ENTANGLEMENT TRANSFORMATIONS AND QUANTUM ERROR CORRECTION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

YUSUF GÜL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF PHILOSOPHY OF DOCTORATE
IN
PHYSICS

JULY 2009

Approval of the thesis:

ENTANGLEMENT TRANSFORMATIONS AND QUANTUM ERROR CORRECTION

submitted by **YUSUF GÜL** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Physics Department, Middle East Technical University** by,

Prof. Dr. Canan ÖZGEN _____
Dean, Gradute School of **Natural and Applied Sciences**

Prof. Dr. Sinan BİLİKMEN _____
Head of Department, **Physics**

Prof. Dr. Namık Kemal PAK _____
Supervisor, **Physics Department, METU**

Examining Committee Members:

Prof. Dr.Müge BOZ
Engineering Physics, Hacettepe University _____

Prof.Dr. Namık Kemal PAK
Physics, Middle East Technical University _____

Prof. Dr. Ferruh ÖZBUDAK
Mathematics, Middle East Technical University _____

Assoc. Prof. Yusuf İPEKOĞLU
Physics, Middle East Technical University _____

Assoc. Prof. Dr. Sadi TURGUT
Physics, Middle East Technical University _____

Date: July 7, 2009

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: YUSUF GÜL

Signature :

ABSTRACT

ENTANGLEMENT TRANSFORMATIONS AND QUANTUM ERROR CORRECTION

Gül, Yusuf

Ph.D., Department of Physics

Supervisor : Prof. Dr. Namık Kemal Pak

July 2009, 77 pages

The main subject of this thesis is the investigation of the transformations of pure multipartite entangled states having Schmidt rank 2 by using only local operations assisted with classical communications (LOCC). A new parameterization is used for describing the entangled state of p particles distributed to p distant, spatially separated persons. Product, bipartite and truly multipartite states are identified in this new parametrization. Moreover, alternative parameterizations of local operations carried out by each party are provided. For the case of a deterministic transformation to a truly multipartite final state, one can find an analytic expression that determines whether such a transformation is possible. In this case, a chain of measurements by each party for carrying out the transformation is found. It can also be seen that, under deterministic LOCC transformations, there are some quantities that remain invariant. For the purpose of applying the results of this thesis in the context of the quantum information and computation, brief reviews of the entanglement purification, measurement based quantum computation and quantum codes are given.

Keywords: Quantum information theory, quantum computation, entanglement.

ÖZ

DOLANIKLIK DÖNÜŞÜMLER VE KUANTUM HATA DÜZELTME

Gül, Yusuf
Doktora, Fizik Bölümü
Tez Yöneticisi : Prof. Dr. Namık Kemal Pak

Temmuz 2008, 77 sayfa

Bu tezin konusu rankı iki olan çok partili saf dolanık durumların dönüşümlerinin klasik iletişimle desteklenen yerel ölçümler kullanılarak sorgulanmasıdır. Uzaysal olarak ayrık, birbirinden uzak p kişiye p parçası dağıtılarak elde edilen dolanıklık durumlarını belirten yeni bir parametrizasyon geliştirildi. Bu yeni parametrizazyon da çarpımlı, ikili ve tamamen parçalı durumlar tanımlandı. Ayrıca her bir parti tarafından yapılan lokal operasyonların parametrizasyonu geliştirildi. Tamamen parçalı son durumlara belirlenebilir dönüşümler yapılırken böyle bir dönüşümün mümkün olup olmadığını belirten analitik ifade bulunabileceği gösterildi. Bu durumda, dönüşümü yapmak için her parti tarafından yapılan bir ölçümler zinciri bulundu. Yine görülüyor ki, belirlenebilir dönüşümler altında bazı değerler değişmez olarak kalıyor. Bu tezin sonuçlarını kuvantum bilgi ve hesaplama alanında uygulamak amacıyla, dolanıklık saflaştırması, ölçüm temelli kuvantum hesaplama ve kuvantum kodları gözden geçirildi.

Anahtar Kelimeler: Kuantum bilgi kuramı, kuantum hesaplama, dolanıklık.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my mentors Dr. N. K. PAK, Dr. S. TURGUT, and Dr. F. ÖZBUDAK for their guidance on the way of thinking, on doing research, and for their unending incentive patience.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The classical theory of computing is based on the Church-Turing principle. In Turing's terms, this principle can be expressed as,

"Every function which would naturally be regarded as computable can be computed by the universal Turing machine".

In this statement the model of computation is classical and any stage of computation is described by numbers. These numbers are used in specification of the state of the computation which is measurable in physical sense.

As the computers get smaller and smaller with the advent of technology, one encounters with new challenges of these scales, namely the new laws and rules of the quantum mechanics. But, in the quantum model as well as the classical one, Turing machine cannot be described by Church- Turing principle since the statement "Every function which would naturally be regarded as computable" need a concrete definition for being natural and computable. For any function to be computable, this statement should be modified in accordance with the physical nature of the quantum mechanics which describes the state of the computation with its own rules which are different from the classical computation model.

The construction of the classical reversible machine [4,5] equivalent to Turing machine made the Quantum mechanics important for computational tasks. Benioff [1] constructed the reversible Turing machines based on the unitary evolution of quantum system. But this was a quantum machine, not a quantum computer. Feynman [2], in his seminal paper, introduced universal quantum simulator which consists of a lattice of spin system with nearest-neighbour interactions. This quantum simulator has

great advantage over classical ones in speeding up the computations using quantum parallelism in quantum Turing machine. In quantum parallelism, one can use several computational bases at the same time and this makes quantum computers much more powerful than the classical ones. Later, Deutsch [3] expressed the computational task as the programs which are the symbolic representations of some laws of the physics. In this framework, instead of Turing-Thesis describing any function as naturally computable, he treats computational task as the simulation of one physical process by another. This physical approach to the computing and the challenge of manufacturing the universal quantum computing machines placed Quantum mechanics at the center of the studies in the new computation and information [6-9].

Entanglement, quantum correlations and interferences [14-22], which have no classical counterparts, lead us to new directions in the realm of computing machines. Entanglement is observed in composite systems; the basis of the Hilbert space of this composite system is described by tensor product of the basis of the Hilbert spaces of individual subsystems. The general state of the composite system is described as the superposition of the bases of individual systems. A composite system is called entangled or non-separable state if one cannot write it in the tensor product of the basis of the Hilbert spaces of subsystems. On the contrary, non-entangled states are separable. The non-classical properties of entangled states are shown by Einstein-Podolsky and Rosen. Thought in the context of the principles of special theory of relativity, these authors concluded that quantum mechanics is incomplete on the basis of the reality and locality assumptions. That is, if one can predict the value of a physical quantity with certainty, then this value has physical **reality** and, nothing is faster than the speed of light in the transmission of the results of the **local** operations acting in the state space of the individual subsystems. Contrary to Einstein's local realism, standard quantum mechanics accept the wavefunction as mathematical tool, not as a physical reality. The non-local property of quantum mechanics comes from the predictions of the correlations and there is no influence of the measurement performed on the one system over the others. If there is no a priori assigned values of the composite system shared by many parties, then one cannot predict the values of the results of the measurements of the others. Assuming the EPR argument is true, Bell obtained inequalities which shows that the predictions of quantum mechanics con-

tradicts possibility of the existence of Einstein's local realism. Quantum mechanics introduce the correlations obtained from the result of the measurements of the entangled states. These correlations between distant parties make quantum information non-local and help us overcome some limitations of classical information [10-13]. As in the Young's double slit experiment, probabilistic nature of quantum mechanics lead us to use destructive and constructive interferences in entangled states. Together with the correlations, interferences is used in implementing the quantum algorithms.

Following the EPR argument, Entanglement transformations play an important role in understanding the nature of entanglement. Combining with the Local Operations and Classical Communication protocols (LOCC), they help us understand the physical nature of the theory of quantum information and computation. One particular form of entanglement transformations is called entanglement distillation. These are studied widely in quantum information theory to obtain Einstein-Podolsky-Rosen (EPR) pairs from an ensemble of entangled states [27-30]. Deterministic entanglement transformations are described as the transformations such that the conversion probability between entangled states is unity. When the entanglement transformations are not succeeded with unity, i.e, conversion probability between entangled states is not unity, they are called probabilistic transformations. In the deterministic transformations for bipartite states, two parties , say Alice and Bob spatially separated from each other, can convert one entangled state into the other with certainty by Local Operations and Classical Communications (LOCC), where each party is only allowed to act on his own subsystem locally . The conditions for deterministic entanglement transformations for pure bipartite entangled states are obtained using the linear algebraic majorization theory [41].

With the exception of the bipartite entangled states, multipartite states are not entangled in a straight manner. Classifications and characterizations of them are required to be employed for quantum informational tasks. Due to the subtle properties of multipartite entangled states, the challenge with the multipartite entanglement transformations concentrated on the quantification of entanglement [31-38] and possible conversion protocols between them [39-44]. As a most commonly studied multipar-

tite entangled states in quantum information and computation, Greenberger-Horne-Zeilinger (GHZ) states and W-states are three particle entangled states and all entangled states are obtained from these states. But one cannot obtain these two states from each other. Reducibilities, equivalences, and partial entropies of a pair of multipartite pure states and exact reducibilities between GHZ and EPR states are given in [45]. Allowing each party to make a local operation and to communicate classically with the rest of the parties leads a splitting of the subsequent processes into several branches. Each branch corresponds to the entangled states. Along the particular branches, transformations between entangles states are succeeded with some probability. In each round of these processes, success probabilities of converting entangled states depends on the previous local operations. In this manner stochastic LOCC is studied in [46]. Performing LOCC individual positive operator-valued measurements is applied in subsystem of each parties and optimal distillation of (GHZ) state from an arbitrary pure state is obtained by one successful branch protocols [47].

The employment of entangled states and their conversion makes new directions in quantum informational tasks, namely transmission of quantum information by using entanglement as a resource. In the transmission of quantum information through a communication channel, quantum data compression [27] and quantum teleportation [28] play a central role. In quantum data compression, transmission of a quantum information through channel is carried out by quantum states and quantified by the fidelity which measures resemblance of input quantum states to the output quantum states . In quantum teleportation, entanglement shared by the sender and receiver via a noisy channel is used as the source for information transmission. Both techniques suffer from noise as well as imperfect operations in communication channels and computation processes. In quantum informational tasks, entanglement purification combined with quantum teleportation appears as a good candidate to generate entangled states with perfect entanglement. In quantum teleportation, entangled states shared by distant parties (say Alice and Bob) behave as a communication channel. When we send maximally entangled qubits over noisy channel, it is not easy to obtain maximally entangled qubits at the output. For these non-maximally entangled qubits one finds non-unit fidelity. Entanglement purification [28,30,48] helps us to increase the

fidelity of some of these qubits at the expense of decreasing the number of maximally entangled qubits by concentrating or distilling the entanglement of the total ensemble into much less number of copies at the output. Experiments [49-54] with photons and atoms, and entanglement swapping [55-59] gives new insights in entanglement based quantum communication and computational applications. Entanglement purification is mostly used in quantum repeater [58-67] for long distance communication and quantum computation in which gates are teleportation-based [68-71]. In the multipartite case, entanglement purification protocols are constructed by Graph states and stabilizers [72-74]. Since imperfections in measurement processes plays very important role in the one-way quantum computation model [75-77], entanglement purification becomes an efficient tool in fault-tolerant quantum computation [78].

As another employment of entanglement in quantum informational and computational tasks, one can use entanglement in encoding the information and reach efficient quantum codes using the physical nature of information and computation. In both encoding and error syndrome processes entanglement becomes crucial and in spite of the No-Cloning theorem [24-27] quantum error correction is constructed [79-84]. The complete processes of the encoding and decoding is described by the quantum restoration circuits [85,86]. Using the parallelism with the classical error correcting codes, quantum codes are obtained by the Calderbank-Shor-Steane (CSS) construction [82-84] and the stabilizer states [99-102] for binary case. The extension to non-binary case is done by orthogonal geometry [87-90,98,103] and algebraic geometry [91-97].

In encoding the information in a quantum system, one can use both entanglement and entanglement transformations as physical resource.

In the first case, logical qubits obtained by entanglement in quantum network model consist of the quantum gates. Due to the collapse of the wavefunction, a quantum measurement alters the quantum state by projecting it into one of the eigenstates and it is impossible to distinguish two non-orthogonal states transformed by two different error operators. Shor noticed the role of the entanglement in encoding and decoding stages of quantum information. In the encoding stage, as in the classical error cor-

rection, he used the physical qubits with a definite initial state in adding redundancy to the information qubits. Then, making these local auxiliary qubits entangled with the information qubits, he obtained the logical qubits. One can make a local auxiliary qubit entangled with its system qubit and the global state becomes an entangled state between the system and the auxiliary qubits. For example, in one qubit error correction case, the logical qubits are GHZ-states. In the decoding stage, measurement is used to detect the error syndrome on the particular qubit. To overcome the collapse of the wavefunction in the measurement processes, he used the ancillary qubits. These ancillary qubits are just local auxilary qubits with initial states as in the encoding stages. Making these ancillary qubits entangled with the logical qubits, he made measurements on the ancillary qubits instead of the information qubits. Then, in detecting the error syndrome, he used the correlations coming from the entanglement between these ancillary and logical qubits. This approach, in the terminology of Shor, is called "fight entanglement with entanglement", contains mainly two entanglement generation processes. That is, Entangling one qubit with (n-1) qubits, and entangling these n qubits with ancilla qubits and constructing error syndrome by correlations and without measurement. These items above are combined in Quantum restoration circuits containing both encoding and decoding stages. Parity of the n-qubit is given as the eigenvalue of the operator $\sigma_{z,1}, \sigma_{z,2}, , , , \sigma_{z,n}$ where $+1$ corresponds to even parity and -1 corresponds to odd parity in error syndrome detection. Together with LOCC, this makes restoration circuits capable of error correction on logical qubits. In this framework, the logical qubits appear as entangled multipartite entangled states and the complete process of transmission of logical qubits via restoration circuits can be treated as conversion of the entangled states into each other. In the same way, due to the error correction capability of these restoration circuits, the logical qubits are treated as quantum error correcting codes. This makes our treatment possible for two things, namely entanglement transformations, and the quantum codes.

In the second case, cluster qubits take the place of logical qubits of the first case. Connection between entanglement transformations and quantum codes is constructed by quantum simulation following Feynman universal quantum simulator. First, consider a d-dimensional lattice containing arrays of the interacting particles described

by Ising model. These states are called cluster states and both entangled and product states are obtained from cluster states using transformations by LOCC. For such an entanglement transformation Cluster of qubits and measurements satisfy maximal connectedness and persistency of entanglement. Namely, the set of n-qubits in a multipartite state is maximally connected if a pure Bell state is obtained by tracing out the other qubits. And, persistency of entanglement gives us the number of local measurements to make the entangled state completely disentangled. To obtain Bell state from these n-qubit state, LOCC on selective qubits is carried out and correlations are used for persistency of entanglement.One qubit measurements transforms the cluster states into product states, and this is used once. Because of the irreversible character of this scheme, it is called one-way quantum computer. Cluster states can be described easily by mathematical graph theory. Introducing the vertices of a graph as local quantum system, say qubits, and the edges as two particle interactions we can use graph theory in quantum mechanics. The Ising model interactions can be described in graph formalism and its eigenvalues lead us to the stabilizer formalism. When we use graphs in quantum algorithms, we obtain the quantum state as the stabilizer code.

This thesis mainly concentrated on the nature of the entanglement and its transformations following physical description of Feynman and Deutsch about the information and computation. In chapter II, we investigate the entanglement purification which is used to obtain entangled states from mixed states and its applications in quantum communication on long distances under noise effects and measurement based quantum computation. This chapter only contains the technical review that motivates us to study the topics in chapter three. In chapter III, we investigate rank two entanglement transformations for deterministic case. In the case of deterministic transformations of states by many parties, we considered the general LOCC transformation by successive measurements of all parties. Each step in the process consists of a local measurement by a party (say the kth) and the announcement of the measurement result to the other parties by classical communication. Two or more successive measurements by the same party can always be considered as a single measurement. For this reason, it can be assumed that two successive local operations are carried out by different parties.

After each local measurement, classical information is sent to the other parties. All of the parties may use this information for applying a local unitary to their particles in order to change their states to some standard state.

Apart from that, the classical communication is used for parties to choose their local measurements depending on the results of the previous measurements. For example, suppose that the first party has done the very first local measurement and obtained a particular result, say ℓ_1. Then, the party that will make the second measurement and the measurement itself will be chosen depending on the value of ℓ_1. Similarly, after the second measurement is done and the result ℓ_2 is obtained, the third party and her measurement will be chosen depending on the value of (ℓ_1, ℓ_2), etc. In this way, several measurements will be made until the time when it is stopped. Obviously, the number of measurement steps at the stopping point may also be dependent on the measurement results. It should also be obvious that any party may do several measurements until the last step is reached.

CHAPTER 2

ENTANGLEMENT TRANSFORMATIONS AND ERROR CORRECTION

2.1 Entanglement Transformations

A quantum state $|\Psi\rangle \in \mathcal{H}$ is separable if it can be factorized as [9-11]

$$|\Psi\rangle = \otimes_{i=1}^{n} |\psi_i\rangle, \quad |\psi_i\rangle \in \mathcal{H}_i \tag{2.1}$$

where

$$\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i. \tag{2.2}$$

If it cannot be factored as (2.1), it is called entangled.

When the system is composed of two subsystem A and B, one can write the state of this composite system as

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} C_{ij} |a_i\rangle_A |b_j\rangle_B \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{2.3}$$

where $\{|a_i\rangle_A\} \in \mathcal{H}_A$ and $\{|b_j\rangle_B\} \in \mathcal{H}_B$ are the orthonormal bases with dimension d_A and d_B respectively.

Using the biorthonormal decomposition, namely Schmidt decomposition, one can write the state $|\Psi\rangle_{AB}$ in terms of the orthonormal vectors $\{|u_k\rangle_A\} \in \mathcal{H}_A$ and $\{|v_k\rangle_B\} \in \mathcal{H}_B$. as

$$|\Psi\rangle_{AB} = \sum_{k}^{r} \sqrt{w_k} |u_k\rangle_A |v_k\rangle_B, \quad w_k > 0, \quad \sum_{k}^{r} w_k = 1 \tag{2.4}$$

The coefficients w_k are called Schmidt weights and $r < d = \min\{d_A, d_B\}$ is the Schmidt rank of the state $|\Psi\rangle_{AB}$.

In quantum computational and informational tasks, the most commonly used entangled states are EPR or Bell-states

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle] \tag{2.5}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle] \tag{2.6}$$

and GHZ-states

$$|GHZ\rangle = \frac{1}{\sqrt{2}}[|000\rangle \pm |111\rangle] \tag{2.7}$$

Now, let us consider the Bell state [10,12,13,104,105]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.8}$$

which is pure state with the corresponding density matrix $\rho = |\psi\rangle\langle\psi|$ belongs to $H = H_1 \otimes H_2$ Hilbert space of bipartite system of parties 1 and 2

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.9}$$

The partial trace of it becomes

$$\rho_1 = tr_2\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.10}$$

Since $\rho_1 \neq \rho_1^2$ it's a mixed state and this shows that a pure bipartite state ρ is transformed to a maximally mixed state ρ_1 belonging to the subsystem H_1.

Thinking about the previous transformation from pure to the mixed state, purification can be seen as to find a pure density matrix of the two subsystems whose partial trace over the second system gives the density matrix of the given system.

Different from the purification of a mixed state [40], entanglement purification protocols (EPP) are schemes which are used for the distillation of pure Bell states from the mixed states which occurs during the transmission of the pure entangled state through

noisy quantum channels [28,29.30,35,39]. Enhancing the classical Communication between two parties, these protocols are considered as one-way classical communication (1-EPP) and two-way classical communication (2-EPP) purification protocols in which each party is allowed to apply the local Unitary transformation in his/her own subsystem [30].

