.2.2 Entanglement Measures and LOCC Operations

In both theoretical and experimental settings, it is often useful to define a distance measure on state space so that one can meaningfully discuss how "close" two states are to one another. Various distance measures have been proposed [50], but one of the most useful is the **fidelity** between two states. For two general states ρ and σ, their fidelity is defined as $F(\rho, \sigma) = tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}$. The fidelity measure has many rich properties in general [101], but for our purposes it is enough to observe that the fidelity of pure states $|\psi\rangle$ and $|\phi\rangle$ reduces to $tr\sqrt{|\psi\rangle\langle\psi|\phi\rangle\langle\phi|\psi\rangle\langle\psi|} = |\langle\psi|\phi\rangle|$. Interpreting this geometrically, the fidelity measures the closeness of two states by the degree of their inner product. From a physical perspective, the fidelity between two pure states stipulates how well the states can be distinguished [64]; if one is given either the state $|\psi\rangle$ or $|\phi\rangle$ with equal probability, the maximum probability of correctly identifying the state is $P_{max}(|\psi\rangle, |\phi\rangle) = 1 - |\langle\psi|\phi\rangle|$ [62, 37, 85].

A related project in quantum information has involved trying to quantify the amount of entanglement present in some state of a given system [87]. Shortly after work began in this direction, it was realized that no single quantification or entanglement measure can fully capture a state's non-classical properties. Quite generally, any valid entanglement measure is some function mapping quantum states to the real numbers that satisfies a list of certain properties [104]. While the details of these properties are not important to the present discussion, we note that one necessary property of any entanglement measure is its vanishing when acting on separable states. As separability is an NP-Hard problem, *this implies that the evaluation of any mixed state entanglement measure is NP-Hard.*

However, there are entanglement measures that apply only to pure states. One such example is the **geometric measure of entanglement** $G_M : \mathbb{C}^{d_1} \otimes ... \otimes \mathbb{C}^{d_N} \to \mathbb{R}$ defined as

$$G_M(|\psi\rangle) = \max |\langle \omega | \psi \rangle|$$

where the maximization is taken over all product states $|\omega\rangle$. The geometric measure has been studied in some detail within the quantum information community [92, 7, 110, 82], however, its computational complexity has yet to be considered. In Chapter IV we will prove that calculating the geometric measure is NP-Hard.

The proceeding discussion has pertained entirely to the analysis and classification of states realized by some quantum system. We now consider the *dynamics* of a quantum system and the states physically accessible to it. In general, any change of state in a closed quantum system is described by a unitary evolution; if a closed system is in state $|\psi(t_0)\rangle$ at time t_0, any future state can be described by $U|\psi(t_0)\rangle$, with U a unitary operator. When some external object interacts with the system, it is no longer closed and its evolution need not be unitary. Any such interaction can be modeled by a measurement process on the system, also known as a **quantum operation**. The most general physically realizable quantum operation is described by a set of operators $\{M_k\}_{k=1...m}$ that satisfy the trace preserving constraint $\sum_{k=1}^{m} M_k^\dagger M_k = I$ [90, 81]. For a system initially in state $|\psi\rangle$, the act of measurement $\{M_k\}_{k=1...m}$ causes the state change $|\psi\rangle \to \frac{M_k|\psi\rangle}{\sqrt{p_k}}$ with probability $\langle\psi|M_k^\dagger M_k|\psi\rangle$, and an observer would report obtaining outcome k. Note that if we inquire whether a particular transformation $|\psi\rangle \to |\phi\rangle$ is possible with just some nonzero probability, it is enough to ask whether there exists an operator M such that $M|\psi\rangle = |\phi\rangle$. Indeed, if this equality holds, then by defining $\hat{M} = \frac{M}{\sqrt{||M^\dagger M||}}$, the operation $\{\hat{M}, \sqrt{I - \hat{M}^\dagger \hat{M}}\}$ constitutes a valid measurement that transforms $|\psi\rangle \to |\phi\rangle$ with probability $\frac{1}{||M^\dagger M||}$. Here, $||\cdot||$ denotes the operator norm: $||M|| = \sup\{\langle\psi|M_k^\dagger M_k|\psi\rangle : \langle\psi|\psi\rangle = 1\}$.

For states shared between multiple parties, additional constraints are typically placed on the type of feasible quantum operations to better reflect physical scenarios. When entanglement is distributed among many parties, it generally becomes very difficult to manipulate the system as a whole without introducing corruptive environmental interactions, a consideration obviously relevant to any long-distance quantum communication. One solution to this problem is to concede the ability of global operations and require that the only quantum operations performed are done so locally, by each party acting just on his/her particular subsystem. While still allowing parties to share classical information with one another, manipulation protocols of this type are the local operations and classical communication (LOCC) operations first described in the Introduction. With respect to any meaningful entanglement measure, the set of LOCC operations are precisely those multipartite operations that cannot on average increase the entanglement of a system but may introduce classical correlations among the subsystems [107]. Although this definition is relatively intuitive, translating it into a formal mathematical characterization is still a large open problem in quantum information.

Fortunately, any LOCC operation belongs to the more general class of *separable operations* which does have a rather special and compact mathematical form. In an N-party system $\mathbb{C}^{d_1} \otimes ... \otimes \mathbb{C}^{d_N}$, a quantum operation $\{M_k\}_{k=1...m}$ is called separable if each M_k has a tensor product form: $M_k = \bigotimes_{i=1}^N A_{ki}$ where A_{ki} acts on the space $\mathbb{C}^{d_i}$. To see that every LOCC operation is a separable operation, consider the simple case of just two parties sharing a state $|\psi\rangle$. If Alice first applies a local operation described by operators $\{A_k\}_{k=1...m_1}$ and obtains outcome j_1, the resultant state is $\frac{1}{\sqrt{p_{j_1}}} A_{j_1} \otimes I_B|\psi\rangle$. She then communicates to Bob her measurement result, and based on this knowledge, Bob applies local operators $\{B_k^{(j_1)}\}_{k=1\ldots m_2}$. If he obtains outcome j_2, then the state becomes $\frac{1}{\sqrt{p_{j_1}p_{j_2}}}A_{j_1} \otimes B_{j_2}^{(j_1)}|\psi\rangle$. This process is then repeated, and a tree of measurement outcomes is obtained. After the M^{th} round, each branch of the tree will correspond to the action of an operator

$$(A_{j_{M-1}}^{(j_{M-2},j_{M-3},\ldots,j_1)}A_{j_{M-3}}^{(j_{M-4},\ldots,j_1)}\cdots A_{j_1}) \otimes (B_{j_M}^{(j_{M-1},j_{M-2},\ldots,j_1)}B_{j_{M-2}}^{(j_{M-3},\ldots,j_1)}\cdots B_{j_2}^{(j_1)})$$

which is in tensor product form. Hence the entire operation is described by a set of tensor product operators and so by definition is a separable operation. The final state of every branch in an LOCC protocol is of the form $(A_i \otimes B_i)|\psi\rangle$. It should be noted that, as a somewhat surprising result, the class of separable operations is strictly larger than the class of LOCC [12, 23].

In many cases, we may only want to consider LOCC operations that succeed with a nonzero probability. Such transformations are called **Stochastic Local Operations assisted by Classical Communication** (SLOCC). Hence, an SLOCC transformation simply refers to the transformation corresponding to some single branch in an LOCC protocol. For notation, a state $|\psi\rangle$ that can be transformed into $|\phi\rangle$ by SLOCC with just some nonzero probability will be denoted as $|\psi\rangle \xrightarrow{\text{SLOCC}} |\phi\rangle$. If a specific probability p is given for the transformation, then the description will be $|\psi\rangle \xrightarrow{\text{SLOCC}} |\phi\rangle$ "with success probability p." If $p = 1$, the transformation is called deterministic and symbolized as $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle$.

As we observe above, for some initial state $|\psi\rangle_{1\ldots N}$, every possible final state in an LOCC protocol can be written as $(A_1 \otimes \ldots \otimes A_N)|\psi\rangle_{1\ldots N}$. The action of any element from $\mathbb{C}^{d_1\times d_1} \otimes \ldots \otimes \mathbb{C}^{d_N\times d_N}$ on $|\psi\rangle_{1\ldots N}$ is called a **contraction** on the state $|\psi\rangle$, or a one-shot transformation. Contractions on bipartite pure states have a very nice representation. Let $|\psi\rangle_{AB}$ be any such state, and Ψ its corresponding matrix representation, i.e. $|\psi\rangle_{AB} = (I \otimes \Psi)|\Phi_r\rangle$. Then it is easy to verify that the contraction $(A \otimes B)|\psi\rangle$ corresponds to the matrix transformation $\Psi \to A\Psi B^T$.

We now observe a very important fact that provides a good starting point for investigating any SLOCC convertibility problem.

Lemma 1. [39] *For N-partite states, $|\psi\rangle$ and $|\phi\rangle$, $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ iff there exists local operators $A_1, ..., A_N$ such that $(A_1 \otimes ... \otimes A_N)|\psi\rangle = |\phi\rangle$.*

Indeed, if this equality holds, then for some nonzero λ we have $(\hat{A}_1 \otimes ... \otimes \hat{A}_N)|\psi\rangle = \lambda|\phi\rangle$ where $||\hat{A}_k A_k^\dagger|| \leq 1$. Consequently for the LOCC protocol in which the k^{th} party performs the operation $\{\hat{A}_k, \sqrt{I - A_k A_k^\dagger}\}$, $|\phi\rangle$, the state $|\phi\rangle$ will be obtained with some nonzero probability $|\lambda|^2$. In summary, then, every contraction corresponds to some probabilistic LOCC transformation.

2.2.3 Entanglement Partial Ordering

Finally, we close the chapter by describing how convertibility can be used to order some multipartite state space. A natural ordering of $d_1 \otimes ... \otimes d_N$ can be generated by defining $|\psi\rangle \geq |\phi\rangle$ iff $|\psi\rangle \to |\phi\rangle$ by an operation belonging *any* specified class of quantum operations. In general, this will only define a partial ordering of state space regardless of what class of operations are considered. Every partial ordering induces an equivalence relation by $|\psi\rangle \sim |\phi\rangle$ iff $|\psi\rangle \geq |\phi\rangle$ and $|\phi\rangle \geq |\psi\rangle$. Consequently for any class of quantum operations, we can consider the equivalence classes it generates in state space by using this operational definition of equivalence.

Bennett *et al.* made the important observation that if one uses deterministic LOCC convertibility to define a partial ordering, then two states are equivalent iff they are related by a local unitary (LU) transformation [13]. Thus LOCC equivalence classes are simply the orbits of local unitary operations in multipartite systems. However, such a partitioning is too fine for most interests; even in the two-qubit case, there exists an infinite number of LU equivalence classes. A much coarser partitioning is achieved by considering the partial ordering of SLOCC convertibility: $|\psi\rangle \geq |\phi\rangle$ iff $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$. By the above discussion, if two states are equivalent by this convertibility criterion, then there exists two contractions $(A_1 \otimes ... \otimes A_N)|\psi\rangle = |\phi\rangle$ and $(A'_1 \otimes ... \otimes A'_n)|\phi\rangle = |\psi\rangle$. Combining these equations we have $(A'_1 A_1 \otimes ... \otimes A'_N A_N)|\psi\rangle = |\psi\rangle$. Then by considering the bipartition of $|\psi\rangle$ between party i and the other $N-1$ parties, we have $(A'_i A_i)\Psi(\bigotimes_{j \neq i} A'_j A_j) = \Psi$ which implies that all the A_k and A'_k must be full rank matrices. Conversely, if $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ by local invertible operators, i.e. $(A_1 \otimes ... \otimes A_N)|\psi\rangle = |\phi\rangle$, then obviously $|\phi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\psi\rangle$ by contraction $A_1^{-1} \otimes ... \otimes A_N^{-1}$. Therefore, we have just demonstrated that SLOCC equivalence classes are precisely the orbits under local invertible linear transformations [39]. We will return to this characterization in the next chapter, but it will be very important in Chapter V when we consider SLOCC equivalence in $2 \otimes m \otimes n$ systems.

CHAPTER III

Bipartite Transformations

In this chapter, we will review the major results in the study of bipartite entanglement transformations. For pure states, most of the interesting questions have been answered and can be summarized using the the language of vector majorization. However, there are still new results to be found and we succeed in providing two such original contributions below. In Section 3.2, we resolve a problem left open in Ref. [35] concerning the maximum probability of one-way classical communication SLOCC transformations in bipartite systems. We are able to present a semi-definite program to solve the problem which can be solved efficiently using convex optimization computer packages such as SeDuMi. This result will become even more interesting in Chapter IV when we find the optimization of one-way SLOCC contractions in multipartite systems to be NP-Hard. Finally in Section 3.3 we consider the problem of simultaneous local unitary (LU) equivalence between pairs of bipartite states. We present a randomized polynomial-time decision algorithm that solves this problem while also having applicability in a wide range of other problems. Although nearly all content in this thesis applies to pure states, in Section 3.3 we also consider mixed state LU equivalence.

3.1 Overview of Known Results

Before proceeding, we should emphasize that the object of investigation in this thesis is *exact* state transformations on finite-dimensional systems. Nevertheless, we must at least mention the alternative consideration of *asymptotic* LOCC transformations since this is a fundamental concept in quantum information. We say that $|\psi\rangle$ can be asymptotically transformed into $|\phi\rangle$ at a rate R if for every $\delta > 0$, there exists an integer n and an LOCC protocol that maps $|\psi\rangle^{\otimes Rn} \overset{\text{LOCC}}{\longrightarrow} \rho$ such that $F(\rho, |\phi\rangle^{\otimes n}) > 1 - \delta$. One motivation for studying asymptotic transformations is to formally justify the interpretation of entanglement as a fungible resource for information processing. If two states possess a different amount of entanglement, then by considering multiple copies of each state in the correct ratio, we would hope to obtain two multi-copied states of the same entanglement and thus of equal value for any entanglement-assisted task.

As an analogy, suppose I own stock A valued at x dollars and you own stock B valued at y dollars. If we want to fairly trade stocks, then I should give you $\frac{y}{x}$ shares of A for every share of B you give me. But if we can only trade shares in integer amounts - I trade an integer n and you an integer m - then the best we can do is hope there exists n and m such that $n\frac{y}{x} = m$. While this may not be possible if x or y is irrational, it is always possible to approach $\frac{y}{x}$ arbitrarily close by making sufficiently large enough choices for m and n. In this case, we have an exchange of monetary value being as close to equal as desired. This is the idea of asymptotic entanglement transformations; while two states $|\psi\rangle$ and $|\phi\rangle$ may not possess the same amount of entanglement, we would still like to move between the states in a manner that preserves the entanglement and hence is reversible. For bipartite states, this is always possible by taking many copies of each state and extending to the asymptotic regime. In a beautiful result by Bennett and coworkers, for bipartite states $|\psi\rangle$ and $|\phi\rangle$ the transformations $|\psi\rangle^{\otimes m} \overset{\text{LOCC}}{\longrightarrow} |\phi\rangle^{\otimes n}$ and $|\phi\rangle^{\otimes n} \overset{\text{LOCC}}{\longrightarrow} |\psi\rangle^{\otimes m}$ are asymptotically possible at a rate $\frac{m}{n} \approx \frac{S(|\phi\rangle)}{S(|\psi\rangle)}$ where $S(|\cdot\rangle) = -tr(\rho_A \log_2 \rho_A)$ indicates the von Neumann entropy for $\rho_A = tr_B(|\cdot\rangle\langle\cdot|)$ [9].

As important as asymptotic theory is to quantum information, the study of finite transformations is vitally important to the community as well. For one thing, only a finite number of states are encountered in any experimental scenario. True it is possible to obtain a nearly "lossless" exchange of entanglement between two bipartite states, but the amount of shared entanglement required to obtain this fidelity only grows with the desired precision. Another concern is that asymptotic analysis only deals with sharply peaked averages, and hence there will always be a nonzero probability of deviating from these averages [75]. In order to study exact transformations and not just average behavior, one must abandon the asymptotic framework and consider finite copy transformations.

For bipartite transformations of this type, one of the most fascinating discoveries is how neatly the subject can be packaged in terms of vector majorization theory. Let $x^{\uparrow} = (x_1, ..., x_n)$ and $y^{\uparrow} = (y_1, ..., y_n)$ be two elements of $\mathbb{R}^n$ ordered such that $x_i \leq x_j$ for $i < j$ and likewise for $y^{\uparrow}$. The ordered vector $x^{\uparrow}$ is said to **supermajorize** $y^{\uparrow}$, denoted by $x^{\uparrow} \prec^w y^{\uparrow}$, if

$$\sum_{j=1}^{k} x_j^{\uparrow} \geq \sum_{j=1}^{k} y_j^{\uparrow} \quad 1 \leq k \leq n.$$

If $x^{\uparrow} \prec^w y^{\uparrow}$ and in addition $\sum_{j=1}^{n} x_j^{\uparrow} = \sum_{j=1}^{n} y_j^{\uparrow}$, then $x^{\uparrow}$ is said to **majorize** $y^{\uparrow}$, denoted by $x^{\uparrow} \prec y^{\uparrow}$.

Foundational work on the theory bipartite entanglement transformations was done by Lo and Popescu [75]. Using their results, Nielsen was the first to develop a full connection between this problem and majorization theory [80], while other researchers were able to complement or generalize his work [67, 106, 35]. We summarize the findings of the above investigators. In the following, for state $|\psi\rangle$, let $\lambda(\psi)^{\uparrow}$ denote the vector of non-decreasing eigenvalues belonging to the matrix $\psi\psi^{\dagger}$, where ψ is the matrix representation of $|\psi\rangle$ (see

Section 2.2.1).

Theorem 3.1.

(a) *Two bipartite states $|\psi\rangle$ and $|\phi\rangle$ are LU equivalent iff they have the same Schmidt coefficients (including multiplicity).*

(b) [75, 106] *For any $|\psi\rangle$ and $|\phi\rangle$, the transformation $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ is possible iff $Sch(\psi) \geq Sch(\phi)$.*

(c) [80, 106, 35] *The transformation $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ can occur with probability p iff*

$$\lambda(\psi)^{\uparrow} \prec^{w} p\lambda(\phi)^{\uparrow}.$$

Although (a) is essentially a statement of the singular value decomposition, we include it in the theorem since LU convertibility is a very important type of entanglement transformation. In Section 2.2.2, we mentioned an area of research that attempts to quantify the amount of entanglement present in the state of some system. As noted, one property that all measures satisfy is that the vanish for separable states. Another common property of all useful measures is that entanglement cannot increase on average under LOCC operations; *global* actions are required to increase entanglement [107]. Because of the reversibility in unitary evolution, an immediate consequence of this is that for all entanglement measures, entanglement remains constant under local unitary operations (LU). As a result, studying LU equivalence is important since it identifies states that have the same amount of entanglement.

We also note that item (b) is actually a consequence of item (c). However, we state it in isolation because of its independent importance when we compare it to multipartite case. In terms of computational cost, Theorem (3.1) shows thats nearly all important bipartite entanglement transformation questions can be solved relatively quickly, even by just using a pocket calculator.

Concerning the ordering of bipartite state space, item (c) characterizes the partial ordering induced by LOCC convertibility: $|\psi\rangle \geq |\phi\rangle$ iff $|\psi\rangle \overset{\text{LOCC}}{\longrightarrow} |\phi\rangle$ iff $\lambda(\psi) \prec \lambda(\phi)$. As mentioned in Section 2.2.3, states are equivalent iff they both satisfy (a). Of course, LOCC generates only a partial ordering of states since there exists vectors in which neither majorizes the other. On other hand, item (b) shows that SLOCC convertibility provides a *total* ordering: $|\psi\rangle \geq |\phi\rangle$ iff $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ iff $Sch(|\psi\rangle) \geq Sch(|\phi\rangle)$. We will observe in Chapter V that, in general, SLOCC convertibility only induces a partial ordering in multipartite systems.

3.2 Optimizing One-Way Transformations

One of the key steps in proving Theorem (3.1) is a result first presented by Lo and Popescu [75]. For any operators A and B, there exists an A' and unitary operator U such that $(A \otimes B)|\psi\rangle = (A' \otimes U)|\psi\rangle$. If we take A and B to be SLOCC operators of Alice and Bob respectively, this physically says that any Alice and Bob contraction can be replaced by another contraction in which Alice applies some operator and Bob acts with a unitary operation. Note that if $(A \otimes B)|\psi\rangle$ is the final state in one branch of an LOCC protocol, this requires both parties to classically communicate (over the phone) to one another that A and B were, in fact, the operators they happened to apply during the measurement process. However, if $(A' \otimes U)|\psi\rangle$ is the final state in one branch of an LOCC protocol, than only Alice needs to inform Bob that she applied A' since Bob's action is deterministic; i.e. Alice needs no confirmation on what operator Bob performs since there is no indeterminism in his applying a unitary operation.

Since every branch in an LOCC protocol corresponds to single contraction on the original state, any round in which Bob acts can be equivalently replaced by a round in which Alice applies some measurement, broadcasts her measurement result classically, and then Bob applies the suitable unitary based on this result. Consequently, there is no stochastic element at all to Bob's action and therefore it is unnecessary for him to communicate anything to Alice throughout the whole transformation. Therefore, in summary, Lo and Popescu's result shows that *for bipartite pure state transformations, one-way classical communication between Alice and Bob is just as strong as two-way communication* [75].

Despite the power of this finding, it should be stressed that when replacing a contraction $(A \otimes B)|\psi\rangle$ with $(A' \otimes U)|\psi\rangle$, the probability of realizing the branch $(A' \otimes U)|\psi\rangle$ in the corresponding new LOCC protocol will, in general, not be as large as realizing the branch $(A \otimes B)|\psi\rangle$ in the original protocol. For deterministic transformations, this does not matter since every branch obtains the same final state and thus the probability of individual branches is irrelevant. However, for general SLOCC transformations, this is not the case.

The natural question, then, is for bipartite pure state transformations, what is the maximum one-shot probability of $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$ if only one-way classical communication is allowed between Alice and Bob? In Ref. [35], the authors provide a criterion stipulating when such a transformation can occur with some probability, but no algorithmic procedure is given to decide whether this criterion is satisfied. Below we state the problem as a semi-definite programming procedure that can be solved in polynomial computation time. In Section 4.2 we will see that this problem is NP-Hard in the multipartite setting.

