THE UNIVERSITY OF CALGARY

# Pure state entanglement and stabilizer representations

by

Jop Briët

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

September, 2006

# THE UNIVERSITY OF CALGARY

# FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Pure state entanglement and stabilizer representations" submitted by Jop Briët in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Supervisor, Dr. David L. Feder
Department of Physics and Astronomy

Co-Supervisor, Dr. Peter Høyer
Department of Computer Science

Dr. David W. Hobill
Department of Physics and Astronomy

Dr. Gilad Gour
Department of Mathematics and Statistics

Date

# Abstract

This thesis is concerned with entanglement in quantum systems and representation of the states of these systems using finite Abelian groups called stabilizers. In particular, $n$-qubit pure states are studied. Because entanglement plays a very important role in the theory of quantum information processing it is a topic of much interest in this field.

Entangled states are classified using physically possible operations under a typical configuration; spatially separated parties who each hold part of the quantum system over which a possibly entangled state is distributed. The most general of these operations are stochastic local operations and classical communications (SLOCC). Entanglement is quantified using functions of the density matrix of a state which behave monotonically under local operations and classical communication (LOCC).

Although entangled states usually depend on an exponential number of parameters, a special subclass of $n$-qubit pure states known as stabilizer states can efficiently be represented by finite Abelian groups known as stabilizers. This formalism plays a crucial role in quantum error correction [16] and stabilizer states are used in a revolutionary scheme for quantum computation known as measurement based computation [32, 34]. A homomorphism between stabilizer states and simple graphs has been found which opened up a new way of studying their properties [36, 40] in an intuitive and efficient manner. Using this representation, equivalency classes under local unitary operations can be defined by only $n^2$ real parameters. The research done for this project was driven by the wish to generalize the conventional stabilizer formalism for all $n$-qubit pure states and the idea of using it to distinguish SLOCC-

inequivalent states. What is presented in chapters 1, 2 and 3 of this thesis is an overview of the topics that are relevant to the research in this project. The original work and findings are contained in chapter 4.

# Acknowledgements

I would like to express enormous gratitude to those who have supported me during this project. These amazing people around me continuously dissolved uncertainty and frustration with patience, energy and love. Thank you Mom, Dad, Gijs, Stijn, Sasha, Claar, Brandy, David, Peter and my dear friends.

# Table of Contents

# List of Figures

# Chapter 1

# Introduction

## 1.1 Classical states of natural systems

One can naturally describe everything in the world in terms of systems and their states. A system is an isolated part of nature with which one can interact in some way. One way to mathematically represent the state of a classical system is by a vector. This thesis is concerned with computational states, so only systems which can be in a *discrete* number of different states will be considered. Therefore, the only vector representations of physical states will be discrete ones, which can be written down as either row, or column vectors. A simple example is the state of a *bit*, a two-level system that lies at the heart of modern day computation. The two possible states can be represented by the two dimensional vectors $\binom{1}{0}$ and $\binom{0}{1}$. These vectors are linearly independent, which means that there is no non-trivial linear combination of them that sums to zero. These two vectors are said to be part of a two dimensional vector space, which means that the maximum number of linearly independent vectors in this space is two. It also means that any vector in this space can be expressed as a linear combination of two linearly independent vectors. A set of two linearly independent vectors is called a *basis* for this vector space. The vector representations of distinguishable states must be chosen such that there is no ambiguity in which state they represent. This requirement can be satisfied by choosing the vectors such that they are not only linearly independent, but also have an *inner product* of zero.

The inner product associates a scalar with a pair of vectors and for discrete vector spaces can be defined as

$$(v, w) = \sum_{i=1}^{n} v_i^* w_i,$$

where $v$ and $w$ are vectors in an $n$-dimensional vectors space and $v_i^*$ denotes the complex conjugate of the $i$'th entry of $v$. In the example of a bit given above, it can be seen that the vectors indeed have an inner product of zero. Of course bits are not the only possibility. General systems which can be in a discrete number of states can be referred to as $n$-level systems.

## 1.2 Quantum states

If the state of a system is not known with complete certainty, the best way to possibly describe it is in terms of a probabilistic distribution of states it might be in. The outcome of a coin flip is an easy example of such a distribution, and can be represented in vector form as $\binom{0.5}{0.5} = 0.5\binom{1}{0} + 0.5\binom{0}{1}$. This says that each outcome, heads $= \binom{1}{0}$ and tails $= \binom{0}{1}$ can be expected with equal probability. Naturally, the sum of all probabilities must equal unity. This ensures that the system is certainly in one of the states of the probabilistic distribution.

Although a probabilistic distribution of states might seem to provide the most information possible if the exact state is not known, there are processes in nature that indicate that this is in fact not sufficient to accurately describe them. These are processes which only be understood if the states of the systems involved are described in terms of a *superposition of states*, as opposed to a probabilistic distribution of states. A superposition of states is a probabilistic distribution of states whose probabilities

of occurrence are given in terms of *probability amplitudes.* A probability amplitude is a complex number, whose absolute square represents a probability.

### 1.2.1 The qubit

The basic building block of the theory of quantum information and computation is the quantum bit, or *qubit.* A qubit is a *superposition* of the states of a regular bit. A regular bit can only be in one of two separate states which can be represented by the Dirac kets or two dimensional vectors

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

This representation is called the *computational basis.* Note that this representation is not unique. Any set of two orthonormal vectors would provide an equally valid reprentation. A qubit can now be represented as a probabilistic distribution

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{1.1}$$

where the coefficients $\alpha$ and $\beta$ are probability amplitudes, whose squares represent the probabilities to find the qubit in one of the bit states. Since the total probability of the qubit being in one of the two possible states of a classical bit must be one, the coefficients must satisfy $|\alpha|^2 + |\beta|^2 = 1$. This requirement implies that all vectors representing qubits have unit length, or an inner product of one. Qubits are often represented graphically inside of a unit sphere known as the Bloch sphere. A qubit is drawn as a directed line connecting the center of the sphere to somewhere on its surface. The point where it touches the surface corresponds to the probability amplitudes of each of the bit states.

### 1.2.2 The qudit

After the introduction of the qubit, the generalization to higher-level quantum systems is easily understood. A *qudit*, which is a $d$-level quantum system that can be represented in terms of the basis

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \; \cdots, \; |d-1\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{1.2}$$

A general quantum state would in this case take the form

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{d-1} |d-1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \tag{1.3}$$

As might be noticed, the number of possible states of a quantum system is vastly larger than those of a classical system with the same number of levels. For example, an $n$-bit system can be in $2^n$ different possible states. An $n$-qubit system however, can assume many more states because of the possibility of superposition of states, and another property which is the topic of the next chapter; *entanglement*.

One of the major problems in the theory in quantum information processing is the classification of entangled states and the quantification of this property. In chapter 2, a broad introduction is presented of entangled pure states, their representations, the effect of the operations under which entanglement classes are defined, basic entanglement quantifying functions, a detailed description of the three-qubit pure state

case, the problem with classifying pure states of larger systems and two important examples of applications of this property in states of large systems. The theory of Pauli stabilizers is contained in chapter 3. A different representation of a subclass of entangled $n$-qubit pure states in terms of a finite Abelian group turns out to yield a highly useful tool for the description and construction of highly entangled states, of which two important applications are given as examples. The work done to attempt to generalize the stabilizer description of pure states and its possible use is presented in chapter 4. Particularly, its use for the description of two- and three-qubit pure states is analyzed using simple examples and information contained in the previous two chapters.

# Chapter 2

# Entangled pure states

## 2.1 Introduction

In the previous chapter the concept of single multi-level systems, in particular qubits, was introduced. In this chapter, the study of the properties of systems which are composed of conjunctions of multi-level systems is discussed. Section 2.2 presents the description two-body pure states; a simple example that illustrates basic properties of multi-body pure states. These states can be divided into two classes, *separable* and *entangled*. Separable states are those which can be described as a concatenation of single-body states. Entangled states possess the interesting property that they can only be attributed to an overall state of the system which can not be broken down in terms of a conjunction of parts. The Schmidt decomposition is presented as a mathematical tool which allows a two-body pure state to be written in a standard form. In section 2.3 the generalization of this is discussed. Entanglement in quantum systems has been found to be a powerful resourse for myriad information processing related tasks, for examples see [18, 37, 16, 19, 33, 23, 32, 34, 22, 39]. Because of this, the quantification of entanglement and classification of pure states are topics of much interest. Section 2.4 presents a mathematical description of the most general operations that can be performed on a quantum system. A very important subclass of general quantum operations are those known as *local operations and classical communication* (LOCC), and *stochastic* LOCC (SLOCC). It is these operations that

are used to define entanglement quantifying functions, *entanglement monotones*, and under which pure state classes are identified. In section 2.5, the properties that two quantum states must posses in order to belong to the same entanglement class are presented. For three-qubit pure states there turn out to be only two SLOCC-inequivalent classes. A discussion of how these can be identified is contained in section 2.8. The classification of inequivalent pure states is in general far from trivial. The biggest problem which lies at the heart of general multi-qubit pure state classification is explained in section 2.9. Section 2.10 presents two examples of major applications in the theory of quantum information processing.

## 2.2 A two-body system

This section introduces a system composed of two quantum subsystems, interchangeably referred to as bodies or constituents. The properties of such systems are introduced using the simplest example: a system of two qubits. The states of this system can be described by vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$. A simple example of a two-qubit state is one where both qubits are in the state $|0\rangle$, in which case the state of the whole system can be represented by $|0\rangle \otimes |0\rangle$ or $|00\rangle$. In regular vector notation this state would be represented by the vector

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

As will be shown shortly, this type of state is part of a special subclass of all the possible two-qubit states. Because the states of the individual qubits are separately well defined, this type of state is usually referred to as *separable.* A general separable state of two qubits in states $|\psi\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|\phi\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ is written as

$$|\psi\rangle|\phi\rangle \equiv \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ \beta_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}.$$

The other class of two-qubit states is comprised of all the states which cannot be written in the form of a tensor product of individual qubit states. These states are not separable, but *entangled.* The most important difference is that entangled states cannot be prepared by single qubit operations, which will be discussed in detail in section 2.4. The most familiar examples of two-qubit entangled states are the Bell states

$$\begin{aligned} |\beta_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left(\tfrac{1}{\sqrt{2}}, 0, 0, \tfrac{1}{\sqrt{2}}\right)^T \\ |\beta_{01}\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \left(0, \tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0\right)^T \\ |\beta_{10}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \left(\tfrac{1}{\sqrt{2}}, 0, 0, -\tfrac{1}{\sqrt{2}}\right)^T \\ |\beta_{11}\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \left(0, \tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}}, 0\right)^T. \end{aligned}$$

The key property of entangled states is that they can only be described as a whole, and not as a conjunction of parts. As can be seen from the Bell states, if a collection of systems is in an entangled state, there ceases to be a single identifiable state of each of its constituents.

### 2.2.1 The Schmidt decomposition

The Schmidt decomposition is a powerful tool which can be used to put pure states of a conjunction of two systems in a standard form [38]. The following theorem shows how this works by introducing a pure state $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ of two systems '$a$' and '$b$' which have $n$ and $m$ levels respectively.

**Theorem 2.1.** *Let $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ be a vector representation of the state of some two-body system whose two constituents are labeled by 'a' and 'b'. With coefficients $A_{ij}$ and orthonormal bases $|a_i\rangle$ and $|b_j\rangle$, the state is explicitly written as*

$$|\psi\rangle = \sum_{i,j=1}^{n,m} A_{ij} \, |a_i\rangle |b_j\rangle \, . \tag{2.1}$$

*Then the matrix $A$ can be decomposed in a way such that $|\psi\rangle$ can be written as*

$$|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_k \, |a'_k\rangle |b'_k\rangle \, , \; n_\psi \leq \min(n, m). \tag{2.2}$$

*Proof.* Start by considering the *singular value decomposition* (SVD) of the matrix $A$. If $A$ is an $m \times n$ matrix, then the SVD-theorem says that there exists a $\min(n, m) \times \min(n, m)$ diagonal matrix $\Lambda$ such that

$$A = U \Lambda V^\dagger, \tag{2.3}$$

where $U$ and $V$ are unitary matrices. These matrices can be constructed by letting the eigenvectors of the matrix $AA^\dagger$ make up the columns of $U$, the eigenvectors of $A^\dagger A$ make up the columns of $V$ and the entries of $\Lambda$ be the square roots of the eigenvalues of $AA^\dagger$ and $A^\dagger A$. Using this, the state $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i,j,k=1}^{n,m,n_\psi} U_{ik} \Lambda_{kk} V_{kj} \, |a_i\rangle |b_j\rangle \tag{2.4}$$

Define the unitary transformations $U$ and $V$ such that

$$\begin{aligned} |a'_k\rangle &= \sum_{i=1}^{n} U_{ik} |a_i\rangle \\ |b'_k\rangle &= \sum_{j=1}^{m} V^*_{kj} |b_j\rangle , \end{aligned}$$

and let $\Lambda_{kk} = \lambda_k$ to get

$$|\psi\rangle = \sum_{k=1}^{n_\psi} \Lambda_{kk} \left( \sum_{i=1}^{n} U_{ik} |a_i\rangle \right) \left( \sum_{j=1}^{m} V^*_{kj} |b_j\rangle \right) = \sum_{k=1}^{n_\psi} \lambda_k |a'_k\rangle |b'_k\rangle \tag{2.5}$$

as asserted in the theorem. □

The coefficients $\lambda_k$ are referred to as the Schmidt coefficents. The total number of non-vanishing $\lambda_k$'s, $n_\psi$, is known as the *Schmidt number* of the state $|\psi\rangle$. A very useful feature of this decomposition is that it allows for quick distinction of separable and entangled states. All states with Schmidt number equal to unity can be written in the form $|\psi\rangle = |a'_k\rangle|b'_k\rangle$, which implies that they are separable. All states with higher Schmidt numbers can not be represented in such a form and must therefore be entangled states. This property of the Schmidt number indicates that it could be a useful tool to study entanglement.

If the two systems '$a$' and '$b$' are both qubits, then the Schmidt decomposition of their combined state again takes on the general form $|\psi\rangle = \sum_{k=1}^{n_\psi} \lambda_k |a'_k\rangle|b'_k\rangle$, where $|a'_k\rangle$ and $|b'_k\rangle$ are orthonormal basis vectors for the states of the individual qubits. Although it may be self-evident, it should be noted that classical systems and systems with zero degrees of freedom (single-level systems) can not be in an entangled state because they can not be in a superposition of states, as required for entanglement.

## 2.3 $n$-body systems

With the attempt to generalize the notion of a standard representation to pure states of $n$-qubit systems comes the disappointing realization that this is far from trivial. The highly useful Schmidt decomposition turns out to only be generalizable to multi-body systems for a very limited number of states.

### 2.3.1 Higher order Schmidt decompositions

The Schmidt decomposition merely asserts that a double sum of the form (2.1) can be converted into a single sum like (2.2) through unitary operations $U$ and $V$. A possible higher order Schmidt decomposition would imply writing a higher order sum as a single sum. This is generally not possible, however [29, 30]. Consider for example the triple sum

$$|\psi\rangle = \sum_{ijk} A_{ijk} |a_i\rangle|b_j\rangle|c_k\rangle \,. \tag{2.6}$$

The desired higher order Schmidt decomposition would thus be of the form

$$\sum_i \lambda_i |a_i'\rangle|b_i'\rangle|c_i'\rangle \,, \tag{2.7}$$

where $|a_i'\rangle$, $|b_i'\rangle$ and $|c_i'\rangle$ are new orthonormal basis vectors. But Schmidt's theorem only asserts that the triple sum (2.6) can be unitarily converted in to

$$\sum_i \lambda_i |a_i'\rangle|bc_i'\rangle \,, \ \sum_i \lambda_i |b_i'\rangle|ac_i'\rangle \,, \text{ or } \sum_i \lambda_i |c_i'\rangle|ab_i'\rangle \,,$$

where $|bc_i'\rangle$, $|ac_i'\rangle$ and $|ab_i'\rangle$ are the states of the conjoined systems '$bc$', '$ac$' and '$ab$' respectively. A decomposition of the form (2.7) is only possible if the vectors $|bc_i'\rangle$, $|ac_i'\rangle$ and $|ab_i'\rangle$ are product vectors. That is $|bc_i'\rangle = |b_i\rangle|c_i\rangle$, $|ac_i'\rangle = |a_i\rangle|c_i\rangle$ and

$|ab'_i\rangle = |a_i\rangle|b_i\rangle$. In other words, this says that the vector

$$|bc'_i\rangle = \sum_{jk} W_{ijk} |b_j\rangle|c_k\rangle \tag{2.8}$$

is such that the rank of $W_i$ is one for all $i$ and $W_i^\dagger W_j = W_i W_j^\dagger = 0$ if $i \neq j$ , and similarly for $|ac'_i\rangle$ and $|ab'_i\rangle$. This shows that a generalized Schmidt decomposition of the form (2.7) is only possible for a very select set of states.

### 2.3.2 Minimal product decomposition

Since the Schmidt decomposition is such a powerful tool, a generalization of it for multipartite systems is desirable. A literal generalization of it was proved impossible, but the next best thing seems to be the *minimal product decomposition* [14, 20]. The minimal product decomposition of a higher order sum is defined as

$$|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i |a'_i\rangle|b'_i\rangle\cdots, \tag{2.9}$$

where vectors $|a'\rangle$, $|b'\rangle$, etc., are such that $n_\psi$ has the lowest possible value (in this case these vectors are only orthonormal if a higher order Schmidt decomposition *is* possible). The minimal value of $n_\psi$ is a generalization of the Schmidt number called the Schmidt *rank*. The calculation of the Schmidt rank is unfortunately a difficult task. Consider the following example.

**Example 2.1.** *A given 3-qubit pure state $|\psi\rangle$ can be written in Dirac notation and*

*vector form as*

$$|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i \left(\alpha_i^{(1)}|0\rangle + \beta_i^{(1)}|1\rangle\right) \otimes \left(\alpha_i^{(2)}|0\rangle + \beta_i^{(2)}|1\rangle\right) \otimes \left(\alpha_i^{(3)}|0\rangle + \beta_i^{(3)}|1\rangle\right)$$

$$= \begin{pmatrix} \sum_{i=1}^{n_\psi} \lambda_i \alpha_i^{(1)} \alpha_i^{(2)} \alpha_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \alpha_i^{(1)} \alpha_i^{(2)} \beta_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \alpha_i^{(1)} \beta_i^{(2)} \alpha_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \alpha_i^{(1)} \beta_i^{(2)} \beta_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \beta_i^{(1)} \alpha_i^{(2)} \alpha_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \beta_i^{(1)} \alpha_i^{(2)} \beta_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \beta_i^{(1)} \beta_i^{(2)} \alpha_i^{(3)} \\ \sum_{i=1}^{n_\psi} \lambda_i \beta_i^{(1)} \beta_i^{(2)} \beta_i^{(3)} \end{pmatrix}.$$

*In order to find the Schmidt rank of this state-vector, the values for all coefficients $\lambda_i$, $\alpha_i$ and $\beta_i$ have to be found for which $n_\psi$ is minimal.*

For general $n$-qubit pure states, this starts off as a non-linear system of $2^n$ equations of $(2n+1) \cdot 2^n$ polynomials for which common null spaces have to be found.

## 2.4 General quantum operations

The goal of this chapter is to introduce quantification of entanglement and classification of entangled pure states. Since these topics are highly intertwined with the notion of state-transformations, a rigorous mathematical description of physically reasonable operations is introduced first. What is presented in this section is an adapted version of part of the work in [42]. Let us first consider all *admissible operations* $\mathcal{E}$ on a single quantum system with density matrix $\rho$.

### 2.4.1 Density matrices

The representation of pure states can take on the form of various mathematical objects. Besides the vector representation, another commonly used representation is a density matrix $\rho$. In this representation, a pure state is now represented by a matrix $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is its vector representation and $\langle\psi|$ is its complex transpose. This is an object which satisfies the properties of an *orthogonal projector*: $\rho^2 = \rho$ and $\rho^\dagger = \rho$.

