UNIVERSITY OF CALGARY

Analysing SLOCC-Equivalence of Graph States and Arbitrary Pure Quantum States

by

Adam D'Souza

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, 2008

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 "Analysing SLOCC-Equivalence of Graph States and Arbitrary Pure Quantum States" submitted by Adam D'Souza 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. Barry C. Sanders
Department of Physics and Astronomy

Dr. Karl-Peter Marzlin
Department of Physics and Astronomy

Dr. Gilad Gour
Department of Mathematics and Statistics

External examiner, Dr. Peter Høyer
Department of Computer Science

September 19, 2008

Date

Abstract

The classification of pure quantum states in terms of the resources they provide with regards to performing computational tasks is an important problem. From a fundamental standpoint, such a classification could give insight into the specific features of quantum information that differentiate it from its classical counterpart. From the pragmatic perspective, exhaustive knowledge of the specific forms that a particular resource can take could lead to simplifications in the implementations of various quantum information processing protocols. One means of classifying pure states is to divide them into classes whose members are interconvertible by means of protocols consisting solely of local operations and classical communication (LOCC). If the conversion succeeds with a probability less than unity, then the pure states are said to be equivalent under stochastic LOCC, or SLOCC.

There is a special class of states called stabiliser states, having some interesting properties. Firstly, stabiliser states are efficiently describable in terms of a linearly rather than exponentially growing number of parameters in the size of the Hilbert space of the system. Secondly, the class of stabiliser states is sufficiently rich that such states can be used for a variety of important quantum information processing tasks, most notably quantum error correction and measurement based quantum computing. Since any state that is SLOCC-equivalent to a stabiliser state can be used to perform the same tasks, it is a problem of interest to characterise such states. All stabiliser states are equivalent under local unitary operations to a specific kind of stabiliser state known as a graph state. Thus, it is sufficient for our purposes to consider SLOCC-equivalence to graph states in particular.

Suppose one is given two multipartite pure states $|\psi\rangle$ and $|\phi\rangle$ which may or may not be connected by a separable, invertible operator S, the diagnostic criterion for SLOCC

equivalence or inequivalence. One approach to testing the SLOCC-equivalence of $|\phi\rangle$ and $|\psi\rangle$ is to attempt to solve the relationship $|\phi\rangle = S|\psi\rangle$ explicitly for S. This is in general difficult, as the equations are multivariate polynomial equations with degree equal to the number of particles on which $|\psi\rangle$ and $|\phi\rangle$ are defined. In this thesis, a set of necessary conditions for the equivalence of $|\psi\rangle$ and $|\phi\rangle$ are given, using the stabiliser formalism, in the special case that $|\phi\rangle$ is a graph state. The evaluation of these conditions involves the solution of multivariate polynomial equations, but most of these conditions have degree much lower than the number of particles. A discussion of how the set of conditions may be extended to one that is sufficient to guarantee SLOCC-equivalence is also presented.

Acknowledgements

I am deeply grateful to my parents Tony and Ida, my sister Olivia, my brother-in-law John and all of my family and friends for their constant love and unwavering support. I am grateful to Paul Fairie for helping me with the figures in this thesis. I appreciate the work of my entire committee in advising me academically through regular committee meetings. I would like to thank the Natural Sciences and Engineering Research Council (NSERC), the Informatics Circle of Research Excellence (iCORE) and the Alberta Ingenuity Fund (AIF) for providing funding for my Master's research. I would like to thank Dr. Barry Sanders for assisting me in securing funding for my research. Finally, I am indebted to Dr. David Feder, of whom I could not have asked for more as a supervisor.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The classification of quantum states in terms of the characteristics they possess that allow them to be used for quantum information processing jobs is an important task. Many realistic quantum information processing tasks take the form of a situation in which a quantum system, or resource, consisting of some number of two-level quantum systems called qubits, is distributed over a number of spatially separated parties, and these parties are required to alter the quantum state of the resource in some predetermined way so as to produce a desired output. The parties can usually communicate classical information to each other as well (for example over the telephone), but they are usually unable to exchange quantum information. Thus, in their quest to solve the task presented to them, the parties are restricted to protocols in which each party is able to perform local operations and classical communication (LOCC). If the resource can be deterministically converted into the final quantum state by means of LOCC alone, then the resource and the final state are said to be LOCC-equivalent. If there is a LOCC protocol that effects the conversion with some finite probability rather than with certainty, then the initial and final states are said to be equivalent under stochastic LOCC (SLOCC). Two different quantum states that are SLOCC-equivalent to each other can be used to perform the same information processing tasks, although not necessarily with equal probabilities of success. Therefore, the classification of quantum states into equivalence classes under SLOCC is of obvious interest to quantum information theorists.

A particularly interesting class of quantum states is the so-called stabiliser states. These states have a compact, elegant description in terms of finite abelian groups called stabilisers. They are also known to serve as resources for some important quantum

information processing tasks, most notably quantum error correction and measurement-based quantum computing. It is not usually trivial to create a stabiliser state in an experimental setting in a way that is stable and relatively free of errors. For example, in the case of measurement-based quantum computing (MBQC), the required resource state is a specific kind of stabiliser state known as a cluster state. The principal experimental realisations of cluster states have thus far relied on some dynamical process, and the result is a resource state that is unstable and subject to decoherence. A potential road to circumventing this problem is to create some environment in which the ground state encodes a cluster state. This ground state must be non-degenerate and there must be a large energy gap between the ground state and the first excited state. It has been proven that cluster states themselves cannot arise as the non-degenerate ground states of any physically realisable Hamiltonian involving n-body interactions where n is at most 2. However, it might be possible to produce states that are SLOCC-equivalent to cluster states as non-degenerate ground states of such Hamiltonians. Such states can likely serve as resources for probabilistic MBQC.

It is generally a hard problem to determine SLOCC-equivalence of two arbitrary pure quantum states. The task of dividing up the complete set of pure states on n-qubits into disjoint SLOCC-equivalence classes has been accomplished for the cases $n = 2$ (two classes) and $n = 3$ (six classes). The cases where $n \geq 4$ turn out to be much more complicated, and it appears that there are an infinite number of SLOCC-equivalence classes in this case. Nevertheless, there are cases in which it is interesting simply to determine whether some specific quantum state is SLOCC-equivalent to another. For example, if a particular pure state is known to be the non-degenerate ground state of a gapped, physically realisable Hamiltonian, it could be useful to determine whether this state is SLOCC-equivalent to a cluster state. This problem should be much simpler than the general SLOCC classification problem. This thesis tackles the specific case in which

the given pure state is to be tested for SLOCC-equivalence to a specific kind of stabiliser state known as a graph state. The specific problem considered herein can be stated as follows: given an n-qubit graph state $|g\rangle$ and an n qubit pure state $|\psi\rangle$, determine whether or not there is an operator $S = \bigotimes_{i=0}^{n-1} S_i$ such that $|\psi\rangle = S|g\rangle$, where the S_i are single-qubit invertible operators. The solution of this problem implies the solution of the more general case of testing equivalence to a stabiliser state, as all stabiliser states are known to be locally equivalent to a graph state.

The approach taken here is to use the stabiliser formalism, most commonly seen in quantum information in the context of quantum error correction, to determine a set of necessary and sufficient conditions under which some given quantum pure state is SLOCC-equivalent to a graph state. Graph states can be described by the kind of stabilisers that are usually seen in the literature on quantum information, those whose elements consist of tensor products of operators from the Pauli group. Due to the structure of SLOCC transformations, it is shown in this thesis that SLOCC-transformed graph states can also be described by stabilisers comprising operators of the form of tensor products of local operators. In this case, the local operators are not from the Pauli group, but they have the same multiplication table (and therefore commutation relations) as the Pauli group, and are related to the Pauli group elements by similarity transformations. An arbitrary quantum state that is SLOCC-equivalent to a graph state must therefore possess a stabiliser whose elements are built from such local Pauli-like operators. This thesis gives a set of conditions involving the given state and some graph state (on the same number of qubits) that the Pauli-like operators must obey given their existence. We can therefore, given an arbitrary quantum pure state, assume the existence of a stabiliser for this state comprising Pauli-like local operators, and test the conditions for some graph state. If these conditions are not satisfiable, then our assumption of the existence of the Pauli-like operators was invalid, and the given state is inequivalent to

the graph state under SLOCC. The conditions derived herein thereby constitute a set of necessary conditions for SLOCC-equivalence of an arbitrary pure state and a graph state on the same number of qubits. Although the existence of a similar set of sufficient conditions is not proven, some discussion as to how one might construct these conditions is given in the conclusions. Furthermore, the form taken by the conditions allow them to be tested more easily than any similar conditions based on solving for the existence of an SLOCC-transformation between the given state and the graph state directly. Solving for an explicit SLOCC-transformation involves solving a system of multivariate polynomial equations, each having degree equal to the number of qubits in the system. It is known that the general problem of solving even systems of multivariate polynomials of degree 2 is NP-complete. However, there is cause for hope; it is sometimes possible to solve overdefined systems of multivariate polynomial equations, such as the system in which we are interested, efficiently. The necessary conditions for SLOCC-equivalence between a graph state and an arbitrary pure state given in this thesis are also in the form of multivariate polynomial equations, but with reduced degree. Specifically, for an n-qubit system, there are $\binom{n}{k}$ conditions of degree k.

The thesis is structured as follows: background information on quantum information processing is found in Chapter 2. Important concepts regarding SLOCC-equivalence are detailed in Chapter 3. The necessary background on the general stabiliser formalism and the standard way in which it arises in quantum information theory is presented in Chapter 4. The new contributions of this thesis, namely the derivation of the necessary conditions for SLOCC-equivalence between a graph state and an arbitrary quantum pure state, are provided in Chapter 5. Finally, the conclusions of this thesis and some ideas as to how to construct a set of sufficient conditions for SLOCC-equivalence, as well as possible future applications to MBQC, are the subject of Chapter 6.

Chapter 2

Introduction to Quantum Information Processing

2.1 The power of quantum information processing

Quantum information processing is an exciting and relatively new field of research that harnesses the properties of quantum mechanics for the purposes of computing. Although there is no conclusive proof as yet, it appears that quantum computers offer significant efficiency improvements over their classical counterparts with regards to performing certain computational tasks. For example, Grover's algorithm for quantum information processors gives us a means for searching for a marked item in an unsorted database in a time proportional to the square root of the number of entries in the database, a quadratic speed-up over the best known algorithm for a classical computer [1]. In 1994, Shor demonstrated how a quantum computer can factor large numbers in a time polynomial in the size of the number, an exponential speed-up over the best known classical algorithm [2]. This result has important implications for communication security, as current cryptography schemes such as RSA encryption rely upon the hardness of the factoring problem for their security [3]. Perhaps most excitingly, Feynman conjectured in 1982 [4] and then Lloyd showed in 1996 [5] that it is possible to simulate quantum systems efficiently with a quantum computer, a task that is intractable by any known means on classical computers because the quantity of complex numbers required to specify quantum systems increases exponentially as a function of the number of particles in the system. Quantum simulation is of tremendous importance to scientists who study the behaviour of quantum systems. Therefore, quantum computers appear to be a truly fascinating technological prospect.

2.2 Qubits

2.2.1 Classical bits and qubits

In classical information theory, the basic unit of information is called the *classical bit*, or just the *bit*. Abstractly speaking, a bit of information is a single character representing either the number 0 or the number 1. The physical realisation of bits is some physical system that only exists in one of two physically distinguishable states, one corresponding to 0 and the other to 1. For example, a bit can be realised by means of an electrical circuit containing a switch. If the switch is open and no current flows through the circuit, then the bit is said to be in state 0. If the switch is closed and current flows, then the bit is in state 1. These states can be distinguished by means of a measurement of the current in the circuit.

Analogously, in quantum information theory, the basic unit of information is called the *quantum bit*, or just the *qubit* [6]. Similar to the bit, a qubit is a physical (quantum) system that can exist in one of two physically distinguishable states, corresponding to the 0 state and the 1 state. However, due to their quantum nature, qubits are also able to exist in a superposition of the 0 and 1 states. For instance, a qubit can be physically realised by a spin-$\frac{1}{2}$ particle. The 0 and 1 states respectively correspond to the amount of the total spin of the particle projected onto some fixed axis being $+\frac{1}{2}$ or $-\frac{1}{2}$ in units of the reduced Planck constant $\hbar$. These states can be distinguished from each other by measuring the chosen component of total spin, for example with a Stern-Gerlach apparatus [7]. The superposition property of qubits is essential to the working of many interesting quantum algorithms, those that either improve on their best known classical counterparts or describe tasks that are impossible with classical information.

2.2.2 Dirac notation for quantum state vectors

Throughout this thesis, *Dirac notation* will be used to describe quantum states. In this notation, a quantum state will be represented by a construction called a *ket*. The kets corresponding to the zero and one states of a qubit will be denoted as $|0\rangle$ and $|1\rangle$ respectively. These states constitute an orthonormal basis for the Hilbert space of the qubit, called the *computational basis* [6]. In this notation, an arbitrary quantum pure state (i.e. one that can be regarded as a superposition of $|0\rangle$ and $|1\rangle$ would look like

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.1}$$

where $a, b \in \mathbb{C}$. The coefficients a and b will obey the relation

$$|a|^2 + |b|^2 = 1 \tag{2.2}$$

and a quantum state for which this is true is said to be *normalised*. For a normalised quantum state, the quantities $|a|^2$ and $|b|^2$ can be interpreted as the probabilities that an attempt to reveal the state of the system, via a so-called measurement in the computational basis, would yield state $|0\rangle$ and state $|1\rangle$ respectively.

It should be noted that it is not always possible to describe the state of a quantum system using this formalism. Those quantum states that can be specified in this way are called *pure states*. If Alice knows that a quantum system is in a pure state, and also knows the state of the system, then she knows all the information about the system that can be known. There is another class of quantum states, called *mixed states*, that cannot be described with the formalism of this section. A more advanced formalism, the *density matrix* representation of quantum states, addresses this issue [8, 9]. The density matrix representation is discussed in section 2.6.

2.2.3 Column vector notation

Quantum states can be viewed as vectors in a Hilbert space, and can thus be represented as column vectors. For example, we can use the qubit states $|0\rangle$ and $|1\rangle$ to specify an orthonormal basis for the Hilbert space of the qubit, represented in vector form as

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.3}$$

and

$$|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{2.4}$$

and thus the general superposition state of Equation (2.1) would be written as

$$\begin{aligned} |\psi\rangle &= a|0\rangle + b|1\rangle \\ &\equiv a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} a \\ b \end{bmatrix}. \end{aligned}$$

Due to the existence of this concrete representation of abstract kets in a Hilbert space in terms of column vectors, the terms 'state', 'vector' and 'state vector' will often be used interchangeably in this thesis. The basis consisting of the vectors $|0\rangle$ and $|1\rangle$ is called the *computational basis* for the Hilbert space, and the vectors $|0\rangle$ and $|1\rangle$ themselves are called *computational basis vectors* or *computational basis states.*

2.2.4 Dual vectors and inner products

Every vector in a Hilbert space has a corresponding *dual vector.* In Dirac notation, the dual vector of a quantum state represented by a ket is denoted using a construct called a *bra.* The bra corresponding to a ket $|\psi\rangle$ looks like $\langle\psi|$. In vector representation, the

dual vector of a column vector representing a ket is given by a row vector denoting the corresponding bra. The bra vector is the *adjoint*, or complex conjugate transpose of the dual column vector. Denoting the adjoint operator by the symbol † and complex conjugation by $*$, we have

$$\begin{aligned} \langle\psi| &= |\psi\rangle^\dagger \\ &\equiv \begin{bmatrix} a \\ b \end{bmatrix}^\dagger \\ &= \begin{bmatrix} a^* & b^* \end{bmatrix}. \end{aligned}$$

The *inner product* between two state vectors $|\psi\rangle$ and $|\phi\rangle$ is given by the product of the dual vector $\langle\psi|$ with $|\phi\rangle$, denoted by $\langle\psi|\phi\rangle$. With this definition in mind, the normalisation condition from Equation (2.2) is given by

$$\langle\psi|\psi\rangle = 1. \tag{2.5}$$

2.2.5 Multiple-qubit systems

Product states

The *Kronecker product*, denoted by $\otimes$, is used in the description of multiple-qubit systems. Suppose two qubits are individually in the state $|0\rangle$. Then their combined state would be given by $|0\rangle \otimes |0\rangle$, which can be written more compactly as $|00\rangle$. There are three other possible combined states in which each of the individual qubits is in a computational basis state; these are the states $|01\rangle$, $|10\rangle$ and $|11\rangle$. Together, these four combined states form a basis for the Hilbert space of the two-qubit system, and this basis is again called the computatational basis for the two-qubit Hilbert space. For example, if qubit 1 is in the state $|\psi_1\rangle = a_1|0\rangle + b_1|1\rangle$ and qubit 2 is in the state $|\psi_2\rangle = a_2|0\rangle + b_2|1\rangle$, then the total state $|\psi_{\text{tot}}\rangle$ of the combined system expressed in the computational basis is given

by

$$
\begin{aligned}
|\psi_{\text{tot}}\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle && (2.6)\\
&= (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) && (2.7)\\
&= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle && (2.8)\\
&\equiv \begin{bmatrix} a_1a_2 \\ a_1b_2 \\ b_1a_2 \\ b_1b_2 \end{bmatrix}. && (2.9)
\end{aligned}
$$

The state $|\psi_{\text{tot}}\rangle$ is called a *product state*, because it is just the Kronecker product of two single-qubit states. In general, a product state is any multi-qubit state that can be written as the Kronecker product of single-qubit states. Note that while the Hilbert space of each individual qubit had dimension 2, the Hilbert space of the combined system has dimension 4. In general, the Hilbert space of a combined n-qubit system will be 2^n-dimensional. The computational basis vectors are given by the set B, where

$$B = \{\ |k_1k_2\ldots k_n\rangle\ |\ k_i \in \{0,1\}\ \text{for all}\ i \in \{1,2,\ldots,n\}\ \}. \tag{2.10}$$

The labels of the kets in B just look like binary representations of the decimal numbers from 0 to $2^n - 1$, so we label these kets with decimal number labels. With the understanding that k_i refers to the ith digit in the binary representation of the decimal number k, we can just rewrite the definition of B from equation (2.10) as

$$B = \{\ |k\rangle\ |\ k_i \in \{0,1\}\ \text{for all}\ i \in \{1,2,\ldots,n\}\ \}. \tag{2.11}$$

For example, in the case of two qubits, the computational basis vectors would be labelled $|0\rangle \equiv |00\rangle$, $|1\rangle \equiv |01\rangle$, $|2\rangle \equiv |10\rangle$ and $|3\rangle \equiv |11\rangle$. The combined state for n qubits each in state $|\psi_i\rangle = a_{i,0}|0\rangle + a_{i,1}|1\rangle$ with the label i running from 0 to $n-1$ can thus be written

as

$$|\psi_{\text{tot}}\rangle = \bigotimes_{i=0}^{n-1} |\psi_i\rangle \tag{2.12}$$

$$= \bigotimes_{i=0}^{n-1} \sum_{j=0}^{1} a_{i,j}|j\rangle \tag{2.13}$$

$$= \sum_{k_0=0}^{1} \sum_{k_1=0}^{1} \cdots \sum_{k_{n-1}=0}^{1} a_{0,k_0} a_{1,k_1} \ldots a_{n-1,k_{n-1}} |k_0 k_1 \ldots k_n\rangle \tag{2.14}$$

$$= \sum_{k=0}^{n-1} c_k |k\rangle, \tag{2.15}$$

where

$$c_k = a_{0,k_0} a_{1,k_1} \ldots a_{n-1,k_{n-1}}. \tag{2.16}$$

The dual vector for the combined state is, naturally, given by

$$\langle\psi_{\text{tot}}| = \bigotimes_{i=0}^{n-1} \langle\psi_i| \tag{2.17}$$

$$= \sum_{k=0}^{n-1} c_k^* \langle k|, \tag{2.18}$$

where c_k^* is the complex conjugate of c_k as defined in Equation (2.16). It is straightforward to show that inner products for two product states are described by the rule

$$\left(\bigotimes_{i=0}^{n-1} \langle\psi_i| \right) \left(\bigotimes_{j=0}^{n-1} |\phi_j\rangle \right) = \prod_{i=0}^{n-1} \langle\psi_i|\phi_i\rangle. \tag{2.19}$$

As a consequence, any product state that is a product of normalised single-qubit state is itself normalised.

Entangled states

Product states are not the only kind of multi-qubit states. A system of multiple qubits can also be in an *entangled state*, one that cannot be written as the Kronecker product of single-qubit states. The signature of an entangled state is the absence of a solution to the system of equations (2.16) for the coefficients $a_{i,j}$ of the single-qubit states given the coefficients c_k of the state of the total system.

Example 2.2.1. A simple example is the two-qubit Bell state [10],

$$|\psi_{\text{Bell}}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.20}$$

For this state, the computational basis coefficients are $c_0 = \frac{1}{\sqrt{2}}$, $c_1 = 0$, $c_2 = 0$ and $c_3 = \frac{1}{\sqrt{2}}$. It is clear that there is no solution to the system of multivariate polynomial equations

$$c_0 = a_{0,0}a_{1,0} \tag{2.21}$$

$$c_1 = a_{0,0}a_{1,1} \tag{2.22}$$

$$c_2 = a_{0,1}a_{1,0} \tag{2.23}$$

$$c_3 = a_{0,1}a_{1,1} \tag{2.24}$$

and thus, the state $|\psi_{\text{Bell}}\rangle$ is entangled.

The physical significance of entangled states is that there are correlations between the states of the individual qubits. The fact that $c_1 = c_2 = 0$ means that there is no probability of measuring qubit 1 to be in state $|0\rangle$ and qubit 2 in state $|1\rangle$ simultaneously, nor is there any probability of finding qubit 1 in state $|1\rangle$ and qubit 2 in state $|0\rangle$ simultaneously.

2.3 Quantum logic gates

Classical and quantum computers process information by manipulating bits and qubits respectively. These manipulations occur by means of *logic gates*. Abstractly, a classical logic gate takes one or more bits as input and, depending on the states of the input bit, produces one or more bits as output. For example, the NOT gate takes a single bit as input and then flips the state of the bit. If the input bit was in state 0, the output bit will be in state 1, and vice-versa. If the bit were realised as an electrical circuit with

a switch as described in section 2.2.1, then the NOT gate has the effect of flipping the switch. The AND gate is an example of a multi-bit gate: it takes two bits as input and produces an output bit that is in state 1 if both the input bits were in state 1 and in state 0 otherwise.

Quantum logic gates follow the same principles, but act on qubits instead of bits. The quantum analogue of the NOT gate, which is called the *Pauli X gate*, maps an input qubit in state $|0\rangle$ to an output qubit in state $|1\rangle$ and an input qubit in state $|1\rangle$ to an output qubit in state $|0\rangle$. The difference between the classical NOT gate and the Pauli X gate is that the input qubit can be in a superposition of the states $|0\rangle$ and $|1\rangle$, in which case the output qubit will also be in a superposition of these states. The precise action of this gate can be written as

$$X\left(a|0\rangle + b|1\rangle\right) = \left(b|0\rangle + a|1\rangle\right). \tag{2.25}$$

In the above equation, X represents the gate being applied, and it is written to the left of the state to which it is applied. The output qubit is in the state on the right hand side of the equation. The logic gate is a linear operator that acts on quantum states represented by vectors in a Hilbert space. Throughout this thesis, the terms gate and operator will thus be used interchangeably.

Similarly to how quantum states can be represented by column vectors, operators can be expressed as matrices. The action of an operator is then described by multiplying the matrix on the right by the column vector representing the state on which the operator is acting, with the result being a column vector expressing the state of the output qubit. In general, a linear operator $\mathcal{O}$ can be expressed in any orthonormal basis $\{|i\rangle\}$ in either Dirac notation as

$$\mathcal{O} = \sum_i \sum_j o_{ij} |i\rangle\langle j| \tag{2.26}$$

a switch as described in section 2.2.1, then the NOT gate has the effect of flipping the switch. The AND gate is an example of a multi-bit gate: it takes two bits as input and produces an output bit that is in state 1 if both the input bits were in state 1 and in state 0 otherwise.

