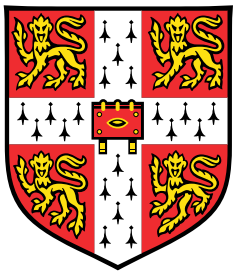
Quantum Information Processing using the Power-of-SWAP

Generation, Characterization and Application of Quantum Entanglement in Physical Systems with $SWAP^{1/n}$ Gates



Mrittunjoy Guha Majumdar

Department of Physics
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Christ's College

November 2018

I would like to dedicate this thesis to my loving parents *Rupendra Guha Majumdar* and *Karabi M. G. Majumdar*, and my brother *Tirthankar Guha Majumdar*.

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 60,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Mrittunjoy Guha Majumdar
November 2018

Acknowledgements

I would like to acknowledge the unmatchable support and guidance from my PhD supervisor Professor Crispin H. W. Barnes. His continued belief in me and the project played a key role in the completion of the project. I would also like to acknowledge the role played by my research group colleagues Dr. Edmund Owen, David Arvidsson-Shukur and Hugo Lepage, in terms of discussions on conceptual points and helping with simulations of some of the applications of Power-of-SWAP based quantum computing. I would also like to acknowledge the support and guidance given by Dr. Jacek Mosakowski and Dr. Alexei Andreev early in the project.

I would like to acknowledge the contribution of Niall Devlin and Yordan Yordanov. Yordan helped me with looking into one of the ways of finding the quantum vector states for Power-of-SWAP based quantum computing, while discussions with Niall were helpful in devising ways to characterize entanglement using permutation symmetries of states. I would also like to acknowledge the contributions of Sathyageeshwar Subrahmanian, Department of Applied Mathematics and Theoretical Physics (DAMTP), University of Cambridge, with whom I worked on the sections on studying the accessibility of quantum states using circuits comprising entirely of $SWAP^{1/n}$.

I would also like to acknowledge the contribution of my family and friends for being there with me during the highs and lows of this project, strong and steadfast in their support.

Abstract

This project is a comprehensive investigation into the application of the exchange interaction, particularly with the realization of the $SWAP^{1/n}$ quantum operator, in quantum information processing. We study the generation, characterization and application of entanglement in such systems. Given the non-commutativity of neighbouring $SWAP^{1/n}$ gates, the mathematical study of combinations of these gates is an interesting avenue of research that we have explored, though due to the exponential scaling of the complexity of the problem with the number of qubits in the system, numerical techniques, though good for few-qubit systems, are found to be inefficient for this research problem when we look at systems with higher number of qubits. Since the group of $SWAP^{1/n}$ operators is found to be isomorphic to the symmetric group S_n, we employ group-theoretic methods to find the relevant invariant subspaces and associated vector-states. Some interesting patterns of states are found including one-dimensional invariant subspaces spanned by W-states and the Hamming-weight preserving symmetry of the vectors spanning the various invariant subspaces. We also devise new ways of characterizing entanglement and approach the separability problem by looking at permutation symmetries of subsystems of quantum states. This idea is found to form a bridge with the entanglement characterization tool of Peres-Horodecki's Partial Positive Transpose (PPT), for mixed quantum states. We also look at quantum information task-oriented 'distance' measures of entanglement, besides devising a new entanglement witness in the 'engle'. In terms of applications, we define five different formalisms for quantum computing: the circuit-based model, the encoded qubit model, the cluster-state model, functional quantum computation and the qudit-based model. Later in the thesis, we explore the idea of quantum computing based on decoherence-free subspaces. We also investigate ways of applying the $SWAP^{1/n}$ in entanglement swapping for quantum repeaters, quantum communication protocols and quantum memory.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

> *"A classical computation is like a solo voice—one line of pure tones succeeding each other. A quantum computation is like a symphony—many lines of tones interfering with one another."*
>
> — Seth Lloyd

At a conference, in 1981, co-organised by MIT and IBM, Richard Feynman, in his famously irreverent way, urged the world to build a quantum computer. He said: *"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."* In the early twentieth century, quantum theory brought about a revolution, unmatched by most other contemporary ideas, besides Einstein's Relativity arguably. It had an elegant mathematical theory that explained the bizarre behaviour of subatomic particles. Although in 1932 John von Neumann [2] had encapsulated the basic elements of a nonrelativistic quantum theory in a coherent whole, it was Einstein, Podolsky, and Rosen (famously referred to, collectively, as EPR) [3] and Schrödinger [4] who first recognized what they referred to as *'spooky action at a distance'*, which later formed the backbone of Quantum Information Theory. Paradoxically, quantum entanglement, considered to be the most nonclassical manifestation of quantum mechanics, was used by Einstein, Podolsky, and Rosen in their attempt to ascribe values to physical quantities prior to measurement. It was Bell who showed that in fact it was entanglement which ruled such a possibility of a *hidden variable theory* out in 1964 [5]. He did this by positing his famous no-go theorem that if local hidden variables exist, experiments could be performed involving quantum entanglement where the result would satisfy a Bell inequality. However, *Aspect et al* [6] and *Kwiat et al* [7] found violations of these inequalities in experiments [8].

It wasn't until the last decade of the twentieth century that it was realised that the world of *quantumness* could be used to define and manipulate bits and logic operations in a computer. Quantum computation came into focus primarily after it was found that certain problems that could not be solved using classical algorithms or methods could be solved using quantum computation and algorithms, in far lesser time if a classical counterpart existed. A primary example of an early problem that was solved in this manner was that of factoring large numbers by Peter Shor using a quantum algorithm [9]. Today one has various methods in the domain of quantum algorithms to solve cryptosystems (such as the RSA cryptosystem) and even certain NP-hard problems. It has thus become clear that a quantum computer, once built, would be something to be reckoned with, and an extremely useful tool for computational purposes. In C. Altman's words, *"An omni-linked world populated with intelligent artifacts will bring sweeping changes to virtually every facet of modern life – from science and education to industry and commerce – leaving no segment of society unaffected by its advance".* Quantum computation may just be the most intelligent of them all, by quite a distance.

One may ask,

> *"What makes Quantum Mechanics a powerful tool for computational purposes?"*

One explanation is that the basis for computation is infinite-dimensional since quantum mechanics allows for superposition, constrained by normalization conditions. At the very foundation of this formalism (of quantum computation) is the quantum bit (or qubit) [10], which is a quantum system that, like an ordinary classical bit, has two accessible states (often denoted by $|0\rangle$ and $|1\rangle$) but, unlike an ordinary computer bit, could exist in a superposition of these two states:

$$\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \tag{1.1}$$

where α and β are probability amplitudes. There are two primary physical operations that can be performed on pure qubit states: operation by a quantum logic gate and measurement in standard basis. Mathematically, upon being operated by a quantum logic gate, the qubit undergoes a unitary transformation. Using standard basis measurement, information about the state of the qubit can be obtained.

The other key reason for the power of quantum mechanics for computation purposes is that qubits can display *entanglement*, which is an important distinguishing feature between a quantum bit and a classical bit. Entanglement is a nonlocal property which allows qubits to express higher correlations than in classical systems. Entanglement conditions allow

for subsystem manipulation of a quantum system such that multi-partite algorithms can be realized efficiently and quickly.

So, a key question is

> *"How much better is quantum computation better than its classical counterpart?"*

The answer to this question is still not known conclusively, just as is the case for the computing power of classical machines. This question has to be addressed on two fronts: qualitative and quantitative. Quantitatively, the answer has an unexpected form: *quantum-ness* and the computational tools associated with it do not speed up all tasks of information processing by a uniform amount [11]. Considering how the number of steps required to complete a computational task grows with the number of (quantum) bits involved, it is found that different computational tasks have different degrees of speed-up. Some tasks are not faster than their classical counterparts at all. An example of the same would be the computation task of finding the n^{th} iterate of a function $f(x)$: $f(f(...f(x)...))$. Some processes are moderately faster than their classical counterparts, such as search-algorithms for finding an element in a database of n entries [12], while certain other quantum computational processes are exponentially faster than their classical counterparts, such as Shor's algorithm for factoring an n-digit number [9].

Communication has both qualitative and quantitative improvements for the quantum case over the classical counterparts [13, 14]. For certain tasks there is a quadratic reduction of the amount of data communicated for the completion of the task, if quantum states are used rather than classical states [15]. For example, the *appointment scheduling problem* is one such case [16]:

> *Let Alice and Bob be the two users of the quantum computation process. Both are very busy but would like to meet up. They need to find a convenient time when they are both free for doing so. They each have a calendar, which we consider to be n-bit strings x (for Alice) and y (for Bob). If the calendar is free on day i, for Alice (Bob), then* $x_i = 1$ *(*$y_i = 1$*). Mathematically, Alice and Bob want to find a day such that* $x_i = y_i = 1$ *or establish that no such index exists.*

Kalyanasundaram and Schnitger [17] proved that the *appointment scheduling problem* requires at least *cn* classical bits of communication in the worst case, whereas *Burhman et al* [15] showed that this problem can be solved with the exchange of $c\sqrt{n}log(n)$ quantum bits

using Grover's search algorithm [12], where c is some real positive constant and sufficiently large n. For other computational tasks there is an exponential gap between the quantum model and its classical counterpart. One famous example of this is the *set disjointness problem* [18, 19] that relates to the allocation of non-overlapping sections of a shared memory in a distributed computation protocol:

> *Let W be a set of size n. Alice and Bob want to generate a pair of subsets (U,V), such that $U \subset W$ is known to Alice, $V \subset W$ is known to Bob, and the pair (U,V) is a random variable that is uniformly distributed on the set of all pairs with $|U| = |V| = \sqrt{n}$ and $|U \cap V| = 0$.*

Ambainis et al [19] showed that the *set disjointness problem* can be solved with the communication of only $O(log(n))$ quantum bits, while it can be done by any classical probabilistic protocols with communication of atleast $O(\sqrt{n})$ bits.

Last but not the least, there are tasks that are can be accomplished only using quantum models and that have no classical counterparts. One such computational task is *Quantum Cryptography*, which provides confidentiality of communication between parties that is impossible to be realized classically [20]. This is also true for winning strategies for some games, such as the *guessing games*, which can only be possible using quantum resources [21–24].

1.1 Physical Realization of Quantum Computation

Having looked into the manner in which quantum computing can make computational tasks and processes faster and qualitatively more efficient than classical counterparts, we need to look into the question of

> *"How can quantum information processing be physically realized?"*

According to David P. DiVincenzo [25], there are certain essential conditions for the realization for the physical realization of Quantum Computation:

> 1. *Well-characterized qubits and a scalable physical system*: Given the importance of the qubit as the fundamental building block of quantum information processing, the qubits in any physical realization should be well defined and characterized. A qubit is a two-level state, conventionally defined as $|0\rangle$ and $|1\rangle$. Any physical realization of

a quantum bit should have a well-defined separation of these two levels, which are usually related to distinct values of certain properties of the qubits (such as energy and polarization), and in case the qubit does have other levels, the physical process should be designed such that the probability of the system ever going into these level is infintesimal. Other physical parameters, including the internal Hamiltonian of the system, couplings between the states of the qubit and to external fields that are used for manipulations of the qubit, besides the interactions of the qubit with other qubits, must be known. There is a great variety of physical realizations of qubits that have been implemented, such as charge qubits [26–28], spin qubits [29–33] and flux qubits [34–36].