In matrix form, the transformation $M \otimes U|\psi\rangle = \sqrt{p}|\phi\rangle$ becomes $M\psi = \sqrt{p}\phi U^\dagger$. To maximize p, the equivalent formulations are:

$$\begin{aligned}
&\max\ p && && \min\ ||M^\dagger M|| \\
&\text{s.t. } M\psi = \sqrt{p}\phi U^\dagger, && \Leftrightarrow && \text{s.t. } M\psi = \phi U^\dagger, \\
&\quad U \text{ is unitary}, && && \quad U \text{ is unitary}. \\
&\quad ||M^\dagger M|| \leq 1. && &&
\end{aligned} \tag{3.1}$$

By a polar decomposition of ϕ, we have $\phi U^\dagger = \sqrt{\phi\phi^\dagger} W = W\sqrt{\phi^\dagger\phi}$. So the second constraint on the right becomes $M\psi = W\sqrt{\phi^\dagger\phi}$ where W is some unitary. But this is true iff $\psi^\dagger M^\dagger M\psi = \phi^\dagger\phi$. In other words, we want to minimize the largest eigenvalue of some matrix X subject to $\psi^\dagger X\psi = \phi^\dagger\phi$ and $X \geq 0$. This can be phrased as the semidefinite minimization problem [103]:

$$\begin{aligned} \min\ & \lambda \\ \text{s.t.}\ & \lambda I - X \geq 0 \\ & \psi^\dagger X \psi = \phi^\dagger \phi, \\ & X \geq 0. \end{aligned} \tag{3.2}$$

It is desirable to express the above in terms of real variables. Since X is hermitian, it has the expansion $X = X_0 + iX_1$ where X_0 is real symmetric and X_1 is real skew-symmetric. In this case, it is easy to verify that $X \geq 0$ iff $\tilde{X} = \left(\begin{smallmatrix} X_0 & -X_1 \\ X_1 & X_0 \end{smallmatrix}\right) \geq 0$ where $\tilde{X}$ is a real symmetric matrix. The first constraint above becomes $(\lambda I - X_0) + iX_1 \geq 0$ which is again true iff $\lambda I - \tilde{X} \geq 0$. To handle the second constraint, we decompose into real and imaginary parts $\psi = \psi_0 + i\psi_1$ and $\phi = \phi_0 + i\phi_1$. Then let $\tilde{\psi} = \left(\begin{smallmatrix} \psi_0 & -\psi_1 \\ \psi_1 & \psi_0 \end{smallmatrix}\right)$ and $\tilde{\phi} = \left(\begin{smallmatrix} \phi_0^\dagger\phi_0 + \phi_1^\dagger\phi_1 & -\phi_0^\dagger\phi_1 + \phi_1^\dagger\phi_0 \\ \phi_0^\dagger\phi_1 - \phi_1^\dagger\phi_0 & \phi_0^\dagger\phi_0 + \phi_1^\dagger\phi_1 \end{smallmatrix}\right)$, and so the final real SDP is

$$\begin{aligned} \min\ & \lambda \\ \text{s.t.}\ & \lambda I - \tilde{X} \geq 0 \\ & \tilde{\psi}^\dagger \tilde{X} \tilde{\psi} = \tilde{\phi}^\dagger \tilde{\phi}, \\ & \tilde{X} \geq 0. \end{aligned} \tag{3.3}$$

As discussed in [103], efficient algorithm are known that can solve this problem

3.3 Deciding Unitary Equivalence Between Sets of States

Theorem (3.1) part (a) presents an easy criterion for deciding when two bipartite pure states are LU equivalent. Here, we generalize and investigate the question of when two sets of bipartite states are simultaneously related by a local unitary operation. More precisely, given two sets of possibly mixed states $\{\rho_0, ..., \rho_m\}$ and $\{\sigma_0, ..., \sigma_m\}$ shared between parties Alice and Bob, when is it possible for the duo to apply a fixed local unitary operation that can pairwise transform $\rho_i \xrightarrow{\text{LU}} \sigma_i$ for $0 \leq i < m$. Physically, this corresponds to the scenario in which Alice and Bob are secretly given one of $m+1$ possible states and they wish to know the full range of final states they could possibly obtain through local actions without changing the amount of entanglement in their shared state.

For generic (possibly mixed) states, equivalence between a single pair ρ and σ is determined by a set of trace invariants [5, 99], however, the full solution to bipartite mixed state LU equivalence still remains open. The generalization of this question to simultaneous LU equivalence between multiple pairs of states has yet to be addressed, and such an investigation nicely complements previous work on simultaneous state transformations under global operations [20, 19, 45] and simultaneous *stochastic* local state transformations between two pairs of pure states [65].

We note that our result will also decide LU equivalence of generic bipartite mixed states, although the set of "generic states" in our case is different than those in [5, 99]. Generic here means that the set of states to which our algorithm does not apply has measure zero. Specifically, our algorithm can be applied to states that have distinct eigenvalues. If $\rho = \sum_i c_i|\phi_i\rangle\langle\phi_i|$ with $c_i > c_{i+1}$ and $\sigma = \sum_i c_i'|\phi_i'\rangle\langle\phi_i'|$ with $c_i' > c_{i+1}'$, then ρ and σ are LU iff $c_i = c_i'$ and $|\phi_i\rangle, |\phi_i'\rangle$ are LU equivalent for all i.

The above question generalizes the purely linear algebraic problem of deciding for $m+1$ pairs of $d_1 \times d_2$ matrices (X_i, Y_i) whether there exists unitary matrices U and V such that $UX_iV^\dagger = Y_i$ for all i. To our knowledge, this problem has not yet been studied either in the linear algebra community, although Radjavi has solved the special case of square matrices and $U = V$ [88]. The problem can be phrased in a manner better suited for deeper analysis by introducing degree m matrix polynomials $\mathcal{P}(\lambda) = \sum_{i=0}^{m} \lambda^i X_i$ and $\mathcal{Q}(\lambda) = \sum_{i=0}^{m} \lambda^i Y_i$. Two matrix polynomials are called unitarily equivalent if $U\mathcal{P}V^\dagger = \mathcal{Q}$, and we see that $UX_iV^\dagger = Y_i$ for all i if and only if their corresponding matrix polynomials are unitarily equivalent. We also note a more general notion of matrix polynomial equivalence in which $\mathcal{P} \sim \mathcal{Q}$ if there exists invertible scalar matrices A and B such that $A\mathcal{P}B^{-1} = \mathcal{Q}$. We will study matrix polynomials in much greater detail in Chapter V, but for the moment we do not need that heavy of machinery.

In this section, we present a randomized polynomial-time algorithm that decides whether two sets of bipartite pure states can be made equivalent by a fixed local unitary operation. For sets of N-partite mixed states, the algorithm can be used to decide whether each pair is simultaneous equivalent under the same *unilocal* unitary operation. These are special operations in which just a single party applies a local unitary while the other subsystems are left unperturbed. Our algorithm applies to sets of any size and the probability of failure can be made arbitrarily small since the randomness arises from a polynomial identity testing subroutine in the algorithm. One underlying technique of the algorithm is a linear relaxation of quadratic matrix constraints which also works to decide when two degree m matrix polynomials are equivalent in the more general sense of invertible transforming matrices A and B. Physically, this corresponds to the less interesting question of whether a set of SLOCC transformations is possible in the exact same branch of some fixed LOCC protocol.

The actual problem we will consider is a bit more general than the one described in the previous paragraphs and will be called the **Unitary Equivalence Problem** (UEP):

> Suppose G_1 and G_2 are two subrings of $\mathbb{C}^{d_1\times d_1}$ of $\mathbb{C}^{d_2\times d_2}$ respectively whose invertible elements form a group under matrix multiplication. For two sets of matrices $\{X_i\}_{i=0,\dots,m}$ and $\{Y_i\}_{i=0,\dots,m}$ with $X_i, Y_i \in \mathbb{C}^{d_1\times d_2}$, decide if there exists a unitary

solution U and V to the system of equations

$$\chi = \{UX_iV^\dagger = Y_i : U \in G_1, V \in G_2\}. \tag{3.4}$$

The UEP formulation generalizes many different unitary equivalence problems. For instance, if we let $G_1 = \mathbb{C}^{d_1 \times d_1}$ and $G_2 = \mathbb{C}^{d_2 \times d_2}$, we recover the question of whether there exists general unitaries U and V such that $UX_iV^\dagger = Y_i$ for all pairs (X_i, Y_i). If we furthermore consider $d_1 = d_2$ with one pair of matrices both being the identity matrix (I_{d_1}, I_{d_1}), the question becomes whether $UX_iU^\dagger = Y_i$ for all i. An example of a nontrivial subring G_1 is the set $\{M \otimes I_b : M \in \mathbb{C}^{a \times a}\}$ where $ab = d_1$.

It is easy to see the connection between UEP and the simultaneous LU equivalence of bipartite states. The states of a $d_1 \times d_2$-dimensional bipartite system can be represented as vectors $|\psi\rangle$ in the product space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, and linear operators on this space correspond to physical actions on the system. By choosing some basis $|i\rangle_1$ and $|i\rangle_2$ for spaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$ respectively, any state can be written as $|\psi\rangle = (I \otimes \psi)|\Phi\rangle$ where $|\Phi\rangle = \sum_{i=1}^{d} |i\rangle_1 |i\rangle_2$. This allows for a bipartite pure state $|\psi\rangle$ to be identified with the matrix $\psi \in \mathbb{C}^{d_1 \times d_2}$ so that the transformation $|\psi\rangle \rightarrow (A \otimes B)|\psi\rangle$ corresponds to $\psi \rightarrow A\psi B^T$. Consequently, simultaneous LU equivalence between states $\{|\psi_i\rangle\}_{i=0\ldots m}$ and $\{|\phi_i\rangle\}_{i=0\ldots m}$ amounts to whether $U\psi_iV^\dagger = \phi_i$ for all i. For bipartite mixed states, the UEP is encountered only in the restricted setting of unilocal equivalence. Since mixed states themselves are represented by elements in $\mathbb{C}^{d_1 d_2 \times d_1 d_2}$, unilocal unitary equivalence between states ρ and σ is the question of whether $(U \otimes I_{d_2})\rho(U^\dagger \otimes I_{d_2}) = \sigma$, which as noted above is an UEP instance. Note that in the case of simultaneous unilocal equivalence of mixed states, the reduction to UEP applies to systems with an arbitrary number of parties.

3.3.1 The Algorithm

As we will see in greater detail, the UEP can be solved by determining whether or not a particular system of quadratic equations has a nontrivial solution. One strategy sometimes helpful for dealing with quadratic constraints is to relax the problem into a system of linear equations such that a solution to the new equations will solve the original with high probability. We demonstrate this idea on the problem of deciding whether two $d_1 \times d_2$ (assume $d_2 \geq d_1$) matrix polynomials $\mathcal{P} = \sum_{i=0}^{m} \lambda^i X_i$ and $\mathcal{Q} = \sum_{i=0}^{m} \lambda^i Y_i$ are generally equivalent. In other words, does the system of equations

$$\chi_1 = \{AX_iB^{-1} = Y_i : A \in \mathbb{C}^{d_1 \times d_1}, B \in \mathbb{C}^{d_2 \times d_2} \ , 0 \leq i < m\} \tag{3.5}$$

have a nonzero solution for invertible A and B? As noted before, this corresponds to the question of whether we can probabilistically transform pairs of bipartite states under the same LOCC protocol with the guarantee that the transformation occurs under one particular measurement outcome. Clearly χ_1 has such a solution iff there are nonzero invertible solutions to

$$\chi_1' = \{AX_i = Y_iB : A \in \mathbb{C}^{d_1 \times d_1}, B \in \mathbb{C}^{d_2 \times d_2} \ , 0 \leq i < m\}. \tag{3.6}$$

There are $O(md_2^2)$ linear equations in χ_1' which can be solved thus placing constraints on the $2d_1d_2$ free variables of A and B. A matrix solution space to χ_1' is then generated by expressing $A \oplus B$ in terms of the remaining free variables, and χ_1 has a solution iff there exists a nonsingular element in this space.

A standard randomized algorithm for deciding whether a matrix subspace has a full rank element consists of evaluating the degree $\leq 2d_2^2$ real polynomial $|Det(A \oplus B)|^2$ for randomly selected values of the free variables. The Schwartz-Zippel Lemma states that for some n-variate polynomial $f(x_1, \cdots, x_n)$ over a field $\mathbb{K}$ and having degree no greater than d, if f is not identically zero, then $\text{Prob}[f(x_1', \cdots, x_n') = 0] \leq \frac{d}{|X|}$ where each x_i' is independently sampled from some finite set $X \subset \mathbb{K}$ [36, 91, 114]. We will return to the general problem of polynomial identity testing in the next chapter with a more detailed discussion.

Using the Schwartz-Zippel Lemma, to test with success probability at least $1 - \frac{2d_2^2}{|X|}$ whether $|Det(A \otimes B)|^2$ is identically zero, one evaluates it on values randomly chosen from set $X \subset \mathbb{R}$ and decides a zero identity if and only if the evaluation output is zero. As any polynomial number of linear equations can be solved in a polynomial amount of time in order to obtain the space $A \otimes B$, we thus have an efficient method for deciding whether $\mathcal{P} \sim \mathcal{Q}$ up to any probabilistic degree of certainty.

The solve χ, we employ a similar approach but need to add additional constraints. Consider the system

$$\chi' = \{AX_i = Y_iB, X_iB^\dagger = A^\dagger Y_i : A, A^\dagger \in G_1, B, B^\dagger \in G_2; , 0 \leq i < m\}. \tag{3.7}$$

Then we have

Theorem 3.2. *χ has a solution iff χ' has an invertible solution A and B.*

Proof. If such a solution for χ' exists, then $A^\dagger AX_i = X_iB^\dagger B$ and $AA^\dagger Y_i = Y_iBB^\dagger$. But these equations imply $p(A^\dagger A)X_i = X_ip(B^\dagger B)$ and $p(AA^\dagger)Y_i = Y_ip(BB^\dagger)$ where p is any polynomial function. Let x_i denote the distinct eigenvalues from the combined spectrums $\lambda(A^\dagger A) \cup \lambda(B^\dagger B)$. Let X be the Vandermonde matrix of the x_i and v column matrix whose entries are $\sqrt{x_i}^{-1}$. Then the entries of $X^{-1}v$ provide the coefficients of a polynomial $p(t)$ such that $p(A^\dagger A) = \sqrt{A^\dagger A}^{-1}$ and $p(B^\dagger B) = \sqrt{B^\dagger B}^{-1}$. Note also that $p(A^\dagger A) \in G_1$ and $p(B^\dagger B) \in G_2$. Define unitary matrices $U = A\sqrt{A^\dagger A}^{-1} \in G_1$ and $V = B\sqrt{B^\dagger B}^{-1} \in G_2$. Then $UX_i = AX_i\sqrt{B^\dagger B}^{-1} = Y_iB\sqrt{B^\dagger B}^{-1} = Y_iV$. □

With $\{\omega_i^{G_1}\}$ and $\{\omega_i^{G_2}\}$ being bases for G_1 and G_2 respectively. Then χ' represents $O(md_2^2)$ linear constraints on $O(md_2^2)$ free variables. A solution matrix space $A \oplus B$ can be generated, and like before, a polynomial identity test can be applied to decide with arbitrarily high probability whether this space contains a nonsingular element. If a nonsingular element is found, use the A and B to form unitaries U and V as in Theorem (3.2).

In closing, we have studied the general problem of determining when a set of matrix transformations can be simultaneously achieved by a left and right unitary action. Physically, this corresponds to performing multiple transformations between bipartite pure states with the same local action so that the amount of entanglement remains unchanged. Our analysis also extends to the situation of simultaneous unilocal unitary transformations on N-partite mixed states. We have developed a polynomial-time randomized algorithm that decides the problem with high probability and also provides a unitary solution if it exists.

CHAPTER IV

Multipartite to Bipartite Transformations

In this chapter we obtain a first glimpse of how complicated matters can become when more than two parties are considered. In Section 4.1, we consider the problem of deciding if some multiparty entangled pure state can be converted, with a non-zero success probability, into a given bipartite pure state shared between two specified parties through local quantum operations and classical communication. We show that this question is equivalent to the well-known computational problem of deciding if a multivariate polynomial is identically zero. Similar to the technique used in Section 3.3.1, efficient randomized algorithms developed to study the latter can thus be applied to our question. As a result, a given transformation is possible if and only if it is generically attainable by a simple randomized protocol. In Section 4.2, we demonstrate how the problem of tensor norm computation can be reduced to the problem of optimizing SLOCC multiparitite to bipartite transformations constrained by one-way classical communication. Because calculating the tensor norm is NP-Hard, this implies that finding the maximum problem of a single branch in a one-way LOCC scheme is also NP-Hard.

4.1 Multipartite to Bipartite Entanglement Transformations and Polynomial Identity Testing

In the previous chapter we saw how most questions of bipartite pure entanglement transformations can be resolved quite easily. The simple results of the last chapter have no straightforward extension when more parties are considered. At the same time, however, bipartite pure entanglement is often sufficient to perform many quantum information processing tasks. Unfortunately, in practice it becomes very difficult to preserve bipartite pure entanglement as the two systems may interact with other systems thus returning the situation to the multipartite setting. Consequently, a very natural question to ask is what bipartite pure states shared between two specified parties can be obtained from some originally multipartite entangled state.

Previous work on this problem have introduced concepts of entanglement of assistance [96], concurrence of assistance [53], random state entanglement [47], and entanglement combing [112]. Results in these references pertain primarily to the many-copy regime or are restricted to qubit systems and the question of general finite copy bipartite distillation still remains open. In particular, the entanglement combing procedure of Ref. [112] studies the asymptotic generation of bipartite pure states between one fixed party and any other in the system. In contrast, here we examine distillation to some fixed bipartite subsystem in the finite copy scenario because it not only reflects realistic experimental scenarios, but it also provides insight into the complex structure of single multiparitite entangled states. The general multipartite problem, then, is to decide for parties (j,k) and bipartite state $|\phi\rangle$ whether there exists a stochastic local transformation (SLOCC) that obtains state $|\phi\rangle_{jk}$ from some initial n-partite state $|\psi\rangle_{1\ldots n}$: $|\psi\rangle_{1\ldots n} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{jk}|0\rangle_{\overline{jk}}$.

In this section, we show that when given classical descriptions of $|\psi\rangle_{1\ldots n}$ and $|\phi\rangle_{jk}$, deciding convertibility is equivalent to Polynomial Identity Testing (PIT), which is the task of determining whether two polynomials given in algebraic formulas are equivalent (or equivalently, if a polynomial is identically zero). PIT is a classical problem in theoretical computer science with many important applications, such as in perfect matching [40], multiset equality testing [15], and primality testing [3]. In particular, it is known that PIT admits a polynomial time *randomized* algorithm but is not known to have a *deterministic* polynomial time algorithm. The failure to "derandomize" the algorithm is shown [68] to arise from the difficulty of proving super-polynomial lower bounds on general computation models: if PIT is in P, then some other problems would not have an efficient algorithm. Thus PIT has played a central role in studying the fundamental (and open) question of whether randomness is useful in computation, i.e. whether BPP=P (see Section 2.1 for definitions). The equivalence of the convertibility question to PIT implies that the search for a polynomial-time algorithm for the former will remain hard or even impossible since none has been found for the latter.

In the rest of this section, we present the formal statement of our result and its proof. We first discuss tripartite systems and then generalize to n parties. For a tripartite pure state $|\psi\rangle_{ABC}$, Alice and Bob's joint state is described by $\rho^{\psi}_{AB} = Tr_C({}_{ABC}|\psi\rangle\langle\psi|_{ABC})$, with a mixed state representation $\sum_{i=1}^{n} p_i|e_i\rangle\langle e_i|$, where $\langle e_i|e_j\rangle = \delta_{ij}$ and $p_i > 0$. The "subnormalized" eigenstates $\{|\tilde{e}_i\rangle = \sqrt{p_i}|e_i\rangle\}_{i=1\cdots n}$ span the space $supp(\rho^{\psi}_{AB})$ called the support of ρ^{ψ}_{AB}. An ensemble of pure states $\{|\tilde{q}_j\rangle\}_{j=1\cdots t}$ satisfies $\sum_{j=1}^{t} |\tilde{q}_j\rangle\langle\tilde{q}_j| = \rho^{\psi}_{AB}$ if and only if there exists a unitary matrix $U = [u_{ij}]_{1\leq i,j\leq t}$, such that

$$|\tilde{q}_j\rangle = \sum_{i=1}^{n} u_{ij}|\tilde{e}_i\rangle, \tag{4.1}$$

where $|\tilde{e}_i\rangle$ is the zero vector for $i > n$ [61]. Furthermore, there is a one-to-one correspondence between a measurement of Charlie consisting of rank-one measure operators and a unitary matrix U that defines the resultant pure state ensemble through Eq. (4.1) shared by Alice and Bob following Charlie's measurement.

Theorem 4.3. *Let $|\phi\rangle_{AB}$ be a bipartite pure state with Schmidt rank d. Then for tripartite state $|\psi\rangle_{ABC}$, $|\psi\rangle_{ABC} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{AB}$ if and only if there exists $|\phi'\rangle_{AB} \in \text{supp}(\rho_{AB})$ such that $rk(|\phi'\rangle_{AB}) \geq d$.*

Proof. Let $|\psi\rangle_{ABC} = \sum_{i=1}^{n} |\tilde{e}_i\rangle_{AB}|e_i\rangle_C$ be a Schmidt decomposition of $|\psi\rangle_{ABC}$. ($\Rightarrow$) If the transformation is possible, then there are linear operators A, B, C such that $A \otimes B \otimes C|\psi\rangle_{ABC} = |\phi\rangle_{AB}|0\rangle_C$ [39]. Consequently, $|\phi\rangle_{AB} = A \otimes B|\phi'\rangle$, for $|\phi'\rangle = \sum_{i=1}^{n}\langle\eta|e_i\rangle_C|\tilde{e}_i\rangle_{AB}$ where Charlie has applied the rank one operator $C = |0\rangle\langle\eta|$. Since $|\phi'\rangle \in \text{supp}(\rho_{AB})$ and $A \otimes B$ cannot increase the Schmidt rank of $|\phi'\rangle$, we have $rk(|\phi'\rangle) \geq d$. ($\Leftarrow$) Conversely, assume the existence of $|\phi'\rangle \in \text{supp}(\rho_{AB})$ with $\langle\phi'|\phi'\rangle = 1$ and $rk(|\phi'\rangle) \geq d$. Then $|\phi'\rangle$ has a unique representation $|\phi'\rangle = \sum_{i=1}^{n} \alpha_i|\tilde{e}_i\rangle_{AB}$, for some complex numbers α_i, $1 \leq i \leq n$, with $w = \sum_{i=1}^{n} |\alpha_i|^2 \geq 1$. Let $|P\rangle = \sum_{i=1}^{n} \alpha_i|e_i\rangle_C/\sqrt{w}$, If Charlie applies the projective measurement $\{|P\rangle\langle P|, I_C - |P\rangle\langle P|\}$, with probability $1/w > 0$ he observes $|P\rangle$ and Alice and Bob are left with $|\phi'\rangle$. Alice and Bob can then convert $|\phi'\rangle$ into $|\phi\rangle$ with nonzero probability because the target state's Schmidt rank is not higher [106]. □

A unidirectional protocol like that described above is often called "one-shot" as Charlie's involvement consists of just making a measurement with rank-one measure operators and broadcasting the result to Alice and Bob. Hence $|\psi\rangle_{ABC}$ can be converted to $|\phi\rangle_{AB}$ with a nonzero probability if and only if it can be done so by a one-shot protocol. The situation is strikingly different in the case of deterministic transformations since there exist tripartite to bipartite conversions that require bidirectional collaboration between the parties in order to occur with probability one [54].