Quantum logic gates follow the same principles, but act on qubits instead of bits. The quantum analogue of the NOT gate, which is called the *Pauli X gate*, maps an input qubit in state $|0\rangle$ to an output qubit in state $|1\rangle$ and an input qubit in state $|1\rangle$ to an output qubit in state $|0\rangle$. The difference between the classical NOT gate and the Pauli X gate is that the input qubit can be in a superposition of the states $|0\rangle$ and $|1\rangle$, in which case the output qubit will also be in a superposition of these states. The precise action of this gate can be written as

$$X\left(a|0\rangle + b|1\rangle\right) = \left(b|0\rangle + a|1\rangle\right). \tag{2.25}$$

In the above equation, X represents the gate being applied, and it is written to the left of the state to which it is applied. The output qubit is in the state on the right hand side of the equation. The logic gate is a linear operator that acts on quantum states represented by vectors in a Hilbert space. Throughout this thesis, the terms gate and operator will thus be used interchangeably.

Similarly to how quantum states can be represented by column vectors, operators can be expressed as matrices. The action of an operator is then described by multiplying the matrix on the right by the column vector representing the state on which the operator is acting, with the result being a column vector expressing the state of the output qubit. In general, a linear operator $\mathcal{O}$ can be expressed in any orthonormal basis $\{|i\rangle\}$ in either Dirac notation as

$$\mathcal{O} = \sum_i \sum_j o_{ij} |i\rangle\langle j| \tag{2.26}$$

or in matrix notation as

$$\mathcal{O} = \begin{bmatrix} o_{00} & o_{01} & \cdots & o_{0(n-1)} \\ o_{10} & o_{11} & \cdots & o_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ o_{(n-1)0} & o_{(n-1)1} & \cdots & o_{(n-1)(n-1)} \end{bmatrix}, \tag{2.27}$$

where the quantities o_{ij} are called the *matrix elements* of $\mathcal{O}$. For example, the X operator is represented in the computational basis using Dirac notation as

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{2.28}$$

and in matrix notation as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.29}$$

Equation (2.25) can then be written in the computational basis as

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}. \tag{2.30}$$

The matrix notations of several important quantum gates in the computational basis are summarised in Table 2.1. The gates $R_x(\xi)$ and $R_z(\xi)$ describe rotations of the pure state vector of a single qubit about axes of the *Bloch sphere*, a convenient visualisation of the space of single-qubit pure states [11].

Notice that the action of the X operator is completely specified by its effect on the computational basis states $|0\rangle$ and $|1\rangle$, since it is a linear operator. In quantum information processing, operators are typically *unitary*.

Definition 2.3.1. *A unitary operator is an operator U obeying the property that $U^\dagger = U^{-1}$, i.e. $UU^\dagger = U^\dagger U = I$.*

Unitary operators are used in quantum information theory because they preserve the norm of a vector (the inner product of a vector with its own dual vector). This means

Symbol	Name	Matrix Notation
$I^{(2)}$	single-qubit identity operator	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
X	Pauli-X (or NOT)	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Y	Pauli-Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Z	Pauli-Z (or phase)	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
H	Hadamard	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
$R_x(\xi)$	rotation about x-axis by ξ	$\begin{bmatrix} \cos\frac{\xi}{2} & -i\sin\frac{\xi}{2} \\ -i\sin\frac{\xi}{2} & \cos\frac{\xi}{2} \end{bmatrix}$
$R_z(\xi)$	rotation about z-axis by ξ	$\begin{bmatrix} e^{-i\frac{\xi}{2}} & 0 \\ 0 & e^{i\frac{\xi}{2}} \end{bmatrix}$
CZ	controlled-Z (or controlled-phase)	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$

Table 2.1: Matrix notations in computational basis for some important quantum logic gates

that a state that is initially normalised remains normalised if a unitary operator acts upon it, thereby ensuring conservation of probability. The coefficients of the state vector encode the probability of observing the quantum system to be in the corresponding basis state, and these probabilities must add to unity in order for the description of the quantum system to be complete. A non-unitary operation that does not preserve the norm of the state would physically correspond to some mechanism of probability loss, such as particles escaping the system or information about the system being lost.

2.4 Quantum measurements

It is clear that both classical bits and qubits are capable of representing information, as their physical states encode information. In order to be able to do computation with these entities, it is also necessary to be able to access this information. This is done by means of *measurements*. As mentioned in section 2.2.1, the state of a classical bit represented by an electrical circuit is determined by measuring the current (for example with an ammeter) flowing through the circuit and then identifying zero current with the state 0 and non-zero current with the state 1. Since classical bits do not have the ability to be in a superposition of states, they will always be definitively in either state 0 or state 1, and the measurement merely reveals the state of the bit without altering it.

Quantum measurements (i.e. measurements of quantum systems, such as qubits) are somewhat more complex and the physical mechanism that occurs in quantum measurements, as well as the meaning of the measurement results, is today a matter of debate amongst physicists. The entire formalism of quantum mechanics is based on a basic set of statements known as the *postulates of quantum mechanics*, and all of the mathematical structure is designed in keeping with these postulates. It should be noted that although there are many interpretations of quantum mechanics that are consistent with the pos-

tulates, the mathematical formalism used to do calculations does not depend in any way on the chosen interpretation. An in-depth treatment of the postulates and the formalism of quantum measurements can be found in [12].

A qubit can exist in a superposition of states $|0\rangle$ and $|1\rangle$. The most common kind of measurement of qubits performed in experiments is known as the *projective measurement*, which will be described more formally in section 2.4.2 below. The essence of a projective measurement revolves around a particular type of quantum operator called an *observable*. According to the postulates of quantum mechanics, an observable is an operator that is *Hermitian*, meaning that it is equal to its own adjoint.

Definition 2.4.1. *A Hermitian operator O is one that obeys the property $O = O^\dagger$.*

Definition 2.4.2. *In quantum mechanics, an observable is a Hermitian operator.*

Examples of observables include quantities such as position, momentum, total angular momentum, spin, and so on. A projective measurement is a measurement of a particular observable corresponding to some property of the quantum system. According to the postulates of quantum mechanics; when an observable is measured, the result of the measurement is a number corresponding to one of the eigenvalues of the observable and immediately following the measurement, the state of the system will be the eigenvector of the observable corresponding to that eigenvalue. When the value of a physical observable is measured, the outcome of the measurement should be a real number. This is guaranteed to happen since observables are Hermitian operators and all eigenvalues of Hermitian operators are real. Furthermore, eigenvectors of Hermitian operators corresponding to distinct eigenvalues are always orthogonal, meaning that if the spectrum of the observable is non-degenerate, then the set of possible states of the system after the measurement form an orthonormal basis for the Hilbert space of the system. These points are clarified in Examples 2.4.5 and 2.4.6.

2.4.1 General measurement postulate

Formally, a quantum measurement is specified by a set of measurement outcomes $\{i\}$, corresponding to a set of measurement operators $\{M_i\}$ which form a *complete* set.

Definition 2.4.3. *A complete set of operators $\{O_i\}$ is one obeying the property $\sum_i O_i^\dagger O_i = I$.*

If the state of the quantum system on which the measurement is being performed is $|\psi\rangle$, then the measurement outcome i occurs with probability

$$p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle \tag{2.31}$$

and the state of the system after the measurement is given by

$$|\psi^{(i)}\rangle = \frac{1}{\sqrt{p_i}} M_i|\psi\rangle. \tag{2.32}$$

The completeness of the measurement operators guarantees that the probabilities of each of the outcomes sum to 1, thus guaranteeing that no possible measurement outcomes have been neglected:

$$\begin{aligned}
\sum_i p_i &= \sum_i \langle\psi|M_i^\dagger M_i|\psi\rangle \\
&= \langle\psi|\left(\sum_i M_i^\dagger M_i\right)|\psi\rangle \\
&= \langle\psi|I|\psi\rangle \\
&= \langle\psi|\psi\rangle \\
&= 1
\end{aligned}$$

2.4.2 Projective measurements

Projective measurements are the most common type of measurement found in experimental settings, and also the most common kind that are used in quantum mechanics. In a projective measurement, all of the measurement operators are *projectors.*

Definition 2.4.4. *A projector is a Hermitian operator $\mathcal{P}$ obeying the condition $\mathcal{P}^2 = \mathcal{P}$.*

Example 2.4.5. Consider the quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$, and the observable

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{2.33}$$

which can be written in matrix form in the computational basis as

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.34}$$

The eigenvectors of this observable are $|0\rangle$ and $|1\rangle$, corresponding to eigenvalues $+1$ and -1 respectively. We can define a projective measurement in the eigenbasis of Z by means of the measurement operators

$$\begin{aligned} M_0 &= |0\rangle\langle 0| \\ M_1 &= |1\rangle\langle 1|, \end{aligned}$$

where M_0 and M_1 correspond to the measurement outcomes $+1$ and -1 respectively. The probability of measurement outcome $+1$ is

$$\begin{aligned} p_0 &= \langle\psi|M_0 M_0^\dagger|\psi\rangle \\ &= \left(a^*\langle 0| + b^*\langle 1|\right)|0\rangle\langle 0|0\rangle\langle 0|\left(a|0\rangle + b|1\rangle\right) \\ &= \left(\left(a^*\langle 0| + b^*\langle 1|\right)|0\rangle\right)\left(\langle 0|\left(a|0\rangle + b|1\rangle\right)\right) \\ &= a^* a \\ &= |a|^2 . \end{aligned}$$

The state of the system after measurement outcome $+1$ is

$$\begin{aligned} |\psi^{(0)}\rangle &= \frac{1}{\sqrt{p_0}} M_0|\psi\rangle \\ &= \frac{1}{\sqrt{|a|^2}}|0\rangle\langle 0|\left(a|0\rangle + b|1\rangle\right) \\ &= \frac{1}{|a|}\left(a|0\rangle\right) \\ &= |0\rangle, \end{aligned}$$

up to a global phase. Similarly, the measurement outcome -1 leaves the system in the state $|1\rangle$ and occurs with probability $|b|^2$. The possible states of the system after the measurement are just the computational basis states, which indeed constitute an orthonormal basis for the Hilbert space of the system.

In general, the probabilities of the various outcomes of a projective measurement of a Hermitian operator $\mathcal{O}$ on the state $|\psi\rangle$ can be read off by writing $|\psi\rangle$ in the eigenbasis of $\mathcal{O}$ and then calculating $|a_i|^2$, where a_i is the coefficient in front of the basis vector corresponding to the relevant measurement outcome.

Example 2.4.6. Consider the operator X defined in equations (2.25) and (2.29). The eigenvalues of this operator are ± 1, corresponding to eigenstates $|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ respectively. Now note that the state $|\psi\rangle$ from the previous example can be written as

$$\begin{aligned}
|\psi\rangle &= a|0\rangle + b|1\rangle \\
&= \frac{1}{2}(a|0\rangle + a|1\rangle + b|0\rangle + b|1\rangle + a|0\rangle - a|1\rangle - b|0\rangle + b|1\rangle) \\
&= \frac{1}{\sqrt{2}}(a+b)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(a-b)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \frac{1}{\sqrt{2}}(a+b)|+\rangle + \frac{1}{\sqrt{2}}(a-b)|-\rangle
\end{aligned}$$

Thus, a measurement of X will yield ± 1 with probability $\frac{1}{2}|a \pm b|^2$, and the state of the system will be collapsed to $|\pm\rangle$. This is an example of a measurement in the orthonormal basis $\{|+\rangle, |-\rangle\}$, commonly referred to as the *X-basis*.

2.4.3 Positive Operator-Valued Measure measurements

Projective measurements are not the most general type of measurements that are possible. A projective measurement of an observable with a non-degenerate spectrum always corresponds to a measurement in an orthonormal basis. However, it is possible in principle to perform measurements in a non-orthogonal basis, and these types of measurements

are described by *positive operator-valued measure measurements* (POVM measurements, or just POVMs). The reasons for the name of this type of measurement are technical, and not of relevance to the subject of this thesis. It is not simple to describe the action of a POVM on a system by inspection, as was frequently the case for projective measurements. Instead, the full set of measurement operators must be written down explicitly and the probabilities of the measurement outcomes and the resulting states of the system must be formally calculated. Although POVMs cannot typically be implemented directly in the lab, a result called *Neumark's theorem* shows how a POVM can be implemented as a projective measurement in a higher-dimensional Hilbert space [13].

2.5 The circuit model

The *circuit model* [11] of quantum computation is a means of describing algorithms for quantum information processors. In this model, qubits are initialised in some specified state, then they are acted upon by quantum operators (i.e. logic gates) and finally, output is obtained by means of measurement of some subset of the qubits. An algorithm can be depicted diagramatically as a *circuit.* Logical flow in a circuit diagram goes from left to right. Qubits are represented as wires, with the initial state of a qubit written to the left of the wire representing it. Operators are represented by boxes with the name (or symbol) of the operator written inside them. Measurement in the computational basis is depicted as a meter.

Example 2.5.1. Quantum teleportation is a quantum algorithm allowing one party, Alice, to transfer the state of a qubit that she has in her possession to another party, Bob, provided she and Bob share an entangled pair of qubits and are allowed to communicate the results of measurements to each other. The quantum teleportation algorithm is depicted by the circuit in Figure 2.1.

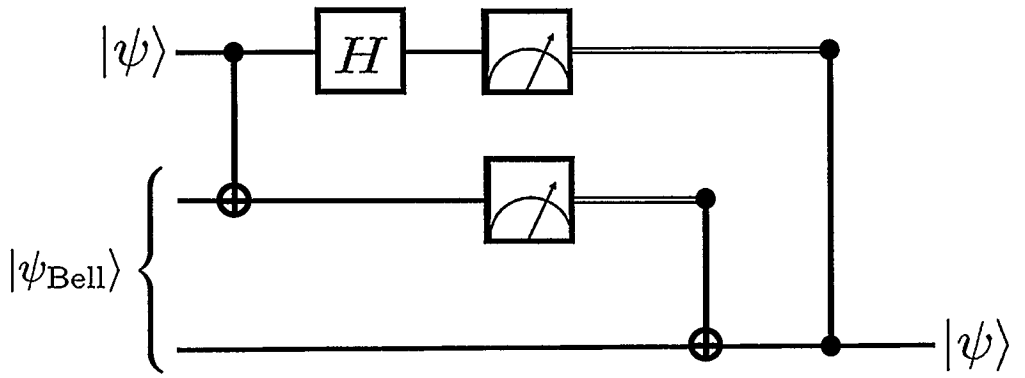


Figure 2.1: Circuit diagram for quantum teleportation algorithm.

The steps of this algorithm can be read off the diagram above, from left to right. Alice begins with a qubit in state $|\psi\rangle$, as well as the first qubit of a pair of entangled qubits in the state $|\psi_{Bell}\rangle$ defined in Equation (2.20), qubit 2. The second qubit of this pair, qubit 3, is in Bob's possession. Alice then performs a controlled-X gate with qubit 1 as the control and qubit 2 as the target, thereby generating entanglement between qubits 1 and 2. She applies a Hadamard gate to qubit 1 and then measures it in the computational basis (this pair of actions can together be thought of as measuring qubit 1 in the X-basis), and sends the result to Bob. She also measures qubit 2 in the computational basis and sends that result to Bob. Based on these measurement results, Bob then performs one of four possible sequences of operations to qubit 3, following which the final state of qubit 3 (which is in Bob's possession) will be the same as the initial state of qubit 1 (which was in Alice's possession), thereby effecting the teleportation.

Example 2.5.2. Gate teleportation, another quantum algorithm, can be viewed as a generalisation of the regular teleportation algorithm described above. In this case, Alice teleports the state of qubit 1, along with a rotation in Hilbert space about the z-axis, to Bob. The only difference between the algorithms is the operation Alice performs on qubit 1 before her computational basis measurement (or equivalently, the basis in which

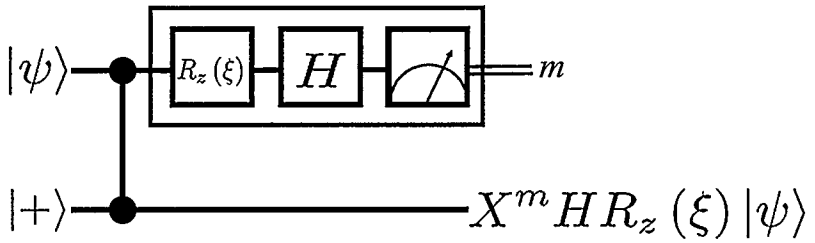


Figure 2.2: Circuit diagram for single-qubit gate teleportation. The set of operations inside the red box is equivalent to a measurement in the ξ basis

she does the measurement). By measuring in the basis

$$\left\{|\xi_+\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + e^{-i\frac{\xi}{2}}|1\rangle\right), |\xi_-\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle - e^{-i\frac{\xi}{2}}|1\rangle\right)\right\} \tag{2.35}$$

which will be called the ξ-basis in this thesis, where $0 \leq \xi < 2\pi$, Alice teleports the state $R_z(\xi)|\psi\rangle$ to Bob rather than just the state $|\psi\rangle$.

2.6 Density matrices and mixed states

The Dirac state vector formalism of section 2.2.2 is not capable of describing the most general types of quantum states possible. For example, suppose that Alice possesses a qubit in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Suppose then that she has a black box that performs a projective measurement on the qubit, but does not reveal the outcome to her. In this scenario, the superposition exhibited by the qubit between the two computational basis states has been destroyed and it has been collapsed into one of the states $|0\rangle$ or $|1\rangle$, each outcome occurring with probability $\frac{1}{2}$. However, Alice does not know which outcome has occurred. From the point of view of the information about the system available to Alice, the state of the qubit is now a mixture (not a superposition) of the states $|0\rangle$ and $|1\rangle$. Such a type of quantum state is called a *mixed state*, and it cannot be described using the state vector formalism. Instead, we use the *density matrix* or *density operator* formalism to describe the state [8, 9].

Definition 2.6.1. *The density matrix or density operator ρ corresponding to a pure quantum state $|\psi\rangle$ is given by*

$$\rho = |\psi\rangle\langle\psi|. \tag{2.36}$$

All of the information contained in $|\psi\rangle$ is encoded in the corresponding density matrix ρ. Thus, ρ can be viewed as a different way of expressing the state of a quantum system. This formalism can be used to describe mixed states as well. A mixed state of a system can be viewed as an ensemble of the pure states (described by density matrices ρ_k) in which the system could exist, together with the corresponding probabilities p_k of the system being in the various pure states. Such an ensemble is usual denoted by $\{(p_k, \rho_k)\}$. Then, a density matrix can be written down for the mixed state described by this ensemble.

Definition 2.6.2. *Consider a quantum system that exists in a mixed state corresponding to an ensemble $\{(p_k, \rho_k)\}$. The density matrix ρ describing this mixed state is given by*

$$\rho = \sum_k p_k \rho_k. \tag{2.37}$$

Example 2.6.3. The ensemble corresponding to Alice's mixed state from the beginning of this section would be denoted by $\left\{(\frac{1}{2}, |0\rangle\langle 0|), (\frac{1}{2}, |1\rangle\langle 1|)\right\}$, where $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ are the density matrix representations of the two (pure) computational basis states. The density matrix corresponding to this mixed state is given by

$$\begin{aligned} \rho &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\ &\equiv \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}. \end{aligned}$$

A density matrix ρ can be classified as a pure or mixed state using its rank. If it is a pure state, then it will have rank $r(\rho) = 1$. If it is a mixed state, then it will have rank $r(\rho) > 1$. The description of the information about a multipartite system possessed by any one party is given by the *reduced density matrix* [9] corresponding to that party.

Definition 2.6.4. *Let ρ_{AB} be a density matrix describing a quantum state distributed between parties A and B. Let $\{i_A\}$, $\{i_B\}$ be a set of independent basis vectors for the subsystems corresponding to party A and B respectively, such that*

$$\rho_{AB} = \sum_{i_A,i_B,j_A,j_B} (\rho_{AB})_{i_A j_A i_B j_B} |i_A\rangle|i_B\rangle\langle j_A|\langle j_B|. \tag{2.38}$$

Then the reduced density matrix ρ_A corresponding to party A is given by

$$\rho_A = Tr_B(\rho_{AB}) \tag{2.39}$$

$$= \sum_{i_A,i_B,j_A,j_B} (\rho_{AB})_{i_A j_A i_B j_B} |i_A\rangle\langle j_A|\langle i_B|j_B\rangle. \tag{2.40}$$

The operation $Tr_B(\rho_{AB})$ is called the partial trace over B of ρ_{AB}.

The reduced density matrix is a convenient tool for determining whether or not a multipartite system is entangled. Suppose ρ_{AB} is a bipartite state distributed between parties A and B. Then, the subsystem belonging to A is entangled with the one belonging to B if and only if the rank of the reduced density matrix ρ_A is 1. This method of diagnosing entanglement will prove useful the discussion of equivalence under stochastic local operations and classical communication found in Chapter 3.

2.7 Admissible Quantum Operations

The density matrix formalism allows us to generalise our description of the types of operations that can be performed on a quantum state, such as gates and measurements, to mixed states. Any operation that can be physically performed on a quantum state is called an *admissible quantum operation.* All admissible quantum operations on a state descibed by density matrix ρ can be decomposed into combinations of elements from a set of four basic operations [14]:

1. Unitary operations. A unitary operation U effects the transformation

$$\rho \rightarrow U\rho U^\dagger. \tag{2.41}$$

2. Projective measurements. These map the single state $|\rho\rangle$ to an ensemble of pure states $\{\rho_k\}$ if the measurement outcome is recorded. In this case, the effect on the state of the system is

$$\rho \rightarrow \{p_k, \rho_k\}. \tag{2.42}$$

If the outcome is not recorded, then the state is mapped to the mixed state realised by the aforementioned ensemble. Each ρ_k corresponds to a measurement outcome that occurs with probability p_k. Specifically, if the measurement is given by measurement operators $\{M_k\}$, then $\rho_k = M_k \rho M_k^\dagger$. For this situation, the effect on the system is

$$\rho \rightarrow \sum_k p_k \rho_k. \tag{2.43}$$

3. Addition of unentangled ancillary systems. If the ancillary systems are in the state ρ_a, then the effect on the state of the subsystem is

$$\rho_i \rightarrow \rho_i \otimes \rho_a. \tag{2.44}$$

4. Removal of a subsystem from the whole system. This amounts to erasing all knowledge about a particular subsystem i of the total state ρ. Deletion of subsystem i effects the transformation

$$\rho \rightarrow \mathrm{Tr}_i(\rho), \tag{2.45}$$

where Tr_i denotes the *partial trace* over subsystem i.

Any admissible quantum operation can be decomposed into products of these four basic constituents. Formally, an admissible operation $\mathcal{E}$ has the effect

$$\rho \rightarrow \mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{2.46}$$

where the E_i are called *Kraus operators* and obey the condition $\sum_i E_i E_i^\dagger \leq I$. Equality of this condition is satisfied if no measurement outcomes are recorded, allowing measurements to evolve the initial state to a mixed state and thereby preserving the trace of the

density matrix. If measurement results are recorded, then the state is mapped to a single element of an ensemble of states, which will have trace less than unity. In this situation, some of the outcomes of the operation, $\rho_i = E_i \rho E_i^\dagger$, are rendered impossible.

Chapter 3

Local Transformations and Equivalence Classes

3.1 Introduction

The purely quantum property of entanglement that was discussed in Section 2.2.5 is crucially important for several quantum information processing tasks. Despite its importance, much of the essential nature of entanglement remains poorly understood. Furthermore, not all entangled states are created equal; for example, the teleportation scheme of Example 2.5.1 only succeeds with unit probability if a Bell state, which is in a sense the maximally entangled pure state on two qubits, is available for Alice and Bob to share. If instead they share a 'less entangled' two-qubit state, then they will only be able to perform the teleportation with probability less than one. One approach to improving our understanding of entanglement is to classify quantum states distributed over multiple spatially separated parties in terms of whether they can be interconverted purely by means of local operations and classical communications. This chapter gives some background into the topic of classifying quantum states in this way.