One-way classical communication (1-EPP) entanglement purification protocols play an important role in preparing maximally entangled states for Quantum Teleportation [23,29,30,35,39] to use as a quantum communication channel. Entanglement Concentration and it's inverse process entanglement dilution [29] are the protocols which are used to concentrate the entanglement in any pure bipartite state into maximally entangled states by Local Operations and Classical Communications (LOCC). For a given initial entangled state $|\psi_{AB}\rangle$, the final state $|\psi'_{AB}\rangle$ is prepared by LOCC and the entanglement is quantified by its entropy of entanglement [31-38]

$$E(|\psi_{AB}\rangle) = S(\rho_A) = S(\rho_B) \tag{2.11}$$

where

$$S(\rho) = -Tr\rho log_2\rho \tag{2.12}$$

is the von Neumann entropy.

Now, we assume n-partly entangled state is distributed among two parties each having the n-subsystem and they become sharing nE initial entanglement [29]. The initial entangled state is described by

$$|\Psi\rangle^{\otimes n} = (\alpha|0\rangle_{1i}|0\rangle_{2i} + \beta|1\rangle_{1i}|1\rangle_{2i})^{\bigotimes n}. \tag{2.13}$$

The coefficients of the superposition becomes using binomial terms $\alpha^{n-k}\beta^k$ and allowing each party to perform local unitaries and measurement on their own subsystems we see that the probability distribution of getting the output k is

$$p_k = C(n,k)(\alpha^2)^{n-k}(\beta^2)^k \tag{2.14}$$

binomial where

$$C(n,k) = \frac{n!}{k!(n-k)!}. \tag{2.15}$$

After performing the measurement two parties are left with maximally entangled state which has more entropy of entanglement than the initial state. Besides this entanglement entropy, the expected entropy is bounded by initial pure state entropy $E(\Psi)$ and $E(\Psi) - H$ where H is the Shannon entropy. In asymptotic case the fidelity and probability reaches unity.

Two-way classical communication $(2 - EPP)$ purification protocols can be used to distill the pure maximally entangled states and to classify the entanglement transformation between pure entangled states by using the majorization theory from linear algebra [41].

Theorem(Nielsen): A pure bipartite entangled state $|\psi\rangle$ is transformed to another pure bipartite state $|\phi\rangle$ by LOCC iff

$$\lambda_\psi \prec \lambda_\phi \tag{2.16}$$

where $\lambda_\psi = tr_A|\psi\rangle\langle\psi|$ and $\lambda_\phi = tr_A|\phi\rangle\langle\phi|$ are the eigenvalues of the reduced density matrices of the states.

Proof of this theorem directly leads following the facts about existence of some mathematical preliminaries

1.Existence of the equivalence between the one-way and two- way classical communication protocols

2. For some unitary operator U, any matrix A is written as $A = \sqrt{AA^\dagger}U$.

3. Vector of eigenvalues of $\rho^{'} = \sum p_i U_i \rho U_i$ is majorized by the vector eigenvalues of ρ.

4. $x \prec y$ implies the existence of the matrix D such that $x = Dy$

5. Repeated use of the Schmidt decomposition is allowed.

Consider the states

$$|\psi\rangle = \sqrt{0.6}|11\rangle + \sqrt{0.3}|22\rangle + \sqrt{0.1}|33\rangle \tag{2.17}$$

$$|\phi\rangle = \sqrt{0.15}|11\rangle + \sqrt{0.7}|22\rangle + \sqrt{0.15}|33\rangle \tag{2.18}$$

Taking the trace over first subsystem A $tr_A|\psi\rangle\langle\psi| = 0.6|1\rangle\langle 1| + 0.3|2\rangle\langle 2| + 0.1|3\rangle\langle 3|$ and $tr_A|\phi\rangle\langle\phi| = 0.15|1\rangle\langle 1| + 0.7|2\rangle\langle 2| + 0.15|3\rangle\langle 3|$ leads to the majorization relation in terms of the ordered list

$$\begin{pmatrix} 0.6 \\ 0.3 \\ 0.1 \end{pmatrix} \not\prec \begin{pmatrix} 0.15 \\ 0.70 \\ 0.15 \end{pmatrix}. \tag{2.19}$$

Since Nielsen's theorem is not satisfied we cannot do an entanglement transformation.

The motivation behind to the attempt to classify the three and more qubit entangled state in an equivalence classes [45,46,47] stem from the fact that all entangled pure states of two qubits are equivalent to the Einstein-Podolski-Rosen (EPR) state. For three qubit states, there exist equivalence between truly tripartite entangled pure states and the Greenberger-Horne-Zeilinger (GHZ) state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2.20}$$

or W-states.

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{2.21}$$

These two states are inacessible from each other by LOCC even for a small probability, whereas we can obtain EPR pair from both of the GHZ and W-states. Although there is an equivalence between pure bipartite states and EPR states in asymptotic case, for entanglement shared between three or more parties it is not easy to find such an equivalence in asymptotic case by LOCC. This makes us to use LOCC without

imposing certainty called Stochastic LOCC(SLOCC) [46,47].

In conversion protocol of the pure multipartite states we are interested branches instead of one-way and two-way protocols in pure multipartite states. Since each party use LOCC in his own subsystem one by one and communicate by the other parties classically, in conversion of multipartite entangled state the sequence of applications of local unitaries and measurements become dependent to the last parties results. This histories of applications will be described as branch which occurs with a finite probability among the others.

Under SLOCC we would convert a three qubit entangled state $|\psi\rangle$ into $|\phi\rangle$ with some probability by the local unitaries such that

$$|\phi\rangle = A \otimes B \otimes C|\psi\rangle \tag{2.22}$$

where in each round operators act its own subsystem sequentially appearing as a branch to complete the process. To reach a two way convertibility between three qubit states $|\psi\rangle$ and $|\phi\rangle$ reduced density matrices of each parties should have rank two density matrices which implies the existence of the inverse operators of A, B, C.

2.2 Entanglement Purification and Error Correction

Entanglement purification in the presence of errors appears as the production of less number of distilled finite block of EPR pairs which are much more entangled but less than the possible entangled states [30,110]. In quantum error correction redundancy is added to the information qubit and from a finite block of encoded n-qubits we obtain correction for k-qubits compared for which k is less than n. This parallelism make the derivation of Quantum Error Correction Codes (QECC) from 1− EPP. Equivalence of the 1− EPP to quantum error correction is given in for the Pauli-diagonal channel

$$N = \sum_{k=0}^{3} p_k \sigma_k \rho \sigma_k \tag{2.23}$$

and a mixed state

$$\hat{E} = I \otimes N(|\Phi\rangle\langle\Phi|) \tag{2.24}$$

obtained from the output of the channel through which a part of a maximally entangled state Φ is sent. Distillable entanglement in one way protocol and channel capacity are the same when there is equivalence between them.

When we use quantum repeater [59-66], the effects of errors on entanglement connection appears due to both imperfect local operations and measurements, for example, the local two-qubit unitary operator U_{ij} acting on state ρ is described as

$$U_{ij}\rho U_{ij}^{\dagger} \rightarrow (1-\beta)U_{ij}\rho U_{ij}^{\dagger} + \frac{\beta}{4}Tr_{ij}\rho \otimes I_{ij} \tag{2.25}$$

where β is the error probability, $Tr_{ij}\rho$ is the partial trace over the subsystem i and j and I_{ij} is the identity matrix. In terms of the measurement error probability δ the projective measurement operator is written as

$$P_o = (1-\delta)|0\rangle\langle 0| + \delta|1\rangle\langle 1| \tag{2.26}$$

for the state $|0\rangle$ and in terms of the the memory error probability $\mu = 1 - e^{-\gamma\tau_c} \approx \gamma\tau_c$

$$\rho \rightarrow (1-\mu)\rho + \frac{\mu}{2}Tr_i\rho \otimes I_i \tag{2.27}$$

$Tr_i\rho$ is the partial trace over the subsystem i and I_i is the identity matrix for subsystem i.

The encoding in quantum repeater [107] with repetition code is done by the CSS codes and using the logical qubit

$$|\tilde{0}\rangle = |000\rangle \quad and \quad |\tilde{1}\rangle = |111\rangle \tag{2.28}$$

the encoding process is taken in three steps:

1. Generation of encoded Bell pair

$$|\tilde{\Phi}^{+}\rangle_{12} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_1|\tilde{0}\rangle_2 + |\tilde{1}\rangle_1|\tilde{1}\rangle_2) \tag{2.29}$$

between neighboring stations 1 and 2 where three for memory qubits and three for ancillary qubits. In memory qubits we prepare $\frac{1}{\sqrt{2}}(|\tilde{0}\rangle_1 + |\tilde{1}\rangle_1)$ and $|\tilde{0}\rangle_1$. In ancillary qubits, we generate three copies of physical Bell pairs $(\frac{|0\rangle_1|0\rangle_2+|1\rangle_1|1\rangle_2}{\sqrt{2}})^{\otimes 3}$ and we implement the teleportation controlled-NOT (CNOT) gates on memory qubits. Then we obtain the encoded Bell pair by the transformation

$$\frac{1}{\sqrt{2}}(|000\rangle_1 + |111\rangle_1) \otimes |000\rangle_1 \rightarrow \frac{1}{\sqrt{2}}(|000\rangle_1|000\rangle_2 + |111\rangle_1|111\rangle_2) \tag{2.30}$$

for stations 1, 2 and generalize it to the neighboring stations j and j+1 for $j = 2, .., L-1$ by $|\tilde{\Phi}^{+}\rangle_{i,j+1}$.

2. Connection of entanglement between encoded Bell pairs $|\tilde{\Phi}^{+}\rangle_{12}$ and $|\tilde{\Phi}^{+}\rangle_{23}$ referring the right and left encoding blocks by $2a$ and $2b$ on the mid station 2

3. Station 2 announce the outcomes of the Bell measurements.

These three step for quantum repeater can be generalized from three-qubit repetition code to any $[n, k, 2t + 1]$ CSS code which contains two two classical error correcting codes C^X and C^Z and error syndrome for them are obtained by measurements in the X or Z basis.

2.3 Measurement Based Quantum Computation

In measurement based computation information is stored in cluster states [75,76]. In writing information into the cluster states we use an ensemble of qubits located on a d-dimensional lattice with sides a and the interaction of the qubits are described by the Hamiltonian

$$H_{int} = \hbar g(t) \sum_{a,a^{'}} f(a - a^{'}) \frac{1 + \sigma_z^{(a)}}{2} \frac{1 - \sigma_z^{(a)}}{2} \tag{2.31}$$

which is equivalent to the quantum Ising model. $g(t)f(a - a^{'})$describes the coupling strength. In quantum information this interaction describes the simultaneous conditional phase gates between gates at sites a and $a^{'}$.and read out by the one-particle measurements. Corresponding to the interaction Hamiltonian (2.24) the cluster states are written as

$$|\Phi\rangle_{\mathcal{C}} = \bigotimes_{c \in C} (|0\rangle_c \otimes_{\gamma \in \Gamma} \sigma_z^{(c+\gamma)} + |1\rangle_c) \tag{2.32}$$

with the convention that $\sigma_z^{(c+\gamma)} \equiv 1$ when $c + \gamma \notin \mathcal{C}$.

These cluster states satisfy the set of eigenvalue equations

$$K_a |\Phi\rangle_{\mathcal{C}} = \kappa |\Phi\rangle_{\mathcal{C}} \tag{2.33}$$

where

$$K_a = \sigma_x^{(a)} \otimes_{\gamma \in \Gamma \cup -\Gamma} \sigma_z^{(a+\gamma)} \tag{2.34}$$

for $a \in \mathcal{C}$ and $\Gamma \cup -\Gamma$ specifies the sites of all qubits which interacts with a.

To transform these entangled cluster states into a Bell state we measure all qubits in the neighborhood of the the path $\mathcal{P} \subset \mathcal{C}$ connecting the sites c and c' for $c, c' \in \mathcal{C}$.

Besides the Bell states, using LOCC, one can obtain the class of the multipartite states

$$|\Psi\rangle = \alpha|00...0\rangle + \beta|11...1\rangle \tag{2.35}$$

where for the values $\alpha = \beta = \frac{1}{\sqrt{2}}$, GHZ-states are obtained.

The stabilizer states corresponds to the $\kappa = (-1)^{K_a}$ value and the eigenvalue equation is written in the form

$$K_a|\Phi\rangle_{\mathcal{C}} = (-1)^{\kappa_a}|\Phi\rangle_{\mathcal{C}} \tag{2.36}$$

where $\kappa_a \in 0, 1$ and this allows us to write graphs states in the form

$$\sigma_x^{(a)} \otimes (\sigma_z^{(b)})^{\Gamma_{ab}}|\Phi\rangle_{\mathcal{C}} = (-1)^{\kappa_a}|\Phi\rangle_{\mathcal{C}} \tag{2.37}$$

where a,b are the edges of the graphs which are occupied by the qubits and Γ_{ab} is the adjacency matrix taking values only 0 and 1. In this way we treat the cluster states particular case of graph states.

CHAPTER 3

RANK TWO ENTANGLEMENT TRANSFORMATIONS

3.1 The Description of the States and the Local Operations

Any local operation on a rank-2 state transforms it either to a rank-2 state or to a product state. Hence, analyzing the possible effects of local measurements on these states are somewhat simpler than the ones on other multipartite entangled states. The main goal of this section is to understand the LOCC-convertibility properties of the rank-2 states. In other words, given a rank-2 state $|\psi\rangle$, under which cases are these p parties able to transform it to another given rank-2 state $|\phi\rangle$ by LOCC? LOCC convertibility can be studied for *deterministic transformations* where a single final state $|\phi\rangle$ is desired to be produced with probability 1, or for *probabilistic transformations* where a number of different final states are needed to be produced with known probabilities.

In order to be able to study the LOCC transformations, it is necessary to have a good parametrization of the rank-2 states and the local operations that can be applied on them. For this purpose, we first start with the description of a possible parametrization of rank-2 states.

3.1.1 The parametrization of states

By definition, any rank-2 state $|\psi\rangle$ can be expressed in the form

$$|\psi\rangle = \frac{1}{\sqrt{N}} \left(|\alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_p\rangle + z|\beta_1 \otimes \beta_2 \otimes \cdots \otimes \beta_p\rangle \right) \tag{3.1}$$

where $|\alpha_k\rangle$ and $|\beta_k\rangle$ are *normalized* states in the Hilbert space $\mathcal{H}_k$ of the particle possessed by the party-k, where their relative phases are adjusted suitably such that they have a real, non-negative inner product $c_k = \langle\alpha_k|\beta_k\rangle$ (i.e., $c_k \geq 0$), and z is a complex number. Here N is the normalization factor

$$N = 1 + |z|^2 + c_1 c_2 \cdots c_p (z + z^*) \quad . \tag{3.2}$$

The overall phase of the state $|\psi\rangle$ can be eliminated by absorbing it into the overall phase of a pair $\{|\alpha_k\rangle, |\beta_k\rangle\}$ for one of the parties without any problem.

Apart from the individual states used, this state depends on one complex parameter z, and p real parameters $c_1, \ldots, c_p$, the *cosines*, which are numbers from the closed $[0, 1]$ interval. The collection of these parameters will be denoted by $\lambda = (z; c_1, c_2, \ldots, c_p)$. The $(p+1)$-tuple λ will be considered as a point in a space Λ which is essentially $\mathbb{C} \times [0, 1]^p$. However, there are a few adjustments that need to be made before defining the space Λ precisely. First, if $|\psi\rangle$ is a rank-2 state, then the complex number z has to be non-zero. However, treating the product states (i.e., rank-1 states) by the same parametrization has some advantages. For this reason, we tend to include $z = 0$ values as possible values of this parameter. Moreover, the value $z = \infty$ should also be included as a possible value for this parameter, for which case $|\psi\rangle$ is again a product state. In other words, the parameter z can be chosen from the extended complex numbers $\mathbb{C}' = \mathbb{C} \cup \{\infty\}$. Apart from this, note that the point $\lambda_0 = (z = -1; c_1 = 1, \ldots, c_p = 1)$ cannot possibly be identified with a state. As a result, we exclude this point from Λ. Hence, the parameter space Λ is defined as $\Lambda = \mathbb{C}' \times [0, 1]^p \setminus \{(-1; 1, 1, \ldots, 1)\}$. Consequently, any rank-2 or rank-1 state can be expressed by using a point λ in the space Λ.

At this point, it is appropriate to describe various types of states represented as points in Λ. There are essentially three types of states that can be described as a point in Λ. (1) The first one of these are the product states. These are included as points in Λ for completeness, due to the fact that some local operations produce them. (2) Next, bipartite entangled states between any two parties (say party-k_1 and party-k_2) can also be described as a point in Λ. For such states, the other parties are unentangled. For these states, it turns out that the cosines can be chosen in a multitude of different ways which turns out to be a nuisance. (3) The rest of the states will be called as

truly multipartite states. Any state which is not a product or a bipartite entangled state will be considered as truly multipartite. In this case, there are at least three parties which are entangled.

The following set of rules gives us the conditions which enables us to recognize the type of the state from the parametrization. Let $\lambda = (z; c_1, c_2, \ldots, c_p)$.

(1) The point λ corresponds to a product state if either (i) $z = 0$, or (ii) $z = \infty$ or (iii) cosines are 1 for at least $p - 1$ parties. (Example: The following points for three-partite states correspond to product states: $\lambda_1 = (0; 0.2, 0.3, 0.4)$, $\lambda_2 = (\infty; 0.2, 0.3, 0.4)$, $\lambda_3 = (5 + i; 0.2, 1, 1)$, $\lambda_4 = (5 + i; 1, 1, 1)$.)

(2) The point λ corresponds to a bipartite entangled state if $z \neq 0, \infty$ and the cosines are equal to 1 for *exactly* $p-2$ parties. For example, for a bipartite state between parties k_1 and k_2, only the cosines c_{k_1} and c_{k_2} are different from 1; the rest of the cosines should be 1. (Example: $\lambda_5 = (5 + i; 0.2, 0.3, 1)$ is a bipartite entangled state between party-1 and party-2.)

(3) The point λ corresponds to a truly multipartite state if $z \neq 0, \infty$ and the cosines c_k are less than 1 for three or more parties. (Example: $\lambda_6 = (5 + i; 0.2, 0.3, 0.4)$ is a truly multipartite entangled state. Similarly the state $\lambda_7 = (5 + i; 0.2, 0.3, 0.4, 1, 1, 1)$ is also truly multipartite entangled. The point λ_7 corresponds to a state for 6 parties, but in this special case the last three parties are unentangled.)

The rules above can easily be justified in terms of the concurrences of a given state. Concurrence for party k is simply defined as the concurrence of the state $|\psi\rangle$ considered as an entangled state between party-k and the rest. It is defined as

$$\mathcal{C}_k = 2\sqrt{\det \rho^{(k)}} \tag{3.3}$$

where $\rho^{(k)}$ is the reduced density matrix of the state $|\psi\rangle$ for the party k, which is given by $\rho^{(k)} = \mathrm{tr}_{1,2,\ldots,k-1,k+1,\ldots,p}|\psi\rangle\langle\psi|$. It is straightforward to compute the concurrences for the state in Eq. (3.1) as

$$\mathcal{C}_k = \frac{2|z|\sqrt{1 - c_k^2}\sqrt{1 - (c_1 \cdots c_{k-1}c_{k+1} \cdots c_p)^2}}{N} \quad . \tag{3.4}$$

The non-zero value of the concurrence $\mathcal{C}_k$ is an indication that the kth particle is entangled with the others. In other words, $\mathcal{C}_k = 0$ if and only if party-k is unentangled. Note that for $z \neq 0, \infty$, the concurrence $\mathcal{C}_k$ can be non-zero if and only if $c_k < 1$ and there is another cosine which is less than 1.

It is obvious that the cases $z = 0$ and $z = \infty$ gives product states. For the case for which $z \neq 0, \infty$ we have the following possibilities: (1) If all cosines are 1, or if only one of them is less than 1, then all concurrences vanish, $\mathcal{C}_1 = \cdots = \mathcal{C}_p = 0$, and the state is a product state. (2) If only two cosines, say c_{k_1} and c_{k_2} are less than 1, then $\mathcal{C}_{k_1} = \mathcal{C}_{k_2}$ are nonzero and the rest of the concurrences vanish, in which case we have a bipartite entangled state between parties k_1 and k_2. (3) Finally, if three or more cosines are less than 1, then the concurrence $\mathcal{C}_k$ will be non-zero if and only if $c_k < 1$. Hence all parties with a cosine less than 1 are entangled. Since there are at least three entangled parties, this is a truly multipartite state.