According to Theorem 4.3, the problem of deciding conversion is reduced to whether a Schmidt rank d state exists in some subspace of $H_A \otimes H_B$. This question is a generalization of one sometimes referred to as Edmonds' Problem [40]: if $M(d_A, d_B)$ is the linear space of $d_B \times d_A$ matrices with complex coefficients and V is some subspace of $M(d_A, d_B)$, decide whether there exists a rank $d = \min\{d_A, d_B\}$ (i.e. full rank) matrix in V. Intuitively, one would expect that an upper bound exists on the dimension s of subspaces containing only states of rank strictly less than d. Indeed, Flanders provides the bound $s < d \cdot \max\{d_A, d_B\}$ [46, 33]. Thus,

Corollary 1. *If $rk(|\phi\rangle) = d$ and $\dim[supp(\rho^{\psi}_{AB})] \geq d \cdot \max\{d_A, d_B\}$, then $|\psi\rangle_{ABC} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{AB}$.*

It requires more work when $\dim[supp(\rho^{\psi}_{AB})] < d \cdot \max\{d_A, d_B\}$. As recognized by previous investigators, determining whether a matrix subspace is singular can be cast into a polynomial identity testing question [56, 76]. We generalize their approach to the subject at hand. Letting $\{\tilde{\Pi}_i\}_{i=1\cdots n}$ denote the nonzero subnormalized eigenstates of ρ^{ψ}_{AB} in matrix form, any state in $supp(\rho^{\psi}_{AB})$ can be expressed as

$$\Pi(\mathbf{u}) = u_1\tilde{\Pi}_1 + \cdots + u_n\tilde{\Pi}_n, \tag{4.2}$$

where $\mathbf{u} = (u_1, \cdots, u_n)$ is an n-dimensional complex vector. Construct the following real-valued function

$$g(\mathbf{u}) = \sum_{\kappa_d} |\det(\kappa_d)|^2, \tag{4.3}$$

where κ_d ranges over the set of $d \times d$ sub-matrices of $\Pi(\mathbf{u})$ and $\det(\kappa_d)$ denotes the determinant of κ_d. Note that g is a nonnegative polynomial of degree no greater than $2d$ in the real variables $\{a_i, b_i\}_{i=1\cdots n}$ where $u_i = a_i + \mathbf{i}b_i$. Then deciding whether g is identically zero is the same as determining whether a Schmidt rank d state is obtainable from $|\psi\rangle_{ABC}$ since $g(\mathbf{u}) \equiv 0$ if and only if no matrix of rank at least d exists in the span of $\{\tilde{\Pi}_i\}_{i=1\cdots n}$.

It is important to note that Theorem 4.3 cannot be nontrivially extended to more than three parties. In general, for chosen parties (j, k) and some rank d state $|\phi\rangle_{jk}$, the existence of $|\phi'\rangle \in supp(\rho_{jk})$ with rank at least d is not sufficient for the transformation $|\psi\rangle_{1\ldots n} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{jk}$. This can easily be seen by the transformation $|\Phi\rangle_{AC}|\Phi\rangle_{BD} \overset{\text{SLOCC}}{\longrightarrow} |\Phi\rangle_{AB}$

where $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ [71]. If Charlie and David act locally, Alice and Bob will never share entanglement, not even probabilistically. However, $|\Phi\rangle \in supp(\rho_{AB})$.

Nevertheless, a similar criterion as above can be constructed for deciding convertibility when more than three parties are involved. Without loss of generality, assume parties $n-1$ and n are to obtain state $|\phi\rangle$. Let $\{|i_j\rangle_j\}_{i_j=1...n_j}$ be a local basis for party j and expand the initial state as $|\psi\rangle_{1...n} = \sum_{\mathbf{i}} |i_1\rangle_1...|i_{n-2}\rangle_{n-2}|\mathbf{i}\rangle_{n-1,n}$ where $\mathbf{i}$ indexes $i_1, ...i_{n-2}$. The transformation is possible iff it can be accomplished when parties $1, ..., n-2$ perform the separable operator $|0\rangle\langle\eta|$ with $|\eta\rangle = \sum_{\mathbf{i}} a_{i_1}...a_{i_{n-2}}|i_1\rangle_1...|i_{n-2}\rangle_{n-2}$ and arbitrary coefficients $\mathbf{a} = (a_{i_1}, ..., a_{n-2})$. To decide feasibility, we again map the $|\mathbf{i}\rangle_{n-1,n}$ to matrices $\Pi_{\mathbf{i}}$ and construct the polynomial matrix $\Pi(\mathbf{a}) = \sum_{\mathbf{i}} a_{i_1}...a_{i_{n-2}}\Pi_{\mathbf{i}}$. A key difference between $\Pi(\mathbf{a})$ and (4.2) above is that the former does not represent a matrix subspace. This explains why every state in $supp(\rho_{n-1,n})$ cannot be obtained from $|\psi\rangle_{1...n}$ by LOCC. Using $\Pi(\mathbf{a})$, we then form an analogous expression to (4.3) that will be a polynomial of degree no greater than n^{2d}. A rank d state can then be had by parties $n-1$ and n iff this polynomial is not identically zero. Hence for both tripartite and general n-partite cases, transformation feasibility is decided by whether or not a certain polynomial is identically zero.

As mentioned above, Polynomial Identity Testing is a classic problem in theoretical computer science with many important applications [79, 76, 68]. In general, given two polynomials $f(\mathbf{x})$ and $p(\mathbf{x})$, it can always be decided if $f = p$ by multiplying out the polynomials and checking whether their coefficients match. However, the number of multiplications required for this procedure scales exponentially in the degree of the polynomials and at the present no sub-exponential deterministic algorithm is known for polynomial identity testing [79, 6].

On the other hand, if one considers the special case of three parties in which Charlie's system is a qubit, a deterministic efficient algorithm exists to decide whether (4.3) is identically zero. Here, (4.2) becomes a linear combination of two matrices, more commonly called a matrix pencil. Well-known analysis of matrix pencils can be applied to decide whether the given matrix subspace is singular (see [48, 26] and also Section 5.2). Specifically, when $d_B \geq d_A$ ($d_A \geq d_B$), (4.3) is identically zero iff the matrix pencil (4.2) has more than $d_A - d$ right ($d_B - d$ left) minimal indices. The minimal indice structure of a pencil can be efficiently determined through a Gaussian Elimination procedure [48].

Returning to the general case, if one relaxes the deterministic condition, randomized polynomial-time algorithms exist that can decide with a high probability of success [6]. As we saw in the previous chapter, unless this polynomial is identically zero, by the Schwartz-Zippel Lemma [91] the probability that it will evaluate to zero can be made arbitrarily small by sampling the evaluation points from a sufficiently large set of rational numbers. Using this result on the analysis of g in Eq. (4.3) allows for the following classification of the n-partite to bipartite conversion problem.

Theorem 4.4. *There exists a polynomial time randomized algorithm that, given states $|\psi\rangle_{1\ldots n}$ and $|\phi\rangle_{jk}$, decides correctly if $|\psi\rangle_{1\ldots n} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{jk}$ is feasible with probability $\geq 2/3$.*

In other words, the problem of deciding multipartite to bipartite SLOCC convertibility belongs to the complexity class BPP, which consists of decision problems solvable by Bounded-error Probabilistic Polynomial time algorithms. The error probability $1/3$ can be made exponentially small by repeating the algorithm and outputting the majority of the outputs of each repetition.

The randomized algorithm described above can be used to construct an LOCC protocol that completes any feasible n-partite to bipartite transformation with nonzero probability. We describe the procedure for three parties, but its generalization is straightforward. First, Charlie makes $2n$ independent samplings $a_1, b_1, a_2, b_2, \cdots, a_n, b_n$ from the integer set $\{1, \cdots, M\}$, where M is an integer larger than $2d$. Then he constructs

$\mathbf{u} = (a_1 + \mathbf{i}b_1, \cdots, a_n + \mathbf{i}b_n)$ and evaluates $g(\mathbf{u})$ in Eq. (4.3). If $g(\mathbf{u})$ is nonzero, the state $|P\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{n} u_i |e_i\rangle$ is formed with N being the appropriate normalization factor. By the Schwartz-Zippel lemma, such a $\mathbf{u}$ can be found with success probability at least $1 - \frac{2d}{M}$ in the case that g is not identically zero, and an appropriate M can be chosen to make this probability sufficiently large. Then Charlie performs a projective measurement $\{|P\rangle\langle P|, I_C - |P\rangle\langle P|\}$, and Alice and Bob will share the unnormalized state $\Pi_{\phi'}(\mathbf{u}) = \sum_{i=1}^{n} u_i \tilde{\Pi}_i$ with nonzero probability when the outcome is $|P\rangle$. They will then be able to probabilistically obtain the desired target state $|\phi\rangle$ as $|\phi'\rangle$ is with Schmidt rank at least d. One drawback of the above procedure is that we need to evaluate $g(\mathbf{u})$. However, the explicit form of g is unknown and may be very complicated as we need to sum over all determinants of $d \times d$ sub-matrices of $\Pi(\mathbf{u})$. Fortunately, we can avoid evaluating $g(\mathbf{u})$ directly by checking whether the matrix rank of $\Pi(\mathbf{u})$ is larger than d, which can be done efficiently in polynomial time of n and $d_{A(B)}$.

It is interesting how the problem can be turned around by reducing any polynomial identity testing question to a decision of SLOCC convertibility. In an important work by Valiant [102] (slightly improved in [74]), he shows that any polynomial $p(x_1, \cdots, x_m)$ over a field $\mathbb{K}$ of formula size e can be expressed as the determinant of some $(e+2) \times (e+2)$ matrix $\Pi_p(x_1, \cdots, x_m)$ with entries in $\{x_1, ..., x_m\}$ and the underlying field [102], and the construction of Π_p from p can be done in polynomial time. Let $\Pi_p = \Pi_0 + \sum_{i=1}^{m} x_i \Pi_i$, where $\Pi_i \in \mathbb{K}^{(e+2)\times(e+2)}$, $0 \leq i \leq m$. We claim that $Span\{\Pi_i : 0 \leq i \leq m\}$ contains a nonsingular matrix if and only if $\Pi_0 + Span\{\Pi_i : 1 \leq i \leq m\}$ does. The "only if" direction is trivial. Assume that $A = \sum_{i=0}^{m} \alpha_i \Pi_i$ is nonsingular. If $\alpha_0 \neq 0$, then $\Pi_0 + \sum_{i=1}^{m} \frac{\alpha_i}{\alpha_0} \Pi_i$ is nonsingular. Otherwise, for sufficiently large k, $\det(\Pi_0 + kA) > 0$. Thus $\Pi_0 + Span\{\Pi_i : 1 \leq i \leq m\}$ contains a nonsingular matrix.

To conclude the reduction, for each i, $0 \leq i \leq m$, let $|e_i\rangle$ be the bipartite state corresponding to Π_i, and $\rho_{AB} = \frac{1}{n}\sum_{i=1}^{n}|e_i\rangle\langle e_i|$. Letting $|\psi\rangle_{ABC}$ be a purification of ρ_{AB} and $|\phi\rangle_{AB}$ any rank n bipartite state, $p(x_1, \cdots, x_m)$ is not identically zero if and only if $|\psi\rangle_{ABC} \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle_{AB}$.

In conclusion, the results of this section help contribute to the complexity hierarchy of SLOCC pure state transformations. For bipartite transformations, the question of convertibility reduces to matrix rank calculations, which can be done in deterministic polynomial time. As seen here, for multipartite to bipartite conversions, determining feasibility is equivalent to testing the identity of a given polynomial, which can be done in randomized polynomial time. For three systems with Charlie having a qubit, the algorithm can be derandomized, but it is a major open problem whether this derandomization can be accomplished in all cases. In Chapter V, we will consider the next level of SLOCC hierarchy in which the target state may be three-way entangled.

4.2 Multipartite Transformations with One-Way Classical Communication and the Geometric Measure of Entanglement

In Section 3.3, we considered the problem of finding the maximum probability for a bipartite SLOCC transformation when the classical communication is unidirectional. Here we consider a generalization of the problem still within the multipartite to bipartite transformation setting. Suppose that from some initial N-partite state, we wish to obtain pure entanglement between Alice and Bob. But also assume that the only possible outgoing classical communication possible is from the $N-2$ parties other than Alice and Bob. What is the maximum probability of a one-shot transformation under such circumstances? Like before, the inability for Alice and Bob to share their measurement results means that the each contraction of $|\psi\rangle_{1\ldots N} \to |\phi\rangle_{AB}$ must take the form $(U_A \otimes U_B \otimes A_3 \otimes ... \otimes A_N)|\psi\rangle_{1\ldots N} = \sqrt{p}|\phi\rangle_{AB}|0\rangle_{\overline{AB}}$. To prove this problem is NP-Hard, we will use the fact that computing the geometric measure a entanglement is NP-Hard, a complexity result that may be of interest on its own.

Recall from Section 2.2.2 that for a multipartite pure state $|\psi\rangle$, the geometric measure of entanglement is the distance of $|\psi\rangle$ to the nearest product state as measured by the fidelity: $G_M(|\psi\rangle = \min_\omega |\langle\omega|\psi\rangle|$ where ω is a product state. For tripartite states, this problem is

$$\max_{|A\rangle|B\rangle|C\rangle} |\langle A|\langle B|\langle C|\psi\rangle|^2 \tag{4.4}$$

where $|A\rangle \in \mathbb{C}^{d_A}$, $|B\rangle \in \mathbb{C}^{d_B}$, $\mathbb{C}^{d_C}$, and all three have unit length. In mathematical literature, (4.4) is equivalently called the **tensor spectral norm** of $|\psi\rangle$. Very recently, calculating the tensor spectral norm problem has been shown to be NP-Hard when $|\psi\rangle$, $|A\rangle$, $|B\rangle$, and $|C\rangle$ are all *real* [59]. This, however, does not immediately imply that finding $G_M(|\psi\rangle)$ is NP-Hard since even if $|\psi\rangle$ is real, the $|A\rangle$, $|B\rangle$, and $|C\rangle$ that maximize (4.4) may be complex. It is quite possible that the authors in [59] took the following generalization for granted, but we include it here for completion.

For a tensor $|\psi\rangle = \sum c_{ijk}|i\rangle_A|j\rangle_B|k\rangle_C$, (4.4) is equivalent to the problem

$$\max_{|A\rangle|B\rangle} \{|\delta|^2 : \langle A|\langle B|\psi\rangle = \delta|C\rangle \text{ where } |\langle A|A\rangle| = |\langle B|B\rangle| = |\langle C|C\rangle| = 1\}. \tag{4.5}$$

We want to show that if $c_{ijk} \in \mathbb{R}$ then we can restrict our search to real product states $|A\rangle, |B\rangle, |C\rangle$.

Lemma 2. *For any $|\psi\rangle \in \mathbb{R}^{n_A n_B n_C}$, there exists states $|A\rangle \in \mathbb{C}^{n_A}$, $|B\rangle \in \mathbb{C}^{n_B}$, $|C\rangle \in \mathbb{C}^{n_C}$ and $\delta \in \mathbb{C}$ such that $\langle A|\langle B|\psi\rangle = \delta|C\rangle$ iff there exists states $|\psi'\rangle \in \mathbb{R}^{2n_A 2n_B 2n_C}$, $|A'\rangle \in \mathbb{R}^{2n_A}$, $|B'\rangle \in \mathbb{R}^{2n_B}$, $|C'\rangle \in \mathbb{C}^{n_C}$ and $\delta' \in \mathbb{R}$ such that $\langle A'|\langle B'|\psi'\rangle = \delta'|C'\rangle$ where $\delta' = |\delta|$.*

Proof. For a fixed k, we let $C_k(i,j) = c_{ijk}$ be a one slice matrix of the tensor c_{ijk}. Then we have $\langle A|\langle B|\psi\rangle = \sum_k \langle A|C_k|B^*\rangle|c_k\rangle = \sum_k r_k|c_k\rangle$ and so $|\delta|^2 = \sum |r_k|^2$. Decomposing into real vectors $|A\rangle = |a\rangle + i|\tilde{a}\rangle$ and $|B^*\rangle = |b\rangle + i|\tilde{b}\rangle$ yields $r_k = \langle a|C_k|b\rangle - \langle\tilde{a}|C_k|\tilde{b}\rangle + i(\langle\tilde{a}|C_k|b\rangle + \langle a|C_k|\tilde{b}\rangle)$. As a result, we have $|\delta|^2 = \sum_k(\langle a|C_k|b\rangle - \langle\tilde{a}|C_k|\tilde{b}\rangle)^2 + (\langle\tilde{a}|C_k|b\rangle + \langle a|C_k|\tilde{b}\rangle)^2$. We now define a new tensor c'_{ijk} by the slices $C'_k(i,j) = \begin{pmatrix} C_k(i,j) & 0 \\ 0 & -C_k(i,j) \end{pmatrix}$ for $k = 1...n_C$ and $C'_k(i,j) = \begin{pmatrix} 0 & C_k(i,j) \\ C_k(i,j) & 0 \end{pmatrix}$ for $k = n_C+1...2n_C$. Then we define the concatenated real vectors $|A'\rangle = |a\tilde{a}\rangle$ and $|B'\rangle = |b\tilde{b}\rangle$. Consequently, $r'_k = \langle a|C_k|b\rangle - \langle\tilde{a}|C_k|\tilde{b}\rangle$ for $k = 1...n_C$ and $r'_k = \langle\tilde{a}|C_k|b\rangle + \langle a|C_k|\tilde{b}\rangle$ for $k = n_C + 1...2n_C$. This is a one-to-one construction. □

Consequently, we see that the tensor spectral norm of real tensors reduces to the tensor spectral norm of complex tensors. Therefore,

Lemma 3. *For some multipartite state $|\psi\rangle$ and $q \in \mathbb{Q}$, deciding whether $G_M(|\psi\rangle) \leq q$ is NP-Hard.*

While this NP-Hardness already exists in tripartite states, in contrast, we should mention that computing G_M is quite easy for bipartite states. Indeed for any bipartite state $|\psi\rangle$ its geometric measure is given by its largest Schmidt coefficient (spectral norm of Ψ), which, in fact is why its multipartite generalization is also called a spectral norm.

Returning to our discussion on one-way SLOCC transformations, let $|Z\rangle$ be any tripartite state and let $|Z^\perp\rangle$ be some state such that $tr_{\bar{j}}(|Z\rangle\langle Z|) \perp tr_{\bar{j}}(|Z^\perp\rangle\langle Z^\perp|)$ for each party j. Consider the 5-partite state $|\psi\rangle = \frac{1}{\sqrt{2}}(|\Phi\rangle|Z\rangle + |01\rangle|Z^\perp\rangle)$ where $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If Alice and Bob are only restricted to unitary operations on their ends, transformation $|\psi\rangle \to |\Phi\rangle|000\rangle$ is possible iff $\langle\omega|Z^\perp\rangle = 0$ where $|\omega\rangle$ is the product state projected by the other three parties. This is because the action of the other three parties must be a projection so that Alice and Bob sure pure entanglement, and if $\langle\omega|Z^\perp\rangle \neq 0$, then after projecting $|\omega\rangle$ Alice and Bob would share $a|\Phi\rangle + b|01\rangle$ with $b \neq 0$, a state clearly not LU equivalent to $|\Phi\rangle$. As a result, the optimal probability of the entire transformation is given by maximizing $\langle \omega | Z \rangle$, or in other words, by computing the geometric measure of $|Z\rangle$. Thus, we have proven the problem to be NP-Hard.

CHAPTER V

Tripartite Transformations

In this chapter we consider entanglement transformations in tripartite systems. The increase in complexity generated by the additional party can already be anticipated after comparing the difficulties in computing Schmidt rank versus tripartite tensor rank as noted in Chapter II, and more strikingly, in computing the geometric measure of entanglement in bipartite versus tripartite states as seen in the last chapter. Our discussion here will break into three parts. First we will review previous research conducted on entanglement transformations in tripartite systems. The general difficulty inherent in studying tripartite entanglement has limited the number of results discovered on this subject. Second, we will examine reversible SLOCC convertibility in $2 \otimes m \otimes n$ systems. Here we use the rich theory of matrix pencils to represent states in these dimensions and show that certain transformation decision problems can be efficiently solved when one of the systems is a qubit. Finally, we tackle genuine tripartite transformations in their full generality. We find this to be an intractable project and discover that fundamental questions in tensor analysis are encoded in the theory of tripartite entanglement.

5.1 Overview of Known Results

The first thorough investigation of tripartite entanglement was conducted by Dür *et al.* [39], with precursory work done in [1]. They examined systems of dimensions $2 \otimes 2 \otimes 2$, the simplest of all tripartite systems, and classified the different forms of entanglement that can be shared by three qubits with respect to SLOCC equivalence. Recall that two states are SLOCC equivalent iff they can both be SLOCC converted from one to the other. For bipartite pure states, this ability is captured entirely by the Schmidt ranks of the states: $|\psi\rangle_{AB} \sim |\phi\rangle_{AB}$ iff $Sch(\psi) = Sch(\phi)$. Furthermore, SLOCC equivalence is a total ordering on the bipartite state space with a decrease in Schmidt rank sufficient for SLOCC convertibility. In contrast, one of the most interesting results demonstrated in [39] is that SLOCC convertibility is not a total ordering for three qubit states.

The $2 \otimes 2 \otimes 2$ state space can be partitioned into six SLOCC equivalence classes. The set of product states constitutes one class, and the three different ways pure bipartite entanglement can be distributed among the parties correspond to three more. The remaining two classes contain genuinely tripartite entangled states. Respective state representatives for these two classes are $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. Any state belonging to the GHZ class cannot be SLOCC converted to any state in the W class and vice versa. Given some three qubit state, it still remains a non-trivial matter to decide which entanglement class it belongs. Although following the publication of Ref. [39] methods were designed to answer this question, the algorithm we present in the next section can also achieve this feat in an efficient manner.