3.2 Local Operations and Classical Communication

It is not possible to create an entangled state of qubits from a separable state using only single-qubit operations. Suppose we are given an initial state $|\psi_{in}\rangle = \bigotimes_i |\psi_i\rangle$, defined on n qubits, and we apply a single-qubit operation to each qubit, so that the total operation

has the form $\mathcal{O} = \bigotimes_{i=0}^{n-1} \mathcal{O}_i$. Then, the output state $|\psi_{\text{out}}\rangle$ is given by

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \mathcal{O}|\psi_{\text{in}}\rangle \\ &= \left(\bigotimes_{i=0}^{n-1} \mathcal{O}_i\right)\left(\bigotimes_{j=0}^{n-1} |\psi_j\rangle\right) \\ &= \bigotimes_{i=0}^{n-1} \mathcal{O}_i|\psi_i\rangle, \end{aligned}$$

which is clearly separable as well. Thus, in order to produce an entangled state from a separable one in the circuit model of quantum computation, it is necessary to use gates that operate on multiple qubits, such as for example the *controlled-Z* gate from Table 2.1. All universal gate sets will necessarily contain at least one true two-qubit gate. In other words, if Alice and Bob each possess a qubit, and these qubits are not entangled, then they will not be able to entangle these qubits regardless of what operations they perform to their respective qubits, assuming they do not have access to each other's qubits. This statement is true even if they are allowed to communicate classically with each other (such as over the telephone). The situation faced by Alice and Bob is a realistic one; real quantum information processing tasks could certainly require spatially separated parties in isolated laboratories to share an entangled system. These parties are restricted to performing *local operations* on their subsystems alone.

Definition 3.2.1. *An admissible quantum operation $\mathcal{E}$ that maps an n-qubit input state ρ to the output $\sum_i E_i \rho E_i^\dagger$ is called a local operation if and only if all of the E_i operators can be written in the form*

$$E_i = \bigotimes_{j=0}^{n-1} E_{ij},$$

where the E_{ij} are single-qubit operators.

Operations that can be performed by the individual parties in such a setting are collectively called *Local Operations and Classical Communications* (LOCC).

Definition 3.2.2. *A quantum information processing protocol that deterministically converts a given input state possessed by many parties into a desired output state possessed by many parties, which uses only local operations by the parties on their own parts of the system, plus communication of classical information between the parties, is called a local operations and classical communication (LOCC) protocol.*

Example 3.2.3. Suppose Alice and Bob share the (entangled) Bell state of Equation 2.20, and wish to convert it into the unentangled state $|00\rangle$. This can easily be accomplished, as follows: Alice measures her qubit in the computational basis. If she obtains the result 0, then the total state is collapsed to $|00\rangle$, and the task is finished. If she obtains the result 1, then the total state is $|11\rangle$, and Alice and Bob each have to perform X operations on their qubits. The protocol is summarised as follows:

1. Alice measures her qubit in the computational basis and communicates the result to Bob classically.
2. If the result was 0, then Alice and Bob do nothing. If the result was 1, then Alice and Bob each apply the Pauli X gate to their respective qubits.

Since the unentangled output cannot be turned into an entangled state by means of local operations alone, the LOCC protocol is clearly not reversible.

Two states $|\psi\rangle$ and $|\phi\rangle$ that are mutually interconvertible by means of LOCC protocols are said to be *LOCC-equivalent.* Similarly, two states that are mutually interconvertible by means of solely local unitary operations by the parties are said to be *LU-equivalent.* It has been shown that LOCC-equivalence and LU-equivalence amount to the same thing, i.e. that two LOCC-equivalent states are also LU-equivalent [15, 16, 14]. This is problematic, as local unitary transformations of a state can be viewed as merely changing the local bases used to express the state of the system, which has no real effect on the entanglement properties of the system. Qualitatively speaking, two states that are

LOCC-equivalent must therefore have precisely the same amount of entanglement, which can be quantified by *entanglement monotones* (to be introduced in Section 3.4). Since entanglement monotones can be continuously varying functions, the amount of entanglement can be viewed as a continuous parameter that characterises LOCC-equivalence classes. Any two states that have different amounts of entanglement will be LOCC-inequivalent. The fact that there are infinitely many entanglement classes as specified by LOCC-equivalence casts into doubt the utility of such a scheme for entanglement characterisation. It could be more useful to have a classification scheme that allows for 'coarser graining' of entanglement classes, such that they are characterised by discrete rather than continuous parameters, so that there are a finite number of such classes. For systems of three or fewer qubits, such a scheme is available, based on equivalence under *Stochastic Local Operations and Classical Communication* (SLOCC).

3.3 Stochastic LOCC

In Section 3.2, the protocols considered were those that transformed a given input state to some specific output state with certainty. But, in protocols where both local measurements and communication of measurement results are allowed, it is possible to have rounds of the protocol in which some party performs an operation that is conditioned on the result of some other party's measurement. Since measurements in general have multiple possible outcomes, this means that certain protocols consisting of local operations and classical communication can have a number of different branches that occur with generally different probabilities, depending upon the results of certain intermediate measurements. The different branches of the protocol can lead to different output states, which means that it is possible to design protocols comprised solely of local operations and classical communication that convert an input state to a desired output state with a

probability less than 1. Such protocols are called *stochastic local operations and classical communications* (SLOCC) protocols [15].

Definition 3.3.1. *A quantum information processing protocol that takes a multipartite input state ρ and transforms it into one of a set of possible output states ρ_k, each occurring with some probability $p_k < 1$, that consists solely of local gates and measurements, plus communication of classical information between the parties, is called a stochastic local operations and classical communications (SLOCC) protocol.*

Similarly to how LOCC-equivalence was defined, we call two pure states $|\psi\rangle$ and $|\phi\rangle$ *SLOCC-equivalent* if and only if they can be mutually interconverted with probability $0 < p < 1$. It has been shown [16] that two pure states are SLOCC-equivalent if and only if there exists a separable, invertible operator that connects them. Since this condition is both necessary and sufficient for SLOCC-equivalence of two pure states, it can be regarded as an alternate definition of SLOCC-equivalence for pure states.

Definition 3.3.2. *Two n-qubit pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ are SLOCC-equivalent if and only if there exists an operator $S = \bigotimes_{i=0}^{n-1} S_i$ such that*

$$|\psi_1\rangle = S|\psi_2\rangle, \tag{3.1}$$

where the $\{S_i\}$ are all invertible single-qubit operators.

3.4 Entanglement monotones

Because LOCC protocols are unable to generate entanglement, they can naturally be used to define means of quantifying the amount of entanglement present in a system. Similarly, since SLOCC protocols cannot increase the amount of entanglement present on average, they too can be used to define quantitative measures of entanglement. This is done by means of so-called *entanglement monotones* [14].

Definition 3.4.1. *An entanglement monotone is a magnitude*

$$\mu : \rho \rightarrow \mu(\rho) \in \mathbb{R}^{+} \tag{3.2}$$

satisfying the following conditions:

1. *For any ρ and any local operation mapping ρ to an ensemble $\{p_k, \rho_k\}$,*

$$\mu(\rho) \geq \sum_k p_k \mu(\rho_k). \tag{3.3}$$

2. *For any ensemble $\{q_k, \rho_k\}$,*

$$\sum_k q_k \mu(\rho_k) \geq \mu\left(\sum_k p_k \rho_k\right). \tag{3.4}$$

The first condition ensures that an entanglement monotone is non-increasing on average under local transformations. The second condition states that if information about a system is locally dismissed, so that an ensemble of states is mapped to the mixed state realised by that ensemble, then the entanglement monotone is still non-increasing. A different kind of entanglement measure called a *type-II entanglement monotone* [17] can also be defined using the criterion of non-increasing behaviour under LOCC transformations, but we will not concern ourselves with this type of measure here.

The first significant effort towards quantifying entanglement came in the form of the development of the *entropy of entanglement* by Bennett et al. [18], which provided a well-defined way of determining the amount of entanglement possessed by a large number of copies of a bipartite pure state. Rapid progress ensued from this starting point, and measures of entanglement for mixed states and single copies of pure states were developed [19, 14, 20], culminating in the complete classification of all two-qubit and three-qubit pure quantum states into SLOCC equivalence classes. The two-qubit case is quite trivial: all entangled bipartite states are SLOCC equivalent to the Bell state $|\psi_{Bell}\rangle$ of Equation (2.20), and all separable states are in a different class. The three-qubit case is

more complex, and the classification uses an entanglement monotone called the *3-tangle*, introduced in [20]. It is shown in [16] that any genuinely tripartite entangled three-qubit pure states described by density matrix ρ_{ABC}, one obeying $r(\rho_A) = r(\rho_B) = r(\rho_C) = 2$, i.e. one for which all of the reduced density matrices have maximal rank, falls into one of precisely two distinct SLOCC equivalence classes. Denoting the 3-tangle of ρ_{ABC} as τ_{ABC}, the classes are:

1. Those states having $\tau_{ABC} > 0$. All states in this class are SLOCC-equivalent to

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C\right). \tag{3.5}$$

2. Those states having $\tau_{ABC} = 0$. All states in this class are SLOCC-equivalent to

$$|W_3\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle_A|0\rangle_B|1\rangle_C + |0\rangle_A|1\rangle_B|0\rangle_C + |1\rangle_A|0\rangle_B|0\rangle_C\right). \tag{3.6}$$

The situation is immensely more complicated for four or more qubits, and it has been shown that there are an infinite number of SLOCC-equivalence classes on four qubits [21]. This essentially means that the scheme for exhaustively classifying quantum states based on their entanglement by means of SLOCC-equivalence breaks down for four or more qubits, and a new paradigm must be found. Nevertheless, as SLOCC-equivalent quantum states can be used in the same quantum information processing tasks, it is still useful to be able to test SLOCC-equivalence between quantum states on four or more qubits.

3.5 Testing SLOCC-equivalence of specific pure states by brute force

States that are in the same SLOCC equivalence class must be capable of performing the same quantum information tasks, although in general with differing probabilities of success. Consider therefore a scenario in which we want to perform a task requiring the

pure resource state $|\psi_0\rangle$, and we are unsure as to how to obtain a copy of $|\psi_0\rangle$, but we do have a means for obtaining some different pure state $|\psi_1\rangle$. If $|\psi_0\rangle$ and $|\psi_1\rangle$ are SLOCC-equivalent, then we can perhaps use the state $|\psi_1\rangle$ that we have to perform the desired task. In such a situation, the classification of the entire set of quantum pure states into SLOCC equivalence classes is more than we require; we are merely interested in testing whether $|\psi_0\rangle$ and $|\psi_1\rangle$ specifically are interconvertible by SLOCC. Suppose (and this can always be arranged) that $|\psi_0\rangle$ and $|\psi_1\rangle$ are both defined on the same number of qubits, n. The most obvious way to try and determine SLOCC-equivalence of $|\psi_0\rangle$ and $|\psi_1\rangle$ is to attempt to solve for the SLOCC operator S connecting them. Suppose S is composed of the tensor product of single-qubit operators S_i, i.e. $S = \bigotimes_{i=0}^{n-1} S_i$, where the subscript i refers to the qubit on which S_i is acting. If the $\{S_i\}$ are complex, invertible, two-by-two matrices, then there are four complex or eight real unknown matrix elements per single-qubit operator, for a total of $8n$ real unknowns to be found. The relation

$$|\psi_1\rangle = S|\psi_0\rangle \tag{3.7}$$

leads to a system of $2n$ multivariate polynomial equations of degree n in $8n$ unknowns to be solved. For example, suppose

$$|\psi_0\rangle = \begin{bmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{02} \\ \psi_{03} \end{bmatrix}$$

$$|\psi_1\rangle = \begin{bmatrix} \psi_{10} \\ \psi_{11} \\ \psi_{12} \\ \psi_{13} \end{bmatrix}$$

$$S_0 = \begin{bmatrix} s_{000} & s_{001} \\ s_{010} & s_{011} \end{bmatrix}$$

$$S_1 = \begin{bmatrix} s_{100} & s_{101} \\ s_{110} & s_{111} \end{bmatrix}.$$

Then the system of degree-two (i.e. quadratic) multivariate polynomial equations to be solved is

$$\begin{bmatrix} \psi_{10} \\ \psi_{11} \\ \psi_{12} \\ \psi_{13} \end{bmatrix} = \begin{bmatrix} s_{000}s_{100} & s_{000}s_{101} & s_{001}s_{100} & s_{001}s_{101} \\ s_{000}s_{110} & s_{000}s_{111} & s_{001}s_{110} & s_{001}s_{111} \\ s_{010}s_{100} & s_{010}s_{101} & s_{011}s_{100} & s_{011}s_{101} \\ s_{010}s_{110} & s_{010}s_{111} & s_{011}s_{110} & s_{011}s_{111} \end{bmatrix} \begin{bmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{02} \\ \psi_{03} \end{bmatrix}. \tag{3.8}$$

In this case, there are 8 equations (considering the real and imaginary parts of the equations above separately) for 16 real unknowns, so multiple solutions may exist. This is not the case for $n \geq 6$, at which point the system becomes overdefined. At first glance it may appear that the difficulty of this problem is influenced significantly by the fact that the number of equations in the system increases exponentially in the number of qubits. However, this should not pose a significant problem as the number of unknowns

only increases linearly and therefore the size of the subportion of the system that needs to be solved also grows linearly. The real source of difficulty in the solution of this problem lies in the multivariate polynomial nature of the system of equations to be solved. In the way the problem is cast, the degree of the polynomial equations is equal to the number of qubits, i.e. grows linearly. The general problem of solving systems of multivariate polynomial equations is known to be NP-complete [22]. However, there are some indications that the solution of overdefined systems, such as the one considered here for $n \geq 6$, may be more efficiently soluble. For example, an efficient algorithm for solving 'sufficiently' overdefined systems of multivariate quadratic equations is presented in [22]. This gives us hope that our problem, which is simpler than the general problem of solving multivariate polynomial equations, may also be efficiently solved. One way to simplify the problem is to convert these multivariate polynomial equations into a different system of multivariate polynomial equations of lower degree, constituting necessary and sufficient conditions for SLOCC-equivalence. An idea for deriving necessary conditions is presented in Chapter 5, and some thoughts as to how to proceed towards a full set of necessary and sufficient conditions can be found in Chapter 6.

Chapter 4

Stabiliser States and the Walsh-Hadamard Construction

4.1 Stabiliser states

The number of coefficients needed to specify the state of a quantum system grows exponentially in the number of particles comprising the system. For example, the state vector of an n-qubit system has 2^n components. With a large enough system, this description can become very unwieldy. There is a class of states that can be described more compactly, using resources that grow linearly in the number of qubits. This is the class of *stabiliser states* [23], which can be completely specified by means of a mathematical construction called a *stabiliser* (see for example [24]). Stabilisers in turn are examples of a mathematical structure called a *group* [24, 25].

Definition 4.1.1. *A group* $\{\mathcal{G}, \diamond\}$ *is a set of elements* $\mathcal{G}$ *together with a binary operation* $\diamond$ *obeying the following four axioms:*

1. *Closure.* $g_i \diamond g_j \in \mathcal{G} \ \forall \ g_i, g_j \in \{\mathcal{G}, \diamond\}$.
2. *Existence of identity.* $\exists \ e \in \{\mathcal{G}, \diamond\}$ *such that* $g_i \diamond e = e \diamond g_i = g_i \ \forall \ g_i \in \{\mathcal{G}, \diamond\}$.
3. *Existence of inverses.* $\forall \ g_i \in \{\mathcal{G}, \diamond\}, \ \exists \ g_i^{-1} \in \{\mathcal{G}, \diamond\}$ *such that* $g_i \diamond g_i^{-1} = g_i^{-1} \diamond g_i = e$.
4. *Associativity.* $(g_i \diamond g_j) \diamond g_k = g_i \diamond (g_j \diamond g_k) \ \forall \ g_i, g_j, g_k \in \{\mathcal{G}, \diamond\}$.

A group $\{\mathcal{G}, \diamond\}$ where the cardinality of $\mathcal{G}$ is finite is called a *finite group* [24]. Some groups that are important in theoretical physics have elements described by continuously varying parameters and are known as *continuous groups* [25]. This thesis be primarily concerned with finite groups. If the operation $\diamond$ is commutative, then $\{\mathcal{G}, \diamond\}$ is called an *abelian group*. For example, the group of invertible n-by-n matrices whose elements

belong to the field $\mathbb{F}$, under matrix multiplication, called the *general linear group* and denoted $GL(n, \mathbb{F})$, is a group that is neither finite nor abelian. The real numbers of modulus 1 under multiplication, denoted $\{\{1, -1\}, \times\}$, is both finite and abelian. The group of integers under addition, $\{\mathbb{Z}, +\}$, is abelian but not finite. An important example of a finite, non-Abelian group is the *single-qubit Pauli group* $\{\mathcal{G}_1, *\}$ [23], where $*$ means matrix multiplication, which consists of the set of matrices

$$\mathcal{G}_1 = \left\{\pm I^{(2)}, \pm iI^{(2)}, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\right\} \tag{4.1}$$

where

$$I^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4.2}$$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.3}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{4.4}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.5}$$

The matrices X, Y and Z are called the *Pauli matrices.* Table 4.1 summarises some common examples of groups. For more information on basic groups, the reader is encouraged to consult [24].

For simplicity, the symbol $\diamond$ will be dropped, so that $g_i g_j$ is understood to mean $g_i \diamond g_j$. Sometimes the group $\{\mathcal{G}, \diamond\}$ will be referred to as $\mathcal{G}$. Two more ideas are necessary in order to describe the concept of a stabiliser: the *subgroup* and the *group action* [24].

Definition 4.1.2. *A set $S_\mathcal{G}$ subgroup is called a subgroup of a group $\mathcal{G}$ under the binary operation $\diamond$ if and only if:*

Group	Identity	Inverse of group element g	Finite?	Abelian?
$\{\{1,-1\},\times\}$	1	g	Yes	Yes
$\{\mathcal{G}_1,*\}$	$I^{(2)}$	Either g or $\pm ig$	Yes	No
$\{\mathbb{Z},+\}$	0	$-g$	No	Yes
$\{\mathbb{R}-0,\times\}$	1	$\frac{1}{g}$	No	Yes
$\{GL(n,\mathbb{R}),*\}$	$I^{(n)}$	g^{-1}	No	No

Table 4.1: Common examples of groups.

1. $S_{\mathcal{G}} \subseteq \mathcal{G}$.

2. $S_{\mathcal{G}}$ *is itself a group under* $\diamond$.

Definition 4.1.3. *A left group action is a binary function*

$$\mathcal{G} \star T \rightarrow T \tag{4.6}$$

between a group $\mathcal{G}$ *and a set* T *obeying the following two axioms:*

1. $(g_1 g_2) \star t = g_1 \star (g_2 \star t) \ \forall \ g_1, g_2 \in \mathcal{G}, t \in T$.

2. $e \star t = t$ *for* e *the identity element of* $\mathcal{G}$.

If a group action $\star$ *exists between* $\mathcal{G}$ *and* T*, then* $\mathcal{G}$ *is said to act on* T *on the left under* $\star$.

An analogous definition exists for a *right group action*, but it will not be needed here. For the sake of notational simplicity, the symbol $\star$ will be dropped. We are now ready to define the meaning of the term stabiliser.

Definition 4.1.4. *Consider a group* $\mathcal{G}$ *under a binary operation* $\diamond$*, that acts on a set* T *on the left under a binary operation* $\star$*. The set* $stab_{\mathcal{G}}(t)$ *defined by*

$$stab_{\mathcal{G}}(t) = \{ \ g_i \in G \mid g_i \star t = t \ for \ t \in T \ \} \tag{4.7}$$

is called the stabiliser subgroup of t *in* $\mathcal{G}$*. In this thesis, we will use the term stabiliser to mean stabiliser subgroup.*

The stabiliser of t is essentially a group of operations on t that 'fixes' t. It is easy to prove that $\text{stab}_{\mathcal{G}}(t)$ is a subgroup of $\mathcal{G}$. By definition, $\text{stab}_{\mathcal{G}}(t)$ is a subset of $\mathcal{G}$, so all that remains to be proven is that $\text{stab}_{\mathcal{G}}(t)$ is a group under the binary operation of $\mathcal{G}$ (call it $\diamond$).

Theorem 4.1.5. *Given a group $\mathcal{G}$ that acts on the left of a set T, the stabiliser $\text{stab}_{\mathcal{G}}(t)$ of $t \in T$ in $\mathcal{G}$ is a group under the same operation as $\mathcal{G}$.*

Proof. Denote $\text{stab}_{\mathcal{G}}(t)$ by S for compactness. We will check that S obeys each of the four group axioms under the group operation of $\mathcal{G}$.

1. *Closure.* Suppose $s_i, s_j \in S$. Then,

$$\begin{aligned}(s_i s_j)\, t &= s_i\,(s_j t) \text{ (axiom 1 of left group action)} \\ &= s_i t \text{ (since } s_j \text{ fixes } t) \\ &= t \text{ (since } s_i \text{ fixes } t),\end{aligned}$$

   which immediately gives $s_i s_j \in S$.

2. *Identity.* Let e be the identity element of $\mathcal{G}$. Then, $et = t$ (by axiom 2 of the left group action). Thus, $e \in S$.

3. *Inverse.* Let $g \in S, g^{-1} \in \mathcal{G}$ such that $gg^{-1} = g^{-1}g = e$ with e the identity element of $\mathcal{G}$. Then,

$$\begin{aligned}t &= et \text{ (axiom 2 of left group action)} \\ &= \left(g^{-1}g\right) t \\ &= g^{-1}\,(gt) \text{ (axiom 1 of group action)} \\ &= g^{-1}t \text{ (since } g \text{ fixes } t),\end{aligned}$$

   thereby demonstrating that $g^{-1} \in S$.

4. *Associativity.* The associativity of S follows directly from the associativity of $\mathcal{G}$.

□

In quantum information science, typically the stabilisers with which we are concerned are subsets of the *n-qubit Pauli groups* [23], which are examples of finite abelian groups, and the set on which they act is the set of state vectors in a Hilbert space. For the remainder of this thesis, any such stabiliser will be called a *Pauli stabiliser.* A detailed overview of Pauli stabilisers can be found in [23]. The properties of Pauli stabilisers that are germane to the subject of this thesis are summarised in this section.

Definition 4.1.6. *The n-qubit Pauli group $\mathcal{G}_n$ is the group consisting of all possible tensor products of operators from the single-qubit Pauli group $\mathcal{G}_1$ such that the result is an n-qubit operator.*

Definition 4.1.7. *Any stabiliser that is a subgroup of an n-qubit Pauli group shall be called a Pauli stabiliser.*

Any Pauli stabiliser is obviously a finite group, since the single-qubit Pauli group is explicitly finite and thus only a finite number of operators can be generated from this group through Kronecker products. It is also straightforward to show that Pauli stabilisers are abelian.

Theorem 4.1.8. *Any Pauli stabiliser $stab_{\mathcal{G}_n}(|\psi\rangle)$ is abelian.*

Proof. It can be checked that all elements of the single-qubit Pauli group $\mathcal{G}_1$ either commute or anticommute, i.e. $g_i g_j = \pm g_j g_i \; \forall \; g_i, g_j \in \mathcal{G}_1$. This fact immediately implies that all elements of $\mathcal{G}_n$ either commute or anticommute. Thus, in order to show that $\text{stab}_{\mathcal{G}_n}|\psi\rangle$ is abelian, all that remains is to show the impossibility of two stabiliser elements anticommuting. Two facts need to be established in order to prove this. Firstly, as can

be easily checked, all elements of the single-qubit Pauli group square to $\pm I^{(2)}$. Secondly, $-I^{(n)}$ can never be an element of any Pauli stabiliser.

Lemma 4.1.9. *$-I^{(n)} \notin stab_{\mathcal{G}_n}(|\psi\rangle)$, where $-I^{(n)}$ is the negation of the n-qubit identity matrix.*

Proof.

$$\begin{aligned} -I^{(n)}|\psi\rangle &= -\left(I^{(n)}|\psi\rangle\right) \\ &= -|\psi\rangle \end{aligned}$$

Now $|\psi\rangle \neq -|\psi\rangle$ unless all entries of $|\psi\rangle$ are zero, which is not possible since $|\psi\rangle$ must be normalisable, i.e. have non-zero norm. Thus, $-I^{(n)}$ does not fix $|\psi\rangle$. □

The above two facts immediately imply that any stabiliser element must square to the (positive) identity matrix. We now return to the main proof. Suppose $g_i g_j = -g_j g_i$ for some pair of elements $g_i, g_j \in \text{stab}_{\mathcal{G}_n}(|\psi\rangle)$. Closure ensures that $g_i g_j \in \text{stab}_{\mathcal{G}_n}(|\psi\rangle)$ and thus that $-g_j g_i = (-g_j)(g_i) \in \text{stab}_{\mathcal{G}_n}(|\psi\rangle)$, and thus that $-g_j \in \text{stab}_{\mathcal{G}_n}(|\psi\rangle)$. But, since g_j squares to the identity, we have

$$\begin{aligned} (-g_j)(g_j) &= -(g_j g_j) \\ &= -I^{(n)} \in \text{stab}_{\mathcal{G}_n}(|\psi\rangle), \end{aligned}$$

a contradiction. □

The concept of a Pauli stabiliser is best clarified through example.