### 2.4.2 Operations on a single system

An operation $\mathcal{E}$ on a state $\rho$ is said to be admissible if its yield, $\mathcal{E}(\rho)$ is also a density matrix. Admissible operations can be physically described as the set of the following four procedures.

1. *Unitary operations.* The state $\rho$ is transformed by an operation which is mathematically represented by a unitary matrix $U$. The effect can be represented by

$$\rho \mapsto \rho' = U\rho U^\dagger. \tag{2.10}$$

   This is a process that simply rotates the eigenvectors of $\rho$. Any unitary matrix is invertible and thus leaves the Hilbert space $\mathcal{H}$ in which $\rho$ lives invariant.

2. *von Neumann measurements.* A von Neumann measurement is a set of operations $\{M_i\}$ such that for all indices $i$, $M_i = M_i^\dagger$ and $M_i^2 = M_i$ and $\sum_i M_i^\dagger M_i = I$. These are also known as *projective measurements.* The matrices $\{M_i\}$ are orthogonal projectors, just like density matrices of pure states. The effect of a von Neumann measurement $\{M_i\}$ on a density matrix $\rho$ is that

it maps it to an ensemble

$$\rho \mapsto \{p_i, \rho_i\}, \tag{2.11}$$

where $p_i$ is the probability of $\rho$ being transformed into a new density matrix $\rho_i$ after the operation $M_i$. These type of operations are not necessarily invertible and it is therefore possible that they decrease the size of the Hilbert space.

**Example 2.2.** *Consider the von Neumann measurement* $\{M_1, M_2\}$ *and the density matrix* $\rho$ *such that*

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; M_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{and} \quad \rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \tag{2.12}$$

*Here* $\rho = |\psi\rangle\langle\psi|$ *is the density matrix of the pure state* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. *The conditions of a von Neumann measurement are satisfied and these operations map* $\rho$ *to*

$$\begin{aligned} M_1 \rho M_1^\dagger &= \rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| \\ M_2 \rho M_2^\dagger &= \rho_2 = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}|1\rangle\langle 1|, \end{aligned}$$

*which can be interpreted as* $\rho$ *being mapped to* $\rho_1$ *or* $\rho_2$ *each with probability* $p_1 = p_2 = \frac{1}{2}$, *hence the ensemble* $\{\frac{1}{2}, \rho_1; \frac{1}{2}, \rho_2\}$.

3. *Addition of an uncorrelated ancilla.* An extra quantum system '$a$' in a state $\rho_a$ is added to the existing system. The overall density matrix is transformed as

$$\rho \mapsto \rho \otimes \rho_a. \tag{2.13}$$

This operation is does not leave the Hilbert space invariant, but is reversible because simply removing the system $a$, which is the next point, brings us back to the original state.

4. *Dismissal of information.* All information of the state $\rho$ of a system is dismissed as if it ceases to exist. This is mathematically equivalent to taking the trace over all degrees of freedom of the density matrix.

$$\rho \mapsto \mathrm{Tr}\rho. \tag{2.14}$$

After information has been lost it can not be retrieved, hence an operation of this sort is not reversible.

Any admissible operation $\mathcal{E}$ can be decomposed into a combination of these four. Its action on a density matrix $\rho$ is

$$\rho \mapsto \mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \tag{2.15}$$

where the *Kraus operators* $E_i$ satisfy $\sum_i E_i^\dagger E_i = I$. This implies that the operation is trace-preserving and therefore indeed maps a density matrix $\rho$ to a new density matrix $\mathcal{E}(\rho)$. This describes the most general *quantum* operation and assumes that any possible measurement outcomes are not registered, therefore leaving the state in an ensemble $\{p_i, \rho_i\}$. If actual measurements *are* performed however the operations ceases to be trace-preserving. Some possible outcomes $\rho_i = E_i \rho E_i^\dagger$ are then simply disregarded. A general non-trace-preserving operation utilizes an incomplete set of Kraus operators $E_i$ with indices $\omega \subset \{i\}$, where in a complete set of Kraus operators, all indices in the set $\{i\}$ would appear. The non-trace-preserving operation $\mathcal{E}_\omega$ on $\rho$

is represented as

$$\rho \mapsto \mathcal{E}_\omega(\rho) = \sum_{i\in\omega} E_i \rho E_i^\dagger, \tag{2.16}$$

where the incomplete set of Kraus operators $E_i$ satisfy $\sum_{i\in\omega} E_i^\dagger E_i < I$. As a result of this, the trace of $\rho$ is decreased to some value $p_\omega = \mathrm{Tr}[\mathcal{E}_\omega(\rho)] < 1$, which means that this operation yields the density matrix

$$\rho_\omega = \frac{\mathcal{E}_\omega(\rho)}{p_\omega}, \tag{2.17}$$

with probability $p_\omega$. In terms of measurements this can be understood as only regarding an incomplete set of all possible measurement outcomes. As an example, consider the non-trace-preserving operation $\mathcal{E}_0 = |0\rangle\langle 0|\rho|0\rangle\langle 0|$, which utilizes only a single Kraus operator $|0\rangle\langle 0|$. It maps the state $\rho$ to $\rho_0 = |0\rangle\langle 0|$ with probability $p_0 = \mathrm{Tr}[|0\rangle\langle 0|\rho|0\rangle\langle 0|]$. Because the set operations $\{\mathcal{E}_\omega, \mathcal{E}_{\bar{\omega}}\}$, where $\bar{\omega}$ is the complement of $\omega$ such that the union $\omega \cup \bar{\omega} = \{i\}$, must together still form an admissible quantum operation, the condition $\sum_{i\in\omega} E_i^\dagger E_i + \sum_{i\in\bar{\omega}} E_i^\dagger E_i = I$ is satisfied because this involves a complete set of Kraus operators.

### 2.4.3 Operations on composite systems

When the system is composed of a collection of subsystems, the form of the allowable operations is not much different. The exception is however, that measurement outcomes may or may not be shared between the parties that are in possession these subsystems. This additional operation is called *classical communication*. Consider for example a quantum state $\rho$ of a conjunction of two subsystems '$a$' and '$b$' in possession of parties $A$ and $B$. Each party can perform admissible operations on their subsystem, whose states are represented by density matrices $\rho_a$ and $\rho_b$ respectively.

An admissible operation which is performed only by party $A$, while party $B$ leaves its subsystem alone is called a *local operation.* It is implemented by means of an operator $\mathcal{E}_{A,\omega}$ using Kraus operators of the form $E_{A,i} \otimes I_B$, where the $E_{A,i}$ satisfy $\sum_{i\in\omega} E_{A,i}^\dagger E_{A,i} \leq I_A$ as before and the index $A$ indicates that it only affects the state $\rho_a$. The general *multi-local* operations on a composite system are implemented by means of operators of the form $E_{A,i} \otimes E_{B,i} \otimes \cdots$.

In conjunction the with classical communication of measurement outcomes, the amount of information about the state for all the parties increases. If measurement outcomes were kept private or were dismissed completely, the state would have to be described as a probabilistic distribution of outcomes. From now on (multi-) local operations and classical communications will be referred to as the single abbreviation LOCC. Two states $|\psi\rangle$ and $|\phi\rangle$ which can be transformed into each other, either one way or both ways, with certainty using only LOCC, are said to belong to the same class under LOCC. If however, if this transformation only works with some probability, the states are said to belong to the same class under *stochastic* LOCC, which from now on will be referred to as SLOCC.

## 2.5 Entanglement and reduced density matrices

The *partial trace* of a density matrix of a multi-body system is a tool which can be used to determine the state of a subsystem which may be entangled with the rest. The density matrix which represents the state of a subsystem is called a *reduced density matrix.* As will be shown, the form of a reduced density matrix reveals if a subsystem is entangled with the rest of the system or not. It plays an important role

in the study of entanglement quantification and pure state classification.

### 2.5.1 Reduced density matrices

The concept of a reduced density matrix is important for describing the state of a subsystem of a larger, possibly entangled many-body system. As introduced in section 2.4.1, a density matrix of some pure state $|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i |x_i\rangle$ can be written as

$$\rho^\psi = |\psi\rangle\langle\psi| = \left(\sum_{i=1}^{n_\psi} \lambda_i |x_i\rangle\right)\left(\sum_{j=1}^{n_\psi} \lambda_j \langle x_j|\right) = \sum_{i,j=1}^{n_\psi} \lambda_i \lambda_j^* |x_i\rangle\langle x_j|. \tag{2.18}$$

The reduced density matrix of a subsystem '$a$', now is calculated by taking the partial trace over the part of the system which is complementary to '$a$'. For example, let $|\psi\rangle = \sum_{i=1}^{n_\psi} |a_i\rangle|b_i\rangle$ be the Schmidt decomposition of the state of the combined subsystems '$a$' and '$b$', then the reduced density matrix of system '$a$' can be found by computing

$$\rho_a^\psi \;=\; \sum_{i=1}^{n_\psi} \langle b_i|\, \rho^\psi\, |b_i\rangle = \sum_{i=1}^{n_\psi} |a_i\rangle\langle a_i|.$$

Note that if the state is entangled, the reduced density matrix $\rho_a^\psi$ is not one of a pure state as introduced in section 2.4.1.

### 2.5.2 Entanglement and density matrix rank

Together with the Schmidt decomposition theorem a connection can be made between the rank of a reduced density matrix and its entanglement properties with the complement of the system. The following proposition shows this with the example of an $n$-qubit system. It is readily generalized to states of larger many-body systems.

**Proposition 2.1.** *Let $\rho_a$ be the reduced density matrix of a single qubit with label 'a' of an n-qubit pure state. Then qubit 'a' is unentangled if the rank $r(\rho_a) = 1$ and entangled with at least one other qubit if $r(\rho_a) = 2$.*

*Proof.* Let the Schmidt decomposition of the $n$-qubit pure state be

$$|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i |a_i\rangle|x_i\rangle\,, \tag{2.19}$$

where $|a_i\rangle$ are (is) the orthonormal vector(s) of the single qubit state $\rho_a$, and $|x_i\rangle$ the orthonormal vector(s) of the state $\rho_x = \mathrm{Tr}_a\rho$ of the system complementary to '$a$', which is temporarily labeled '$x$'. This representation can always be achieved by applying a unitary transformation on the states $|a_i\rangle$ such that the reduced density matrix $\rho_a$ is diagonal [1]. Note that unitary transformations can not change the entanglement properties of the state. Then if qubit '$a$' is not entangled with the rest of the system, there will only be a single term in the Schmidt decomposition (2.19), and the state will just be $|\psi\rangle = |a\rangle|x\rangle$. The reduced density matrix of this pure state will then just be of the form

$$\rho_a = |a\rangle\langle a|\langle x|x\rangle = |a\rangle\langle a|, \tag{2.20}$$

which is a rank-one matrix. If the Schmidt decomposition (2.19) has two terms, which means that qubit '$a$' is entangled with at least one other part of the rest of the system, then the reduced density matrix will be

$$\begin{aligned}\rho_a &= |\lambda_1|^2|a_1\rangle\langle a_1|\langle x_1|x_1\rangle + |\lambda_2|^2|a_2\rangle\langle a_2|\langle x_2|x_2\rangle + \\ &\quad \lambda_1\lambda_2^*|a_2\rangle\langle a_1|\langle x_2|x_1\rangle + \lambda_2\lambda_1^*|a_1\rangle\langle a_2|\langle x_1|x_2\rangle \\ &= |\lambda_1|^2|a_1\rangle\langle a_1| + |\lambda_2|^2|a_2\rangle\langle a_2|,\end{aligned}$$

[1] Proof of this can be found on pages 59-60 of [31]

since $|x_i\rangle\langle x_j| = \delta_{ij}$. This is a rank-two matrix because it has two non-zero terms in its spectral decomposition. □

This shows that there is an intimate relationship between the rank of a reduced density matrix of some subsystem and its entanglement with another. Intuitively it can be reasoned that if some system '$a$' is entangled with system '$b$', the converse must also be true. The established connection between entanglement and the rank of reduced density matrices leads us to the following lemma which confirms this idea in a mathematical sense.

**Lemma 2.1.** *The rank of a reduced density matrix of some system is equal to the rank of the complementary reduced density matrix.*

*Proof.* Consider a conjunction of subsystems '$a$' and '$b$'. The density matrix of its pure state $|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i |a_i\rangle|b_i\rangle$ can be represented by

$$\rho^\psi = \sum_{i,j=1}^{n_\psi} \lambda_i \lambda_j^* |a_i\rangle|b_i\rangle\langle a_j|\langle b_j| \tag{2.21}$$

The partial traces $\rho_a = \mathrm{Tr}_b \rho^\psi$ and $\rho_b = \mathrm{Tr}_a \rho^\psi$ give rise to the density matrices

$$\rho_a^\psi = \sum_{i=1}^{n_\psi} |\lambda_i|^2 |a_i\rangle\langle a_i| \quad \text{and} \quad \rho_b^\psi = \sum_{i=1}^{n_\psi} |\lambda_i|^2 |b_i\rangle\langle b_i| \tag{2.22}$$

which have an equal number of non-zero terms $|\lambda_i|^2$ and thus have equal ranks. □

This not only shows that the systems '$a$' and '$b$' must indeed be entangled *with each other* since $r(\rho_a) = n_\psi$ implies $r(\rho_b) = n_\psi$ and vise versa, it has also become apparent that $\rho_a$ and $\rho_b$ have equivalent spectral decompositions up to a possible difference in orthonormal basis. Yet another thing which can be deduced is that the maximal Schmidt number of a two-qubit state is 2 which follows from the fact that the maximal rank of a single-qubit reduced density matrix is 2.

### 2.5.3 Effect of operations on reduced density matrix rank

The following proposition, lemma and corollary are here to show what the effect of admissible multi-local operations is on the rank of reduced density matrices of multi-body pure states. The facts they convey are used for the study of pure state classification. The following proposition introduces an operator representation which greatly simplifies the demonstration of the effects of operators on state-vectors.

**Proposition 2.2.** *Any linear operator $A \in \mathbb{C}^{m\times n}$ which acts on an n-dimensional vector space $V \in \mathbb{C}^n$ can be written in the form*

$$A = \sum_{i=1}^{n} |\mu_i\rangle\langle x_i|, \tag{2.23}$$

*where $|x_i\rangle$ is an orthonormal basis for $V$.*

*Proof.* The singular value decomposition (SVD) of the matrix $A$ ensures that it can be written in the form

$$A = U\Lambda V^\dagger = \sum_j \lambda_j u_j v_j^\dagger, \tag{2.24}$$

where $u_j \in \mathbb{C}^n$ and $v_j \in \mathbb{C}^m$ are the $j$'th column vectors of the matrices $U \in \mathbb{C}^{m\times m}$ and $V \in \mathbb{C}^{n\times n}$ respectively (see Appendix A). This is the *spectral decomposition* of $A$. Using the orthonormal basis vectors $|x_i\rangle$ for the vector space $V$, each vector $v_j$ can be expressed as $v_j = \sum_{i=1}^n \alpha_{ij} |x_i\rangle$, which in turn allows $A$ to be written as

$$\begin{aligned} A &= \sum_j \lambda_j u_j \left( \sum_{i=1}^n \alpha_{ij}^* \langle x_i| \right) \\ &= \sum_{i=1}^n \left( \sum_j \lambda_j \alpha_{ij}^* u_i \right) \langle x_i| \\ &= \sum_{i=1}^n |\mu_i\rangle\langle x_i|, \end{aligned}$$

where $|\mu_i\rangle = \sum_j \lambda_j \alpha^*_{ij} u_i$. Note that two different representations were used for a vector, for example $u_j$ and $|\mu_i\rangle$. □

With this in hand, it can now be shown what the effect is of a general local operation $\mathcal{E}$, composed of a single Kraus operator $E_A$, on a reduced density matrix $\rho_a$ of an $n$-level quantum system '$a$'. This is what is presented in the following lemma and corollary.

**Lemma 2.2.** *Let $|\psi\rangle, |\phi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ be bipartite vectors with reduced density matrices $\rho_a^\psi$, $\rho_b^\psi$, $\rho_a^\phi$ and $\rho_b^\phi$ respectively, and let $E_A \in \mathbb{C}^{n\times n}$ be a Kraus operator such that*

$$|\phi\rangle = E_A \otimes I_B |\psi\rangle . \tag{2.25}$$

*Then the ranks of the reduced density matrices satisfy $r(\rho_a^\psi) \geq r(\rho_a^\phi)$ and $r(\rho_b^\psi) \geq r(\rho_b^\phi)$.*

*Proof.* [13] Appendix A. Consider the Schmidt decomposition of state $|\psi\rangle$,

$$|\psi\rangle = \sum_{i=1}^{n_\psi} \lambda_i |i\rangle|i\rangle , \; n_\psi \leq \min(m, n). \tag{2.26}$$

Then the reduced density matrix of system '$a$' is $\rho_a^\psi = \sum_{i=1}^{n_\psi} |\lambda_i|^2 |i\rangle\langle i|$. As shown in lemma 2.2, the operator $E_A$ can be written as $E_A = \sum_{i=1}^{n} |\mu_i\rangle\langle i|$. So the effect of this operation on $\rho_a^\psi$ can then be concisely written as

$$\begin{aligned} \rho_a^\phi &= E_A \rho_a^\psi E_A^\dagger \\ &= \sum_{i=1}^{n_\psi} |\lambda_i|^2 |\mu_i\rangle\langle\mu_i|. \end{aligned}$$

It follows now that the rank $r(\rho_a^\phi) \leq n_\psi$ because the vectors $|\mu_i\rangle$ are not necessarily linearly independent. The equalities only hold if all vectors $|\mu_1\rangle, \ldots, |\mu_{n_\psi}\rangle$ are linearly independent.

□

**Corollary 2.1.** *If the vectors* $|\psi\rangle$ *and* $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \cdots \otimes \mathcal{H}_N$ *are connected by a multi-local operator as* $|\phi\rangle = E_A \otimes E_B \otimes \cdots \otimes E_N |\psi\rangle$*, then the local ranks satisfy* $r(\rho_\kappa^\psi) \geq r(\rho_\kappa^\phi)$*,* $\kappa = a, b, \ldots, n$*.*

*Proof.* [13] Appendix A. The operator $E_A \otimes E_B \otimes \cdots \otimes E_N$ can be implemented by subsequent applications of the operators $E_A \otimes I_B \otimes \cdots \otimes I_N$, $I_A \otimes E_B \otimes \cdots \otimes I_N$, etc. Repeated application of the previous lemma and lemma 2.1 then shows that the local ranks $r(\rho_a)$, $r(\rho_b)$, etc. either stay invariant or decrease under these operations. □

What this implies is that for multi-qubit systems, the number of entangled qubits can only stay the same, or decrease under (multi-) local operations. This supports the idea that entanglement is a trait which cannot be attributed to individual properties of a many-body entangled system.

## 2.6 Quantifying entanglement

Entanglement is a property of multi-body systems, and can not be understood in terms of the aggregate properties of individual constituents. Therefore it can be intuitively understood that operations which only affect a multi-body state multi-locally can not increase the degree of quantum correlations between the separated constituents of the system. This is a powerful idea which is integral to the notion of entanglement quantification and pure state classification. The knowledge of the effects of general quantum operations is now used for the introduction of entanglement monotones, functions which serve to quantify the amount of entanglement present in multi-body systems.

### 2.6.1 Entanglement monotones

A quantitative measure of entanglement carries with it the requirement of being a monotonic function whose behavior depends highly on the action of multi-local operators. Consider the state $\rho$ of a multi-body system and the admissible local operator $\mathcal{E}_{A,\omega}$ which acts on a subsystem '$a$', in conjunction with identity operators of the other subsystems. An entanglement monotone $f : \rho \mapsto f(\rho)$ satisfies

1. For an admissible local quantum operation $\mathcal{E}_{A,\omega}(\rho) = \sum_{i\in\omega} E_{A,i}\rho E_{A,i}^{\dagger}$ performed by party A on a density matrix $\rho$

$$f(\rho) \geq \sum_{i\in\omega} p_i f(\rho_i), \tag{2.27}$$

   where $\rho_i = \frac{1}{p_i} E_{A,i}\rho E_{A,i}^{\dagger}$ and $p_i = \mathrm{Tr}[E_{A,i}\rho E_{A,i}^{\dagger}] = \mathrm{Tr}[E_{A,i}E_{A,i}^{\dagger}]$ since $\mathrm{Tr}\rho = 1$.