2. *Easy initialization of the state of the qubits to a simple fiducial state* $|000...\rangle$: Ease of implementation of a quantum computation is linked to the ease of initialization of the quantum bits used to a known value before the process. Qubits can be initialized using quantum operations [37–41], spin injection [42, 43], resonant coupling with a tunable environment [44] or measurements [45–51]. Processes such as microwave-induced cooling of superconducting qubits [52], Purcell filters [53], cooling the collective motion of trapped ions [54], production of photonic qubits using ultraviolet light impinged on β-Barium Borate (BBO) crystals [55], fine-structure splitting [56] and rapid electric-field ionization of a resonantly excited exciton [57] are some of the physical processes to initialize quantum bits in physical implementations of quantum computation. Certain kinds of implementations such as Nuclear Magnetic Resonance (NMR) cannot be a feasible implementation of quantum computation until the problem of the inability to cool macroscopic materials to their ground state (which is taken as the qubit $|0\rangle$) in bulk spin-resonance quantum computation is resolved [58, 59].

3. *Relevant Decoherence times longer than the gate operation time*: Decoherence is the physical phenomenon of qubits becoming entangled with their environment, thereby effectively 'collapsing' the state of the quantum computer to a definite quantum state [60–62]. Decoherence is significant in the domain of quantum physics as it is the principal mechanism for the emergence of classical behavior in quantum systems with the loss of *quantumness* [63]. As the quantum nature of the qubits and quantum computer is fundamental for the advantage of using them over their classical counterparts, presence of decoherence is counterproductive to an efficient implementation of quantum computation [64]. Thus, the time taken for decoherence to set in should be longer than the time taken for any unique quantum features or processes in a quantum

information process to be carried out. The decoherence time should be for the 'relevant' degrees of freedom for the computation; for instance, for a quantum computer that uses the spin-degree of freedom, decoherence in position or orbital of the qubit is not *relevant*. Since decoherence is very system-specific, caution has to be taken to gauge where exactly what kinds of timescales are involved. There have been a lot of experimental studies to study decoherence in physical systems. Michel Brune and his colleagues [60, 65] at Ecole Normale Supérieure performed experiments in which they manipulated electromagnetic fields into a Schrödinger-cat-like superposition state using rubidium atoms, in which they found two primary characteristic results: the fast evolution of the system comprising of the atoms and the measurement device towards a statistical mixture state during a measurement process, and faster rate of decoherence for greater distances between components of a multiparticle system. *Sackett et al* [66] used ion traps to study the decoherence of ions because of radiation. *Kokorowski et al* [67] studied the decoherence in spatially separated atomic superpositions due to spontaneous photonic scattering. Cheng and Raymer [68] found the averaged decoherence rate times for optical beams traversing dense, multiple-scattering dielectric media.

4. *Universality of accessible Quantum Gates*: Any quantum information process or algorithm is specified in terms of a sequence of unitary transformations acting on some of the qubits that comprise the quantum computer. This is usually no more than three qubits, as in the case of the Toffoli gate. The way this is usually done is to identify Hamiltonians that can generate these unitary transformations: $U = e^{\frac{iHt}{\hbar}}$, where t is the time of operation of the Hamiltonian H. Even though we would ideally like to be able to realize any random unitary transformation with a physical process, the number of such transformations accessible using a certain Hamiltonian related to the physical process is limited. The point that helps is that we need only a limited number of basic *universal* gates to realize all possible quantum operations.

DiVincenzo [69] gave a proof that showed that quantum gates operating on two (quantum) bits are sufficient to construct any general quantum circuit. *Barenco et al* [70] showed that a set of gates that consists of all one-qubit gates and the two-qubit CNOT gate $U_{CNOT} : U_{CNOT}(x,y) \rightarrow (x, x \oplus y)$ acting on qubits (x,y) is universal. But what happens if one has interactions in a physical system that cannot be shut off, such as certain two-body interactions in Nuclear Magnetic Resonance (NMR) Quantum Computing? In such cases one uses selective 'refocussing' sequences of the controllable interactions to correct for these stray interactions. *Leung et al* [71] presented a

scheme that couples any pair of spins in a hetero-nuclear spin system, and showed that in many systems, selective recoupling is possible, thereby presenting an instance of a refocussing sequence that can implemented efficiently.

Other problems, such as inability to turn on the desired interaction between a pair of qubits, arise in implementations of quantum computing. For example, no direct interaction is available between the ionic qubits in an ion-trap scheme in the ion-trap scheme [72–74]. In such cases, auxiliary quantum systems (or 'bus qubits') are introduced to work around this problem; for instance, the vibrational state of the ion chain in an ion-trap is used for mediating the 'interactions'. However, since each quantum system has a certain amount of decoherence associated with it, the introduction of such an auxiliary system leads to increasing decoherence, as seen in cavity-quantum electrodynamics and ion-trap schemes. Besides, quantum gates have random and systematic errors associated with the Hamiltonians used to implement them [75]. These are further sources of decoherence and can be corrected for, by error correction methods. The unreliability factor because of random errors is in the same vicinity as the decoherence threshold: the magnitude of random errors should be roughly $10^{-4} - 10^{-5}$ per gate operation for a successful implementation of a quantum information processing task [75–79]. For error correction, gate operations using coded qubits should be realizable. For most popular error correction techniques, the so-called 'stabilizer codes' are used. Stabilizer codes are used to ascertain the occurrence of an error and to determine the kind of error (such as bit flip or phase flip error) that may have taken place.

Definition 1.1. An $[n,k]$ stabilizer quantum error-correcting code has the encoding of k logical qubits into n physical qubits. The stabilizer S for the error-correcting code is an Abelian subgroup of the n-fold Pauli group Π_n: $S \subset \Pi_n$, which does not contain the operator the n-qubit identity operator: $-I \otimes n$. The simultaneous eigenspace +1 of the operators comprises the *codespace*.

Error-correcting codes have physical qubits that comprise logical qubits with the base-level quantum gates being the regular one-qubit and CNOT gates [80–83]. In some cases, such as in implementations of quantum error-correcting codes using quantum-dot [84, 85] or semiconductor impurities [86, 87], only two qubit gates are enough to implement general quantum computation when blocks of three or four qubits are used as logical qubits [88].

5. *Measurement*: The role of measurement of properties of a quantum particle is as important as the evolution of it, under the, or without the, influence of external quantum operations [45, 89]. The concept of quantum measurement is placed at the core of the problem of the interpretation of quantum mechanics [90, 63]. According to the Copenhagen interpretation, generally, any physical system does not have any definite properties before being measured, and quantum mechanics can only predict the probabilities with which a certain measurement will produce a particular result for the property for which the measurement was carried out [91, 92]. Practically, for any successful implementation of quantum computation, we require a qubit-specific measurement capability in the physical system.

Measurements can be of two-kinds: *strong* and *weak* measurement [45, 60, 93]. Quantum wave-function collapse due to measurement of observables associated with a quantum system is one of two processes by which such systems can evolve in time, with the the other process being the continuous evolution via the Schrödinger equation. One can avoid the collapse of the wavefunction using what is known as a *weak measurement*, which gives very little information about the state of the quantum system but also perturbs it very slightly, thereby not leading to the collapse of the wavefunction [94, 95]. Weak measurements have been used in precision metrology [96], for protecting entanglement from thermal noise [97] and quantum phase estimation [98].

A point of interest here is that while an efficiency of 100% is desired in any quantum computation, one can make-do with a lot less due to a trade-off between quantum efficiency and available resources. In general, if quantum efficiency ε is available for a computation with a single qubit, then copying it to more than $\frac{1}{\varepsilon}$ qubits and measuring all of these will result in a reliable outcome. So, a quantum efficiency of 5% would be usable for quantum computation if twenty copies are used of the same output qubit. Even with quantum efficiency lower than 1% one can have a successful quantum computation, such as in the bulk model of Nuclear Magnetic Resonance (NMR) Quantum Computing, with a macroscopic number of copies of the same quantum computer running simultaneously. The final measurement is done as an ensemble average over the whole sample.

6. The ability to interconvert stationary and flying qubits: Realization of an interface between stationary and flying qubits is required for distributed quantum computation and long-distance quantum communication [99]. While stationary qubits are often used

in scalable quantum computation, quantum communication research has largely been based on the use of single-photons as flying qubits that can carry quantum information over long distances. For such an application and quantum information processing task, the availability of a quantum interface between flying and stationary qubits is crucial, as is done in systems such as those with entanglement between a solid-state spin qubit and a photonic flying qubit [100–105]. The demonstration of spin–photon entanglement has enabled distant spin-based entanglement [106], unconditional quantum teleportation [107] and been used in quantum repeaters [108], besides being useful in helping connect few-qubit nodes in a quantum network [109, 110], such as the *Quantum Internet* [111].

7. The ability faithfully to transmit flying qubits between specified locations

Quantum Computing can be realized in a number of physical systems, following from DiVincenzo's criteria for a successful implementation of quantum computation. Quantum Computation has been realized in physical systems such as photonic systems [112–114], electron spins and quantum dots [115–118], nuclear spin [119–121], optical lattices [122–124], Josephson junctions [125, 126] and superconducting circuits [127, 128]. Irrespective of the physical system the quantum computing architecture is realized on, the important point on this front is to check whether the quantum computing thus realized is universal, and can be used for any general computation or information processing task. DiVincenzo's criteria give us a list of physical conditions for the successful realization while the universality conditions give us conditions relating to the '*software*' of this computing formalism.

1.2 Universality in Quantum Computation

It has been known for several years that the theory of quantum computers is fundamentally different from that of the classical theory of computation, which is essentially given by the theory of the universal Turing machine. We may identify three important differences. Firstly, the properties of quantum computers are not postulated *inabstracto* as in the case of classical Turing machines but are derived entirely from the laws of physics. One cannot capture the correct quantum theory by intuition alone, as was often done by pioneers in classical computation theory such as Turing, Godel and Church [129–131]. One cannot falsely assume that its foundations are self-evident or purely abstract.

Secondly, quantum computers can perform certain classical tasks, such as factorization such as the Shor's algorithm [9] and quantum search algorithms such as the one given by Grover [132] which have no classical analogues using similar number of resources. These algorithms and processes can be overwhelmingly more efficient than any known classical algorithm. Thirdly, quantum computers can perform new computational tasks, such as quantum cryptography [133–136], which are beyond the reach and scope of any classical computer. However, given that there seem to be a wide variety of things we can do with a quantum computer, the key point to be resolved is whether a system can realize all possible computations, in what is known as the *Universality* problem. The key question then is

"What makes a certain system capable of universal quantum computation?"

Computation can be thought of as the transformation and creation of symbols ('output') from other symbols ('input'), with these 'symbols' being physical objects here. A '*universal set of components*' would be one which is adequate for the construction of computers that can perform any physically possible computation, and a universal computer would be a single machine that can perform any physically possible computation. The three concepts of universality i.e. in the computers, in the components therein and the computation itself, are all closely linked, since if the solution to a computation problem could be created by a certain physical system (computer) but there was no systematic way to build that computer, then the solution would not be 'computable'. Moreover, for any universal computer, there has to be a universal set of components that is needed to build it.

These ideas are formally encapsulated in the Church-Turing hypothesis, which states that any real-world computation can be translated into an equivalent computation involving a Turing machine. David Deutsch asserted this as a physical principle in 1985 [137]:

> *Every finitely realizible physical system can be perfectly simulated by a universal model computing machine operating by finite means.*

The reason the realm of classical physics and Universal Turing Machines don't go well together is because the former is continuous while the latter is discrete. This is, however, not the case for quantum systems.

To understand how this happens, one has to understand that the idea of *computational equivalence* of two computers is fundamentally different for quantum computers due to the fact that even though input states fed into such a computer can be controlled, the act of measurement gives rise to a probabilistic outcome. Given this idiosyncratic property of

quantum systems, we say that any two quantum computing machines are computationally equivalent under given labellings (of 'input' and 'output') if in any possible experiment(s) in which their inputs are prepared equivalently under the 'input labellings', the measured values of the observables (corresponding to the 'output' labelling) for the two machines would be statistically indistinguishable and the probability distribution functions for the outputs from the two machines would be identical. Given two quantum computing machines a composite machine, whose set of computable functions contains the union of the computable functions of the individual computers, can be constructed. The question then is why cannot we just keep on taking such unions *ad infinitem* to realize all possible algorithms?