Example 4.1.10. Suppose $\mathcal{G}$ is the single-qubit Pauli group $\mathcal{G}_1$ and T is the Hilbert space of a single qubit, so that t is a single-qubit pure state. Specifically, suppose t is the

state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. It can easily be verified that the matrices $I^{(2)}, X \in \mathcal{G}_1$ fix $|+\rangle$.

$$\begin{aligned} I^{(2)}|+\rangle &\equiv I^{(2)}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}\left(I^{(2)}|0\rangle + I^{(2)}|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &\equiv |+\rangle \end{aligned}$$

$$\begin{aligned} X|+\rangle &\equiv X\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}(X|0\rangle + X|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \\ &\equiv |+\rangle \end{aligned}$$

It can also easily be verified that no other element in $\mathcal{G}_1$ fixes $|+\rangle$. Thus, the stabiliser of $|+\rangle$ in $\mathcal{G}_1$ is said to be

$$\text{stab}_{\mathcal{G}_1}(|+\rangle) = \{I, X\}. \tag{4.8}$$

The stabiliser can readily be verified to be a group under operator composition (or matrix multiplication).

Example 4.1.11. Consider the two-qubit Bell state $|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We can verify that the operator $X \otimes X \in \mathcal{G}_2$ fixes $|\psi_{Bell}\rangle$.

$$\begin{aligned} (X \otimes X)(|\psi_{Bell}\rangle) &= (X \otimes X)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(X|0\rangle \otimes X|0\rangle + X|1\rangle \otimes X|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= |\psi_{Bell}\rangle \end{aligned}$$

It can be similarly verified that $Z \otimes Z$ is also a stabiliser element. Therefore, we can infer that the product of these two operators,

$$\begin{aligned}(X \otimes X)(Z \otimes Z) &= (XZ \otimes XZ) \\ &= (-iY \otimes -iY) \\ &= -(Y \otimes Y),\end{aligned}$$

is also a stabiliser element. Similarly, the product of any of these operators with itself, $I^{(2)} \otimes I^{(2)} \equiv I^{(4)}$, is also a stabiliser element. No other elements of $\mathcal{G}_2$ fix $|\psi_{Bell}\rangle$, so the full Pauli stabiliser is given by

$$\text{stab}_{\mathcal{G}_2}(|\psi_{Bell}\rangle) = \left\{I^{(4)}, X \otimes X, Z \otimes Z, -Y \otimes Y\right\}. \tag{4.9}$$

In the above examples, the states $|+\rangle$ and $|\psi_{Bell}\rangle$ are completely specified by their Pauli stabilisers, which contain 2^1 and 2^2 elements respectively. Saying that a state is stabilised or fixed by some operator is equivalent to saying that it is an eigenvector of this operator with eigenvalue 1. Since $|+\rangle$ is the unique eigenvector of X with eigenvalue 1, saying that X stabilises a state $|\psi\rangle$ completely specifies that state (up to an overall phase); in this case, $|\psi\rangle$ is the state $|+\rangle$. Similarly, it can be verified that $|\psi_{Bell}\rangle$ is the unique simultaneous eigenvector of $X \otimes X$ and $Z \otimes Z$ with eigenvalue 1. In general, any n independent elements of a Pauli stabiliser will completely specify a single n-qubit quantum state that is fixed by all of them. Such a set of elements are referred to as the *generators* of the Pauli stabiliser. Since each of the generators square to the identity and commute with each other, the total number of operators that can be produced by multiplying the generators together is 2^n. This will be the minimal size of any group that completely specifies the state. Thus, a Pauli stabiliser with n generators and 2^n elements completely specifies a single n-qubit state, which is known as a *stabiliser state.*

Definition 4.1.12. *Any pure n-qubit quantum state that is completely specified by a Pauli stabiliser with n generators and 2^n elements is called a stabiliser state.*

Thus, this special class of n-qubit quantum states can be completely specified by the n generators of its Pauli stabiliser, rather than the 2^n complex coefficients in its vector representation. The representation of stabiliser states in terms of their Pauli stabilisers rather than their vector coefficients is thus convenient and efficient. Although Pauli stabilisers are typically used in quantum information science in the context of a class of quantum error correcting codes known as *stabiliser codes* [23], for the purposes of this thesis they are merely used as a tool for compactly describing a class of quantum states.

4.2 Graph states

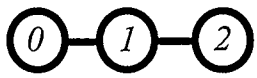
Within the class of stabiliser states lies a subclass of states that can be described in terms of mathematical *graphs* [26]. These states are called *graph states* (a thorough review of which can be found in [27]), and it has been shown that every stabiliser state is equivalent to a graph state under local unitary transformations (see, for example, [28]). A graph $G = (V, E)$ is a set of vertices V together with a set of edges E that connect pairs of vertices. If two vertices are labelled $i, j \in V$, then an edge from i to j is represented by the pair (i, j). Graph states always correspond to *simple* graphs, those having at most one edge between any pair of vertices and no edges connecting vertices to themselves. Such graphs can be described by means of an *adjacency matrix*, defined below.

Definition 4.2.1. *An adjacency matrix A for a simple graph G with n vertices labelled $i \in V$ with $V = \{0, 1, \ldots, n-1\}$ and a set of edges E is an n-by-n matrix whose elements $A_{i,j}$ are equal to 1 if there is an edge between vertices i and j and 0 otherwise.*

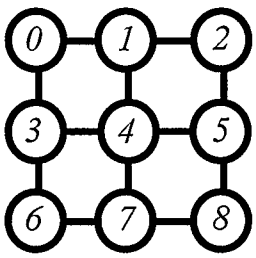
The set of vertices connected to a vertex i by edges is called the *neighbourhood* of i and denoted $\mathrm{ngbh}(i)$.

Some depictions of simple graphs are shown in Figure 4.1. Graph states can now be defined in a constructive way using these concepts.

(a) Three-vertex graph (not fully connected).



(b) Three-vertex linear graph.



(c) Three-by-three connected two-dimensional graph.

Figure 4.1: Some examples of simple, undirected, unweighted graphs. Open circles represent vertices and solid lines edges. The numbers inside the circles label the vertices. Element (i, j) of the adjacency matrix will be 0 if there is no edge between vertices i and j and 1 if there is an edge. The graph in Figure 4.1(a) defines a graph state in which one of the qubits is unentangled with the rest, as the vertex representing this qubit is not connected to any others. The graph in Figure 4.1(b) is the underlying graph for the so-called three-qubit cluster state, and the one in Figure 4.1(c) for the three-by-three cluster state.

Definition 4.2.2. *A graph state $|g\rangle$ is a stabiliser state whose Pauli stabiliser is specified by a simple graph G using the following process:*

1. *Associate each vertex of G with a qubit.*
2. *For each vertex i, construct the operator $g_i = X_i \bigotimes_{j \in ngbh(i)} Z_j$, where X_k refers to single-qubit operator X acting on qubit k and Z_k to single-qubit operator Z acting on qubit k. The group S generated by the operators $\{g_i, i \in \{0, 1, \ldots, n-1\}\}$ is the Pauli stabiliser for $|g\rangle$.*

The above definition was given in [27]. Graph states have a number of applications in quantum information, and it is thus useful to have a thorough understanding of them.

Example 4.2.3. *Two-qubit cluster state.* Consider the two-qubit cluster state $|g\rangle$ whose underlying graph is the two-vertex graph with a single undirected edge connecting them (the two-vertex analogue of the middle example of Figure 4.1). The adjacency matrix of this graph is given by

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{4.10}$$

The process outlined above for constructing the generators of the Pauli stabiliser for this graph state is equivalent to putting a Pauli X in position i for row i of A, and a Pauli Z for every position in row i where the entry is a 1. Thus, the generators are given as follows.

$$\text{Row 1: } \begin{bmatrix} 0 & 1 \end{bmatrix} \rightarrow X_0 \otimes Z_1 \tag{4.11}$$

$$\text{Row 2: } \begin{bmatrix} 0 & 1 \end{bmatrix} \rightarrow Z_0 \otimes X_1 \tag{4.12}$$

The last two elements of the Pauli stabiliser are found by constructing products of the generators. The full stabiliser is given by

$$\text{stab}_{g_2}(|g\rangle) = \left\{ I^{(4)}, X_0 \otimes Z_1, Z_0 \otimes X_1, Y_0 \otimes Y_1 \right\}. \tag{4.13}$$

As a demonstration that the generators completely specify the graph state, we can find the state vector for the graph state based solely on the generators. Let the expression of the state vector for $|g\rangle$ in the computational basis be

$$|g\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle. \tag{4.14}$$

Since the generators fix the graph state, we have two equations to solve for the unknown coefficients:

$$|g\rangle = (X_0 \otimes Z_1)\,|g\rangle.$$

Expanding the above expression in the computational basis yields

$$\begin{aligned} a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle &= (X_0 \otimes Z_1)\,(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle) \\ &= a_0|10\rangle - a_1|11\rangle + a_2|00\rangle - a_3|01\rangle. \end{aligned}$$

Comparing coefficients on the left- and right-hand sides of the previous expression gives

$$a_0 = a_2 \tag{4.15}$$

$$a_1 = -a_3. \tag{4.16}$$

Next, consider

$$|g\rangle = (Z_0 \otimes X_1)\,|g\rangle. \tag{4.17}$$

This implies that

$$\begin{aligned} a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle &= (Z_0 \otimes X_1)\,(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle) \\ &= a_0|01\rangle + a_1|00\rangle - a_2|11\rangle - a_3|10\rangle. \end{aligned}$$

We immediately obtain from here the conditions

$$a_0 = a_1 \tag{4.18}$$

$$a_2 = -a_3. \tag{4.19}$$

From equations (4.15), (4.16), (4.18) and (4.19), it is necessary that

$$a_0 = a_1 = a_2 = -a_3. \tag{4.20}$$

Imposing the condition that $|g\rangle$ be normalised immediately sets $a_0 = 1/2$ and thus, the state vector can be written as

$$|g\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right). \tag{4.21}$$

The method in the above example for solving for the state vector of an n-qubit graph state $|g\rangle$ corresponding to a graph G with adjacency matrix A can always be carried out for an arbitrary graph state, giving us an analytical expression for the state vector purely in terms of the adjacency matrix and the number of qubits. Introducing the notation $|i\rangle = \bigotimes_{j=0}^{n-1} |i_j\rangle$ for computational basis vectors, where $i_j \in \{0, 1\}$ is the jth digit in the binary representation of i, we can write

$$|g\rangle = \frac{1}{2^{n/2}} \sum_{i=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2} \sum_{k=j+1}^{n-1} A_{jk} i_j i_k} |i\rangle. \tag{4.22}$$

4.3 Constructing generalised stabilisers from density matrices of pure states

A simple method of constructing a generalised stabiliser for a n-qubit pure state $|\psi\rangle$, one whose elements are not necessarily from the n-qubit Pauli group $\mathcal{G}_n$, was shown in [29]. Consider the density matrix of the state, $\rho = |\psi\rangle\langle\psi|$. Since ρ is a pure-state density matrix, it will have eigenvalues 1 (non-degenerate) and 0 ($(2^n - 1)$-fold degenerate). It is easy to see that the unique eigenvector corresponding to eigenvalue 1 is the state $|\psi\rangle$ itself:

$$\begin{aligned} \rho|\psi\rangle &= |\psi\rangle\langle\psi|\psi\rangle \\ &= |\psi\rangle, \end{aligned}$$

where it has been assumed that $|\psi\rangle$ is normalised. Since ρ is Hermitian, any vector orthogonal to $|\psi\rangle$ is thus an eigenvector of ρ with eigenvalue 0, and since this eigenvalue is $(2^n - 1)$-fold degenerate, it is possible to find a basis of $2^n - 1$ linearly independent eigenvectors spanning the eigenspace of ρ corresponding to eigenvalue 0. Suppose we use an orthonormal basis $\{\ |v_i\rangle\ \mid i \in \{0, 1, \ldots, 2^n - 1\}\ \}$ obeying the eigenvalue relations

$$\rho|v_i\rangle = \delta_{i,0}|v_i\rangle, \tag{4.23}$$

implying that $|v_0\rangle = |\psi\rangle$. Then we can construct a set of orthonormal projectors $\{f_i\}$ defined by

$$f_i = |v_i\rangle\langle v_i|. \tag{4.24}$$

Since the $|v_i\rangle$ are orthonormal, we have $\langle v_i|v_j\rangle = \delta_{i,j}$ and thus

$$\begin{aligned} f_i|\psi\rangle &= |v_i\rangle\langle v_i|v_0\rangle \\ &= \delta_{i,0}|v_i\rangle. \end{aligned}$$

We can thus see that any operator of the form

$$s_i = f_0 + \sum_{j=1}^{2^n-1} a_{ij} f_j \text{ with } a_{ij} \in \mathbb{R} \text{ for all } i, j \tag{4.25}$$

has $|\psi\rangle$ as an eigenvector with eigenvalue 1, and is thus an element of some general stabiliser of $|\psi\rangle$. Evidently there are an infinite number of such operators. Thus, the remaining task is to choose appropriate values for the a_{ij} with $i, j \in \{0, 1, \ldots, 2^n - 1\}$ such that the 2^n operators s_i form a group. A suitable choice is the matrix elements of the so-called *Walsh-Hadamard transform matrix* [30, 29], defined below.

Definition 4.3.1. *The single-qubit Walsh-Hadamard transform matrix (WHT) is the matrix*

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{4.26}$$

The n-qubit WHT is the matrix

$$\begin{aligned} W_n &= \bigotimes_{i=0}^{n-1} W_1 \\ &\equiv W_1^{\otimes n}. \end{aligned} \tag{4.27}$$

The following lemma gives a convenient way to express the matrix elements of W_n.

Lemma 4.3.2. *The (i,j) matrix element of the n-qubit WHT can be written as*

$$(W_n)_{ij} = (-1)^{\sum_{k=0}^{n-1} i_k j_k} \tag{4.28}$$

where i_k is the kth bit from the left in the n-bit binary representation of i (padded with 0s on the left as necessary).

Proof. The proof proceeds by means of induction. Consider the case $n = 1$. We have

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{4.29}$$

We explicitly see that

$$\begin{aligned} (W_1)_{00} &= 1 = (-1)^{0 \cdot 0} \\ (W_1)_{01} &= 1 = (-1)^{0 \cdot 1} \\ (W_1)_{10} &= 1 = (-1)^{1 \cdot 0} \\ (W_1)_{11} &= -1 = (-1)^{1 \cdot 1} \end{aligned}$$

Now suppose the claim is true for W_t, i.e.

$$(W_t)_{rs} = (-1)^{\sum_{k=0}^{t-1} r_k s_k}, \tag{4.30}$$

and consider the case of W_{t+1}. We can express W_{t+1} in block form as

$$\begin{aligned} W_{t+1} &= W_1 \otimes W_t \\ &= \begin{bmatrix} (W_1)_{00} W_t & (W_1)_{01} W_t \\ (W_1)_{10} W_t & (W_1)_{11} W_t \end{bmatrix} \end{aligned} \tag{4.31}$$

Label the block $(W_1)_{ab} W_t$ as block ab. Clearly, each element $(W_{t+1})_{rs}$ falls into one of the four blocks. The value of each matrix element is determined by the block in which it is contained and the relative position of that matrix element within its block. Each of these quantities can be determined from the indices r and s. Specifically, for identifying the block, we have

$r \geq 2^t$?	$s \geq 2^t$?	Block containing $(W_{t+1})_{rs}$
No	No	Block 00
No	Yes	Block 01
Yes	No	Block 10
Yes	Yes	Block 11

In other words, if r and s are expressed as $(t+1)$-bit strings, then a and b correspond to the first bit of r and s respectively. The indices describing the relative position of the matrix element within block ab are $r - 2^t \cdot a$ and $s - 2^t \cdot b$ (i.e. the last t bits of the $(t+1)$-bit representations of r and s. The matrix element of W_{t+1} is then determined from this fact, together with equations (4.30) and (4.31), to be

$$\begin{aligned} (W_{t+1})_{rs} &= (W_1)_{ab} \cdot (W_t)_{r-a\cdot 2^t, s-b\cdot 2^t} \\ &= (-1)^{a\cdot b} \cdot (-1)^{\sum_{k=0}^{t-1} (r-a\cdot 2^t)_k (s-b\cdot 2^t)_k} \\ &= (-1)^{a\cdot b + \sum_{k=0}^{t-1} (r-a\cdot 2^t)_k (s-b\cdot 2^t)_k} \end{aligned} \tag{4.32}$$

The first term in the exponent in equation (4.32) corresponds to the product of the first bit in r with the first bit in s. The second term in the exponent above is the sum of the bitwise products of the last t out of the $t+1$ bits in r with the corresponding bits in s.

We can thus combine the two terms under one summation over all $(t+1)$ digits of r and s,

$$(W_{t+1})_{rs} = (-1)^{\sum_{k=0}^{t} r_k s_k}, \tag{4.33}$$

thus completing the proof. □

The WHT can be used to give a constructive method for finding a stabiliser (in the general sense, not the quantum information sense of a Pauli stabiliser in particular). Any particular n-qubit quantum pure state will have an infinite number of general stabilisers whose elements belong to $\mathrm{SU}(2^n)$, the group of 2^n-by-2^n unitary operators. In the case of a stabiliser state in particular, one of these general stabilisers will be in the form of a Pauli stabiliser, whose elements are separable and composed of Pauli operators, belonging to the set $\mathrm{SU}(2)^{\otimes n}$. First, we will review the constructive method of finding a general stabiliser for a general quantum pure state, given in reference [29]. Then, in the special case of a stabiliser state, we will show how to construct the unique Pauli stabiliser for this state, a new result.

Theorem 4.3.3. *Suppose an n-qubit pure state $|\psi\rangle$ has density matrix $\rho = |\psi\rangle\langle\psi|$ with orthonormal eigenvectors $\{|v_i\rangle\}$ corresponding to eigenvalues $\delta_{i,0}$ such that*

$$s_i = \sum_{j=0}^{2^n-1} a_{ij} f_j \tag{4.34}$$

where $i, j \in \{0, 1, \ldots, 2^n - 1\}$ and $f_j = |v_j\rangle\langle v_j|$. Then, the set $\{s_i\}$ of cardinality 2^n defined by

$$a_{ij} = (W_n)_{ij}, \tag{4.35}$$

i.e. a_{ij} is the (i,j) matrix element of the n-qubit WHT, is a general stabiliser for $|\psi\rangle$.

Proof. The following facts must be established in order to complete the proof:

1. Each operator s_i fixes $|\psi\rangle$.
2. The $\{s_i\}$ form a group of order 2^n under composition or, equivalently, matrix multiplication.

First, note that

$$\begin{aligned} a_{i0} &= (-1)^{\sum_{k=0}^{n-1} i_k \cdot 0_k} \\ &= (-1)^{\sum_{k=0}^{n-1} i_k \cdot 0} \\ &= (-1)^{\sum_{k=0}^{n-1} 0} \\ &= 1. \end{aligned}$$

Thus, all of the s_i are in the form of the operators in equation (4.25), meaning that they all fix $|\psi\rangle$. Similarly, it can be proven that $a_{0i} = 1$ for all i. Now, we prove that the s_i form a group of order 2^n. Since W_n has 2^n rows, the cardinality of the set $\{s_i\}$ is clearly 2^n. Thus, we just need to check that the four group axioms are obeyed. First, we demonstrate closure, i.e. that $s_i s_j = s_k$ for $i, j, k \in \{0, 1, \ldots, 2^n - 1\}$:

$$\begin{aligned} s_i s_j &= \left(\sum_{k=0}^{2^n-1} a_{ik} f_k \right) \left(\sum_{l=0}^{2^n-1} a_{jl} f_l \right) \\ &= \sum_{k=0}^{2^n-1} \sum_{l=0}^{2^n-1} a_{ik} a_{jl} f_k f_l \\ &= \sum_{k=0}^{2^n-1} \sum_{l=0}^{2^n-1} (-1)^{\sum_{r=0}^{n-1} i_r k_r} (-1)^{\sum_{s=0}^{n-1} j_s l_s} |v_k\rangle \text{ (from Equation (4.28))} \\ &= \langle v_k | v_l \rangle \langle v_l | \\ &= \sum_{k=0}^{2^n-1} \sum_{l=0}^{2^n-1} (-1)^{\sum_{r=0}^{n-1} (i_r k_r + j_r l_r)} \delta_{kl} |v_k\rangle \langle v_l| \\ &= \sum_{k=0}^{2^n-1} (-1)^{\sum_{r=0}^{n-1} (i_r + j_r) k_r} |v_k\rangle \langle v_k|. \end{aligned}$$

Since the value of $(-1)^p$ depends only on whether p is odd or even, we can do all of the arithmetic in the exponent of the summand above modulo 2. Denoting bitwise addition

modulo 2 by the symbol $\oplus$, we have

$$\begin{aligned} s_i s_j &= \sum_{k=0}^{2^n-1} (-1)^{\sum_{r=0}^{n-1}(i_r \oplus j_r)k_r} |v_k\rangle\langle v_k| \\ &= \sum_{k=0}^{2^n-1} a_{(i\oplus j)k} f_k \\ &= s_{i\oplus j}, \end{aligned}$$

thus indicating closure. Next we show that s_0 is the n-qubit identity matrix:

$$\begin{aligned} s_0 &= \sum_{j=0}^{2^n-1} a_{0j} f_j \\ &= \sum_{j=0}^{2^n-1} f_j \\ &= \sum_{j=0}^{2^n-1} |v_j\rangle\langle v_j| \\ &= I^{(2^n)}, \end{aligned}$$

where the last step is due to the completeness property of the eigenvectors of Hermitian operators. Therefore, the set contains the identity element. It is trivial to show that each element is its own inverse:

$$\begin{aligned} s_i s_i &= s_{i\oplus i} \\ &= s_0. \end{aligned}$$

The operation under which the elements are combined is matrix multiplication, which is known to be associative, and the proof is complete. □

As an illustration of the use of the above theorem, we will once again turn to the Bell state and explicitly construct a stabiliser for it.

Example 4.3.4. Consider the Bell state

$$\begin{aligned} |\psi_{Bell}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \end{aligned}$$

We have $|v_0\rangle = |\psi_{Bell}\rangle$, and we choose the other $|v_i\rangle$ such that all of the vectors are mutually orthonormal. There are an infinite number of such choices available, so pick, for example,

$$|v_0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \quad |v_1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |v_2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |v_3\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}. \tag{4.36}$$

From this choice, we obtain

$$f_0 = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \tag{4.37}$$

$$f_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.38}$$

$$f_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.39}$$

$$f_3 = \begin{bmatrix} \frac{1}{2} & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}. \tag{4.40}$$

The two-qubit WHT whose rows tell us how to combine the f_is is given by

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \tag{4.41}$$

which in turn leads to the stabiliser elements

$$\begin{aligned} s_0 &= f_0 + f_1 + f_2 + f_3 \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{aligned} \tag{4.42}$$

$$\begin{aligned} s_1 &= f_0 - f_1 + f_2 - f_3 \\ &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \end{aligned} \tag{4.43}$$

$$
\begin{aligned}
s_2 &= f_0 + f_1 - f_2 - f_3 \\
&= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}
\end{aligned} \tag{4.44}
$$

$$
\begin{aligned}
s_3 &= f_0 - f_1 - f_2 + f_3 \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}
\end{aligned} \tag{4.45}
$$

These four matrices do indeed stabilise $|\psi_{Bell}\rangle$, but they (specifically s_1 and s_2) are not separable. Thus, the stabiliser we have obtained here is not the same as the one from Example 4.1.11. Because of the freedom we have in choosing $|v_1\rangle$ and $|v_2\rangle$, the stabiliser yielded by this constructive method is not unique.

In the case where $|\psi\rangle$ is a stabiliser state it is in fact possible to determine systematically the basis of eigenvectors of $\rho = |\psi\rangle\langle\psi|$ that is required to give rise to the separable (Pauli) stabiliser for $|\psi\rangle$. This subject will be addressed in Theorem 5.3.3 of Chapter 5, in which the new contributions presented in this thesis are discussed.