3.1.2 LU equivalence

Next, we need to provide a description of local unitary (LU) equivalence between states that are expressed by using the parametrization given above. We say that two states $|\psi\rangle$ and $|\phi\rangle$ are LU-equivalent, if we can find local unitary operators V_k on each local Hilbert space $\mathcal{H}_k$ such that $|\psi\rangle = (V_1 \otimes \cdots \otimes V_p)|\phi\rangle$. Obviously, LU-equivalent states can be converted into each other by LOCC, with necessary local quantum operations being the indicated unitaries. The opposite is also true. If two states $|\psi\rangle$ and $|\phi\rangle$ are LOCC-convertible into each other, in other words if

- $|\psi\rangle$ can be transformed into $|\phi\rangle$ by LOCC and
- $|\phi\rangle$ can be transformed into $|\psi\rangle$ by LOCC,

then $|\psi\rangle$ and $|\phi\rangle$ are LU equivalent [28,30].

It is straightforward to show that any two states described by the same parameter $\lambda = (z; c_1, \ldots, c_p)$ are LU-equivalent. Such states differ only in the pairs of states $\{|\alpha_k\rangle, |\beta_k\rangle\}$ chosen from $\mathcal{H}_k$ and the inner-product preserving property of the unitary operators immediately leads to the LU-equivalence. Hence, the points λ of Λ denotes

a collection states which are all LU-equivalent. Such states are all LU-equivalent to the following representative state

$$|\Phi(\lambda)\rangle = \frac{1}{\sqrt{N(\lambda)}}\left(|0\otimes 0\otimes\cdots\otimes 0\rangle + z|w_{c_1}\otimes w_{c_2}\otimes\cdots\otimes w_{c_p}\rangle\right) \tag{3.5}$$

where $|w_{c_k}\rangle = c_k|0\rangle + \sqrt{1-c_k^2}|1\rangle$ and

$$N(\lambda) = 1 + |z|^2 + c_1c_2\cdots c_p(z+z^*) \tag{3.6}$$

Apart from this, it is possible to express the *same* state by using two different points, say λ and λ'. Expressed in a different way, there might be different points λ and λ' of Λ such that the representative states $|\Phi(\lambda)\rangle$ and $|\Phi(\lambda')\rangle$ are LU-equivalent. We will say that the points λ and λ' are (LU) equivalent if this happens and denote it as $\lambda \sim \lambda'$. Our job is now to express this relation in terms of the individual z and cosine parameters.

For any given point λ of Λ, let us define its "conjugate" $\hat{\lambda}$ by

$$\text{if } \lambda = (z; c_1, c_2, \ldots, c_p) \quad \text{then} \quad \hat{\lambda} = (\frac{1}{z}; c_1, c_2, \ldots, c_p) \quad . \tag{3.7}$$

It can be seen easily that $\lambda \sim \hat{\lambda}$. It turns out that, for most points of the space Λ, the corresponding equivalence class is formed by this pair of points. But there are exceptions. Below, the precise criteria for deciding whether two given points of Λ are equivalent are given. Once this equivalence relation is handled, the set of equivalence classes $\Lambda/\sim$ is identical with the set of LU-equivalence classes of states. The solution of the LOCC convertibility problem should obviously be expressed in terms of these equivalence classes. In other words, instead of saying that a state $|\psi\rangle$ can be LOCC converted to another state $|\phi\rangle$, we will always be saying that an LU-equivalence class of states can be LOCC-converted to another LU-equivalence class. This makes $\Lambda/\sim$ as the central mathematical object that should be used for describing LOCC convertibility property of states. (However, due to its simplicity, it might still be easier to work with Λ rather than $\Lambda/\sim$.)

For determining whether two given points, say $\lambda = (z; c_1, c_2, \ldots, c_p)$ and $\lambda' = (z'; c_1', c_2', \ldots, c_p')$ are LU-equivalent, we make use of the types of these states. The rules of LU-equivalence can be summarized as follows.

(1) if λ is product state, then $\lambda \sim \lambda'$ if and only if λ' is a product state. This is a rather obvious statement.

(2) If λ is a bipartite entangled state between party-k and party-ℓ, then $\lambda \sim \lambda'$ if and only if λ' is also a bipartite state between the same parties and they have the same "concurrence", in other words

$$\frac{|z|\sqrt{1-c_k^2}\sqrt{1-c_\ell^2}}{N(\lambda)} = \frac{|z'|\sqrt{1-c_k'^2}\sqrt{1-c_\ell'^2}}{N(\lambda')} \tag{3.8}$$

This result is also straightforward.

(3) If λ is truly multipartite then $\lambda \sim \lambda'$ if and only if (a) the corresponding cosines are identical (i.e., $c_k = c_k'$ for all k) and (b) the following condition holds for z depending on whether there is a vanishing cosine:
(i) when no cosines vanish, either $z' = z$ or $z' = 1/z$,
(ii) when there is a vanishing cosine, either $|z'| = |z|$ or $|z'| = 1/|z|$.
(Examples: The only other point $\lambda_1 = (1+i; 0.2, 0.3, 0.4)$ is equivalent to is $\hat{\lambda}_1 = ((1-i)/2; 0.2, 0.3, 0.4)$. However, the point $\lambda_2 = (1+i; 0, 0.3, 0.4)$ has a vanishing cosine and therefore λ_2 is equivalent to all points of the form $(\sqrt{2}e^{i\theta}; 0, 0.3, 0.4)$ and of the form $(e^{i\theta}/\sqrt{2}; 0, 0.3, 0.4)$ for all θ. In this case, the equivalence class of λ_2 contains infinitely many points. Finally, the point $\lambda_3 = (1; 0.2, 0.3, 0.4)$ is equivalent only to itself. Similarly, $\lambda_4 = (-1; 0.2, 0.3, 0.4)$ is also equivalent only to itself.)

Although the statements for the product and bipartite states looks rather straightforward, it is still necessary to provide a proof for the case of truly multipartite states. The following lemma covers this case but it is also valid for a larger class of entangled states having larger Schmidt ranks.

Lemma: *Let $|\psi\rangle$ be a state of p particles which is expressed as*

$$|\psi\rangle = \sum_{i=1}^{r} |\varphi_i^{(1)} \otimes \varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle \tag{3.9}$$

where, for each k, $F^{(k)} = \left\{|\varphi_1^{(k)}\rangle, |\varphi_2^{(k)}\rangle, \ldots, |\varphi_r^{(k)}\rangle\right\}$ is a set of r non-zero *vectors from the Hilbert space $\mathcal{H}_k$. Then the following statements hold.*

(a) If there is a party ℓ where the set $F^{(\ell)}$ is linearly independent, then the set of r vectors $\left\{|\varphi_i^{(1)} \otimes \varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle\right\}_{i=1}^{r}$ is also linearly independent. Moreover,

for any party k other than the ℓth, the support of the reduced density matrix of the kth party is the same as the linear span of $F^{(k)}$. (i.e., $\forall k \neq \ell$, $\mathrm{supp}\,\rho^{(k)} = \mathrm{span}\,F^{(k)}$.)

(b) *If there are at least two parties ℓ_1 and ℓ_2 where the sets $F^{(\ell_1)}$ and $F^{(\ell_2)}$ are both linearly independent, then $|\psi\rangle$ has Schmidt rank r.*

(c) *If there are at least three parties ℓ_1, ℓ_2 and ℓ_3 where the sets $F^{(\ell_1)}$, $F^{(\ell_2)}$ and $F^{(\ell_3)}$ are all linearly independent, then the expression of $|\psi\rangle$ as a superposition of r product states is unique. In other words, if $|\beta_i^{(k)}\rangle$ are vectors such that*

$$|\psi\rangle = \sum_{i=1}^{r} |\beta_i^{(1)} \otimes \beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle \tag{3.10}$$

then there is a permutation Q of r objects such that for any $i = 1, \ldots, r$ we have

$$|\beta_i^{(1)} \otimes \beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle = |\varphi_{Qi}^{(1)} \otimes \varphi_{Qi}^{(2)} \otimes \cdots \otimes \varphi_{Qi}^{(p)}\rangle \quad . \tag{3.11}$$

It should be noted that the vectors $|\varphi_i^{(k)}\rangle$ are not required to be normalized; they just need to be non-zero. Any linear coefficient should be considered to be absorbed into one of these vectors. Basically, depending on the number of parties k where $F^{(k)}$ are linearly independent, we make progressively stronger claims detailed above.

Proof: First we show (a). Let us assume that $\ell = 1$ without loss of generality. Let us suppose that there are numbers $a_1, a_2, \ldots, a_r$ such that

$$\sum_{i=1}^{r} a_i |\varphi_i^{(1)} \otimes \varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle = 0 \quad . \tag{3.12}$$

Let $|\Theta\rangle$ be any vector in the Hilbert space of all parties except the 1st, i.e., $|\Theta\rangle \in \otimes_{k\neq 1}\mathcal{H}_k$. Then, the above expansion leads to

$$\sum_{i=1}^{r} |\varphi_i^{(1)}\rangle \left(a_i \langle\Theta|\varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle \right) = 0 \quad . \tag{3.13}$$

But, as the set $F^{(1)}$ is linearly independent, we should have $a_i \langle\Theta\rangle \varphi_i^{(2)\rangle \otimes \cdots \otimes \varphi_i^{(p)}} = 0$ for all i and for all $|\Theta\rangle$. Now, since we can choose $|\Theta\rangle$ to be equal to $|\varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle$, the only way all of these terms to be zero is that we have $a_1 = a_2 = \cdots = a_r = 0$. In other words, the set of vectors $\left\{ |\varphi_i^{(1)} \otimes \varphi_i^{(2)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle \right\}_{i=1}^{r}$ are linearly independent.

To show the second part, let us suppose that $k = 2$ without loss of generality (these assumptions are made to simplify the notation). The reduced density matrix for the second party is

$$\rho^{(2)} = \sum_{i,j=1}^{r} S_{ji} |\varphi_i^{(2)}\rangle\langle\varphi_j^{(2)}| \quad . \tag{3.14}$$

where S is the overlap matrix given by $S_{ij} = \langle\chi_i|\chi_j\rangle$ where $|\chi_i\rangle = |\varphi_i^{(1)} \otimes \varphi_i^{(3)} \otimes \cdots \otimes \varphi_i^{(p)}\rangle$. Now, by applying the same argument above, we can see that the set of r-vectors $\{|\chi_i\rangle\}_{i=1}^r$ is also linearly independent. Therefore, the overlap matrix S is strictly positive definite. From the expression of $\rho^{(2)}$, it is obvious that the support of $\rho^{(2)}$ is included in span $F^{(2)}$. To show that these two subspaces are identical, let us suppose the contrary. Let $|\varphi'\rangle$ be a non-zero vector in span $F^{(2)}$ but orthogonal to the support of $\rho^{(2)}$. Then, at least one of $b_i = \langle\varphi_i^{(2)}|\varphi'\rangle$ is non-zero and therefore $\langle\varphi'|\rho^{(2)}|\varphi'\rangle = \sum_{ij} S_{ji} b_j^* b_i > 0$, which is a contradiction. This then shows that the two subspaces are identical, i.e., supp $\rho^{(2)} =$ span $F^{(2)}$.

As a side remark, it should be noted that the set $F^{(2)}$ can possibly be linearly dependent, in which case dim span $F^{(2)} < r$. The proof above only shows that the subspace spanned by the non-zero eigenvectors of $\rho^{(2)}$ is the same as the subspace span $F^{(2)}$. Hence, the matrix rank of $\rho^{(2)}$ is the same as the number of linearly independent vectors in $F^{(2)}$.

We then continue with part (b). Since there are at least two parties where the associated set of vectors $F^{(\ell_1)}$ and $F^{(\ell_2)}$ are linearly independent, the conclusion in part (a) can be extended to all parties. In other words, for any k (including $k = \ell_1$ and $k = \ell_2$) we have supp $\rho^{(k)} =$ span $F^{(k)}$. In particular, the matrix ranks of the reduced density matrices $\rho^{(\ell_1)}$ and $\rho^{(\ell_2)}$ are both equal to r. This shows that $|\psi\rangle$ cannot be written as a sum of a lesser number of product states. Hence, the Schmidt rank of $|\psi\rangle$ is r.

Finally, we consider the statement in part (c). Let $B^{(k)} = \left\{|\beta_1^{(k)}\rangle, |\beta_2^{(k)}\rangle, \ldots, |\beta_r^{(k)}\rangle\right\}$. First, since the Schmidt rank of $|\psi\rangle$ is r, all of the vectors $|\beta_i^{(k)}\rangle$ are non-zero. Next, we note that the obvious statement about the support of the reduced density matrices, i.e., supp $\rho^{(k)} \subset$ span $B^{(k)}$ holds in general. But for $k = \ell_1, \ell_2, \ell_3$, the dimension of the support is r. As each $B^{(k)}$ contains r vectors, we conclude that the sets $B^{(\ell_1)}$, $B^{(\ell_2)}$ and $B^{(\ell_3)}$ are also linearly independent. In short, the prerequisite conditions for part (c) is

satisfied for the new vectors $|\beta_i^{(k)}\rangle$ as well. Therefore, we have span $B^{(k)} =$ span $F^{(k)}$.

At this point, let us suppose that $(\ell_1, \ell_2, \ell_3) = (1, 2, 3)$, without loss of generality. Since span $B^{(1)} =$ span $F^{(1)}$ and $B^{(1)}$ is linearly independent, there is an $r \times r$ matrix Z such that

$$|\beta_i^{(1)}\rangle = \sum_{j=1}^{r} Z_{ji} |\varphi_j^{(1)}\rangle \quad . \tag{3.15}$$

Inserting this into the expansions of $|\psi\rangle$ we get

$$\sum_j |\varphi_j^{(1)} \otimes \varphi_j^{(2)} \otimes \cdots \otimes \varphi_j^{(p)}\rangle = \sum_{ij} Z_{ji} |\varphi_j^{(1)} \otimes \beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle \quad . \tag{3.16}$$

Using the linear independence of $F^{(1)}$, we get

$$|\varphi_j^{(2)} \otimes \cdots \otimes \varphi_j^{(p)}\rangle = \sum_{i=1}^{r} Z_{ji} |\beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle \tag{3.17}$$

which must hold true for all r. In here we see that a rank-1 state (product state) is expanded as a sum of r product states. Note that $B^{(2)}$ and $B^{(3)}$ are both linearly independent and therefore part (b) of this lemma can be applied to this expression. It then directly follows that only one number in the sequence $Z_{j1}, Z_{j2}, \ldots, Z_{jr}$ can be non-zero (otherwise we get a contradiction for the Schmidt rank of the state on the left-hand side). As Z is a square matrix, each row and each column should contain only one non-zero entry.

Let Q be the permutation that gives the index of the non-zero entry for a given column. In other words, $Z_{ji} \neq 0$ only for $j = Q_i$. Then, we have

$$|\beta_i^{(1)}\rangle = Z_{Q_i i} |\varphi_{Q_i}^{(1)}\rangle \quad , \tag{3.18}$$

$$|\varphi_{Q_i}^{(2)} \otimes \cdots \otimes \varphi_{Q_i}^{(p)}\rangle = Z_{Q_i i} |\beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle \quad , \tag{3.19}$$

$$\implies |\beta_i^{(1)} \otimes \beta_i^{(2)} \otimes \cdots \otimes \beta_i^{(p)}\rangle = |\varphi_{Q_i}^{(1)} \otimes \varphi_{Q_i}^{(2)} \otimes \cdots \otimes \varphi_{Q_i}^{(p)}\rangle \quad , \tag{3.20}$$

which is what is needed to be proved.□

At this point, let us briefly investigate the implication of the lemma for the rank-2 states. Let $|\psi\rangle$ be the state defined by Eq. (3.1) and suppose that $z \neq 0, \infty$. In this case, the conditions in the lemma are satisfied with $r = 2$. Here, the statement that the set $F^{(k)} = \{|\alpha_k\rangle, |\beta_k\rangle\}$ is linearly independent is identical with the statement $c_k < 1$. Hence, part (b) of lemma says that as long as there are two cosines that are

less than 1, then the state is a rank-2 entangled state (and hence it can never be a product state). Part (c) of the lemma implies that if there are at least three cosines less than 1, then the expansion of $|\psi\rangle$ is unique. The most one can do in here is to exchange the places of the first two terms. Consequently, the cosines of individual parties cannot change. The third rule of LU-equivalence follows from here.

3.1.3 Measurements by a Single Party

In this section, we investigate the local operations carried out by a single party and their description on the space Λ. Consider the local operations applied by party k. Such operations can be described by the general measurement formalism, i.e., by a set of measurement operators $\{M_\ell\}_{\ell=1}^n$ on $\mathcal{H}_k$ which satisfy the probability-sum condition

$$\sum_{\ell=1}^{n} M_\ell^\dagger M_\ell = \mathbb{1}_k \quad . \tag{3.21}$$

Let us suppose that the initial state is $|\psi\rangle$ given in Eq. (3.1) and has parameters $\lambda = (z; c_1, \ldots, c_p)$. The measurement changes the state into $(M_\ell \otimes \mathbb{1}'_k)|\psi\rangle$ (up to normalization) with probability $p_\ell = \langle\psi|(M_\ell^\dagger M_\ell)\otimes\mathbb{1}'_k|\psi\rangle$. Here, $\mathbb{1}'_k$ denotes the identity operator acting on all parties except the kth one.

Our first job is to find out the parameters $\lambda^{(\ell)}$ for the final states. For this purpose, let us define A_ℓ, B_ℓ, C_ℓ and γ_ℓ as

$$A_\ell = \|M_\ell|\alpha_k\rangle\| \quad , \tag{3.22}$$

$$B_\ell = \|M_\ell|\beta_k\rangle\| \quad , \tag{3.23}$$

$$C_\ell e^{i\gamma_\ell} = \frac{1}{A_\ell B_\ell}\langle\alpha_k|M_\ell^\dagger M_\ell|\beta_k\rangle \quad . \tag{3.24}$$

Here we take C_ℓ to be a non-negative real number and define the phase γ_ℓ accordingly. By Schwarz inequality we also have $C_\ell \leq 1$. The parameters A_ℓ and B_ℓ are also necessarily non-negative.

When the kth party carries out the measurement, the outcome ℓ occurs with proba-

bility p_ℓ and the final state becomes $\lambda^{(\ell)} = (z^{(\ell)}; c_1, \ldots, c_{k-1}, C_\ell, c_{k+1}, \ldots, c_p)$, where

$$z^{(\ell)} = z\frac{B_\ell e^{i\gamma_\ell}}{A_\ell} \quad , \tag{3.25}$$

$$p_\ell = A_\ell^2 \frac{N(\lambda^{(\ell)})}{N(\lambda)} \tag{3.26}$$

$$= \frac{A_\ell^2 + |z|^2 B_\ell^2 + A_\ell B_\ell c_1 \cdots c_{k-1} C_\ell c_{k+1} \cdots c_p (z e^{i\gamma_\ell} + z^* e^{-i\gamma_\ell})}{N(\lambda)} \quad . \tag{3.27}$$

Hence, to describe the effect of the measurement, we need the values of four real parameters for each outcome: A_ℓ, B_ℓ, C_ℓ and γ_ℓ. Obviously, possible values of these parameters are restricted by the probability-sum condition (3.21), which turns out to be the only restriction on them. These parameters then provides a parametrization of the local measurement done by party k.