The answer lies not in logic but in physics. As Deutsch [137] put it, one soon reaches a point where adding additional hardware to a computing system does not alter the number of computable functions for the computer. Moreover, functions for computers that map real numbers to others, this set of functions is always a subset of the ones that can be realized using Turing Machines. All Turing Machine-computable functions are recursive functions, since they depend on each intermediate halting configuration of the system, and it is known that the set of recursive functions is denumerable and infinitely smaller than all the functions from real numbers to themselves.

The way around this is encapsulated in Deutsch's words 'by finite means'. If we think of the computing process happening in a sequence of steps who duration has a non-zero lower bound, then it operates 'by finite means' if

a) Only one finite subsystem of the system is in motion during any one step

b) The motion depends only on the state of a finite subsystem

c) The rule that specifies the motion of the subsystem(s) can be given in a finite manner, mathematically.

Turing machines are seen to satisfy these conditions, as do universal quantum computer, while classical computers do not since classical systems tend to be continuous and therefore the condition of a discrete input is not possible in that case.

1.2.1 Universal Quantum Computation using Heisenberg Hamiltonian and Exchange Interaction

The Heisenberg Hamiltonian is ubiquitous in condensed matter physics. Be it in spin chains [138–140], Kagome lattices [141, 142], ferromagnetic films [143] or intermolecular exchange interaction [144], the Heisenberg Hamiltonain has played a key role in various applications of condensed matter systems, including in quantum computing [115, 145, 25, 146]. Recent solid-state approaches to realize quantum computation have used quantum dots, nuclear spins and electron spins, many of which directly employ the Heisenberg Hamiltonian and exchange interaction [115, 25]. In architectures for circuit-based quantum computing, the basic two-qubit quantum gate can be generated by using a tunable exchange interaction between spins:

$$H = \sum_{i,j} J_{ij} S_i . S_j \tag{1.2}$$

while the one-qubit gates are realized using a controlled local magnetic field [147]. There is however a small problem in this method: compared to the Heisenberg operation, the one-qubit operations are a lot slower, and require much more materials and device complexity, thereby potentially contributing to an increase in the decoherence rate.

Universal Quantum Computation for the Heisenberg Hamiltonian, particularly using exchange interaction without local magnetic fields, was proposed by DiVincenzo et al [25]. In their proposal, the Heisenberg interaction alone is sufficient to implement any quantum computer circuit. However, this is done using encoded logical qubits: three qubit encoding for one-qubit gates and ten qubit encoding in two-qubit operations. Even though this architecture has lesser complexity than its counterparts that have single-qubit gates using local magnetic fields, the encoding does lead to a significant increase in resources needed for large multi-qubit cases.

In this project, we look into the kinds of computations that can be realized using a sequence of Power-of-SWAP gates on single qubits. The accessibility of the states and the entanglement generated therein using such circuits is explored and studied closely, besides the investigation and improvement of five different models of quantum computing using $SWAP^{1/n}$.

1.3 Non-Commutativity of $SWAP^{1/n}$ Gates and Group Theory

The $SWAP^{1/n}$ quantum gate has certain characteristics that make it interesting to study. One of the most important characteristic properties of this gate is that, unlike gates such as the CPHASE gate, combinations of the $SWAP^{1/n}$ gate are not commutative in general. There are two factors which particularly define the non-commutativity of combinations of $SWAP^{1/n}$ gates:

1. ***Kind of states***: Since the $SWAP^{1/n}$ gate only operates upon two-qubit states of the form

$$|\psi\rangle = \alpha|01\rangle + \beta|10\rangle; \alpha, \beta \in \mathbb{C} \tag{1.3}$$

For states of the form

$$|\psi'\rangle = \delta|00\rangle + \varepsilon|11\rangle; \delta, \varepsilon \in \mathbb{C} \tag{1.4}$$

the $SWAP^{1/n}$ gate does not change the state at all. Hence, wherever we have states with components that are of the latter form, the commutativity of states follows through.

For example, the state $|\psi\rangle_{in} = |000\rangle_{123}$ (where the subscripts denote the index number of the qubits) will have commutativity relation $[\sqrt{SWAP}_{12}, \sqrt{SWAP}_{23}] = 0$ and the order of operation of the $\sqrt{SWAP}$ on the first and second or second and third qubits is not important. The output state is always $|\psi\rangle_{out} = |000\rangle$.

2. ***Distance between qubits***: The distance between qubits for consecutive operations of $SWAP^{1/n}$ gates is very important. If these consecutive operations are on any common qubit(s), the non-commutativity of the $SWAP^{1/n}$ gate comes through.

For example, for the input state $|\psi\rangle_{in} = |010\rangle_{123}$, the following operations are considered:

$$\sqrt{SWAP}_{12}\sqrt{SWAP}_{23}|010\rangle \rightarrow \tfrac{i}{2}|010\rangle + \tfrac{1}{2}|100\rangle + \tfrac{1}{2}(1-i)|001\rangle$$

$$\sqrt{SWAP}_{23}\sqrt{SWAP}_{212}|010\rangle \rightarrow \tfrac{i}{2}|010\rangle + \tfrac{1}{2}(1-i)|100\rangle + \tfrac{1}{2}|001\rangle$$

which shows us that the commutative relation $[\sqrt{SWAP}_{12}, \sqrt{SWAP}_{23}] = 0$ is violated for this case.

However, for a state like $|\psi\rangle_{in} = |0101\rangle_{1234}$, consecutive operation of $\sqrt{SWAP}$ on non-common, unshared qubits such as the (12) and (34) leads to a commutation relation of the form $[\sqrt{SWAP}_{12}, \sqrt{SWAP}_{34}] = 0$

1.4 Entanglement and Separability

Often we are told that at the fundamental level of nature, one requires a quantum description of reality rather than a classical one. However, the meaning of this and all its possible implications are not trivial [148]. Mathematically, the possible pure states of a quantum system form a vector space, the Hilbert space H. Let us consider a multipartite quantum system consisting of n subsystems. As per the classical description of the system, the total pure state space of the system is given by the Cartesian product of the n subsystem spaces, which means that the total state is always a product state of the subsystems. However, in the quantum formalism, the total Hilbert space H is a tensor product of the subsystem Hilbert spaces: $H = \otimes_{l=1}^{n} H_l$. Then the superposition principle allows us to write the total state of the system as

$$|\psi\rangle = \sum_{i_1,\ldots,i_n} c_{i_1\ldots i_n} |i_1\rangle \otimes \ldots \otimes |i_n\rangle \tag{1.5}$$

which cannot in general be described as a product of states of individual subsystems $|\psi\rangle \neq |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$. Thus, it is not possible, in general, to assign a single state vector to any one of the subsystems. This effectively expresses the phenomenon of entanglement that, in contrast to the occurrence of classical superposition, allows us to create an exponentially large superposition with only a certain linear amount of physical resources.

In practice, one encounters mixed rather than pure states in nature. Entanglement of mixed states is no longer equivalent to being non-expressable as product of subsystem states, as in the case of pure states. Instead, one calls an n-qubit mixed state entangled if it cannot be written as a convex combination of product states [149]:

$$\rho \neq \sum_i p_i \rho_1^i \otimes \ldots \otimes \rho_1^n \tag{1.6}$$

where $\rho = |\psi\rangle\langle\psi|$ and the partial density matrix ρ_k can be found by tracing out all the qubits except the k^{th} qubit. Here p_i is the probability of finding the composite system in the state $\rho_1^i \otimes \ldots \otimes \rho_1^n$. The states that do not follow the condition in equation (2) are said to be *separable*. In practice, it is often difficult to decide if a given state is separable or not based

on this definition alone, in what comprises the separability problem, which will be discussed later in this chapter. The aforementioned definition is negative, since a state is said to be entangled if it cannot be written in the form in equation (2). Physically, the definition of an entangled state is usually made in terms of the physical resources needed for the preparation of that state [149]: a multipartite state is said to be entangled if it cannot be prepared from classical correlations using only local quantum operations. We also have a positive definition of entanglement proposed recently by *Masanes et al* [150], which defines the phenomenon in terms of the non-locality in quantum states rather than in terms of their preparation. For the set C of bipartite states that do not violate the Clauser-Horne-Shimony-Holt (CHSH) inequality with a single copy, even after stochastic local operations without communication, we have [150]

Theorem 1.1. A bipartite state σ is entangled if, and only if, there exists a state $\rho \in C$ such that $\sigma \otimes \rho$ is not in C.

Entanglement is important also because it is the basis for the idea of *decoherence*, the loss of quantum-ness, of a quantum particle due to entanglement with its environment. However, entanglement has lately been found to be a very specific type of quantum correlation. In this chapter, we will approach this topic via two distinct methods: one involving the use of the concept of *quantum discord* (and entanglement) while the other is using separability criterion for multipartite quantum systems.

1.4.1 The Separability Problem

The fundamental question in the theory of quantum correlations and entanglement is is which states are separable and which are not. The case for a pure bipartite system is simple: any bipartite pure state $|\psi_{AB}\rangle \in H_{AB} = H_A \otimes H_B$ is called separable only if it can be written as a product of two vectors corresponding to Hilbert spaces of the subsystems:

$$|\psi_{AB}\rangle = |\phi_A\rangle|\psi_B\rangle \tag{1.7}$$

If the quantum state $|\psi_{AB}\rangle$ is written in terms of an orthonormal product basis $\{|e_A^i\rangle \otimes |e_B^j\rangle\}$ as

$$|\psi_{AB}\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} A_{ij}^{\psi} |e_A^i\rangle \otimes |e_B^j\rangle \tag{1.8}$$

then it is a product only if the matrix of coefficients $\{A_{ij}^{\psi}$ has rank 1. More generally, the rank of this matrix: $r(\psi) \leq min[d_A, d_B]$ is called the Schmidt Rank of the vector ψ. This is

always equal to either of the ranks of the reduced density matrices: $\rho_A^\psi = Tr_B|\psi_{AB}\rangle\langle\psi_{AB}|$ and $\rho_B^\psi = Tr_A|\psi_{AB}\rangle\langle\psi_{AB}|$. There always exists a product basis $\{|\tilde{e}_A^i\rangle \otimes |\tilde{e}_B^j\rangle\}$ in which the vector can be expressed as

$$|\psi_{AB}\rangle = \sum_{i=0}^{r(\psi)} a_i |\tilde{e}_A^i\rangle \otimes |\tilde{e}_B^i\rangle \tag{1.9}$$

where the strictly positive numbers $a_i = \{\sqrt{p_i}\}$ correspond to the nonzero singular eigenvalues [110] of A^ψ, and p_i are the nonzero elements of the spectrum of either of the reduced density matrices.

For more practical cases, due to the presence of noise from the environment and decoherence, and the emergence of mixed quantum states from pure ones, we must study the separability of mixed states as well. Any bipartite state ρ_{AB} defined on Hilbert space $H_{AB} = H_A \otimes H_B$ is separable [149] only if it cannot be represented or approximated by states of the form

$$\rho_{AB} = \sum_{i=1}^{k} p_i \rho_A^i \otimes \rho_B^i \tag{1.10}$$

where ρ_A^i and ρ_B^i are defined on local Hilbert spaces H_A and H_B. Horodecki [151] showed that shown that any separable state on the Hilbert space $H = H_A \otimes H_B$ can be written as a convex combination of N pure product states with $N \leq (dim(H))^2$. Thus, the set of all separable states defined in this way is found to be convex, compact, and invariant under the product unitary operations $U_A \otimes U_B$.