Chapter 5

Necessary Conditions for SLOCC-Equivalence Between Graph States and Arbitrary Quantum Pure States

5.1 Introduction

Since the types of tasks that can be accomplished with different kinds of quantum states vary depending upon the SLOCC class to which these states belong, it would be beneficial to have a systematic scheme for SLOCC-classification of quantum pure states. On two qubits, it is known that all pure states are SLOCC-equivalent [18]. On three qubits there are precisely two inequivalent classes exhibiting true tripartite ex, represented by the GHZ-state and the W-state [16]. Unfortunately, the classification based on SLOCC-equivalence breaks down for four-qubit states, as it was shown by Wallach in 2005 that there are an infinite number of SLOCC-equivalence classes on four qubits [21]. Nevertheless, since quantum pure states that are SLOCC-equivalent to each other are capable of performing the same kinds of quantum information processing tasks, it is still an interesting challenge to determine SLOCC-equivalence of quantum pure states on four or more qubits. Since it is known that stabiliser states are useful for a number of such tasks, for example quantum error correction [23] and measurement-based quantum computing [31], it would behoove us to find a means of testing SLOCC-convertibility between arbitrary quantum pure states and stabiliser states. The primary focus of this thesis is to elucidate some ideas with regards to accomplishing the task of determining SLOCC-equivalence between stabiliser states and arbitrary quantum pure states, for which there is no known efficient means in general. The specific question that we are interested in answering can be stated as follows: given an n-qubit pure state $|\psi\rangle$ and an n-qubit graph state $|g\rangle$, does

there exist an n-qubit SLOCC operator S such that $|\psi\rangle = S|g\rangle$? It is inefficient in general to attempt to solve for S explicitly. An alternative approach, the one embraced by this thesis, is to construct a set of easily evaluated conditions on $|\psi\rangle$ that are necessary and sufficient for SLOCC-equivalence between $|\psi\rangle$ and $|g\rangle$. In this chapter, a set of necessary conditions for the SLOCC-equivalence of an arbitrary quantum pure state to a graph state will be provided. Some ideas regarding how to find a set of sufficient conditions will be discussed in Chapter 6. The remainder of this chapter comprises my original research contributions.

5.2 SLOCC-transformed stabilisers

The principal idea that was investigated in the hope of finding a means of checking for interconvertibility between stabiliser states and arbitrary quantum pure states is the fact that SLOCC-transformed stabiliser states have separable (in general non-Pauli) stabilisers themselves. This is demonstrated demonstrated by Lemmas 5.2.1 and 5.2.2 below.

Lemma 5.2.1. *Suppose that an n-qubit pure state $|\tilde{s}\rangle$ is SLOCC-connected to a stabiliser state $|s\rangle$, i.e.*

$$|\tilde{s}\rangle = \bigotimes_{i=0}^{n-1} S_i |s\rangle. \tag{5.1}$$

for some set of invertible single-qubit operators S_i. If σ_i is an element of the Pauli stabiliser for $|s\rangle$, i.e.

$$\begin{aligned} \sigma_i|s\rangle &= \bigotimes_{j=0}^{n-1} \sigma_{ij}|s\rangle \\ &= |s\rangle \end{aligned}$$

where the σ_{ij} are single-qubit Pauli group operators, then the operator

$$\tilde{\sigma}_i = \bigotimes_{j=0}^{n-1} S_j \sigma_{ij} S_j^{-1} \tag{5.2}$$

is a separable, generally non-Pauli operator that fixes $|\tilde{s}\rangle$.

Proof. It is self-evident from the form of equation (5.2) that $\tilde{\sigma}_i$ is separable. For convenience, let $S = \bigotimes_{i=0}^{n-1} S_i$. Then

$$\begin{aligned} \tilde{\sigma}_i|\tilde{s}\rangle &= \left(S\sigma_{ij}S^{-1}\right)\left(S|s\rangle\right) \\ &= S\sigma_{ij}|s\rangle \\ &= S|s\rangle \\ &= |\tilde{s}\rangle. \end{aligned}$$

□

Lemma 5.2.2. *The set of operators* $\tilde{\Sigma} = \{\tilde{\sigma}_i\}$ *whose elements are defined in equation (5.2) is a group of order* 2^n.

Proof. As usual, we check the four group axioms one at a time.

1. *Closure.*

$$\begin{aligned} \tilde{\sigma}_i\tilde{\sigma}_j &= \left(S\sigma_iS^{-1}\right)\left(S\sigma_jS^{-1}\right) \\ &= S\sigma_i\sigma_jS^{-1} \\ &= S\sigma_{i\oplus j}S^{-1} \\ &= \tilde{\sigma}_{i\oplus j}. \end{aligned}$$

2. *Identity.*

$$\begin{aligned} \tilde{\sigma}_0 &= S\sigma_0S^{-1} \\ &= SI^{(n)}S^{-1} \\ &= SS^{-1} \\ &= I^{(n)}. \end{aligned}$$

3. *Inverse.* Every element of $\{\tilde{\sigma}_i\}$ is its own inverse:

$$\begin{aligned}
\tilde{\sigma}_i\tilde{\sigma}_i &= \bigotimes_{j=0}^{n-1} S_j\sigma_{ij}S_j^{-1} \bigotimes_{k=0}^{n-1} S_k\sigma_{ik}S_k^{-1} \\
&= \bigotimes_{j=0}^{n-1} S_j\sigma_{ij}S_j^{-1}S_j\sigma_{ij}S_j^{-1} \\
&= \bigotimes_{j=0}^{n-1} S_j\sigma_{ij}\sigma_{ij}S_j^{-1} \\
&= \bigotimes_{j=0}^{n-1} S_jS_j^{-1} \\
&= \bigotimes_{j=0}^{n-1} I_j^{(2)} \qquad (5.3) \\
&= I^{(n)}. \qquad (5.4)
\end{aligned}$$

4. *Associativity.* As usual, this property follows directly from the associativity of matrix multiplication.

□

We will refer to the group consisting of the transformed stabiliser elements as a *SLOCC-transformed Pauli stabiliser*, and define some notation for it.

Definition 5.2.3. *Suppose G is a group of n-qubit Pauli operators and S is an n-qubit SLOCC operator. Then the symbol $\tilde{G}^{(S)}$ denotes the group that results from transforming G by S, or more specifically,*

$$\begin{aligned}
\tilde{G}^{(S)} &= SGS^{-1} \\
&= \left\{ Sg_iS^{-1} \mid g_i \in G \right\}.
\end{aligned}$$

$\tilde{G}^{(S)}$ shall be called a SLOCC-transformed Pauli stabiliser, and its elements will be denoted $\tilde{g}_i^{(S)} \equiv Sg_iS^{-1}$.

For notational convenience, the superscript (S) will be dropped whenever there is no possibility for confusion, so the group transformed by S will be written merely as $\tilde{G}$, and the elements of the group as $\tilde{g}$. As an example of the above notation, the single-qubit Pauli group transformed by the SLOCC operator S shall be denoted either as $\tilde{\mathcal{G}}_1{}^{(S)}$ or simply as $\tilde{\mathcal{G}}_1$. Note well from the proof of the existence of inverses that each local operator that occurs in any element of the stabiliser $\tilde{\Sigma}$ from Lemma 5.2.2 squares to the identity, Equation (5.3). This property is useful, because any element of $GL(2,\mathbb{C})$ that squares to the identity and is not itself a multiple of the identity has only two free complex parameters, rather than the usual four, thereby halving the number of unknowns appearing in the system of equations (3.7). First, we show how to write any matrix from $\tilde{\Sigma}$ in terms of three unknowns.

Lemma 5.2.4. *A matrix $M \in GL(2,\mathbb{C})$ obeying $M^2 = I^{(2)}$ either also obeys $M = \pm I^{(2)}$ or can be written as*

$$M = \pm \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix} \tag{5.5}$$

where $u, v \in \mathbb{C}$.

Proof. Let

$$M = \begin{bmatrix} t & u \\ v & w \end{bmatrix} \tag{5.6}$$

with $t, u, v, w \in \mathbb{C}$. Then,

$$\begin{aligned} M^2 &= \begin{bmatrix} t & u \\ v & w \end{bmatrix} \begin{bmatrix} t & u \\ v & w \end{bmatrix} \\ &= \begin{bmatrix} t^2+uv & u(t+w) \\ v(t+w) & w^2+uv \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{5.7}$$

Equation (5.7) admits two cases.

$$\text{CASE I: } t+w \neq 0.$$

In this case we find that

$$\begin{aligned} u &= v = 0 \\ \text{and thus that} t^2 &= w^2 = 1. \\ \text{But, } t &\neq -w, \text{ so} \\ t &= w = \pm 1 \text{ and thus,} \\ M &= \pm I^{(2)}. \end{aligned}$$

All matrices corresponding to this case have determinant 1.

$$\text{CASE II: } t+w = 0.$$

In this case,

$$t = -w = \pm\sqrt{1-uv} \text{ and thus,}$$

$$M = \pm \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix}.$$

All matrices falling into this category have determinant -1. □

All elements of $\tilde{\Sigma}$ that have determinant -1 and square to the identity fall under case II in Lemma 5.2.4. Thus, they have three unknowns: u, v and the overall sign. However, the overall sign can be fixed to be positive.

Lemma 5.2.5. *Any operator* $\tilde{\sigma} = S\sigma S^{-1}$, *where* $S \in GL(2,\mathbb{C})$ *and* $\sigma \in \mathcal{G}_1$, $det(\sigma) = -1$, *can be written as*

$$\tilde{\sigma} = \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix}, \tag{5.8}$$

where $u, v \in \mathbb{C}$.

Proof. From case II of Lemma 5.2.4, we know that

$$\tilde{\sigma} = \pm \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix},$$

where $u, v \in \mathbb{C}$. Suppose that

$$\tilde{\sigma} = - \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix}.$$

Then

$$\begin{aligned} -\tilde{\sigma} &= \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix} \\ &= -S\sigma S^{-1} \\ &= S\left(-\sigma\right)S^{-1}. \end{aligned} \tag{5.9}$$

Now, note the following relations:

$$\begin{aligned} -X &= YXY \\ -Y &= HYH \\ -Z &= XZX. \end{aligned}$$

Thus, for any single-qubit Pauli operator σ that is not proportional to the identity element, there is a matrix $T \in GL(2, \mathbb{C})$ such that

$$-\sigma = T\sigma T^{-1}. \tag{5.10}$$

Putting (5.10) into (5.9) yields

$$\begin{aligned} \begin{bmatrix} \sqrt{1-uv} & u \\ v & -\sqrt{1-uv} \end{bmatrix} &= ST\sigma T^{-1}S^{-1} \\ &= (ST)\,\sigma\,(ST)^{-1} \\ &= S'\sigma\left(S'\right)^{-1}, \end{aligned}$$

where $S' = ST \in GL(2, \mathbb{C})$. In other words, the positive sign in Equation (5.5) can always be chosen. □

If a separable stabiliser composed of local operators that square to the identity exists for some given pure state $|\psi\rangle$, the state $|\psi\rangle$ is SLOCC-equivalent to a stabiliser state. Recall that it is possible to construct stabilisers of a pure state $|\psi\rangle$ as described in Section 4.3, and that the stabiliser obtained is not necessarily separable. It turns out to be true that if $|\psi\rangle$ is a stabiliser state, there is always a choice of orthonormal eigenbasis for $\rho = |\psi\rangle\langle\psi|$ such that the constructed stabiliser is separable. This will be demonstrated in the next section.

5.3 Constructing separable stabilisers for graph states

Since all stabiliser states are local-unitarily equivalent to graph states, the problem of constructing separable stabilisers for stabiliser states can be reduced to the consideration of graph states. Suppose an n-qubit graph state $|g\rangle$ is provided. The key to constructing the separable stabiliser for this state is in the selection of the particular orthonormal eigenbasis for $|\rho\rangle = |g\rangle\langle g|$ that accomplishes this. Fortunately, the correct choice of basis can be obtained straightforwardly by means of local Pauli Z operations on the original graph state. The specific basis is given in Lemma 5.3.1 and Corollary 5.3.2, and then the correctness of this choice of basis is demonstrated in Theorem 5.3.3.

Lemma 5.3.1. *Suppose a (normalised) n-qubit graph state $|g\rangle$ is provided. The vectors in the set $\{|v_i\rangle\}$ of cardinality 2^n, defined by*

$$|v_i\rangle = \left(\bigotimes_{j=0}^{n-1} Z_j^{i_j}\right)|g\rangle, \tag{5.11}$$

are an orthonormal set of vectors, where Z_j is the Pauli-Z matrix operating on qubit j and i_j is the jth bit in the n-bit binary expression for the index i obeying $0 \leq i < 2^n - 1$.

Proof. Consider the inner product $\langle v_i|v_j\rangle$. We can use the binary form of $|g\rangle$ from Equation 4.22 to write

$$\begin{aligned} |v_i\rangle &= \left(\bigotimes_{k=0}^{n-1} Z_k^{i_k}\right) \frac{1}{2^{n/2}} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk} l_j l_k} |l\rangle \\ &= \frac{1}{2^{n/2}} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk} l_j l_k} \left(\bigotimes_{k=0}^{n-1} Z_k^{i_k}\right) |l\rangle \end{aligned} \tag{5.12}$$

Z_k acts if and only if $i_k = 1$. If it does act, then it has no effect if qubit k is in state $|0\rangle$, i.e. $l_k = 0$, and it introduces a factor of -1 if qubit k is in state $|1\rangle$, i.e. $l_k = 1$. Thus, for the four possible combinations of i_k and l_k, there is a factor of -1 introduced for every k such that $i_k = l_k = 1$. This can be expressed mathematically as

$$\begin{aligned} \left(\bigotimes_{k=0}^{n-1} Z_k^{i_k}\right) |l\rangle &= \left(\bigotimes_{k=0}^{n-1} Z_k^{i_k} |l_k\rangle\right) \\ &= \left(\bigotimes_{k=0}^{n-1} (-1)^{i_k l_k} |l_k\rangle\right) \\ &= (-1)^{\sum_{k=0}^{n-1} i_k l_k} |l\rangle. \end{aligned} \tag{5.13}$$

Substituting Equation (5.13) into Equation (5.12), we get

$$|v_i\rangle = \frac{1}{2^{n/2}} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk} l_j l_k} (-1)^{\sum_{q=0}^{n-1} i_q l_q} |l\rangle \tag{5.14}$$

The inner product of two of these vectors is thus given by

$$\begin{aligned} \langle v_i|v_j\rangle &= \left(\frac{1}{2^{n/2}} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk} l_j l_k} (-1)^{\sum_{q=0}^{n-1} i_q l_q} \langle l|\right) \\ &\times \left(\frac{1}{2^{n/2}} \sum_{m=0}^{2^{n-1}} (-1)^{\sum_{r=0}^{n-2}\sum_{s=l+1}^{n-1} A_{rs} m_r m_s} (-1)^{\sum_{p=0}^{n-1} j_p m_p} |m\rangle\right) \\ &= \frac{1}{2^n} \sum_{l=0}^{2^{n-1}} \sum_{m=0}^{2^{n-1}} (-1)^{\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk}(l_j l_k + m_j m_k)} (-1)^{\sum_{q=0}^{n-1}(i_q l_q + j_q m_q)} \delta_{lm} \\ &= \frac{1}{2^n} \sum_{l=0}^{2^{n-1}} (-1)^{2\sum_{j=0}^{n-2}\sum_{k=l+1}^{n-1} A_{jk} l_j l_k} (-1)^{\sum_{q=0}^{n-1}(i_q \oplus j_q) l_q} \\ &= \frac{1}{2^n} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{q=0}^{n-1}(i_q \oplus j_q) l_q} \end{aligned} \tag{5.15}$$

Suppose first that $i = j$. In this case, it is clear that $i_q \oplus j_q \equiv 0$ for all q, and thus Equation (5.15) reduces to

$$\begin{aligned}
\langle v_i | v_j \rangle &= \frac{1}{2^n} \sum_{l=0}^{2^{n-1}} (-1)^{\sum_{q=0}^{n-1} 0 \cdot l_q} \\
&= \frac{1}{2^n} \sum_{l=0}^{2^{n-1}} 1 \\
&= \frac{1}{2^n} 2^n \\
&= 1. \qquad (5.16)
\end{aligned}$$

Next, consider the case $i \neq j$. Then, it is possible to choose at least one q such that $i_q \oplus j_q \equiv 1$, allowing us to rewrite Equation (5.15) as

$$\begin{aligned}
\langle v_i | v_j \rangle &= \frac{1}{2^n} \sum_{l_0=0}^{1} \sum_{l_1=0}^{1} \cdots \sum_{l_{n-1}=0}^{1} (-1)^{\sum_{r=0}^{n-1} (i_r \oplus j_r) l_r} \\
&= \frac{1}{2^n} \prod_{s=0}^{n-1} \left(\sum_{l_s=0}^{1} (-1)^{(i_s \oplus j_s) l_s} \right) \\
&= \frac{1}{2^n} \left(\sum_{l_q=0}^{1} (-1)^{(i_q \oplus j_q) l_q} \right) \prod_{s \neq q} \left(\sum_{l_s=0}^{1} (-1)^{(i_s \oplus j_s) l_s} \right) \\
&= \frac{1}{2^n} \left((-1)^{1 \cdot 0} + (-1)^{1 \cdot 1} \right) \prod_{s \neq q} \left(\sum_{l_s=0}^{1} (-1)^{(i_s \oplus j_s) l_s} \right) \\
&= \frac{1}{2^n} (1 - 1) \prod_{s \neq q} \left(\sum_{l_s=0}^{1} (-1)^{(i_s \oplus j_s) l_s} \right) \\
&= 0. \qquad (5.17)
\end{aligned}$$

Combining equations (5.16) and (5.17) gives us the desired result of

$$\langle v_i | v_j \rangle = \delta_{ij}. \qquad (5.18)$$

□

Corollary 5.3.2. *The set* $\{|v_i\rangle\}$ *defined in Equation (5.11) is an orthonormal basis of eigenvectors for the density matrix* $\rho = |g\rangle\langle g|$ *with eigenvalues* $\delta_{i,0}$.

Proof. It is clear from the definition of $|v_i\rangle$ that $|v_0\rangle = |g\rangle$. Thus,

$$\begin{aligned}
\rho|v_0\rangle &= |g\rangle\langle g|g\rangle \\
&= |g\rangle \\
&= |v_0\rangle \text{ and} \\
\rho|v_{i\neq 0}\rangle &= |v_0\rangle\langle v_0|v_{i\neq 0}\rangle \\
&= 0.
\end{aligned}$$

□

Theorem 5.3.3. *Suppose an n-qubit graph state $|g\rangle$ is provided. The orthonormal basis $\{|v_i\rangle\}$ for the density matrix $\rho = |g\rangle\langle g|$ defined in Equation (5.11) gives a separable Pauli stabiliser for $|g\rangle$ when used in the constructive algorithm of Theorem 4.3.3.*

Proof. The proof of this statement, although somewhat tedious, is relatively straightforward. Consider the stabiliser element s_i. We will show that it is a separable Pauli operator.

$$s_i = \sum_{l=0}^{2^n-1} (W_n)_{il} |v_l\rangle\langle v_l| \tag{5.19}$$

Use equations (4.28) and (5.11) to expand this expression:

$$\begin{aligned}
s_i &= \frac{1}{2^n} \sum_{l=0}^{2^n-1} (-1)^{\sum_{m=0}^{n-1} k_m l_m} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{\sum_{a=0}^{n-2} \sum_{b=a+1}^{n-1} A_{ab}(x_a x_b + y_a y_b)} \\
&\times (-1)^{\sum_{d=0}^{n-1} l_d (x_d + y_d)} |x\rangle\langle y| \\
&= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{\sum_{a=0}^{n-2} \sum_{b=a+1}^{n-1} A_{ab}(x_a x_b + y_a y_b)} \qquad (5.20) \\
&\times \sum_{l=0}^{2^n-1} (-1)^{\sum_{m=0}^{n-1} l_m (x_m + y_m + k_m)} |x\rangle\langle y|. \qquad (5.21)
\end{aligned}$$

The operator s_i is fully separable if and only if none of its matrix elements depend on more than one bit of x or y. Thus, we need to remove the explicit dependence of the stabiliser matrix elements on the cross terms $x_a x_b$ and $y_a y_b$. The factor $(-1)^{\sum_{a=0}^{n-2} \sum_{b=a+1}^{n-1} A_{ab}(x_a x_b + y_a y_b)}$

above depends on the properties of the underlying graph (i.e. the adjacency matrix), whereas the factor $(-1)^{\sum_{m=0}^{n-1} l_m(x_m+y_m+k_m)}$ does not. We can rewrite this graph-independent portion as follows:

$$\begin{aligned}
\sum_{l=0}^{2^n-1}(-1)^{\sum_{m=0}^{n-1} l_m(x_m+y_m+k_m)} &= \sum_{l=0}^{2^n-1}\left(\prod_{m=0}^{n-1}(-1)^{l_m(x_m+y_m+k_m)}\right) \\
&= \sum_{l_0=0}^{1}\sum_{l_1=0}^{1}\cdots\sum_{l_{n-1}=0}^{1}\left(\prod_{m=0}^{n-1}(-1)^{l_m(x_m+y_m+k_m)}\right) \\
&= \prod_{m=0}^{n-1}\left(\sum_{l_m=0}^{1}(-1)^{l_m(x_m+y_m+k_m)}\right) \\
&= \prod_{m=0}^{n-1}\left[1+(-1)^{x_m+y_m+k_m}\right] \\
&= \prod_{m=0}^{n-1} 2\delta_{x_m,y_m\oplus k_m}, \qquad (5.22)
\end{aligned}$$

where the equality of the last two lines above is straightforward to verify. Substituting Equation (5.22) into Equation (5.21) and using the fact that regular integer arithmetic is equivalent to arithmetic modulo 2 when it appears in a power to which the number -1 is raised gives

$$\begin{aligned}
s_k &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1}A_{ab}(x_ax_b\oplus y_ay_b)}\left(\prod_{m=0}^{n-1}2\delta_{x_m,y_m\oplus k_m}\right)|x\rangle\langle y| \\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1}A_{ab}((y_a\oplus k_a)(y_b\oplus k_b)\oplus y_ay_b)}\cdot 2^n\left(\prod_{m=0}^{n-1}\delta_{x_m,y_m\oplus k_m}\right)|x\rangle\langle y| \\
&= \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1}A_{ab}(y_ay_b\oplus y_ak_b\oplus y_bk_a\oplus k_ak_b\oplus y_ay_b)}\left(\prod_{m=0}^{n-1}\delta_{x_m,y_m\oplus k_m}\right)|x\rangle\langle y| \\
&= \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1}A_{ab}(y_ak_b\oplus y_bk_a\oplus k_ak_b)}\left(\prod_{m=0}^{n-1}\delta_{x_m,y_m\oplus k_m}\right)|x\rangle\langle y|, \qquad (5.23)
\end{aligned}$$

In Equation (5.23), it can now be seen that the matrix elements of s_k do not depend on cross terms like x_ax_b or y_ay_b and thus, the matrix elements are separable as promised. We can go further and show that the separable operators are, in fact, single-qubit Pauli

operators.

$$\begin{aligned} s_k &= \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} (-1)^{\sum_{c=0}^{n-2}\sum_{d=c+1}^{n-1} A_{cd}(y_c k_d + y_d k_c)} \\ &\times \left(\prod_{m=0}^{n-1} \delta_{x_m, y_m \oplus k_m}\right) |x\rangle\langle y|. \end{aligned} \tag{5.24}$$

Since $A_{cd} = A_{dc}$ (the underlying graph is undirected), it is true that

$$\sum_{c=0}^{n-2}\sum_{d=c+1}^{n-1} A_{cd}\,(y_c k_d + y_d k_c) = \sum_{c=0}^{n-2}\sum_{d=c+1}^{n-1} A_{cd} y_c k_d + \sum_{l=0}^{n-2}\sum_{m=l+1}^{n-1} A_{lm} y_m k_l.$$

The above pair of sums can be condensed into a single sum over all possible indices c and d labelling the matrix elements A_{cd}, because the diagonal matrix elements A_{ii} are all equal to zero (since the graph is simple):

$$\sum_{c=0}^{n-2}\sum_{d=c+1}^{n-1} A_{cd}\,(y_c k_d + y_d k_c) = \sum_{c=0}^{n-1}\sum_{d=0}^{n-1} A_{cd} y_c k_d. \tag{5.25}$$

Substituting Equation (5.25) into Equation (5.24) gives us

$$\begin{aligned} s_k &= \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} (-1)^{\sum_{c=0}^{n-1}\sum_{d=0}^{n-1} A_{cd} y_c k_d} \\ &\times \left(\prod_{m=0}^{n-1} \delta_{x_m, y_m \oplus k_m}\right) |x\rangle\langle y| \\ &= (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} \left(\prod_{c=0}^{n-1} (-1)^{\sum_{d=0}^{n-1} A_{cd} y_c k_d}\right) \\ &\times \left(\prod_{m=0}^{n-1} \delta_{x_m, y_m \oplus k_m}\right) |x\rangle\langle y| \\ &= (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} \sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} \left(\prod_{m=0}^{n-1} (-1)^{y_m \sum_{d=0}^{n-1} A_{md} k_d}\, \delta_{x_m, y_m \oplus k_m}\right) |x\rangle\langle y|, \end{aligned}$$

which can be written explicitly as the Kronecker product of single-qubit operators as

$$\begin{aligned} s_k &= (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} \\ &\times \bigotimes_{m=0}^{n-1} \left(\sum_{r=0}^{1}\sum_{s=0}^{1} (-1)^{s \sum_{d=0}^{n-1} A_{md} k_d}\, \delta_{r, s\oplus k_m} |r\rangle\langle s|\right) \\ &= (-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)} \\ &\times \bigotimes_{m=0}^{n-1} \left(\sum_{r=0}^{1}\sum_{s=0}^{1} (-1)^{s \sum_{d=0}^{n-1} A_{md} k_d}\, \delta_{r\oplus s, k_m} |r\rangle\langle s|\right). \end{aligned} \tag{5.26}$$

k_m	$\sum_{d=0}^{n-1} A_{md}k_d \bmod 2$	S_m
0	0	$I^{(2)}$
0	1	Z
1	0	X
1	1	$-iY$

Table 5.1: Possible values of single-qubit operator S_m appearing in Equation (5.27).