First parametrization of local measurements. *A local measurement by party-k on a state $\lambda = (z; c_1, \ldots, c_p)$ can be described by*

(i) a set of outcomes,

(ii) non-negative numbers A_ℓ, B_ℓ, C_ℓ and angles γ_ℓ for each outcome ℓ,

(iii) where the rules for final states and their corresponding probabilities are given in (3.25,3.26)

if and only if these parameters satisfy the following conditions

$$\sum_{\ell=1}^{n} A_\ell^2 = \sum_{\ell=1}^{n} B_\ell^2 = 1 \quad , \tag{3.28}$$

$$\sum_{\ell=1}^{n} A_\ell B_\ell C_\ell e^{i\gamma_\ell} = c_k \quad , \tag{3.29}$$

$$C_\ell \leq 1 \quad . \tag{3.30}$$

Proof: It is straightforward to show that these conditions are necessary, implied by the probability sum rule in Eq. (3.21). Here, we will show the opposite. Namely, if A_ℓ, B_ℓ, C_ℓ and γ_ℓ are parameters satisfying (3.28-3.30), then we can find a set of measurement operators $\{M_\ell\}$ which produce these parameters. Without loss of generality, let us consider the case where $c_k < 1$ (otherwise, party k is unentangled with the remaining

parties and what she does has no effect on the state). The proof is as follows: Let $|\alpha_k^\perp\rangle$ and $|\beta_k^\perp\rangle$ be the "dual basis" satisfying

$$\langle\alpha_k^\perp|\alpha_k\rangle = \langle\beta_k^\perp|\beta_k\rangle = 1 \quad , \tag{3.31}$$

$$\langle\alpha_k^\perp|\beta_k\rangle = \langle\beta_k^\perp|\alpha_k\rangle = 0 \quad . \tag{3.32}$$

These states are well-defined. They are simply defined as follows:

$$|\alpha_k^\perp\rangle = \frac{1}{1-c_k^2}\left(|\alpha_k\rangle - c_k|\beta_k\rangle\right) \quad , \tag{3.33}$$

$$|\beta_k^\perp\rangle = \frac{1}{1-c_k^2}\left(-c_k|\alpha_k\rangle + |\beta_k\rangle\right) \quad . \tag{3.34}$$

Define the operators P_ℓ on $\mathcal{H}_k$ as follows,

$$\begin{aligned} P_\ell = {} & A_\ell^2|\alpha_k^\perp\rangle\langle\alpha_k^\perp| + B_\ell^2|\beta_k^\perp\rangle\langle\beta_k^\perp| + \\ & \Big(A_\ell B_\ell C_\ell e^{i\gamma_\ell}|\alpha_k^\perp\rangle\langle\beta_k^\perp| + h.c.\Big) \end{aligned} \tag{3.35}$$

It is straightforward to show that P_ℓ is positive semidefinite (where the inequality $C_\ell \leq 1$ is employed) and $\sum_\ell P_\ell = \mathbb{1}_k$ (where the remaining restrictions, (3.28) and (3.29), are employed). In short, the set of operators $\{P_\ell\}$ forms a positive-operator valued measure (POVM). We simply define $M_\ell = \sqrt{P_\ell}$. It is then easy to check that the same parameters are produced by these measurement operators. □

There are a number of remarks that should be made about the parametrization of local measurements described above. Notice that this parametrization *depends on the initial state* λ through the appearance of the cosine c_k in (3.29). Our next observation is that such a local measurement does not change the cosines of the other parties, i.e., $c_{k'}$ remains the same for $k' \neq k$. The only change is in the cosine for party k (i.e., c_k becomes C_ℓ now) and the parameter z.

Let us consider the special case $c_k = 1$, which is excluded from the proof given above. Physically, this case does not need any further elaboration because party-k cannot do anything to change the state. Mathematically, the conditions in Eq. (3.28-3.30) imply the same conclusion because applying the Schwarz inequality for Eq. (3.29) we can see that $C_\ell = 1$, $\gamma_\ell = 0$ and $A_\ell = B_\ell$ for all ℓ. Hence $z^{(\ell)} = z$ and $\lambda^{(\ell)} = \lambda$; i.e., nothing changes for any outcome. In short, the description of the local measurement given above can also be extended to the case $c_k = 1$ without any mathematical problem.

Another remark is about simplifying the transformation parameters. A simplification becomes necessary if two possible outcomes produce the same points in Λ, i.e., we have $\ell \neq \ell'$ but $\lambda^{(\ell)} = \lambda^{(\ell')}$. In other words, the individual parameters satisfy $C_\ell = C_{\ell'}$, $\gamma_\ell = \gamma_{\ell'}$ and $B_\ell/A_\ell = B_{\ell'}/A_{\ell'}$. If such a situation occurs, then it is possible to construct a new local operation where these two outcomes appear as a single outcome. We will denote the new, constructed measurement by tildes, $\tilde{A}_m$, etc. The new parameters are identical with the old parameters for all $m \neq \ell, \ell'$. But, $m = \ell'$ is absent from the list of outcomes and for $m = \ell$ we have

$$\tilde{A}_\ell = \sqrt{A_\ell^2 + A_{\ell'}^2} \quad , \tag{3.36}$$

$$\tilde{B}_\ell = \sqrt{B_\ell^2 + B_{\ell'}^2} \quad , \tag{3.37}$$

$$\tilde{C}_\ell = C_\ell \quad , \tag{3.38}$$

$$\tilde{\gamma}_\ell = \gamma_\ell \quad . \tag{3.39}$$

It is then easy to show that this new parameter set satisfies the relations in Eq. (3.28-3.30). Furthermore, we have $\tilde{\lambda}^{(\ell)} = \lambda^{(\ell)} = \lambda^{(\ell')}$ and new probabilities satisfying $\tilde{p}_\ell = p_\ell + p'_\ell$.

In conclusion, when considering a particular local measurement, it can be safely assumed that the final points $\lambda^{(\ell)}$ are different for each outcome ℓ. Expressed differently, we can assume that the set of values of pairs $(z^{(\ell)}, C_\ell)$ are different. Note that it is still possible for different outcomes to be LU equivalent, e.g., we might have $\lambda^{(1)} \sim \lambda^{(2)}$ and $\lambda^{(1)} \neq \lambda^{(2)}$. Appearance of LU-equivalent points of Λ cannot be eliminated by any trick.

The special measurements where either $A_\ell = 0$ or $B_\ell = 0$ produces a product state (where $z^{(\ell)}$ is either 0 or ∞). If $|\psi\rangle$ is a truly multipartite state, then this is the only possibility for party-k to collapse the whole state to a product state. If $A_\ell = 0$, then the corresponding probability p_ℓ has to be computed by a limiting procedure. Note that, the cases $A_\ell = B_\ell = 0$ can be discarded as this implies that the corresponding POVM operator is zero and hence the transformation has 0 probability of occurrence.

Finally, the following simple, but general property of local measurements will be very useful later on.

Theorem 1. *Consider a local measurement by party-k on a state corresponding to*

point $\lambda = (z; c_1, \ldots, c_p)$ *where* $|z| \geq 1$. *Then,*

(a) There is at least one outcome ℓ *for which* $C_\ell \geq c_k$.

(b) There is at least one outcome m *for which* $|z|^{(m)} \geq |z|$.

If ≤ 1, then part (b) should be expressed as: There is at least one outcome m for which $|z|^{(m)} \leq |z|$. Both (a) and (b) can be interpreted as stating that there is at least one outcome where the final state is "closer to the product states". However, it is not known whether being "close to product states" can be defined unambiguously. Here, the interpretation seems likely based on the fact that $z = \infty$ (or $z = 0$) correspond to a product state. Similarly, if all cosines are 1, the state is a product state. The distribution of values of these two parameters makes it look like that the state is approaching to product states.

Proof: We start with (a). If $c_k = 0$, there is nothing to be shown. So, consider only the cases $c_k > 0$. let us assume the "contrary" and suppose that $C_\ell \leq c_k$ for all ℓ. Then we have

$$c_k = \sum_\ell A_\ell B_\ell C_\ell e^{i\gamma_\ell} \leq \sum_\ell A_\ell B_\ell C_\ell \tag{3.40}$$

$$\leq c_k \sum_\ell A_\ell B_\ell \leq c_k \sqrt{(\sum_\ell A_\ell^2)(\sum_\ell B_\ell^2)} = c_k \tag{3.41}$$

and, as a result, all inequalities must be equalities. Namely, we should have $\gamma_\ell = 0$ when $A_\ell B_\ell C_\ell \neq 0$, $C_\ell = c_k$ when $A_\ell B_\ell \neq 0$ and $A_\ell = B_\ell$ from the Schwarz inequality. The last relation rules out the product-state producing outcomes ($A_\ell = 0$ or $B_\ell = 0$) and hence we have $C_\ell = c_k$ and $\gamma_\ell = 0$ for all ℓ. This means that all outcomes are identical and the state has not changed (i.e., party-k has done a local unitary transformation only).

What we have shown above is that, for any measurement, there should be an ℓ such that $C_\ell \geq c_k$ for some ℓ. Moreover, if the local operation is not a local unitary, then we should have the strict inequality $C_\ell > c_k$ for some ℓ. (Note: This last statement cannot be extended to the cases where $c_k = 0$. For such states, it is possible to find local measurements that are not local unitaries in such a way that $C_\ell = 0$ for all outcomes.)

For showing part (b), let us assume that $|z|^{(\ell)} \leq |z|$ for all outcomes ℓ. This implies that $B_\ell \leq A_\ell$. Finally,

$$1 = \sum_\ell B_\ell^2 \leq \sum_\ell A_\ell^2 = 1 \tag{3.42}$$

implies that all inequalities must have been equalities, i.e., $A_\ell = B_\ell$ and hence $|z|^{(\ell)} = |z|$ for all ℓ. Therefore the conclusion follows.□

For the local measurement described above, the restrictions (3.28,3.29) imply the following identities

$$\sum_\ell p_\ell \frac{1}{N(\lambda^{(\ell)})} = \frac{1}{N(\lambda)} \quad , \tag{3.43}$$

$$\sum_\ell p_\ell \frac{|z^{(\ell)}|^2}{N(\lambda^{(\ell)})} = \frac{|z|^2}{N(\lambda)} \quad , \tag{3.44}$$

$$\sum_\ell p_\ell \frac{z^{(\ell)} C_\ell}{N(\lambda^{(\ell)})} = \frac{z c_k}{N(\lambda)} \quad . \tag{3.45}$$

Note that the last relation is complex, i.e., it actually contains two real relations. These relations are valid for all special cases as well, without any exceptions. One important feature of these relations is that they are expressed entirely in terms of two real parameters (the probability p_ℓ and the final cosine C_ℓ) and one complex parameter ($z^{(\ell)}$). More importantly, these relations form a basis for an alternative parametrization of the measurement by local party k.

Second parametrization of local measurements. *A local measurement by party k on the state $\lambda = (z; c_1, \ldots, c_p)$ can be described by*

(i) a set of outcomes,

(ii) and one complex number $z^{(\ell)}$ and two real numbers $C_\ell, p_\ell \in [0,1]$ defined for each outcome ℓ,

(iii) where the transition rule is that the outcome ℓ occurs with probability p_ℓ and the final state becomes $\lambda^{(\ell)} = (z^{(\ell)}; c_1, \ldots, c_{k-1}, C_\ell, c_{k+1}, \ldots, c_p)$

if p_ℓ satisfy the probability sum rule (i.e., $\sum_\ell p_\ell = 1$) and the relations (3.43) and (3.45) are satisfied. (Note that (3.44) follows from these two relations.)

Proof: What we need to show is that given $z^{(\ell)}$, C_ℓ and p_ℓ satisfying the stated conditions, we can find A_ℓ, B_ℓ and γ_ℓ satisfying the conditions of the first parametrization. We define

$$A_\ell = \sqrt{\frac{p_\ell N(\lambda)}{N(\lambda^{(\ell)})}} \tag{3.46}$$

$$B_\ell = \frac{|z^{(\ell)}|}{|z|}\sqrt{\frac{p_\ell N(\lambda)}{N(\lambda^{(\ell)})}} \tag{3.47}$$

$$\gamma_\ell = \arg\left(z^{(\ell)}/z\right) \tag{3.48}$$

It is then easy to check that Eq. (3.28-3.30) are satisfied.

But there are some special cases that need to be concentrated on. These are situations where the definitions of A_ℓ, B_ℓ or γ_ℓ are problemmatic. (1) First, let us consider the special case $z = 0$. Namely, the initial state is a product state. Obviously, a product state can only be transformed to product states. Therefore, we only need to check that our equations indeed produces this result. Using Eq. (3.44), we can see that for all ℓ, we either have $z^{(\ell)} = 0$ or $N(\lambda^{(\ell)}) = \infty$. The latter can happen only with $z^{(\ell)} = \infty$, which is itself a product state. As a result, in this case, the new parameters define a valid transformation (we do not need to check if A_ℓ, B_ℓ, γ_ℓ satisfy the desired properties). Note that the same conclusion holds for the $z = \infty$ case as well.

(2) Next, consider the situation where $z \neq 0, \infty$ but $N(\lambda) = 0$. This can happen only when $c_1 = c_2 = \ldots = c_p = 1$ and $z = -1$. However, this point has specifically been excluded from Λ.

(3) Next, suppose that $z \neq 0, \infty$ and $N(\lambda) \neq 0$. In such a case, note that $N(\lambda^{(\ell)}) \neq 0$ for any ℓ with $p_\ell \neq 0$. Hence, A_ℓ is well defined. For B_ℓ, we have to check the case where $N(\lambda^{(\ell)}) = \infty$. But this can happen only when $z^{(\ell)} = \infty$ and B_ℓ can be defined by the limiting procedure. In the limit, we should take $N(\lambda^{(\ell)})/|z^{(\ell)}|^2 = 1$. As a result, if $z^{(\ell)} = \infty$, then we define $A_\ell = 0$ and $B_\ell = \sqrt{p_\ell N(\lambda)}$, but γ_ℓ can be arbitrary. The relations (3.28) and (3.29) are satisfied in this case. Finally, the special case where $z^{(\ell)} = 0$ also does not create a problem. In that case we take $A = \sqrt{p_\ell}$ and $B_\ell = 0$; γ_ℓ is again arbitrary. These cases do not create any problem too. With this, the proof of the claim is completed.□

3.1.4 Some monotones

The relations (3.43-3.45) may be useful in constructing new entanglement monotones. Entanglement monotones are those functions of states which never increase on the average under probabilistic LOCC transformations. [38,42] For pure states, f is a monotone if whenever the state $|\psi\rangle$ is converted by LOCC into states $|\phi_\ell\rangle$ with probabilities p_ℓ, then

$$p(\psi) \geq \sum_\ell p_\ell f(\phi_\ell) \quad . \tag{3.49}$$

Obviously, it is sufficient to check this inequality only for local operations. Note that monotones have the same value for LU-equivalent states.

A new monotone f for rank-2 states can be defined as follows: For a state with parameter point λ,

$$f(\lambda) = \min_{\lambda' \sim \lambda} \frac{1}{N(\lambda')} \quad , \tag{3.50}$$

in other words, the smallest value for N^{-1} among LU equivalent points is an entanglement monotone. For a truly multipartite state $\lambda = (z; c_1, c_2, \ldots, c_p)$, we have

$$f(\lambda) = \begin{cases} N(\lambda)^{-1} & \text{if } |z| \geq 1, \\ N(\hat{\lambda})^{-1} = N(\lambda)/|z|^2 & \text{if } |z| \leq 1. \end{cases} \tag{3.51}$$

The fact that this is a monotone can be seen easily from (3.43), when we take into account the fact that we can choose the initial parameter point λ such that $|z| \geq 1$. What is now left is to give the values of this monotone for product and bipartite states. For product states, obviously taking $z = \infty$ gives us the minimum of $f = 0$. For a bipartite state between parties k_1 and k_2 with concurrence $\mathcal{C}_{k_1} = \mathcal{C}_{k_2} = \mathcal{C}$, the minimum is obtained for the parameter point λ for which $c_{k_1} = c_{k_2} = 0$, i.e., in the Schmidt decomposed form. Hence, it can easily be found that

$$f(\lambda) = \frac{1}{2}\left(1 - \sqrt{1 - \mathcal{C}^2}\right) \quad . \tag{3.52}$$

3.1.5 The Ability of a Single Party to Obtain a Product State

In this subsection, we will try to answer the quaestion "what a single party can do if she wants to destroy the entanglement?" Suppose that the party k wants to reduce

the whole state to a product state. Consider the case where all parties except k are not doing any local operations. The question is to find the maximum success probability of party-k. We consider an arbitrary truly multipartite state such that $c_k < 1$.

Remember that party k produces a product state only when either $A_\ell = 0$ or $B_\ell = 0$. Without loss of generality, we can suppose that the first two ℓ values correspond to these cases ($A_1 = 0$ and $B_2 = 0$). We can show that, for a given A_2 and B_1, we can find an appropriate set of parameters A_ℓ, B_ℓ, C_ℓ and γ_ℓ if and only if

$$(1 - A_2^2)(1 - B_1^2) \geq c_k^2 \quad . \tag{3.53}$$

The success probability can be expressed as

$$p_{succ} = p_1 + p_2 = \frac{A_2^2 + B_1^2|z|^2}{N(\lambda)} \tag{3.54}$$

Our job is to maximize the probability above subject to the restriction above. The final result for the maximum probability of success is

$$p_{succ,max} = \frac{1}{N(\lambda)} \begin{cases} (1 - c_k^2)\|z|^2 & \text{if } \ 1/c_k < |z| \quad , \\ 1 + |z|^2 - 2c_k|z| & \text{if } \ c_k \leq |z| \leq 1/c_k \quad , \\ 1 - c_k^2 & \text{if } \ |z| < c_k \quad . \end{cases} \tag{3.55}$$

These expressions probably tell us the level of command of party-k on the entanglement of the state.

We can then check the particular cases. If $c_k = 1$, we can see that $p_{succ,max} = 0$ as we have discussed above. If $c_k = 0$, then we have $p_{succ,max} = 1$. In that case, party-k has the largest "command" on the entanglement.

3.2 Deterministic Transformations of States by Many Parties

For deterministic transformations, it is required that all of the possible final states are the same state up to LU equivalence. In other words, when the parties start from an initial state $\lambda = (z; c_1, \ldots, c_p)$ and desire to obtain a final state $\lambda' = (z'; c_1', \ldots, c_p')$, all final states after every possible chain of local operations is a point of Λ which is LU-equivalent to λ'. If a protocol of local measurements can be found, we say that λ can be (deterministically) converted or transformed into λ' by LOCC.

Below, the conditions that enable us to decide if λ can be converted to λ' by LOCC are given. But, in here, only the case where λ represents a truly multipartite state is investigated. (Otherwise, the transformations rules are already known: i.e., if λ is a bipartite state, then the transformation conditions are Nielsen's majorization condition [41]; if λ is product state, then it can be converted only into product states.) Moreover, we are going to assume that λ' is also a truly multipartite state. The transformation into bipartite states seems to be a rather difficult problem.

Because of LU equivalence between λ and $\hat{\lambda}$, the initial point can be chosen to be either of these points. Here, we will choose λ in such a way that $|z| \geq 1$, a convention which will simplify some of the discussions. Similarly for the final state; it will be assumed that $|z'| \geq 1$. Now, if LOCC conversion of λ to λ' is possible, theorem 1 above implies the following necessary conditions: $|z'| \geq \|z|$ and $c'_k \geq c_k$ for all parties k. In other words, the z parameter and the cosine parameters for all parties approach to "those of a product state". It appears that if both λ and λ' are points with a vanishing cosine, then these conditions are also sufficient.

3.2.1 Deterministic transformation into states with vanishing cosine

Essentially, if λ to λ' conversion is possible and λ' has vanishing cosines, then λ should also have vanishing cosines for the same parties. Hence, the first case we will take up is the transformation between states with vanishing cosines. Luckily, the rules of transformation are very simple.

Theorem 2. *Let $\lambda = (z; c_1, \ldots, c_p)$ and $\lambda' = (z'; c'_1, \ldots, c'_p)$ be such that $|z| \geq 1$, $|z'| \geq 1$, both of these states are truly multipartite and both have a vanishing cosine parameter. Then λ can be LOCC converted into λ' if and only if $|z'| \geq |z|$ and $c'_k \geq c_k$ for all parties k. Proof:* Necessity is obvious as it follows from theorem 1. We can prove sufficiency step by step. We will first show that, if λ has a vanishing cosine, then it is possible to increase one of the parameters in any desired amount. After that, we summarize the protocol that needs to be followed in the conversion of λ into λ'. Without loss of generality, we can suppose that the first party, $k = 1$, has a vanishing cosine for both states, i.e., $c_1 = c'_1 = 0$. Moreover, without loss of generality we can assume that both z and z' are positive real numbers (by using LU-equivalence).