However, the problem of determining whether a state ρ_{AB} is separable or not remains. In particular, the separable decomposition of the state may not have anything in common with the eigen-decomposition. So for instance, there are many separable states that have entangled or non-product eigenvectors.

1.4.2 Separability Criteria for Bipartite Case

There are a number of standard criterion for determining the separability of a quantum system in a bipartite case. In this sub-section we will discuss about the same, before moving onto an algorithm developed for this project to determine the separability class of a certain quantum state.

Density Matrices, PPT Criterion and Best Separable Approximation (BSA)

A quantum system consisting of two subsystems is separable if its density matrix can be written as

$$\rho = \sum_{ijkl} a_{kl}^{ij} |i\rangle\langle j| \otimes |k\rangle\langle l| \tag{1.11}$$

where states $|i\rangle$ and $|j\rangle$ are in the Hilbert Space H_A while $|k\rangle$ and $|l\rangle$ are in the Hilbert Space H_B for the composite system $H_A \otimes H_B$.

A necessary condition for separability of quantum states was given by Peres in 1996 [152]. It is called the positive partial transpose (PPT) criterion. It considers the partial transpose (with respect to the party B) of the aforementioned density matrix, which is

$$\rho^{T_B} = I \otimes T(\rho) = \sum_{ijkl} a_{kl}^{ij} |i\rangle\langle j| \otimes (|k\rangle\langle l|)^T = \sum_{ijkl} a_{kl}^{ij} |i\rangle\langle j| \otimes |l\rangle\langle k| = \sum_{ijkl} a_{lk}^{ij} |i\rangle\langle j| \otimes |k\rangle\langle l| \tag{1.12}$$

The statement of the PPT criterion is then given by

> ***Statement 1.1.*** If ρ is separable, then all the eigenvalues of ρ^{T_B} are non-negative.

There is a slight exception for the test: If the eigenvalues are non-negative, and the dimension is larger than 6, the test is inconclusive. The physical significance and interpretation of the partial transposition is in terms of a partial time reversal in the system.

Lewenstein, Karnas and Sanpera [153, 154] took the study of Density Matrices for separability further by putting forward the idea of the *Best Separable Approximation (BSA)* of these Density Matrices. The range of entangled density operators can be studied to formulate an algorithm of optimal decomposition of mixed states into a separable part and an inseparable part. In this method, projections on product vectors are subtracted from a given density matrix in such a way that the remainder remains positively defined.

> ***Theorem 1.2.*** For any density matrix ρ and and for any (fixed) countable set V of product vectors belonging to the range of ρ: $|e_\alpha, f_\alpha\rangle \in R(\rho)$, there exist $\Lambda(V) \geq 0$ and a separable matrix
>
> $$\rho_s^*(V) = \sum_\alpha \Lambda_\alpha P_\alpha \tag{1.13}$$
>
> where $P_\alpha = |e_\alpha\rangle|f_\alpha\rangle\langle e_\alpha|\langle f_\alpha|$, while all $\Lambda_\alpha \geq 0$, such that $\delta\rho = \rho - \Lambda\rho_s^* \geq 0$, and that $\rho_s^*(V)$ provides the optimal separable approximation (OSA) to ρ since $Tr(\delta\rho)$ is mini-

mal or, equivalently Λ is maximal. There exists also the best separable approximation $\rho_s^*(V)$ for which $\Lambda = max_V \Lambda(V)$. Also, $\Lambda(V) \leq \Lambda(V')$ when $V' \subset V$.

Generally, one could define the best separable approximations ρ_s of ρ by seeking that $||\rho - \rho_s||$ is minimal with respect to some norm in the Banach space of operators. Here we minimize $Tr(\rho - \Lambda\rho_s)$ with respect to all ρ_ss such that $\rho - \Lambda\rho_s \geq 0$. But a natural next question would be: how does the process of constructing best separable approximations of a given density matrix work? For understanding this, we will need to give two definitions first:

Definition 1.2(a). A non-negative parameter Λ is called *maximal* with respect to a density matrix ρ, and the projection operator $P = |\psi\rangle\langle\psi|$ if $\rho - \Lambda P \geq 0$, and for every $\varepsilon \geq 0$, the matrix $\rho - (\Lambda + \varepsilon)P$ is not positive definite.

Definition 1.2(b). A pair of non-negative parameters (Λ_1, Λ_2) is called *maximal* with respect to a density matrix ρ and a pair of projection operators $P_1 = |\psi_1\rangle\langle\psi_1|$, $P_2 = |\psi_2\rangle\langle\psi_2|$, if $\rho - \Lambda_1 P_1 - \Lambda_2 P_2 \geq 0$, Λ_1 is maximal with respect to $\rho - \Lambda_2 P_2$ and to the projector P_1, Λ_2 is maximal with respect to $\rho - \Lambda_1 P_1$ and to the projector P_2, and the sum $\Lambda_1 + \Lambda_2$ is maximal.

Given these definitions, one can put forward a second theorem to see how the process of construct the best separable approximation of a density matrix works.

Theorem 1.3. Given the set V of product vectors $|e_\alpha, f_\alpha\rangle \in R(\rho)$, the matrix $\rho_s^*(V) = \sum_\alpha \Lambda_\alpha P_\alpha$ is the optimal separable approximation (OSA) of the density matrix ρ if

- all Λ_α are maximal with respect to $\rho_\alpha = \rho - \sum_{\alpha' \neq \alpha} \Lambda_{\alpha'} P_{\alpha'}$ and to the projector P_α
- all pairs $(\Lambda_\alpha, \Lambda_\beta)$ are maximal with respect to $\rho_{\alpha\beta} = \rho - \sum_{\alpha' \neq \alpha,\beta} \Lambda_{\alpha'} P_{\alpha'}$ and to the projection operators (P_α, P_β).

If ρ is a density matrix for a two qubit system, Lewenstein and Sanpera said that ρ has a unique decomposition of the form

$$\rho = (1 - \lambda)|\psi\rangle\langle\psi| + \lambda\rho_s \tag{1.14}$$

where ρ_s is a separable density matrix, $|\psi\rangle$ is a pure entangled state and the parameter $\lambda \in [0, 1]$ is maximal.

Positive Maps and Separability

The PPT criterion, discussed in the previous section, initiated a general discussion of the problem of separable states in terms of linear positive maps [155] since the PPT criterion demands the positivity of the operator $[I_A \otimes T_B](\rho_{AB})$, where T_B is the transposition map acting on the second subsystem of the composite system. The transposition map is a positive map: it maps a positive operator on H_B into a positive one, but it is not completely positive. A map μ is completely positive only if $I \otimes \mu$ is positive for identity map I on any finite-dimensional system. It has been recognized that any positive map M, which is not completely positive, provides a necessary, nontrivial separability criterion in the form

$$[I_A \otimes M_B](\rho_{AB}) \geq 0 \tag{1.15}$$

This would correspond to the non-negativity of the spectrum of the following matrix:

$$[I_A \otimes M_B](\rho_{AB}) = \begin{pmatrix} M(\rho_{00}) & \dots & M(\rho_{0d_A-1}) \\ M(\rho_{10}) & \dots & M(\rho_{1d_A-1}) \\ \dots & \dots & \dots \\ M(\rho_{d_A-10}) & \dots & M(\rho_{d_A-1d_A-1}) \end{pmatrix} \tag{1.16}$$

with $\rho_{ij} = \langle i| \otimes I |\rho_{AB}| j\rangle \otimes I$. This condition provides a necessary and sufficient condition for separability. The state ρ_{AB} is separable only if the condition (12) is satisfied for all *Positive (P)* but not *Completely Positive (CP)* maps M: $\nu(H_B) \to \nu(H_A)$ where H_A and H_B describe the left and right subsystems of the system AB.

In low dimensions, the sufficiency of the PPT criterion for separability follows from the fact that all positive maps $M{:}\nu(C^d) \to \nu(C^{d'})$ where $d = 2, d' = 2$, and $d = 2, d' = 3$ are *decomposable*:

$$M_{dec} = M_{CP}^{(1)} + M_{CP}^{(2)}.T \tag{1.17}$$

where $M_{CP}^{(i)}$ stand for some *Completely Positive (CP)* maps and T stands for transposition. *Horodecki et al* [155] showed that among all decomposable maps the transposition map T is the *strongest* map: there is no decomposable map that can reveal entanglement which is not already detected by the transposition map.

1.4.3 Separability Criteria for Multipartite Case

A pure n-qubit state $|\psi_{k-sep}\rangle$ is called k-separable only if it can be written as a product of k substates:

$$|\psi_{k-sep}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_k\rangle \tag{1.18}$$

A mixed state ρ_{k-sep} is called k-separable only if it has a decomposition into k-separable pure states:

$$\rho_{k-sep} = \sum_i p_i |\psi^i_{k-sep}\rangle\langle\psi^i_{k-sep}| \tag{1.19}$$

Some of the interesting cases of multipartite separability are given by

- An n-qubit state is called fully separable only if it is n-separable.
- A state is called genuinely n-partite entangled only if it is not bi-separable (2-separable)
- The pure states composing a k-separable mixed state may be themselves k-separable under *different* partitions. Thus, in general, a k-separable mixed state is not separable with respect to any specific partition, thereby making k-separability difficult to observe in such cases.
- If a state is k-separable, it is automatically also k'-separable for all $k' < k$.

Permutation Operators and Separability

Any separable quantum state has a certain symmetry in the separable qubits for a superposition state. This can be probed and analysed by permuting these qubits across the superposition. To formulate a criterion for k-separability, let us define certain permutation operators P_{ij} operating on two copies of an n-partite state.

> ***Definition 1.3.*** Permutation Operators swap the i^{th} and j^{th} subsystems of two copies of a quantum state respectively:
>
> $$P_{ij}|\psi_{a_1a_2...a_n}\rangle \otimes |\psi_{b_1b_2...b_n}\rangle = |\psi_{a_1a_2...a_{i-1}b_ja_{i+1}...a_n}\rangle \otimes |\psi_{b_1b_2...b_{j-1}a_ib_{j+1}...b_n}\rangle \tag{1.20}$$
>
> where the a_i and b_j indicate the subsystems of the first and second copy of the state, respectively.