2. For any *ensemble* $\{q_i, \rho_i\}$ such that $\rho = \sum_i q_i\rho_i$

$$\sum_i q_i f(\rho_i) \geq f(\rho). \tag{2.28}$$

   N.B. This is a different statement than 1. because in this case $\rho$ is a probabilistic ensemble of the $\rho_i$ and in 1. $\rho$ is equal to a single $\rho_i$.

3. The value of an entanglement monotone is constant for separable states under LOCC and SLOCC. This value can artificially be set to zero for the sake of simplicity, $f(\rho) = 0$ if $\rho$ is separable.

These two properties define the appropriate behavior of an entanglement monotone. As will be elaborated on in section 2.7, an entanglement monotone must be invariant under reversible LOCC. This is a result of the fact that LOCC keep the degree of quantum correlation invariant if they can be applied reversibly.

### 2.6.2 Entropy of entanglement

For two-qubit or more general two-body states entanglement was suggested to be parameterized by the Shannon entropy of the squares of the Schmidt coefficients [1],

$$E(\psi) = -\sum_i |\lambda_i|^2 \log_2 |\lambda_i|^2. \tag{2.29}$$

This is equivalent to the von Neumann entropy of the reduced density matrices of one of the two subsystems, $E(\rho) = -\mathrm{Tr}(\rho_a \log_2(\rho_a))$. This function is maximal when the Schmidt coefficients have equal absolute values of $\frac{1}{\sqrt{2}}$. Equivalently this function achieves its maximal value of unity when the eigenvalues of one of the reduced density matrices $\rho_a$ are both $\frac{1}{2}$. If this is the case, the two systems are in this thesis said to be *maximally entangled.* The simplest example of maximally entangled systems are those in one of the Bell states.

### 2.6.3 Concurrence

The concurrence came about when defining another measure for entanglement for bi-partite pure states [21, 43]. For two-qubit pure states the starting point is a canonical orthonormonal basis, referred to as the 'magic basis'. This basis is defined in terms of the four Bell states as follows

$$\begin{aligned}
|e_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|e_2\rangle &= \frac{1}{\sqrt{2}} i(|00\rangle - |11\rangle) \\
|e_3\rangle &= \frac{1}{\sqrt{2}} i(|01\rangle + |10\rangle) \\
|e_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned}$$

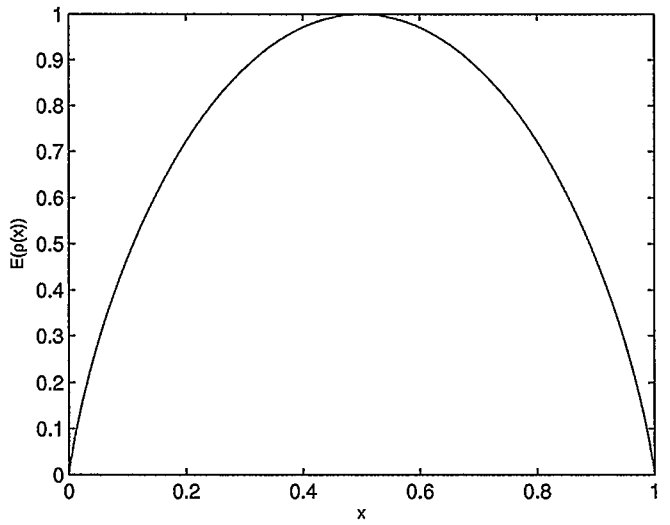



Figure 2.1: A plot of the entropy of entanglement $E(\rho) = -\mathrm{Tr}\rho_a \log_2(\rho_a)$ for all possible absolute values of the two-qubit pure state density matrix eigenvalues. The reduced density matrix is given by $\rho_a = x|a_1\rangle\langle a_1| + (1-x)|a_2\rangle\langle a_2|$, where $x \in [0,1]$

Using this basis, any two-qubit pure state $|\psi\rangle$ can be expressed in the form $|\psi\rangle = \sum_{i=1}^{4} \alpha_i |e_i\rangle$, where $\sum_{i=1}^{4} |\alpha_i|^2 = 1$ so that $|\psi\rangle$ is normalized. The concurrence $C(\psi)$ is then defined as the value $C(\psi) = \left|\sum_{i=1}^{4} \alpha_i^2\right|$. The concurrence for general two-qubit density matrices $\rho$ is expressed in terms of the square roots $\lambda_i$ of the eigenvalues of the matrix $\rho\tilde{\rho} = \rho(\sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y)$. Here $\rho^*$ denotes the complex conjugation of $\rho$ when expressed in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and $\sigma_y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$. The concurrence is now the function

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{2.30}$$

where the eigenvalues $\lambda_i$ are represented in decreasing order according to the index $i$ ($\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$).

### 2.6.4 Tangle

Tangle is an entanglement monotone which can be used to quantify entanglement of two- and three-qubit systems. For two-qubit states the function can be expressed as the square of the concurrence $\tau_{ab} = C^2$. For two-qubit pure states it reduces to $\tau = 4\det(|\rho_a|)$, where $\rho_a$ is the reduced density matrix of one of the qubits [8, 13, 25]. The 3-tangle is an entanglement monotone of 3-qubit states and uses the concurrence of the subsystems. The 3-tangle for 3-qubit pure states of systems '$a$', '$b$' and '$c$' is given by

$$\tau = 4\det(|\rho_a|) - C_{ab}^2 - C_{ac}^2, \tag{2.31}$$

where $\rho_a$ is the reduced density matrix of a single qubit (after qubits '$b$' and '$c$' have been traced out), and $C_{ab}$ and $C_{ac}$ are the concurrence values of reduced density matrices $\rho_{ab}$ and $\rho_{ac}$ (here qubits '$c$' and '$b$' have been traced out respectively).

### 2.6.5 Schmidt measure

The Schmidt measure is an entanglement monotone that has extensively been used in the study of entanglement in graph states [15, 20, 19], which will be introduced in the next chapter. The Schmidt measure is a function of the Schmidt rank $n_\psi$, introduced in section 2.3.2 and is defined as $P(\rho^\psi) = \log_2(n_\psi)$. Note that this is a *discontinuous* function of the integer $n_\psi$. Of this list, this is the only entanglement monotone which is invariant under SLOCC, as opposed to LOCC.

## 2.7 Entangled pure-state classification

Two $n$-qubit pure-states $|\psi\rangle$ and $|\phi\rangle$ are said to belong to the same *entanglement class* if there exists a multi-local operation under which a single copy of one can be converted into a single copy of the other with some non-zero probability. That is, if this is true for SLOCC operations. If a transformation can be achieved by LOCC, it can be done with certainty (*i.e.,* probability one). Two states are said to be *equivalent* under a certain type of multi-local operation if they can be transformed into each other in both directions. This implies that a reversible operation relates them. The orbit of states of a certain reversible multi-local operation constitutes an entanglement class. The fact that these operations must be reversible places a restriction on the possible operators under which entanglement classes can be defined, namely that these operators must be invertible. It was shown in [42, 13, 3] that the only LOCC operations which leave the entanglement class invariant are multi-local unitary operations, from now on referred to as LU. Reversible SLOCC operations are shown to fall under the group of invertible multi-local operators, which is the multi-local general linear group.

**Theorem 2.2.** *Let $|\psi\rangle$ and $|\phi\rangle$ be two pure states of the same quantum system. Then the existence of an invertible multi-local operator which can transform them into each other is a necessary and sufficient condition for these states to be SLOCC-equivalent.*

*Proof.* [13] Appendix A. As preliminary remark, it is worthwhile to evoke lemma 2.2 which shows that the Schmidt numbers must be equal, $n_\psi = n_\phi$. This is because the lemma shows that if this in not the case, one of the transformations $|\psi\rangle \rightarrow |\phi\rangle$ or $|\phi\rangle \rightarrow |\psi\rangle$ is impossible. Additionally, it is assumed that any SLOCC operation can

be represented by a multi-local operator.

For simplicity, but without loss of generality, let $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ be two-qubit states with equal Schmidt numbers $n$. The two qubits, labeled '$a$' and '$b$', are held by parties $A$ and $B$. Let the Schmidt decompositions of $|\psi\rangle$ and $|\phi\rangle$ by such that

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{n} \lambda_i^{\psi} |a_i^{\psi}\rangle |b_i^{\psi}\rangle \\ |\phi\rangle &= \sum_{i=1}^{n} \lambda_i^{\phi} |a_i^{\phi}\rangle |b_i^{\phi}\rangle , \end{aligned}$$

where $|a_i^{\psi}\rangle$, $|b_i^{\psi}\rangle$, $|a_i^{\phi}\rangle$ and $|b_i^{\phi}\rangle$ are orthonormal basis vectors. In order to simplify the argument a little more, set $|b_i^{\psi}\rangle = |b_i^{\phi}\rangle = |b_i\rangle$. This does not take away from the validity of the generalized argument, but does make it easier to convey. An operator which converts $|\psi\rangle$ into $|\phi\rangle$ can readily be defined with the operator

$$E_A = \sum_{i=1}^{n} \frac{\lambda_i^{\phi}}{\lambda_i^{\psi}} |a_i^{\phi}\rangle\langle a_i^{\psi}| \tag{2.32}$$

and the identity operator $I_B$, so that $E_A \otimes I_B |\psi\rangle = |\phi\rangle$. If the operator $E_A$ only has one non-zero eigenvalue, it can always be made invertible by adding to it the term $|a_2^{\phi}\rangle\langle a_2^{\psi}|$ so that

$$E_A = \frac{\lambda_1^{\phi}}{\lambda_1^{\psi}} |a_1^{\phi}\rangle\langle a_1^{\psi}| + |a_2^{\phi}\rangle\langle a_2^{\psi}|. \tag{2.33}$$

The inverse of this matrix is then

$$E_A^{-1} = \begin{cases} \frac{\lambda_1^{\psi}}{\lambda_1^{\phi}} |a_1^{\psi}\rangle\langle a_1^{\phi}| + \frac{\lambda_2^{\psi}}{\lambda_2^{\phi}} |a_2^{\psi}\rangle\langle a_2^{\phi}|, & n = 2 \\ \frac{\lambda_1^{\psi}}{\lambda_1^{\phi}} |a_1^{\psi}\rangle\langle a_1^{\phi}| + |a_2^{\psi}\rangle\langle a_2^{\phi}|, & n = 1 \end{cases} \tag{2.34}$$

if $n = 1$, which gives $E_A E_A^{-1} = E_A^{-1} E_A = I_A$. The operator $E_A \otimes I_B$ is now an invertible operator which transforms $|\psi\rangle$ to $|\phi\rangle$, and its inverse $E_A^{-1} \otimes I_B$ does the reverse operation. This proof is easily generalized to the case in which $|b_i^{\psi}\rangle \neq |b_i^{\phi}\rangle$

and pure states of the form $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \otimes \cdots$ by iteratively following the proposed procedure with operators of the form $E_A \otimes I_B \otimes \cdots$, $I_A \otimes E_B \otimes \cdots$, etc. The overall invertible multi-local operator will then have the form $E_A \otimes E_B \otimes \cdots$, with inverse $E_A^{-1} \otimes E_B^{-1} \otimes \cdots$. □

A general invertible operator of the form $E_A = \sum_{i=1}^{n} \lambda_i |b_i\rangle\langle a_i|$ with $|b_i\rangle$ and $|a_i\rangle$ being orthonormal basis vectors for an $n$-dimensional vectors space, satisfies

$$E_A^\dagger E_A = \sum_{i=1}^{n} |\lambda_i|^2 |a_i\rangle\langle a_i| \leq I_A. \tag{2.35}$$

This implies that the probability with which an invertible operator converts some pure state into another is generally less than one because $\mathrm{Tr}(E_A^\dagger E_A) = \sum_i |\lambda_i|^2$ . This means that states which are related by an invertible multi-local operator are SLOCC-equivalent. The operation can be performed with certain success only if the equality holds. The equality holds only when $|\lambda_i|^2 = 1$ for all $\lambda_i$. States which can be transformed into each other with certainty are LOCC equivalent, and since only unitary matrices have the required properties, LOCC-equivalent states are related by multi-local unitary operators, LU.

The existence of an invertible multi-local operator which transforms two states into each other, in order for the two states to be SLOCC-equivalent says that such an operator must be in the *general linear group* $\mathrm{GL}_2(\mathbb{C})^{\otimes n}$ if these are states of multi-*qubit* systems. The general linear group is the set of all invertible square matrices. These matrices all have non-zero determinants because they would otherwise not be invertible. For all intents and purposes, it suffices to limit the attention to matrices in the *special linear group* $\mathrm{SL}_2(\mathbb{C})^{\otimes n}$, which are all invertible matrices with determinant 1. The reason for this is that the determinant only introduces a physically

insignificant complex constant in the transformed states.

**Theorem 2.3.** *Two states are LOCC equivalent if and only if they are LU equivalent.*

*Proof.* This was shown in the above discussion. Other proofs exist however, see [3, 42]. □

### 2.7.1 Invertible operations and the minimal product decomposition

Besides asking what properties the operations must possess in order to respect an entanglement class, it is natural to ask what properties two states must possess in order to possibly belong to the same entanglement class. It is now shown that equal Schmidt rank is a necessary, however not sufficient condition.

**Proposition 2.3.** *An invertible local operator cannot change the number of terms in a minimal product decomposition of a pure state. (This is given as an observation in [13]).*

*Proof.* Let the minimal product decomposition of some state $|\psi\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ be

$$|\psi\rangle = |a_1\rangle|b_1\rangle + |a_2\rangle|b_2\rangle\,, \tag{2.36}$$

where $|a_i\rangle$ and $|b_i\rangle$ are sets of orthonormal vectors. The effect of an invertible operator $E_A \otimes E_B$, where $E_A$ and $E_B$ act on the subspaces defined by orthonormal vectors $|a_i\rangle$ and $|b_i\rangle$ respectively, then is

$$\begin{aligned} E_A \otimes E_B\,|\psi\rangle &= E_A\,|a_1\rangle \otimes E_B\,|b_2\rangle + E_A\,|a_2\rangle \otimes E_B\,|b_2\rangle \\ &= |a_1'\rangle|b_1'\rangle + |a_2'\rangle|b_2'\rangle\,. \end{aligned}$$

Since $E_A \otimes E_B$ is an invertible operator, the vectors $|a_i'\rangle$ and $|b_i'\rangle$ are linearly independent and $E_A \otimes E_B |\psi\rangle$ has the same number of terms in its minimal product decomposition as $|\psi\rangle$. □

This shows that the Schmidt rank is invariant under invertible local operations and therefore that states with different Schmidt rank belong to different equivalency classes.

### 2.7.2 A two-qubit example

It may be helpful to study a simple concrete example of an invertible operation on a two-qubit system.

**Example 2.3.** *Consider the Schmidt decoposition of a two-qubit pure state*

$$|\psi\rangle = \lambda_1 |a_1\rangle|b_1\rangle + \lambda_2 |a_2\rangle|b_2\rangle . \tag{2.37}$$

*Here the fact is used that the maximal Schmidt number of a two-qubit system is 2, as deduced in section 2.5.2. An invertible local operation $E_A \otimes I_B$ can be represented by its spectral decomposition,*

$$E_A \otimes I_B = \frac{\lambda_1'}{\lambda_1}|a_1'\rangle\langle a_1| \otimes I_B + \frac{\lambda_2'}{\lambda_2}|a_2'\rangle\langle a_2| \otimes I_B, \tag{2.38}$$

*so that its effect on $|\psi\rangle$ is*

$$E_A \otimes I_B |\psi\rangle = \lambda_1' |a_1'\rangle|b_1\rangle + \lambda_2' |a_2'\rangle|b_2\rangle . \tag{2.39}$$

*Here neither $\lambda_1'$ or $\lambda_2'$ are zero since $E_A \otimes I_B$ is assumed to be invertible, so the Schmidt number indeed stays the same. The probability of this operation succeeding is*

$$p = Tr(E_A \otimes I_B|\psi\rangle\langle\psi|E_A^\dagger \otimes I_B) = |\lambda_1'|^2 + |\lambda_2'|^2, \tag{2.40}$$

*which is unity only if the operation was a local unitary transformation and is less otherwise. Although this system is still in an entangled state if the value of p is not unity, the value of an entanglement monotone will have changed. For example, the entropy of entanglement changed from* $-(|\lambda_1|^2 \log_2 |\lambda_1|^2 + |\lambda_2|^2 \log_2 |\lambda_2|^2)$ *to* $-(|\frac{\lambda_1'}{p}|^2 \log_2 |\frac{\lambda_1'}{p}|^2 + |\frac{\lambda_2'}{p}|^2 \log_2 |\frac{\lambda_2'}{p}|^2)$. *Since this operation is invertible it now becomes apparent that the value of an entanglement monotone can decrease, but also increase. The pitfall of this is, however, that such an operation can only succeed with finite probability. This illustrates that SLOCC operations can be used to define larger entanglement classes than LOCC operations.*

From the above example it becomes apparent that there are only two SLOCC-inequivalent two-qubit pure state classes, namely separable states and entangled states. If no entanglement is present in the state at all, there is no multi-local operation that can change that. But if the state is only the slightest bit entangled, there exists an invertible operator which can transform it to any other two-qubit pure state that is also entangled.

## 2.8 Genuine tripartite entanglement

It turns out that for two-qubit systems, there is only a single class of entangled states. A surprising result in [13] however shows, that for three-qubit pure states, there are two genuine tripartite entanglement classes which are inequivalent under SLOCC. These are three-qubit pure states whose reduced density matrices all have rank 2, implying that all three qubits are somehow entangled with the rest of the system. The two classes are represented by the canonical three-qubit entangled

states $|GHZ\rangle$ and $|W\rangle$. The formalisms already presented in this chapter, and the following lemmas are used to show that $|GHZ\rangle$ and $|W\rangle$ indeed belong to different entanglement classes under SLOCC.

### 2.8.1 Product vectors

A key ingredient for the study of classes of fully entangled three-qubit pure states is the existence of product states in a subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$. What sets the two classes apart is the difference in their Schmidt ranks. The following lemma is used to prove that there indeed exist two fully entangled three-qubit pure states with different Schmidt ranks. The term *fully entangled* is introduced to describe pure states in which all the reduced density matrices have rank larger than one.