(1) First, we show that the 1st party can increase the absolute value of the z parameter. In other words, the state $\lambda = (z; 0, c_2, \ldots, c_p)$ can be converted to $\tilde{\lambda} = (z'; 0, c_2, \ldots, c_p)$ for any real number z' with $z' > z$. (If $z' = z$, nothing needs to be done.) In terms of the first parametrization of local measurements, this can be achieved by a two outcome measurement, having the following parameters

$$A_1 = \sqrt{\frac{z'^2 z^2 - 1}{z'^4 - 1}} \quad , \tag{3.56}$$

$$A_2 = z' \sqrt{\frac{z'^2 - z^2}{z'^4 - 1}} \quad , \tag{3.57}$$

$$B_1 = \frac{z'}{z} \sqrt{\frac{z'^2 z^2 - 1}{z'^4 - 1}} \quad , \tag{3.58}$$

$$B_2 = \frac{1}{z} \sqrt{\frac{z'^2 - z^2}{z'^4 - 1}} \quad , \tag{3.59}$$

$$C_1 = C_2 = \gamma_1 = \gamma_2 = 0 \quad . \tag{3.60}$$

It can be easily seen that the conditions (3.28-3.30) are satisfied by these parameters. Although this is not needed, the parameters for the second parametrization can also be given and the possibility of the transformation can be seen from this viewpoint. They are

$$z^{(1)} = z' \quad , \tag{3.61}$$

$$z^{(2)} = \frac{1}{z'} \quad , \tag{3.62}$$

$$p_1 = \frac{z'^2 z^2 - 1}{(z^2 + 1)(z'^2 - 1)} \quad , \tag{3.63}$$

$$p_2 = \frac{z'^2 - z^2}{(z^2 + 1)(z'^2 - 1)} \quad , \tag{3.64}$$

$$C_1 = C_2 = 0 \quad . \tag{3.65}$$

In that case, it can easily be checked that the conditions (3.43) and (3.45) are satisfied. Thus, whichever parametrization used, we always get the final states $\tilde{\lambda}$ and $\hat{\tilde{\lambda}}$ with total probability 1. Therefore, 1st party can convert λ into $\tilde{\lambda}$. In other words, he can increase the modulus of the z parameter.

(2) Second, it will be shown that any party other than the 1st one, can increase their own cosine parameter to any desired value. For this purpose let us consider a given $c_k \geq 0$ (initial cosine can be zero) and another desired one c'_k where $c'_k > c_k$. We exclude the possibility $c'_k = c_k$ because in that case nothing needs to be done. Then the kth party can do the following two outcome measurement (where the first

parametrization is shown only)

$$A_1 = A_2 = B_1 = B_2 = \frac{1}{\sqrt{2}} \quad , \tag{3.66}$$

$$C_1 = C_2 = c'_k \quad , \tag{3.67}$$

$$\gamma_1 = -\gamma_2 = \arccos \frac{c_k}{c'_k} \quad . \tag{3.68}$$

Then it is trivial to check that the conditions (3.28-3.30) are satisfied. Moreover, for both outcomes, the final point is LU-equivalent to $(z; 0, c_2, \ldots, c_{k-1}, c'_k, c_{k+1}, \ldots, c_p)$ (if the initial state is $(z; 0, c_2, \ldots, c_{k-1}, c_k, c_{k+1}, \ldots, c_p)$). Note that, if the initial cosine vanishes ($c_k = 0$), then $\gamma_1 = -\gamma_2 = \pi/2$, independent of the final cosine.

It is obvious what the conversion protocol is. All parties do a single measurement to complete their part of the job. The 1st party increases only the modulus of z parameter. The rest of the parties increase their cosines. The order of these local operations are immaterial. Note that each individual local operation is also deterministic.□

Next case that we will deal with are the transformations from λ without a vanishing cosine to another, truly multipartite state λ'. Obviously, by theorem 1, all cosines of λ' should be non-zero as well. Before stating the rules of the transformation, it is necessary to give an alternative parametrization of the complex z parameter which appears to be very useful.

3.2.2 An alternative parametrization of complex numbers

Let z be a complex number having the polar decomposition $z = \exp(\rho + i\theta)$. We define the real valued functions $n = n(z)$ and $s = s(z)$ as follows,

$$n = \frac{\cos\theta}{\cosh\rho} \quad , \tag{3.69}$$

$$s = \frac{\sin\theta}{\sinh\rho} \quad . \tag{3.70}$$

First, note that n takes on values in the closed $[-1, 1]$ interval, but s takes on values in the closed $[-\infty, +\infty]$ interval. In particular, s has the value $\pm\infty$ on the unit circle $|z| = 1$. At the special points $z = \pm 1$ of the unit circle, however, s does not have a definite value, neither does it have a limit. Fortunately, these two points are the only places where n reaches its boundary values, namely $n = +1$ only at $z = 1$. Similarly, $n = -1$ only at $z = -1$.

The correspondence between z and the pair is two-to-one. If z is replaced with $1/z$, then these two functions do not change: $n(1/z) = n(z)$ and $s(1/z) = s(z)$. The opposite is also true, i.e., if $n(z) = n(z')$ and $s(z) = s(z')$ then we either have $z = z'$ or $z = 1/z'$. To see this, it is sufficient to express the following functions of polar coordinates,

$$\cosh\rho = \sqrt{\frac{1+s^2}{n^2+s^2}} \quad , \tag{3.71}$$

$$\cos\theta = n\sqrt{\frac{1+s^2}{n^2+s^2}} \quad , \tag{3.72}$$

$$|\sinh\rho| = \sqrt{\frac{1-n^2}{n^2+s^2}} \quad , \tag{3.73}$$

$$|\sin\theta| = |s|\sqrt{\frac{1-n^2}{n^2+s^2}} \quad . \tag{3.74}$$

The first two relations state that different points on the complex plane that have the same values for the (n, s) pair should be such that ρ and θ have the same magnitude but probably they have different sign. This leaves us four possibilities. Investigation of all possibilities leads us to the conclusion stated above. As a result, the correspondence between the (n, s) pair and the complex numbers outside the unit circle ($|z| > 1$) is one-to-one. The complex conjugation and negation of the complex number z leads to simple transformations of the (n, s) pair, which are listed below,

$$z \to \frac{1}{z} \quad , \quad (n,s) \to (n,s) \quad , \tag{3.75}$$

$$z \to z^* \quad , \quad (n,s) \to (n,-s) \quad , \tag{3.76}$$

$$z \to -z \quad , \quad (n,s) \to (-n,-s) \quad . \tag{3.77}$$

Hence, in terms of the sign of these two functions, the complex plane (outside unit circle) is divided into four regions, the four quadrants.

Next, we consider the curves that are defined as the sets of complex numbers for which the ratio s/n is constant. These curves will be very important for us as it will be found that under deterministic LOCC transformations, the z parameter of the states cannot leave these curves. In here, we just note the following relation

$$z - \frac{1}{z} = \pm\frac{2\sqrt{1-n^2}\sqrt{1+s^2}}{n^2+s^2}(n+is) \quad , \tag{3.78}$$

which implies that the complex number $z - 1/z$ has an invariant phase along these curves. Since the transformation $z \to z^{-1}$ changes this phase angle by π, we tend to

define it modulo π. Hence,

$$\phi = \arg\left(z - \frac{1}{z}\right) \pmod{\pi} = \arctan\frac{s}{n} = \arctan\frac{\tan\theta}{\tanh\rho} \quad . \tag{3.79}$$

This angle appears to be an invariant under deterministic LOCC.

3.2.3 Transformations from states with non-zero cosines

In here, we consider the transformation of the state $\lambda = (z; c_1, \ldots, c_p)$ into $\lambda'(z'; c'_1, \ldots, c'_p)$ where both states have non-zero cosines. Moreover, we again require both states to be truly multipartite. Hence, for both of these points, there are at most two points in Λ that can be LU-equivalent. We choose these two points such that $|z|' \geq 1$ and $|z| \geq 1$. The following theorem handles the LOCC transformation rule for such states.

Theorem 3. *Let λ and λ' be as described above, having non-zero cosines. Let (n, s) and (n', s') denote the values of the n and s functions of their z parameters. It is possible to convert λ into λ' by LOCC if and only if*

(a) $c'_k \geq c_k$ for all parties k, and

(b) the following equality is satisfied

$$\frac{n'}{n} = \frac{s'}{s} = \frac{c_1 c_2 \ldots c_p}{c'_1 c'_2 \ldots c'_p} \quad . \tag{3.80}$$

Proof: First we show necessity. If λ can be converted into λ', then part (a) follows from theorem 1. The relation in (b) follows from the extension of the relations (3.43-3.45) into the whole protocol. Let us use L for denoting the outcomes of all measurements in the conversion protocol, i.e., $L = (\ell_1, \ell_2, \cdots, \ell_N)$ where ℓ_i is the result of ith local operation and N is the (random) number of operations. Let p_L denote the probability of the outcome L. Let $\lambda^{(L)}$ denote the final state after the last measurement when L has occurred (note that these are states that are directly obtained from the second parametrization of local operations; they should not be replaced with their LU-equivalents). Let $\lambda^{(L)} = (z^{(L)}; c_1^{(L)}, \ldots, c_p^{(L)})$ and let us use $c(\lambda^{(L)})$ for denoting the product of all cosines for the state in question, i.e., $c(\lambda^{(L)}) = c_1^{(L)} \cdots c_p^{(L)}$. Now,

the relations (3.43-3.45) immediately lead to

$$\sum_L p_L \frac{1}{N(\lambda^{(L)})} = \frac{1}{N(\lambda)} \quad , \tag{3.81}$$

$$\sum_L p_L \frac{|z^{(L)}|^2}{N(\lambda^{(L)})} = \frac{|z|^2}{N(\lambda)} \quad , \tag{3.82}$$

$$\sum_L p_L \frac{z^{(L)} c(\lambda^{(L)})}{N(\lambda^{(L)})} = \frac{z c(\lambda)}{N(\lambda)} \quad . \tag{3.83}$$

All of these relations are valid for all probabilistic transformations as well. However, for the current deterministic transformation, all final states can be either $\lambda^{(L)} = \lambda'$ or $\lambda^{(L)} = \hat{\lambda}'$. Hence, we can collect all terms within the summation into just two terms with total probabilities p and $q = (1-p)$ respectively. Using, $N(\hat{\lambda}') = N(\lambda')/|z'|^2$, the relations above can be expressed as

$$p\frac{1}{N(\lambda')} + q\frac{|z'|^2}{N(\lambda')} = \frac{1}{N(\lambda)} \quad , \tag{3.84}$$

$$p\frac{|z'|^2}{N(\lambda')} + q\frac{1}{N(\lambda')} = \frac{|z|^2}{N(\lambda)} \quad , \tag{3.85}$$

$$\frac{pz' + qz'^*}{N(\lambda')} c(\lambda') = \frac{z c(\lambda)}{N(\lambda)} \quad . \tag{3.86}$$

(Note that these equations are valid for the cases $z' = \pm 1$ as well, for which $\hat{\lambda}' = \lambda'$ and there should only be a single term. For these special cases, the equation above holds for all possible probabilities p.) These equations are equivalent with the following four equations

$$\frac{N(\lambda')}{N(\lambda)} = \frac{|z'|^2 + 1}{|z|^2 + 1} \quad , \tag{3.87}$$

$$(p-q)\frac{|z'|^2 - 1}{|z'|^2 + 1} = \frac{|z|^2 - 1}{|z|^2 + 1} \quad , \tag{3.88}$$

$$\frac{\mathrm{Re}\, z'}{|z'|^2 + 1} c(\lambda') = \frac{\mathrm{Re}\, z}{|z|^2 + 1} c(\lambda) \quad , \tag{3.89}$$

$$(p-q)\frac{\mathrm{Im}\, z'}{|z'|^2 + 1} c(\lambda') = \frac{\mathrm{Im}\, z}{|z|^2 + 1} c(\lambda) \quad . \tag{3.90}$$

Expressing the last three relations in terms of n and s, we get the desired relation. This completes the proof of necessity. (Again, note that for the special cases $z' = \pm 1$, the equations do not depend on the precise value of $p - q$.)

For the sufficiency part of the proof, we will argue that the parties consecutively make a deterministic transformation by a local operation to bring the initial state to the

desired final state. Hence, there will be a chain of points $\lambda^{(k)}$

$$\lambda^{(0)} = \lambda \to \lambda^{(1)} \to \lambda^{(2)} \to \cdots \to \lambda^{(p)} = \lambda'$$

where party-k takes the kth turn to change the state point from $\lambda^{(k-1)}$ into $\lambda^{(k)}$. Here, the intermediate points are given as

$$\begin{aligned}
\lambda^{(0)} &= (z^{(0)}; c_1, c_2, c_3, \ldots, c_p) \quad , \\
\lambda^{(1)} &= (z^{(1)}; c_1', c_2, c_3, \ldots, c_p) \quad , \\
\lambda^{(2)} &= (z^{(2)}; c_1', c_2', c_3, \ldots, c_p) \quad , \\
\cdots &\quad \cdots \\
\lambda^{(p)} &= (z^{(p)}; c_1', c_2', c_3', \ldots, c_p') \quad ,
\end{aligned}$$

where $z^{(0)} = z$ and $z^{(p)} = z'$. The kth party essentially increases her cosine from c_k to c_k' while this change is associated by a definite change in the value of the z parameter from $z^{(k-1)}$ to $z^{(k)}$. The latter essentially shifts along a curve, one of the constant s/n curves, by a definite amount. Hence, by finding out the curve that the points z and z' lie, we can easily find the necessary intermediate points $z^{(k)}$. Since all intermediate points have definite n and s values (e.g., $n(z^{(1)}) = n(z)c_1/c_1'$, etc.), there is no problem of finding the values of $z^{(1)}, \ldots, z^{(p-1)}$. Hence, what is left for us is to show that any transition by a single party (say from $\lambda^{(k-1)}$ to $\lambda^{(k)}$ by the kth party) can be carried out. Obviously, we only need to consider the cases for which $c_k' > c_k$ (otherwise, for $c_k' = c_k$, we have $\lambda^{(k-1)} = \lambda^{(k)}$ and no local operation by the kth party is necessary.)

Before going to the actual proof let us note special points and curves on the complex plane. Note that the special values of 0 and ∞ for n or s cannot change in these deterministic transformations. Specifically, these correspond to (a) the real axis, $\mathrm{Im}\, z = 0$, where $s = 0$; (b) the imaginary axis, $\mathrm{Re}\, z = 0$, where $n = 0$; (c) and the unit circle, $|z| = 1$ where $s = \pm\infty$. These are curves that are invariant under deterministic LOCC transformations. Hence, their intersections, specifically $z = \pm 1, \pm i$ need special attention. For example, the points ± 1: These points can *never* appear as a final state, because they have extreme n' values of ± 1 and the relation in part (b) of theorem can never be satisfied except for the trivial case of $\lambda' = \lambda$. However, it will be seen that, the initial value $z = \pm 1$ can be met, while the final z' does not need to be on the unit circle or the real axis.

Now, let us consider the local measurement done by the kth party to transform her state from $\lambda^{(k-1)}$ to $\lambda^{(k)}$. This is a deterministic transformation with two outcomes, but here the outcomes will be denoted as $\pm$ to distinguish it from the notation of the chain. The special cases of interest are

(I) When $z^{(k)}$ and $z^{(k-1)}$ are not on the unit circle, i.e., both $\rho^{(k)}$ and $\rho^{(k-1)}$ are strictly positive (here $z^{(m)} = \exp(\rho^{(m)} + i\theta^{(m)})$.). Using the second parametrization of local operations, the parameters of transformation are

$$p_{\pm} = \frac{1}{2}\left(1 \pm \frac{\tanh \rho^{(k-1)}}{\tanh \rho^{(k)}}\right) \quad , \tag{3.91}$$

$$C_{\pm} = c'_k \quad , \tag{3.92}$$

$$z^{+} = z^{(k)} \quad , \tag{3.93}$$

$$z^{-} = 1/z^{(k)} \quad . \tag{3.94}$$

Now, it is straightforward, but tedious, to check that $p_{\pm}$ are probabilities and the parameters given above satisfy the conditions (3.43) and (3.45). Finally, it is trivial to see that the final state is LU-equivalent to $\lambda^{(k)}$.

(II) Either z or z' are on the unit circle, (in which case both points must be on the unit circle and therefore $\rho^{(k-1)} = \rho^{(k)} = 0$), but both points are different from $\pm 1, \pm i$. In other words, $\theta^{(k-1)}$ and $\theta^{(k)}$ are not an integer multiple of $\pi/2$. In this case, the parametrization above in part I is valid, except that the probabilities should be expressed in terms of the polar angles

$$p_{\pm} = \frac{1}{2}\left(1 \pm \frac{\tan \theta^{(k-1)}}{\tan \theta^{(k)}}\right) \tag{3.95}$$

Here too, it is straightforward, but tedious, to check that this local operation describes the needed transformation.

Now, with I and II, we have handled all cases except the ones where either $z^{(k-1)}$ or $z^{(k)}$ is one of $\pm 1, \pm i$. The remaining special cases are handled below.

(III) The case where either $z^{(k)} = \pm i$ or $z^{(k-1)} = \pm i$. Since the complex numbers $\pm i$ have (n, s) parametrization given by $(n, s) = (0, \pm\infty)$, by part (b) of the current theorem, we cannot leave this point by LOCC transformations. Hence both of the z parameters should be $\pm i$. Moreover, as z parameters of points in Λ, i and

$-i$ correspond to LU-equivalent points. Hence, we can write $z^{(k-1)} = z^{(k)} = i$ without loss of generality. The main idea is that, even though the z parameter does not change, the kth party can increase her cosine for this special case. The parameters of the transformation are given as

$$p_{\pm} = \frac{1}{2}\left(1 \pm \frac{c_k}{c'_k}\right) \quad , \tag{3.96}$$

$$C_{\pm} = c'_k \quad , \tag{3.97}$$

$$z_{\pm} = \pm i \quad . \tag{3.98}$$

(IV) The case where $z^{(k)} = \pm 1$. This final point have an extreme n value of ± 1. Hence, by part (b) of the theorem, the only way this final point is reached is that $z^{(k-1)} = z^{(k)}$ and $c'_k = c_k$. In other words $\lambda^{(k-1)} = \lambda^{(k)}$ and no transformation is needed.

(V) The case where $z^{(k-1)} = \pm 1$. In here we will show that any point in the complex plane, except the imaginary axis is reachable. Note that by part (b) of the theorem, the point $z^{(k)}$ satisfies $n(z^{(k)}) = \pm(c_k/c'_k)$. However, due to the fact that $s(z^{(k-1)})$ does not have a definite value, $s(z^{(k)})$ is arbitrary. Hence, suppose that $z^{(k)}$ is a number on the complex plane such that

$$n(z^{(k)}) = \frac{2\mathrm{Re}\, z^{(k)}}{|z^{(k)}|^2 + 1} = \pm\frac{c_k}{c'_k} \quad . \tag{3.99}$$

Then, the parameters of the local measurement by the kth party in second parametrization are given by

$$p_{\pm} = \frac{1}{2} \quad , \tag{3.100}$$

$$C_{\pm} = c'_k \quad , \tag{3.101}$$

$$z_{+} = z^{(k)} \quad , \tag{3.102}$$

$$z_{-} = \frac{1}{z^{(k)}} \quad . \tag{3.103}$$

Once it is observed that

$$N(\lambda^{(k)}) = 1 + |z^{(k)}|^2 + c'_1 \cdots c'_k c_{k+1} \cdots c_p (2\mathrm{Re}\, z^{(k)}) \quad , \tag{3.104}$$

$$= \left(1 + |z^{(k)}|^2\right)\left(1 + c'_1 \cdots c'_{k-1} c_k c_{k+1} \cdots c_p\, n(z^{(k)})\frac{c'_k}{c_k}\right) \tag{3.105}$$

$$= \left(1 + |z^{(k)}|^2\right)\frac{N(\lambda^{(k-1)})}{2} \tag{3.106}$$

it becomes straightforward to verify that the relations (3.43) and (3.45) are satisfied and the desired final state is produced. □

3.2.4 Transformations from states with vanishing cosines to those without any

Let Λ_M denote the truly multipartite points in Λ. Above, we have been describing the LOCC transformation rule among two points in this set. Specifically, let Λ_{M0} be the set of truly multipartite points with a vanishing cosine. Let, Λ'_{M0} be the set of other truly multipartite points. Theorem 2 describes the LOCC transition rule between points in Λ_{M0} while theorem 3 describes it for points in Λ'_{M0}. What is left is to give the rules of transition between these two sets. It is obvious that no state in Λ'_{M0} can be transformed to one in Λ_{M0} due to the cosine rule of theorem 1. The following theorem handles the transitions from Λ_{M0} into Λ'_{M0}.