If we consider the effect of the permutation operator on the separable partition $\tilde{\alpha}$ in a state,

$$P^\dagger_{\tilde{\alpha}ij}\rho^{\otimes 2}P_{\tilde{\alpha}ij} = \rho^{\otimes 2} \tag{1.21}$$

where permutation operators $P_{\alpha ij}$ are the operators permuting the two copies of all subsystems contained in the i^{th} subset and j^{th} subset of the partition α respectively. Now, if the state ρ is a pure state and we have a general separable state $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$,

$$\langle\phi_1|\rho|\phi_2\rangle = \sqrt{\langle\phi_1|\rho|\phi_1\rangle\langle\phi_2|\rho|\phi_2\rangle} \tag{1.22}$$

Due to the presence of two indices in the permutation operator (i, j), we can write the term $\sqrt{\langle\phi_1|\rho|\phi_1\rangle\langle\phi_2|\rho|\phi_2\rangle}$ as $\prod_{i,j=1}^{k}(\sqrt{\langle\phi_1|\rho|\phi_1\rangle\langle\phi_2|\rho|\phi_2\rangle})^{\frac{1}{k^2}}$. Considering $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$

$$\prod_{i,j=1}^{k}(\sqrt{\langle\phi_1|\rho|\phi_1\rangle\langle\phi_2|\rho|\phi_2\rangle})^{\frac{1}{k^2}} = \prod_{i,j=1}^{k}(\sqrt{\langle\phi_1|\langle\phi_2|\rho^{\otimes 2}|\phi_1\rangle|\phi_2\rangle})^{\frac{1}{k^2}} = \prod_{i,j=1}^{k}(\langle\phi|\rho^{\otimes 2}|\phi\rangle)^{\frac{1}{2k^2}} \tag{1.23}$$

Using equations (17) and (18),

$$\prod_{i,j=1}^{k}(\langle\phi|P_{\tilde{\alpha}ij}^{\dagger}\rho^{\otimes 2}P_{\tilde{\alpha}ij}|\phi\rangle)^{\frac{1}{2k^2}} = \langle\phi_1|\rho|\phi_2\rangle \tag{1.24}$$

Now, if we consider P_{tot}, the total permutation operator for permuting the two copies of a state, we have

$$P_{tot}|\phi\rangle = P_{tot}|\phi_1\rangle \otimes |\phi_2\rangle = |\phi_2\rangle \otimes |\phi_1\rangle \tag{1.25}$$

We can write the RHS of equation (20) as

$$\langle\phi_1|\rho|\phi_2\rangle = \sqrt{\langle\phi_2|\rho|\phi_1\rangle\langle\phi_1|\rho|\phi_2\rangle} = \sqrt{\langle\phi_2|\langle\phi_1|\rho^{\otimes 2}|\phi_1\rangle|\phi_2\rangle} \tag{1.26}$$

Using equations (21) and (22),

$$\langle\phi_1|\rho|\phi_2\rangle = \sqrt{\langle\phi_2|\langle\phi_1|\rho^{\otimes 2}|\phi_1\rangle|\phi_2\rangle} = \sqrt{\langle\phi_1|\langle\phi_2|P_{tot}\rho^{\otimes 2}|\phi_1\rangle|\phi_2\rangle} = \sqrt{\langle\phi|P_{tot}\rho^{\otimes 2}|\phi\rangle} \tag{1.27}$$

Using equation (20) and (23), we have

$$\sqrt{\langle\phi|P_{tot}\rho^{\otimes 2}|\phi\rangle} - \prod_{i,j=1}^{k}(\langle\phi|P_{\tilde{\alpha}ij}^{\dagger}\rho^{\otimes 2}P_{\tilde{\alpha}ij}|\phi\rangle)^{\frac{1}{2k^2}} = 0 \tag{1.28}$$

If we include all the partitions in the quantum state for the second term in equation (24), we have

$$\sqrt{\langle\phi|P_{tot}\rho^{\otimes 2}|\phi\rangle} - \sum_{\{\alpha\}}\prod_{i,j=1}^{k}(\langle\phi|P_{\alpha ij}^{\dagger}\rho^{\otimes 2}P_{\tilde{\alpha}ij}|\phi\rangle)^{\frac{1}{2k^2}} \leq 0 \tag{1.29}$$

This is because of the contribution of the other partitions being non-negative diagonal terms which make the equation above stand true. This comprises a theorem and criterion formulated by *Ma et al* for k-separability based on permutation operators:

Theorem 1.4. Every k-separable state satisfies

$$\sqrt{\langle\phi|\rho^{\otimes 2}P_{tot}|\phi\rangle} - \sum_{\{\alpha\}}\Big(\prod_{i,j=1}^{k}\langle\phi|P_{\alpha ij}^{\dagger}\rho^{\otimes 2}P_{\alpha ij}|\phi\rangle\Big)^{\frac{1}{2k^2}} \leq 0 \tag{1.30}$$

1.5 Decoherence-Free Subspaces

One of the biggest problems in the physical realization of quantum computation is the fragility of quantum systems and the presence of noise and decoherence [156, 157, 64, 60, 61, 158, 159, 62, 160]. Therefore the protection of quantum information is an important task in the realm of quantum information processing. Decoherence-Free Subspaces are one of the key areas of research in this direction [161]. The fundamental rationale behind the use of this technique is the presence of logical qubits that are encoded within these subspaces which do not decohere because of reasons of symmetry. To explore this idea further, let us begin by assuming that we have two systems: A and B, defined by the Hilbert spaces H_A and H_B, respectively. The dynamics of these two systems can be generated by

$$H = H_A + H_B + H_{AB} \tag{1.31}$$

where H_A and H_B are the Hamiltonians corresponding to the pure dynamics of systems A and B, respectively, and H_{AB} is the interaction between the two systems. Using the Kraus representation for this system, we have for the reduced dynamics of A for an initial state $\rho_A(0)$,

$$\rho_A(0) \to \rho_A(t) = \sum_{\alpha} K_{\alpha}(t)\rho_A(0)K_{\alpha}^{\dagger}(t) \tag{1.32}$$

after the partial trace over system B is completed. The Kraus operators $K_\alpha(t)$ satisfy the relation $\sum_\alpha K_\alpha^\dagger(t)K_\alpha(t) = I_A \forall t$, where I_A is the identity operator on the system (A). This representation results in non-unitary evolution in the system Hilbert space H_A. In this context, we can define decoherence as:

Definition 1.4 (Decoherence). The phenomenon of non-unitary evolution of an open quantum system is known as decoherence.

An open system which undergoes purely unitary evolution is said to be decoherence-free. For example, if we have a process where a participant Alice wants to send a message (in the form of more than one bits) to Bob, and a third participant Eve wants to mess it up by *flipping the bits*: $|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$. Given N bits shared by Alice with Bob, and when all Eve can do is to flip all bits simultaneously, we can have Alice and Bob agree to encode their bits into logical bits with the bit-string pairs $x_1x_2...x_N$ and $y_1y_2...y_N$, where $y_i = x_i \oplus 1$. This encoding strategy gives $N-1$ logical bits given N physical bits. Thus, for very large values of N, the number of logical bits is almost the same as the number of physical bits.

This is however still an example in the classical realm. The most basic form of Decoherence-Free Subspace emerges for the case of *collective dephasing*. Let us say that we have a system of N qubits that is symmetrically coupled to a 'bath', another quantum system, and undergoes a dephasing process (U_{cd}): $|0\rangle \xrightarrow{U_{cd}} |0\rangle, |1\rangle \xrightarrow{U_{cd}} e^{i\phi}|1\rangle$, effectively putting a random phase ϕ between the basis states $|0\rangle$ and $|1\rangle$. If we now define two logical qubits: $|0_L\rangle = |01\rangle$ and $|1_L\rangle = |10\rangle$, we can see that the combination $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \xrightarrow{U_{cd}} e^{i\phi}|\psi\rangle$, and the overall phase acquired is clearly unimportant. Hence, we find that the two-dimensional subspace

$$DFS_2(1) = Span\{|01\rangle, |10\rangle\} \tag{1.33}$$

is decoherence-free, given the collective dephasing operation. Similarly, we find that the subspaces $DFS_2(2) = Span\{|00\rangle\}$ and $DFS_2(0) = Span\{|11\rangle\}$ are decoherence-free subspaces too, as they acquire an overall phase of 1 and $e^{2i\phi}$ respectively upon the operation of the collective dephasing. However, since the phases are different for the different decoherence-free subspaces, there is no coherence *between* the subspaces.

We generalize this to N qubits: let λ_N denote the number of 0's in a computational basis state. Then, any subspace spanned by states with constant λ_N is decoherence-free against collective dephasing, and can be denoted by $DFS_N(\lambda_N)$.

1.5.1 Decoherence-free Subspaces for Vectors associated with $\sqrt{SWAP}$ and $SWAP^{1/n}$ Quantum Gates

Assuming we are given a system in which our computation is taking place and a 'bath' is connected to the system, the Hamiltonian governing the whole system can be written as

$$H = H_A \otimes I_B + I_A \otimes H_B + H_{AB} \tag{1.34}$$

where H_A acts only on the system, H_B acts only on the bath, and H_{AB} governs the interaction between the two. Without loss of generality, we can write the interaction Hamiltonian as

$$H_{AB} = \sum_{\alpha} A_\alpha \otimes B_\alpha \tag{1.35}$$

where each A_α is a pure-system operator and each B_α is a pure-bath operator. The Hilbert space can be written $H = H_A \otimes H_B$, and $H_A = H_G \oplus H_N$ (H_G is the 'good' portion and H_N is the decoherence-affected, "noisy" subspace) where

$$H_G = Span\{|\gamma_i\rangle\} \tag{1.36}$$

$$H_N = Span\{|\nu_k\rangle\} \tag{1.37}$$

$$H_B = Span\{|\beta_j\rangle\} \tag{1.38}$$

Let us have the following assumptions

- The system is initialized in the *good* subspace

$$\rho_S = \rho_G \oplus 0 = \sum_{i,j} r_{ij} |\gamma_i\rangle\langle\gamma_j| \oplus 0 \tag{1.39}$$

- The basis states of the good subspace are the eigenvectors of the interaction hamiltonian

$$A_\alpha |\gamma_i\rangle = c_\alpha |\gamma_i\rangle, c_\alpha \in \mathbb{C} \tag{1.40}$$

- The basis states of the *good* subspace, when acted on by the system Hamiltonian, remain within the good subspace

$$H_A |\gamma_i\rangle \in H_G \tag{1.41}$$

With these assumptions in hand and considering $U(t) = e^{-iHt}$, we can posit the following theorem:

Theorem 1.5. The evolution of an open system A, in contact and interacting with a 'bath' B, represented together in the Hilbert Space $H = H_A \otimes H_B$, is given by

$$\rho_A(t) = U_{A|H_G}(\rho_G(0)) U^\dagger_{A|H_G} \tag{1.42}$$

where $H_A = H_G \oplus H_N$, with H_G being the 'good' portion of the system and H_N being the decoherence-affected, 'noisy' subspace, and $U_{A|H_G}(t) = e^{-iH_{A|H_G}t}$ is the projection of the

unitary operator $U_A(t)$ only on the *good* subspace. $\rho_G(0)$ is the initial state in the *good* subspace.

Proof. Let us take the state $|\psi\rangle = |\gamma_i\rangle_A \otimes |\beta_j\rangle_B$. Using equations (1.34), (1.35), (1.40) and (1.41),

$$\begin{aligned} H|\psi\rangle &= (H_A \otimes I_B + I_A \otimes H_B + H_{AB})(|\gamma_i\rangle_A \otimes |\beta_j\rangle_B) \\ &= (H_A \otimes I_B + I_A \otimes H_B + \sum_\alpha A_\alpha \otimes B_\alpha)(|\gamma_i\rangle_A \otimes |\beta_j\rangle_B) \end{aligned} \quad (1.43)$$

Simplifying these terms,

$$\begin{aligned} &H_A|\gamma_i\rangle_A \otimes |\beta_j\rangle_B + |\gamma_i\rangle_A \otimes H_B|\beta_j\rangle_B + (\sum_\alpha A_\alpha \otimes B_\alpha)(|\gamma_i\rangle_A \otimes |\beta_j\rangle_B) \\ &\quad = H_A|\gamma_i\rangle_A \otimes |\beta_j\rangle_B + |\gamma_i\rangle_A \otimes H_B|\beta_j\rangle_B + (\sum_\alpha c_\alpha |\gamma_i\rangle_A \otimes B_\alpha|\beta_j\rangle_B) \\ &\quad = (H_A \otimes I_B)(|\gamma_i\rangle_A \otimes |\beta_j\rangle_B) + |\gamma_i\rangle_A \otimes H_B + \sum_\alpha c_\alpha B_\alpha)|\beta_j\rangle_B \\ &\quad = (H_A \otimes I_B + I_A \otimes H_{B'})(|\gamma_i\rangle_A \otimes |\beta_j\rangle_B) \end{aligned} \quad (1.44)$$

where $H_{B'}$ acts only on the 'bath'. If we use this hamiltonian in the unitary evolution operator,

$$U(t) = e^{-i(H_A \otimes I_B + I_A \otimes H_{B'})t} = U_A(t) \otimes U_C(t) \quad (1.45)$$

where $U_x(t) = e^{-iH_x t}$, where $x = A, C$ and $H_C = I_A \otimes H_{B'}$.