Even for three qubits states, there does not seem to be any easy method for calculating the optimal probability for a given transformation (below the problem in higher dimensions is shown to be NP-Hard). However, the results of [39] imply that when attempting to find some general method for optimizing a three qubit transformation with all parties entangled, one need only consider transformations within the same class, be it GHZ or W. This is helpful since GHZ and W states can be identified by their tensor rank, so the problem becomes fully characterized as transformations between states with the same tensor rank.

In particular, tensors of rank two, such as those in the GHZ class, possess nice properties which enabled early progress on the question of optimally transforming $|GHZ\rangle$ into some target state [2]. General results were obtained for deciding deterministic transformations of *real* three qubit states [97], and novel techniques have recently revived life into the problem by improving both upper and lower bounds on the probability for transforming two GHZ-type states [34]. The most complete result has come from Turgut *et al.* who has provided a straightforward algorithm for deciding whether one GHZ-type state can be deterministically transformed into another [100]. These impressive results suggest that this problem might be solvable and perhaps one day an efficient method for calculating the maximum probability of a given three qubit transformation will be discovered.

5.2 Equivalence in $2 \otimes m \otimes n$ Systems

In this section we study the SLOCC equivalence classes of tripartite pure states in systems of dimensions $2 \otimes m \otimes n$. This can be seen as one generalization of Dür *et al.*'s work described above. Previously, their results were already extended in another direction by Verstraete and co-workers who investigated four qubit systems and found there to be an infinite number of equivalence classes [105]. For an arbitrary number of subsystems, Miyake has shown how multidimensional determinate theory can be used to obtain general properties and results concerning SLOCC equivalence [77]. Specific to tripartite $2 \otimes 2 \otimes n$ systems, Miyake and Verstraete have also completely characterized the equivalence class hierarchy and found that for $n \geq 4$ exactly nine different classes exist [78]. Using the method of successive Schmidt decompositions, Cornelio and Piza obtained partial results concerning the equivalence classes in $2 \otimes m \otimes n$ systems [32]. Chen *et al.* completed the finite orbit picture by enumerating all 26 equivalence classes in $2 \otimes 3 \otimes 6$ systems, and showed that for the $3 \otimes 3 \otimes 3$ and $2 \otimes 4 \otimes 4$ systems (and all systems of higher dimensions), there are an infinite number of SLOCC equivalence classes. They used a technique called "the range criterion" [21], which states that two states are SLOCC equivalent if and only if the ranks of the reduced density operators are identical and their supports are related by local invertible linear operations. While these results are quite interesting, the tools used to obtain them appear rather *ad hoc* and neither the range criterion nor any previous technique provide an efficient algorithm (or any algorithm at all) for determining SLOCC equivalence. The non-invertible hierarchy among the 26 classes has also remained an open problem. In another work, Cheng *et al.* tackle the restricted problem of $2{\otimes}n{\otimes}n$ equivalence by an approach that most closely resembles the one used in this section [94]. However, the authors err in their analysis and we correct their oversight here while encompassing the style of their analysis in a much broader framework.

The main insight of this section is that the theory of matrix pencils is the perfect tool for analyzing SLOCC equivalence in $2 \otimes m \otimes n$ systems. For two matrices $R, S \in \mathbb{C}^{m \times n}$, the linear matrix polynomial $\mu R + \lambda S$ is called a matrix pencil. A fundamental result is the existence of a canonical form, discovered by Kronecker (see, e.g., Gantmacher [48]), to which all pencils are uniquely related by an invertible matrix transformation $A(\mu R+\lambda S)B$. The theory of matrix pencils remains an important subject of study for its applications in control and systems theory. An example is the computation of the generalized eigenvalues [1]. The efficient computation of the Kronecker canonical forms, other canonical forms, and related problems is still an active field of research, e.g. see Ref. [8] and following articles. We also note that the underlying object of our study, the representations of $GL_2(\mathbb{C}) \times GL_m(\mathbb{C}) \times GL_n(\mathbb{C})$, has been investigated in the mathematical literature with an emphasis on the geometry of equivalent matrix pencils (see Ref. [86] and references within).

The connection with our problem is that each quantum pure state in a $2{\otimes}m{\otimes}n$ space can

[1] For two matrices R and S, a vector x and a constant λ, if $Rx = \lambda Sx$, λ is a generalized eigenvalue of (R, S) and x the associated eigenvector. The set of generalized eigenvalues are precisely $\{\lambda/\mu : \det(\mu R + \lambda S) = 0\}$(see, e.g., Section 7.7 of Ref. [52])

be represented as a matrix pencil (see Section 5.2.2 for details). In short, just as any $m \otimes n$ bipartite pure state corresponds to a matrix or bilinear form $R : \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}; (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T R\mathbf{y}$, every $2 \otimes m \otimes n$ tripartite pure state corresponds to a matrix pencil or trilinear form $\mu R + \lambda S : \mathbb{C}^2 \times \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}; (a, b, \mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}^T (aR + bS)\mathbf{y}$. The local operations on the second and third subsystem map the corresponding pencil to an equivalent one. While actions on the first subsystem may bring the pencil to an inequivalent one, we show that if two states are SLOCC equivalent, the operation on the first subsystem can be selected from a small number of choices. As a consequence, we derive the first efficient algorithm for determining SLOCC equivalence in general $2 \otimes m \otimes n$ quantum systems. We present a canonical form for $2 \otimes m \otimes n$ pure states and an algorithm to calculate it such that two states are equivalent if and only if the have the same canonical form. For the systems having a finite number of equivalence classes, we rederive the previously known equivalence orbits and then represent them using our defined canonical forms. We also determine all possible non-invertible transformations among these equivalence classes.

The rest of this section begins with a brief introduction to some main results in matrix pencil theory. In Section 5.2.2 we develop the relationship between tripartite pure states and matrix pencils which then allows us to derive necessary and sufficient conditions for the SLOCC convertibility of $2 \otimes m \otimes n$ states. Section 5.2.3 presents a polynomial-time algorithm for deciding when two states are SLOCC equivalent, and Section 5.2.4 establishes a unique canonical form to which every $2 \otimes m \otimes n$ pure state is SLOCC equivalent. The canonical forms for $2 \otimes 3 \otimes n$ systems are explicitly given in Section 5.2.5, and Section 5.2.6 develops the SLOCC hierarchy within these systems. The section closes with some brief concluding remarks.

5.2.1 Matrix Pencils

The theory of matrix pencils was first developed by Kronecker over a century ago. A completely thorough treatment of the subject can be found in Gantmacher's two volume texts [48] from which we will here only cite the main definitions and results. For a more modern treatment, see Ref. [51]. Given two complex $m \times n$ matrices R and S, we form the homogeneous matrix polynomial $\mathcal{P}_{(R,S)} = \mu R + \lambda S$ in variables μ and λ. For concreteness, we will use the pencil $\mathcal{P}_0 = \begin{pmatrix} -\mu+\lambda & 3\mu+\lambda & \mu & 2\mu+\lambda \\ -\mu & 0 & \mu & 0 \\ 0 & \mu+\lambda & 0 & \mu+\lambda \end{pmatrix}$ as an example. Two pencils $\mathcal{P}_{(R,S)}$ and $\mathcal{P}_{(R',S')}$ are **strictly equivalent** if there exists invertible matrices B and C independent of μ and λ such that $\mu R' + \lambda S' = B(\mu R + \lambda S)C^T$. It immediately follows that $\mathcal{P}_{(R,S)}$ and $\mathcal{P}_{(R',S')}$ are strictly equivalent if and only if there exists invertible B and C such that $BRC^T = R'$ and $BSC^T = S'$.

The **rank** of $\mathcal{P}_{(R,S)}$ is the largest r such that there exists an r-minor of $\mathcal{P}_{(R,S)}$ not identically zero (not equaling zero upon every complex substitution for μ and λ). For $i \leq r$ we let $D_i(\mu, \lambda)$ denote the highest degree polynomial, monic with respect to λ, that divides each of $\mathcal{P}_{(R,S)}$'s i-minors. It can be seen that $\mathcal{P}_0$ is rank three with all 3-minors being divisible by $\mu(\mu + \lambda)$. The **invariant polynomials** of pencil $\mathcal{P}_{(R,S)}$ are the homogeneous polynomials $E_i(\mu, \lambda) = \frac{D_i(\mu,\lambda)}{D_{i-1}(\mu,\lambda)}$ for $i = 1...r$ where $D_0(\mu, \lambda) \equiv 1$. There will be a unique factorization of $D_r(\mu, \lambda)$ as $D_r(\mu, \lambda) = \mu^{r-k} p_1 \cdot ... \cdot p_k$ where p_i is of the form $\mu x_i + \lambda$ for $x_i \in \mathbb{C}$, and the invariant polynomials will likewise have a factorization in terms of these p_i and powers of μ. In fact, we can identify each distinct p_i (suppose there are f of them) with its μ-coefficient x_i, and the factor μ with the element $x_{f+1} = +\infty$ so that the degree one divisors of all the invariant polynomials are specified by elements from $\mathbb{C}^* = \mathbb{C} \cup \{+\infty\}$. These distinct x_i values from $\mathbb{C}^*$ generated by the factorization of $D_r(\mu, \lambda)$ are called the **eigenvalues** of $\mathcal{P}_{(R,S)}$. To each eigenvalue x_i, there is a corresponding **eigenvalue size signature** which is a sequence of integers $X^i = (n^i_1, ..., n^i_r)$ such that n^i_j is the highest power of $\mu x_i + \lambda$ that divides invariant polynomial $E_j(\mu, \lambda)$ if $x_i \neq +\infty$, and n^i_j is the highest power of μ that divides $E_j(\mu, \lambda)$ if $x_i = +\infty$. The **elementary divisors** of the pencil is then the multiset $\{\{(\mu x_i + \lambda)^{n^i_j}\}_{j=1...r} : x_i \neq +\infty, 1 \leq i \leq f\} \bigcup \{\{\mu^{n^i_j}\}_{j=1...r} : x_i = +\infty\}$. In our example pencil $\mathcal{P}_0$, $E_3(\mu, \lambda) = \mu$, $E_2(\mu, \lambda) = \mu + \lambda$, and $E_1(\mu, \lambda) = 1$. Thus $\mathcal{P}_0$ has eigenvalues $\{1, +\infty\}$ with respective size signatures $(0, 1, 0)$ and $(0, 0, 1)$.

While each pencil has a unique set of eigenvalues $\{x_1, ..., x_f\}$ and corresponding size signatures $\{X^1, ..., X^f\}$, it will be desirable to have some canonical way of uniquely specifying these values. To do this, we first fix some total ordering for sequences of integers and some total ordering for elements of $\mathbb{C}^*$. Next, eigenvalues $\{x_1, ..., x_f\}$ are ordered non-decreasingly according to their size signatures, and finally for eigenvalues having the same size signatures, they are ordered non-decreasingly according to their position in $\mathbb{C}^*$. Every pencil $\mathcal{P}_{(R,S)}$ then has a unique **canonical sequence** of eigenvalues $\hat{x} = (x_1, ..., x_f)$ with their size signatures forming a non-decreasing sequence $\hat{X} = (X^1, ..., X^f)$.

For pencil $\mathcal{P}_{(R,S)}$, consider the set of polynomial vectors $\mathbf{x}_i(\mu, \lambda)$ such that $(\mu R + \lambda S)\mathbf{x}_i(\mu, \lambda) \equiv 0$. This set is a finitely generated module over the ring of polynomials, and any homogeneous basis will have elements of the form

$$\mathbf{x}_i(\mu, \lambda) = \sum_{j=0}^{\epsilon_i} x_{ij} \mu^{\epsilon_i - j} \lambda^j$$

with degrees $\epsilon_1 \leq ... \leq \epsilon_p$. An important property of any $\mathbf{x}_i(\mu, \lambda)$ belonging to such a basis is that *the* x_{ij} *are linearly independent* [48]. Likewise, the set of polynomial vectors satisfying $\mathcal{P}^T_{(R,S)} \mathbf{x}_i(\mu, \lambda) = 0$ will have a homogeneous basis whose elements have degrees $\nu_1 \leq ... \leq \nu_q$. The values $\epsilon_1, ..., \epsilon_p$ and $\nu_1, ..., \nu_q$ are called the **minimal indices** of $\mathcal{P}_{R,S}$. In particular, the number of ϵ_i that are zero will be called the **zero index number**, and the number of ν_i that are zero will be called the **transpose zero index number**. For the pencil $\mathcal{P}_0$, it can be readily verified that $\mathcal{P}_0([1, 0, 1, 0]^T \mu + [0, -1, 0, 1]^T \lambda) = 0$, and $\mathcal{P}_0$ has a single minimal indice of $\epsilon_1 = 1$. With this overview, we can now state the main theorem characterizing strictly equivalent pencils.

Lemma 4 (Kronecker, [48])**.** *Two matrix pencils are strictly equivalent if and only if they have the same rank, elementary divisors, and minimal indices. Moreover, suppose that $\mathcal{P}_{(R,S)}$ has a canonical sequence of eigenvalues $\hat{x} = (x_1, ..., x_f)$ with size signatures $\hat{X} = (X^1, ..., X^f)$, minimal indices $\epsilon_1 \leq ... \leq \epsilon_p$ and $\nu_1 \leq ... \leq \nu_q$, a zero index number of g, and a transpose zero index number of h. Then $\mathcal{P}_{(R,S)}$ is strictly equivalent to the canonical block-form diagonal pencil*

$$\{F^0, L_{\epsilon_{g+1}}, ..., L_{\epsilon_p}, L^T_{\nu_{h+1}}, ..., L^T_{\nu_q}, J\} \tag{5.1}$$

where F^0 is the $h \times g$ zero matrix, $L_\epsilon = \left.\overbrace{\begin{pmatrix} \lambda & \mu & 0 & ... & 0 \\ 0 & \lambda & \mu & ... & 0 \\ & ... & & & \\ 0 & 0 & ... & \lambda & \mu \end{pmatrix}}^{\epsilon+1}\right\}\epsilon$ *, and* $J = \bigoplus_{i=1}^{f} M^i$ *where*

$$M^i = \begin{cases} \bigoplus_{j=1}^{r} [(\mu x_i + \lambda) I_{n^i_j} + \mu H_{n^i_j}] \ \ if \ \ x_i \neq +\infty, \\ \\ \bigoplus_{j=1}^{r} [\mu I_{n^i_j} + \lambda H_{n^i_j}] \ \ if \ \ x_i = +\infty, \end{cases}$$

I_t being the $t \times t$ identity matrix and H_t the $t \times t$ matrix whose only nonzero elements are ones on the superdiagonal.

Note that by our ordering of the eigenvalues and minimal indices, every pencil is equivalent to one and only one **Kronecker Canonical Form (KCF)** as defined above. Our example pencil $\mathcal{P}_0$ has the KCF of $\begin{pmatrix} \lambda & \mu & 0 & 0 \\ 0 & 0 & \mu+\lambda & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$.

5.2.2 Connection to $2 \otimes m \otimes n$ Pure States

Any $2 \otimes m \otimes n$ state can be expressed in bra-ket form as $|\psi\rangle = |0\rangle_A |R\rangle_{BC} + |1\rangle_A |S\rangle_{BC}$. By choosing local bases $\{|i\rangle_B\}_{i=0...m-1}$ and $\{|i\rangle_C\}_{i=0...n-1}$ for Bob and Charlie respectively, we can express the state as

$$|\psi\rangle = (|0\rangle_A(R\otimes I) + |1\rangle_A(S\otimes I))\,|\Phi_n\rangle = \left(|0\rangle_A(I\otimes R^T) + |1\rangle_A(I\otimes S^T)\right)|\Phi_m\rangle \qquad (5.2)$$

where $R_{ij} = \alpha_{ij}$, $S_{ij} = \beta_{ij}$, and $|\Phi_k\rangle = \sum_{i=0}^{k-1}|i\rangle_B|i\rangle_C$. Thus, there is a one-to-one correspondence between a $2\otimes m\otimes n$ pure state $|\psi\rangle = |0\rangle_A|R\rangle_{BC} + |1\rangle_A|S\rangle_{BC}$ and the pair of matrices (R,S), so that to every $|\psi\rangle$ and choice of indeterminates μ,λ, we can uniquely associate the pencil $\mathcal{P}_{(R,S)}$ which we shall equivalently denote as $\mathcal{P}_\psi$.

There exists a nice relationship between the structure of $\mathcal{P}_\psi$ and the local ranks of each subsystem. The reduced states of Bob and Charlie are obtained by performing a partial trace on the matrix $|\psi\rangle\langle\psi|$. From above, then, it follows that

$$\begin{aligned}\rho_B &= tr_{AC}(|\psi\rangle\langle\psi|) = RR^\dagger + SS^\dagger\\ \rho_C &= tr_{AB}(|\psi\rangle\langle\psi|) = R^T\bar{R} + S^T\bar{S}.\end{aligned} \qquad (5.3)$$

Here, "T" denotes the matrix transpose with respect to the basis $|i\rangle_{BC}\langle j|$ and "-" the complex conjugate of its entries. Also note that since Alice has a two dimensional system, her subsystem will either have full rank or $|\psi\rangle$ is a product state of the form $|\psi\rangle = |\hat{0}\rangle_A|\phi\rangle_{BC}$. In this case, we say Alice is **separated** from Bob and Charlie. Combining these facts, we can prove the following.

Lemma 5. *(i) Bob and Charlie share pure entanglement (Alice separated) if and only if $\mathcal{P}_\psi$ can be expressed as a matrix polynomial in one indeterminate $\hat{\lambda}$; i.e.*

$$\mu R + \lambda S = \hat{\lambda}\hat{S}, \qquad (5.4)$$

and (ii) Bob and Charlie's local ranks are $m-h$ and $n-g$ respectively where g is the zero index number of $\mathcal{P}_\psi$ and h its transpose zero index number.

Proof. (i) Alice is unentangled if and only if up to an overall phase, the state can be written as $|0\rangle(|R\rangle + |S\rangle) + \alpha|1\rangle(|R\rangle + |S\rangle)$ which happens if and only if its associated pencil is $(\mu+\lambda\alpha)R+(\mu+\lambda\alpha)S = (\mu+\lambda\alpha)(R+S) = \hat{\lambda}\hat{S}$. (ii) By definition, the zero index number is the number of linearly independent constant vectors $|v_i\rangle$ such that $R|v_i\rangle = S|v_i\rangle = 0$. In this case, we must also have $\bar{R}|\bar{v}_i\rangle = \bar{S}|\bar{v}_i\rangle = 0$. It follows from (5.3) that $\rho_C|\bar{v}_i\rangle = 0$ if and only if $\bar{R}|\bar{v}_i\rangle = \bar{S}|\bar{v}_i\rangle = 0$ and since complex conjugation does not affect linear dependence, we have $rank(\rho_C) = n - g$. An analogous argument shows that $rank(\rho_B) = m - h$. □

We now want to observe the effect of local invertible operators implemented by Alice, Bob, and Charlie; i.e. an SLOCC transformation. Any such operation can be decomposed as $(A \otimes I_{BC})(I_A \otimes B \otimes C)$ where Bob and Charlie first act, and then Alice follows alone. When Bob and Charlie perform the invertible operator $B \otimes C$, it is easy to check that the transformation $|R\rangle_{BC} \to B \otimes C|R\rangle_{BC}$ corresponds to $R \to BRC^T$ and likewise for S. Thus, the action of Bob and Charlie initiates the matrix pencil transformation $\mu R + \lambda S \to B(\mu R + \lambda S)C^T$. In other words, *local invertible operators of Bob and Charlie map matrix pencils to strictly equivalent ones.*

Any invertible operation by Alice can be represented by a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad-bc \neq 0$. Then the most general action by Alice will transform the state $|\psi\rangle$ as:

$$|0\rangle_A|R\rangle_{BC} + |1\rangle_A|S\rangle_{BC} \to |0\rangle_A(a|R\rangle_{BC} + c|S\rangle_{BC}) + |1\rangle_A(b|R\rangle_{BC} + d|S\rangle_{BC}). \tag{5.5}$$

Hence, the corresponding pencil transformation is $\mu R + \lambda S \to (\mu a + \lambda b)R + (\mu c + \lambda d)S = \hat{\mu}R + \hat{\lambda}S$ where $\hat{\mu} = \mu a + \lambda b$ and $\hat{\lambda} = \mu c + \lambda d$.

While obviously such a coordinate change does not alter the rank, what concerns us is how the transformation $(\mu, \lambda) \to (\hat{\mu}, \hat{\lambda})$ affects the eigenvalues and minimal indices of a given pencil. For the latter, care must be taken since minimal indices are defined by the degree of polynomials in variables μ and λ. Nevertheless, the following lemma shows minimal indices to be an SLOCC invariant in $2 \otimes m \otimes n$ systems.

Lemma 6. *The minimal indices of a given pencil remain invariant under the action of*

Alice.

Proof. Let r denote the rank of the given pencil. Under an invertible transformation $(\mu,\lambda)\to(\hat{\mu},\hat{\lambda})=(a\mu+b\lambda,c\mu+d\lambda)$, a polynomial r-component vector

$$p(\mu,\lambda)=\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}x_{ij}\mu^i\lambda^j$$

is identically zero iff $p(\hat{\mu},\hat{\lambda})\equiv 0$. To see this, we can introduce the standard basis $\{\mathbf{e}_k\}_{k=1\ldots r}$ and consider $p(\mu,\lambda)$ as an rmn-component vector in the space spanned by basis $\mu^i\lambda^j\mathbf{e}_k$. Then the transformation $(\mu,\lambda)\to(\hat{\mu},\hat{\lambda})$ induces a homomorphism on this space which thus cannot map any nonzero zero vector to zero. Consequently, for any set of polynomial vectors $\{\mathbf{x}_i(\mu,\lambda)\}_{i=1\ldots n}$ (a) $(\mu R+\lambda S)\mathbf{x}_i(\mu,\lambda)\equiv 0$ iff $(\hat{\mu}R+\hat{\lambda}S)\mathbf{x}_i(\hat{\mu},\hat{\lambda})\equiv 0$, and (b) $\{\mathbf{x}_i(\mu,\lambda)\}_{i=1\ldots n}$ is linearly independent iff $\{\mathbf{x}_i(\hat{\mu},\hat{\lambda})\}_{i=1\ldots n}$ is linearly independent, where linear independence means that for polynomials $\{p_i(\mu,\lambda)\}_{i=1\ldots n}$, $\sum_{i=1}^n p_i(\mu,\lambda)\mathbf{x}_i(\mu,\lambda)\equiv 0\Rightarrow p_i(\mu,\lambda)\equiv 0$ for all i. Next, we claim that (c) for any set of linearly independent scalar vectors $\{x_{ij}\}_{j=0\ldots\epsilon}$ with $x_{i\epsilon}\neq 0$, the highest degree of λ having a nonzero vector coefficient in $\mathbf{x}_i(\hat{\mu},\hat{\lambda})=\sum_{j=0}^{\epsilon}x_{ij}\hat{\mu}^{\epsilon-j}\hat{\lambda}^j$ is the same as that in $\mathbf{x}_i(\mu,\lambda)=\sum_{j=0}^{\epsilon}x_{ij}\mu^{\epsilon-j}\lambda^j$. This follows because the coefficient of λ^ϵ in $\sum_{j=0}^{\epsilon}x_{ij}\hat{\mu}^{\epsilon-j}\hat{\lambda}^j=\sum_{j=0}^{\epsilon}x_{ij}(a\mu+b\lambda)^{\epsilon-j}(c\mu+d\lambda)^j$ is $\sum_{j=0}^{\epsilon}x_{ij}b^{\epsilon-j}d^j$ which is non-vanishing due to the linear independence of $\{x_{ij}\}_{j=0\ldots\epsilon}$.