Theorem 4. *Let $\lambda = (z; c_1, \ldots, c_p)$ be a state with a vanishing cosine and $\lambda' = (z'; c'_1, \ldots, c'_p)$ be a state having non-zero cosines. The point λ can be transformed into point λ' if and only if*

(a) $c'_k \geq c_k$ for all k,

(b) $|z| = 1$.

(c) z' is purely imaginary.

Proof: Note that by LU-equivalence we can choose z to be real positive with $z \geq 1$ and z' to be satisfying $|z'| \geq 1$. Hence part (b) can be stated as $z = 1$.

For proving the necessity of the conditions, we use the relations (3.81-3.83) again. Moreover, the results (3.87-3.90) are valid as well. Simply use $c(\lambda) = 0$ and $c(\lambda') \neq 0$ in the last two equations. From (3.89) we get $\mathrm{Re}\, z' = 0$. In Eq. (3.90), we use $\mathrm{Im}\, z' = (z'/i) \neq 0$ and then find $p = q$. This then leads to $|z|| = 1$. Finally, part (a) follows from theorem 1.

For proving sufficiency, we make use of theorem 2. Without loss of generality, let us suppose that the first party has vanishing cosine, i.e., $c_1 = 0$. In theorem 2, it is shown that all parties except the first can increase their cosines to any desired value without changing anything else. Hence, the initial state $\lambda = (z; 0, c_2, \ldots, c_p)$ can be transformed into $\tilde{\lambda} = (z; 0, c'_2, \ldots, c'_p)$. Now, at this point, 1st party will do a single measurement and change the state from $\tilde{\lambda}$ into $\lambda' = (z'; c'_1, c'_2, \ldots, c'_p)$. The

needed measurement has two outcomes and the following parameters in the second parametrization

$$p_{\pm} = \frac{1}{2} \quad , \tag{3.107}$$

$$C_{\pm} = c_1' \quad , \tag{3.108}$$

$$z_{+} = z' \quad , \tag{3.109}$$

$$z_{-} = \frac{1}{z'} \quad . \tag{3.110}$$

It is trivial to check that the relations (3.43) and (3.45) are satisfied and the measurement produces the desired final state.□

3.2.5 Invariants under deterministic LOCC transformations

It can be seen that, under *deterministic* LOCC transformations, there are some quantities that remain invariant. One of these is the phase angle of $z - z^{-1}$ modulo π. Another invariant is

$$\frac{N(\lambda)}{1+|z|^2} = 1 + c_1 \cdots c_p n(z) \quad , \tag{3.111}$$

yet another is $c_1 \cdots c_p s(z)$, etc.

Although the deterministic transitions from a given state are allowed only to a restricted set of states, it might be useful to consider also the sets of states that can be transformed into a given state. In that case, the truly multipartite states are separated into various disjoint sets, which will be denoted by M_ξ where ξ is a continuous parameter to be described below. For $\lambda = (z; c_1, \ldots, c_p)$, we say that λ is in set M_ξ if

$$\xi = c_1 c_2 \cdots c_p \, \frac{z + z^*}{1+|z|^2} = c_1 c_2 \cdots c_p \; n(z) = \frac{N(\lambda)}{1+|z|^2} \quad . \tag{3.112}$$

Note that ξ can take on values only in the open interval $(-1, 1)$ for truly multipartite states. This quantity is an invariant of deterministic transformations provided the final state is also truly multipartite. Hence, it is not possible to transform any state in one of these states to another state in another set. (However, it should be noted that if probabilistic transformations are allowed, then it becomes possible to leave these sets.)The class M_0 is specially treated in theorems 2 and 4. Basically M_0 contain those states having vanishing cosines as well as those states having a purely imaginary z parameter. All states in this set can be obtained from a single LU-equivalent class of

"ancestor state", the so-called GHZ state $\lambda_{\mathrm{GHZ}} = (1; 0, 0, \ldots, 0)$, in other words states which are LU-equivalent to

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|0, 0, \ldots, 0\rangle + |1, 1, \ldots, 1\rangle \right) \quad . \tag{3.113}$$

Note that these states correspond to a single point of $\Lambda/\sim$ since all of them are LU-equivalent.

An interesting special subset of M_0 is formed from states with non-zero cosines having a z-parameter equal to $\pm i$, i.e., the set L_i, which is defined as

$$L_i = \{(z; c_1, c_2, \ldots, c_p) : c_1 \cdots c_p \neq 0 \ , \ z = \pm i\} \tag{3.114}$$

Note that L_i is also invariant under deterministic LOCC. If a state in L_i is transformed deterministically to a truly multipartite state, then the final state must be in L_i as well. As a result, only the cosines of the state can be increased in a deterministic transformations. It is not possible to change the z parameter to anything other than $\pm i$. (Obviously, this conclusion does not hold if the final state is bipartite entangled.)

The sets M_ξ for $\xi \neq 0$ do contain infinitely many LU-equivalence classes of "ancestor states". These ancestor states are those members of M_ξ that has a z parameter equal to $+1$ (if $\xi > 0$) or -1 (if $\xi < 0$), i.e.,

$$A_\xi = \{(\operatorname{sgn} \xi; c_1, c_2, \ldots, c_p) \in \Lambda_M : c_1 c_2 \cdots c_p = |\xi|\} \quad . \tag{3.115}$$

These states cannot be obtained deterministically from any other rank-2 state. However, they are all ancestors of states in M_ξ, i.e., any state in M_ξ can be obtained from one of these ancestors. Moreover, any non-ancestor state can be obtained from an infinite number of ancestors. Because of this many-to-many relationship of LOCC-convertibility, the set M_ξ forms a single connected whole.

CHAPTER 4

CONCLUSION

In this thesis we mainly concentrated on the deterministic transformations of pure multipartite states having rank-2. These pure multipartite states are described as points in $\Lambda - space$ in terms of the complex parameters z and cosines. Using this new parametrization description of product, bipartite and truly multipartite states and the rules LU- equivalence between them are given.

Local operations of parties are described in terms of the general measurements. In this way measurement done by the single party is parameterized and probabilities for the measurement outcomes are identified. It is seen that this parametrization depends on cosine of the initial state and cosines of the other parties is not affected by local measurement of a single party. When two possible outcomes produce the same points in $\Lambda - space$, one can choose to construct a new local operation where these two outcomes appear as a single outcome.

As a minor application of the parametrization of states and local operations, we investigate some aspects of LOCC conversion phenomenon. If the initial state is a product state, then obviously there is nothing to be done. If the state is bipartite entangled between k and another party, then this can be done with certainty. Also, if k is unentangled from the rest, then success probability is 0. Then, excluding these special cases, we considered an arbitrary truly multipartite state.

In deterministic transformations of states by many parties, it is seen that possible final states are the same state up to LU equivalence and after every possible chain of local operations, all final states are described as an LU-equivalent point in $\Lambda - space$.

In the case of deterministic transformation into states with vanishing cosine, same

parties should have vanishing cosines. It is seen that, in LOCC conversion, any party other than the 1st one, can increase their own cosine parameter to any desired value without regarding the order of these local operations are immaterial and the 1st party increases only the modulus of z parameter.

An alternative parametrization of complex numbers is given in describing transformations from states with non-zero cosines and with vanishing cosines to those without any, requiring both states to be truly multipartite and LU-equivalent.

The quantities which are under deterministic LOCC transformations is identified. These quantities are used to describe disjoint sets and the truly multipartite states are separated into the sets in deterministic transitions.

Besides the deterministic transitions from a given state to a restricted set of states, we considered the sets of states that can be transformed into a given state and showed that the truly multipartite states are separated into various disjoint sets. It is shown that transforming any state in one of these states to another state in another set is not possible. Among the infinitely many equivalence classes of ancestor states, those states in which only the cosines of the state can be increased in a deterministic transformations is described.

The deterministic LOCC convertibility problem for rank-2 states have not been completely solved obviously, because there is nothing known about the transformation of truly multipartite states into bipartite states. There is nothing known also about the probabilistic transformations. But, probably the approach taken above, i.e., parameterizing the states and subsequently parameterizing the local operations as above might prove useful for these problems as well.

Following the results of this thesis about the nature of the entanglement and its transformations, we will continue to extend this work to find the possible applications in encoding quantum information.

Since the mixed states are the ensembles of pure states, our approach to the entanglement purification is based on the connection of entanglement, namely entanglement

swapping, for pure states in the application of quantum information and computation. Instead of thinking the transformations of the Bell states with vanishing cosines, we considered the multipartite entangled states in terms of the parametrization of complex numbers and investigated the transformations with non-zero cosines. We investigate the way of bringing the initial state to desired final state by a chain of local operations in a deterministic manner. In terms of these states we will try to reach the schemes of encoding quantum information in quantum repeaters for a long distance quantum communication networks [107]. A technical chapter which sets necessary tools for this future works is given in the appendices. The quantum repeaters may be chosen as hybrid quantum repeaters which contains both discrete and continuous variables.

The connection between entanglement and quantum codes is established in two ways depending on the nature of the physical resource in communication and computation. First is the way in which we use physical qubits as logical qubits, and in the second we use entanglement transformations as physical resource in quantum communication and computation.

As an application of this thesis, we will use entanglement as resource for the quantum informational tasks and study entanglement-assisted quantum error-correcting codes (EAQECC). Since, it is possible to construct an EAQECC from any classical linear code, we will use classical linear codes to find good quantum codes in the needs of particular applications. In the hybrid construction of quantum codes such as quantum code that can transmit both classical and quantum information at the same time, we will try to reach a non-binary stabilizer state and Qudit Stabilizer States constructions of quantum codes. Besides the classical linear codes, we will try to use Quantum Codes From Algebraic Geometry Codes in EAQECC applications.

Concerning the relation between entanglement transformations and quantum codes, we considered the ability of a single party to obtain a product state. Since product states are obtained from entangled states by destroying entanglement, the question we tried to answer is "what a single party can do if she wants to destroy the entanglement?". Besides the parametrization of states, we also use the parametrization of the local measurements. Then, we obtained the conditions of success probability of

LOCC conversion into product states is being unity.

Using the mapping between The one-way quantum computer model(1WQC) and Teleportation-based quantum computer (TQC) we will use quantum encoding schemes to use unified derivations of measurement-based schemes for quantum computational and informational tasks. In this way, Construction of graph states will be important tool.

Rank-Two entanglement transformations with or without raising the rank of the multipartite states to higher orders stand as a bridge between quantum informational tasks and quantum codes. In this respect, this study will be helpful in rendering the description of computational and informational processes more physical.

REFERENCES

[1] P.A.Benioff,Quantum Mechanical Models of Turing Machines That Dissipate No Energy , Phys. Rev. Lett. 48, 1581 (1982)..

[2] R. P. Feynman, Simulating Physics with Computers, *Int. J. Theor. Phys.* **21**, 467 (1982).

[3] D. Deutsch, Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer, *Proc. R. Soc. Lond. A* **400**, 97 (1985).

[4] R. Landauer,Irreversibility and heat generation in the computing process ,IBM J. Res. Dev. 5, 183 (1961).

[5] C. H. Bennett, Logical Reversibility of Computation, *IBM J. Res. Develop.* **17**, 525 (1973).

[6] P.W. Shor, *Proceedings of the* 35^{th} *Annual Symposium on The Fundamentals of Computer Science*, Los Alamitos, IEEE Press (1994)

[7] L. Grover, *Proceedings of the* 28^{th} *Annual Symposium on The Theory of Computing*, (NY: ACM Press), pp 212 (1996)

[8] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P.W. Shor, T. Sleator, J. Smolin and H. Weinfurter, "Elementary gates for quantum computation" *Phys.Rev. A*, **52**, 3457 (1995)

[9] A. Galindo and M. A. Martı´n-Delgado,Information and computation: Classical and quantum aspects, Rev. Mod. Phys. 74 347(2002)

[10] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, New York (2000).

[11] G. Benenti and G. Casati, Gi. Strini *Principles of quantum computation and information* , World Scientific Pub.,Singapore ; River Edge, NJ (2004).

[12] M.O. Scully and M.S. Zubairy "Quantum Optics", Cambridge University Press, Cambridge, (1997)

[13] J.J. Sakurai, *Modern Quantum Mechanics*, Addsison-Wesley Publishing Company (1993)

[14] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?",*Phys. Rev.* **47**, 777, (1935)

[15] N. Bohr, Can Quantum Mechanical Description of Physical Reality be Considered Complete?, *Phys. Rev.* **48**, 696 (1935).

[16] E. Schrödinger, "Discussion of probability relations between separated systems", *Proc. Cambridge Philos. Soc.* **31**, 555 (1935)

[17] E. Schrödinger, "Probability relations between separated systems", *Proc. Cambridge Philos. Soc.* **32**, 446 (1936)

[18] J.S. Bell, "On the Problem of Hidden Variables in Quantum Mechanics", *Rev. Mod. Phys.* **38**, 447, (1966)

[19] J. Clauser, M. Horne, A. Shimony, and R. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories" *Phys. Rev. Lett.* **23**, 880 (1969)

[20] J.S. Hodges, P. Cappellaro, T. F. Havel, R. Martinez, and D. G. Cory "Experimental implementation of a logical Bell state encoding" *Phys. Rev. A* **75**, 042320 (2007)

[21] D.N. Mermin, "What is quantum mechanics trying to tell us?", *Am. J. Phys.* **66**, 753 (1998)

[22] A. Peres, "Collective tests for quantum nonlocality" *Phys. Rev. A* **54**, 2685, (1996)

[23] C.H. Bennett, G. Brassard, C. Crepeau, R. Josa, A. Peres, and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev Lett.* **70**, 1895, (1993)

[24] W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot be Cloned", *Nature* **299**, 802 (1982)

[25] C.H. Bennett and G. Brassard in *Proc. IEEE Int. Conf. Computers. Systems and Signaling Processes* (1984)

[26] C.H. Bennett and P.W.Shor, "Quantum Information Theory", *IEEE Trans. Inform. Theory* **44**, 2724 (1998)

[27] B. Schumacher "Quantum Coding", *Phys. Rev. A* **51**, 2738 (1995)

[28] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, andW.Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, *Phys. Rev. Lett.* **76**, 722 (1996).

[29] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations" *Phys. Rev A* **53**, 2046, (1996)

[30] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed-state entanglement and quantum error correction" *Phys. Rev A* **54**, 3824, (1996)

[31] V. Coffman, J. Kundu, and W.K. Wooters, "Distributed Entanglement", *Phys. Rev.A* **61**, 052306 (2000)

[32] S. Hill and W. K. Wootters,"Entanglement of a Pair of Quantum Bits" *Phys. Rev. Lett.* **78**, 5022 (1997)

[33] W. K. Wootters, "Entanglement of Formation of an Arbitrary State of Two Qubits" *Phys. Rev. Lett.* **80**, 2245 (1998)

[34] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying Entanglement, Phys. Rev. Lett. 78, 2275 (1997).

[35] V. Vedral andM. Plenio, EntanglementMeasures and Purification Procedures, Phys. Rev. A 57, 1619 (1998).

[36] N. Linden, S.Massar, and S. Popescu, Purifying Noisy Entanglement Requires Collective Measurements, Phys. Rev. Lett. 81, 3279 (1998).

[37] N. Linden and S. Popescu, On Multi-Particle Entanglement, Fortsch. Phys. 46, 567 (1998).

[38] G. Vidal, Entanglement Monotones, J. Mod. Opt. 47, 355 (2000).

[39] M. Horodecki, P. Horodecki, and R. Horodecki, "Inseparable Two Spin-1/2 Density Matrices Can Be Distilled to a Singlet Form" *Phys. Rev. Lett.* **78**, 574 (1997)

[40] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a Bound Entanglement in Nature, Phys. Rev. Lett. 80, 5239 (2000).

[41] M. A. Nielsen, Conditions for a Class of Entanglement Transformations, Phys. Rev. Lett. 83, 436 (1999).

[42] G. Vidal, Entanglement of Pure States for a Single Copy, Phys. Rev. Lett. 83, 1046 (1999).

[43] G. Vidal, D. Jonathan, and M. A. Nielsen, Approximate Transformations and Robust Manipulation of Bipartite Pure State Entanglement, Phys. Rev. A 62, 012304 (2000).

[44] D. Jonathan and M. B. Plenio, Minimal Conditions for Local Pure-State Entanglement Manipulation, Phys. Rev. Lett. 83, 1455 (1999).

[45] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, quant-ph/9908073.

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

[47] A. Acin, E. Jane, W. Dür, and G. Vidal, Optimal Distillation of a Greenberger-Horne-Zeilinger State, Phys. Rev. Lett. 85, 4811 (2000).

[48] Deutsch D., Ekert A., Jozsa R., Macchiavello C., Popescu S. and Sanpera A. ,Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels, Phys. Rev. Lett. 77 2818 (1996)

[49] Pan J-W., Simon C., Brukner C. and Zeilinger A., Entanglement purification for quantum communication, Nature 410 1067 (2001).

[50] Kwiat P G, Barraza-Lopez S., Stefanov A. and Gisin N. ,Experimental entanglement distillation and 'hidden' non-locality, Nature 409 1014 (2001).

[51] Pan J-W., Gasparoni S., Ursin R., Weihs G. and Zeilinger A.,Experimental entanglement purification of arbitrary unknown states, Nature 423 417 (2003).

[52] Yamamoto T., Koashi M., Ö zdemir S. K. and Imoto N.,Experimental extraction of an entangled photon pair from two identically decohered pairs, Nature 421 343 (2003).

[53] Resch K. J., Walther P., Brukner C., Steinberg A. M., Pan J-W. and Zeilinger A., Quantum Nonlocality Obtained from Local States by Entanglement Purification, Phys. Rev. Lett. 94 040504 (2005).

[54] Reichle R., Leibfried D., Knill E., Britton J., Blakestad R. B., Jost J. D., Langer C., Ozeri R., Seidelin S. and Wineland D. J., Experimental purification of two-atom entanglement, Nature 443 838 (2006).

[55] Zukowski M., Zeilinger A., Horne M. A. and Ekert A.,"Event-ready-detectors" Bell experiment via entanglement swapping, Phys. Rev. Lett. 71 4287 (1993).

[56] Bose S., Vedral V. and Knight P. L.,Multiparticle generalization of entanglement swapping, Phys. Rev. A 57 822 (1998).

[57] Pan J-W., Bouwmeester D., Weinfurter H. and Zeilinger A.,Experimental Entanglement Swapping: Entangling Photons That Never Interacted, Phys. Rev. Lett. 80 3891 (1998).

[58] de Riedmatten H., Marcikic I., van Houwelingen J. A. W., Tittel W., Zbinden H. and Gisin N., Long-distance entanglement swapping with photons from separated sources, Phys. Rev. A 71 050302 (2005).

[59] Briegel H-J., Dür W, Cirac J I and Zoller P., Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. 81 5932 (1998).

[60] Dür W., Briegel H-J., Cirac J. I. and Zoller P.,Quantum repeaters based on entanglement purification, Phys. Rev. A 59 169 (1999).

[61] Childress L., Taylor J M., Sorensen S. A. and Lukin M. D. ,Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters, Phys. Rev. A 72 052330 (2005).

[62] Childress L., Taylor J. M., Sorensen A. S. and Lukin M. D. Phys. Rev. Lett. ,Fault-Tolerant Quantum Communication Based on Solid-State Photon Emitters, 96 070504 (2006).