To find $\rho(t)$ we apply this unitary operator to $\rho(0)$ with $\rho_A(0) = \rho_G(0) \oplus 0$.

$$\rho(t) = U(\rho_A(0) \otimes \rho_B(0))U^\dagger = U_A(\rho_G(0) \oplus 0)U_A^\dagger \otimes U_C \rho_B U_C^\dagger \quad (1.46)$$

Taking the partial trace with respect to the 'bath' subsystem,

$$\rho_A(t) = Tr_B[U_A(\rho_G(0) \oplus 0)U_A^\dagger \otimes U_C \rho_B U_C^\dagger] = U_A(\rho_G(0) \oplus 0)U_A^\dagger \quad (1.47)$$

If we project the operator U_A to the good subspace $U_A^G = U_{A|H_G}$, we have

$$\rho_A(t) = U_{A|H_G}(\rho_G(0))U_{A|H_G}^\dagger \quad (1.48)$$

This completes the proof. □

In our project, we look at how decoherence-free subspaces emerge naturally out of the idea of invariant subspaces for the $SWAP^{1/n}$ operators.

1.6 Cluster-State Quantum Computation

Cluster State Quantum Computation [162–165] is a method of quantum computing which relies on generation, manipulation and read-out of qubits constituting a cluster-array of elements. Information is introduced into the cluster, processed, and read out from the cluster by one-particle measurements. Entanglement generated in the cluster basis serves as the underlying resource for quantum computation. Cluster states can be created efficiently in a physical system with an Ising-type interaction, at low temperatures, between two-state particles in a lattice. In Raussendorf's model [162], to create a cluster state $|\phi\rangle_C$ on the

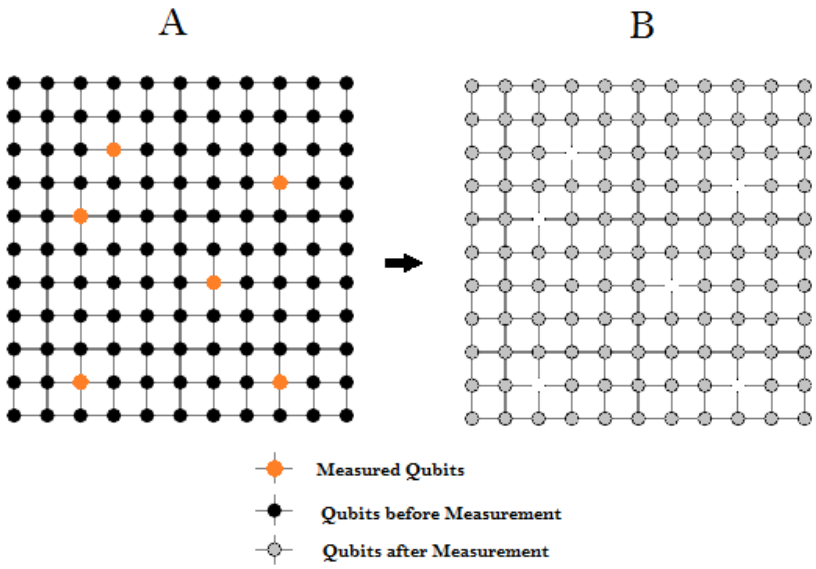


Fig. 1.1 Representation of Static Cluster State Model. In this illustrative example of a static cluster state, A is the cluster before the single-qubit measurements on the cluster, while B is the cluster after the single-qubit measurements are performed. The blank positions in B represent qubits that have been removed from the cluster-state after measurement

cluster C from a product state $\otimes|+\rangle_a$ (with $a \in C$), where $\sigma_x^a|\pm\rangle_a = \pm|\pm\rangle_a$, the interaction is switched on for a finite time interval, and is switched off thereafter ($|\pm\rangle_a = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. A cluster of neighboring particles can become entangled in a single step since the (Ising) Hamiltonian acts uniformly on the entire lattice. To process information (and the logical

qubits) with this cluster one needs to only measure the particles in a certain basis and order. The point to note is that there exist both physical and logical qubits on such lattice-clusters: the former are the physical elements comprising the lattice while the latter can be composed of a combination of physical qubits that can be operated upon in a regularized manner. Measurements of qubits in the σ_z basis effectively remove the respective qubits from the cluster, thereby providing us with a method to structure the cluster state on the lattice.

One can effectively define and isolate functionally useful qubits in 'wires' of quantum data, while removing the remaining qubits from the structure altogether. The σ_z measurement effectively projects the cluster state into a composite state of the measured qubits and the unmeasured ones. On the sub-cluster comprising of the unmeasured qubits, quantum gates can be implemented using measurements of observables σ_x, σ_y (the Pauli matrices) and their linear combinations. Observables of the form $cos(\theta)\sigma_x \pm sin(\theta)\sigma_y$ are measured to realize arbitrary rotations of logical qubits. The sequence and measurement basis for the cluster qubit measurements is of paramount importance for subsquent qubit measurements in a quantum 'wire' in the cluster, thereby creating a temporal order of measurements that has primary significance.

One can establish the universality of a quantum architecture or model by checking if any quantum logic network can be simulated efficiently on it. It is found that Cluster State Quantum Computing does realize this condition, with the realization of a set of Universal Quantum Gates. Cluster states are quantum states of two-level systems (qubits) located on a cluster. This cluster is a connected subset of a simple cubic lattice in $d \geq 1$ dimensions. The cluster states $|\phi_\kappa\rangle_C$ obey the set of eigenvalue equations

$$K^{(a)}|\phi_\kappa\rangle_C = (-1)^{\kappa_a}|\phi_\kappa\rangle_C \tag{1.49}$$

with

$$K^{(a)} = \sigma_x^{(a)} \otimes \sigma_z^{(b)} \tag{1.50}$$

Here a refers to lattice points on the cluster and $b \in Neighbourhood(a)$. $\kappa := \{\kappa_a \in \{0,1\} | a \in C\}$ is a set of parameters which specify the cluster state.

Some examples of cluster states on 2 and 3 qubits are as follows,

$$|\phi\rangle_{C_2} = \frac{1}{\sqrt{2}}(|0\rangle_1|+\rangle_2 + |1\rangle_1|-\rangle_2) \tag{1.51}$$

$$|\phi\rangle_{C_3} = \frac{1}{\sqrt{2}}(|+\rangle_1|0\rangle_2|+\rangle_3 + |-\rangle_1|1\rangle_2|-\rangle_3) \tag{1.52}$$

$|\phi\rangle_{C_2}$ is local unitary equivalent to a Bell state and $|\phi\rangle_{C_3}$ is local unitary equivalent to the Greenberger Horne-Zeilinger(GHZ) state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3) \tag{1.53}$$

Ways to create a cluster state in principle are to measure all the correlation operators $K^{(a)}, a \in C$ of on an arbitrary $|C|$-qubit state. Another way with the creation of a product state $|+\rangle_C = \otimes|+\rangle_a, a \in C$ and the operation of the unitary transformation $S^{(C)}$:

$$S^{(C)} = \prod_{a,b \in C | b-a \in \gamma_d} S^{ab} \tag{1.54}$$

is applied to the state $|+\rangle$. For the cases of dimension $d = 1,2,3$, we have $\gamma_1 = \{1\}$, $\gamma_2 = \{(1,0)^T, (0,1)^T\}$ and $\gamma_3 = \{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T\}$, and the two-qubit transformation S^{ab} is such that the state e $|1\rangle_a \times |1\rangle_b$ acquires a phase of π under its action while the remaining states $|0\rangle_a \times |0\rangle_b$, $|0\rangle_a \times |1\rangle_b$ and $|1\rangle_a \times |0\rangle_b$ acquire no phase. Thus S^{ab} has the form

$$S^{ab} = |0\rangle_a\langle 0| \otimes \mathbb{I}^{(b)} + |1\rangle_a\langle 1| \otimes \sigma_z^{(b)} \tag{1.55}$$

Boykin et al [166] proved that Hadamard (H), $T(\pi/8)$ and CNOT comprise a universal set of gates. In Raussendorf's model, the CNOT gate can be realized in the following way:

CNOT

The CNOT gate can be realized using a simple four-qubit mechanism. In the configuration shown in Figure 1.2, qubits 1 and 4 are the input target and control qubits respectively. We can summarize the operation as follows, with the appropriate initialization (in the σ_z basis). An entanglement operation, given by the *CPHASE* between connected qubits, as shown in Figure 3, is performed and then subsequently qubits 1 and 2 are read out in the σ_x basis:

$$|i_1\rangle_{1,z} \otimes |+\rangle_2 \otimes |+\rangle_3 \otimes |i_4\rangle_{4,z} \xrightarrow{S} |s_1\rangle_{1,x} \otimes |s_2\rangle_{2,x} \otimes U_{\Sigma_{34}}|i_1 + i_4 mod 2\rangle_{3,z} \otimes |4_i\rangle_{4,z} \tag{1.56}$$

where $U_{\Sigma_{34}} = \sigma_z^{(3)s_1+1}\sigma_x^{(3)s_2}\sigma_z^{(4)s_1}$, with measurement results $s_i = 0/1$ projecting a particular qubit to the $s_i\rangle$ state. Raussendorf, in his cluster state model, also discussed how to realize a CNOT gate (Figure 1.3) using a 15 qubit basis. A CNOT gate can be

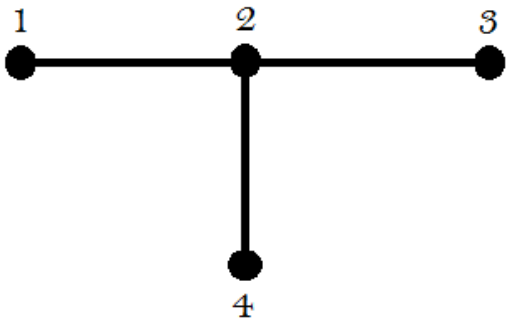


Fig. 1.2 Realization of CNOT gate on a Cluster State

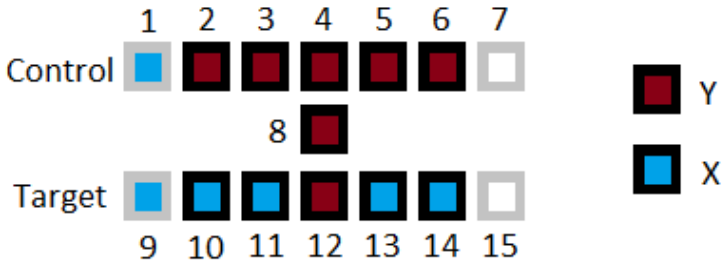


Fig. 1.3 Realization of CNOT gate on a Cluster State using fifteen qubits

realized on a cluster state of 15 qubits with all measurements performed simultaneously.

Step 1: Prepare the state $|\psi\rangle_{C_{15}} = |\psi_{in}\rangle_{\{1,9\}} \otimes |+\rangle_i \forall i \in C_{15}, i \neq 1, i \neq 9$.

Step 2: Entangle the cluster qubits C_{15} using the unitary operation $S^{(C15)}$.

Step 3: Measure all qubits of C_{15} except for output qubits 7, 15. These measurements can be performed simultaneously. Qubits 1, 9, 10, 11, 13 and 14 are measured in the σ_x-eigenbasis and qubits 2-6, 8 and 12 in the σ_y-eigenbasis.