From (a), (c) and the linear independence of $\{x_{ij}\}_{j=0\ldots\epsilon_i}$ noted in the introductory discussion for any fundamental set of vectors, $\mathbf{x}_1(\mu,\lambda)$ is a minimum degree polynomial in the null space of $\mu R+\lambda S$ iff $\mathbf{x}_1(\hat{\mu},\hat{\lambda})$ is a minimum degree polynomial in the null space of $\hat{\mu}R+\hat{\lambda}S$. Now suppose that $\{\mathbf{x}_i(\mu,\lambda)\}_{i=1\ldots n}$ are the first n vectors in a fundamental set for $\mu R+\lambda S$ iff $\{\mathbf{x}_i(\hat{\mu},\hat{\lambda})\}_{i=1\ldots n}$ are the first n vectors in a fundamental set for $\hat{\mu}R+\hat{\lambda}S$. Then by (c), $\mu R+\lambda S$ and $\hat{\mu}R+\hat{\lambda}S$ will have the same first n minimal indices. From (a), (b) and (c) again, $\mathbf{x}_{n+1}(\hat{\mu},\hat{\lambda})$ will be the next vector in the same fundamental set for $\mu R+\lambda S$ iff $\mathbf{x}_{n+1}(\hat{\mu},\hat{\lambda})$ is likewise for $\hat{\mu}R+\hat{\lambda}S$. Hence by induction and by running the exact same argument on $(\mu R+\lambda S)^T$, the lemma is proven. □

As for the elementary divisors, Alice's transformation does have an effect. By direct substitution, it follows immediately that after normalization, the divisors transform as

$$\mu^n \to \begin{cases} (\mu\frac{a}{b}+\lambda)^n & \text{if } \ b \neq 0 \\ \\ \mu^n & \text{if } \ b = 0, \end{cases} \quad \text{and} \quad (\mu x_i + \lambda)^n \to \begin{cases} (\mu\frac{ax_i+c}{bx_i+d}+\lambda)^n & \text{if } \ bx_i+d \neq 0 \\ \\ \mu^n & \text{if } \ bx_i+d = 0. \end{cases}$$

We see that eigenvalues transform as

$$x_i \to \begin{cases} \text{for } \ b=0 & \begin{cases} \frac{ax_i+c}{bx_i+d} \ \text{ if } \ x_i \neq -d/b, +\infty, \\ \\ +\infty \ \text{ if } \ x_i = +\infty, \end{cases} \\ \\ \text{for } \ b \neq 0 & \begin{cases} +\infty \ \text{ if } \ x_i = -d/b, \\ \\ a/b \ \text{ if } \ x_i = +\infty. \end{cases} \end{cases} \tag{5.6}$$

which exactly defines a **linear fractional transformation** on the extended complex line $\mathbb{C}^*$. As a result, we have

Theorem 5.5. *Two $2 \otimes m \otimes n$ states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent if and only if their corresponding pencils are of the same rank, have the same minimal indices, and there exists a linear fractional transformation (LFT) relating the eigenvalues x_i of $\mathcal{P}_\psi$ to the eigenvalues y_i of $\mathcal{P}_\phi$ such that x_i and y_i have the same size signatures; i.e. for all i*

$$\frac{ax_i+c}{bx_i+d} = y_i \quad (ad-bc \neq 0) \tag{5.7}$$

with eigenvalue size signatures remaining invariant.

A nice property of LFTs is the following which we will rely on heavily.

Proposition 1. *Given any two trios $\{x_1, x_2, x_3\}$ and $\{y_1, y_2, y_3\}$ each with distinct values, there always exists a unique LFT relating the sets [16]. The form of the transformation is* *given by the determinants*

$$a = \begin{vmatrix} x_1y_1 & y_1 & 1 \\ x_2y_2 & y_2 & 1 \\ x_3y_3 & y_3 & 1 \end{vmatrix}, \quad b = \begin{vmatrix} x_1y_1 & x_1 & y_1 \\ x_2y_2 & x_2 & y_2 \\ x_3y_3 & x_3 & y_3 \end{vmatrix}, \quad c = \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}, \quad \textit{and } d = \begin{vmatrix} x_1y_1 & x_1 & 1 \\ x_2y_2 & x_2 & 1 \\ x_3y_3 & x_3 & 1 \end{vmatrix}. \tag{5.8}$$

A corollary of the uniqueness in an LFT relating three distinct numbers is the infinitude of SLOCC equivalence classes among states with four distinct elementary divisors. Indeed, for each x_1, there exist infinite values for x_2 such that states having eigenvalues $(0, 1, 2, x_1)$ and $(0, 1, 2, x_2)$ are inequivalent; this follows because there are only a finite number of LFTs that map the first three numbers onto themselves. As a result, we can always find an infinite set $\{x_1, x_2, ...\}$ such that states with eigenvalues $(0, 1, 2, x_1)$ and $(0, 1, 2, x_2)$ are inequivalent for each x_i. Since states of $2 \otimes m \otimes n$ systems can have at least four distinct elementary divisors if and only if $min\{m, n\} \geq 4$, this leads to the following.

Corollary 2. *Systems of dimension $2 \otimes m \otimes n$ have an infinite number of SLOCC equivalence classes if and only if $min\{m, n\} \geq 4$.*

By slightly generalizing our current analysis, we can strengthen the previous result and prove that for any $p \otimes m \otimes n$ quantum system, a finite number of orbits requires at least one of the subsystems to be a qubit. To accomplish this, it is sufficient to study the dimensions $3 \otimes 3 \otimes 3$ in which a third indeterminate can be introduced to represent any state by the pencil $\lambda R + \mu S + \omega T$. The following lemma proves the infinitude of SLOCC equivalence classes in such systems by using a family of states introduced in [21] where an alternative argument is given for the following result.

Lemma 7. *Consider the family of states*

$$|\psi_t\rangle = |0\rangle(|00\rangle + |12\rangle) + |1\rangle(|11\rangle + |02\rangle) + |2\rangle(t|22\rangle + |10\rangle).$$

For every distinct $t, s \in \mathbb{C}$, $|\psi_t\rangle$ and $|\psi_s\rangle$ are SLOCC inequivalent.

Proof. Suppose the contrary and that $A \otimes B \otimes C|\psi_t\rangle = |\psi_s\rangle$ for some invertible operations. The corresponding matrix pencil of $|\psi_t\rangle$ is

$$\mathcal{P}_{\psi_t}(\mu, \lambda, \omega) = \begin{pmatrix} \mu & \cdot & \lambda \\ \omega & \lambda & \cdot \\ \cdot & \mu & t\omega \end{pmatrix}. \tag{5.9}$$

Alice's operation induces the mapping $x = (\mu, \lambda, \omega)^T \to Ax = (\hat{\mu}, \hat{\lambda}, \hat{\omega})^T$, and after her action, the pencils $\mathcal{P}_{\psi_t}(\hat{\mu}, \hat{\lambda}, \hat{\omega})$ and $\mathcal{P}_{\psi_s}(\mu, \lambda, \omega)$ are strictly equivalent. Thus by invariance of the determinant, we must have

$$\hat{\mu}\hat{\lambda}\hat{\omega} = g\mu\lambda\omega \tag{5.10}$$

where g is some constant. Eq. (5.10) can be true only if, up to an overall permutation, x transforms as $(\hat{\mu}, \hat{\lambda}, \hat{\omega})^T = (a\mu, b\lambda, c\omega)$ where $abc = g \neq 0$. As a result, B and C satisfy

$$B \begin{pmatrix} a\mu & \cdot & b\lambda \\ c\omega & b\lambda & \cdot \\ \cdot & a\mu & ct\omega \end{pmatrix} = \begin{pmatrix} \mu & \cdot & \lambda \\ \omega & \lambda & \cdot \\ \cdot & \mu & s\omega \end{pmatrix} C^{T^{-1}}. \tag{5.11}$$

Since the action of B and $C^{T^{-1}}$ is to perform elementary row and column operations respectively, Eq. (5.11) implies the existence of some constants $\{r_i, c_i\}_{i=1\ldots3}$ such that

$$\begin{cases} ar_1 = c_1, \;\; ar_3 = c_2, \;\; br_1 = c_3, \\ cr_2 = c_1, \;\; br_2 = c_2, \;\; tcr_3 = sc_3. \end{cases}$$

However, these equations can all be simultaneously satisfied only if $t = s$. □

5.2.3 Equivalence Algorithm

Using Theorem (5.5), we can construct an algorithm for determining whether two general $2 \otimes m \otimes n$ pure states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent.

(I) Input pencils $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ and determine their rank, minimal indices, eigenvalues and corresponding eigenvalue size signatures. If the rank, minimal indices, and set of eigenvalue size signatures are not the same, $|\psi\rangle$ and $|\phi\rangle$ are inequivalent. If they are and $\mathcal{P}_\psi$ has less than three eigenvalues, $|\psi\rangle$ and $|\phi\rangle$ are equivalent. If $\mathcal{P}_\psi$ has three or more eigenvalues, proceed to the next step.

(II) Fix any three eigenvalues x_i of $\mathcal{P}_\psi$. Choose any sequence of three eigenvalues y_i belonging to $\mathcal{P}_\psi$ having the same size signatures as the x_i. Determine the LFT relating (x_1, y_1), (x_2, y_2), and (x_3, y_3) according to (5.8). Choose a new x_i and determine if the LFT relates it to any remaining y_i with the same size signature. By uniqueness of the LFT, if there is no such y_i, the states are not equivalent. If there is, choose another x_i and repeat the search on the remaining y_i.

(III) If a perfect matching exists for all x_i and y_i, then the states are equivalent. If not, repeat step (II) by choosing another ordered trio of the y_i. If no LFT exists for all possible trios, the states are not equivalent.

The Kronecker canonical form of an $m \times n$ pencil can be computed in time $O(m^2n)$ (see the algorithm by Beelen and Van Dooren [8]). For sets of t elementary divisors, Step (II) of this algorithm will require at most $O(t^3)$ steps. Thus the total running time is $O(m^2n + \min\{m, n\}^3)$. Furthermore, the algorithm is constructive in nature because if two states are SLOCC equivalent, we determine the the specific a, b, c, d constituting Alice's operator in the transformation $|\psi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$. The operators Bob and Charlie are to perform can be determined from the invertible matrices that bring pencils $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ to their canonical forms of (5.1) and are so-obtained by a Gaussian elimination procedure [48]. Hence, not only does our algorithm determine whether two states are equivalent, but it provides the necessary operators achieving the transformations.

5.2.4 The State Kronecker Canonical Form

We now wish to define a unique canonical form, which we will call the **State Kronecker canonical form (SKCF)**, to which every state in dimensions $2 \otimes m \otimes n$ is SLOCC equivalent. To compute the SKCF of a state $|\psi\rangle$, denoted as F_ψ, we first compute the Kronecker canonical form (KCF) of pencil $\mathcal{P}_\psi$, which according to Lemma (4) is specified completely by its minimal indices and its canonical sequence of eigenvalues $\hat{x}$ with corresponding size signature sequence $\hat{X}$. Under an SLOCC transformation, both the minimal indices and the sequence $\hat{X}$ remain invariant. Thus we just need some canonical way to choose the eigenvalues with respect to an LFT; the following algorithm suffices:

- Input canonical eigenvalue sequence $\hat{x} = (x_1, ..., x_f)$ of pencil $\mathcal{P}_\psi$. If $f < 3$, then let θ_0 be the LFT that maps $(x_1, ..., x_f)$ to the first f elements of $(0, 1, \infty)$. Apply θ_0 to $\mathcal{P}_\psi$ and output F_ψ as the KCF of this resultant pencil.

- If $f \geq 3$, let $\mathcal{B}_i$ be the set of all eigenvalues with the same size signature as x_i. Let

  $$T_\psi = \{\{\theta(x_1), ..., \theta(x_f)\}\colon \theta \text{ is an LFT mapping distinct elements}$$
  $$(x_i, x_j, x_k) \mapsto (0, 1, \infty) \text{ for } x_i \in \mathcal{B}_1,\ x_j \in \mathcal{B}_2,\ x_k \in \mathcal{B}_3\}.$$

  Note that this set must be of finite size. With respect to some fixed total ordering of sequences of complex numbers, let θ_0 be the LFT that realizes the minimal element in T_ψ. Apply θ_0 to $\mathcal{P}_\psi$ and output F_ψ as the KCF of this resultant pencil.

Theorem 5.6. *States $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent iff they have the same State Kronecker Canonical Form F_ψ and F_ϕ.*

Proof. If the states have the same SKCF F, then for both $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ there is an LFT that maps each to some form strictly equivalent to F. Since the set of LFTs is closed under composition and inversion, there exists an SLOCC transformation relating $|\psi\rangle$ and $|\phi\rangle$.

Conversely, suppose $|\psi\rangle$ and $|\phi\rangle$ are SLOCC equivalent. Let $\mathcal{P}_\psi$ and $\mathcal{P}_\phi$ have respective canonical sequences of eigenvalues $(x_1, ..., x_f)$ and $(y_1, ..., y_f)$, and note that they will have the *same* corresponding size signature sequence $(X^1, ..., X^f)$. The additional invariance in minimal indices then implies that the states will have the same SKCF if $T_\psi = T_\phi$. Now, there is some invertible LFT $\bar{\theta}$ so that $\{y_1, ..., y_f\} = \{\bar{\theta}(x_1), ..., \bar{\theta}(x_f)\}$, and thus x_i will have the same size signature as x_j iff $\bar{\theta}(x_i)$ has the same size signature as y_j. Then again since the set of LFTs form a group under composition, we have $\{\theta(y_1), ..., \theta(y_f)\} \in T_\psi \Rightarrow \{\theta\bar{\theta}(x_1), ..., \theta\bar{\theta}(x_f)\} \in T_\phi$, and likewise $\{\theta(x_1), ..., \theta(x_f)\} \in T_\psi \Rightarrow \{\theta\bar{\theta}^{-1}(y_1), ..., \theta\bar{\theta}(x_f)\} \in T_\phi$. □

5.2.5 All Tripartite Systems with a Finite SLOCC Equivalence Partitioning

As a result of Corollary 2 and Lemma 7, for tripartite systems, a finite number of SLOCC equivalence classes exists only in systems of low dimensions. To count and characterize all the orbits, we just need to find what combination of minimal indices and elementary divisors fit in an $m \times n$ matrix of form (5.1). A few simplifications assist in this process. First, since any $m \times n$ pencil is simply the matrix transpose of an $n \times m$ one, it is enough to just consider $m \leq n$. Next, for a given dimension, we must only study the equivalence classes with Bob and Charlie having maximal local ranks since any rank deficient case will correspond to a class of maximum local ranks in a smaller dimension. To this end, Lemma (5) allows us to immediately determine the local ranks associated with each equivalence class. Furthermore, as evident from the Schmidt decomposition of any state with respect to bipartition AB:C, Charlie's local rank cannot exceed the product of Alice and Bob's. Consequently, if $n \geq 2m$, any state of a $2 \otimes m \otimes n$ system is the same as one in a $2 \otimes m \otimes 2m$ system up to a local change of basis on Charlie's part. This means that for the task of finite enumeration, we only need to consider systems up to dimensions $2 \otimes 2 \otimes 4$ and $2 \otimes 3 \otimes 6$.

One further property of each equivalence class that we are able to study is the tensor rank. The tensor rank of a state is the minimum number of product states whose linear span contains the state, and this quantity turns out to be invariant under invertible SLOCC transformations [39]. For bipartite systems, the tensor rank is equivalent to the Schmidt rank, and a non-increase in Schmidt rank is also a sufficient condition for SLOCC convertibility between two such states; SLOCC equivalence classes are characterized completely by the Schmidt rank. Interestingly, in three qubit systems, tensor rank is also sufficient to distinguish between the various equivalence classes. However, we find that even for systems having a finite partitioning, the tensor rank is an insufficient measure for determining SLOCC equivalence. Our results follow from previous research on the tensor rank of matrix pencils done by Ja' Ja' [63] and rederived in Ref. [18].

Lemma 8. [63],[18] *Let $\mathcal{P}_{(R,S)}$ be a pencil with no infinite divisors in canonical form* (4) *with minimal indices $\epsilon_1, ..., \epsilon_p$ and $\nu_1, ..., \nu_q$ and J an $l \times l$- sized pencil. Furthermore, let $\delta(J)$ denote the number of invariant polynomials containing at least one nonlinear elementary divisor. Then the tensor rank of $\mathcal{P}_{(R,S)}$ is given by*

$$\sum_{i=1}^{p}(\epsilon_i + 1) + \sum_{j=1}^{q}(\nu_j + 1) + l + \delta(J). \tag{5.12}$$

A summary of all the equivalence classes is presented in Table 5.1 and the State Kronecker Canonical Forms representing each class are given below. We see that there are 26 distinct SLOCC classes for $2 \otimes 3 \otimes n$ ($n \geq 6$) systems. This reproduces the findings of Chen *et al.* [21] here obtained in an entirely different way by using matrix pencil analysis.

Representative	Local Ranks	Tensor Rank	Representative	Local Ranks	Tensor Rank
(A:B:C)	(1,1,1)	1	(AB:C)	(2,2,1)	2
(AC:B)	(2,1,2)	2	(A:BC-1)	(1,2,2)	2
(ABC-1)	(2,2,2)	2	(ABC-2)	(2,2,2)	3
(ABC-3)	(2,2,3)	3	(ABC-4)	(2,2,3)	3
(ABC-5)	(2,2,4)	4	(ABC-6)	(2,3,2)	3
(ABC-7)	(2,3,2)	3	(ABC-8)	(2,3,3)	3
(ABC-9)	(2,3,3)	3	(A:BC-2)	(1,3,3)	2
(ABC-10)	(2,3,3)	4	(ABC-11)	(2,3,3)	4
(ABC-12)	(2,3,3)	4	(ABC-13)	(2,3,3)	4
(ABC-14)	(2,3,4)	4	(ABC-15)	(2,3,4)	4
(ABC-16)	(2,3,4)	5	(ABC-17)	(2,3,4)	4
(ABC-18)	(2,3,4)	4	(ABC-19)	(2,3,5)	5
(ABC-20)	(2,3,5)	5	(ABC-21)	(2,3,5)	6

Table 5.1: Summary Equivalence Classes in $2 \otimes 3 \otimes 6$ Systems

$2 \otimes 2 \otimes 2$ Systems

Here the states are represented as 2×2 pencils. We first consider the case with no minimal indices. Here there can only be two or one distinct elementary divisors with the latter having possible signatures of $(1,1)$ and $(0,2)$. In matrix and bra-ket form, these correspond to the unnormalized states

$$\begin{matrix} \left(\begin{smallmatrix} \lambda & \cdot \\ \cdot & \mu+\lambda \end{smallmatrix}\right)\text{(ABC-1) ``GHZ-class''} & \left(\begin{smallmatrix} \lambda & \cdot \\ \cdot & \lambda \end{smallmatrix}\right)\text{(A:BC-1)} & \left(\begin{smallmatrix} \lambda & \mu \\ \cdot & \lambda \end{smallmatrix}\right)\text{(ABC-2) ``W-class''} \\ (|0\rangle + |1\rangle)|11\rangle + |100\rangle & |100\rangle + |111\rangle & |001\rangle + |100\rangle + |111\rangle. \end{matrix}$$

By Lemma (8), the tensor rank of (ABC-1) is two and indeed by the invertible transformation $|1\rangle(\langle 0| + \langle 1|) + |0\rangle\langle 1|$ on Alice's part, the state can be brought into the standard form $|000\rangle + |111\rangle$. On the other hand, (ABC-2) has an elementary divisor of λ^2 so its tensor rank is three. Likewise, it can be put in the standard form $|100\rangle + |010\rangle + |001\rangle$ by an SLOCC transformation. By Lemma 5, (A:BC-1) represents a state of pure entanglement shared between Bob and Charlie.

Evidently, by examining Lemma (4), the only possible classes included in three qubit systems are those with Bob and Charlie having non-maximal local ranks. When $h = 1, g = 0$, the only possibility is $\epsilon_1 = 1$, while for $h = 0, g = 1$ it must be $\nu_1 = 1$. The case of

$h = 1, g = 1$, there are no non-zero minimal indices. These three states are given by

$$\left(\begin{smallmatrix} \cdot & \cdot \\ \lambda & \mu \end{smallmatrix}\right)_{\text{(AC:B)}} \qquad \left(\begin{smallmatrix} \cdot & \lambda \\ \cdot & \mu \end{smallmatrix}\right)_{\text{(AB:C)}} \qquad \left(\begin{smallmatrix} \cdot & \cdot \\ \cdot & \mu \end{smallmatrix}\right)_{\text{(A:B:C)}}$$

$$|011\rangle + |101\rangle \qquad |011\rangle + |101\rangle \qquad |011\rangle.$$

We see that (A:B:C) represents the product states while (AC:B) and (AB:C) are the bipartite pure entanglement with respect to the specified partitioning.

$2 \otimes 2 \otimes 3$ **Systems**

Since we are only concerned with the states of maximal local ranks for Bob and Charlie, we only consider pencils having $h = g = 0$. The only possible minimal indices are $\epsilon_1 = 1$ and $\epsilon_1 = 2$ which correspond to the states

$$\left(\begin{smallmatrix} \lambda & \mu & \cdot \\ \cdot & \cdot & \lambda \end{smallmatrix}\right)_{\text{(ABC-3)}} \qquad \left(\begin{smallmatrix} \lambda & \mu & \cdot \\ \cdot & \lambda & \mu \end{smallmatrix}\right)_{\text{(ABC-4)}}$$

$$|001\rangle + |100\rangle + |112\rangle \qquad |001\rangle + |012\rangle + |100\rangle + |111\rangle.$$

The state (ABC-3) has a single elementary divisor of λ while (ABC-4) has none. According to Lemma (8), the tensor rank of both these states is three. In fact, an explicit three-term expansion of (ABC-3) is given by $\frac{1}{2}|+_{01}\rangle|+_{01}\rangle|+_{12}\rangle + \frac{1}{2}|-_{01}\rangle|-_{01}\rangle|-_{12}\rangle + |1\rangle|0\rangle|+_{02}\rangle$ where $|\pm_{ij}\rangle = |i\rangle \pm |j\rangle$.