**Lemma 2.3.** *For every two-dimensional subspace of* $\mathbb{C}_2 \otimes \mathbb{C}_2$ *there is a basis that contains at least one product state, i.e., a state* $|\pi\rangle = |\pi_1\rangle |\pi_2\rangle$.[2]

*Proof.* [18]. Let the subspace be generated by $\{|b_1\rangle, |b_2\rangle\}$. A product state $|\pi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ satisfies

$$\langle 00|\pi\rangle\langle 11|\pi\rangle = \langle 01|\pi\rangle\langle 10|\pi\rangle. \tag{2.41}$$

Inserting $|\pi\rangle = \eta_1 |b_1\rangle + \eta_2 |b_2\rangle$ in equation (2.41) yields a quadratic equation for the complex coefficients $\eta_1$ and $\eta_2$:

$$0 = c_1\eta_1^2 + c_{12}\eta_1\eta_2 + c_2\eta_2^2 \tag{2.42}$$

[2] *This is the way this lemma is posed in [18]. It seems however that the proof shows that it should hold true for* any *basis of a two-dimensional subspace.*

with

$$\begin{aligned} c_1 &= \langle 00|b_1\rangle\langle 11|b_1\rangle - \langle 01|b_1\rangle\langle 10|b_1\rangle, \\ c_{12} &= \langle 00|b_1\rangle\langle 11|b_2\rangle + \langle 11|b_1\rangle\langle 00|b_2\rangle - \langle 01|b_1\rangle\langle 10|b_2\rangle - \langle 10|b_1\rangle\langle 01|b_2\rangle, \\ c_2 &= \langle 00|b_2\rangle\langle 11|b_2\rangle - \langle 01|b_2\rangle\langle 10|b_2\rangle. \end{aligned}$$

If $c_1$ vanishes then $|b_1\rangle$ is a product state and the lemma holds. Similarly, $|b_2\rangle$ is a product state if $c_2 = 0$. Now consider the case $c_1 \neq 0$ and $c_1 \neq 0$. The solutions of equation (2.42) are given by

$$\eta_1 = \frac{-c_{12} \pm \sqrt{c_{12}^2 - 4c_1c_2}}{2c_1}\eta_2. \tag{2.43}$$

For $c_1 \neq 0$ and $c_2 \neq 0$ there is at least one nontrivial solution with $\eta_1 \neq 0$ and $\eta_2 \neq 0$ and thus a product state exists. □

A two-dimensional subspace in $\mathbb{C}^2 \otimes \mathbb{C}^2$ can be seen as a plane defined by two orthonormal unit vectors, which lies in a four-dimensional space. According to equation (2.43), there exists only one product vector in the plane defined by orthogonal vectors $|b_1\rangle$ and $|b_2\rangle$ if $c_{12}^2 = 4c_1c_2$ and two otherwise. If two product vectors exist, then they are orthogonal when $c_2 = -c_1$. This is precisely the reason why a higher order Schmidt decomposition as proposed in section 2.3.1 is sometimes impossible.

### 2.8.2 Two inequivalent classes under SLOCC

A fully entangled three-qubit pure state $|\psi\rangle$ of qubits '$a$', '$b$' and '$c$' has the property that its reduced density matrices $\rho_a$, $\rho_b$ and $\rho_c$ all have rank 2 (by proposition 2.5.2). Therefore its Schmidt decomposition must have at least two terms. Let $|a_i\rangle$ and $|bc_i\rangle$

be orthonormal bases for the vector spaces of qubit-systems '$a$' and '$bc$'. The Schmidt decomposition of a fully entangled three-qubit pure state can then be represented by

$$|\psi\rangle = \lambda_0 |a_0\rangle|bc_0\rangle + \lambda_1 |a_1\rangle|bc_1\rangle . \tag{2.44}$$

The vectors $|bc_0\rangle$ and $|bc_1\rangle$ define a two-dimensional subspace in $\mathbb{C}^2 \otimes \mathbb{C}^2$ since they are two orthonormal two-qubit state vectors. As shown in lemma 2.3 there are either one, or two product vectors in this subspace. This means that only two SLOCC-inequivalent fully entangled three-qubit pure state classes exist; one which has Schmidt rank 2, and one which has Schmidt rank 3. If these vectors are such that two orthonormal product vectors $|b_0\rangle|c_0\rangle$ and $|b_1\rangle|c_1\rangle$ exist in the subspace, then there is a state

$$|\psi\rangle = |a_0\rangle|b_0\rangle|c_0\rangle + |a_1\rangle|b_1\rangle|c_1\rangle , \tag{2.45}$$

which is a state with only two terms in its minimal product decomposition and falls under the class defined by $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. On the other hand, if $|bc_0\rangle$ and $|bc_1\rangle$ define a subspace in which there exists only a single product vector, the state $|\psi\rangle$ has more than two terms in its minimal product decomposition. All states with this property turn out to be SLOCC equivalent to the canonical $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$-state [13]. The fact that these two states have a different number of terms in their minimal product decomposition proves that they are SLOCC-inequivalent by theorem 2.2 and proposition 2.3, and that there are indeed two SLOCC-inequivalent fully entangled three-qubit pure state-classes.

## 2.9 Entanglement classes of larger systems

Finding exactly what the minimal product decomposition for a certain state is, however, far from trivial, as discussed in [20]. Not only does this pose a considerable problem for finding entanglement classes, the rate at which the number of possible classes grows with the number of qubits is perhaps what causes the most important obstacle. Defining entanglement classes by means of LU or SLOCC operations has an important implication for the number of classes in $n$-qubit systems. A general $n$-qubit pure state requires $2^{n+1} - 1$ real parameters to be defined, disregarding an overall phase. An $n$-qubit LU operator requires only $3n - 1$ parameters, and an element from $SL_2(\mathbb{C})^{\otimes n}$, representing an SLOCC operation, requires $6n$ parameters. This implies that it takes at least $2^{n+1}-3n-2$ or $2^{n+1}-6n-2$ real numbers to parameterize inequivalent pure states. For systems composed of more than three qubits, this number is greater than one. As soon as a continuous parameter is needed to classify inequivalent states, this results in an infinite number of inequivalent classes.

## 2.10 Utilizing entanglement

### 2.10.1 Quantum teleportation

Quantum teleportation of an unknown pure state $|\psi\rangle$ from a party $A$, call her Alice, to a party $B$, call him Bob, is most easily explained using the circuit model of quantum computation. The protocol was originally conceived in 1993 [2]. It provides a means to transport a quantum state between parties without attempting to copy it, which was proved impossible by the *no-cloning theorem*, or having the parties physically exchange the medium on which it is stored. A Bell state of which each party holds

one qubit is the physical resourse which allows for this transaction. The protocol is graphically depicted in figure 2.2.

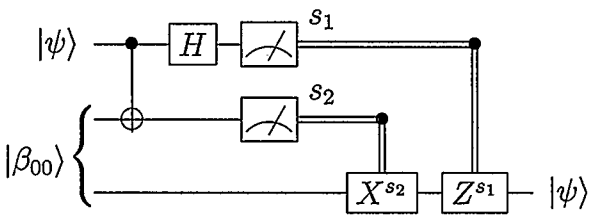



Figure 2.2: Quantum circuit diagram of the single qubit-state teleportation protocol.

Initially, Alice holds qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and one of the qubits in the Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and Bob holds the other qubit of $|\beta_{00}\rangle$. So the initial three-qubit state is

$$|\tau_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right]. \tag{2.46}$$

The protocol is completed in four steps:

1. Alice performs a *controlled-not operation* in which $|\psi\rangle$ is the control and her Bell qubit is the target. The matrix form of this operation is

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2.47}$$

which in the circuit diagram is depicted as

Bob effectively performs an identity operation $I_B$ on his qubit, so the overall effect on the entire state is

$$|\tau_1\rangle = CNOT_A \otimes I_B \, |\psi\rangle \, |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha \, |0\rangle \, (|00\rangle + |11\rangle) + \beta \, |1\rangle \, (|10\rangle + |01\rangle)\right]. \tag{2.48}$$

2. Next, Alice performs a Hadamard operation on her first qubit, represented by ——$\boxed{H}$. The matrix representation of this operator is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.49}$$

The state is now transformed to

$$\begin{aligned} |\tau_2\rangle &= H_A \otimes I_A \otimes I_B \, |\tau_1\rangle \\ &= \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \\ &= \frac{1}{2} [|00\rangle \, (\alpha \, |0\rangle + \beta \, |1\rangle) + |01\rangle \, (\alpha \, |1\rangle + \beta \, |0\rangle) \\ &\quad + |10\rangle \, (\alpha \, |0\rangle - \beta \, |1\rangle) + |11\rangle \, (\alpha \, |1\rangle - \beta \, |0\rangle)], \end{aligned}$$

where the terms have simply be rearranged to obtain $|\tau_2\rangle$ in its final form.

3. Alice performs a von Neumann measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on her two qubits (——$\boxed{\nearrow}$), obtaining the outcomes $\{|s_1 s_2\rangle\}$, $s_1, s_1 \in \{0, 1\}$ each with probability $\frac{1}{4}$.

4. Depending on the outcomes $s_1$ and $s_2$, Bob performs the operations

$$X^0 = Z^0 = I, \; X^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Z^1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.50}$$

obtaining the state $|\psi\rangle$ with 100% probability.

This is not the way the protocol was originally described in [2], but it allows for an easy-to-understand pictorial description. The way it was originally presented does not involve a Hadamard transformation or a CNOT-gate. The only two operations are a von Neumann measurement

$$\{|\beta_{00}\rangle\langle\beta_{00}|, |\beta_{01}\rangle\langle\beta_{01}|, |\beta_{10}\rangle\langle\beta_{10}|, |\beta_{11}\rangle\langle\beta_{11}|\} \tag{2.51}$$

by Alice, and then $X$ and/or $Z$ by Bob depending on Alice's outcome. This protocol can be generalized to mixed states and states of higher level systems. But the reader is referred to the original paper for these discussions.

### 2.10.2 Shor's algorithm

Perhaps the most dramatic manifestation of the power of quantum computation is the efficiency with which Shor's algorithm factors any integer [39]. Up until now, the algorithm is exponentially faster than the best known classical algorithms, which run in exponential time or super-polynomial time, depending on the factorization. It has however not been proven that a classical polynomial time algorithm does not exist. It has been shown by several authors that the speed-up of this algorithm over the classical algorithm is greatest if entanglement is present during some of its operations [22]. More generally, it was shown that the presence of multi-partite entanglement is necessary for a quantum algorithm to require exponentially less resources than an equivalent classical algorithm. Since this thesis is not concerned with computation specifically, the reader is referred to [27, 31] for more detailed discussions of quantum algorithms. For an analysis of where in the algorithm entanglement plays a role, consider the article [24].

# Chapter 3

# Pauli stabilizers

## 3.1 Introduction

An important subclass of $n$-qubit pure states is formed by the so-called *stabilizer states*. These states have the special property that they can be described with only $\mathcal{O}(n)$ parameters, as opposed to general quantum states which require an exponential number of parameters. This does not take away from their usefulness however. They came about in the theory of quantum error correction [16, 6, 5] (and others) and are crucial in one-way model of quantum computation [33]. These states can be represented by Abelian groups known as *stabilizers*, which are composed of tensor products of the Pauli matrices. To avoid confusion it should be noted that, with the eye on the generalization of this in Chapter 4, the name Pauli stabilizer might be more appropriate. However, in quantum information processing, the word stabilizer is generally reserved for the objects defined in this chapter and this will be respected throughout this thesis. A consequence of this representation is that these states are LU-equivalent to some *graph state*, states which can be represented by $n$-vertex undirected simple graphs [36, 40]. In this chapter, properties of stabilizers, stabilizer states and graph states are presented. Section 3.2 introduces stabilizers and stabilizer states. Section 3.3 discusses an interesting finding regarding SLOCC-classes of stabilizers states, namely that these can be easily found using only LU operations. Graph states and graph-state classes are introduced in section 3.4. A few short words

about the applications of stabilizer states and graph states are found in section 3.5.

## 3.2 Stabilizer States

The stabilizers and stabilizer states presented in this section are represented by Abelian groups in $\mathcal{G}_n$, the group of tensor products of $n$ elements of the Pauli group, which will be introduced shortly. This is not the only possible representation, but it allows for some of the basic properties to be readily derived. To begin this, the foundation of all stabilizers is presented first. The basic building blocks of the stabilizer theory are the Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.1}$$

These are Hermitian and unitary so their squares all equal the identity, $\sigma_i^2 = I$ with $i \in \{x, y, z\}$. Pairs of these matrices *anti-commute*,

$$\{\sigma_i, \sigma_j\} = \sigma_i\sigma_j + \sigma_j\sigma_i = 0 \tag{3.2}$$

for all $i \neq j$. The product of two Pauli matrices yields another Pauli with a complex phase, for example $\sigma_x\sigma_y = i\sigma_z$. From this example it is clear that $(\sigma_x\sigma_y)^\dagger = \sigma_y\sigma_x = -i\sigma_z$, which in turn confirms that these matrices anti-commute. The rest of the product relations can be readily derived from this example and the fact that $\sigma_i^2 = I$.

The Pauli group $\mathcal{G}_1$ is composed of the set of all possible products of the Pauli matrices,

$$\mathcal{G}_1 \stackrel{def}{=} \{\pm I, \pm iI, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}. \tag{3.3}$$

This group is also known as the quaternionic group. Its non-trivial elements anti-commute, like the Pauli matrices. The elements written with a factor $i$ are now *anti*-Hermitian however. For these matrices $(\pm i\sigma_i)^2 = -I$.

Next, the group $\mathcal{G}_2$ is composed of the set of tensor products of elements from $\mathcal{G}_1$. Therefore this group can be represented by $\mathcal{G}_2 = \mathcal{G}_1 \otimes \mathcal{G}_1$. Its elements can either commute, or anti-commute. As before, its elements can be either Hermitian or anti-Hermitian. The properties of of $\mathcal{G}_2$ are common to any of the groups $\mathcal{G}_n = \mathcal{G}_1^{\otimes n}$ with $n \geq 2$. Now that this mathematical tool has been gathered, it is time to define what a stabilizer is. It should be noted that no distinction is made between a (state-) vector $|\psi\rangle$ and a *ray*, which is the set $\{\alpha |\psi\rangle : \alpha \in \mathbb{C},\ \alpha \neq 0\}$.

**Definition 3.1.** *The stabilizer $S$ is an Abelian (which means commuting) subgroup of $\mathcal{G}_n$ that has a set of common eigenvectors $T = \{|\psi_i\rangle\}$ with eigenvalue +1. The set $T$ will be referred to as the coding space, which is a term borrowed from quantum error correction.*

$$S \stackrel{def}{=} \{M : M |\psi_i\rangle = |\psi_i\rangle\,,\ M \in \mathcal{G}_n\}. \tag{3.4}$$

A stabilizer must be an Abelian group because only commuting operators have complete sets of common eigenvectors (as required by the definition). Besides this, all elements $M$ of a stabilizer $S$ have the following properties.

**Proposition 3.1.** *All elements $M$ of a stabilizer $S$ are Hermitian and are not equal to $-I$.*

*Proof.* Let $|\psi\rangle \in T$ be a vector in the coding space of the stabilizer $S$. Then the operator $-I$ satisfies $-I |\psi\rangle = -|\psi\rangle$, immediately excluding this as a possible element of $S$. By contradition it can be proved that any $M \in S$ is a Hermitian operator.

To this end, suppose that $M$ is anti-Hermitian. Since $M \in S$, $M|\psi\rangle = |\psi\rangle$ and therefore

$$M^2|\psi\rangle = M|\psi\rangle = |\psi\rangle . \tag{3.5}$$

But since $M$ is assumed to be anti-Hermitian, the following should also be true:

$$M^2|\psi\rangle = -I|\psi\rangle = -|\psi\rangle . \tag{3.6}$$

The assumption has led to contradictory statements, showing that it was wrong. Since any $M \in \mathcal{G}_n$ is either Hermitian or anti-Hermitian, it can be concluded that any stabilizer element $M \in S$ must be a Hermitian operator. □

A stabilizer $S$ can be defined by a subset of its elements known as the *generator*. This is a collection of its elements such that any element of $S$ can be written as a product of them. The smallest generator is a subset of elements $M_1, M_2, \ldots, M_l$ with $0 \leq l \leq |S|$, where $|S|$ denotes the *cardinality*, which is the total number of elements, of $S$, such that these elements are independent. A set is said to be independent if no non-trivial product of its elements yields the identity. A consequence of this is that no product of generator elements can yield a matrix which is already in the generating set. If this were the case then there would be a non-trivial product of generator matrices yielding the identity because of the fact that all stabilizer elements are unitary and Hermitian. Using the notion of a generator and the fact that any stabilizer is an Abelian group, the following lemma can be formulated.

**Lemma 3.1.** *Let $S$ be a stabilizer in $\mathcal{G}_n$. Then its cardinality $|S| = 2^l$ for some $0 \leq l \leq n$.*

*Proof.* Let $S$ have a generator of $l$ independent elements $M_1, M_2, \ldots, M_l$. Then, since $S$ is Abelian, and all $M_i$ are Hermitian, any element $M \in S$ can be written as

$$M^{\mathbf{x}} = M_1^{x_1} M_2^{x_2} \cdots M_l^{x_l}, \tag{3.7}$$

where $x_i \in \{0,1\}$ and $\mathbf{x} \in \{0,1\}^l$. There are $2^l$ different vectors $\mathbf{x}$, so $S$ contains at most $2^l$ different elements $M^{\mathbf{x}}$.

Suppose now, that $l \leq |S| < 2^l$. This means that there are at least two different vectors $\mathbf{x}_1, \mathbf{x}_2$ which give rise to the same stabilizer element $M^{\mathbf{x}_1} = M^{\mathbf{x}_2}$. But since any element $M^{\mathbf{x}} \in S$ is Hermitian and unitary, it is then possible for a non-trivial product of the generator elements to give rise to the identity. This is in contradiction with the properties of a generator, as described above and it can therefore be concluded that the cardinality $|S| = 2^l$ exactly. □

A stabilizer can be used as an alternative representation of a special class of pure states known as stabilizer states. In order to prove that this is possible, the following proposition and lemma are used.

**Proposition 3.2.** *Let $S \in \mathcal{G}_n$ be a stabilizer of cardinality $|S| = 2^l$ with $0 \leq l \leq n$. Then the normalized sum*

$$\rho = \frac{1}{2^n} \sum_{M \in S} M, \tag{3.8}$$

*satisfies the properties of an orthogonal projector up to a normalization factor.*

*Proof.* Recall that an orthogonal projector $P$ satisfies $P^\dagger = P$ and $P^2 = P$. Firstly, since all $M \in S$ are Hermitian, $\rho^\dagger = \rho$, satisfying the first property of an orthogonal projector. Secondly,

$$\rho^2 = \frac{1}{2^n} \sum_{M \in S} (M\rho) = \frac{|S|}{2^n} \rho. \tag{3.9}$$

This follows from the fact that for any $M_i \in S$, $M_i\rho = \frac{1}{2^n}\sum_{M\in S} M_i M = \frac{1}{2^n}\sum_{M\in S} M$, since $S$ is a closed group. This shows that the second property of an orthogonal projector is satisfied up to a factor $\frac{|S|}{2^n}$. □

What can be deduced from these properties of an object $\rho$ is that it is a positive semi-definite matrix, meaning that it only has eigenvalues which are greater than or equal to zero. It also has unit trace. It is no coincidence that these properties are is also satisfied by density matrices. The second property was somewhat artificially implemented by using the normalization factor $\frac{1}{2^n}$, which causes the trace of $\rho$ to be one. The only element of $\mathcal{G}_n$ which has a non-zero trace is the $2^n \times 2^n$ identity matrix, hence the factor $\frac{1}{2^n}$ normalizes $\rho$. This now leads to the following lemma and theorem.