The factor $(-1)^{\sum_{a=0}^{n-2}\sum_{b=a+1}^{n-1} A_{ab}(k_a k_b)}$ only affects the overall sign appearing in front of the stabiliser element s_k, depending upon the index k and the adjacency matrix A of the underlying graph. Now consider the single-qubit operator

$$\begin{aligned} S_m &= \sum_{r=0}^{1}\sum_{s=0}^{1} (-1)^{s\sum_{d=0}^{n-1} A_{md}k_d}\, \delta_{r\oplus s,k_m} |r\rangle\langle s| \\ &\equiv \begin{bmatrix} \delta_{0,k_m} & (-1)^{\sum_{d=0}^{n-1} A_{md}k_d}\, \delta_{1,k_m} \\ \delta_{1,k_m} & (-1)^{\sum_{d=0}^{n-1} A_{md}k_d}\, \delta_{0,k_m} \end{bmatrix}. \end{aligned} \tag{5.27}$$

There are four possibilities as to what this operator could be, which are summarised in Table 5.3. They are all single-qubit Pauli operators, thus completing the proof. □

To demonstrate the value of Theorem 5.3.3, we will turn yet again to the Bell state previously studied in Example 4.3.4.

Example 5.3.4. Consider the Bell state

$$\begin{aligned} |\psi_{\text{Bell}}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \end{aligned}$$

This is not a graph state; however, it is equivalent under the local unitary transformation $I_0^{(2)} \otimes H_1$ to the two-qubit connected graph state

$$|g\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle). \tag{5.28}$$

In accordance with Equation (5.11), we choose the eigenbasis $\{|v_i\rangle\}$ of $\rho = |g\rangle\langle g|$ as follows:

$$\begin{aligned} |v_0\rangle &= \left(I_0^{(2)} \otimes I_1^{(2)}\right) \cdot \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right) \\ &= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right) \\ &\equiv \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \end{aligned}$$

$$\begin{aligned} |v_1\rangle &= \left(I_0^{(2)} \otimes Z_1\right) \cdot \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right) \\ &= \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right) \\ &\equiv \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \end{aligned}$$

$$\begin{aligned} |v_2\rangle &= \left(Z_0 \otimes I_1^{(2)}\right) \cdot \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right) \\ &= \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle + |11\rangle\right) \\ &\equiv \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \end{aligned}$$

$$
\begin{aligned}
|v_3\rangle &= (Z_0 \otimes Z_1) \cdot \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\
&= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle) \\
&\equiv \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{bmatrix},
\end{aligned}
$$

thereby finding the f_i defined in Theorem 4.3.3 to be

$$f_0 = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{5.29}$$

$$f_1 = \frac{1}{4}\begin{bmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{bmatrix} \tag{5.30}$$

$$f_2 = \frac{1}{4}\begin{bmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix} \tag{5.31}$$

$$f_3 = \frac{1}{4}\begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}. \tag{5.32}$$

From here we obtain the stabiliser elements

$$
\begin{aligned}
s_0 &= f_0 + f_1 + f_2 + f_3 \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} && (5.33) \\
&= I_0^{(2)} \otimes I_1^{(2)}. && (5.34)
\end{aligned}
$$

$$
\begin{aligned}
s_1 &= f_0 - f_1 + f_2 - f_3 \\
&= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} && (5.35) \\
&= Z_0 \otimes X_1. && (5.36)
\end{aligned}
$$

$$
\begin{aligned}
s_2 &= f_0 + f_1 - f_2 - f_3 \\
&= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} && (5.37) \\
&= X_0 \otimes Z_1. && (5.38)
\end{aligned}
$$

$$
\begin{aligned}
s_3 &= f_0 - f_1 - f_2 + f_3 \\
&= \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} && (5.39) \\
&= Y_0 \otimes Y_1. && (5.40)
\end{aligned}
$$

From here, it is straightforward to obtain the Pauli stabiliser of $|\psi_{\text{Bell}}\rangle$:

$$\begin{aligned}
\tilde{s}_0 &= \left(I_0^{(2)} \otimes H_1\right)\left(I_0^{(2)} \otimes I_1^{(2)}\right)\left(I_0^{(2)} \otimes H_1\right) \\
&= I_0^{(2)} I_0^{(2)} I_0^{(2)} \otimes H_1 I_1^{(2)} H_1 \\
&= I_0^{(2)} \otimes I_1^{(2)}.
\end{aligned}$$

$$\begin{aligned}
\tilde{s}_1 &= \left(I_0^{(2)} \otimes H_1\right)(Z_0 \otimes X_1)\left(I_0^{(2)} \otimes H_1\right) \\
&= I_0^{(2)} Z_0 I_0^{(2)} \otimes H_1 X_1 H_1 \\
&= Z_0 \otimes Z_1.
\end{aligned}$$

$$\begin{aligned}
\tilde{s}_2 &= \left(I_0^{(2)} \otimes H_1\right)(X_0 \otimes Z_1)\left(I_0^{(2)} \otimes H_1\right) \\
&= I_0^{(2)} X_0 I_0^{(2)} \otimes H_1 Z_1 H_1 \\
&= X_0 \otimes X_1.
\end{aligned}$$

$$\begin{aligned}
\tilde{s}_3 &= \left(I_0^{(2)} \otimes H_1\right)(Y_0 \otimes Y_1)\left(I_0^{(2)} \otimes H_1\right) \\
&= I_0^{(2)} Y_0 I_0^{(2)} \otimes H_1 Y_1 H_1 \\
&= -Y_0 \otimes Y_1.
\end{aligned}$$

The Pauli stabiliser of $|\psi_{\text{Bell}}\rangle$ is therefore seen to be $\left\{I_0^{(2)} \otimes I_1^{(2)}, Z_0 \otimes Z_1, X_0 \otimes X_1, -Y_0 \otimes Y_1\right\}$, in agreement with Equation (4.9).

5.4 Constructing separable stabilisers for SLOCC-transformed graph states

As discussed in Section 5.2, a SLOCC-transformed stabiliser state has a separable, generally non-Pauli stabiliser whose elements are composed of tensor products of single-qubit operators that square to the identity. In our scenario of interest, some state $|\tilde{s}\rangle$ is given, and the problem is to find out whether there exists a SLOCC transformation S connecting $|\tilde{s}\rangle$ to some known stabiliser state $|s\rangle$. The approach described here is to attempt

to explicitly construct the SLOCC-transformed stabiliser of $|\tilde{s}\rangle$ using an extension of the constructive algorithm given in theorems 4.3.3 and 5.3.3. The algorithm as given only works for graph states, although it can easily be used for all stabiliser states, as shown in Example 5.3.4. The generalisation to SLOCC-transformed stabiliser states, however, is not trivial. Consider the SLOCC-transformed stabiliser state $|\tilde{s}\rangle$. Since $|s\rangle$ was fixed by the operators $\{\sigma_j\}$, $|\tilde{s}\rangle$ will be fixed by the operators $\{\tilde{\sigma}_j\}$, given by

$$\begin{aligned}
\tilde{\sigma}_j &= S\sigma_j S^{-1} \\
&= S\left(\sum_{k=0}^{2^n-1} (W_n)_{jk} |v_k\rangle\langle v_k|\right) S^{-1} \\
&= \sum_{k=0}^{2^n-1} (W_n)_{jk} \left(S|v_k\rangle\langle v_k|S^{-1}\right) \\
&= \sum_{k=0}^{2^n-1} (W_n)_{jk} \tilde{f}_k
\end{aligned}$$

where $\tilde{f}_k = S|v_k\rangle\langle v_k|S^{-1}$. Whereas the f_k could be determined from the knowledge of $|v_k\rangle$ alone, constructing the $\tilde{f}_k$ requires knowledge of $S|v_k\rangle$ and $\langle v_k|S^{-1}$, which are not known. These vectors are the right and left eigenvectors respectively of the matrix $\tilde{\rho} = S\rho S^{-1}$:

$$\begin{aligned}
\tilde{\rho}\left(S|v_k\rangle\right) &= S|v_0\rangle\langle v_0|S^{-1}S|v_k\rangle \\
&= S|v_0\rangle\langle v_0|v_k\rangle \\
&= \delta_{0,k}\left(S|v_k\rangle\right).
\end{aligned}$$

$$\begin{aligned}
\left(\langle v_k|S^{-1}\right)\tilde{\rho} &= \langle v_k|S^{-1}S|v_0\rangle\langle v_0|S^{-1} \\
&= \langle v_k||v_0\rangle\langle v_0|S^{-1} \\
&= \left(\langle v_k|S^{-1}\right)\delta_{0,k}.
\end{aligned}$$

This was not an issue in the case of the graph state because ρ is a Hermitian matrix, and the left eigenvectors of Hermitian matrices are the adjoints of the right eigenvectors.

However, $\tilde{\rho}$ is not Hermitian unless S is unitary. In order to construct the separable stabiliser for $|\tilde{s}\rangle$, we will need to find both a left and a right orthonormal eigenbasis for $\tilde{\rho}$. Due to the degeneracy of the eigenvalue 0, there are an infinite number of choices of right eigenbases, and there are also an infinite number of possible left eigenbases. However, there is a specific choice for each of these bases such that the $\tilde{\sigma_k}$ operators are separable. The basis of right eigenvectors, denoted $\{|v_{k,R}\rangle\}$, can be written as

$$\begin{aligned} |v_{k,R}\rangle &= S|v_k\rangle \\ &= S\left(\bigotimes_{j=0}^{n-1} Z_j^{k_j}\right)|v_0\rangle \\ &= S\left(\bigotimes_{j=0}^{n-1} Z_j^{k_j}\right)S^{-1}S|v_0\rangle \\ &= \left(\bigotimes_{j=0}^{n-1} S_j Z_j^{k_j} S_j^{-1}\right)S|v_0\rangle \\ &= \left(\bigotimes_{j=0}^{n-1} \tilde{Z}_j^{k_j}\right)|\tilde{s}\rangle, \end{aligned} \tag{5.41}$$

where Z_j is the Pauli-Z gate acting on qubit j and

$$\tilde{Z}_j = S_j Z_j S_j^{-1}. \tag{5.42}$$

Similarly, the basis of left eigenvectors is denoted by $\{\langle v_{k,L}|\}$ and given by

$$\begin{aligned} \langle v_{k,L}| &= \langle v_k|S^{-1} \\ &= \langle \tilde{s}'|\left(\bigotimes_{j=0}^{n-1} \tilde{Z}_j^{k_j}\right), \end{aligned} \tag{5.43}$$

where

$$\langle \tilde{s}'| = \langle s|S^{-1}. \tag{5.44}$$

At this point it will be convenient to define some notation for groups that are transformed by the SLOCC operator S.

Definition 5.4.1. *Suppose G is a group of n-qubit operators and S is an n-qubit SLOCC operator. Then the symbol $\tilde{G}^{(S)}$ denotes the group that results from transforming G by S, or more specifically,*

$$\begin{aligned} \tilde{G}^{(S)} &= SGS^{-1} \\ &= \{\, Sg_iS^{-1} \mid g_i \in G \,\} \\ &= \{\, \tilde{g}_i^{(S)} \mid g_i \in G \,\}, \end{aligned}$$

where $\tilde{g}_i{}^{(S)} = Sg_iS^{-1}$.

It is straightforward to verify in the usual way that $\tilde{G}^{(S)}$ is a group, so it will not be done here. For notational convenience, the superscript (S) will be dropped whenever there is no possibility for confusion, so the group transformed by S will be written merely as $\tilde{G}$, and the elements of the group as $\tilde{g}$. Using the above notation, it can be seen for example that the operators $\tilde{Z}_j$ from Equation (5.42) belong to the group $\tilde{\mathcal{G}}_1$, the single-qubit Pauli group transformed by the SLOCC operator S.

It can be shown that the left and right eigenbases of equations (5.43) and (5.41) are orthonormal relative to each other.

Lemma 5.4.2. *The basis vectors $\{\langle v_{k,L}|\}$ that are left eigenvectors of the matrix $\tilde{\rho} = S|g\rangle\langle g|S^{-1}$, defined in Equation (5.43), where $|g\rangle$ is an n-qubit graph state and S is an n-qubit SLOCC operator, obey the orthonormality relations*

$$\langle v_{j,L}|v_{k,R}\rangle = \delta_{j,k} \tag{5.45}$$

with the elements of the basis of right eigenvectors $\{|v_{k,R}\rangle\}$ of $\tilde{\rho}$ defined in Equation (5.41).

Proof.

$$\begin{aligned}\langle v_{j,L}|v_{k,R}\rangle &= \langle v_j|S^{-1}S|v_k\rangle \\ &= \langle v_j|v_k\rangle \text{ (where the } \{|v_k\rangle\} \text{ are right eigenvectors of } \rho = |g\rangle\langle g|) \\ &= \delta_{j,k}.\end{aligned}$$

□

We can now state the central theorem regarding the construction of the separable (non-Pauli) stabiliser of a SLOCC-transformed graph state.

Theorem 5.4.3. *Suppose we have an n-qubit graph state $|g\rangle$ and an n-qubit SLOCC operator S. Then the set of operators $\sigma = \{\tilde{\sigma}_j\}$ given by*

$$\tilde{\sigma}_j = \sum_{k=0}^{2^n-1} (W_n)_{jk} |v_{k,R}\rangle\langle v_{k,L}| \tag{5.46}$$

form a separable (in general non-Pauli) stabiliser for the SLOCC-transformed graph state $|\tilde{g}\rangle = S|g\rangle$, where the $\{|v_{k,R}\rangle\}$ and $\{\langle v_{k,L}|\}$ are defined in equations (5.41) and (5.43) respectively.

Proof. Since S is an n-qubit SLOCC operator, it can be written as

$$S = \bigotimes_{i=0}^{n-1} S_i, \tag{5.47}$$

where the S_i are all single-qubit, invertible operators. Now, note that

$$\begin{aligned}\tilde{\sigma}_j &= \sum_{k=0}^{2^n-1} (W_n)_{jk} |v_{k,R}\rangle\langle v_{k,L}| \\ &= \sum_{k=0}^{2^n-1} (W_n)_{jk} S|v_k\rangle\langle v_k|S^{-1} \\ &= S\left(\sum_{k=0}^{2^n-1} (W_n)_{jk} |v_k\rangle\langle v_k|\right) S^{-1} \\ &= S\sigma_j S^{-1} \\ &= \bigotimes_{k=0}^{n-1} S_k \sigma_{jk} S_k^{-1},\end{aligned} \tag{5.48}$$

where $\sigma_j = \bigotimes_{k=0}^{n-1} \sigma_{jk}$ is an element of the separable Pauli stabiliser for $|g\rangle$. The operators $\tilde{\sigma}_j$ in Equation (5.48) are precisely the ones found in Equation (5.2) and are thus known to form a stabiliser for $|\tilde{g}\rangle$. □

The orthonormality relations from Equation (5.45) give us a system of multivariate polynomial equations that can be solved for the unknown $\tilde{Z}_i$ operators:

$$\begin{aligned}\langle v_{j,L}|v_{k,R}\rangle &= \langle v_{0,L}| \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i}\right) \left(\bigotimes_{l=0}^{n-1} \tilde{Z}_l^{k_l}\right) |v_{0,R}\rangle \\ &= \langle v_{0,L}| \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i \oplus k_i}\right) |v_{0,R}\rangle.\end{aligned}$$

Therefore,

$$\begin{aligned}\langle v_{0,L}| \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i \oplus k_i}\right) |v_{0,R}\rangle &= \delta_{j,k} \\ \langle v_{0,L}| \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i}\right) |v_{0,R}\rangle &= \delta_{j,0}.\end{aligned} \tag{5.49}$$

Equation (5.49) is a system of 2^n equations in $4n$ real unknowns for the matrix elements of the $\tilde{Z}_i$ operators. It will be shown shortly that only 2^{n-1} of these equations give useful conditions on the $\tilde{Z}_i$ operators, while the rest are automatically satisfied regardless of the pure state $|\psi\rangle$ being considered. As a direct consequence of Theorem 5.4.3, it can be seen that the conditions (5.49) are necessary, although not sufficient, for the states $|g\rangle$ and $|\psi\rangle$ to be SLOCC-equivalent. These orthonormality conditions as written exhibit a serious practical problem, namely that $\langle\phi| = \langle v_{0,L}|$ is unknown. However, this problem can be alleviated by writing $\langle\phi|$ in terms of $|\psi\rangle$ and the unknown S_i operators in the computational basis.

Remark 5.4.4. The inverse of a matrix $S_i \in GL(2,\mathbb{C})$ can be written as

$$(S_i)^{-1} = \frac{1}{\det(S_i)} Y S_i^T Y, \tag{5.50}$$

where S_i^T denotes the transpose of S_i, $\det(S_i)$ is the determinant of S_i and Y is the standard Pauli-Y matrix.

This above fact can easily be checked, and is very useful: it allows us to write $\langle\phi|$ in terms of $\langle g|$ and the SLOCC operator S. The expression (5.51) given in Lemma 5.4.5 below also contains local operators σ_{ij} from the Pauli stabiliser for $|g\rangle$. This feature will prove to be useful for simplifying (5.51).

Lemma 5.4.5. *Suppose we have an n-qubit pure state $|\psi\rangle$, an n-qubit graph state $|g\rangle$ with Pauli stabiliser*

$$\begin{aligned}\Sigma &= stab_{\mathcal{G}_n}(|g\rangle) \\ &= \left\{ \sigma_i \;\middle|\; \sigma_i = \bigotimes_{j=0}^{n-1} \sigma_{ij},\ \sigma_{ij} \in \mathcal{G}_1 \right\}\end{aligned}$$

and an operator $S = \bigotimes_{i=0}^{n-1} S_i$ with $S_i \in GL(2,\mathbb{C})\ \forall\ i \in \{0,1,\ldots,n-1\}$ such that $|\psi\rangle = S|g\rangle$. Then the bra vector $\langle\phi| = \langle g|S^{-1}$ can be written in any basis where $|g\rangle \in \mathbb{R}^{2^n}$ as

$$\langle\phi| = \frac{1}{det(S_0)} (\langle\psi|)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \mathcal{O}_k, \tag{5.51}$$

where $\mathcal{O}_k = S_k Y_k \sigma_{jk} S_k^{-1} \in \tilde{\mathcal{G}}_1$

Proof.

$$\begin{aligned}\langle\phi| &= \langle g|S^{-1} \\ &= \langle g| \bigotimes_{i=0}^{n-1} S_i^{-1} \\ &= \langle g| \bigotimes_{i=0}^{n-1} \frac{Y_i S_i^T Y_i}{\det(S_i)} \text{ (from Remark 5.4.4)} \\ &= \frac{1}{\prod_{i=0}^{n-1} \det(S_i)} \langle g| \bigotimes_{i=0}^{n-1} Y_i S_i^T Y_i.\end{aligned}$$

Without loss of generality, we can set $\det(S_i) = 1$ for all $i \neq 0$, so that

$$\langle\phi| = \frac{1}{\det(S_0)} \langle g| \bigotimes_{i=0}^{n-1} Y_i S_i^T Y_i. \tag{5.52}$$

At this point, we can use a trick: since the graph state $|g\rangle$ is known, its Pauli stabiliser $\Sigma = \text{stab}_{\mathcal{G}_n}(|g\rangle)$ is also known. For a stabiliser element $\sigma_i \in \Sigma$, we have

$$\begin{aligned} \sigma_i|g\rangle &= |g\rangle, \text{ so} \\ \langle g|\sigma_i^\dagger &= \langle g|\sigma_i \text{ (since } \sigma_i \text{ is Hermitian)} \\ &= \langle g|. \end{aligned}$$

Because of this relationship, we can insert a stabiliser element into Equation (5.52) as follows:

$$\begin{aligned} \langle\phi| &= \frac{1}{\det(S_0)}\langle g|\sigma_j \bigotimes_{i=0}^{n-1} Y_i S_i^T Y_i \\ &= \frac{1}{\det(S_0)}\langle g| \left(\bigotimes_{k=0}^{n-1} \sigma_{jk}\right)\left(\bigotimes_{i=0}^{n-1} Y_i S_i^T Y_i\right) \\ &= \frac{1}{\det(S_0)}\langle g| \bigotimes_{k=0}^{n-1} \sigma_{jk} Y_k S_k^T Y_k. \end{aligned} \tag{5.53}$$

Now, we have $|\psi\rangle = S|g\rangle$ by assumption, and thus

$$\begin{aligned} S^{-1}|\psi\rangle &= |g\rangle, \text{ implying} \\ \langle g| &= \langle\psi|\left(S^{-1}\right)^\dagger \\ &= \langle\psi|\left(\left(S^{-1}\right)^T\right)^*. \end{aligned} \tag{5.54}$$

Taking the transpose of both sides of Equation (5.50) gives us

$$\begin{aligned} \left(S_i^{-1}\right)^T &= \frac{1}{\det(S_i)} Y^T S_i Y^T \\ &= \frac{1}{\det(S_i)} Y S_i Y \text{ (since } Y^T = -Y). \end{aligned} \tag{5.55}$$

Substituting (5.55) into (5.54) yields

$$\begin{aligned} \langle g| &= \frac{1}{\det(S_0)}^* \langle\psi|\left(\bigotimes_{i=0}^{n-1} Y_i S_i Y_i\right)^* \text{ and thus,} \\ (\langle g|)^* &= \frac{1}{\det(S_0)} (\langle\psi|)^* \bigotimes_{i=0}^{n-1} Y_i S_i Y_i. \end{aligned}$$

In any basis where $\langle g|$ is completely real (such as the computational basis, with all elements being ± 1), we have $(\langle g|)^* = \langle g|$, and thus that

$$\langle g| = \frac{1}{\det(S_0)} (\langle \psi|)^* \bigotimes_{i=0}^{n-1} Y_i S_i Y_i \text{ (in a basis where } |g\rangle \in \mathbb{R}^{2^n}). \tag{5.56}$$

Putting (5.56) into (5.53), we see that

$$\begin{aligned} \langle \phi| &= \frac{1}{\det(S_0)} \frac{1}{\det(S_0)} (\langle \psi|)^* \left(\bigotimes_{i=0}^{n-1} Y_i S_i Y_i \right) \left(\bigotimes_{k=0}^{n-1} \sigma_{jk} Y_k S_k^T Y_k \right) \\ &= \frac{1}{\det(S_0)\det(S_0)} (\langle \psi|)^* \bigotimes_{k=0}^{n-1} Y_k S_k Y_k \sigma_{jk} Y_k S_k^T Y_k. \end{aligned} \tag{5.57}$$