$2 \otimes 2 \otimes n$ **Systems for** $n \geq 4$

As noted in the discussion above, it is enough to consider $2 \otimes 2 \otimes 4$ systems. For states with Bob and Charlie having full local ranks, the only possible minimal indices are $\epsilon_1 = \epsilon_2 = 1$ which corresponds to the state

$$\left(\begin{smallmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu \end{smallmatrix}\right)_{\text{(ABC-5)}}$$

$$|001\rangle + |013\rangle + |100\rangle + |112\rangle.$$

$2 \otimes 3 \otimes 2$ **Systems**

These pencils are simply the transpose of 2×3 pencils and thus contribute two equivalence classes of states with maximal local ranks:

$$\begin{pmatrix} \lambda & \cdot \\ \mu & \cdot \\ \cdot & \lambda \end{pmatrix}\text{(ABC-6)} = \text{(ABC-3)}^T \qquad \begin{pmatrix} \lambda & \cdot \\ \mu & \lambda \\ \cdot & \mu \end{pmatrix}\text{(ABC-7)} = \text{(ABC-4)}^T$$

$$|010\rangle + |100\rangle + |121\rangle \qquad |010\rangle + |021\rangle + |100\rangle + |111\rangle.$$

$2 \otimes 3 \otimes 3$ Systems

Here we have 3×3 pencils and for those having no minimal indices, the representative states are

$$\begin{pmatrix} \lambda & \cdot & \cdot \\ \cdot & \mu{+}\lambda & \cdot \\ \cdot & \cdot & \mu \end{pmatrix}\text{(ABC-8)} \qquad \begin{pmatrix} \lambda & \cdot & \cdot \\ \cdot & \lambda & \cdot \\ \cdot & \cdot & \mu{+}\lambda \end{pmatrix}\text{(ABC-9)} \qquad \begin{pmatrix} \lambda & \cdot & \cdot \\ \cdot & \lambda & \cdot \\ \cdot & \cdot & \lambda \end{pmatrix}\text{(A:BC-2)}$$

$$|100\rangle{+}(|0\rangle + |1\rangle)|11\rangle + |022\rangle \qquad |100\rangle + |111\rangle + |022\rangle \qquad |100\rangle + |111\rangle + |122\rangle$$

$$\begin{pmatrix} \lambda & \mu & \cdot \\ \cdot & \lambda & \cdot \\ \cdot & \cdot & \lambda \end{pmatrix}\text{(ABC-10)} \qquad \begin{pmatrix} \lambda & \mu & \cdot \\ \cdot & \lambda & \cdot \\ \cdot & \cdot & \mu{+}\lambda \end{pmatrix}\text{(ABC-11)} \qquad \begin{pmatrix} \lambda & \mu & \cdot \\ \cdot & \lambda & \mu \\ \cdot & \cdot & \lambda \end{pmatrix}\text{(ABC-12)}$$

$$|001\rangle{+}|100\rangle + |111\rangle + |122\rangle \qquad |001\rangle + |100\rangle + |111\rangle + (|0\rangle + |1\rangle)|22\rangle \qquad |001\rangle + |012\rangle + |100\rangle + |111\rangle + |122\rangle.$$

For 3×3 pencils, the only possible minimal indices are $\epsilon_1 = \nu_1 = 1$ corresponding to the representative state

$$\begin{pmatrix} \lambda & \mu & \cdot \\ \cdot & \cdot & \mu \\ \cdot & \cdot & \lambda \end{pmatrix}\text{(ABC-13)}$$

$$|001\rangle{+}|012\rangle + |100\rangle + |122\rangle.$$

$2 \otimes 3 \otimes 4$ Systems

For a minimal indice of $\epsilon_1 = 1$, we have the classes represented by

$$\begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \lambda & \cdot \\ \cdot & \cdot & \cdot & \lambda \end{pmatrix}\text{(ABC-14)} \qquad \begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \lambda & \cdot \\ \cdot & \cdot & \cdot & \lambda{+}\mu \end{pmatrix}\text{(ABC-15)} \qquad \begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu \\ \cdot & \cdot & \cdot & \lambda \end{pmatrix}\text{(ABC-16)}$$

$$|001\rangle + |100\rangle + |112\rangle + |123\rangle \qquad |001\rangle + |100\rangle + |112\rangle {+}(|0\rangle + |1\rangle)|23\rangle \qquad |001\rangle + |013\rangle + |100\rangle {+}|112\rangle + |123\rangle.$$

We also have the states with $\epsilon_1 = 2$ and $\epsilon_1 = 3$ respectively:

$$\begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \lambda \end{pmatrix} \text{(ABC-17)} \qquad \begin{pmatrix} \lambda & \mu & \cdot & \cdot \\ \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \lambda & \mu \end{pmatrix} \text{(ABC-18)}$$

$$|001\rangle + |012\rangle + |100\rangle + |111\rangle + |123\rangle \qquad |001\rangle + |012\rangle + |023\rangle + |100\rangle + |111\rangle + |122\rangle.$$

$2 \otimes 3 \otimes 5$ Systems

The possibilities are $\epsilon_1 = 1, \epsilon_2 = 1$ and $\epsilon_1 = 1, \epsilon_2 = 2$ corresponding to

$$\begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \cdot & \lambda \end{pmatrix} \text{(ABC-19)} \qquad \begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot \\ \cdot & \cdot & \lambda & \mu & \cdot \\ \cdot & \cdot & \cdot & \lambda & \mu \end{pmatrix} \text{(ABC-20)}$$

$$|001\rangle + |013\rangle + |100\rangle \qquad |001\rangle + |013\rangle + |024\rangle$$

$$+ |112\rangle + |124\rangle \qquad + |100\rangle + |112\rangle + |123\rangle.$$

$2 \otimes 3 \otimes n$ Systems for $n \geq 6$

We must only consider $n = 6$ which allows for $\epsilon_1 = 1, \epsilon_2 = 1, \epsilon_3 = 1$ with representative

$$\begin{pmatrix} \lambda & \mu & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \lambda & \mu & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \lambda & \mu \end{pmatrix} \text{(ABC-21)}$$

$$|001\rangle + |013\rangle + |025\rangle + |100\rangle + |112\rangle + |124\rangle.$$

5.2.6 Non-Invertible Transformations

A natural question is whether it is possible to transform from one class to another via non-invertible transformations. One obvious constraint is that states with full local ranks cannot preserve their ranks under a non-invertible transformation. Consequently, we cannot non-reversibly convert among inequivalent states with the same local ranks. A possible conjecture might be that unidirectional convertibility is achievable if none of the local ranks increase and at least one decreases; certainly three qubit systems satisfy this hypothesis. This, however, is false in general as we will now observe.

Let $|\psi\rangle$ be some state having maximal local ranks of $(2, m, n)$ and suppose $|\phi\rangle$ is a state with ranks $(2, m, n-1)$. If $|\phi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\psi\rangle$, Alice and Bob's matrices inducing the transformation will be full rank while Charlie's will have rank $n-1$. As for the latter, any such operator can be decomposed into a series of elementary column operations (permutations, column-multiplications, column-additions) on $\mathcal{P}_\psi$ which results in exactly $n-1$ linearly independent columns. If column i is the resultant linearly dependent column, then immediately after all column-additions of the i^{th} column are performed, the remaining $n-1$ columns must correspond to some state SLOCC equivalent to $|\phi\rangle$. As a result, we obtain the following criterion.

Theorem 5.7. *Let $|\psi\rangle$ and $|\phi\rangle$ be states with local ranks $(2,m,n)$ and $(2,m,n-1)$, and let $c_1,...,c_n$ denote the columns of $\mathcal{P}_\psi(\mu,\lambda)$. Then $|\phi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\psi\rangle$ iff for some $1 \leq i \leq n$, there exists constants $a_1,..,a_{i-1},a_{i+1},...,a_n$ and some invertible linear transformation $(\mu,\lambda)\to(\hat{\mu},\hat{\lambda})$ such that the pencil $\mathcal{P}_{\psi_i}(\hat{\mu},\hat{\lambda}) = [c_1+a_1c_i,...,c_n+a_nc_i]$ is strictly equivalent to $\mathcal{P}_\phi(\mu,\lambda)$.*

In general, for transformations in which Charlie's rank decreases to $n-k$, one need only modify this theorem by considering subpencils of $\mathcal{P}_\psi$ having $n-k$ columns where to each of the columns is added a linear combination of the k non-included columns. Likewise, to account for transformations when Bob's local rank decreases, the above criterion can be applied with the analysis conducted on the rows of $\mathcal{P}_\psi(\mu,\lambda)$ instead of its columns.

On the surface, Theorem 5.7 has limited value since it involves a search for values a_1,..,a_{i-1}, a_{i+1},...,a_n over the complex numbers. However, in many cases, it is easy to see whether or not such a collection of numbers can be found. For example, for $1 \leq i \leq 4$ in (ABC-19), upon any choice of the a_j and any transformation $\hat{\mu},\hat{\lambda}$, the resultant pencil $\mathcal{P}_{\psi_i}(\hat{\mu},\hat{\lambda})$ will either be rank two or it will have an elementary divisor of degree at least one. However, the state (ABC-18) is rank three with no non-trivial elementary divisors. Thus, the transformation (ABC-19)→(ABC-18) is impossible. On the other hand, for the state (ABC-17), when $i=1$, we have $\det\mathcal{P}_{\psi_1}(\mu,\lambda) = \lambda[\lambda^2 - \mu(\frac{a_2}{a_3}\lambda + \frac{1}{a_3}\mu)]$ for $a_3 \neq 0$. The state (ABC-8) has $\det \mathcal{P}_{\phi}(\mu,\lambda) = \lambda(\mu+\lambda)(2\mu+\lambda)$. By choosing $c_2 = \frac{3}{2}$ and $c_3 = -\frac{1}{2}$, these polynomials become equal as well as the elementary divisors, the ranks, and the minimal indices of the pencils. Thus (ABC-17)→(ABC-8) is achievable by SLOCC.

In a manner similar to that just described, we have used Theorem 5.7 to analyze all possible transformations among the $2\otimes 3\otimes n$ equivalence classes. Figure (5.1) below depicts the SLOCC hierarchy among the classes.

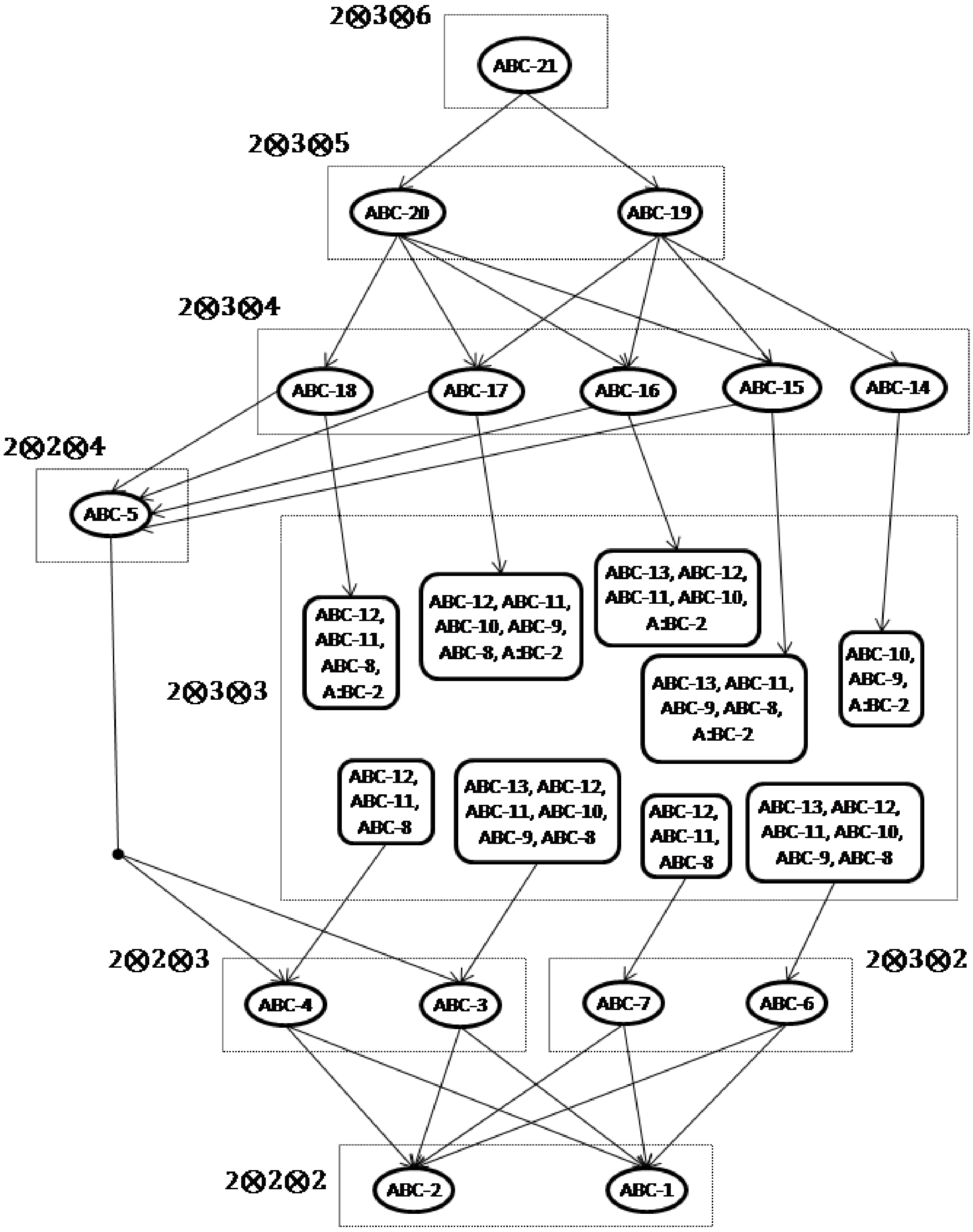
2⊗3⊗6
ABC-21
2⊗3⊗5
ABC-20
ABC-19
2⊗3⊗4
ABC-18
ABC-17
ABC-16
ABC-15
ABC-14
2⊗2⊗4
ABC-5
ABC-13, ABC-12, ABC-11, ABC-10, A:BC-2
ABC-12, ABC-11, ABC-10, ABC-9, ABC-8, A:BC-2
ABC-12, ABC-11, ABC-8, A:BC-2
ABC-10, ABC-9, A:BC-2
ABC-13, ABC-11, ABC-9, ABC-8, A:BC-2
2⊗3⊗3
ABC-12, ABC-11, ABC-8
ABC-13, ABC-12, ABC-11, ABC-10, ABC-9, ABC-8
ABC-12, ABC-11, ABC-8
ABC-13, ABC-12, ABC-11, ABC-10, ABC-9, ABC-8
2⊗2⊗3
ABC-4
ABC-3
ABC-7
ABC-6
2⊗3⊗2
2⊗2⊗2
ABC-2
ABC-1

Figure 5.1: Complete Hierarchy of SLOCC Equivalence Classes; Arrows Indicate a Non-invertible Transformation.

Conclusions and Future Research

In this section, we have used the theory of matrix pencils to study $2 \otimes m \otimes n$ pure quantum states. In doing so, we were able to derive a polynomial time algorithm for deciding SLOCC equivalence of such states. For all tripartite systems having a finite number of equivalence classes, we have obtained canonical state representatives and determined the partial ordering among these classes based on a criterion for general SLOCC convertibility in $2 \otimes m \otimes n$ systems. It is interesting to note that in the hierarchy chart of Fig. 2, there exists certain transformations that are impossible even though the local rank of Charlie decreases by two. The transformation (ABC-14) to (ABC-7) is such example.

A natural extension of this work is to find efficient algorithms for deciding LOCC equivalence, LOCC convertibility, and general SLOCC convertibility in $2 \otimes m \otimes n$ systems. Another natural next line of inquiry might to consider $p \otimes m \otimes n$ systems and their corresponding degree p matrix polynomials. Indeed, much research has been conducted on higher degree elements, especially those having special properties such as being symmetric [51]. Unfortunately, there exists no corresponding characterization like Kronecker's for strict equivalence of matrix pencils of degree greater than two. Making the project of generalizing to higher degrees more dubious is the fact that determining SLOCC equivalence for $p \otimes m \otimes n$ can be reduced from a tensor rank calculation on a set of p bilinear forms [24], and this problem has no known solution for $p > 2$ (the general problem is, in fact, NP-Hard [57])[18].

As noted above, we are not the first to study SLOCC convertibility in multipartite systems, and it would be interesting to try and develop the relationship between our results and the work of others. For example, Miyake's results involve "hyperdeterminants" and their singularities [77]. It would be valuable to investigate the correspondence between matrix pencils and hyperdeterminants or to introduce the connection to the quantum information community if such a correspondence has already been obtained. In another work, Liang *et al.* have recently proven a set of conditions both necessary and sufficient for the convertibility of two qubit mixed bell-diagonal states [72]. As these mixed states can be considered pure with respect to a $2 \otimes 2 \otimes 4$ system, it would be fruitful to study transformations between tripartite "purified" bell diagonal states via our matrix pencil construction and compare it to the convertibility conditions in Ref. [72]. Doing so might suggest ways in which purified tripartite pencils can assist in deciding equivalence between general $2 \otimes n$ mixed states.

5.3 Tripartite Transformations, Tensor Rank and Matrix Multiplication

In this section, we ask whether there is some relatively simple criterion for determining the convertibility of arbitrary tripartite states like there is for bipartite states. As a complete solution to the convertibility problem should be able to determine whether one state can be transformed into another with a nonzero probability, we focus our attention on the class of SLOCC protocols to judge the difficulty of the complete problem. Ultimately we find that no simple criterion exists for testing the possibility of a general tripartite entanglement transformation. In addition, through the course of investigating this problem many other interesting results are obtained concerning specific tripartite transformation rates. The novel conversion rates are derived in part from our observation that the tensor rank is *not a multiplicative quantity*, something previously thought to be true in the quantum information community [42], but a result already acknowledged in algebraic complexity theory (see exercise 14.12 of [18]). We now summarize our main findings.

Denote by $|\Phi^3\rangle$ the unnormalized tripartite state where any two parties share an (unnormalized) EPR state $|\Phi\rangle = |00\rangle + |11\rangle$, i.e. $|\Phi^3\rangle = |\Phi\rangle_{AB}|\Phi\rangle_{AC}|\Phi\rangle_{BC} = \sum_{i,j,k=0}^{1} |ij\rangle_A |ik\rangle_B |jk\rangle_C$. The following statements are true:

Theorem 5.8.

(a) The following problem is NP-hard: Given the classical description (e.g. a binary encoding) of two tripartite states $|\phi\rangle$ and $|\psi\rangle$, decide if $|\phi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\psi\rangle$.

(b) $|GHZ\rangle^{\otimes 3} \overset{\text{SLOCC}}{\longrightarrow} |W\rangle^{\otimes 2}$.

(c) $|GHZ\rangle^{\otimes 17} \overset{\text{SLOCC}}{\longrightarrow} |\Phi^3\rangle^{\otimes 6}$.

(d) Let $\lambda = inf\{u : |GHZ\rangle^{\otimes \lfloor un \rfloor} \overset{\text{SLOCC}}{\longrightarrow} |\Phi^3\rangle^{\otimes n}$ for sufficiently large $n\}$. Then λ is precisely the exponent for matrix multiplication*, i.e., the smallest real number ω such that two N by N matrices can be multiplied with $O(N^{\omega})$ number of multiplications between linear functions on entries of the first matrix and linear functions on entries of the second matrix.*

Previously, only one copy of the W state is known to be convertible from three copies of GHZ and result (b) provides an improvement to this rate. Transformation (c) is important because it reveals that the three-party EPR extraction rate from GHZ is greater than one, a previously unknown possibility. Our main technical tool is tensor rank, which as you may recall from Section 2.2.1, is a quantity intrinsic to every state indicating the minimum number of product states whose linear span contains that state. As emphasized, the proof of Theorem 5.8 depends on the non-multiplicativity of the tensor rank, i.e. $rk(|\phi\rangle \otimes |\psi\rangle) \neq rk(|\phi\rangle)rk(|\psi\rangle)$.

Tensor rank has been used in algebraic complexity theory as it captures the complexity of computing a set of bilinear maps [18] and in particular the multiplicative complexity of multiplying two matrices. A set of bilinear maps are polynomials with respect to two distinct groups of indeterminates. The **multiplicative complexity** of the set is the minimum number of multiplications between the two groups required to evaluate all the polynomials. The multiplication of two $N \times N$ matrices produces a set of N^2 bilinear maps, one for each entry in the $N \times N$ product. The complexity of $N \times N$ matrix multiplication is denoted by $\mu(N, N)$ and the current best upper and lower bounds for $\mu(N, N)$ are $O(N^{2.36})$ and

$\frac{5}{2}N^2 - 3N$ respectively [30, 14]. The complexity of matrix multiplication is also expressed as $\mu(N, N) = O(N^\omega)$ where ω is called the **exponent for matrix multiplication** and defined as the smallest real number such that an algorithm exists for multiplying two $N \times N$ matrices using $O(N^\omega)$ multiplications. While ω is hypothesized to be two, determining the validity of this conjecture is a major open problem in computational science; this implies the difficulty in determining λ of (d). For more details, a good reference is chapter 28 of [31].

Tensor rank analysis has already shown to be valuable in quantum information as it is the distinguishing property between the $|GHZ\rangle$ and $|W\rangle$ equivalence classes of three qubits [39, 17]. It has also been useful in characterizing the entanglement in graph states [58] as well as studying the distinguishability of states by separable operations [38]. An important property of the tensor rank is that it cannot increase under SLOCC:

Proposition 2.

If $|\phi\rangle \overset{\text{SLOCC}}{\longrightarrow} |\psi\rangle$ *then* $rk(|\phi\rangle) \geq rk(|\psi\rangle)$ [75].

Through Proposition 2, the monotonic nature of the tensor rank makes studying it physically worthwhile. Unfortunately, determining the rank of an arbitrary state is a very difficult problem [57] which is ultimately why there is no simple convertibility test applicable to all tripartite transformations. However, in some special cases it is possible to calculate the tensor rank or at least determine some useful bounds. In this section, we establish our main results described above by examining the ranks of certain tripartite states. The following statements are true where each is in a one-to-one correspondence with the main results stated earlier.

Lemma 9.

(a') $|\phi\rangle \in H_A \otimes H_B \otimes H_C$ can be SLOCC converted from state $\frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle_A |i\rangle_B |i\rangle_C$ if and only if $rk(|\phi\rangle) \leq N$.