**Lemma 3.2.** *Let $S \in \mathcal{G}_n$ be a stabilizer of cardinality $|S| = 2^n$. Then the projector $\rho = \frac{1}{2^n}\sum_{M\in S} M$ has a unique non-zero eigenvalue $+1$, which occurs with multiplicity one.*

*Proof.* Consider the spectral decomposition

$$\rho = \sum_{i=1}^{m} \lambda_i |\psi_i\rangle\langle\psi_i|, \tag{3.10}$$

for some $0 \leq m \leq 2^n$, whose value is as yet unknown, and orthonormal $2^n$-dimensional vectors $|\psi_i\rangle$. Proposition 3.2 tell us that $\rho^2 = \rho$ because $|S| = 2^n$. This implies that $\mathrm{Tr}\rho = \mathrm{Tr}(\rho^2) = 1$ and since the trace is simply the sum of eigenvalues,

$$\sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \lambda_i^2 = 1. \tag{3.11}$$

Since all $\lambda_i$ are positive, this can only be true if $m = 1$ and the only eigenvalue is $\lambda = 1$. This shows that $\rho = |\psi\rangle\langle\psi|$ and thus only has a single eigenvector $|\psi\rangle$. □

**Theorem 3.1.** *A stabilizer $S \in \mathcal{G}_n$ with cardinality $|S| = 2^n$ uniquely stabilizes a single vector $|\psi\rangle$.*

*Proof.* A contradictory assumption that the coding space of $S$ contains more than a single element can be shown to lead to contradictory statements, proving the theorem to be correct. To this end, consider the stabilizer to stabilize two vectors $|\psi_1\rangle$ and $|\psi_2\rangle$. This means that in the spectral decomposition of the operators $M \in S$, both these vectors appear as eigenvectors with eigenvalue $+1$. Subsequently, the sum

$$\rho = \frac{1}{2^n} \sum_{M \in S} M = \frac{1}{2^n} \sum_{i=1}^{2^n} M_i = \frac{1}{2^n} \sum_{i=1}^{2^n} \left( \sum_{j=1}^{2^n} \lambda_{ij} |\psi_j\rangle\langle\psi_j| \right), \tag{3.12}$$

contains the term $|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$. This implies, however that $\rho$ has at least two eigenvectors with non-zero eigenvalues, which is contradictory to what was proved in lemma 3.2. This proves that the assumption was wrong, and that $S$ indeed only stabilizes a single vector. □

Since a stabilizer $S \in \mathcal{G}_n$ with cardinality $2^n$ stabilizes only a single vector, it can be used to uniquely define this vector and thus be used as a different representation. States which allow such a representation are commonly referred to as *stabilizer states.* Of course, introducing an overall factor or phase would not change the stabilizer of a stabilizer state. This is however physically insignificant and will therefore not be taken in consideration. If a stabilizer $S \in \mathcal{G}_n$ has cardinality $0 < |S| < 2^n$, it stabilizes multiple pure states, and therefore also some mixed states. This is a property which is applied in the theory of quantum error correction, which will be briefly discussed in section 3.5.1.

## 3.3 Stabilizer states, SLOCC $\equiv$ LU

Defining equivalency classes for stabilizer states turns out to be a great deal simpler then for most other entangled states. Unlike for general $n$-qubit states, for stabilizer states, SLOCC-equivalence implies LU-equivalence. The key realization leading to this conclusion originated from the construction of a so-called normal form of fully entangled states [41].

### 3.3.1 A normal form

In [41] an algorithm is presented which, when performed on a fully entangled $n$-qubit pure state vector, converges to a vector which is called the normal form of that state vector[1]. This normal form can be defined as follows.

**Definition 3.2.** *The normal form of a fully entangled n-qubit pure state $|\psi\rangle$ is such that the reduced density matrices $\rho_i$ of qubits labeled 'i' where $i \in \{1, \ldots, n\}$, are proportional to the identity matrix $\rho_i = cI$, where c is some proportionality factor.*

Since the assumption is made that the state is fully entangled, all the reduced density matrices $\rho_i$ must have rank 2, as proved in lemma 2.1. The following is part of the proof of the existence of an SLOCC operator which can bring a fully entangled $n$-qubit pure state into its normal form, adapted from the proof as presented in [40]. The original more in-depth version can be found in [41].

**Theorem 3.2.** *Let $\rho$ be an n-qubit density operator such that all its single-qubit reduced density matrices are of rank 2. Then there exists an SLOCC operator which*

[1]It should be noted that many different normal forms can be defined. So what it referred to in this thesis as *the normal form* is by no means unique.

*transforms $\rho$ into its normal form.*

*Proof.* Let $\rho$ be an $n$-qubit pure state whose single-qubit reduced density matrices are of rank 2, and let $A_1 \otimes \cdots \otimes A_n$ be a multi-local operator in $\mathrm{SL}_2(\mathbb{C})^{\otimes n}$. The operators $A_i$ which will bring $\rho$ in its normal form can be determined by an iterative process by which in each step, the trace of $\rho$ is minimized by a single party using SLOCC operations. Consider the reduced density matrix $\rho_1 = \mathrm{Tr}_{2,\ldots,n}\rho$. If this matrix is indeed non-singular then the operator

$$X = \det(\rho_1)^{\frac{1}{4}}\rho_1^{-\frac{1}{2}} \tag{3.13}$$

has the property that when acted on $\rho_1$, it yields

$$\begin{aligned} X\rho_1 X^\dagger &= \det(\rho_1)^{\frac{1}{2}}\rho_1^{-\frac{1}{2}}\rho_1\rho_1^{-\frac{1}{2}\dagger} \\ &= \det(\rho_1)^{\frac{1}{2}} I \\ &= cI. \end{aligned}$$

Here the fact was used that $\rho_1$ is an orthogonal projector, thus $\rho_1^{-\frac{1}{2}\dagger} = \rho_1^{-\frac{1}{2}}$. Since $\mathrm{Tr}\rho = 1$,

$$\begin{aligned} \mathrm{Tr}\rho' &= \mathrm{Tr}(X \otimes I \cdots \otimes I)\rho(X \otimes I \cdots \otimes I)^\dagger \\ &= 2\det(\rho_1)^{\frac{1}{2}} \\ &\leq \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\rho) = 1 \end{aligned} \tag{3.14}$$

If the eigenvalues of $\rho_1$ are denoted by $\lambda_1$ and $\lambda_2$ then the inequality 3.14 can be written as

$$2\sqrt{\lambda_1\lambda_2} \leq \lambda_1 + \lambda_2.$$

Equality of these two terms is only satisfied if $\lambda_1 = \lambda_2$, or equivalently if $\rho_1 = cI$. The inequality indicates that the operation $X$ is trace decreasing. So if this type of operation is performed by each of the parties in an iterative fashion, the trace of $\rho$ will keep decreasing unless all the reduced density matrices are proportional to $I$. Since the eigenvalues of $\rho'$ are always positive, they are bounded from below, which implies that all the reduced density matrices converge to operators arbitrarily close to $I$. And since the matrices of the form $X$ are elements of $\mathrm{SL}_2(\mathbb{C})$, the existence of SLOCC operators which bring a density operator to its normal form is proved. □

In the case where one of the qubits is not entangled with the rest of the system, according to proposition 2.1 its reduced density operator has rank one, and its corresponding operator $X$ will have infinite norm which results in $X\rho_1 X^\dagger = 0$ and thus a zero normal form of $\rho$. The matrix $\rho'$ which the normal form of some pure state $\rho$ was pointed out to be unique up to local unitary transformations (LU) in [4], as was originally conjectured in [41]. A local unitary transformation on a matrix $\rho'$ can be defined analogously to such a transformation on a state vector $|\psi\rangle$. It is simply a mapping $U \in U(2)^{\otimes n} : \rho' \mapsto U(\rho')$. A corollary of this and theorem 3.3.1 is that two states $\rho^\psi$ and $\rho^\phi$ can only be SLOCC equivalent if they have LU-equivalent normal forms.

### 3.3.2 Reduced stabilizers

It turns out that the reduction to a normal form has a particularly nice consequence for stabilizer states, namely that SLOCC-equivalence reduces to LU-equivalence because stabilizer states are already in their normal forms. To prove this, a concept is needed which is interesting in its own right, the reduced stabilizer.

Consider what happens to the stabilizer of some $n$-qubit pure state when part of the system is traced out. This is an adapted version of the presentation in [40]. First consider a two qubit pure state of qubits '$a$' and '$b$', represented by its density matrix $\rho$, and its stabilizer $S$. The stabilizer elements $M \in S$ are of the general form $M_i = \sigma_{a_i} \otimes \sigma_{b_i}$. When qubit '$b$' is traced out, the reduced density matrix $\rho_a = \mathrm{Tr}_b(\rho)$ is obtained, representing the state of qubit '$a$'. But since the mathematical objects $\rho$ and $S$ can be used to describe the same state, tracing out the operators $\sigma_{b_i}$ in all $M \in S$ yields the stabilizer $S_a$ for the state represented by the reduced density matrix $\rho_a$. This stabilizer is the reduced stabilizer for the state of qubit '$a$'. The effect of tracing out the operator $\sigma_{b_i}$ in an $M_i \in S$ is

$$\mathrm{Tr}_b M_i = \sigma_{a_i} \otimes \mathrm{Tr}(\sigma_{b_i}), \tag{3.15}$$

which is non-zero only if $\sigma_{b_i} = I$ since the Pauli matrices all have zero trace. Note that for matrices $A_1, A_2, \ldots, A_n$, $\mathrm{Tr}(A_1 \otimes A_2 \otimes \cdots \otimes A_n) = \mathrm{Tr}(A_1) \otimes \mathrm{Tr}(A_2) \otimes \cdots \otimes \mathrm{Tr}(A_n)$. This leads to the concept of the support of a stabilizer element. Suppose for simplicity that the qubits of an $n$-pure state with stabilizer $S$ are labeled with numbers 1 to $n$, and that some subset $\bar{\omega} \subseteq \{1, \ldots, n\}$ of these are traced out. The only elements $M \in S$ which yield non-zero reduced stabilizer elements after this operation are those which act with an identity operation $I$ on the qubits with labels $\bar{\omega}$. The support of an element $M = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \in S$ is defined as the set of number labels $j$ such that $\sigma_j \neq I$. This is written as

$$\mathrm{supp}(M) \stackrel{def}{=} \{j \in \{1, \ldots, n\} : \sigma_j \neq I\}. \tag{3.16}$$

Using this it becomes much simpler to define the reduced stabilizer of a state of which qubits $\bar{\omega}$ have been traced out. The complement of $\bar{\omega}$ are the numbers between

1 and $n$, which are not in $\bar{\omega}$, call this set $\omega$. So qubits with labels $\omega$ are the ones that are not traced over. The only stabilizer elements $M \in S$ that yield non-zero reduced stabilizer elements are those whose support is in $\omega$, so the reduced stabilizer $S_\omega$ can be represented by

$$S_\omega = \{M \in S : \text{supp}(M) \subseteq \omega\}. \tag{3.17}$$

This has an important implication for the normal form of stabilizer states, which is presented in the following lemma.

**Lemma 3.3.** *Let $|\psi\rangle$ be a fully entangled $n$-qubit stabilizer state. Then the reduced density matrices $\rho_i^\psi$ of qubits with labels $i \in \{1, \ldots, n\}$ are such that $\rho_i^\psi = cI$, which means that $|\psi\rangle$ is already in its normal form.*

*Proof.* Following the discussion on reduced stabilizers, let $\omega = i$ and thus $|\omega| = 1$. The rank $r(\rho_i^\psi)$ is either 1 or 2 because it is a $2 \times 2$ matrix. But since it was assumed that the state is fully entangled $r(\rho_i^\psi) = 2$. What this says about the cardinality of the reduced stabilizer is that $|S_i| = 1$ because if $|S_i|$ was 2, $r(\rho_i^\psi)$ would be 1 since $\rho_i^\psi$ would be a pure state by theorem 3.1, which it is not. Therefore $S_i = I^{\otimes n}$ since it must form a closed group under matrix multiplication. Using the identity $\rho^\psi = \frac{1}{2^n} \sum_{M \in S_\psi} M$ it can then be concluded that $\rho_i = cI$. □

This shows that all stabilizer states are already in a SLOCC normal form and therefore that SLOCC-equivalence is equal to LU-equivalence for these types of states.

## 3.4 Graph states

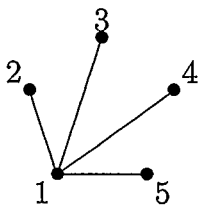
Graph states [37, 36, 10] are a subset of the stabilizer states. These states have the property that the generator of their stabilizer takes the form of an $n \times n$ adjacency matrix $\theta$ of some graph, concatenated with an $n \times n$ identity matrix, $[\theta\ I]^T$.

### 3.4.1 Finite, undirected, simple graphs

A finite, undirected, simple graph $G$ is defined as a pair of mathematical objects $G = (V, E)$. The first is a finite set of *vertices* $V$ which can be labeled by numbers $\{1, 2, \ldots, n\}$ and represented by points on a piece of paper. The second object is a set of *vertex pairs* of vertices in $V$ called *edges* . It is denoted by $E \subset [V]^2$ and can be represented by lines which connect the point representations of $V$ on the piece of paper. A graph is simple if there are no edges connecting vertices to themselves, resulting in loops. Hence $E$ is a proper subset of $[V]^2$, not all elements of $[V]^2$ are included in $E$.

A different way to represent such graphs is by an $n \times n$ *adjacency matrix* $\theta$. Its elements $\theta_{ij} \in \{0, 1\}$ reflect whether an edge between vertices $i$ and $j$ exists or not, by taking on value 1 or 0 respectively.

The number of these types of graphs on an $n$ vertex set can be derived as follows. The number of different possible edges is equal to the number of different pairs of vertices, which is $\binom{n}{2} = \frac{n(n-1)}{2}$. Since an edge either exists or not, there are a total of $2^{\binom{n}{2}}$ different graphs. Note that the number of possible graphs therefore increases exponentially with the number of vertices.




a.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

b.

$$\begin{bmatrix} \sigma_x & \sigma_z & \sigma_z & \sigma_z & \sigma_z \\ \sigma_z & \sigma_x & I & I & I \\ \sigma_z & I & \sigma_x & I & I \\ \sigma_z & I & I & \sigma_x & I \\ \sigma_z & I & I & I & \sigma_x \end{bmatrix}$$

c.

Figure 3.1: **a.** A five vertex 'star graph'. **b.** The adjacency matrix $\theta$ of the five vertex star graph. **c.** The generator of the star graph-state, written in the form of a matrix. Each row corresponds to a generating matrix in which the adjacent Pauli matrices are related by a tensor product $\otimes$.

### 3.4.2 Graph state stabilizers

The adjacency matrix $\theta$ of an $n$-vertex graph $S$ can be used to define the generator of a stabilizer $S$. The elements $M_1, M_2, \ldots M_n$ of the generator of $S$ are defined as

$$M_i = \sigma_x^{(i)} \bigotimes_{k=1}^{n} (\sigma_z^{\theta_{ij}})^{(j)}, \tag{3.18}$$

where the superscripts $^{(i)}$ and $^{(j)}$ indicate that the operator $\sigma_x$ or $\sigma_z$ acts on the $i$'th and $j$'th qubit respectively, and the symbol $\bigotimes$ indicates that there is tensor product $\otimes$ between all terms $\sigma^{(i)}$. If $\theta_{ij} = 0$ then the operator $\sigma_z^{\theta_{ij}} = I$. This is a generator of $n$ independent elements and therefore gives rise to a stabilizer of cardinality $|S| = 2^n$. As proved in theorem 3.1, this stabilizer represents single state, which in this case would be referred to as a *graph state.* Since the generator of the stabilizer, which completely defines the stabilizer group, which in turn completely defines a graph state, is now represented by a $2n \times n$ matrix containing only zeros and ones, any graph state can be specified by only $2n^2$ bits of information.

### 3.4.3 Binary description of stabilizer states

The efficient description of $n$-qubit pure states is not restricted to graph states only, but is also allowed by all stabilizer states. The graph representation does not apply anymore, but stabilizer states can still be represented by $2n \times n$ binary matrices. Similar to the representation of a graph state-stabilizer, the generator of a general stabilizer state is a concatenation of an $n \times n$ "$\sigma_z$-matrix" and an $n \times n$ "$\sigma_x$-matrix". It is perhaps best explained with a simple example.

**Example 3.1.** *Consider the stabilizer of the $|GHZ\rangle$-state, which can be represented in the form of a generator matrix*

$$\begin{bmatrix} \sigma_x & \sigma_x & \sigma_x \\ \sigma_z & \sigma_z & I \\ I & \sigma_z & \sigma_z \end{bmatrix}, \tag{3.19}$$

*where the three rows represent the three generators $M_1 = \sigma_x \otimes \sigma_x \otimes \sigma_x$, $M_2 = \sigma_z \otimes \sigma_z \otimes I$ and $M_3 = I \otimes \sigma_z \otimes \sigma_z$. This matrix can now be represented by the binary matrix*

$$\left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right], \tag{3.20}$$

*where the left $n \times n$ matrix represents $\sigma_z$'s by 1's, and the right $n \times n$ matrix represents $\sigma_x$'s by 1's.*

### 3.4.4 Local Clifford equivalence

The single qubit Clifford group, $\mathcal{C}_1$ is the name given to the *normalizer* of the Pauli group $N(\mathcal{G}_1)$. This means that all elements of the clifford group $\tau \in \mathcal{C}_1$ are $2 \times 2$

matrices which have the property $\tau\sigma_i\tau^\dagger = \sigma_j$ for $i,j \in \{x,y,z\}$. This group is considerably larger than the Pauli group, but can be generated by only two matrices

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{3.21}$$

and consists of 192 different elements. The local Clifford group LC is defined similarly to the group $\mathcal{G}_n$, as $\mathrm{LC} = C_1^{\otimes n}$. To avoid confusion, it should be noted that there does not seem to be a direct connection between the Clifford group and Clifford algebras. The group was given this name because this connection was speculated to exist, however it has thus far not been found [17].

It has been shown that all stabilizer states as defined above are LU-equivalent to a graph state [40]. The LU-mapping between stabilizer state and graph state is not unique however. This makes the study of LC-equivalence of graph states more interesting then studying equivalence classes of general stabilizer states because the set of graph states lies higher in the LC-equivalence hierarchy. An important open problem is to determine whether LU-equivalence of two graph states implies that they are LC-equivalent. An *efficient* (i.e., polynomial running time) algorithm

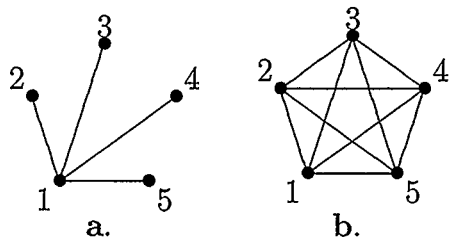



Figure 3.2: **a.** The five-vertex star graph. **b.** The five-vertex star graph after local complementation has been performed about vertex 1. The result is the five-vertex full graph.

has been found which is capable of recognizing whether two graph states are LC equivalent or not [9]. This makes the question of whether LU-equivalence implies LC-equivalence of graph states very interesting, since if this is indeed that case, one could efficiently distinguish locally in-equivalent stabilizer states/codes. It turns out that all LC-equivalent graph states can be found through *local complementation* of their pictorial graph representations, an operation which has an operator equivalent in the local Clifford group [40, 19].

Local complementation is most easily explained by a simple example. It is an operation involving a single vertex on a graph, for example vertex 1. on the five vertex star graph in figure 3.4.2. The operation has the effect that it inverts the edges of the qubits in the *neighborhood* of vertex 1. The neighborhood of some vertex $i$ is defined as all vertices $j$ which appear in a pair with $i$ in the edge set. Pictorially, these are the vertices $j$ which are connected to vertex $i$ by a line. In the case of the five vertex star graph, local complementation about vertex 1 yields the graph depicted in figure 3.2 **b.**

## 3.5 Utilizing stabilizer states

### 3.5.1 Error correction

Quantum error correction codes were designed to prevent information stored in quantum states from being lost due to unwanted interactions with the environment. For a complete account or introduction the reader is referred to [16, 40]. As was explained

in Chapter 2, a general operation $\mathcal{E}$ on a quantum state $\rho$ can be represented by

$$\rho \mapsto \mathcal{E}(\rho) = \sum_a E_a \rho E_a^\dagger, \tag{3.22}$$

where the set $E_a$ are Kraus operators. It is these operations that error correction codes are designed to protect against. A code that encodes $k$ logical qubits in $n$ physical qubits is a set of $k$ pure states $|\psi_i\rangle$ that are a superposition of $2^k$ different basis vectors. The general form of a codeword is thus $|\psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=1}^{2^k} \alpha_i |x_{1i} x_{2i} \dots x_{ni}\rangle$, where $x_{ji} \in \{0, 1\}$. If two errors $E_a$ and $E_b$ can be corrected, then any combination $\alpha E_a + \beta E_b$ can be corrected as well. So only a complete basis of errors needs to be taken into account. The basis of choice is that which is composed of tensor products of Pauli's, which is the group $\mathcal{G}_n$. In order to preserve a code, it must be possible to distinguish between two errors $E_a$ and $E_b$. This means that an error $E_a$ on codeword $|\psi_i\rangle$ must not be confused with an error $E_b$ on codeword $|\psi_j\rangle$. Therefore

$$\langle\psi_i| E_a^\dagger E_b |\psi_j\rangle = 0, \tag{3.23}$$

for $i \neq j$ if the code can distinguish these two errors. Another requirement is that the quantity $\langle\psi_i| E_a E_b^\dagger |\psi_i\rangle$ must be the same for all the codewords when measuring the errors. This is because no information about the codewords should be gained in order for their delicate superposition of states not to get ruined. The two given conditions can be represented simultaneously by the equation

$$\langle\psi_i| E_a^\dagger E_b |\psi_j\rangle = c_{ab} \delta_{ab}, \tag{3.24}$$

where $c_{ab} \in \mathbb{C}$.