[63] Hartmann L., Kraus B., Briegel H-J. and Dür W. ,Role of memory errors in quantum repeaters, Phys. Rev. A 75 032310 (2007).

[64] Enk S J., Cirac J. I. and Zoller P. ,Photonic Channels for Quantum Communication, Science 279 205 (1998).

[65] Duan L-M., Lukin M. D., Cirac J. I. and Zoller P. ,Long-distance quantum communication with atomic ensembles and linear optics, Nature 414 413 (2001).

[66] Klein A., Dorner U., Moura Alves C. and Jaksch D.,Robust implementations of quantum repeaters, Phys. Rev. A 73 012332 (2006).

[67] Simon C., de Riedmatten H., Afzelius M., Sangouard N., Zbinden H. and Gisin N. ,Quantum Repeaters with Photon Pair Sources and Multimode Memories, Phys. Rev. Lett. 98 190503 (2007).

[68] Dür W. and Cirac J. I. ,Nonlocal operations: Purification, storage, compression, tomography, and probabilistic implementation, Phys. Rev. A 64 012317 (2001)

[69] Gottesman D., The Heisenberg Representation of Quantum Computers, Preprint quant-ph/9807006 (1998)

[70] Gottesman D. and Chuang I. L. ,Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature 402 390 (1999).

[71] Eisert J., Jacobs K., Papadopoulos P. and Plenio M. B. ,Optimal local implementation of nonlocal quantum gates, Phys. Rev. A 62 052317 (2000)

[72] Dür W, Aschauer H and Briegel H-J. ,Multiparticle Entanglement Purification for Graph States, Phys. Rev. Lett. 91 107903 (2003).

[73] Aschauer H, Dür W. and Briegel H-J. ,Multiparticle entanglement purification for two-colorable graph states, Phys. Rev. A 71 012319 (2005).

[74] Kruszynska C, Miyake A, Briegel H-J. and Dür W. ,Entanglement purification protocols for all graph states, Phys. Rev. A 74 052316 (2006).

[75] Raussendorf R, Browne D and Briegel H-J. ,Measurement-based quantum computation on cluster states, Phys. Rev. A 68 022312 (2003).

[76] Briegel H-J and Raussendorf R. ,Persistent Entanglement in Arrays of Interacting Particles, Phys. Rev. Lett. 86 910 (2001).

[77] Raussendorf R and Briegel H-J.,A One-Way Quantum Computer, Phys. Rev. Lett. 86 5188 (2001).

[78] Raussendorf R and Harrington J. ,Fault-Tolerant Quantum Computation with High Threshold in Two Dimensions, Phys. Rev. Lett. 98 190504 (2007).

[79] P. W. Shor, Scheme for reducing decoherence in quantum memory Phys. Rev. A 52 , 2493 (1995).

[80] E. Knill and R. Laflamme, A theory of quantum error-correcting codes, Phys. Rev. A 55 900 (1997).

[81] D. Gottesman, A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound. Phys. Rev. A 54 1862(1996).

[82] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist. Phys. Rev. A, 54 1098 (1996).

[83] A. Steane, Error Correcting Codes in Quantum Theory. Phys. Rev. Letters, 77 (5): 793 (1996).

[84] A. Steane, Multiple Particle Interference and Quantum Error Correction. Proc. Roy. Soc. London A, 452: 2551 (1996).

[85] D. P. DiVincenzo and P. W. Shor, Fault-Tolerant Error Correction with Efficient Quantum Codes. Phys. Rev. Lett., 77 3260 (1996).

[86] D. P. DiVincenzo. Quantum Gates and Circuits. Phil. Trans. Royal Soc. London A, 454:261 (1998).

[87] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory 47 3065 (2001).

[88] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, Asymptotically good quantum codes, Phys. Rev. A 63 032311 (2001).

[89] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, vol. 44, 1369 (1998).

[90] E. M. Rains, Nonbinary quantum codes, IEEE Trans. Inform. Theory 45 1827 (1999).

[91] A. M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes. IEEE Trans. Inform. Theory 45 2492 (1999).

[92] H. Chen, Some good quantum error-correcting codes from algebraic geometric codes, IEEE Trans. Inform. Theory, 47 2059 (2001).

[93] H. Chen, S. Ling, and C. Xing, Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, IEEE Trans. Inform. Theory, 47 2055 (2001).

[94] K. Feng and Z. Ma, A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, IEEE Trans. Inform. Theory, vol. 50 3323(2004).

[95] J.-L. Kim and J. L. Walker, Nonbinary quantum error-correcting codes from algebraic curves, Discrete Math. 308 3115 (2008).

[96] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary Stabilizer Codes over Finite Fields IEEE Transactions on Information Theory, Volume 52, Issue 11, pages 4892 - 4914, (2006).

[97] P. K. Sarvepalli and A. Klappenecker, Nonbinary quantum codes from Hermitian curves, Applied algebra, algebraic algorithms and error-correcting codes, 136, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.

[98] M. Grassl, W. Geiselmann, and Th. Beth, Quantum Reed-Solomon codes, Applied algebra, algebraic algorithms and error-correcting codes 231 Lecture Notes in Comput. Sci., 1719, Springer, Berlin, 1999.

[99] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. dissertation, California Inst. of Technol., Pasadena, CA, 1997.

[100] R. Matsumoto, Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, IEEE Trans. Inform. Theory 48 2122(2002).

[101] Ambainis A and Gottesman D 2003 Preprint quant-ph/0310097

[102] Matsumoto R 2002 Preprint quant-ph/0209091

[103] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane.,Quantum Error Correction and Orthogonal Geometry, Phys. Rev. Lett. 78 405 (1996)

[104] Frank Gaitan, *Quantum Error Correction and and Fault Tolerant Quantum Computing*, CRC Press, New York (2008)

[105] Dan C. Marinescu and Gabriela M. Marinescu, *Quantum Information and Error Correction From Classical to Quantum Concepts.* online:http://www.cs.ucf.edu/ dcm/QCV2.pdf

[106] K. Feng,Quantum Error-Correcting Codes. Coding theory and cryptology / editor, Harald Niederreiter. Singapore : Singapore University Press ; River Edge, NJ : World Scientific, c2002

[107] Liang Jiang, J. M. Taylor, Kae Nemoto, W. J. Munro, Rodney Van Meter, and M. D. Lukin.,Quantum repeater with encoding, Phys. Rev. A 79 032325 (2009).

[108] Isaac Kremsky, Min-Hsiu Hsieh, Todd A. Brun.,Classical enhancement of quantum-error-correcting codes, Phys. Rev. A 78 012341 (2008)

[109] Xie Chen, Bei Zeng and Isaac L. Chuang.,Nonbinary codeword-stabilized quantum codes, Phys. Rev. A 78 062315 (2008)

[110] Dür W, Briegel H-J.,Entanglement purification and quantum error correction,Rep. Prog. Phys. 70 1381 (2007).

APPENDIX A

TENSOR PRODUCTS

A.1 Representing Composite States in Quantum Mechanics

In quantum mechanics, some of which are seen in the context of quantum information processing, it is necessary to work with multi-particle states.

Suppose that H_1 and H_2 are two Hilbert spaces of dimension N_1 and N_2. We can put these two Hilbert spaces together to construct a larger Hilbert space. We denote this larger space by H and use the tensor product operation symbol $\otimes$. Then we write

$$H = H_1 \otimes H_2 \tag{A.1}$$

where the dimension of the larger space becomes

$$dim(H) = dim(H_1)dim(H_2) = N_1 N_2 \tag{A.2}$$

Now, let $|\phi\rangle \in H_1$ and $|\varphi\rangle \in H_2$ then $|\psi\rangle \in H$ is constructed as

$$|\psi\rangle = |\phi\rangle \otimes |\varphi\rangle \tag{A.3}$$

and it satisfies the linearity. That is,

$$|\psi\rangle \otimes [|\varphi_1\rangle + |\varphi_2\rangle] = |\phi\rangle \otimes |\varphi_1\rangle + |\phi\rangle \otimes |\varphi_2\rangle \tag{A.4}$$

and

$$|\phi\rangle \otimes (\alpha|\varphi\rangle) = \alpha|\phi\rangle \otimes |\varphi\rangle. \tag{A.5}$$

The inner product of two vectors belonging to the larger Hilbert space H is given for

$$\begin{aligned} |\psi_1\rangle &= |\phi_1\rangle \otimes |\varphi_1\rangle \\ |\psi_2\rangle &= |\phi_2\rangle \otimes |\varphi_2\rangle \end{aligned} \tag{A.6}$$

as

$$\langle\psi_1|\psi_2\rangle = (\langle\phi_1| \otimes \langle\varphi_1|)(|\phi_2\rangle \otimes |\varphi_2\rangle) = \langle\phi_1|\phi_2\rangle\langle\varphi_1|\phi_2\rangle \tag{A.7}$$

A.2 Operators and Tensor products

Let A is an operator and acts on $|\phi\rangle \in H_1$ and B is another operator acting on $|\phi\rangle \in H_2$. then we can create an operator $A \otimes B$ acting on $|\phi\rangle \in H$ as follows

$$(A \otimes B)|\psi\rangle = (A \otimes B)(|\phi\rangle \otimes |\varphi\rangle) = (A|\psi\rangle) \otimes (B|\phi\rangle). \tag{A.8}$$

Expressing the operators in terms of the matrices we can define tensor products of matrices. Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}. \tag{A.9}$$

and

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}. \tag{A.10}$$

Then

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}. \tag{A.11}$$

APPENDIX B

QUANTUM CODES

B.1 Quantum Information and Error Correction

In quantum information theory, classical bits are replaced by their quantum analaog called qubit [10] which is in the form

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle \tag{B.1}$$

where the normalization condition $|\alpha|^2 + |\beta|^2 = 1$ implies the conservation of probability.

Representing Qubit as a vector in $\mathbb{C}^2$ lead us to express larger alphabets such as $\mathbb{F}_q$ where $q = p^m$ and p is prime [106]. As an information unit Qubit corresponds to $q = 2$ and for $q > 2$ information unit is called as qudit and described as

$$|v\rangle = \sum_{a_0,..a_{n-1}\epsilon\mathbb{F}_2^n} c_{a_0,...a_{n-1}}|a_0,...a_{n-1}\rangle = \sum_{a\epsilon\mathbb{F}_2^n} c_a|a\rangle \tag{B.2}$$

where n-qubit system can be represented as the n-fold tensor product of the form

$$(\mathbb{C}^q)^n = \mathbb{C}^q \otimes .... \otimes \mathbb{C}^q = \mathbb{C}^{q^n} \tag{B.3}$$

Using this representation we define the quantum code
Definition: A quantum code Q the subspace of $(\mathbb{C}^q)^n = \mathbb{C}^{q^n}$ with the length n and $K = dim_{\mathbb{C}}Q$ for $k = \log_2 K \leq n$

Unlike classical coding theory where adding redundancy to codes in error detection and correction by repetition, this repetition is impossible in the computational pro-

cesses of quantum computer stated in following theorems.

Theorem 1.(No-Cloning Theorem)[104,99] It is impossible to find a quantum operation that copy the state $|\psi\rangle$to $|\psi\rangle \otimes |\psi\rangle$ for any state $|\psi\rangle$.

Proof: To prove the theorem we will assume the existence of such an quantum operation and come to a contradiction at the end of the proof. For a given $|\psi\rangle \neq |\phi\rangle$ the process of copying is implied by $|\psi\rangle \rightarrow |\psi\rangle and |\phi\rangle \rightarrow |\phi\rangle$ then for the superposition of them

$$|\psi\rangle + |\phi\rangle = |\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle \tag{B.4}$$

But in the theorem its argued that

$$|\psi\rangle + |\phi\rangle = (|\psi\rangle + |\phi\rangle|)(|\psi\rangle + |\phi\rangle|) \tag{B.5}$$

which leads a contradiction since

$$|\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle \neq (|\psi\rangle + |\phi\rangle|)(|\psi\rangle + |\phi\rangle|) \tag{B.6}$$

Theorem 2.(Distinguishing Quantum States)[104,99] For a given non-orthogonal quantum state it is impossible to distinguishes them unambiguously.

Proof: Let M be a Hermitian operator associated with eigenvalues m_i and projection operators P_i which allow us to distinguishes two non-orthogonal states $|\psi_a\rangle$ and $|\psi_b\rangle$. Then

$$\langle\psi_a|P_\alpha|\psi_a\rangle = \langle\psi_b|P_\beta|\psi_b\rangle = 1 \tag{B.7}$$

and

$$\langle\psi_a|P_\beta|\psi_a\rangle = \langle\psi_b|P_\alpha|\psi_b\rangle = 0 \tag{B.8}$$

By the assumption $|\psi_a\rangle$ and $|\psi_b\rangle$ are non-orthogonal we can write

$$|\psi_b\rangle = c|\psi_a\rangle + d|\varphi\rangle \tag{B.9}$$

where the normalization condition $|c|^2 + |d|^2 = 1$ and $|\varphi\rangle$ and $|\psi_a\rangle$ are orthogonal to each other. Using

$$\langle\psi_b|P_\beta|\psi_b\rangle = |d|^2\langle\phi|P_\beta|\phi\rangle \tag{B.10}$$

we obtain

$$\langle\psi_b|P_\beta|\psi_b\rangle \leq |d|^2 \tag{B.11}$$

and the condition (7) is satisfied only for $|d|^2 = 1$ which requires $|\psi_b\rangle = |\varphi\rangle$ saying the two states must be orthogonal contradicting our assumption that they are non-orthogonal.

These previous two no-go theorem act as guide in constructing quantum codes. To construct Quantum Error Correcting Codes, adding redundancy without cloning and protecting quantum registers against noise from environment are the two basic issues. Redundancy is simply obtained by direct product of the single-qubit computational basis states and the encoding operation is denoted as $\xi : H_2^k \rightarrow H_2^n$ where H_2^k is the unencoded k-qubit Hilbert space and H_2^n is the encoded n-qubit space which is also identified as the image space C_q just as the classical case. As an example $|\bar{0}\rangle$ is the encoded image of $|0\rangle$ and $|\overline{011}\rangle$ is the encoded image of $|011\rangle$ where r=n-k isthe redundancy added to the quantum codes.

Second theorem plays a central role in analysis of errors on quantum registers due to the interactions with environment. The effect of the environment is described by the trace preserving quantum operation withe error operators E_a. Now let us take quantum register is encoded to two distinct computational basis $|\bar{i}\rangle$ and $|\bar{j}\rangle$ and two different error operators act such a way that $E_a|\bar{i}\rangle$ and $E_b|\bar{j}\rangle$ where the image of one codeword is not easily distinguishable with another one. Using the second theorem,the encoded quantum registers $|\bar{i}\rangle$ and $|\bar{j}\rangle$ should satisfy the condition

$$\langle\bar{i}|E_a^\dagger E_b|\bar{j}\rangle = 0(\bar{i} \neq \bar{j}) \tag{B.12}$$

for the error operators E_a, E_b should be correctable. Since the state are disturbed by the measurement, a quantum operation doing measurement on quantum registers is not allowed for error correction. Instead of taking taking two different computational basis, if we look at the two error operator in the same computational basis in which the need to distinguish the error will disappear and we obtain the condition for the codeword C_q to satisfy

$$\langle\bar{i}|E_a^\dagger E_b|\bar{i}\rangle = \langle\bar{j}|E_a^\dagger E_b|\bar{j}\rangle. \tag{B.13}$$

In other words this condition can be expressed as the environment is unaware of distinguish the encoded computational states. In terms of the codeword basis $|c\rangle \epsilon C_q$ it is written as

$$\lambda_{ab} = \langle \bar{i}|E_a^\dagger E_b|\bar{i}\rangle = \langle c|E_a^\dagger E_b|c\rangle \tag{B.14}$$

and the necessary and sufficient conditions to have an quantum error correcting codes are given by this three conditions.

Definition: Number of qubits where E is not the identity is called the quantum weight $wt(E)$ of an error.

Following this definition we describe the distance of a q-ary quantum code C_q of the length n as [104,105]

$$d = max\{d : \langle u|v\rangle = 0, wt(E) \leq d-1 \Rightarrow \langle u|E|v\rangle = 0\} \tag{B.15}$$

Using these parameters we describe a q-ary quantum code of length n, dimension k, and the minimum distance d by $[[n,k,d]]_q$ and two properties of them:

1. An $[[n,k,d]]_q$ code is pure iff $wt(E) \leq d-1 \Rightarrow \langle u|E|v\rangle = 0$

2.An $[[n,k,d]]_q$ code is non-degenerate iff $wt(E) \leq d-1 \Rightarrow |u\rangle$ and $E|v\rangle$ are linearly independent.

B.2 Error Group and Stabilizer States

There are three basic errors also called Pauli errors [10] acting on a qubit

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle \tag{B.16}$$

such that

$$I = \sigma_I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_I|v\rangle = \alpha|0\rangle + \beta|1\rangle \tag{B.17}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_x|v\rangle = \beta|0\rangle + \alpha|1\rangle \tag{B.18}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_z|v\rangle = \alpha|0\rangle - \beta|1\rangle \tag{B.19}$$

$$\sigma_y = i\sigma_x\sigma_z = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_y|v\rangle = -i\beta|0\rangle + i\alpha|0\rangle \tag{B.20}$$

where there are the relations among them below

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I, \sigma_x\sigma_z = -\sigma_z\sigma_x \tag{B.21}$$

A quantum error operation acting on $(\mathbb{C}^2)^{\otimes n}$is given by [104,106]

$$e = i^\lambda w_0 \otimes w_1 \otimes .... \otimes w_{n-1} \tag{B.22}$$

where $i = \sqrt{-i}$, $\lambda = 0, 1, 2, 3$, $w_j \epsilon \{I, \sigma_x, \sigma_y, \sigma_z\}$, $(0 \leq j \leq n-1)$ and its action on a basis element $|a\rangle = |a_0\rangle \otimes |a_1\rangle \otimes ... \otimes |a_{n-1}\rangle$ where $(a = a_0, .a_{n-1} \epsilon \mathbb{F}_2^n)$ is described by

$$e|a\rangle = i^\lambda (w_0|a_0\rangle) \otimes (w_0|a_0\rangle) \otimes ... \otimes (w_{n-1}|a_{0n-1}\rangle) \tag{B.23}$$

The set of quantum error operators

$$E_n = \{i^\lambda w_0 \otimes .. \otimes w_{n-1} | 0 \leq \lambda \leq 3, w_j \epsilon \{I, \sigma_x, \sigma_y, \sigma_z\}, 0 \leq j \leq n-1\} \tag{B.24}$$

is a finite non-Abelian group.

In this way n-qubit error basis is transformed into Pauli group G_n which is a multiplicative group by allowing to multiply E_n with -1 and $\pm i$. The weight of an operator E_n is defined the number of qubits where $w_j \neq I_j$.

Definition:The 1-qubit Pauli group G_1 is given by

$$G_1 = \{\pm\sigma_I, \pm i\sigma_I, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\} \tag{B.25}$$

Definition: A set of elements $\langle g_1, g_2 ... g_m\rangle$ is called the generator of the group G if the element g_i can be written as a product of (elements from the list $\langle g_1, g_2 ... g_m\rangle$. We

write G = $\langle g_1, g_2 ... g_m \rangle$.

Example:The generators of G_1 are

$$G_1 = \langle \sigma_x, \sigma_z, \sigma_I \rangle \tag{B.26}$$

and every element of G_1 is expressed as the product of the generators

$$\begin{aligned} +\sigma_I &= i\sigma_I i\sigma_I i\sigma_I i\sigma_I \\ -\sigma_I &= i\sigma_I i\sigma_I \\ -i\sigma_I &= i\sigma_I i\sigma_I i\sigma_I \end{aligned} \tag{B.27}$$

$$\begin{aligned} -\sigma_x &= i\sigma_I i\sigma_I \sigma_x \\ +i\sigma_x &= i\sigma_I \sigma_x \\ -i\sigma_x &= i\sigma_I i\sigma_I i\sigma_I \sigma_x \end{aligned} \tag{B.28}$$

$$\begin{aligned} +\sigma_y &= i\sigma_I \sigma_x \sigma_z \\ -\sigma_y &= i\sigma_I i\sigma_I \sigma_x \sigma_z \end{aligned} \tag{B.29}$$

$$\begin{aligned} +i\sigma_y &= i\sigma_I i\sigma_I \sigma_x \sigma_z \\ -i\sigma_y &= i\sigma_I i\sigma_I i\sigma_I \sigma_x \sigma_z \end{aligned} \tag{B.30}$$

$$\begin{aligned} -\sigma_z &= i\sigma_I i\sigma_I \sigma_z \\ +i\sigma_z &= i\sigma_I \sigma_z \\ -i\sigma_z &= i\sigma_I i\sigma_I i\sigma_I \sigma_z \end{aligned} \tag{B.31}$$

Definition: The n-qubit Pauli group consists of all 4^n tensor products of $\sigma_I, \sigma_x, \sigma_y, \sigma_z$ and overall phases of ± 1 and $\pm i$.