(b') $rk(|W\rangle^{\otimes 2}) = 7$.

(c') $rk(|\Phi^3\rangle) = 7$.

(d') $rk(|\Phi^3\rangle^{\otimes n})$ is the multiplicative complexity for multiplying two $2^n \times 2^n$ matrices.

Extending Lemma 9 to prove Theorem 5.8 is straightforward. It follows from item (a') that, given a tripartite tensor $|\phi\rangle$ and a number k, deciding if $rk(|\phi\rangle) \leq k$ can be reduced to the question of whether $\sum_{i=1}^{k} |i\rangle_A|i\rangle_B|i\rangle_C \overset{\text{SLOCC}}{\longrightarrow} |\phi\rangle$. As we indicated in Section 2.2.1, the former problem is shown to be NP-hard by Håstad [57], thus the latter is also NP-hard (item (a)).

Results (b), (c), and (d) follow directly from applying (a') to (b'), (c'), and (d') respectively and using the fact that $rk(|GHZ\rangle^{\otimes n}) = 2^n$. This equality holds since, as evident by taking a Schmidt decomposition with respect to any bipartition, the tensor rank is always lower bounded by the density matrix rank of any subsystem, which is 2^n for all parties in $|GHZ\rangle^{\otimes n}$. The 17 to 6 conversion ratio of (c') is important because 6 copies of $|\Phi^3\rangle$ is a total of 18 EPR pairs. Thus, the stochastic EPR distillation rate from multiple copies of $|GHZ\rangle$ is greater than 1. In fact (d) shows that this rate can be further improved as the upper bound for ω is lowered. However, the distillation is specific in that the EPR pairs must be shared among all three parties. Indeed, if the EPR pairs are held by just two parties, $rk(|\Phi\rangle^{\otimes n}) = 2^n$ so the EPR distillation rate from n copies of $|GHZ\rangle$ equals 1. The related problem of EPR distillation from the W state has recently been studied in [47]. There, the authors show that for a single W state, the probability of extracting an EPR state via LOCC is not only higher if one does not specify which two parties share the state, but it can also be made arbitrarily close to one.

From (d) and the lower bound on $\mu(2^n, 2^n)$, it follows that $2n$ copies of GHZ cannot be converted into n copies of $|\Phi^3\rangle$ with a nonzero probability. This result is stronger than the one derived in [73] where the authors prove strictly by entropy arguments the impossibility of $|GHZ\rangle^{\otimes 2n} \to |\Phi^3\rangle^{\otimes n}$ under deterministic LOCC. Here, we obtain the stronger conclusion except by using tools of algebraic complexity theory. It is an interesting question whether these two seemingly unrelated lines of attack are actually deeply connected.

Now we turn to prove Lemma 9. We will work with unnormalized states below since any overall factor does not affect the tensor rank. For any $|\phi\rangle \in H_A \otimes H_B \otimes H_C$, let ρ_{AB} denote Alice and Bob's subsystem obtained by taking the partial trace $Tr_C(|\phi\rangle\langle\phi|)$. As ρ_{AB} is a positive operator, it has a spectral decomposition $\rho_{AB} = \sum_{k=1}^{m} p_k |\psi_k\rangle\langle\psi_k|$ where $0 < p_k \leq 1$. The vector span of $\{|\psi_k\rangle : 1 \leq k \leq m\}$ is called the support of ρ_{AB} and denoted by $supp(\rho_{AB})$. To proceed, we need the following simple equivalent characterization of a tripartite state's tensor rank.

Lemma 10. *Suppose $|\phi\rangle \in H_A \otimes H_B \otimes H_C$. The tensor rank of $|\phi\rangle$ equals the minimum number of product states in $H_A \otimes H_B$ whose linear span contains the support of $\rho_{AB} = Tr_C(|\phi\rangle\langle\phi|)$.*

Proof. Let k denote $rk(|\phi\rangle)$ and r be the minimum number of product states $\{|\alpha_j\rangle|\beta_j\rangle : 1 \leq j \leq r\}$ whose span contains $supp(\rho_{AB})$. Let $|\phi\rangle = \sum_{i=1}^{m} |i\rangle_{AB}|i\rangle_C$ be a Schmidt decomposition of $|\phi\rangle$. Each $|i\rangle_{AB}$ belongs to $supp(\rho_{AB})$ and so $|i\rangle_{AB} = \sum_{j=1}^{r} \lambda_{i,j}|\alpha_j\rangle|\beta_j\rangle$. Regrouping the $|i\rangle_C$ according to the r product states gives $r \geq k$. However, from $|\phi\rangle = \sum_{i=1}^{k} |a_i\rangle|b_i\rangle|c_i\rangle$ we have $\rho_{AB} = \sum_{i,j=1}^{k} |a_i\rangle|b_i\rangle\langle c_j|c_i\rangle\langle a_j|\langle b_j|$ implying that $supp(\rho_{AB}) \subseteq span\{|a_i\rangle|b_i\rangle : 1 \leq i \leq k\}$. Thus $k \geq r$. □

Using Lemma 10, the general procedure for determining tensor rank is now straightforward. Write $|\phi\rangle = \sum_{i=1}^{m} |i\rangle_{AB}|i\rangle_C$ where the $\{|i\rangle_C : 1 \leq i \leq m\}$ are orthonormal and then determine the minimum number of product states needed to contain the $\{|i\rangle_{AB} : 1 \leq i \leq m\}$. This question can be rephrased in another way by mapping each $|i\rangle_{AB}$ to a bilinear form f_i from the ring of indeterminates $C[\{a_j\},\{b_j\}]$ where each a_j (b_j) is in a one-to-one correspondence with a basis vector from H_a (H_b). Product states in

$H_a \otimes H_b$ correspond to a product of linear forms from $C[\{a_j\}] \times C[\{b_j\}]$ which we refer to as a *non-scalar* multiplication. Thus, we obtain the following fact:

Fact 1. *The minimum number of product states that contain the* $\{|i\rangle_{AB} : 1 \leq i \leq m\}$*, and hence the tensor rank of* $|\phi\rangle$*, is the same number of non-scalar multiplications* $M_k = (\sum_{j=1}^{n_a} \alpha_{k,j} a_j) \times (\sum_{j=1}^{n_b} \beta_{k,j} b_j)$ *needed to calculate the* $\{f_i : 1 \leq i \leq m\}$*.*

We now use the technique outlined above to study the tensor rank of certain tripartite states.

Proof of Lemma 9. (a'): For $\sum_{i=1}^{N} |i\rangle_A|i\rangle_B|i\rangle_C$, the support of ρ_{AB} is spanned by N product states. Thus by Proposition 2 and Lemma 10, a necessary condition for the given transformation is $rk(|\phi\rangle) \leq N$. Now suppose that $|\phi\rangle = \sum_{i=1}^{k} |a_i\rangle|b_i\rangle|c_i\rangle$ where $k \leq N$. Since $\{|i\rangle_A : 1 \leq i \leq N\}$ is an orthonormal set, we can define the linear operator A by $A|i\rangle_A = \begin{cases} |a_i\rangle, & 1 \leq i \leq k \\ 0, & k < i \leq N \end{cases}$. Similarly, operators B and C can be constructed. As noted in [39], the existence of such operators is sufficient for an SLOCC protocol since $|\phi\rangle$ will be obtained when Alice performs the local measurement $\{\frac{A}{||A||}, \sqrt{I_A - \frac{1}{||A||^2} A^\dagger A}\}$ and similarly for Bob and Charlie. Note that (unnormalized) $|GHZ\rangle^{\otimes n}$ can be expressed as $\sum_{i=1}^{2^n} |i\rangle_A|i\rangle_B|i\rangle_C$. (b'): This fact will be proven in the next section, but note that its proof can also be found in [113]. (c'): The corresponding bilinear forms of $|\Phi^3\rangle$ match the set of polynomials obtained when multiplying two 2×2 matrices:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^T \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} f_{00} & f_{01} \\ f_{10} & f_{11} \end{pmatrix} \tag{5.13}$$

where T indicates the matrix transpose. An algorithm for obtaining the f_i using only seven multiplications was discovered by Strassen [98] and later proven to be optimal by

Winograd [111]. These seven non-scalar multiplications are

$$
\begin{aligned}
M_0 &= (a_{00} + a_{11})(b_{00} + b_{11}) & M_1 &= (a_{10} + a_{11})b_{11} \\
M_2 &= a_{00}(b_{01} - b_{11}) & M_3 &= a_{11}(-b_{00} + b_{10}) \\
M_4 &= (a_{00} + a_{01})b_{11} & M_5 &= (-a_{00} + a_{10})(b_{00} + b_{01}) \\
M_6 &= (a_{01} - a_{11})(b_{10} + b_{11}).
\end{aligned}
$$

so that the f_{ij} can be recovered by

$$
\begin{aligned}
f_{00} &= M_0 + M_3 - M_4 + M_6 \\
f_{01} &= M_2 + M_4 \\
f_{10} &= M_1 + M_3 \\
f_{11} &= M_0 + M_2 - M_1 + M_5.
\end{aligned}
$$

Mapping back to bra-ket notation immediately leads an explicit optimal expansion

$$
\begin{aligned}
|\Phi^3\rangle = {} & |\Phi\rangle|\Phi\rangle|\Phi\rangle + |+1\rangle|00\rangle|1-\rangle + |00\rangle|-1\rangle|+1\rangle \\
& - |11\rangle|-0\rangle|+0\rangle - |+0\rangle|11\rangle|0-\rangle - |0-\rangle|0+\rangle|11\rangle + |1-\rangle|1+\rangle|00\rangle
\end{aligned}
$$

with $|\pm\rangle = |0\rangle \pm |1\rangle$. (d'): By taking multiple tensor products of the matrices in (5.13), we see that for n copies of $|\Phi^3\rangle$, the corresponding polynomials are represented by $2^n \times 2^n$ matrix multiplication. Hence, $rk(|\Phi^3\rangle^{\otimes n})$ is the complexity of this operation. □

Another recently reported consequence of the tensor ranks's non-multiplicativity is the existence of stochastic catalysis for entanglement transformations [22]. An interesting phenomena in entanglement theory which we have not mentioned yet is entanglement-assisted transformations. Given a source state $|\psi\rangle$ and a target state $|\phi\rangle$, if there is a state $|c\rangle$ such that the transformation of $|\psi\rangle \otimes |c\rangle$ to $|\phi\rangle \otimes |c\rangle$ is possible by LOCC, then we say that $|\psi\rangle$ can be transformed to $|\phi\rangle$ by *entanglement-assisted (or catalytic)* transformation

(ELOCC). The state $|c\rangle$ is called a **catalysis** for the transformation, and for bipartite pure states, it is known that ELOCC is strictly more powerful than ordinary LOCC [66, 44]. If we are only concerned with a nonzero probability of conversion success, we can further study the stochastic versions of entanglement-assisted transformations (for short, SELOCC). For bipartite pure states, a transformation is realizable by SLOCC if and only if it is possible by SELOCC, as can be seen from the *multiplicative* behavior of the Schmidt rank: $Sch(\Psi \otimes \Phi) = Sch(\Psi)Sch(\Phi)$. Thus stochastic entanglement catalysis is impossible in bipartite systems.

By item (a) in Lemma (9), to demonstrate the effect of stochastic entanglement catalysis, we only need to find a state $|\phi\rangle$ with the following property: $rk(\phi) = n$ and there is some $k \geq 1$ such that $rk(\phi^{\otimes k}) \leq (n-1)^k$. The source state $|\psi\rangle$ can be chosen as an n-partite GHZ state with tensor rank $(n-1)$. While there may be many different states satisfying this property, we have seen that the state $|\Phi^3\rangle$ provides one particular example.

Theorem 5.9. *Consider the state $|\Phi^{(3)}\rangle = |\Phi_2\rangle_{AB} \otimes |\Phi_2\rangle_{BC} \otimes |\Phi_2\rangle_{CA}$, where $|\Phi_2\rangle = |00\rangle + |11\rangle$, and let $|\psi\rangle_{ABC}$ be any generalized GHZ-type state with tensor rank* 6*. Then the transformation of $|\psi\rangle$ to $|\Phi^{(3)}\rangle$ cannot be realized by SLOCC but can be realized by SELOCC.*

Proof. This follows directly from Lemma (9), but repeating in detail, first note that $rk(\Phi^{(3)}) = 7 > 6$ [111]. Hence, $|\psi\rangle$ cannot be SLOCC transformed into $|\Phi^{(3)}\rangle$. The best known algorithm for $d \times d$ matrix multiplication requires $O(d^{2.376})$ multiplication steps [30], and so the tensor rank of $|\Phi^{(3)}\rangle^{\otimes n}$ is $O(2^{2.376n})$. On the other hand, the tensor rank of $|\Psi\rangle^{\otimes n}$ is simply $6^n = 2^{(\log_2 6)n} \approx 2^{2.585n}$, which is larger than $O(2^{2.376n})$ for sufficiently large n. Thus we have confirmed the existence of n (perhaps very large) such that $rk(\Psi^{\otimes n}) \geq rk((\Phi^{(3)})^{\otimes n})$. □

In conclusion, we have found that no easy test exists for determining whether two general tripartite states are probabilistically convertible because any general solution involves a tripartite tensor rank computation. As a result, one must consider tripartite transformations on a case-by-case basis. In this section, specific tensor rank analysis has led to an improved GHZ state to W state SLOCC transformation rate as well as a demonstration of obtaining EPR pairs from GHZ states at a rate greater than one with a nonzero probability. We have also observed the weird phenomenon of SELOCC transformations which can be accomplished only on multipartite systems. An impossible transformation may become possible "free of charge" simply by introducing an additional entangled state.

The connection between tensor rank and entanglement transformation opens many avenues of further research as the techniques of algebraic complexity theory might teach us more about the nature and limitations of SLOCC transformations. Conversely, SLOCC entanglement transformations may provide a unique angle to investigate algebraic complexity theory. For example, can we improve the current best matrix multiplication algorithm by constructing an efficient SLOCC transformation protocol? Another specific problem is to prove strong impossibility results on the GHZ to EPR conversion problem within a hierarchy of SLOCC protocols (e.g. restricting the number of rounds of messages). Such results will shed light on the difficulty of matrix multiplication and may lead to a strong lower bound on ω.

5.4 The Tensor Rank of Symmetric States and $|W\rangle^{\otimes n}$

The results in this section have been obtained through joint collaboration [113, 22], with Chen providing a key insight on the problem (symmetric polynomials connection). Recall that an item left open in the previous section was proving the tensor rank of $|W\rangle^{\otimes 2}$ to be seven. This can be shown by appealing to the fact that $|W\rangle$ belongs to a family of states known as **symmetric states**.

Homogeneous polynomials and symmetric states. A symmetric multipartite state is one that is invariant under any permutation of the parties such as $|W\rangle$. For such a state $|\psi\rangle$, we can ask not only about its tensor rank, but also about its **symmetric tensor rank** $srk(\psi)$: the smallest number of symmetric product states $\{|\phi_i\rangle^{\otimes n}\}_{i=1,\dots,srk(\psi)}$ to provide an expansion $|\psi\rangle = \sum_{i=1}^{srk(\psi)} |\phi_i\rangle^{\otimes n}$. To estimate $srk(\psi)$, and thus upper bound $rk(\psi)$, we introduce a correspondence between symmetric states and homogeneous polynomials.

A homogeneous polynomial of order N in d variables $x_1, \dots, x_d$ is a linear combination of monomials $x^{\underline{j}} = x_1^{j_1} \cdots x_d^{j_d}$ (with a multi-index $\underline{j} = j_1 \dots j_d$), i.e. it has the form

$$h = h(x_1, \cdots, x_d) = \sum_{\underline{j}=j_1,\dots,j_n} a_{\underline{j}} \prod_{i=1}^{d} x_i^{j_i},$$

where the sum extends over all multi-indices with $\sum_{i=1}^{d} j_i = N$. Every homogeneous polynomial has a minimal symmetric decomposition $h = \sum_{i=1}^{pr(h)} (\beta_{1,i}x_1 + \ldots + \beta_{d,i}x_d)^N$, such that there is no other symmetric decomposition with a smaller number of powers than $pr(h)$. We refer to this number as the **polynomial rank** of h. The computation and estimation of polynomial rank is a much-studied problem in algebraic geometry [28, 70].

Homogeneous polynomials of order N are in 1-1-correspondence with N-partite symmetric pure states: introducing a computational basis $\{|x_1\rangle, \dots, |x_d\rangle\}$ for each d-dimensional local system $\mathbb{C}^d$, a monomial $x^{\underline{j}}$ is associated with the Dicke state defined as

$$|D(\underline{j})\rangle := \binom{N}{j_1 \dots j_d}^{1/2} P_{\text{sym}} \left(|x_1\rangle^{\otimes j_1} \otimes \cdots \otimes |x_d\rangle^{\otimes j_d} \right), \tag{5.14}$$

where P_{sym} is the projection onto the Bosonic (fully symmetric) subspace, $P_{\text{sym}} = \frac{1}{N!} \sum_{\pi \in S_N} U_\pi$, the sum extending over all permutation operators U_π of the N systems. General homogeneous polynomials (symmetric states) are associated by linear extension of the above since monomials (Dicke states) form a basis for the homogeneous polynomials (symmetric states). Thus we have proved the following.

Lemma 11. *Every symmetric state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$ is uniquely associated with a homogeneous polynomial $h(\psi)$ of order N in d variables, and vice versa each homogeneous polyno-*

mial h is associated with a symmetric state $|h\rangle$, such that $h(D(\underline{j})) = x^{\underline{j}}$ and $|x^{\underline{j}}\rangle = |D(\underline{j})\rangle$. Under this identification, symmetric tensor rank and polynomial rank are identical: $pr(h) = sr(h)$.

As an example, we examine two copies of the $|W\rangle$ state whose tensor rank is known to be seven [113]. Fully expanded, the unnormalized state reads $|W\rangle^{\otimes 2} = (|003\rangle + |030\rangle + |300\rangle) + (|012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle)$ which is a sum of two Dicke states having corresponding homogeneous polynomials $x_0x_0x_3$ and $x_0x_1x_2$ respectively. These have symmetric expansions $x_0x_0x_3 = \frac{1}{6}((x_0 + x_3)^3 + (x_0 - x_3)^3 - 2x_3^3)$ and $x_0x_1x_2 = \frac{1}{4!}((x_0 + x_1 + x_2)^3 - (-x_0 + x_1 + x_2)^3 - (x_0 - x_1 + x_2)^3 - (x_0 + x_1 - x_2)^3)$. Thus, by the replacement $x_i \to |i\rangle$, we see that $sr(W^{\otimes 2}) \geq rk(W^{\otimes 2}) \geq 7$.

For another example, consider three copies of $|W\rangle$. By Lemma (11), the homogeneous polynomial $h(W^{\otimes 3})$ can be written as $\frac{2}{9}(x_0x_1x_6 + x_0x_2x_5 + x_0x_3x_4 + x_1x_2x_4) + \frac{1}{9}x_0^2x_7$. To compute its polynomial rank, we perform the following linear transformations which do not change the polynomial rank: $y_1 = x_1 + x_2 - x_4, y_2 = x_1 - x_2 + x_4, y_4 = -x_1 + x_2 + x_4, z_3 = 1/2(x_3 + x_5), z_5 = 1/2(x_3 + x_6), z_6 = 1/2(x_5 + x_6)$. By using the fact that the polynomial rank is invariant under scalar multiplication, we can remove constant coefficients and obtain

$$\begin{aligned} pr(h(W^{\otimes 3})) &= pr\big(x_0y_1z_6 + x_0y_2z_5 + x_0y_4z_3 + x_0^2x_7 - y_1^3 - y_2^3 - y_4^3 + (y_1{+}y_2{+}y_4)^3\big) \\ &\leq pr(x_0y_1z_6 - y_1^3) + pr(x_0y_2z_5 - y_2^3) + pr(x_0y_4z_3 - y_4^3) + pr\big((y_1 + y_2 + y_4)^3 + x_0^2x_7\big) \\ &\leq 4 + 4 + 4 + 4 = 16. \end{aligned} \tag{5.15}$$

Here, the last inequality follows from the fact that $pr(x_0^2x_7) = 3$ and $pr(x_iy_jz_k) \leq 4$, as an explicit four term symmetric expansion for $x_iy_jz_k$ can be seen from the $|W\rangle^{\otimes 2}$ example above (actually the inequality is tight). Thus we have,

Theorem 5.10. (a) *$rk(W^{\otimes 3}) \leq 16$,*

(b) *$\lim_{n\to\infty} \sqrt[n]{rk(W^{\otimes n})} \leq \sqrt[3]{16} \approx 2.52$.*

This improves the previously best bound of $rk(W^{\otimes 3}) \leq 21$ [113]. In particular, Theorem 5.10 implies that two tripartite GHZ-type states with tensor rank 4 are sufficient to prepare three $|W\rangle$ states under SLOCC.

These are just upper bounds for the tensor rank of $|W\rangle^{\otimes 2}$ and $|W\rangle^{\otimes 3}$. We now prove a very general lower bound for not only multiple copies of $|W\rangle$, but also multiple copies of the N-party generalized W-state:

$$|W_N\rangle = \frac{1}{\sqrt{N}}(|100...0\rangle_{1...N} + |010...0\rangle_{1...N} + ... + |000...1\rangle_{1...N}).$$

Note that for $N = 2$, we recover the symmetric bipartite state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle$. In proving lower bounds we will use the following lemma.

Lemma 12. *Any state of the form*

$$|W_{N-1}\rangle^{\otimes n} + \sum_{k=1}^{n} \sum_{\pi \in S_N} c_{\pi k} U_\pi \left(|W_{N-1}\rangle^{\otimes k} |0_{N-1}\rangle^{\otimes (n-k)} \right) \tag{5.16}$$

is SLOCC equivalent to $|W_{N-1}\rangle^{\otimes n}$.