The stabilizer construction involves the type of stabilizer introduced in this chapter. An $n$-qubit stabilizer $S$ of cardinality $2^{n-k}$ stabilizes exactly $2^k$ orthogonal states

$|\psi_i\rangle$ which constitute the coding space $T$. These are the codewords of the stabilizer code. This code is robust against any error operator $E = E_a^\dagger E_b$ that anti-commutes with a stabilizer element $M$. This is because for any state $|\psi_i\rangle \in T$,

$$\langle\psi_i| E |\psi_i\rangle = \langle\psi_i| EM |\psi_i\rangle = -\langle\psi_i| EM |\psi_i\rangle = -\langle\psi_i| E |\psi_i\rangle , \qquad (3.25)$$

which can only be true if $\langle\psi_i| E |\psi_i\rangle = 0$ as required by equation (3.24). Of course, if the error $E$ is in the stabilizer $S$, the code will not be affected by it. In general, a stabilizer code is protected against errors that are in the stabilizer, or anti-commute with an element of the stabilizer.

### 3.5.2 Cluster States and Measurement Based Computation

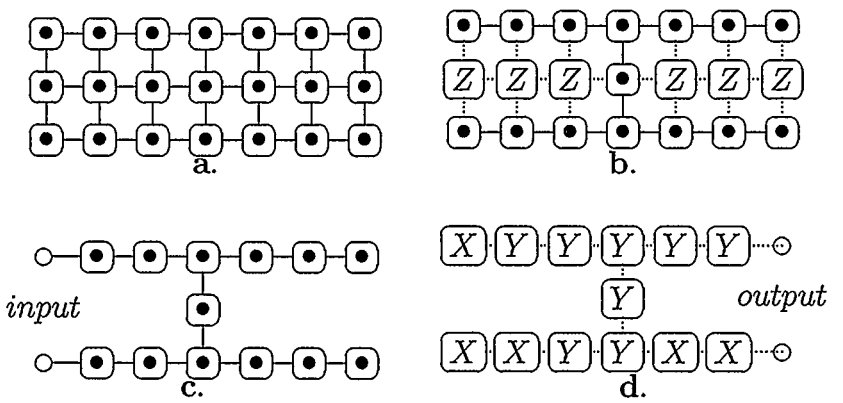



Figure 3.3: This is an example of a cluster-state version of the CNOT gate given in [34]. **a.** A cluster of twenty-one qubits, in a graph-state entangled state. **b.** Unwanted entangled qubits are removed from the cluster by measurements in the $\sigma_z$-basis. **c.** The input state $|\psi\rangle$ is encoded in the left most qubits. **d.** A series of measurements is done resulting in an output state on the right most qubits.

The cluster-state model of quantum computation has made David Deutsch (next to Richard Feynman arguably the father of quantum computation) conclude that

universal quantum computers are only years away from being realized [11]. This model is an invention by Robert Raussendorf and Hans Briegel and for a complete account of it the reader is referred to the articles [32, 34]. The main resource of this model is a highly entangled state shared among a large number of qubits. The state takes on the form of a graph state which can be pictorially by a 1D (chain), 2D or 3D cluster (see figure 3.3). The state is prepared by initializing all qubits in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$-state and then performing an entangling operation between adjacent qubits. The entangling operation can be represented by the two-qubit operator

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{3.26}$$

Parts of the cluster that will not be used in the process are removed by measuring qubits in the basis of the $\sigma_z$-matrix. This corresponds to a von Neumann measurement presented in example 2.2. This is represented in figure 3.3 by the symbol $\boxed{Z}$. The input state is encoded on the left most qubits. Next, a series of measurements in different bases is performed sequentially, disentangling all qubits in the cluster. The result is an output state on the right most qubits which are not measured. After the procedure is completed the cluster has been completely destroyed and has to be rebuilt for the next computation. This is the reason why this model is also known as *one-way measurement based computation*. The example presented in figure 3.3 is a special one because all the measurements are done in a basis of operators belonging to the Clifford group, introduced in section 3.4.4. What is so special about

these measurements is that they can all be performed simultaneously. If the procedure involves more general measurement bases, then the exact steps depend on the outcomes of the measurements. In this case the computation is performed stepwise.

The most important properties of stabilizers as subgroups of $\mathcal{G}_n$ have been studied and discussed. The next chapter is a discussion of a possible generalization of the stabilizer formalism. New stabilizing objects will be defined and will be given the names *general stabilizer* and *observable stabilizer*. The stabilizers presented in this chapter will be referred to as either conventional stabilizers, or simply stabilizers.

# Chapter 4

# General Stabilizers

## 4.1 Introduction

It is the stabilizer representation that make stabilizer states easy to work with and describe. They form a class of states which allow for elegant and intuitive description in terms of simple graphs; all stabilizer states were shown to be LU-equivalent to graph-states [40]. Moreover, stabilizer states are efficiently defined by a number of parameters that is only linear in the number of qubits using the binary description. This chapter is a presentation of the work that was done to attempt to generalize the stabilizer formalism. A more general definition of a stabilizer is formulated and then explored to see in what forms it can be used to represent different $n$-qubit pure states. In particular, the result of this generalization to two- and three-qubit pure states is discussed. In section 4.2 a more general definition of a stabilizer is presented and the most important implications of this generalization are derived. Section 4.3 contains an example of a stabilizer whose definition deviates slightly from the conventional one. It is studied for two- and three-qubit pure states. The generalization is expanded in section 4.4. Here the difference from conventional stabilizers becomes significant and is demonstrated by two examples. A recipe to construct a stabilizer as defined in this chapter for any $n$-qubit pure state is presented in section 4.5. Section 4.6 is a short discussion on finding a stabilizer for the $|W\rangle$-state. This work originated from the idea that since this and the $|GHZ\rangle$-state are

SLOCC-inequivalent, they might have general stabilizer representations which differ in form such that the inequivalence becomes apparent from it more obviously then from the arguments presented in chapter 2.

## 4.2 General stabilizer groups

To generalize the stabilizer formalism, a more general definition of a stabilizer needs to be formulated. As a start, the condition of a stabilizer to be a subgroup of $\mathcal{G}_n$ is dropped to yield the following formal definition.

**Definition 4.1.** *A general stabilizer $S$ is a finite Abelian group of operators which share at least one common eigenvector with eigenvalue +1.*

It should again be noted that (like in chapter 3), no distinction is made between a (state-) vector and a ray. Any vector which is an eigenvector with eigenvalue $+1$ for all elements of a stabilizer $S$ is said to be stabilized by the elements of $S$. The operator $-I$ can of course not be an element of a general stabilizer since $-I\,|\psi\rangle = -\,|\psi\rangle$. Relaxing the definition of a stabilizer by dropping the requirement of it having to be a subgroup of $\mathcal{G}_n$ has as a consequence that its elements are not necessarily Hermitian anymore. What can be said however is the following.

**Proposition 4.1.** *Let $S$ be a general stabilizer which stabilizes a set of vectors $T \stackrel{def}{=} \{|\psi\rangle : M\,|\psi\rangle = |\psi\rangle\,, \forall M \in S\}$. Then there exists a stabilizer $S'$ whose elements $\{M'\}$ are Hermitian and unitary and stabilize only the vectors in $T$.*

*Proof.* Consider the spectral decomposition of an element $M \in S$,

$$M = \sum_{i=1}^{m} \lambda_i |\psi_i\rangle\langle\psi_i|. \tag{4.1}$$

Since all vectors $|\psi_i\rangle \in T$ are stabilized by $M$, they have eigenvectors $\lambda_i = +1$. All $M \in S$ must be of finite order because $S$ is a finite group. This implies that there is some (finite) integer $g$ such that $M^g = E$, where $E$ acts as the identity on all elements $M \in S$. Here a distinction between $E$ and $I$ is made because the eigenvalues of an element $M \in S$ can be zero, in which case $M^g$ is a diagonal matrix with entries 0 and 1. But this implies that all eigenvalues are of the form $\lambda_i \in \{0, e^{2\pi i k_i/g}\}$, where $0 \leq k_i \in \mathbb{N} < g$. This way, if for all $i$ $\lambda_i > 0$, then $M^g = \sum_i \lambda_i^g |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^m |\psi_i\rangle\langle\psi_i| = I$. So the order of the operator $M$ depends on the eigenvalues of the eigenvectors which are not in $T$. The only difference between the elements $M \in S$ are the eigenvalues $\lambda_i$ of the corresponding eigenvectors $|\psi_i\rangle \notin T$.

An operator $M'$ can be defined to have eigenvalues $\lambda_i = +1$ for all $|\psi_i\rangle \in T$ and $\lambda_i = \pm 1$ for all $|\psi_i\rangle \notin T$. This operator stabilizes all vectors $|\psi_i\rangle \in T$ and will have order at most 2. If it has order 2, then $M'^2 = I$, which implies that it is Hermitian and unitary. Any set of operators $M'$ in which all eigenvectors $|\psi_i\rangle \notin T$ have eigenvalue -1 for at least one $M'$ forms a stabilizer $S'$, as asserted to exist in the proposition. □

Operators which are Hermitian are used to mathematically represent *quantum observables*, properties of physical systems which can be experimentally measured or detected. This is a fact that will shortly be used to define a general stabilizer with more desirable properties. A direct result of the proposition is that with $l$ generating operators of order 2, a stabilizer $S$ has a cardinality $|S| = 2^l$ (recall the definition of a generator in section 3.2). This is essentially what is asserted in lemma 3.1. The assumption was that $S \in \mathcal{G}_n$, but the only property that was used of this was

that operators of this type of stabilizer are Hermitian and unitary. The lemma can therefore be generalized for general stabilizers, without having to adjust the proof.

**Lemma 4.1.** *Let $S$ be a general stabilizer whose generating elements are Hermitian, unitary operators $M_1, M_2, \ldots, M_l$. Then its cardinality $|S| = 2^l$ for some $l \in \mathbb{N}$.*

*Proof.* See proof to lemma 3.1. □

The effect of the generating operators having higher orders is that the cardinality of stabilizer increases. Having in mind that the interest lies in the states which are stabilized, the stabilizer might as well be chosen to be as compact as possible because all the information about it is already contained in the generator.

The goal is now to devise a general stabilizer formalism under which general stabilizers can be defined which uniquely represent a single $n$-qubit pure state. It turns out that for general stabilizers, proposition 3.2, lemma 3.2 and theorem 3.1 are readily generalized, but can be proved in exactly the same way. This is because the properties of $\mathcal{G}_n$ that are required by the proofs, are that its elements are Hermitian, unitary and (with the exception of $I$) traceless. So the following three, already proved statements can be made.

**Proposition 4.2.** *Let $S$ be a general stabilizer of cardinality $|S| = 2^l$ with $0 \leq l \leq n$, whose elements are traceless, Hermitian, unitary operators $M_1, M_2, \ldots, M_l \in \mathbb{C}^{2^n \times 2^n}$. Then the normalized sum*

$$\rho = \frac{1}{2^n} \sum_{M \in S} M, \tag{4.2}$$

*satisfies the properties of an orthogonal projector up to a normalization factor.*

*Proof.* See proof of proposition 3.2. □

**Lemma 4.2.** *Let $S$ be a general stabilizer of cardinality $|S| = 2^n$ for some $n \in \mathbb{N}$, whose elements but the identity are traceless, Hermitian, unitary operators $M \in \mathbb{C}^{2^n \times 2^n}$. Then the projector $\rho = \frac{1}{2^n} \sum_{M \in S} M$ has a unique non-zero eigenvalue $+1$, which occurs with multiplicity one.*

*Proof.* See proof to lemma 3.2. □

**Theorem 4.1.** *Let $S$ be a general stabilizer of cardinality $|S| = 2^n$ for some $n \in \mathbb{N}$, whose elements but the identity are traceless, Hermitian, unitary operators $M_1, M_2, \ldots, M_{2^n} \in \mathbb{C}^{2^n \times 2^n}$. Then $S$ stabilizes a unique vector $|\psi\rangle$.*

*Proof.* See proof to theorem 3.1. □

In section 4.5 it will be shown that general stabilizers with the appropriate properties and a generator of size $n$ indeed exist for all possible $n$-qubit states. Now that the desired properties of a general stabilizer have been narrowed down, a definition can be formed of a more desirable subset of the general stabilizers.

**Definition 4.2.** *An observable stabilizer $S$ is an Abelian group, whose elements but the identity $\{M_i\}$ are traceless, Hermitian, unitary operators which have at least one common eigenvector with eigenvalue $+1$.*

## 4.3 A first generalization

Consider an element $M = m_1 \otimes m_2 \otimes \cdots \otimes m_n$ of an observable stabilizer. This element is Hermitian and unitary, and so its constituents $m_i$ can also be chosen to be Hermitian and unitary. A first generalization of the Pauli stabilizers can thus be general stabilizing groups in $\mathrm{SU}(2)^{\otimes n}$ instead of $\mathcal{G}_n$. For two- and three-qubit pure

states this will turn out to have no significant consequences. What this means for pure states of more qubits is still somewhat of an open question. The following two lemmas reveal the most important implications of this generalization.

**Lemma 4.3.** *A multi-local unitary transformation preserves the commutativity of an Abelian group.*

*Proof.* Let $S$ be an Abelian group composed of matrices $\{M_i\}$, and let $U \in U(d)$ be a unitary operator which transforms $S$ to $S'$, the group of transformed elements $\{UM_iU^\dagger\}$. Then any two elements $M_1' = UM_1U^\dagger$ and $M_2' = UM_2U^\dagger$, where $M_1, M_2 \in S$, satisfy the commutation relations

$$\begin{aligned}
[M_1', M_2'] &= [UM_1U^\dagger, UM_2U^\dagger] \\
&= UM_1U^\dagger UM_2U^\dagger - UM_2U^\dagger UM_1U^\dagger \\
&= U\left(M_1M_2 - M_2M_1\right)U^\dagger \\
&= U[M_1, M_2]U^\dagger = 0.
\end{aligned}$$

Since $M_1'$ and $M_2'$ can represent *any* two elements of $S'$, this transformed group is also Abelian. □

Now consider an observable stabilizer $S$ such that $S \in SU(2)^{\otimes n}$. Since an element $M = m_1 \otimes \cdots \otimes m_n \in S$ is Hermitian and unitary, its constituents can always be chosen to have the same property, *i.e.* $m_i^2 = I$ for all labels $i$. This is what is done to prove the following lemma.

**Lemma 4.4.** *Let $M, N \in SU(2)^{\otimes n}$ be Hermitian, unitary matrices, such that*

$$\begin{aligned} M &= m_1 \otimes m_2 \otimes \cdots \otimes m_n \\ N &= n_1 \otimes n_2 \otimes \cdots \otimes n_n \\ m_i^2 = n_i^2 &= I \\ [M, N] &= 0. \end{aligned}$$

*Then the pairs $\{m_i, n_i\}$ either commute or anti-commute.*

*Proof.* From the commutation relation

$$\begin{aligned} [M, N] &= [m_1 \otimes m_2 \otimes \cdots \otimes m_n, n_1 \otimes n_2 \otimes \cdots \otimes n_n] \\ &= m_1 n_1 \otimes \cdots \otimes m_n n_n - n_1 m_1 \otimes \cdots \otimes n_n m_n \\ &= 0, \end{aligned}$$

and $m_i^2 = n_i^2 = I$ it follows that

$$m_i n_i = e^{i\phi_i} n_i m_i, \tag{4.3}$$

such that $\sum_{i=1}^{n} \phi_i = 2^k \pi$, $k \in \mathbb{N}$. But since $n_i^\dagger = n_i$ which follows from $n_i^2 = I$,

$$\begin{aligned} (m_i n_i m_i^\dagger)^\dagger &= e^{-i\phi_i} n_i \\ &= m_i n_i m_i^\dagger \\ &= e^{i\phi_i} n_i, \end{aligned}$$

which implies that $\phi_i = m\pi$, $m \in \mathbb{N}$. It subsequently follows that if $\phi_i = 0 \mod 2\pi$, $m_i$ and $n_i$ commute, but anti-commute if $\phi_i = \pi \mod 2\pi$. □

In the following theorem, the concept of the support of a stabilizer is introduced. This is a generalization of the support of a stabilizer element (see section 3.3.2) and it is defined as follows.

**Definition 4.3.** *The support of a stabilizer $S$ is the union of supports of all its elements $M \in S$,*

$$supp(S) \stackrel{def}{=} \bigcup_{M \in S} supp(M). \tag{4.4}$$

The support of a stabilizer $S$ is thus the set of labels $j$ such that the $j$'th constituent $m_j$ of at least one stabilizer element $M = m_1 \otimes \cdots \otimes m_n \in S$ is not equal to $I$.

Consider now an observable stabilizer $S$ whose elements $M = m_1 \otimes \cdots \otimes m_n$ are such that their constituents $m_i$ are Hermitian and unitary. Let $U$ be an LU operator which maps at least one element $m_j \neq I$ to an element $\sigma_i$ with $i \in \{x, y, z\}$, for each $j \in \text{supp}(S)$. The other transformed elements are labeled $m'_j$. From lemma 4.4 it follows that all constituents $m'_j$ must either commute, or anti-commute with $\sigma_i$. The only matrices which can anti-commute with the Pauli matrices and have order 2, are the Pauli matrices themselves, or sums of the form $\frac{1}{\sqrt{2}}(\sigma_i \pm \sigma_j) : j \neq i$. Because all observable stabilizers in $\text{SU}(2)^{\otimes n}$ are LU-equivalent to observable stabilizers whose elements are composed of Pauli matrices and matrices of the form $\frac{1}{\sqrt{2}}(\sigma_i \pm \sigma_j)$, a name will be given to this set.

$$\mathcal{G}_1^+ \stackrel{def}{=} \left\{ \mathcal{G}_1, \tfrac{1}{\sqrt{2}}(\sigma_x \pm \sigma_y), \tfrac{1}{\sqrt{2}}(\sigma_x \pm \sigma_z), \tfrac{1}{\sqrt{2}}(\sigma_y \pm \sigma_z) \right\}. \tag{4.5}$$

So the operator $U$ transforms all constituents $m_j$, $j \in \text{supp}(S)$ to elements of the set $\mathcal{G}_1^+$, and therefore the stabilizer $S$ to $S' \in \mathcal{G}_n^+$, where $\mathcal{G}_n^+ \stackrel{def}{=} \mathcal{G}_1^{+\otimes n}$. For convenience, states with observable stabilizers in $\text{SU}(2)^{\otimes n}$ will be referred to as $\mathcal{G}_n^+$-stabilizer states.

Recalling what was derived in section 3.3.2, the following statements can be made about states with stabilizers in $\mathcal{G}_n^+$. Since all elements of $\mathcal{G}_1^+$ are traceless, all elements of $\mathcal{G}_n^+$ are traceless, with the exception of the identity of course. This means that these kinds of states are already in the normal form defined in section 3.3.1, and that the only multi-local operation under which equivalence classes can be defined are LU-operations (SLOCC≡LU). What can also be concluded from this is that any qubit '$a$' which is entangled with part of the system, can only be maximally entangled (see section 2.6.2). This is because its reduced density matrix $\rho_a$ would be equal to $\frac{1}{2}I$ and therefore its entropy of entanglement would be 1.