Dependent on the measurement results, the following gate is realized:

$$U'_{CNOT} = U_{\Xi,CNOT} CNOT(c,t) \tag{1.57}$$

where

$$U_{\Xi,CNOT} = \sigma_x^{(c)\gamma_x^{(c)}} \sigma_x^{(t)\gamma_x^{(t)}} \sigma_z^{(c)\gamma_z^{(c)}} \sigma_z^{(t)\gamma_z^{(t)}} \tag{1.58}$$

with

$$\gamma_x^{(c)} = s_2 + s_3 + s_5 + s_6 \tag{1.59}$$

$$\gamma_x^{(t)} = s_2 + s_3 + s_8 + s_{10} + s_{12} + s_{14} \tag{1.60}$$

$$\gamma_z^{(c)} = s_1 + s_3 + s_4 + s_5 + s_8 + s_9 + s_{11} + 1 \tag{1.61}$$

$$\gamma_z^{(t)} = s_9 + s_{11} + s_{13} \tag{1.62}$$

Here, the s_i represent the measurement outcomes on the qubits i.

Arbitrary Rotation

One can realize a general one-qubit rotation (Figure 1.4) via one-qubit measurements on a cluster state. An arbitrary rotation $U_{Rot} \in SU(2)$ can be realized on a chain of five

Fig. 1.4 Realization of arbitrary rotation on a Cluster State

qubits. We consider a rotation in its Euler representation

$$U_{Rot}[\varepsilon, \eta, \tau] = U_x[\tau] U_z[\eta] U_x[\varepsilon] \tag{1.63}$$

where the rotations about the x- and z-axis are $U_x[\alpha] = exp(-i\alpha\sigma_x/2)$, $U_z[\alpha] = exp(-i\alpha\sigma_z/2)$. Initially, the first qubit is prepared in some state $|\psi_{in}\rangle$, which is to be rotated, while the other qubits are prepared in $|+\rangle$. After the five qubits are entangled by the unitary transformation S, the state $|\psi_{in}\rangle$ can be rotated by measuring qubits 1 to 4. At the same time, the state is also swapped to site 5. The qubits 1, 2, 3 and 4 are measured in appropriately chosen bases

$$B_j(\phi_j) = \{\frac{1}{\sqrt{2}}(|0\rangle_j + e^{i\phi_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle_j - e^{i\phi_j}|1\rangle)\} \tag{1.64}$$

where the measurement outcomes $s_j \in \{0,1\}$ for $j = 1,2,3,4$ are obtained. Here, $s_j = 0$ means that qubit j is projected into the first state of $B_j(\phi_j)$. The basis states of all possible measurement bases for this selection lie on the equatorial plane of the Bloch sphere.

Step 1: Preparation of the state $|\psi_{in}\rangle_5 = |\psi_{in}\rangle_1 \otimes |+\rangle_i$, i = 2 to 5.

Step 2: Entanglement of the five qubits of the cluster C_5 via the unitary operation $S^{(C5)}$.

Step 3: Measurement of Qubits 1 to 4 in the following basis and order

- Measurement of Qubit 1 in $B_1(0)$
- Measurement of Qubit 2 in $B_2(-\varepsilon(-1)^{s_1})$
- Measurement of Qubit 3 in $B_3(-\eta(-1)^{s_2})$.
- Measurement of Qubit 4 in $B_4(-\tau(-1)^{s_1+s_3})$

Using this procedure the rotation U'_{Rot} is realized:

$$U'_{Rot}[\varepsilon,\eta,\tau] = U_{\Xi,Rot}U_{Rot}[\varepsilon,\eta,\tau] \tag{1.65}$$

The random byproduct operator has the form

$$U_{\Xi,Rot} = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3} \tag{1.66}$$

This can be corrected for at the end of the computation process. There is a subgroup of rotations which form the subgroup of local operations in the Clifford group, which is the normalizer of the Pauli group. These include the Hadamard and $\frac{\pi}{2}$ gates.

Physical Realization of Cluster State Quantum Computation

Cluster States have been realized on a number of physical systems. In this section, we will briefly review the work done on two of the most popular physical realizations of the cluster state model of quantum computation.

Ionic Systems

The qubits for these systems are defined on ions, as shown in Figure 1.5. The two states of a

qubit are identified with two of the internal states of the ion; for instance, a ground state $|g\rangle = |0\rangle$ and an excited state $|e\rangle = |1\rangle$. One defines the state of the quantum computer on a set of N cold ions interacting with laser light and moving in a linear trap [72]. It is the macroscopic superposition state of quantum registers $|\underline{x}\rangle = |x_{N-1}\rangle_{N-1}...|x_0\rangle_0$, and with $x = \sum_{n=0}^{N-1} x_n 2^n$ (the binary decomposition of x), given by

$$|\psi\rangle = \sum_{x=0}^{2^N-1} c_x|x\rangle = \sum_{\underline{x}=\{0,1\}^N} c_{\underline{x}}|\underline{x}\rangle \tag{1.67}$$

In this system independent manipulation of each qubit is carried out by directing different laser beams to each of these ions. The situation is depicted in Figure 2.16, wherein N ions are confined in a linear trap [167, 72], and are made to interact with different laser beams in standing wave configurations. The confinement of the motion along X, Y and Z directions can be described by a harmonic potential of frequencies $\nu_x \ll \nu_y$, ν_z. The ions are laser cooled in all three dimensions so that they undergo very small oscillations around the equilibrium position [167, 72, 168]. For ionic systems, a number of groups

Fig. 1.5 Basic Circuit-Element of Ionic Quantum Computer with ions as the physical qubits and manipulation by interaction with laser light and movement of the ions in a linear trap

have implemented gate-sets, including two qubit phase gates. *Home et al* [168] implemented a two-qubit quantum logic gate between a pair of trapped 40 Ca ions with 83% fidelity, while *Leibfried et al* [169] demonstrated a universal geometric π-phase gate between two beryllium ion qubits, based on coherent displacements induced by an optical dipole force.

We consider N two-level ions confined in a linear trap. We simultaneously drive the N ions with a laser beam, tuned to $\omega_0 - \nu - \delta$ (ω_0 is the frequency of the transition $|e\rangle \rightarrow |g\rangle$, ν is the frequency of the center-of-mass mode of the collective motion of the two ions, $\delta \ll \nu$, $\hbar \approx 1$). The Hamiltonian for this system is given by

$$H = \nu a^\dagger a + \omega_0 \sum_{j=1}^{N} (\sigma_z)_j + \Omega \sum_{j=1}^{N} (e^{-i(\omega_0-\nu-\delta)t-\eta(a+a^\dagger)+\phi)}\sigma_j^+ + H.C.) \tag{1.68}$$

This can be written as

$$\begin{aligned} H =&[\lambda \sum_{j=1}^{N}(|e_j\rangle\langle e_j|aa^{\dagger}) - \lambda \sum_{j=1}^{N}(|g_j\rangle\langle g_j|a^{\dagger}a)] \\ &+ \lambda \sum_{j,k=1}^{N} \sigma_j^{+}\sigma_k^{-}, j \neq k \end{aligned} \tag{1.69}$$

where $(\sigma_z)_j = \frac{1}{2}(|e_j\rangle\langle e_j| - |g_j\rangle\langle g_j|)$, $\sigma_j^{+} = |e_j\rangle\langle g_j|$ and $\sigma_j^{-} = |g_j\rangle\langle e_j|$ with $|e_j\rangle$ and $|g_j\rangle$ being the excited and ground states of the j^{th} ion. $a^{\dagger}$ and a are the creation and annihilation operators for the center-of-mass mode of the collective motion of the two ions, Ω and ϕ are the Rabi frequency and phase of the laser field. The first two terms in Equation (1.68) describe phonon-number dependent Stark shifts, and the third term describes coupling between the j^{th} and k^{th} ions induced by virtual vibrational excitation. Let us denote the first line (in equation 1.68) as H_1 and second line as H_2. Since $[H_1, H_2] = 0$ the evolution operator (for time of evolution τ) is

$$U_{\tau} = e^{-iH_1\tau}e^{-iH_2\tau} \tag{1.70}$$

Let us assume that the ions are initially in the state $|e_1g_2g_3...g_N\rangle$. For simplicity, we suppose that the vibrational motion is initially in the Fock state $|n\rangle$. After an interaction time τ the state of the system is

$$\begin{aligned} |\psi(\tau)\rangle =& e^{-iH_1\tau}e^{-iH_2\tau}|e_1g_2g_3...g_N\rangle|n\rangle \\ &= e^{i[(N-2)n-1]\lambda\tau}[\frac{N-1+e^{-iN\tau\lambda}}{N}|e_1g_2g_3...g_N\rangle \\ &+ \frac{e^{-iN\tau\lambda}-1}{N}(|g_1e_2g_3...g_N\rangle + ... + |g_1g_2g_3...e_N\rangle)]|n\rangle \end{aligned} \tag{1.71}$$

For certain values of N and τ gives us particular states of interest.

Photonic Systems

Recently, cluster-state entanglement was demonstrated over the continuous variables represented by the quantum amplitudes of the qumodes (electromagnetic field). One such setup is shown in Figure 1.6. This was achieved in the time domain [170, 171], with 104 sequentially addressable entangled qumodes, and in the frequency domain [172], with 60 simultaneously addressable entangled qumodes.The setup for the generation of continuous variable cluster states, as worked on by *Alexander et al* [1], is shown in Figure 1.6. An Optical Polarization Oscillator is pumped at two frequencies $2\nu_0 \pm \Delta\nu$, one of each polarization (Y and Z).

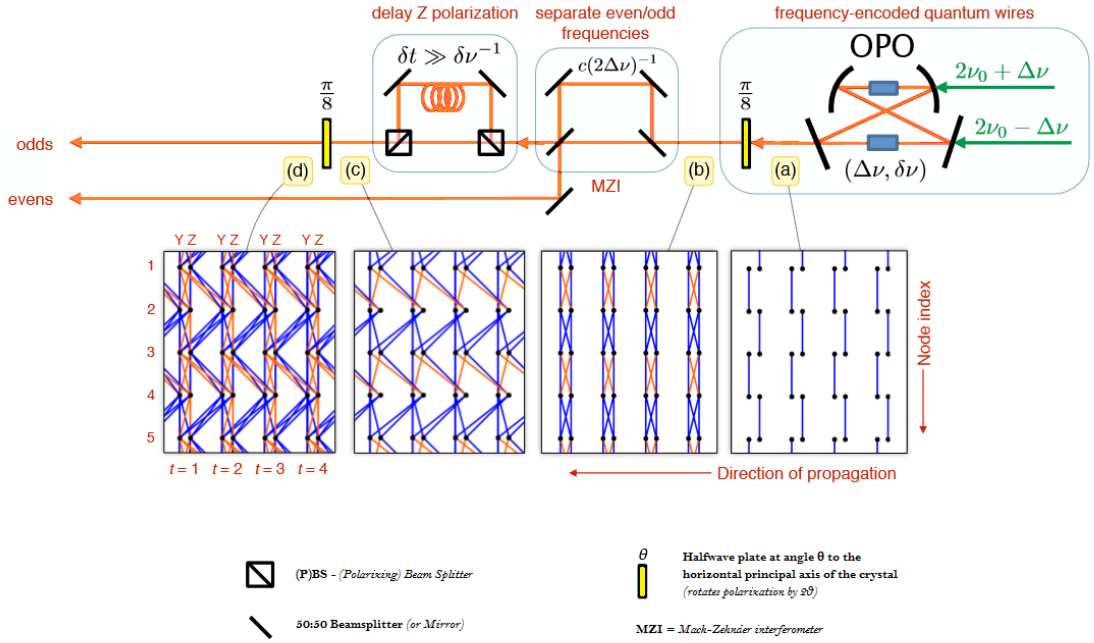


Fig. 1.6 Basic Circuit-Element of a Photonic Quantum Cluster State Computation System [1]

Each pump produces a number of two-mode squeezed states over the frequency comb of the Optical Polarization Oscillator eigenmodes. These modes have linewidth $\delta\nu$ and are spaced by the spectral range $\Delta\nu$. The output frequencies

$$\nu_n = \nu_0 + n\Delta\nu \tag{1.72}$$

has a corresponding frequency index n and an associated macronode index $m = (-1)^n$. Phasematching any two frequencies ν_n and $\nu_{n'}$ requires $n + n' = \pm 1$, and all Two-Mode Squeezed States are generated between adjacent node indices. The well-known two-mode squeezing states Hamiltonian is given by

$$H = i\hbar\xi\hat{a}^\dagger\hat{b}^\dagger + H.c \tag{1.73}$$

where ξ is the overall coupling constant and $\hat{a}^\dagger$ and $\hat{b}^\dagger$ correspond to the two modes. It was shown by *Chen et al* [172] that a Hadamard Interferometer, implemented by a $\pi/8$ Halfwave plate can be used to entangled squeezed modes. This was used to create cluster states on the beams, seperated into odd and even states by a Mach-Zehnder Interferometer [173, 172, 1].