Now, noting that $Y^{-1} = Y$ and taking the inverse of both sides of Equation (5.55) gives us

$$S_i^T = \det(S_i)\, Y S_i^{-1} Y. \tag{5.58}$$

Putting Equation (5.58) into Equation (5.57), we get

$$\begin{aligned} \langle \phi| &= \frac{1}{\det(S_0)\det(S_0)} \det(S_0)\, (\langle \psi|)^* \bigotimes_{k=0}^{n-1} Y_k S_k Y_k \sigma_{jk} Y_k Y_k S_k^{-1} Y_k Y_k \\ &= \frac{1}{\det(S_0)} (\langle \psi|)^* \bigotimes_{k=0}^{n-1} Y_k S_k Y_k \sigma_{jk} S_k^{-1} \\ &= \frac{1}{\det(S_0)} (\langle \psi|)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \left(S_k Y_k \sigma_{jk} S_k^{-1} \right) \qquad (5.59) \\ &= \frac{1}{\det(S_0)} (\langle \psi|)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \mathcal{O}_k, \qquad (5.60) \end{aligned}$$

where $\mathcal{O}_k = S_k Y_k \sigma_{jk} S_k^{-1} \in \tilde{\mathcal{G}}_1$. □

Using Lemma 5.4.5, the conditions from Equation (5.49) can be rewritten in an appropriate basis (one where $|g\rangle$ is real) as

$$\begin{aligned} \langle \phi| \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} \right) |\psi\rangle &= \frac{1}{\det(S_0)} (\langle \psi|)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \mathcal{O}_k \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} \right) |\psi\rangle \\ &= \frac{1}{\det(S_0)} (\langle \psi|)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \mathcal{O}_k \tilde{Z}_k^{j_k} |\psi\rangle \qquad (5.61) \\ &= \delta_{j,0}. \end{aligned}$$

The $\mathcal{O}_k$ operators in the above conditions can be eliminated. Recall the definition

$$\mathcal{O}_k = S_k Y_k \sigma_{jk} S_k^{-1} \in \tilde{\mathcal{G}}_1. \tag{5.62}$$

In the case that $\sigma_{jk} = Y_k$, we find

$$\begin{aligned} \mathcal{O}_k &= S_k Y_k Y_k S_k^{-1} \\ &= S_k S_k^{-1} \\ &= I^{(2)}, \end{aligned}$$

and thus,

$$\begin{aligned} \mathcal{O}_k \tilde{Z}_k^{j_k} &= I^{(2)} \tilde{Z}_k^{j_k} \\ &= \tilde{Z}_k^{j_k}. \end{aligned} \tag{5.63}$$

Similarly, when $\sigma_{jk} = X_k$,

$$\begin{aligned} \mathcal{O}_k &= S_k Y_k X_k S_k^{-1} \\ &= -i S_k Z_k S_k^{-1} \\ &= -i \tilde{Z}_k, \end{aligned}$$

and thus,

$$\begin{aligned} \mathcal{O}_k \tilde{Z}_k^{j_k} &= -i \tilde{Z}_k \tilde{Z}_k^{j_k} \\ &= -i \tilde{Z}_k^{j_k \oplus 1}. \end{aligned} \tag{5.64}$$

Therefore, in the case that $|g\rangle$ has a Pauli stabiliser element σ_j consisting purely of local X and Y operations (up to a constant), the conditions in Equation (5.61) reduce to

$$\begin{aligned} \langle \phi | \left(\bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} \right) |\psi\rangle &= (\langle \psi |)^* Y^{\otimes n} \bigotimes_{k=0}^{n-1} \tilde{Z}_k^{l_k} |\psi\rangle \\ &= (i)^{\sum_{m=0}^{n-1} l_m} \det(S_0)\, \delta_{j,l}, \end{aligned} \tag{5.65}$$

where

$$l_k = \begin{cases} 0 \text{ if } \sigma_{jk} \text{ is proportional to } Y_k \\ 1 \text{ if } \sigma_{jk} \text{ is proportional to } X_k \end{cases}.$$

The quantity $\sum_{m=0}^{n-1} l_m$ corresponds to the number of ones in the n-bit expression for l. It is called the *Hamming weight* of l [32]. It so happens that all graph states have a Pauli stabiliser element that is proportional to a tensor product of X and Y operators, as will be demonstrated in the next section.

5.5 Binary representation of Pauli subgroups and properties of Pauli stabiliser elements

In order to simplify the necessary conditions for SLOCC equivalence given in Equation (5.65), it is necessary to prove that all graph states have a Pauli stabiliser element whose local operations are all proportional to either X or Y. In order to do this, we will use a concept called the *binary representation* of Pauli operators (see, for example, [33]), which for our purposes is essentially a convenient way of writing down Pauli operators.

Definition 5.5.1. *Consider an n-qubit Pauli operator $\sigma \in \mathcal{G}_n$. The binary notation of σ is the $2n$-dimensional row vector $r(\sigma)$ whose elements are given by the conditions in Table 5.2.*

Local operator on qubit i (up to a constant)	*Entry i of $r(\sigma)$*	*Entry $i+n$ of $r(\sigma)$*
$I_i^{(2)}$	0	0
X_i	1	0
Y_i	1	1
Z_i	0	1

Table 5.2: Binary notation $r(\sigma)$ of $\sigma \in \mathcal{G}_n$.

Definition 5.5.2. *The binary representation of a subset Σ of the n-qubit Pauli group,*

$$\Sigma = \{\ \sigma_i \mid \sigma_i \in \mathcal{G}_n\ \forall\ i \in \{0, 1, \ldots, |\Sigma| - 1\}\ \}$$

is the $|\Sigma|$-by-$2n$ matrix $r(\Sigma)$ whose ith row is the vector corresponding to the binary notation $r(\sigma_i)$ of the element σ_i of Σ.

Although the binary notation for an n-qubit Pauli operator neglects the possible overall constants of ± 1 or $\pm i$, no two n-qubit Pauli operators that differ merely by a constant can ever appear in the same stabiliser (as that would imply that $-I^{(n)}$ is also in the stabiliser, which is impossible). The binary representation of a set of independent generators for a stabiliser is also called the *check matrix* corresponding to that stabiliser [32].

Example 5.5.3. Consider the three-qubit linear cluster state $|g_3\rangle$, a graph state defined by the adjacency matrix

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{5.66}$$

The Pauli stabiliser for this state can be generated by the set

$$G(\mathrm{stab}_{g_3}(|g_3\rangle)) = \left\{ X_0 \otimes Z_1 \otimes I_2^{(2)}, Z_0 \otimes X_1 \otimes Z_2, I_0^{(2)} \otimes Z_1 \otimes X_2 \right\}, \tag{5.67}$$

while the full Pauli stabiliser is

$$\begin{aligned} G(\mathrm{stab}_{g_3}(|g_3\rangle)) \;=\; & \Big\{ I_0^{(2)} \otimes I_1^{(2)} \otimes I_2^{(2)}, X_0 \otimes Z_1 \otimes I_2^{(2)}, Z_0 \otimes X_1 \otimes Z_2, I_0^{(2)} \otimes Z_1 \otimes X_2, \\ & Y_0 \otimes Y_1 \otimes Z_2, X_0 \otimes I_1^{(2)} \otimes X_2, Z_0 \otimes Y_1 \otimes Y_2, -Y_0 \otimes X_1 \otimes Y_2 \Big\}. \end{aligned}$$

The binary notation for the operator $Y_0 \otimes Y_1 \otimes Z_2$, for example, is given by

$$r(Y_0 \otimes Y_1 \otimes Z_2) = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The binary notation for the generators of the Pauli stabiliser of $|g_3\rangle$, also called the check matrix corresponding to this stabiliser, is given by

$$r\left(G\left(\mathrm{stab}_{g_3}\left(|g_3\rangle\right)\right)\right) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}. \tag{5.68}$$

Similarly, the binary representation of the entire Pauli stabiliser of $|g_3\rangle$ is

$$r\left(\mathrm{stab}_{g_3}\left(|g_3\rangle\right)\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The binary notation of the stabiliser elements is a so-called *group isomorphism* [24] from the operator depiction of the elements to a binary row vector depiction of the same, meaning that there is a bijective map from the operator depiction to the row vector

depiction. For example,

$$\begin{aligned} r\left(Z_0 \otimes X_1 \otimes Z_2\right) &= \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ r\left(I_0^{(2)} \otimes Z_1 \otimes X_2\right) &= \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

So,

$$\begin{aligned} r\left(Z_0 \otimes Y_1 \otimes Y_2\right) &= r\left(\left(Z_0 \otimes X_1 \otimes Z_2\right)\left(I_0^{(2)} \otimes Z_1 \otimes X_2\right)\right) \\ &= r\left(Z_0 \otimes X_1 \otimes Z_2\right) \oplus r\left(I_0^{(2)} \otimes Z_1 \otimes X_2\right) \\ &= \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \end{aligned}$$

Note that the rows of the binary representation of a set of operators can be permuted arbitrarily.

The binary representation of sets of Pauli operators is a useful tool for classifying Pauli stabiliser elements in terms of how many of the local operators are proportional to X or Y.

Remark 5.5.4. Suppose we have an n-qubit graph state characterised by an adjacency matrix A. Then it can be seen that the generators g_i of the Pauli stabiliser, given in Definition 4.2.2, can be written in their check matrix representation by the n-by-n identity matrix augmented by the adjacency matrix A, i.e.

$$r\left(\mathrm{stab}_{\mathcal{G}_n}\left(|g\rangle\right)\right) = \left(I^{(n)} \,|A\right). \tag{5.69}$$

For example, compare Equation (5.69) with Equation (5.68).

With these ideas, it is easy to show that every graph state has a Pauli stabiliser element composed purely of local X and Y operations.

Lemma 5.5.5. *Any n-qubit graph state $|g\rangle$ has precisely* $\binom{n}{k}$ *(or n choose k) Pauli stabiliser elements for which k of the local Pauli operators composing it are proportional to either X or Y, where $k \in \{0, 1, \ldots, n-1\}$.*

Proof. Suppose the n-by-n adjacency matrix characterising $|g\rangle$ is called A. We can write the binary representation of one set of generators of the Pauli stabiliser of $|g\rangle$ as $r\left(G\left(\text{stab}_{\mathcal{G}_n}\left(|g\rangle\right)\right)\right) = \left(I^{(n)} \,|A\right)$, as discussed previously. Due to the form of the identity matrix, the ith row of $r\left(G\left(\text{stab}_{\mathcal{G}_n}\left(|g\rangle\right)\right)\right)$ (where $i \in \{0, 1, \ldots, n-1\}$) has a 1 in position i and 0s in all of the rest of the positions 0 to $n-1$. Thus, in order to construct a binary row vector which has k 1s and $n-k$ 0s occurring in positions 0 to $n-1$, we must simply choose k of the n rows of $r\left(G\left(\text{stab}_{\mathcal{G}_n}\left(|g\rangle\right)\right)\right)$ and perform elementwise addition modulo 2. There are $\binom{n}{k}$ ways to choose these k rows from the set of n independent rows. Each of the binary rows produced thusly corresponds to a Pauli stabiliser element, k of whose local constituents are proportional to either the Pauli X or the Pauli Y operator. □

In particular, there are precisely $\binom{n}{n} = 1$ Pauli stabiliser elements for which all of the local operators are proportional to X or Y. As an illustration of this point, note that the first three entries of the last row in the binary representation of the stabiliser for the three-qubit linear cluster state in Example 5.5.3 are all 1s, and this row represents the stabiliser element $-Y_0 \otimes X_1 \otimes Y_2$. Let us look at a specific example of using the Pauli stabiliser element composed purely of local X and Y operations to simplify the conditions (5.61) to the form of (5.65).

Example 5.5.6. Consider again the three-qubit linear cluster state $|g_3\rangle$, given in Example 5.5.3. SLOCC-equivalence of $|g_3\rangle$ and some arbitrary three-qubit pure quantum

state $|\psi\rangle$ requires the conditions from Equation (5.65) to be true, namely that

$$\begin{aligned}\langle\phi|\bigotimes_{i=0}^{2}\tilde{Z}_i^{j_i}|\psi\rangle &= (\langle\psi|)^* Y^{\otimes 3}\bigotimes_{i=0}^{2} S_i Y_i \sigma_{ji} S_i^{-1}|\psi\rangle \\ &= (-i)\det(S_0)\,\delta_{j,0}. \end{aligned} \tag{5.70}$$

One of the elements of the Pauli stabiliser for this state was $-Y_0 \otimes X_1 \otimes Y_2$. Thus, with the choice $\sigma_j = -Y_0 \otimes X_1 \otimes Y_2$, Equation (5.59) becomes

$$\begin{aligned}\langle\phi| &= \frac{1}{\det(S_0)}(\langle\psi|)^*(Y_0\otimes Y_1\otimes Y_2)\left(-S_0Y_0Y_0S_0^{-1}\otimes S_1Y_1X_1S_1^{-1}\otimes S_2Y_2Y_2S_2^{-1}\right) \\ &= -i\frac{1}{\det(S_0)}(\langle\psi|)^*(Y_0\otimes Y_1\otimes Y_2)\left(-S_0S_0^{-1}\otimes -S_1Z_1S_1^{-1}\otimes S_2S_2^{-1}\right) \\ &= -i\frac{1}{\det(S_0)}(\langle\psi|)^*(Y_0\otimes Y_1\otimes Y_2)\left(I_0^{(2)}\otimes\tilde{Z}_1\otimes I_2^{(2)}\right) \\ &= -i\frac{1}{\det(S_0)}(\langle\psi|)^* Y^{\otimes n}\bigotimes_{i=0}^{2}\tilde{Z}_i^{2_i},\end{aligned}$$

where $2 \equiv 010$ in three-bit binary representation and thus $2_0 = 0$, $2_1 = 1$ and $2_2 = 0$. Therefore, the orthogonality conditions (5.65) that must be satisfied in order to guarantee SLOCC-equivalence of $|g_3\rangle$ and $|\psi\rangle$ in this case are reduced to

$$(\langle\psi|)^* Y^{\otimes 3}\bigotimes_{i=0}^{2}\tilde{Z}_i^{j_i}|\psi\rangle = i\,(S_0)\,\delta_{j,2}, \tag{5.71}$$

where $j \in \{0,1,\ldots,7\}$. The reader is once again reminded that Equations (5.71) are necessary but insufficient conditions for evaluating the SLOCC-equivalence of $|g_3\rangle$ and $|\psi\rangle$.

5.6 Testing for SLOCC-inequivalence between pure states and graph states

Theorem 5.4.3 gives the conditions (5.65), that are necessary for a pure quantum state to be SLOCC-equivalent to a graph state, although they are insufficient. The determination of the minimal set of necessary and sufficient conditions to guarantee SLOCC-equivalence

is a problem for the future, and will be briefly discussed in Chapter 6. If the conditions (5.65) are not satisfiable, it means that the pure state $|\psi\rangle$ under consideration is SLOCC-inequivalent to the chosen graph state $|g\rangle$ on the same number of qubits. Therefore, the conditions (5.65) give rise to a test for SLOCC-inequivalence. It so happens that not all of these conditions are useful, as some of them are satisfied for any $\left\{\tilde{Z}_i\right\}$ that square to the identity, regardless of the $|\psi\rangle$ vector being considered. The ones that are automatically satisfied are those for which the right hand side is 0 and the left hand side contains an odd number of $\tilde{Z}_i$ operators when $|\psi\rangle$ is on an even number of qubits or an even number of $\tilde{Z}_i$ operators when $|\psi\rangle$ is on an odd number of qubits. This statement will be made concrete, and proven, in Lemma 5.6.2 below. The proof will require the fact that a SLOCC-transformed Z operator $\tilde{Z}$ can be written as a SLOCC-transformed Y operator $\tilde{Y}$ that has undergone a different SLOCC transformation.

Lemma 5.6.1. *Suppose $\tilde{Z} = SZS^{-1}$ where Z is the single-qubit Pauli Z operator and $S \in GL(2,\mathbb{C})$. Then, there exist matrices $T, V \in GL(2,\mathbb{C})$ such that*

$$\tilde{Z} = SZS^{-1} = TYT^{-1} = VXV^{-1}. \tag{5.72}$$

Proof. There exist invertible operators that transform Z to X or to Y. Specifically, note that

$$Z = O_1 X O_1^{-1} \text{ where } O_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5.73}$$

$$Z = O_2 Y O_2^{-1} \text{ where } O_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}. \tag{5.74}$$

From Equation (5.73), we have

$$\begin{aligned}\tilde{Z} &= SZS^{-1} \\ &= SO_1XO_1^{-1}S^{-1} \\ &= (SO_1)\,X\,(SO_1)^{-1} \\ &= VXV^{-1}\end{aligned}$$

where $V = SO_1 \in \mathrm{GL}(2,\mathbb{C})$. Similarly, Equation (5.74) yields

$$\begin{aligned}\tilde{Z} &= SZS^{-1} \\ &= SO_2YO_2^{-1}S^{-1} \\ &= (SO_2)\,Y\,(SO_2)^{-1} \\ &= TYT^{-1}\end{aligned}$$

where $T = SO_2 \in \mathrm{GL}(2,\mathbb{C})$. □

Lemma 5.6.1 essentially says that there is nothing special about SLOCC-transformed Z operators; they can just as well be thought of as SLOCC-transformed X or Y operators. This property allows us to show which of the necessary conditions for SLOCC-equivalence given in Equation (5.65) are superfluous.

Lemma 5.6.2. *Suppose $|\psi\rangle$ is a pure quantum state on n qubits, $\tilde{Z}_i = S_iZ_iS_i^{-1}$ for all $i \in \{0,1,\ldots,n-1\}$ where Z_i is the Pauli Z operator acting on qubit i and $S_i \in GL(2,\mathbb{C})$. Then, the condition*

$$\left[(\langle\psi|)^* Y^{\otimes n}\right] \bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} |\psi\rangle = 0 \tag{5.75}$$

where $j \in \{0,1,\ldots,2^n-1\}$ is automatically satisfied if n is odd and j has even Hamming weight, or if n is even and j has odd Hamming weight.

Proof. First we split up the tensor product in Equation (5.75) into two tensor products, one over the indices where a $\tilde{Z}_i$ operator is acting and one for the rest of the indices:

$$\begin{aligned}\left[(\langle\psi|)^* Y^{\otimes n}\right] \bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} |\psi\rangle &= (\langle\psi|)^* \left(\bigotimes_{k \ni j_k=0} Y_k \right) \left(\bigotimes_{l \ni j_l=1} Y_l \tilde{Z}_l \right) |\psi\rangle \\ &= (\langle\psi|)^* \left(\bigotimes_{k \ni j_k=0} Y_k \right) \left(\bigotimes_{l \ni j_l=1} Y_l T_l Y_l T_l^{-1} \right) |\psi\rangle,\end{aligned}$$

where $T_l \in \mathrm{GL}(2, \mathbb{C})$ and the second line uses the result of Lemma 5.6.1. In the notation for tensor products used above, where not all of the qubits are encompassed by the index, it is assumed that an identity operator acts on any qubits whose index is not encompassed. Now, we use Equation 5.50 to rewrite $Y_l T_l Y_l$, resulting in

$$\begin{aligned}\left[(\langle\psi|)^* Y^{\otimes n}\right] \bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} |\psi\rangle &= (\langle\psi|)^* \left(\bigotimes_{k \ni j_k=0} Y_k \right) \left(\bigotimes_{l \ni j_l=1} \det(T_l) \left(T_l^{-1}\right)^T T_l^{-1} \right) |\psi\rangle \\ = \left[\prod_{p \ni j_p=1} \det(T_p) \right] (|\psi\rangle)^T \left(\bigotimes_{m \ni j_m=1} T_m^{-1} \right)^T \left(\bigotimes_{k \ni j_k=0} Y_k \right) \left(\bigotimes_{l \ni j_l=1} T_l^{-1} \right) |\psi\rangle \\ = \left[\prod_{p \ni j_p=1} \det(T_p) \right] \left(\bigotimes_{m \ni j_m=1} T_m^{-1} |\psi\rangle \right)^T \left(\bigotimes_{k \ni j_k=0} Y_k \right) \left(\bigotimes_{l \ni j_l=1} T_l^{-1} |\psi\rangle \right), \qquad (5.76)\end{aligned}$$

where we broke up the tensor product over the indices with $\tilde{Z}$ operators acting, and realised that $(\langle\psi|)^* = (|\psi\rangle)^T$. Defining

$$|v\rangle = \left(\bigotimes_{l \ni j_l=1} T_l^{-1} |\psi\rangle \right) \qquad (5.77)$$

allows us to rewrite Equation (5.76) as

$$\begin{aligned}\left[(\langle\psi|)^* Y^{\otimes n}\right] \bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} |\psi\rangle &= \left[\prod_{p \ni j_p=1} \det(T_p) \right] (\langle v|)^* \left(\bigotimes_{k \ni j_k=0} Y_k \right) |v\rangle \\ &= \left[\prod_{p \ni j_p=1} \det(T_p) \right] (\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle,\end{aligned}$$

where the last line above uses the more standard Kronecker product notation in which all of the qubit indices are incorporated. Notice that $\left[\prod_{p \ni j_p=1} \det(T_p)\right] (\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{1-j_k}\right) |v\rangle$

is just a complex number, so we can write

$$(\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle = a \in \mathbb{C} \tag{5.78}$$

Taking the transpose of both sides of (5.78) gives us

$$\begin{aligned}
\left[(\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle \right]^T &= [|v\rangle]^T \left[\left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) \right]^T [(\langle v|)^*]^T \\
&= (\langle v|)^* \bigotimes_{k=0}^{n-1} \left(Y_k^{j_k+1} \right)^T |v\rangle \\
&= (\langle v|)^* \bigotimes_{k=0}^{n-1} \left((-1)^{j_k+1} Y_k^{j_k+1} \right) |v\rangle \text{ (using } Y^T = -Y) \\
&= (-1)^{\sum_{l=0}^{n-1}(j_l+1)} (\langle v|)^* \bigotimes_{k=0}^{n-1} Y_k^{j_k+1} |v\rangle \\
&= (-1)^{n+\sum_{l=0}^{n-1} j_l} (\langle v|)^* \bigotimes_{k=0}^{n-1} Y_k^{j_k+1} |v\rangle \qquad (5.79) \\
&= a^T \\
&= a. \qquad (5.80)
\end{aligned}$$

Equations (5.78), (5.79) and (5.80) imply that

$$(-1)^{n+\sum_{l=0}^{n-1} j_l} (\langle v|)^* \bigotimes_{k=0}^{n-1} Y_k^{j_k+1} |v\rangle = (\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle. \tag{5.81}$$

Now $\sum_{l=0}^{n-1} j_l$ is precisely the Hamming weight of j, while n is the number of qubits. If one of these numbers is odd and the other is even, then the sum of the two is odd, meaning that $-1^{n+\sum_{l=0}^{n-1} j_l} = -1$ and thus implying that

$$-(\langle v|)^* \bigotimes_{k=0}^{n-1} Y_k^{j_k+1} |v\rangle = (\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle, \tag{5.82}$$

which is only possible if $(\langle v|)^* \left(\bigotimes_{k=0}^{n-1} Y_k^{j_k+1} \right) |v\rangle = 0$. □

We are now ready to use the conditions (5.65) to test some quantum pure states for SLOCC-equivalence to graph states. We will consider two examples of three-qubit

pure states, both of which are to be tested for SLOCC-equivalence against the three-qubit linear graph state $|g_3\rangle$, which is SLOCC-equivalent to the three-qubit GHZ state. The first of these pure states is a SLOCC-converted W state, which we know from [16] is SLOCC-inequivalent to the three-qubit linear graph (since the latter is in the GHZ class), and the second is a SLOCC-converted GHZ state.