### 4.3.1 $\mathcal{G}_2^+$-stabilizer states

For two-qubit pure states there are only two SLOCC-inequivalent classes; separable states and entangled states, as was shown in section 2.7.2. Because $\mathcal{G}_2^+$-stabilizer states are already in their normal form, their Schmidt decompositions will always look like $\frac{1}{\sqrt{2}}(|a_1b_1\rangle + |a_2b_2\rangle)$ if they are entangled. This follows from the fact that their reduced density matrices $\rho_{a/b}$ always take on the form $\frac{1}{2}I$. This means that they are LU-equivalent to the Bell states, which are stabilizer states. So the $\mathcal{G}_2^+$-stabilizer description provides no class of states which is not already defined by conventional stabilizer states. Nor does it provide any new class of states because the Bell states are LU-equivalent to all possible maximally entangled two-qubit pure states.

### 4.3.2 $\mathcal{G}_3^+$-stabilizer states

For three qubit pure states the question of which class the $\mathcal{G}_3^+$-stabilizer states belongs to becomes a little more interesting because there are two SLOCC-inequivalent

classes of fully entangled pure states, represented by $|GHZ\rangle$ and $|W\rangle$. If one of the qubits is not entangled, the problem simply reduces to the LU-equivalence of a $\mathcal{G}_2^+$-state and a Bell state, which was presented above. This leads to the following claim.

**Claim 4.1.** *Fully entangled $\mathcal{G}_3^+$-stabilizer states are LU-equivalent to $|GHZ\rangle$.*

*Proof.* Since $\mathcal{G}_3^+$-stabilizer states are in their normal form, they are LU-equivalent to any state which they are SLOCC-equivalent to. This means that they are LU-equivalent to either $|GHZ\rangle$ or $|W\rangle$, which represent the two SLOCC-inequivalent three-qubit pure state classes. $|W\rangle$ was shown to have a normal form equal to zero in [41]. This means that the constant of proportionality $c$ between the reduced density matrices of $|W\rangle$ in its normal form, and $I$ is zero. The normal form of a fully entangled $\mathcal{G}_3^+$-stabilizer state is therefore not LU-equivalent to that of $|W\rangle$, and so these states are not SLOCC equivalent to $|W\rangle$. From this it can be deduced that the normal forms of $\mathcal{G}_3^+$-stabilizer states are LU-equivalent to that of $|GHZ\rangle$ because if this were not so, they would constitute a new class of fully entangled 3-qubit pure states under SLOCC. Since these states are already in their normal form, and $|GHZ\rangle$ is too because it is a stabilizer state, they are LU-equivalent. □

As mentioned before, for two- and three-qubit pure states this generalization of the stabilizer description does not cause the number of represented states to increase. In order for this generalization of the stabilizer definition to make a difference for two-and three qubits, they have to assume a different form than just described.

## 4.4 Further generalizations

The form of observable stabilizers suggested above turned out to be useful for the representation of maximally entangled pure states. The next step is to find an observable stabilizer representation for pure states which are not maximally entangled. The requirements of an observable stabilizer leads to the use of larger constituents in the stabilizer elements. For not-fully entangled two-qubit pure states for example, an observable stabilizer of the form $S \in \mathbb{C}^{4\times 4}$ would be required such that the generating matrices have non-zero partial traces.

**Example 4.1.** *Consider a two-qubit pure state $|\psi\rangle$ which is entangled, but not maximally entangled and has a Schmidt decomposition*

$$|\psi\rangle = \lambda_1 |00\rangle + \lambda_2 |11\rangle , \tag{4.6}$$

*such that $0 < |\lambda_1| < |\lambda_2| < 1$ so that its entropy of entanglement $0 < E(|\psi\rangle) < 1$. The observable stabilizer $S_\psi$ of this state requires two generators $M_1$ and $M_2$ and consists of the elements $\{I, M_1, M_2, M_1M_2\}$. These generating matrices can not be of the form $SU(2) \otimes SU(2)$ because then the state would be LU-equivalent to a maximally entangled state, which it is not. The reduced density matrix of qubit 'a' is $\rho_a = |\lambda_1|^2|0\rangle\langle 0| + |\lambda_2|^2|1\rangle\langle 1| = \left(\begin{smallmatrix} |\lambda_1|^2 & 0 \\ 0 & |\lambda_2|^2 \end{smallmatrix}\right)$. Now since*

$$\rho^\psi = \frac{1}{4}(I + M_1 + M_2 + M_1M_2), \tag{4.7}$$

*the reduced density matrix can be written as*

$$\rho_a = Tr_b(\rho) = \frac{1}{4}(Tr_b(I) + Tr_b(M_1) + Tr_b(M_2) + Tr_b(M_1M_2)). \tag{4.8}$$

*The partial trace of the* $4 \times 4$ *identity matrix is simply the* $2 \times 2$ *identity matrix. So* $\rho_a = \frac{1}{2}I + \frac{1}{4}(Tr_b(M_1) + Tr_b(M_2) + Tr_b(M_1M_2))$. *Therefore*

$$\frac{1}{4}(Tr_b(M_1) + Tr_b(M_2) + Tr_b(M_1M_2)) = \begin{pmatrix} |\lambda_1|^2 - \frac{1}{2} & 0 \\ 0 & |\lambda_2|^2 - \frac{1}{2} \end{pmatrix}. \tag{4.9}$$

From this example it becomes clear that an observable stabilizer for a not-fully entangled two-qubit pure state must have elements of which at least one has non-zero partial trace.

**Example 4.2.** *Consider now a three-qubit pure state* $|\psi\rangle$ *in which a qubit 'a' is maximally entangled with two more weakly entangled qubits 'b' and 'c'. This type of state can easily be created by methods applied in the cluster-state model. As the state is created, the transformation of the generator of the observable stabilizer is analyzed.*

1. *Start with a separable stabilizer state* $|\psi\rangle = |+\rangle|+\rangle|+\rangle$. *The generator of its stabilizer is*

$$\begin{bmatrix} \sigma_x & I & I \\ I & \sigma_x & I \\ I & I & \sigma_x \end{bmatrix}. \tag{4.10}$$

2. *Apply the CZ operation on qubits 'a' and 'b' which will fully entangle them and do nothing to qubit 'c'. This transforms the generator of the stabilizer to*

$$\begin{bmatrix} \sigma_x & \sigma_z & I \\ \sigma_z & \sigma_x & I \\ I & I & \sigma_x \end{bmatrix}. \tag{4.11}$$

*Here each element* $M$ *of the generator is transformed as* $(CZ \otimes I)M(CZ \otimes I)^\dagger$.

3. *Next, apply an 'imperfect CZ-gate' of the form*

$$\widetilde{CZ_\phi} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}. \tag{4.12}$$

*to qubits 'b' and 'c'. This has the effect that it entangles a separable two-qubit state* $|+\rangle|+\rangle$ *such that the entropy of entanglement is increases from zero to one as* $\phi$ *ranges from zero to* $\pi$*. This transforms the generator to*

$$\begin{bmatrix} \sigma_x & \sigma_z & I \\ \sigma_z & A & \\ I & B & \end{bmatrix}, \tag{4.13}$$

*where* $A$ *and* $B$ *are now two-qubit operators,*

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{-i\phi} \\ 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{-i\phi} \\ 0 & 0 & e^{i\phi} & 0 \end{pmatrix}, \tag{4.14}$$

*which operate on qubits 'b' and 'c'. The transformation* $(I \otimes \widetilde{CZ_\phi}) M (I \otimes \widetilde{CZ_\phi})^\dagger$ *had no effect on the first generator* $\sigma_x \otimes \sigma_z \otimes I$*. It is easily checked that these generating elements indeed still commute and are traceless, Hermitian and unitary, and they therefore still generate a proper observable stabilizer of the transformed state.*

*The effect of this operation on the original state is that now, the entropy of entanglement for qubit 'a' is unity, whereas it depends on* $\phi$ *for qubits 'b' and 'c'.*

Note that the observable stabilizer for $|W\rangle$ must be of this general form, that is composed of multi-qubit constituents. It can not be of the form presented in example 4.2 because this would require that one of the qubits is maximally entangled. $|W\rangle$ does not have this property because all its reduced density matrices have the form $\rho^W_{a/b/c} = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$, and so the entropy of entanglement is $E(\rho^W_a) = E(\rho^W_b) = E(\rho^W_c) \approx 0.9183$.

## 4.5 Construction of an observable stabilizer

The foregone discussion described the desired properties of observable stabilizers in order to allow for a generalized stabilizer representation of all possible $n$-qubit pure states along with two basic examples. This section is devoted to showing a method to construct an observable stabilizer for a known $n$-qubit state $|\psi\rangle$. To make the discussion easier, $n$-qubit pure states are now represented by their $2^n$-dimensional vectors, which will be given the name $v_1$. To start, the elements of an observable stabilizer will be constructed in terms of their spectral decompositions, which is demonstrated in the following lemma.

**Lemma 4.5.** *For any vector $v_1 \in \mathbb{C}_2^{\otimes n}$ there exist an infinite number of operators for which this vector is an eigenvector with eigenvalue $+1$.*

*Proof.* Let $v_1 \in \mathbb{C}_2^{\otimes n}$ be some normalized vector and the set $v_2, \ldots, v_{2^n}$ be normalized vectors which are orthogonal to each other and $v_1$. This implies that the set $\{v_1, v_2, \ldots, v_{2^n}\}$ forms an orthonormal basis for a $2^n$-dimensional linear vector space $V$. Consider now the set of orthogonal projectors $\{p_i = v_i v_i^\dagger\}$ which are formed from

the basis for $V$. Then any linear superposition

$$M = p_1 + \sum_{i=2}^{2^n} \alpha_i p_i, \tag{4.15}$$

has the property that it has the vector $v_1$ as an eigenvector with eigenvalue $+1$, since $p_i v_1 = \delta_{i1} v_1$. □

This somewhat trivial observation can now be used to show how to narrow down the number of stabilizing matrices in order to form an observable stabilizer for some $n$-qubit pure state. The next step is to restrict the value of the coefficients $\alpha_i$ to 1 or $-1$. The result of this is that a linear superposition $M$ of orthogonal projectors will always be Hermitian. This can easily be seen by taking its complex transpose

$$\begin{aligned} M^\dagger &= p_1^\dagger + \sum_{i=2}^{2^n} ((-1)^{x_i})^* p_i^\dagger \\ &= M, \end{aligned}$$

since $p_i^\dagger = (v_i v_i^\dagger)^\dagger = p_i$ and $x_i \in \{0, 1\}$. It is also not difficult to show that an operator of this form is in fact unitary. This can be done by taking its square

$$\begin{aligned} M^2 &= \left( p_1 + \sum_{i=2}^{2^n} (-1)^{x_i} p_i \right) \left( p_1 + \sum_{i=2}^{2^n} (-1)^{x_i} p_i \right) \\ &= \sum_{i=1}^{2^n} p_i = I. \end{aligned}$$

Here we the fact was used that $p_i p_j = \delta_{ij} p_j$ and that the $v_i$ form a complete orthonormal basis. Note that such a reduction limits the operators to the realm of *quantum observables*. Given a basis $\{v_1, \ldots, v_{2^n}\}$, this construction still allows for $2^{2^n - 1}$ different operators $M$ such that $M v_1 = v_1$.

The way observable stabilizers can be constructed is by letting the coefficients $\alpha_i$ in the sums $\sum_{i=1}^{2^n} \alpha_i p_i$ be the elements of the rows of a Walsh-Hadamard transform

matrix ($WHT$). The stabilizer elements are essentially constructed by applying the Walsh-Hadamard transform to the basis $\{p_i\}$,

$$[M_1, M_2, \ldots, M_{2^n}]^T = WHT[p_1, p_2, \ldots, p_{2^n}]^T. \tag{4.16}$$

The first step is to show that this yields proper observable stabilizers in the sense that they have a cardinality of $2^n$ and can be fully defined by a subset of $n$ generating elements. To this end consider a binary representation of the orthogonal row vectors $h_0 = (1, 1)$ and $h_1 = (1, -1)$ of a $2 \times 2$ $WHT$

$$WHT = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{bmatrix} h_0 \\ h_1 \end{bmatrix}. \tag{4.17}$$

When multiplying two general stabilizer elements $M_1$ and $M_2$, the coefficients $\alpha_{12i}$ of $M_1 M_2 = \sum_{i=1}^{2^n} \alpha_{1i}\alpha_{2i}p_i$ can be found by simply multiplying those of $M_1$ and $M_2$. Since these coefficients are the elements of the rows of the $2 \times 2$ $WHT$, define the products

$$\begin{aligned} h_0^2 &= (1^2, 1^2) = h_0 \\ h_1^2 &= (1^2, -1^2) = h_0 \\ h_0 h_1 &= h_1 h_0 = h_1. \end{aligned} \tag{4.18}$$

Looking at how the subscripts change under these operations, it can be seen that they can be represented with a binary construction. Since $h_{x_1} h_{x_2} = h_{x_1 \oplus x_2}$, were $x_i \in \{0, 1\}$ and the symbol $\oplus$ denotes addition modulo 2, this type of multiplication can be represented by the indices and addition modulo 2 as follows

$$\begin{aligned} h_0 &\mapsto 0 \\ h_1 &\mapsto 1. \end{aligned} \tag{4.19}$$

A $2^n \times 2^n$ *WHT* is represented by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)^{\otimes n}$ and its row vectors then are simply tensor products of $h_0$ and $h_1$. Using this, any $2^n$ dimensional *WHT* can be represented by a binary array.

**Example 4.3.** *Consider the* $8 \times 8$ *WHT*

$$WHT(2^n) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes 3} = \begin{bmatrix} h_0 \otimes h_0 \otimes h_0 \\ h_0 \otimes h_0 \otimes h_1 \\ h_0 \otimes h_1 \otimes h_0 \\ h_1 \otimes h_1 \otimes h_1 \\ h_1 \otimes h_0 \otimes h_0 \\ h_1 \otimes h_0 \otimes h_1 \\ h_1 \otimes h_1 \otimes h_0 \\ h_1 \otimes h_1 \otimes h_1 \end{bmatrix} \mapsto \begin{bmatrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix}. \tag{4.20}$$

*This mapping becomes even more obvious by writing* $h_{x_1} \otimes h_{x_2} \otimes h_{x_3} = h_{x_1 x_2 x_3}$. *The binary vector then appears as a subscript of the row vectors.*

The product of two elements $M_1$ and $M_2$ constructed using a *WHT* can thus be represented by the addition of two binary vectors modulo 2. From this it follows that all rows of a *WHT*, and therefore all elements of an observable stabilizer constructed with it, can be generated by a subset of any $n$ elements excluding the zero-element, which is the identity element in the stabilizer.

**Lemma 4.6.** *The row vectors of an* $2^n \times 2^n$ *WHT can be generated by a subset of* $n$ *non-trivial row vectors.*

*Proof.* Using the mapping $h_{x_1 \cdots x_n} \mapsto \mathbf{x} = x_1 \cdots x_n$ and the $n$-bit binary operation $\oplus$

such that

$$\mathbf{x} \oplus \mathbf{x}' = (x_1 \oplus x_1') \cdots (x_n \oplus x_n'), \tag{4.21}$$

it follows that $n$ linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n$ of such a form, and the operation $\oplus$, span a space of size $2^n$. Since there are only $2^n$ different $n$-dimensional binary vectors it can be concluded all row vectors of $WHT$ can be generated by a subset of size $n$ because this mapping shows that all row vectors $h_{x_1 x_2 \cdots x_n}$ can be generated with products of the form 4.18. □

Lemma 4.6 shows that all the row vectors of a $2^n \times 2^n$ Walsh-Hadamard transform matrix can be generated by a linearly independent subset of size $n$. This leads to the following theorem that proves the aforementioned claim.

**Theorem 4.2.** *For any n-qubit pure state $|\psi\rangle$ there exists an observable stabilizer that only stabilizer $|\psi\rangle$.*

*Proof.* From the results of lemma 4.5 and the form of the $WHT$ it is apparent that a set of operators $S = \{M_1, M_2, \ldots, M_{2^n}\}$ such that

$$M_i = \left[WHT[p_1, p_2, \ldots, p_{2^n}]^T\right]_i, \tag{4.22}$$

where $i$ denotes the $i$'th element in the vector $[M_1, M_2, \ldots, M_{2^n}]^T$, is indeed a group of stabilizing elements for some vector $v_1$. Noting that using this construction, any subset of $n$ elements $M \in S$, excluding the identity element is independent, and evoking theorem 4.1, $S$ can stabilize only a single vector. This is the vector $v_1$ such that $p_1 = v_1 v_1^\dagger$. □

Similar to a vector or orthogonal projector (density matrix), a stabilizer can therefore also be used as a mathematical representation of the state of a physical

object. At least if this state is an $n$-qubit pure state. The correspondence between the state-vector and its stabilizer is however, one-to-many because the choice of the $2^n - 1$ basis vectors $\{v_2, \ldots, v_{2^n}\}$ is arbitrary.

**Example 4.4.** *Consider one of the Bell states*

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{2}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(1,0,0,1)^T. \end{aligned}$$

*In order to form a stabilizer for this state-vector, a complete orthonormal basis is needed. To start, choose the basis*

$$v_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, v_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, v_3 = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, v_4 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}. \tag{4.23}$$

*Following the construction described above, this yields stabilizer elements*

$$M_1 = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, M_2 = \begin{pmatrix}0&0&0&1\\0&1&0&0\\0&0&-1&0\\1&0&0&0\end{pmatrix}$$

$$M_3 = \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}, M_4 = \begin{pmatrix}0&0&0&1\\0&-1&0&0\\0&0&1&0\\1&0&0&0\end{pmatrix}$$

*As mentioned however, this choice of basis is arbitrary. Another possible choice could be*

$$v_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, v_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, v_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}, v_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \tag{4.24}$$

*in which case the stabilizers take on a completely different form.*

$$M_1 = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, M_2 = \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

$$M_3 = \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}, M_4 = \begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&-1&0&0\\1&0&0&0\end{pmatrix}$$

*These matrices all have the form of tensor products of two* $2 \times 2$ *Hermitian unitary matrices, namely the Pauli matrices:*

$$\begin{aligned} M_1 &= I \otimes I \\ M_2 &= \sigma_x \otimes \sigma_x \\ M_3 &= \sigma_z \otimes \sigma_z \\ M_4 &= -\sigma_y \otimes \sigma_y. \end{aligned}$$

*Note that with the first choice of basis, only two of the stabilizer elements (*$M_1$ *and* $M_3$*) take the form of a direct product* $SU(2) \otimes SU(2)$.

It becomes apparent in this example that for general stabilizer states, the form of the conventional stabilizer can be retrieved when using the right choice of basis. Trying to obtain an observable stabilizer with the smallest constituents turns out to be a problem of similar difficulty to finding the minimal product decomposition (see subsection 2.3.2).