Any error in the the Pauli group can be written as [104]

$$e = i^{\lambda} \sigma_{j_1}^1 \otimes .... \otimes \sigma_{j_n}^n \tag{B.32}$$

where $\lambda = 0, 1, 2, 3$, $\sigma_{j_k}^k$ denotes the qubit $k = 1..n$, $j_k = 0, x, y, z$. Using the relation $\sigma_y^k = -i\sigma_x^k\sigma_z^k$ the error operator () takes the form

$$e = i^{\lambda'}\sigma_x(a)\sigma_z(b) \tag{B.33}$$

where $a = a_1...a_n$ and $b = b_1...b_n$ and

$$\sigma_x(a) \equiv (\sigma_x^1)^{a_1} \otimes ... \otimes (\sigma_x^n)^{a_n}, \tag{B.34}$$

$$\sigma_z(b) \equiv (\sigma_z^1)^{b_1} \otimes ... \otimes (\sigma_z^n)^{b_n}. \tag{B.35}$$

The center of the group G_n is given by $C = \{\pm I, \pm iI\}$and each coset $eC = \{\pm e, \pm ie\}$ is taken as the single error

Theorem: [104]
1. The orders of G_n and G_n/C are $|G_n| = 2^{2n+2} = 4^{n+1}$ and $|G_n/C| = 2^{2n}$.
2. For all $e\epsilon G_n$, $(a)e^2 = I$; $(b)e^\dagger = \pm e$, $(c)e^{-1} = e^\dagger$
3. For all $e, f\epsilon G_n$, either $[e, f] = 0 or \{e, f\} = 0$.

Proof:(1) Total numbers of errors in G_n is obtained as $4 \times 2^n \times 2^n$ where 4 comes from the four values of $i^{\lambda'}$ and for each a and b strings there are 2^n possible case leading $|G_n| = 4^{n+1}$. Since eC is a single error one can ignore the factor $i^{\lambda'}$ and obtain $|G_n/C| = 2^{2n}$.
$(2)(a)$ Since $(-1)^{\lambda+a.b} = \pm 1$ then it follows,

$$e^2 = i^{2\lambda}\sigma_x(a)\sigma_z(b)\sigma_x(a)\sigma_z(b)$$

$$= (-1)^\lambda(-1)^{a.b}(\sigma_x(a))^2(\sigma_z(b))^2 = (-1)^{\lambda+a.b}I = \pm I \tag{B.36}$$

(b) Since the Pauli operators are Hermitian

$$e^\dagger = (-i)^\lambda\sigma_z^\dagger(b)\sigma_x^\dagger(a) = (-1)^\lambda(-1)^{a.b}(\sigma_x(a))(\sigma_z(b)) = \pm e$$

(c) Since $\lambda + a.b$ takes integer values $e^{-1} = e = e^\dagger$
(3) Let $e = i^{\lambda_e}\sigma_x(a_e)\sigma_z(b_e)$ and $f = i^{\lambda_f}\sigma_x(a_f)\sigma_z(b_f)$ be two error operators. Then Since $b_e.a_f + b_f.a_e$ is an integer, it follows that $[e, f] = 0$ when its even and $\{e, f\} = 0$

when it is odd.

$$\begin{aligned} ef &= i^{\lambda_e+\lambda_f}\sigma_x(a_e)\sigma_z(b_e)\sigma_x(a_f)\sigma_z(b_f) \\ &= i^{\lambda_e+\lambda_f}(-1)^{b_e.a_f}\sigma_x(a_e)\sigma_x(a_f)\sigma_z(b_e)\sigma_z(b_f) \\ &= i^{\lambda_e+\lambda_f}(-1)^{b_e.a_f}(-1)^{b_f.a_e}\sigma_x(a_f)\sigma_z(b_f)\sigma_x(a_e)\sigma_z(b_e) \\ &= (-1)^{b_e.a_f+b_f.a_e}fe \end{aligned} \tag{B.37}$$

In QECC an encoding operation sends both of the states and operators in to encode one such that
unencoded k-qubit states $|u\rangle \epsilon H_2^k \rightarrow$ n-qubit codewords $|c\rangle = \xi|u\rangle \epsilon H_2^n$ and
unencoded operators $A\epsilon G_k \rightarrow$ encoded operators $\bar{A} = \xi A \xi^\dagger$ which maps codewords $C_q \rightarrow C_q$. For unencoded error operator $e = i^\lambda \sigma_x(a)\sigma_z(b)$ is sent by encoding operation as

$$\begin{aligned} \bar{e} &= \xi[i^\lambda \sigma_x(a)\sigma_z(b)]\xi^\dagger \\ &= i^\lambda X(a)Z(b) \end{aligned} \tag{B.38}$$

where

$$\begin{aligned} X(a) &= (X_1)^{a_1}...(X_1)^{a_k} \\ Z(b) &= (Z_1)^{b_1}...(Z_1)^{b_k} \end{aligned} \tag{B.39}$$

In quantum stabilizer codes the stabilizer group is obtained from a set of $(n-k)$ operators $g_1....g_{n-k}$ which is the generators of the Abelian group S known as the stabilizer of quantum code C_q. Each element in S can be written as

$$s = g_1^{p_1}....g_{n-k}^{p_{n-k}} \tag{B.40}$$

and for all $s\epsilon S$ and $|c\rangle \epsilon C_q$

$$s|c\rangle = |c\rangle. \tag{B.41}$$

Since each elements of the stabilizer group S has order 2 i.e., $g_i^2 = I$ and $p_i = 0, 1$ then for the bit string of length $(n-1)$ one can claim that S is isomorphic to F_2^{n-k}, $p = p_1...p_{n-k}\epsilon F_2^{n-k}$. In F_2^{n-k} the number of bit strings ia also the order of S such that $|S| = 2^{n-k}$.

Using the fact that $g_i^2 = I$, the eigenvalue equation

$$g_i|l_i\rangle = \lambda_i|l_i\rangle \tag{B.42}$$

leads to the

$$g_i^2|l_i\rangle = \lambda_i^2|l_i\rangle \tag{B.43}$$

then $\lambda_i^2 = 1$ and $\lambda_i = (-1)^{l_i}$ where $l_i = 0, 1$.
Since any encoded quantum code C_q lies in a 2^n dimensional Hilbert space H_2^n, the states for H_2^k is constructed as direct product of single qubits

$$|\delta\rangle = |\delta_1\rangle \otimes ..... \otimes |\delta_k\rangle \tag{B.44}$$

where each qubit obeys the eigenvalue equation

$$\sigma_z^j|\delta_j\rangle = (-1)^{\delta_j}|\delta_j\rangle \tag{B.45}$$

for $j = 1, ..., k$.

The encoding operation $\xi : H_2^k \rightarrow H_2^n$ leaves the eigenvalue equation invariant and preserves the eigenvalue $(-1)^{\delta_j}$ in such that in terms of the encoded states $|\bar{\delta}\rangle$ it becomes

$$\begin{aligned} Z_j|\bar{\delta}\rangle &= \xi\sigma_z^j|\delta\rangle \\ &= (-1)^{\delta_j}\xi|\delta\rangle \\ &= (-1)^{\delta_j}|\bar{\delta}\rangle \end{aligned} \tag{B.46}$$

where the set of $\{Z_j : j = 1, .., k\}$ can be chosen as commuting with the generators $\{g_i\}$.

For the encoded quantum codeword $C_q \epsilon H_2^n$, the the basis is described by the set $\{g_1, ..., g_{n-k}; Z_1, ..., Z_k\}$ which has 2^n-dimensional simultaneous eigenstates. Labelling the eigenstates by the bit strings $l = l_1, .., l_{(n-k)}$ and $\bar{\delta} = \bar{\delta}_1, .., \bar{\delta}_k$ the eigenvalue equations can be written in terms of the simultaneous eigenstates as

$$\begin{aligned} g_i|l;\bar{\delta}\rangle &= (-1)^{l_i}|l;\delta\rangle \\ Z_j|l;\bar{\delta}\rangle &= (-1)^{\bar{\delta}_j}|l;\bar{\delta}\rangle \end{aligned} \tag{B.47}$$

where $i = 1, .., n-k; j = 1, .., k$ and $l_i, \bar{\delta}_j = 0, 1.$ and in terms of (41), equation (42) becomes

$$s(p)|l; \bar{\delta}\rangle \quad = \quad (-1)^{l.p}|l; \delta\rangle \tag{B.48}$$

where $l.p = l_1 p_1 + ... + l_{n-k} p_{n-k} (mod 2)$.

In decoding processes, for a quantum stabilizer code with generators $g_1, ..., g_{n-k)}$ and a Pauli error $e \epsilon G_n$, the error syndrome is given by

$$l_i = \begin{cases} 0 & \text{if } [e, g_i] = 0 \quad , \\ 1 & \text{if } \{e, g_i\} = 0 \quad , \end{cases} \tag{B.49}$$

where $(i = 1, ..., n-k)$

B.3 Non-Binary Quantum Stabilizer Codes and Quantum Codes from AG Codes

Let $\mathbb{F}_{p^m}$ be the Galois field of $q = p^m$ elements where p is prime and and m is an integer. Let $\alpha_1, .., \alpha_m$ be the elements of a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and define the linear functional $tr : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ which is called trace function and satisfies [87,95,106]

$$\begin{aligned} tr(l+s) &= tr(l) + tr(s) \\ tr(\alpha l) &= \alpha tr(l) \end{aligned} \tag{B.50}$$

for all $l, s \in \mathbb{F}_{p^m}, \alpha \in \mathbb{F}_p$.

For any $l, s \in \mathbb{F}_{p^m}$ we describe the dit flip and phase flip errors acting on a single qudit as

$$\begin{aligned} T_l|a\rangle &= |a+l\rangle \\ R_s|a\rangle &= \zeta_p^{Tr(sa)}|a\rangle \end{aligned} \tag{B.51}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ is a p^{th} root of unity and $Tr : \mathbb{F}_q \rightarrow \mathbb{F}_p$ is the trace function.

In matrix form the linear operators is expressed as $T_{i,j} = \delta_{(i,j-1)modp}$ and $R_{i,j} = \zeta^i \delta_{i,j}$. where $i = 0, ..., (p-1)$.They satisfy the relations

$$TR = \zeta RT \tag{B.52}$$

and in matrix form

$$T^i R^j = \zeta^{i,j} R^j T^i \tag{B.53}$$

$$(T^i R^j)(T^k R^h) = \zeta^{ih-jk}(T^k R^h)(R^j T^i) \tag{B.54}$$

For $l, s \epsilon \mathbb{F}_{p^m}$ the operators $T_l R_s$ form an orthonormal basis then

$$(T_l R_s)(T_{l'} R_{s'}) = \zeta^{\langle l,s' \rangle - \langle l',s \rangle}(T_{l'} R_{s'})(T_l R_s) \tag{B.55}$$

A quantum error $T_l R_s (l, s \in \mathbb{F}_p)$ acts on a qubit in the basis () as

$$T_l R_s |a\rangle = \zeta_p^{Tr(sa)} |a + l\rangle \quad (a \in \mathbb{F}_p) \tag{B.56}$$

and on an n-qubit the error operator e is written as

$$e = \zeta_p^t w_1 \otimes w_2 \otimes ... \otimes w_n \quad (w_i = T_l R_s, t, l_i, s_i \epsilon \mathbb{F}_p) \tag{B.57}$$

acting on the basis ()of $\mathbb{C}^{p^n}$

$$\begin{aligned} e|a_1....a_n\rangle &= \zeta_p^t (w_1|a_1\rangle) \otimes (w_2)|a_2\rangle \otimes ... \otimes (w_n|a_1\rangle) \\ &= \zeta_p^{t+s_1 a_1 + .. + s_n a_n}(|a_1 + l_1\rangle \otimes .. \otimes |a_n + l_n\rangle) \\ &= \zeta_p^{(s,a)+t}|a + l\rangle \end{aligned} \tag{B.58}$$

where $(s = (s_1, ., s_n), l = (l_1, ., l_n) \in \mathbb{F}_p^n)$.

Non-binary stabilizer codes is obtained by the error operators

$$E_{a,b} = T_{a^{(1)}} R_{b^{(1)}} \otimes T_{a^{(2)}} R_{b^{(2)}} \otimes .... \otimes T_{a^{(n)}} R_{b^{(n)}} \tag{B.59}$$

over the vectors

$$\begin{aligned} a &= (a^{(1)}, a^{(2)}, ..., a^{(n)}), \\ b &= (b^{(1)}, b^{(2)}, ..., b^{(n)}) \end{aligned} \tag{B.60}$$

from the space $\mathbb{F}_{p^m}^n$. The error group for an n-state q-ary system is

$$G_n = \{\zeta^i E_{a,b} : a, b \in \mathbb{F}_{p^m}^n, 0 \leq i \leq p-1\} \tag{B.61}$$

with order p^{2mn+1} and center $Z(G_n) = \langle \zeta I \rangle$ which has order p. The error operators satisfies the relation

$$(E_a E_b)(E_c E_d) = \zeta^{\langle a,d\rangle - \langle b,c\rangle}(E_c E_d)(E_a E_b) \tag{B.62}$$

Corresponding to the linear [n, k, d] code C with error correcting capability $t = \lfloor \frac{d-1}{2} \rfloor$ we can construct $C^\perp$ as the dual of the code C [105]

$$C^\perp = \{\upsilon \in \mathbb{F}_2^n : \upsilon.c = 0 \forall c \in C\} \tag{B.63}$$

and the $dim(C^\perp) = n - k$. C is called weakly self-dual code if $C^\perp \subset C$. These weakly self-dual code C is used to construct the quantum code Q which is a subclass of the larger class of stabilizer codes called as Calderbank-Shor-Steane (CSS)codes. In CSS construction superposition of the codewords of C is used to express the codewords of the quantum code Q.

If $v \in C$ then a quantum state $|c_w\rangle$ is defined in c-basis as

$$|c_w\rangle = 2^{-\frac{dim(C)}{2}} \sum_{c \in C} (-1)^{v.w} |v\rangle, \quad w \in \mathbb{F}_2^n. \tag{B.64}$$

If we use an s-basis where the codewords of the quantum code Q are the set of $|c_w\rangle \forall w \in C$, at first we change the basis by rotating

$$\begin{aligned} |0\rangle &\rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |1\rangle &\rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{B.65}$$

then we obtain the state as

$$|s_w\rangle = 2^{\frac{dim(C^\perp)}{2}} \sum_{c \in C^\perp} |u + w\rangle, \quad w \in \mathbb{F}_2^n \tag{B.66}$$

The dimension of the quantum code Q is

$$dim(Q) = dim(C) - dim(C^\perp) = k - (n-k) = 2k - n \tag{B.67}$$

and it contains 2^{2k-n} codewords.

In Stean's approach [83,84,91], we construct the quantum codes $Q(C_1, C_2)$such that

- C_1 and C_2 are $[n, k_1, d]$ and $[n, k_2, d^{'}]$ and $C_2^{\perp}$ is $[n, n-k_2, d]$ codes;
- $C_2 \subset C_1$;
- C_1 and $C_2^{\perp}$ both corrects t error;
- H_1 and H_2 are the parity check matrices of C_1 and $C_2^{\perp}$.

Then, for $\forall u \in C_1$ we define the state

$$|s_{u+w}\rangle = \frac{1}{2^{\frac{k_2}{2}}} \sum_{u \in C_1, w \in C_1/C_2} |u+w\rangle, \tag{B.68}$$

where $|C_2|$ is the cardinality of C_2 and $C_1/C_2$is the cosets.
When the state $|s_{u+w}^{'}\rangle$ is effected by the errors

$$|s_{(u+w),error}\rangle = \frac{1}{2^{\frac{k_2}{2}}} \sum_{u \in C_1, w \in C_1/C_2} (-1)^{(u+v).e_{pf}} |u+w+e_{bf}\rangle, \tag{B.69}$$

where e_{pf} and e_{bf} are the phase-flip and bit-flip errors.

Up to now we use binary field $GF(2)$ with two elements in CSS construction [82,89,103]. To extend it to the higher q-ary case [89,98] we use the field extension $GF(p^k)$ which is a k-dimensional vector space over $GF(p)$. For a basis B of vector space the extension takes place by the homomorphism $B : GF(p^k) \rightarrow [GF(p)]^k$. Now taking our codewords C as our vectors over the finite field $GF(2^k)$ and $B^{\perp}(C^{\perp})$ as the dual of C w.r.to basis $B^{\perp}$ we express the homomorphism for codewords as

$$B^{\perp}(C^{\perp}) \rightarrow [B(C)]^{\perp} \tag{B.70}$$

For $k = 2$ we obtain $GF(4) = \mathbb{F}_4 = \{0, w, w^2, 1\}$ where $w^2 = w + 1$, $\bar{w} = w^2$, $w^3 = 1$ and $\{w, \bar{w}\}$ is basis for $\mathbb{F}_4$. Using these basis we associate a vector $v \in \mathbb{F}_4$

$$v = aw + b\bar{w}, \quad a, b \in \mathbb{F}_2^n \tag{B.71}$$

In this field classical linear codes which is additive code over $\mathbb{F}_4$ is obtained by

$$D = wC_1 + \bar{w}C_2^{\perp} \subseteq \mathbb{F}4^n \tag{B.72}$$

where C_1 is a $[n_1, k_1, d_1]_2$ code and C_2 is a $[n_2, k_2, d_2]_2$ code satisfying $C_1 \subseteq C_2$

Let X be a smooth, projective, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_{p^m} = \mathbb{F}_q$. Given a divisor A on X defined over $\mathbb{F}_q$, let

$$L(A) = \{f \in \mathbb{F}_q(X) : (f) \geq -A\} \cup \{0\} \tag{B.73}$$

and

$$\Omega(A) = \{\eta \in \Omega(X) : (\eta) \geq A\} \cup \{0\}. \tag{B.74}$$

Let $\ell(A)$ and suppD denote the dimension of $L(A)$ as an $\mathbb{F}_q$ vector space and support of a divisor D.

Algebraic Geometry codes $C_L(D, G)$ and $C_\Omega(D, G)$ can be constructed using divisors $D = \sum_{i=1}^{n} P_i$ and $G = \sum_{i=1}^{m} \alpha_i Q_i$ on X where $P_1, ..., P_n, Q_1, .., Q_m$ are pairwise distinct $\mathbb{F}_q$ rational points and $\alpha_i \in \mathbb{N}$ for all i, $1 \leq i \leq m$. The two algebraic geometry codes are related in that

$$C_L(D, G)^{\perp} = C_\Omega(D, G). \tag{B.75}$$

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name:	**GÜL, Yusuf**
Nationality:	Turkish (TC)
Date of Birth:	Merzifon , TÜRKİYE
Place of Birth:	May 03, 1976
Marital Status:	Single
Phone:	+90 0506 591 1632
e-mail:	ysfgul55@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
Ph.D.	Physics Middle East technical University (METU) Ankara, TÜRKİYE	2009
M.Sc.	Mathematics and Computer Science Cankaya University , TÜRKİYE	2003
B.S.	Physics Education METU, TÜRKİYE	1999

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2000 - 20009	Faculty of Arts and Science,Cankaya University.	Res.Asst.

FIELDS OF RESEARCH INTEREST

Quantum Information, Quantum Computations, Quantum Optics, Quantum Languages, Algorithmic Number Theory, Public Key Cryptography .