Example 5.6.3. SLOCC-converted W state. Suppose we choose the three-qubit SLOCC operator

$$S = S_0 \otimes S_1 \otimes S_2, \tag{5.83}$$

where

$$S_0 = \frac{1}{2}\sqrt{\frac{3}{1097}}\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} \tag{5.84}$$

$$S_1 = \begin{bmatrix} 1 & 4 \\ -2 & 1 \end{bmatrix} \tag{5.85}$$

$$S_2 = \begin{bmatrix} 6 & -3 \\ 2 & 7 \end{bmatrix}, \tag{5.86}$$

chosen arbitrarily, with the mysterious looking prefactor in the definition of S_0 ensuring that the SLOCC-transformed W state remains normalised. The three-qubit W state is given in the computational basis by

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right). \tag{5.87}$$

Define the pure state to be tested as

$$\begin{aligned} |\psi\rangle &= S|W\rangle \\ &= \frac{1}{\sqrt{1097}}\left(\frac{33}{2}|000\rangle + \frac{19}{2}|001\rangle - 6|010\rangle - 10|011\rangle - \frac{3}{2}|100\rangle - \frac{9}{2}|101\rangle - 24|110\rangle\right), \end{aligned}$$

which leads directly to

$$(\langle\psi|)^* Y^{\otimes 3} = \frac{i}{\sqrt{1097}}\left(-24\langle 001| - \frac{9}{2}\langle 010| + \frac{3}{2}\langle 011| - 10\langle 100| + 6\langle 101| - \frac{19}{2}\langle 110| + \frac{33}{2}\langle 111|\right).$$

We now wish to test the state $|\psi\rangle$ for SLOCC-equivalence to the three-qubit linear cluster state

$$|g_3\rangle = \frac{1}{2\sqrt{2}}\left(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle + |111\rangle\right). \tag{5.88}$$

Let us define

$$\tilde{Z}_i = \begin{bmatrix} a_{i00} & a_{i01} \\ a_{i10} & -a_{i00} \end{bmatrix}, i \in \{0,1,2\}. \tag{5.89}$$

The requirement $\tilde{Z}_i^2 = I_i^{(2)}$ gives the three constraints

$$a_{i00}^2 + a_{i01}a_{i10} = 1, i \in \{0,1,2\}. \tag{5.90}$$

Since the number of qubits is odd, the necessary conditions from Equation (5.65) that are not automatically satisfied are the ones in which an odd number of $\tilde{Z}$ operators appear, namely

$$(\langle\psi|)^* Y^{\otimes 3}\left(\tilde{Z}_0 \otimes I_1^{(2)} \otimes I_2^{(2)}\right)|\psi\rangle = 0 \tag{5.91}$$

$$(\langle\psi|)^* Y^{\otimes 3}\left(I_0^{(2)} \otimes \tilde{Z}_1 \otimes I_2^{(2)}\right)|\psi\rangle = i \det S_0 \tag{5.92}$$

$$(\langle\psi|)^* Y^{\otimes 3}\left(I_0^{(2)} \otimes I_1^{(2)} \otimes \tilde{Z}_2\right)|\psi\rangle = 0 \tag{5.93}$$

$$(\langle\psi|)^* Y^{\otimes 3}\left(\tilde{Z}_0 \otimes \tilde{Z}_1 \otimes \tilde{Z}_2\right)|\psi\rangle = 0, \tag{5.94}$$

where the Pauli stabiliser element of $|g_3\rangle$ composed purely of local X and Y operators up to a constant is $-Y_0 \otimes X_1 \otimes Y_2$. Thus, we have 7 necessary conditions to be checked, and we can use Mathematica to do this. Constraints (5.91), (5.92) and (5.93) are linear equations in the unknown $a_{ijk} \in \mathbb{C}$, so we can use them first to eliminate three of the nine unknown complex quantities. It turns out that there is a unique way to eliminate a_{000}, a_{100} and a_{200}, which is given by

$$\begin{aligned} a_{000} &= \frac{1}{2}a_{001} - \frac{1}{2}a_{010} \\ a_{100} &= \frac{-1097}{480}\det(S_0) + a_{101} - \frac{1}{4}a_{110} \\ a_{200} &= -\frac{1}{6}a_{201} + \frac{3}{2}a_{210}. \end{aligned}$$

Backsubstituting these solutions into the conditions allows Mathematica to use the constraints (5.90) to eliminate a_{001}, a_{101} and a_{201}, and it reports eight different possible reductions for these parameters. However, none of them are compatible with Equation (5.94) when $\det(S_0) \neq 0$, thereby ensuring that $|\psi\rangle$ is SLOCC-inequivalent to $|W\rangle$.

Example 5.6.4. SLOCC-converted GHZ state. Suppose we choose the three-qubit SLOCC operator

$$S = S_0 \otimes S_1 \otimes S_2, \tag{5.95}$$

where

$$S_0 = \sqrt{\frac{2}{9319}} \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} \tag{5.96}$$

$$S_1 = \begin{bmatrix} 1 & 4 \\ -2 & 1 \end{bmatrix} \tag{5.97}$$

$$S_2 = \begin{bmatrix} 6 & -3 \\ 2 & 7 \end{bmatrix}. \tag{5.98}$$

Once again the prefactor in the definition of S_0 was chosen in order for $|\psi\rangle = S|g_3\rangle$, where $|g_3\rangle$ is again the three-qubit linear cluster state, to be normalised. We have

$$\begin{aligned} |\psi\rangle &= S|g_3\rangle \\ &= \frac{1}{\sqrt{9319}}\left(-\frac{27}{2}|000\rangle + \frac{47}{2}|001\rangle - \frac{27}{2}|010\rangle - \frac{49}{2}|011\rangle \right. \\ &\quad \left. -69|100\rangle + 49|101\rangle - 24|110\rangle + 8|111\rangle\right) \end{aligned}$$

and

$$\begin{aligned} (\langle\psi|)^* Y^{\otimes 3} &= \frac{i}{\sqrt{9319}}(8\langle 000| - 24\langle 001| + 49\langle 010| + 69\langle 011| \\ &\quad -\frac{49}{2}\langle 100| + \frac{27}{2}\langle 101| - \frac{47}{2}\langle 110| - \frac{27}{2}\langle 111|\Big). \end{aligned} \tag{5.99}$$

The necessary conditions to be satisfied are precisely the same as (5.90), (5.91),(5.92), (5.93) and (5.94) from Example 5.6.3. Solving first Equations (5.91), (5.92) and (5.93), then (5.94) and finally (5.90) is easy for Mathematica, and many solutions are possible. The fact that the solutions for the $\tilde{Z}_i$ operators in this case are not unique may turn out to be important in the construction of sufficient conditions for determining SLOCC-equivalence based on the methods presented in this thesis. This point will be further discussed in Chapter 6. One possible set of solutions provided by Mathematica is Since a solution has been found, the test is inconclusive and it is not immediately possible to say whether $|\psi\rangle$ and $|g_3\rangle$ are SLOCC-equivalent. Since it is already known from [16] that these two states are SLOCC-equivalent, the fact that the conditions (5.65) are satisfiable in this case is desirable. Since a known set of $\tilde{Z}$ operators satisfy the necessary conditions for SLOCC-equivalence, one could in principle use the relationship $\tilde{Z}_i = S_i Z S_i^{-1}$ to fix two of the four free parameters in S_i, and then attempt to solve for the other parameters by brute force.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The goal of this research was to provide an efficiently evaluable set of necessary and sufficient conditions for the equivalence of a pure quantum state $|\psi\rangle$ and a graph state $|g\rangle$ under SLOCC. In equation (5.65), a necessary set of conditions was provided. Many of these multivariate polynomial conditions are easier to evaluate than those required in a brute-force determination of SLOCC-equivalence as described in Section 3.5, due to the fact that they are of lower degree. For example, consider the case in which $|\psi\rangle$ and $|g\rangle$ are defined on n qubits. Evaluation of the conditions

$$|\psi\rangle = \bigotimes_{i=0}^{n-1} S_i |g\rangle \tag{6.1}$$

requires the solution of a system of 2^n multivariate polynomial equations of degree n in $4n$ unknowns; one complex equation for each coefficient of $|\psi\rangle$ and four complex unknowns for each operator S_i. This set of conditions is both necessary and sufficient for SLOCC-equivalence. By constrast, the conditions

$$(\langle\psi|)^* Y^{\otimes n} \bigotimes_{i=0}^{n-1} \tilde{Z}_i^{j_i} |\psi\rangle = \delta_{j,l}, \tag{6.2}$$

precisely as defined in equation (5.65), is necessary although not sufficient for the SLOCC-equivalence desired. However, the degree of many of the equations to be solved is reduced. For example there are $\begin{pmatrix} n \\ k \end{pmatrix}$ polynomial conditions of degree k that need to be satisfied, where k is of the same parity as n, i.e. $(-1)^n = (-1)^k$. In particular, if n is odd, there are n linear conditions ($k = 1$). If any of these conditions are violated, then SLOCC-

inequivalence is guaranteed. Therefore, there is a good chance of detecting SLOCC-inequivalence quite easily using these conditions. Solving these conditions also puts constraints on the SLOCC operators that connect $|\psi\rangle$ and $|g\rangle$, and these constraints can be used to simplify the brute-force version of the problem. Specifically, the constrained S_i operators can be used in equation (6.1), hopefully reducing the difficulty of the problem. This analysis of the efficiency of analysing SLOCC-equivalence using the conditions (5.65) is quite preliminary, and a more detailed analysis should be carried out in the event that a set of sufficient conditions for SLOCC-equivalence is found using the principles of this thesis.

6.2 Future Work

6.2.1 Sufficient conditions for SLOCC-equivalence

An obvious direction of future work is to extend the necessary conditions (5.65) for SLOCC-equivalence between a graph state and a pure state into a set of efficiently evaluable necessary conditions for the same. Such conditions would give rise to a hopefully efficient algorithm by means of which SLOCC-equivalence between graph states and arbitrary pure states could be tested. In Equation (5.61), we inserted a specific choice for the Pauli stabiliser element σ_j of the graph state that was composed specifically of Pauli-X and Y operators, in order to remove the $\mathcal{O}_{jk}$ operators from the conditions. The complete specification of an n-qubit graph state $|g\rangle$, however, requires n independent separable Pauli operators that generate the entire Pauli stabiliser to be given. This is presumably the reason that the conditions (5.65) are necessary but insufficient to guarantee SLOCC-equivalence of $|g\rangle$ and the pure state $|\psi\rangle$ of Equation (5.61). In fact, a larger number of conditions can be obtained by using any of the other elements $\sigma_j \in stab_{\mathcal{G}_n}(g)$ in equation (5.61).

Example 6.2.1. Consider Example 5.5.6 once again. We had

$$\langle\phi| = \frac{1}{\det(S_0)} \left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \bigotimes_{i=0}^{2} S_i Y_i \sigma_{ij} S_i^{-1}, \tag{6.3}$$

and we inserted $\sigma_i = -Y_0 \otimes X_1 \otimes Y_2$ in order to simplify this. However, we could also have inserted $\sigma_i = -Y_0 \otimes Y_1 \otimes Z_2$, which would instead give us

$$\begin{aligned} \langle\phi| &= \frac{1}{\det(S_0)} \left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(-S_0 Y_0 Y_0 S_0^{-1} \otimes S_1 Y_1 Y_1 S_0^{-1} \otimes S_2 Y_2 Z_2 S_2^{-1}\right) \\ &= \frac{1}{\det(S_0)} \left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(-I_0^{(2)} \otimes I^{(1)} \otimes i\tilde{X}_2\right). \end{aligned}$$

In this case, Equations (5.49) can be written as

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(I_0^{(2)} \otimes I_1^{(2)} \otimes \tilde{X}_2\right) = -i\det(S_0) \tag{6.4}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(I_0^{(2)} \otimes I_1^{(2)} \otimes \tilde{Y}_2\right) = 0 \tag{6.5}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(I_0^{(2)} \otimes \tilde{Z}_1 \otimes \tilde{X}_2\right) = 0 \tag{6.6}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(I_0^{(2)} \otimes \tilde{Z}_1 \otimes \tilde{Y}_2\right) = 0 \tag{6.7}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(\tilde{Z}_0 \otimes I_1^{(2)} \otimes \tilde{X}_2\right) = 0 \tag{6.8}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(\tilde{Z}_0 \otimes I_1^{(2)} \otimes \tilde{Y}_2\right) = 0 \tag{6.9}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(\tilde{Z}_0 \otimes \tilde{Z}_1 \otimes \tilde{X}_2\right) = 0 \tag{6.10}$$

$$\left(\langle\psi|\right)^* (Y_0 \otimes Y_1 \otimes Y_2) \left(\tilde{Z}_0 \otimes \tilde{Z}_1 \otimes \tilde{Y}_2\right) = 0. \tag{6.11}$$

Perhaps an optimally efficient test of SLOCC-equivalence can be formulated by selecting elements from the set of necessary conditions such as these in order to form a minimal set of necessary and sufficient conditions. Alternatively, perhaps an even smaller set of efficiently evaluable conditions can be found using the ideas presented in this thesis, or some other ideas, that constitute a sufficient but not necessary set of conditions; this too would be sufficient for creating an algorithm for testing SLOCC-equivalence.

6.2.2 Application to Measurement-Based Quantum Computing

One important application of graph states is to measurement-based quantum computation (MBQC), a distinct model of quantum computing from the circuit model. At least one specific scheme for MBQC, one-way quantum computing (1WQC), has been shown to be equivalently powerful to the circuit model, in the sense that a MBQC computer can efficiently simulate the action of a circuit model quantum computer, and vice-versa [34]. In the MBQC model, computation proceeds as follows:

1. An entangled state, known as a resource state, is created. The configuration of the resource state is tailored to the specific algorithm to be executed.

2. An effective quantum gate is applied to a qubit by means of measurements on the qubit and classical 'feed-forward' of the measurement result.

In MBQC, an initial amount of entanglement is supplied (the resource state), and this entanglement is gradually exhausted by means of measurements until the desired output is achieved. Once the resource state has been created, no further entangling operations are necessary; this is a major advantage of the MBQC model over the circuit model. However, there is a tradeoff, as the entangled resource states necessary for universal MBQC are not trivial to produce.

The first major event in the development of MBQC was the invention by Daniel Gottesman and Isaac Chuang of a probabilistic gate teleportation algorithm similar in spirit to the one from Example 2.5.2 [35]. Variations on this algorithm led to the development of MBQC schemes designed for linear optical implementations [36, 37]. Currently, the best known model for MBQC is *one-way quantum computation* (1WQC), first proposed by Robert Raussendorf and Hans Briegel in 2001 [38]. The name refers to the fact that the model begins with a massive, highly entangled resource state, and the entanglement is used up as the computation proceeds; since there is no entangling gate as

a basic element of 1WQC, the computation is irreversible. This computational model has been proven to have the same computational power as the circuit model [34]. The resource state used in this scheme is called a *cluster state*, which is an instance of a graph state. Examples of the underlying graphs corresponding to one-dimensional and two-dimensional cluster states can be found in Figure 4.1. The measurement patterns that implements the controlled-not or CNOT gate and the arbitrary single-qubit rotation operation $R(\zeta, \eta, \xi) = R_x(\zeta) R_z(\eta) R_x(\xi)$ in the 1WQC scheme can be found in [34]. It has been shown [39] that any sequence of unitary operations on any number of qubits can be expressed purely in terms of CNOT and $R(\zeta, \eta, \xi)$ operators, and therefore, the 1WQC scheme can execute an arbitrary unitary operation. The essential idea is that the measurements are used to teleport the qubits through a gate, as described in Example 2.5.2, in which the gate $R_z(\xi)$ was implemented by means of a judiciously chosen measurement. The implementation of the CNOT gate (or any other true two-qubit gate) requires a two-dimensional cluster state.

A cluster state can be constructed by creating the initial unentangled state $|\psi_{init}\rangle = \bigotimes_i |+\rangle_i$ with each qubit in the state $|+\rangle$ and then applying the CZ-gate from Section 2.3 between all pairs of qubits whose representative vertices in the cluster state graph are connected by edges. An experimental scheme for performing the global entangling operation necessary for producing a cluster state was given in [40] and demonstrated in [41], using collisional interactions in a Bose-Einstein condensate loaded into an optical lattice. However, a cluster state generated in such a dynamical way is likely to be unstable. A different, more passive approach is to cool down a system described by a Hamiltonian $\mathcal{H}$ whose non-degenerate ground state is a cluster state. Unfortunately, it has been proven that no graph state can be the non-degenerate ground state of any Hamiltonian featuring at most two-body interactions [42, 17]. A large body of work has emerged in recent years in an attempt to generate stable resource states, possibly cluster

states but possibly alternative resources, that are suitable for MBQC. Some approaches that have been considered are based on projected entangled pair states or valence bond states [43, 44], the so-called 'gadget construction' [45, 46, 47], matrix product states [48] and using a chain of three-level spin systems [49].

The original motivation of the novel research presented in Chapter 5 of this thesis was also to explore the possibility of universal MBQC using alternative resource states. Specifically, the class of resources that were to be considered was the set of states that are SLOCC-equivalent to cluster states. It stands to reason that a pair of quantum states that are SLOCC-equivalent can be used to perform the same set of quantum information processing tasks, and it could in principle be possible for a SLOCC-transformed cluster state to be the non-degenerate ground state of a physically realisable Hamiltonian. The teleportation of the gate that effects the single-qubit rotation $R_z(\xi)$ from Example 2.5.2 is at the heart of 1WQC. This algorithm corresponds precisely to entangling an input state $|\psi\rangle$ with a 'one-qubit cluster state' $|+\rangle$ to produce the state $|\psi_{in}\rangle = \mathrm{CZ}(|\psi\rangle \otimes |+\rangle)$ and then performing a projective measurement in the ξ-basis defined by

$$\begin{aligned} M_0 &= |\xi_+\rangle\langle\xi_+| \\ M_1 &= |\xi_-\rangle\langle\xi_-|, \end{aligned}$$

on the first qubit of $|\psi_{in}\rangle$, where $|\xi_+\rangle$ and $|\xi_-\rangle$ are defined in Equation (2.35). It can also be executed on the SLOCC-transformed state

$$|\psi'_{in}\rangle = S|\psi_{in}\rangle$$

where S is a SLOCC operator, replacing the projective measurement with a POVM for which the measurement operators $\{M_i\}$ satisfy

$$\begin{aligned} M_0 &= S|\xi_+\rangle\langle\xi_+|S^{-1} \\ M_1 &= S|\xi_-\rangle\langle\xi_-|S^{-1} \\ M_2^\dagger M_2 &= I^{(2)} - M_0^\dagger M_0 - M_1^\dagger M_1. \end{aligned}$$

This time, the teleportation is probabilistic, as the procedure fails should the measurement outcome corresponding to measurement operator M_2 be obtained. This POVM can be translated into projective measurements on a higher dimensional Hilbert space using Neumark's theorem [13]. It should also be possible to design POVM measurement schemes to implement a probabilistic arbitrary single-qubit rotation, and a probabilistic two-qubit entangling gate on a SLOCC-transformed two-dimensional cluster. It would be interesting to try and find a scheme that allows these gates to be executed with a probability arbitrarily close to unity, similar to what Knill, Laflamme and Milburn did for the probabilistic gate teleportation algorithm of Gottesman and Chuang [36, 35].

Bibliography

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pp. 212–219, 1996.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, p. 1484, 1997.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21 (2), pp. 120–126, 1978.

[4] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, pp. 467–488, 1982.

[5] S. Lloyd, "Universal quantum simulators," *Science*, vol. 273, pp. 1073–1078, 1996.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ch. 1, pp. 13–16. Cambridge University Press, 2000.

[7] O. Stern and W. Gerlach, "Der experimentelle nachweis der richtungsquantelung im magnetfeld (the experimental evidence of direction quantisation in the magnetic field)," *Zeitschrift für Physik*, vol. 9, pp. 349–352, 1922.

[8] J. J. Sakurai, *Modern Quantum Mechanics*, ch. 3, pp. 174–181. Addison-Wesley, 1994.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ch. 2, pp. 98–108. Cambridge University Press, 2000.

[10] J. S. Bell and A. Aspect, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*, ch. 2, pp. 14–21. Cambridge University Press, 2004.

[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ch. 1, pp. 17–27. Cambridge University Press, 2000.

[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ch. 2, pp. 80–97. Cambridge University Press, 2000.

[13] A. Peres, "Neumark's theorem and quantum inseparability," *Foundations of Physics*, vol. 20, pp. 1441–1453, 1990.

[14] G. Vidal, "Entanglement monotones," *J. Mod. Opt.*, vol. 47 (2-3), p. 355, 2000.

[15] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure-state entanglement," *Phys. Rev. A*, vol. 63, p. 012307, 2000.

[16] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Phys. Rev. A*, vol. 62, p. 062314, 2000.

[17] M. Van den Nest, K. Luttmer, W. Dür, and H. J. Briegel, "Graph states as ground states of many-body spin-1/2 hamiltonians," *Phys. Rev. A*, vol. 77, p. 012301, 2008.

[18] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Phys. Rev. A*, vol. 53, pp. 2046–2052, 1996.

[19] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," *Phys. Rev. A*, vol. 57, pp. 1619–1633, 1998.

[20] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A*, vol. 61, p. 052306, 2000.

[21] N. R. Wallach, "The hilbert series of measures of entanglement for four qubits," *Acta Appl. Math.*, vol. 86, pp. 203–220, 2005.

[22] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," *Lecture Notes in Computer Science*, vol. 1807, pp. 392–407, 2000.

[23] D. Gottesman, *Stabilizer Codes and Quantum Error Correction.* PhD thesis, California Institute of Technology, 1997.

[24] J. A. Gallian, *Contemporary Abstract Algebra.* Houghton Mifflin, 6 ed., January 2005.

[25] G. B. Arfken and H.-J. Weber, *Mathematical Methods for Physicists*, ch. 4, pp. 237–242. Elsevier Academic, 2005.

[26] B. Bollobs, *Modern Graph Theory.* Springer, 1998.

[27] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, "Entanglement in graph states and its applications," *arXiv: quant-ph/0602096*, 2006.

[28] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *arXiv: quant-ph/0111080v1*, 2001.

[29] J. Briët, "Entanglement and stabilizers," Master's thesis, University of Calgary, 2006.

[30] J. Johnson and M. Püschell, "In search of the optimal walsh-hadamard transform," in *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, vol. 6, pp. 3347–3350, 2000.

[31] R. Jozsa, "An introduction to measurement based quantum computation," *arXiv: quant-ph/0508124v2*, 2005.

[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ch. 10, pp. 445–452. Cambridge University Press, 2000.

[33] M. Van den Nest, J. Dehaene, and B. De Moor, "Graphical description of the action of local clifford transformations on graph states," *Phys. Rev. A*, vol. 69, p. 022316, 2004.

[34] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Phys. Rev. A*, vol. 68, p. 022312, 2003.

[35] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, 1999.

[36] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, pp. 46–52, 2001.

[37] N. Yoran and B. Reznik, "Deterministic linear optics quantum computation with single photon qubits," *Phys. Rev. Lett.*, vol. 91, p. 037903, 2003.

[38] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Phys. Rev. Lett.*, vol. 86, pp. 5188–5191, 2001.

[39] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, pp. 3457–3467, 1995.

[40] D. Jaksch, H. J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller, "Entanglement

of atoms via cold controlled collisions," *Phys. Rev. Lett.*, vol. 82, pp. 1975–1978, 1999.

[41] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch, "Controlled collisions for multi-particle entanglement of optically trapped atoms," *Nature*, vol. 425, pp. 937–940, 2003.

[42] M. A. Nielsen, "Cluster-state quantum computation," *arXiv: quant-ph/0504097*, 2005.

[43] F. Verstraete and J. I. Cirac, "Valence-bond states for quantum computation," *Phys. Rev. A*, vol. 70, p. 060302, 2004.

[44] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, "Valence bond ground states in isotropic quantum antiferromagnets," *Commun. Math. Phys.*, vol. 115, pp. 477–528, 1988.

[45] S. D. Bartlett and T. Rudolph, "A simple 2-local hamiltonian system for which the ground state is a universal resource for quantum computation," *Phys. Rev. A*, vol. 74, p. 040302(R), 2006.

[46] J. Kempe, A. Kitaev, and O. Regev, "The complexity of the local hamiltonian problem," *SIAM J. Comput.*, vol. 35, pp. 1070–1097, 2006.

[47] R. Oliveira and B. M. Terhal, "The complexity of quantum spin systems on a two-dimensional square lattice," *arXiv: quant-ph/0504050*, 2005.

[48] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, "Measurement-based quantum computation beyond the one-way model," *Phys. Rev. A*, vol. 76, p. 052315, 2007.

[49] G. K. Brennen and A. Miyake, "Measurement-based quantum computer in the

gapped ground state of a two-body hamiltonian," *Phys Rev Lett*, vol. 101, p. 010502, 2008.