## 4.6 The $W$-stabilizers

In section 4.3 it was shown that a fully entangled three-qubit $\mathcal{G}_3^+$-state can not be LU-, nor SLOCC-equivalent to the $|W\rangle$-state. What this also indicates is that an observable stabilizer of $|W\rangle$ can not be in $\mathcal{G}_3^+$. A different way to come to this conclusion is by looking at the reduced density matrices of its individual qubits. These are readily verified to have the form

$$\rho_a^W = \rho_b^W = \rho_c^W = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|. \tag{4.25}$$

This shows that the qubits of the $|W\rangle$-state are not maximally entangled in the sense that the von Neumann entropy of the reduced density matrices is not equal to unity, but about 0.9183. As was explained by the examples in section 4.4, general stabilizer states in which less-than-maximal entanglement is present require multi-qubit constituents whose partial trace is not equal to zero. In particular, example 4.2 shows how an imperfect $CZ$-gate $\widetilde{CZ}_\phi$ can be used to create these types of states from a separable state $|+\rangle|+\rangle$. An actual stabilizer for $|W\rangle$ can of course easily be constructed using the method prescribed in section 4.5. A measurement based procedure using the circuit model to create $|W\rangle$ from $|+\rangle|+\rangle|+\rangle$ is given in [12]. In

[26] a very nice representation of a possible $|W\rangle$-state stabilizer is given in terms of the Pauli matrices. A set of generating matrices of this stabilizer is

$$M_1 = \tfrac{1}{3}(2\sigma_x \otimes \sigma_x \otimes \sigma_z + 2\sigma_y \otimes \sigma_z \otimes \sigma_y + \sigma_z \otimes I \otimes I)$$
$$M_2 = \tfrac{1}{3}(2\sigma_z \otimes \sigma_x \otimes \sigma_x + 2\sigma_y \otimes \sigma_y \otimes \sigma_z + I \otimes \sigma_z \otimes I)$$
$$M_3 = \tfrac{1}{3}(2\sigma_x \otimes \sigma_z \otimes \sigma_x + 2\sigma_z \otimes \sigma_y \otimes \sigma_y + I \otimes I \otimes \sigma_z).$$

Because the form of the general stabilizer of $|W\rangle$ can not take on the form of a $\mathcal{G}_3^+$-stabilizer, at least the LU-inequivalence of $|GHZ\rangle$ and $|W\rangle$ is implied from this representation. SLOCC-inequivalence can however not be deduced from the stabilizer representation as was originally hypothesized. It has become clear that the general stabilizer representation obscures the difference between non-maximally entangled $|GHZ\rangle$-class states and $|W\rangle$-class states. This distinction can be made however by using the construction of the normal form. The observable stabilizers of the $|GHZ\rangle$-class states should reduce to normal forms which assume the shape of a $\mathcal{G}_3^+$-stabilizer up to a possible factor $c$, as mentioned in section 3.3.1. When the procedure is performed on $|W\rangle$-class observable stabilizers, it should yield zero, as mentioned in section 4.3.2 and [41]. A possible further generalization of the stabilizer description to subgroups of the special linear group seems to allow for efficient distinction between the $|GHZ\rangle$- and $|W\rangle$-classes. This has not been studied in great detail however and more research is needed to make more definite statements about this possibility.

# Chapter 5

# Conclusions

This is a brief overview of the topics that have been introduced and studied in this thesis and the findings that were made during the course of this project. Sections 5.1 to 5.3 presented the most important subjects that were discussed in the previous chapters and section 5.4 contains a list of open questions resulting from this project.

## 5.1 Entangled pure states

Entanglement is a property of multi-body systems that is unique to the quantum theory of nature only. Whether a system in a pure state is entangled with another can easily be verified by computing the reduced density matrix which represents the state of this system alone. *Multi-local operations and classical communication* (LOCC/SLOCC) were defined in a mathematical manner so that their effects could be rigorously studied. *Entanglement classes* are defined under these operations, as are the desired properties of *entanglement monotones*, monotonic functions tailored to quantify entanglement between multiple systems. For two-body systems, the *Schmidt decomposition* turns out to be a most useful tool for the study of entanglement. To fully grasp the entanglement properties of many-body systems however, is far from trivial. The Schmidt decomposition can not capture all the ways entanglement between many bodies can be viewed. A generalization, the *minimal product decomposition* can accomplish this, but is very difficult to compute and the num-

ber of non-local parameters which are needed to fully define multi-body pure states grows much more rapidly than those than describe the multi-local operations under which classes can be defined. The largest multi-qubit system for which this problem does not yet limit the ability to define classes without continuous parameters is that of three-qubit pure states. Two classes of fully entangled three-qubit pure states were found and defined by the representative states $|GHZ\rangle$ and $|W\rangle$. The two most influential applications of entanglement in quantum information processing, *state-teleportation* and *Shor's factoring algorithm* were presented in section 2.10.2.

## 5.2 Pauli stabilizer representations

An important subclass of $n$-qubit entangled pure states are the *stabilizer states.* Using Abelian subgroups of $\mathcal{G}_n$, the group of $n$-tensor products of elements from the Pauli group, $n$-qubit pure states can be uniquely represented if the cardinality of the group is $2^n$. Such a group has the property that the equivalent vector representation of the pure state is an eigenvector with eigenvalue $+1$ of all the elements contained in it. All elements of such a group are said to stabilize the vector which equivalently represents the pure state. It is because of this that these groups are called *stabilizers.* Stabilizer states have the property that all the reduced density matrices of entangled qubits are equal to $\frac{1}{2}I$, which means these all maximize the von Neumann entropy of entanglement at a value of unity. Another consequence of this is that stabilizer states are in their *normal form.* Two states were found to be SLOCC-equivalent only if they have LU-equivalent normal forms. So for stabilizer states, the search for SLOCC-equivalency classes can be reduced to finding classes of LU-equivalent states. It turns

out that all stabilizer states are LU-equivalent to a subclass known as *graph states.* The stabilizer representation of an $n$-qubit pure state can be reduced to a binary array of size $2n \times n$. Graph states are those for which part of this array can be interpreted as an $n \times n$ adjacency matrix of a finite, simple, undirected graph. An important, so far only partially answered question which arises from this is whether the study of LU-equivalency classes of stabilizer states can be reduced to the study of LC-equivalency classes of graph states. LC operators are composed of operations in the mulit-local Clifford group, which is the normalizer of $\mathcal{G}_n$. An efficient algorithm has been found to recognize the LC-equivalence of two graphs using a simple operation known as *local complementation.* Two beautiful examples of applications of stabilizer theory, error correction and measurement based computation were introduced and roughly explained.

## 5.3 Observable stabilizers

The power and simplicity of the stabilizer representation of $n$-qubit pure states led to the idea to try to generalize it for different $n$-qubit pure states and the hypothesis that it could be used to efficiently identify SLOCC-inequivalent classes. The stabilizer formalism was generalized by defining an observable stabilizer as an Abelian group of Hermitian unitary operators which have at least one eigenvector with eigenvalue $+1$ in common. The application of this generalization as $\mathcal{G}_n^+$ yielded no new insights for two- and three-qubit pure states. This is because $\mathcal{G}_2^+$- and $\mathcal{G}_3^+$-stabilizer states have the property that any present entanglement is maximal in terms of the entropy of entanglement (having a value of unity). Following the discussions from chapters 2

and 3, it could be concluded that these states are LU equivalent to stabilizer states of the same dimension. For general $\mathcal{G}_n^+$ no clear conclusions could be drawn as a result of the realizations regarding LU-incomparability or LU-incommensurability [28, 23, 3, 7, 41]. A broader generalization was made to accommodate the construction of an observable stabilizer description for all $n$-qubit pure states. States in which present entanglement is not maximal (*i.e.*, those for which the reduced density matrices have von Neumann entropy $0 < E(\rho_a) < 1$) turn out to only have stabilizer descriptions in which the elements are composed of multi-qubit constituents (operators). It was deduced that the stabilizer for the $|W\rangle$-state can only have observable stabilizers of this class. The plural is used because it was also found that any $n$-qubit pure state can be stabilized by an infinite number of different observable stabilizers. Only for the special subclass mentioned above are $\mathcal{G}_n$-stabilizer representations also possible (up to multi-local unitary transformations). Observable stabilizers are easily constructed for any $n$-qubit pure state by performing a Walsh-Hadamard transform on a basis of orthogonal projectors, including that which is the density matrix of the state-vector. The pure-state classification under SLOCC using the observable stabilizer description did not turn out to be possible in the manner that was hoped for. It appears that the observable stabilizer description merely gives a means to quickly distinguish LU-inequivalent pure states if composed of the smallest possible constituents.

## 5.4 Future directions

Since the observable stabilizer description yields a new representation of $n$-qubit pure states, it may be possible that previously obscured properties can be more clearly

presented in this way. An interesting question is which type of states belong to the $\mathcal{G}_n^+$-stabilizer states and wether or not these are LU-equivalent to $\mathcal{G}_n$-stabilizer states (conventional stabilizer states). Although not as efficient as the conventional stabilizer formalism, observable stabilizers may be used as an efficient representation of some subclasses of $n$-qubit pure states. The binary description of the conventional stabilizer description may be generalizable to observable stabilizers in order to yield representations in terms of matrices in finite fields. Although non-maximally entangled states required multi-qubit constituents in the stabilizer elements, their representation may be simplified for those which are SLOCC equivalent to conventional stabilizer states, or stabilizer which have observable stabilizers with smaller constituents. This is because the transformation of a stabilizer by invertible operators is easily analyzed, and so may yield more insight in the difference between observable stabilizers for states in the $|GHZ\rangle$- and $|W\rangle$-classes for example. A very recent result indicates that this might indeed be possible by using stabilizing subgroups of the special linear group. It would also be interesting to find out if an efficient algorithm exists to find the observable stabilizer with the smallest possible constituents, given any $n$-qubit pure state. Another possibility may lie in the application of the generalization of the stabilizer formalism to the measurement based model of quantum computation.

# Appendix A

# SVD and spectral decomposition

The singular value and spectral decompositions are invaluable to the study of entanglement. That they are both very useful is of no surprise since they are actually the *same* decomposition expressed in different ways. This is what the following theorem and proof demonstrate.

**Theorem A.1.** *Let the singular value decomposition (SVD) of a complex matrix* $A \in \mathbb{C}^{m\times n}$ *be*

$$A = U\Lambda V^\dagger, \tag{A.1}$$

*where* $U$ *is the matrix whose columns are composed of the eigenvectors of the matrix* $AA^\dagger$, $\Lambda$ *is the diagonal matrix whose elements are* $\lambda_i$ *and* $V$ *is the matrix whose columns are composed of the eigenvectors of the matrix* $A^\dagger A$. *Then this is equivalent to a spectral decomposition*

$$A = \sum_i \lambda_i u_i v_i^\dagger, \tag{A.2}$$

*where* $u_i \in \mathbb{C}^m$ *and* $v_i \in \mathbb{C}^n$ *are the columns of matrices* $U \in \mathbb{C}^{m\times m}$ *and* $V \in \mathbb{C}^{n\times n}$.

*Proof.* This can be proved by showing that both expressions give rise to identical

elements $A_{ij}$ of the matrix $A$. The SVD of $A$ can be written element by element as

$$\begin{aligned} A_{ij} &= [U\Lambda V^\dagger]_{ij} \\ &= \sum_k U_{ik}[\Lambda V^\dagger]_{kj} \\ &= \sum_k U_{ik}\lambda_k V^\dagger_{kj} \\ &= \sum_k \lambda_k U_{ik} V^*_{jk} \\ &= \sum_k \lambda_k u_{ik} v^*_{jk} \end{aligned}$$

Using the fact that $u_{ik}$ and $v_{jk}$ are the $i$'th and $j$'th elements of vectors $u_k$ and $v_k$, the matrix can also be written as $A = \sum_k \lambda_k u_k v_k^\dagger$. From this it becomes apparent that the SVD and spectral decomposition of $A$ are equivalent. □

# Appendix B

# Product vectors

**Lemma B.1.** *For any plane $\mathcal{P}_1$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ defined by two product vectors $|v_1\rangle$ and $|v_2\rangle$, either all the states in this plane are product vectors, or there is no other product vector in it.*

*Proof.* [35], page 827. With the help of SU(2)⊗SU(2) transformations, $|v_1\rangle$ and $|v_2\rangle$ can always be expressed so that

$$\mathcal{P}_1 \equiv \alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta_1 \begin{pmatrix} \cos A \\ \sin A \end{pmatrix} \otimes \begin{pmatrix} \cos B \\ \sin B \end{pmatrix}, \tag{B.1}$$

with $0 \leq A, B \leq \pi/2$; $A$ and $B$ are not simultaneously vanishing, and $\alpha_1, \beta_1 \in \mathbb{C}$. All vectors in $\mathcal{P}_1$ are product vectors if and only if $\sin A \sin B = 0$. If $\sin A \sin B \neq 0$, then the only product vectors in $\mathcal{P}_1$ are the generators of the plane $|v_1\rangle$ and $|v_2\rangle$. □

According to this proof, if all vectors in $\mathcal{P}_1$ are product vectors, then they are LU equivalent to either

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} \alpha_1 + \beta_1 \cos B \\ \beta_1 \sin B \end{pmatrix} \text{ or } \begin{pmatrix} \alpha_1 + \beta_1 \cos A \\ \beta_1 \sin A \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The normalization condition on state vectors imposes restrictions on $\alpha_1$ and $\beta_1$ in this case, which are $\alpha_1\beta_1^* + \alpha_1^*\beta_1 = 0$ and $|\alpha_1|^2 + |\beta_1|^2 = 1$.

**Lemma B.2.** *Any plane $\mathcal{P}_2$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ contains at least one product vector. Some planes contain only one.*

*Proof.* [35], page 827. Consider the plane $\mathcal{P}_2$ generated by two orthogonal vectors. Again, with the help of SU(2)⊗SU(2) transformations, it can be expressed as

$$\mathcal{P}_2 \equiv \alpha_2 \begin{pmatrix} A \\ 0 \\ 0 \\ B \end{pmatrix} + \beta_2 \begin{pmatrix} CB \\ \gamma \\ \delta \\ -CA \end{pmatrix}, \tag{B.2}$$

with $A, B, C \in \mathbb{R}$ and $\gamma, \delta, \alpha_2, \beta_2 \in \mathbb{C}$. Assume that none of the generating vectors is a product vector, that is, $AB \neq 0$ and $C^2AB + \gamma\delta \neq 0$. Then a vector in $\mathcal{P}_2$ is a product vector if and only if

$$\alpha_2^2 AB + \alpha_2\beta_2 C(B^2 - A^2) - \beta_2^2(C^2AB + \gamma\delta) = 0 \tag{B.3}$$

With the above restrictions on $A, B, C, \gamma$ and $\delta$, there is always at least on nonvanishing solution (i.e., $\alpha_2, \beta_2$ such that $\alpha_2\beta_2 \neq 0$) of Eq.B.3. There is sometimes only one nonvanishing solution (see also Ref. [18]) □

# Bibliography


[1] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, *Concentrating partial entanglement by local operations*, Phys. Rev. A **53** (1996), no. 4, 2046–2052.

[2] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Phys. Rev. Lett. **70** (1993), no. 13, 1895–1899.

[3] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal, *Exact and asymptotic measures of multipartite pure-state entanglement*, Phys. Rev. A **63** (2000), no. 1, 012307.

[4] Emmanuel Briand, Jean-Gabriel Luque, and Jean-Yves Thibon, *A complete set of covariants for the four qubit system*, Journal of Physics A **36** (2003), 9915–9927.

[5] Robert Calderbank, Eric M. Rains, Peter W. Shor, and Neil J. A. Sloane, *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78** (1997), no. 3, 405–408.

[6] Robert Calderbank and Peter W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A **54** (1996), no. 2, 1098–1105.

[7] Hilary A. Carteret, Atsushi Higuchi, and Anthony Sudbery, *Multipartite generalization of the schmidt decomposition*, Journal of Mathematical Physics **41**

(2000), no. 12, 7932–7939.

[8] Valerie Coffman, Joydip Kundu, and William K. Wootters, *Distributed entanglement*, Phys. Rev. A **61** (2000), no. 5, 052306.

[9] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor, *Efficient algorithm to recognize the local clifford equivalence of graph states*, Phys. Rev. A **70** (2004), no. 3, 034302.

[10] ———, *Graphical description of the action of local clifford transformations on graph states*, Phys. Rev. A **69** (2004), no. 2, 022316.

[11] David Deutsch, http://www.qubit.org/people/david/, September 2006.

[12] Ellie D'Hondt, *Distributed quantum computation, a measurement based approach*, Ph.D. thesis, Vrije Universiteit Brussel, 2005.

[13] Wolfgang Dür, Guifré Vidal, and Ignacio Cirac, *Three qubits can be entangled in two inequivalent ways*, Phys. Rev. A **62** (2000), no. 6, 062314.

[14] Jens Eisert and Hans J. Briegel, *Schmidt measure as a tool for quantifying multiparticle entanglement*, Phys. Rev. A **64** (2001), no. 2, 022306.

[15] ———, *Schmidt measure as a tool for quantifying multiparticle entanglement*, Phys. Rev. A **64** (2001), no. 2, 022306.

[16] Daniel Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, Caltech., 1998.

[17] Daniel Gottesman, private communication, 2006.

[18] Markus Grassl, Thomas Beth, and Thomas Pellizzari, *Codes for the quantum erasure channel*, Phys. Rev. A **56** (1997), no. 1, 33–38.

[19] Marc Hein, *Entanglement in graph states*, Ph.D. thesis, Universität Innsbruck, 2005.

[20] Marc Hein, Jens Eisert, and Hans J. Briegel, Phys. Rev A **69(6)** (2004), no. 062311.

[21] Scott Hill and William K. Wootters, *Entanglement of a pair of quantum bits*, Phys. Rev. Lett. **78** (1997), no. 26, 5022–5025.

[22] Richard Jozsa and Noah Linden, *On the role of entanglement in quantum computational speed-up*, Proc. Roy. Soc. Lond. A Mat. **459** (2003), 2011–2032.

[23] Julia Kempe, *Multiparticle entanglement and its applications to cryptography*, Phys. Rev. A **60** (1999), no. 2, 910–916.

[24] Vivien Kendon and William J. Munro, *Entanglement and its role in shor's algorithm*, Tech. Report arXiv:quant-ph/0412140, HP Labs, 2005.

[25] Vivien M. Kendon, Kae Nemoto, and William J Munro, *Typical entanglement in multi-qubit systems*, SOCOMP **26** (2001), no. 5, 1484–1509.

[26] Akimasa Miyake and Hans J. Briegel, *Distillation of multipartite entanglement by complementary stabilizer measurements*, Physical Review Letters **95** (2005), no. 22, 220501.

[27] Michael Nielsen and Isaac Chuang, *Quantum computation and quantum information*, Cambrige, 2000.

[28] Michael A. Nielsen, *Conditions for a class of entanglement transformations*, Phys. Rev. Lett. **83** (1999), no. 2, 436–439.

[29] Asher Peres, *Higher order schmidt decomposition*, Phys. Lett. A **202** (1995), 16–17.

[30] Asher Peres and Leslie E. Ballentine, *Quantum theory: Concepts and methods*, American Journal of Physics **63** (1995), no. 3, 285–286.

[31] John Preskill, *Quantum information and computation, lecture notes for physics 229*, -, 1998.

[32] Robert Raussendorf and Hans J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. **86** (2001), no. 22, 5188–5191.

[33] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel, *The one-way quantum computer - a non-network model of quantum computation*, Journ. of Mod. Opt. **49** (2002), no. 2, 1299.

[34] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel, *Measurement-based quantum computation on cluster states*, Physical Review A (Atomic, Molecular, and Optical Physics) **68** (2003), no. 2, 022312.

[35] Anna Sanpera, Rolf Tarrach, and Guifré Vidal, *Local description of quantum inseparability*, Phys. Rev. A **58** (1998), no. 2, 826–830.

[36] Dirk Schlingemann, *Stabilizer codes can be realized as graph codes*, Quant. Inf. Comp. **2** (2002), no. 4, 307.

[37] Dirk Schlingemann and Reinhard F. Werner, *Quantum error-correcting codes associated with graphs*, Phys. Rev. A **65** (2001), no. 1, 012308.

[38] Erhard Schmidt, *Zur theorie der linearen und nichtlinearen integralgleichungen*, Math. Ann. **63** (1907), 433.

[39] Peter Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SOCOMP **26** (1997), no. 5, 1484–1509.

[40] Maarten van den Nest, *Local equivalence of stabilizer states and codes*, Ph.D. thesis, Katholieke Universiteit Leuven, 2005.

[41] Frank Verstraete, Jeroen Dehaene, and Bart De Moor, *Normal forms and entanglement measures for multipartite quantum states*, Physical Review A (Atomic, Molecular, and Optical Physics) **68** (2003), no. 1, 012103.

[42] Guifré Vidal, *Entanglement monotones*, Journ. of Mod. Opt. **47** (2000), 355.

[43] William K. Wooters, *Entanglement of formation of an arbitrary state of two qubits*, SOCOMP **26** (1997), no. 5, 1484–1509.