Proof. We will perform successive SLOCC transformations on (5.16), each transformation eliminating a term in the double sum. Consider term $U_\pi \left(|W_{N-1}\rangle^{\otimes k} |0_{N-1}\rangle^{\otimes (n-k)} \right)$, which can be thought of as n states shared between $N-1$ parties, and suppose that states $i_1, ..., i_{n-k}$ are $|0_{N-1}\rangle$. Then applying the transformation $|W_{N-1}\rangle^{\otimes (i_1,...,i_{n-k})} \rightarrow |W_{N-1}\rangle^{\otimes (i_1,...,i_{n-k})} - c_{\pi k} |0_{N-1}\rangle^{\otimes (i_1,...,i_{n-k})}$, $|0_{N-1}\rangle^{\otimes (i_1,...,i_{n-k})} \rightarrow |0_{N-1}\rangle^{\otimes (i_1,...,i_{n-k})}$ on (5.16) will eliminate the term $U_\pi \left(|W_{N-1}\rangle^{\otimes k} |0_{N-1}\rangle^{\otimes (n-k)} \right)$. The key observation is that this transformation is be achieved by local invertible operators. This procedure is repeated on all remaining terms in the sum until just $|W_{N-1}\rangle^{\otimes n}$ remains. □

To prove a lower bound, we proceed analogously as in [113]. Since $|W_N\rangle^{\otimes n} = (|0\rangle |W_{N-1}\rangle + |1\rangle |0_{N-1}\rangle)^{\otimes n}$, $rk(W_N^{\otimes n})$ is the minimum number of product states whose linear span contains the set $S = \{|W_{N-1}\rangle, |0_{N-1}\rangle\}^{\otimes n}$. Let Φ be the matrix whose rows are the 2^n elements of this set with row 2^n being $|W_{N-1}\rangle^{\otimes n}$. Then there exists some other matrix Θ having $rk(W_N^{\otimes n})$ rows of product states $|\theta_i\rangle$ such that $\Phi = T\Theta$. The first $2^n - 1$ rows of T will have an invertible $2^n - 1 \times 2^n - 1$ submatrix which means the linear span of S is contained by $2^n - 1$ elements from S and $rk(W_N^{\otimes N}) - (2^n - 1)$ product states $|\theta_i\rangle$. Hence, $|W_{N-1}\rangle^{\otimes n} + \sum_{i=1}^{2^n-1} c_i|s_i\rangle = \sum_{i=1}^{rk(W_N^{\otimes N})-2^n-1} d_i|\theta_i\rangle$ where the $|s_i\rangle$ are elements from S. By the previous lemma, then $rk(W_{N-1}^{\otimes n}) \leq rk(W_N^{\otimes n}) - (2^n - 1)$.

When $N = 3$, we obtain the bound $2^n \leq rk(W_3^{\otimes n}) - (2^n - 1)$ since $(|01\rangle + |10\rangle)^{\otimes n}$ has a tensor (Schmidt) rank of 2^n. Thus we obtain $2^{n+1} - 1 \leq rk(W_3^{\otimes n})$ which recovers the result in [113]. Performing a simple inductive argument on N then provides part (a) in the following theorem. Parts (b) and (c) are a consequence of the upper bounds derived above for $|W\rangle^{\otimes 2}$ and $|W\rangle^{\otimes 3}$.

Theorem 5.11. (a) $rk(W_N^{\otimes n}) \geq (N-1)2^n - N + 2$,

(b) $rk(W^{\otimes 2}) = 7$,

(c) $rk(W^{\otimes 3} = 15$ *or* 16.

This, then, proves the remaining piece of Lemma 9.

While the previous discussion has focused on W-class states, we can use Lemma 11 to prove some relationships between between the tensor and symmetric tensor ranks of general symmetric states.

Theorem 5.12. (a) *For multiqubit Dicke states* $|D(m,n)\rangle := P_{sym}(|0^{\otimes m}, 1^{\otimes n}\rangle)$ *with* $m \geq n$, $rk(D(m,n)) = sr(D(m,n)) = m+1$,

(b) *for any N-partite symmetric state* $|\psi\rangle$, $rk(\psi) \leq sr(\psi) \leq 2^{N-1} rk(\psi)$,

(c) $\lim_{n\to\infty} \sqrt[n]{sr(\psi^{\otimes n})} = \lim_{n\to\infty} \sqrt[n]{rk(\psi^{\otimes n})}$.

Proof. (a) The second equality follows from Corollary 4.5 of [70] which states that $pr(x^a y^b) = \max\{a,b\}$ for $a, b > 0$. As $\text{rk}(D(m,n)) \leq \text{srk}(D(m,n))$, to prove the first equality, it suffices to show that the lower bound of $\text{rk}(D(m,n))$ equals $m+1$ too.

We use induction on n. For $n = 1$, the claim is true [39], and we assume it holds for $n-1$. Ignoring normalization, we can rewrite the state $|D(m,n)\rangle$ as

$$\begin{aligned}|D(m,n)\rangle = &|D(m,n-2)\rangle|11\rangle \\ &+|D(m-1,n-1)\rangle(|01\rangle+|10\rangle) \\ &+|D(m-2,n)\rangle|00\rangle. \end{aligned} \tag{5.17}$$

Now we perform the global operation $|1\rangle\langle 11| + \frac{1}{2}|0\rangle(\langle 01| + \langle 10|)$ on the last two systems which cannot increase the rank. The resulting $(m+n-1)$-partite state is just the Dicke state $|D(m,n-1)\rangle$ and so $rk(D(m,n)) \geq \mathrm{rk}(D(m,n-1)) = m+1$. (b) Suppose that $|\psi\rangle$ has an optimal product state expansion $\sum_{i=1}^{rk(\psi)} |A_i\rangle \otimes ... \otimes |N_i\rangle$. As $|\psi\rangle$ is symmetric, we have $|\psi\rangle = \sum_{i=1}^{rk(\psi)} P_{sym}\left(|A_i\rangle \otimes ... \otimes |N_i\rangle\right)$. But this is just a sum of $rk(\psi)$ Dicke states, each one corresponding to the monomial $x_{A_i}....x_{N_i}$. From proposition 11.6 in [70], we have $pr(x_{A_i}....x_{N_i}) \leq 2^{N-1}$ which proves the claim. Part (c) follows directly from (b). □

In closing, we note that the previous lemma only succeeds in proving the tensor and symmetric ranks to be equal in the asymptotic setting. It is an open conjecture that for any symmetric state $|\psi\rangle$, $rk(\psi) = srk(\psi)$ [28]. Indeed for $|W_N\rangle$ and $|W_N\rangle^{\otimes 2}$ this statement is true. It also holds for any GHZ-type state.

CHAPTER VI

Conclusion

A primary goal of this project has been to rigorously justify the sentiment that multiparty entanglement is more complicated than its bipartite counterpart. To achieve this, we have compared the two on the question of transformability from one form to another. Our results are summarized in the following chart.

Operation Type	$\|\psi\rangle_{AB}$ $\downarrow$ $\|\phi\rangle_{AB}$	$\|\psi\rangle_{1\ldots N}$ $\downarrow$ $\|\phi\rangle_{AB}$	$\|0\rangle_A\|\psi_1\rangle_{BC}+\|1\rangle_A\|\psi_2\rangle_{BC}$ $\downarrow$ $\|0\rangle_A\|\phi_1\rangle_{BC}+\|1\rangle_A\|\phi_2\rangle_{BC}$	$\|\psi\rangle_{ABC}$ $\downarrow$ $\|\phi\rangle_{ABC}$
SLOCC with Probability $> p \in \mathbb{Q}$	P	NP-Hard (for 1-shot, 1-way cc)	?	NP-Hard
SLOCC	P	BPP	P for $\min\{d_B, d_c\} \leq 3$	NP-Hard
Invertible SLOCC	P	N/A	P	?

Table 6.1: Computational Complexity of Various Entanglement Transformations

Everything to the right of the $|\psi\rangle_{AB} \rightarrow |\phi\rangle_{AB}$ column are new results contained in this thesis and some also reported in [24, 25, 26]. We indeed see that the complexity in entanglement moves from P to NP-Hard as a third party is added. However, as emphasized in the Introduction, these classifications are based on worst-case computations, or in other words, they reflect the most complicated aspects of tripartite entanglement. For all practical and important entanglement manipulations, the physics may not be that complicated at all. In analogy, while the three-body celestial problem may have no tractable solution, we are still able to send satellites into orbit and predict stellar trajectories with sufficient precision.

An obvious future project is to try and resolve the question marks on this chart. Probably the most worthwhile question remaining is whether there exists a polynomial-time algorithm for deciding general tripartite equivalence. Related to this would be the characterization of all the infinite equivalence classes for each tripartite dimension. If it is correct to interpret entanglement as some resource that can be exchanged in one form to another through state transformations, then the question of reversible SLOCC convertibility becomes highly important. Also note that deterministic LOCC transformations are not included on the chart. Beyond bipartite pure states, very little is known about general deterministic transformations, and it is not clear which tools are best for tackling this problem. Might there be an efficient algorithm for deciding tripartite deterministic transformations while the SLOCC question is NP-Hard?

One feature not captured by Table 6.1 is the manner in which these results were obtained. Their proofs rely on encoding some computational problem of known complexity into a particular entanglement transformation. Via this maneuver, one obtains a physical interpretation of computational complexity in the following sense. Let $\mathcal{D}$ be any decision problem belonging to NP. For some instance x, when questioning whether x is a "yes" instance, what's being asked is whether the physical laws of this universe allow for a certain process to occur. More concretely, as any problem in NP can be phrased as a tensor rank calculation, let $|x\rangle$ be the corresponding tensor encoding for instance x. Then whether $x \in L_{\mathcal{D}}$ depends entirely on whether quantum mechanics allows for a GHZ-type state to be converted to $|x\rangle$ by LOCC. It is quite remarkable that highly abstract computational questions are intimately linked to the physical laws of nature in this way. This example shows the deep connection between complexity theory and theoretical physics in general and demonstrates the value to be gained by recognizing complexity issues in quantum information science.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett.*, 85(7):1560–1563, 2000.

[2] A. Acín, E. Jané, W. Dür, and G. Vidal. Optimal distillation of a greenberger-horne-zeilinger state. *Phys. Rev. Lett.*, 85(22):4811–4814, 2000.

[3] Manindra Agrawal and Somenath Biswas. Primality and identity testing via chinese remaindering. *J. ACM*, 50(4):429–443, 2003.

[4] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of Mathematics*, 160(2):781, 2004.

[5] Sergio Albeverio, Shao-Ming Fei, Preeti Parashar, and Wen-Li Yang. Nonlocal properties and local invariants for bipartite systems. *Phys. Rev. A*, 68(1):010303, 2003.

[6] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* Cambridge University Press, 2009.

[7] H. Barnum and N. Linden. Monotones and invariants for multi-particle quantum states. *Journal of Physics A: Mathematical and Theoretical*, 34:6787, 2001.

[8] Th. Beelen and P. Van Dooren. An improved algorithm for the computation of Kronecker's canonical form of a singular pencil. *Linear Algebra Appl.*, 105:9–65, 1988.

[9] Charles Bennett, Herbert Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4):2046, 1996.

[10] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[11] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[12] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59(2):1070–1091, 1999.

[13] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure state entanglement. *Phys. Rev. A*, 63:012307, 1999.

[14] Markus Bläser. Beyond the alder-strassen bound. *Theor. Comput. Sci.*, 331(1):3–21, 2005.

[15] Manuel Blum and Sampath Kannan. Designing programs that check their work. *J. ACM*, 42(1):269–291, 1995.

[16] James Ward Brown and Ruel V. Churchill. *Complex Variable and Applications.* McGraw Hill, New York, 2004.

[17] Jean-Luc Brylinski.

[18] P. Burgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory.* Springer-Verlag, 1997.

[19] A. Chefles. Deterministic quantum state transformations. *Phys. Lett. A*, 270:14, 2000.

[20] Anthony Chefles and Stephen M Barnett. Quantum state separation, unambiguous discrimination and exact cloning. *Journal of Physics A: Mathematical and General*, 31(50):10097, 1998.

[21] Lin Chen, Yi-Xin Chen, and Yu-Xue Mei. Classification of multipartite entanglement containing infinitely many kinds of states. *Phys. Rev. A*, 74(5):052331, 2006.

[22] Lin Chen, Eric Chitambar, Runyao Duan, Zhengfeng Ji, and Andreas Winter. Tensor rank and stochastic entanglement catalysis for multipartite pure states. arXiv:1003.3059v2, 2010.

[23] Eric Chitambar and Runyao Duan. Nonlocal entanglement transformations achievable by separable operations. *Phys. Rev. Lett.*, 103:110502, 2009.

[24] Eric Chitambar, Runyao Duan, and Yaoyun Shi. Tripartite entanglement transformations and tensor rank. *Phys. Rev. Lett.*, 101(14):140502, 2008.

[25] Eric Chitambar, Runyao Duan, and Yaoyun Shi. Tripartite to bipartite entanglement transformations and polynomial identity testing. arXiv:0908.0440v1, 2009.

[26] Eric Chitambar, Carl A. Miller, and Yaoyun Shi. Matrix pencils and entanglement classification. arXiv:0911.1803, 2009.

[27] A. Cobham. The intrinsic computational difficulty of functions. In *Proceedings of the International Congress for Logic, Methodology, and Philosophy of Science*, pages 24–30. North Holland, 1964.

[28] P. Comon, G. Golub, L.H. Lim, and B. Mourrain. Symmetric tensors and symmetric tensor rank. arXiv:0802.1681v2, 2008.

[29] Stephen A. Cook. The complexity of theorem-proving procedures. In *STOC '71: Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, New York, NY, USA, 1971.

[30] Don Coppersmith and Shmuel Winograd. Matrix multiplication via arithmetic progressions. *J. Symb. Comput.*, 9(3):251–280, 1990.

[31] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Second Edition.* The MIT Press, September 2001.

[32] Marcio F. Cornelio and A. F. R. de Toledo Piza. Classification of tripartite entanglement with one qubit. *Phys. Rev. A*, 73(3):032314, 2006.

[33] Toby Cubitt, Ashley Montanaro, and Andreas Winter. On the dimension of subspaces with bounded schmidt rank. *J. Math. Phys.*, 49(2):022107, 2008.

[34] Wei Cui, Wolfram Helwig, and Hoi-Kwong Lo. Bounds on probability of transformations between multipartite pure states. *Phys. Rev. A*, 81(1):012111, 2010.

[35] G. Mauro DAriano and Massimiliano F. Sacchi. Protocols for entanglement transformations of bipartite pure states. *Phys. Rev. A*, 67(4):042312, 2003.

[36] R. DeMillo and R. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7:193–195, 1978.

[37] D. Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A*, 126(5):303, 1988.

[38] Runyao Duan, Yuan Feng, Yu Xin, and Mingsheng Ying. Distinguishability of quantum states by separable operations. *IEEE Trans. Inf. Theory*, 55:1320, 2009.

[39] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, 2000.

[40] J. Edmonds. Systems of distinct representatives and linear algebra. *J. Res. Nat. Bur. Standards*, 71B:241–245, 1967.

[41] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[42] Jens Eisert and Hans J. Briegel. Schmidt measure as a tool for quantifying multiparticle entanglement. *Phys. Rev. A*, 64(2):022306, Jul 2001.

[43] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. arXiv:quant-ph/0001106v1, 2000.

[44] Y. Feng, R. Duan, and M. Ying. Catalyst-assisted probabilistic entanglement transformation. *Information Theory, IEEE Transactions on*, 51(3):1090 –1101, 2005.

[45] Yuan Feng, Runyao Duan, and Zhengfeng Ji. Condition and capability of quantum state separation. *Phys. Rev. A*, 72:012313, 2005.

[46] H. Flanders. On spaces of linear transformations with bounded rank. *J. Lon. Math. Soc.*, 37:10, 1962.

[47] Ben Fortescue and Hoi-Kwong Lo. Random bipartite entanglement from w and w-like states. *Phys. Rev. Lett.*, 98:260501, 2007.

[48] F.R. Gantmacher. *The Theory of Matrices, Vol. 1 and 2.* Chelsea Publishing Company, 1959.

[49] Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness.* W. H. Freeman & Co., 1990.

[50] Alexei Gilchrist, Nathan K. Langford, and Michael A. Nielsen. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A*, 71(6):062310, 2005.

[51] I. Gohberg, P. Lancaster, and L. Rodman. *Matrix Polynomials.* SIAM, New York, 2009.

[52] Gene H. Golub and Charles F. Van Loan. *Matrix computations.* Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996.

[53] Gilad Gour, David A. Meyer, and Barry C. Sanders. Deterministic entanglement of assistance and monogamy constraints. *Phys. Rev. A*, 72(1):042329, 2005.

[54] Gilad Gour and Robert W. Spekkens. Entanglement of assistance is not a bipartite measure nor a tripartite monotone. *Phys. Rev. A*, 73(6):062331, 2006.

[55] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, 1997.

[56] Leonid Gurvits. Classical deterministic complexity of edmonds' problem and quantum entanglement. In *STOC '03: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing.* ACM, 2003.

[57] Johan Håstad. Tensor rank is np-complete. *J. Algorithms*, 11(4):644–654, 1990.

[58] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69(6):062311, Jun 2004.

[59] Christopher Hillar and Lek-Heng Lim. Most tensor problems are np hard. arXiv:0911.1393v1, 2009.

[60] Ryszard Horodecki, PawełHorodecki, MichałHorodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865, 2009.

[61] Lane P. Hughston, Richard Jozsa, and William K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A*, 183(1):14–18, 1993.

[62] I. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123(6):257, 1987.

[63] Joseph Ja' Ja'. Optimal evaluation of pairs of bilinear forms. In *STOC '78: Proceedings of the tenth annual ACM symposium on Theory of computing*, pages 173–183, New York, NY, USA, 1978. ACM.

[64] G. Jaeger and A. Shimony. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A*, 197(2):83, 1995.

[65] Zhengfeng Ji, Yuan Feng, and Mingsheng Ying. Local cloning of two product states. *Phys. Rev. A*, 72(3):032324, 2005.

[66] Daniel Jonathan and Martin B. Plenio. Entanglement-assisted local manipulation of pure quantum states. *Phys. Rev. Lett.*, 83(17):3566–3569, 1999.

[67] Daniel Jonathan and Martin B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Phys. Rev. Lett.*, 83(7):1455–1458, Aug 1999.

[68] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[69] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* American Mathematical Society, 2002.

[70] J.M. Landsberg and Z. Teitler. On the ranks and border ranks of symmetric tensors. arXiv:0901.0487v3, 2009.

[71] T. Laustsen, F. Verstraete, and S. J. van Enk. Geometry and the complexity of matrix multiplication. *Quantum Information and Computation*, 3:64, 2003.

[72] Yeong-Cherng Liang, Llus Masanes, and Andrew C. Doherty. Convertibility between two-qubit states using stochastic local quantum operations assisted by classical communication. *Phys. Rev. A*, 77(1):012332, 2008.

[73] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland.

[74] Hong Liu and Kenneth W. Regan. Improved construction for universality of determinant and permanent. *Inf. Process. Lett*, 100(6):233, 2006.

[75] Hoi-Kwong Lo and Sandu Popescu. Concentrating entanglement by local actions: Beyond mean values. *Phys. Rev. A*, 63(2):022301, Jan 2001.

[76] Lászlá Lovász. Singular spaces of matrices and their application in combinatorics. *Bol. Soc. Braz. Mat.*, 20(1):87–99, 1989.

[77] Akimasa Miyake. Classification of multipartite entangled states by multidimensional determinants. *Phys. Rev. A*, 67(1):012108, 2003.

[78] Akimasa Miyake and Frank Verstraete. Multipartite entanglement in 2x2xn quantum systems. *Phys. Rev. A*, 69(1):012101, 2004.

[79] R. Motwani and P. Raghavan. *Randomized Algorithms.* Cambridge University Press, 1995.

[80] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2):436–439, Jul 1999.

[81] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[82] Román Orús. Universal geometric entanglement close to quantum phase transitions. *Phys. Rev. Lett.*, 100(13):130502, Apr 2008.

[83] Roger Penrose. *The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics.* Oxford University Press, Inc., 1989.

[84] Allon Percus, Gabriel Istrate, and Christopher Moore, editors. *Computational Complexity and Statistical Physics.* Oxford University Press, 2006.

[85] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128(1):19, 1988.

[86] Dmitri D. Pervouchine. Hierarchy of closures of matrix pencils. *Journal of Lie Theory*, 14:443, 2004.

[87] Martin B. Plenio and S. Virmani. An introduction to entanglement measures. *Quant. Inf. Comp.*, 7:1, 2007.

[88] H. Radjavi. Simultaneous unitary invariants for sets of matrices. *Canad. J. Math.*, 20:1012–1019, 1968.

[89] Norbert Schuch and Frank Verstraete. Computational complexity of interacting electrons and fundamental limitations of density functional theory. *Nature Physics*, 5:732, 2009.

[90] Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54(4):2614–2628, Oct 1996.

[91] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[92] A. Shimony. Degree of entanglement. *Ann. NY. Acad. Sci.*, 755:675, 1995.

[93] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logaritms on a quantum computer. *SIAM J. Comput.*, 26(5):1484, 1997.

[94] Cong-Feng Qiao Shuo Cheng, Junli Li. Classification of the entangled states of $2 \otimes n \otimes n$. arXiv:0804.2291, 2009.

[95] Michael Sipser. *Introduction to the Theory of Computation.* PWS Publishing Co., 1997.

[96] John A. Smolin, Frank Verstraete, and Andreas Winter. Entanglement of assistance and multipartite state distillation. *Phys. Rev. A*, 72(1):052317, 2005.

[97] Federico M. Spedalieri. Local deterministic transformations of three-qubit pure states, 2001. arXiv:quant-ph/0110179.

[98] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(3):354–356, 1969.

[99] Bao-Zhi Sun, Shao-Ming Fei, Xianqing Li-Jost, and Zhi-Xi Wang. A note on equivalence of bipartite states under local unitary transformations. *Journal of Physics A: Mathematical and General*, 39(1):L43, 2006.

[100] S. Turgut, Y. Gül, and N. K. Pak. Deterministic transformations of multipartite entangled states with tensor rank 2. *Phys. Rev. A*, 81(1):012317, 2010.

[101] A. Uhlmann. The transition probability in the state space of a *-algebra. *Reports on Mathematical Physics*, 9:273, 1976.

[102] L. G. Valiant. Completeness classes in algebra. In *STOC '79: Proceedings of the eleventh annual ACM symposium on Theory of computing*, 1979.

[103] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38:49–95, 1994.

[104] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78(12):2275, Aug 1997.

[105] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65(5):052112, Apr 2002.

[106] Guifré Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83(5):1046–1049, Aug 1999.

[107] Guifre Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355, 2000.

[108] John von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton University Press, 1996.

[109] John Watrous. Quantum computational complexity. arXiv:0804.3401v1, 2008.

[110] Tzu-Chieh Wei and Paul M. Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Phys. Rev. A*, 68(4):042307, Oct 2003.

[111] S. Winograd. On multiplication of 2x2 matrices. *Linear Algebra and Its Applications*, 4:381–388, 1971.

[112] Dong Yang and Jens Eisert. Entanglement combing. *Phys. Rev. Lett.*, 103:220501, 2009.

[113] N. Yu, E. Chitambar, C. Guo, and R. Duan. Bounding the tensor rank of $|w\rangle^{\otimes n}$. *Phys. Rev. A*, 81:014301, 2009.

[114] R. Zippel. Probabilistic algorithms for sparse polynomials. *Ph.D. thesis, MIT*, 1979.