In this project, we use the $SWAP^{1/n}$ operator to implement cluster state quantum-computation, using states generated from an initially separable state.

1.7 Quantum Communication and Quantum Memory

Quantum communication refers to the exchanging of information via the transferring of a quantum state from one location to another [108, 174–176, 110]. The basic motivation for quantum communication, much like any task in quantum information processing, allows tasks to be performed in a far more efficient way than its classical counterparts [15]. One of the best known applications of quantum communication is in Quantum Key Distribution (QKD) [177–180]. The realm of quantum-communication theory covers varied fields such as quantum communication complexity [181, 16, 182] and superdense coding [183, 184].

There are a number of ways to realize quantum communication, with the most popular realization being based on photonic systems [185, 186, 174, 187–192]. In such systems, the photons act as the 'flying' mediating qubits. For a standard quantum communication protocol, a user, say Alice, encodes her state into a quantum communication channel, which is usually an entangled quantum system. This entanglement is exploited to prepare the quantum state at another location, say at Bob's terminal [193]. Certain quantum communication models do

not use entanglement as their underlying resource [194].

One of the key problems faced during the realization of quantum computation and communication is that of decoherence and noise. The error probability for quantum communication using noisy channels scales exponentially with the length of the channel. Quantum repeaters are a widely popular element of quantum communication protocols to tackle this problem [108]. Another method to optimally communicate over noisy channels is to divide the network into sections with the capability of keeping quantum states in what are known as quantum memories [195]. The implementation of a quantum communication protocol requires the ability to control the transfer of a message effectively in the time domain as well, and quantum memories assist in the same. Quantum memories are not only helpful in dynamically decoupling a subsystem as and when required [196], they can also be a safe and robust way of storing qubits, especially if supported by concepts such as decoherence-free subspaces [197], as has been looked into, in our project.

The Power-of-SWAP has an inherent symmetry that conserves the Hamming weight of the quantum state representation, and this is built into a system of quantum memory that protects the storage qubits from leakages that break this symmetry. The tuning of the coupling constants for the exchange interaction is found to be an effective tool for transporting quantum states from qubit(s) to a quantum storage unit within the constructed quantum memory. As part of our project, we have looked into the use of the Power-of-SWAP for realizing certain quantum communication protocols and quantum memory.

Chapter 2

Methods

> *"Quantum theory provides us with a striking illustration of the fact that we can fully understand a connection though we can only speak of it in images and parables."*
>
> — Werner Heisenberg

The physical system that we consider comprises of the Heisenberg Hamiltonian with spin-spin coupling. The Heisenberg exchange model is a many-body quantum model, which has has been applied to fields as varied as multipolar exchange interactions and high-temperature superconductivity.

In 1928, Werner Heisenberg proposed the (Heisenberg) model, noting that the interactions had a certain spin-free nature and the model had a symmetric-group character [198, 199]. These two aspects have been of particular interest, particularly to the likes of Eugene Wigner, the pioneer in the foundation for the theory of symmetries in quantum mechanics, and famous chemist F. A. Matsen [200–202]. In 1971, he looked into the spin-free group-theoretic nature [203]. Later, alongwith Cosgrove and Picone, he also looked into a symmetric group-theoretic solution of a special, uniform interaction case of the model in 1971 [204], and relations to spin-correlations in 1975 [205]. Let us briefly follow Heisenberg and Matsen's view in seeking a symmetric-group algebraically motivated solution to the Heisenberg Hamiltonian, which for a collection of N doublet spin-1/2 sites, is given by

$$\mathbf{H} = \sum_{P} \mathbb{J}_P \mathbf{P} \tag{2.1}$$

where $\mathbf{P}$ is a permutation acting on the indices of the sites of the system and J_P is a coupling constant. Often, the non-zero J_P are assumed to be only for transpositions $P = ij$, which

interchange the indices of nearest neighbour sites i and j. In the spin-space, the Dirac-identity

$$(ij) = 2\overrightarrow{S}_i.\overrightarrow{S}_j + \frac{1}{2} \tag{2.2}$$

may be used to express the hamiltonian in terms of the spin operators. Clearly, H is an element of the group algebra of the symmetric group S_n acting on the N spin indices. If we consider the unitary evolution operator U for the hamiltonian H obtained from (1) and (2) in the time-dependent case,

$$H(t) = \mathbb{J}_P(t)\overrightarrow{S}_i.\overrightarrow{S}_j \tag{2.3}$$

$$U_P(t) = \tau exp[-\frac{i}{\hbar}\int_0^t H(t')dt'] = \tau exp[-\frac{i}{\hbar}\mathbb{J}_P(t')\overrightarrow{S}_i.\overrightarrow{S}_j dt'] \tag{2.4}$$

For a constant interaction $\mathbb{J}_P(t) = J_0$ and time $\tau_s s.t. \frac{J_0\tau_s}{\hbar} = \pi mod(2\pi), U_P(\tau_s/2) = U_P(\tau_s)^{1/2}$ performing the so-called 'Square-Root-of-SWAP' gate, that is functionally given by,

$$U_{\sqrt{SWAP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.5}$$

The $\sqrt{SWAP}$ gate is a powerful tool for generating entanglement in physical systems. It is a universal operator and any quantum multiqubit gate can be constructed from only $\sqrt{SWAP}$ and single qubit gates. Looking at the entangling power of a general $SWAP^{1/n}$ gate [206]:

$$E(SWAP^{1/n}) = \frac{1}{12}(1 - cos(\frac{2\pi}{n}))$$

we see that the extremum is when $sin(\frac{2\pi}{n})) = 0$, which can be solved for the maxima at $n = 2$, thereby showing that the entangling power of the $\sqrt{SWAP}$, which is $\frac{1}{6}$, is the maximum among all the partial swap operators. As much as the $\sqrt{SWAP}$ is a powerful tool for entanglement generation, we would like to approach the subject of quantum information processing from a more general standpoint, beginning with all $SWAP^{1/n}$ gates:

$$U_{SWAP^{1/n}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+e^{i\pi/n}) & \frac{1}{2}(1-e^{i\pi/n}) & 0 \\ 0 & \frac{1}{2}(1-e^{i\pi/n}) & \frac{1}{2}(1+e^{i\pi/n}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

For effectively using the $SWAP^{1/n}$ for the generation, characterization and application of quantum entanglement, we must investigate the entanglement generated by applying these operators on any general quantum state. Since separable states are easily available in nature, we shall pose the question:

> *"What kinds of states can be accessed by the operation of $SWAP^{1/n}$ operators on any general quantum state, especially separable quantum states, and what is the entanglement within the states so produced? "*

After resolving these questions, we shall look into ways of applying this entanglement in quantum information processing. Let us look at some numerical methods to approach this problem.

2.1 Numerical Methods

The first way to approach this problem is by using numerical methods to see what kinds of quantum states are accessible, given the independence in choosing an initial state and combination of $\sqrt{SWAP}$ gates.

2.1.1 Accessible States

It is of utmost importance to check what kind of states are accessible using the $\sqrt{SWAP}$ gates. We begin this section with a numerical survey of the states one can access. Let us start with the simple example of three qubits. We can have three qubits with $\sqrt{SWAP}$ gates between all of them, as shown in Figure 2.1.

Application of only a single gate will give 24 instances and associated states:

$\|\psi_{in}\rangle$	Gate Combination	$\|\psi_{out}\rangle$
$\|000\rangle$	A	$\|000\rangle$
$\|000\rangle$	B	$\|000\rangle$
$\|000\rangle$	C	$\|000\rangle$
$\|001\rangle$	A	$\|001\rangle$
$\|001\rangle$	B	$\frac{1}{2}(1+i)\|001\rangle+\frac{1}{2}(1-i)\|010\rangle$
$\|001\rangle$	C	$\frac{1}{2}(1+i)\|001\rangle+\frac{1}{2}(1-i)\|100\rangle$
$\|010\rangle$	A	$\frac{1}{2}(1+i)\|010\rangle+\frac{1}{2}(1-i)\|100\rangle$
$\|010\rangle$	B	$\frac{1}{2}(1+i)\|010\rangle+\frac{1}{2}(1-i)\|001\rangle$

$\|010\rangle$	C	$\|010\rangle$
$\|011\rangle$	A	$\frac{1}{2}(1+i)\|011\rangle+\frac{1}{2}(1-i)\|101\rangle$
$\|011\rangle$	B	$\|011\rangle$
$\|011\rangle$	C	$\frac{1}{2}(1+i)\|011\rangle+\frac{1}{2}(1-i)\|110\rangle$
$\|100\rangle$	A	$\frac{1}{2}(1+i)\|100\rangle+\frac{1}{2}(1-i)\|010\rangle$
$\|100\rangle$	B	$\|100\rangle$
$\|100\rangle$	C	$\frac{1}{2}(1+i)\|100\rangle+\frac{1}{2}(1-i)\|001\rangle$
$\|101\rangle$	A	$\frac{1}{2}(1+i)\|101\rangle+\frac{1}{2}(1-i)\|011\rangle$
$\|101\rangle$	B	$\frac{1}{2}(1+i)\|101\rangle+\frac{1}{2}(1-i)\|110\rangle$
$\|101\rangle$	C	$\|101\rangle$
$\|110\rangle$	A	$\|110\rangle$
$\|110\rangle$	B	$\frac{1}{2}(1+i)\|110\rangle+\frac{1}{2}(1-i)\|101\rangle$
$\|110\rangle$	C	$\frac{1}{2}(1+i)\|110\rangle+\frac{1}{2}(1-i)\|011\rangle$
$\|111\rangle$	A	$\|111\rangle$
$\|111\rangle$	B	$\|111\rangle$
$\|111\rangle$	C	$\|111\rangle$

Table 2.1 Table of cases for Three-Qubit States with one gate

Now if we have two gates, either distinctive or the same twice, which are operated upon the qubits sequentially, we have the following 72 cases and associated accessible states

$\|\psi_{in}\rangle$	Gate Combination	$\|\psi_{out}\rangle$
$\|000\rangle$	AA	$\|000\rangle$
$\|000\rangle$	AB	$\|000\rangle$
$\|000\rangle$	AC	$\|000\rangle$
$\|000\rangle$	BA	$\|000\rangle$
$\|000\rangle$	BB	$\|000\rangle$
$\|000\rangle$	BC	$\|000\rangle$
$\|000\rangle$	CA	$\|000\rangle$
$\|000\rangle$	CB	$\|000\rangle$
$\|000\rangle$	CC	$\|000\rangle$
$\|001\rangle$	AA	$\|001\rangle$
$\|001\rangle$	AB	$\frac{1}{2}(1+i)\|001\rangle+\frac{1}{2}\|010\rangle-\frac{i}{2}\|100\rangle$
$\|001\rangle$	AC	$\frac{1}{2}(1+i)\|001\rangle-\frac{i}{2}\|010\rangle+\frac{1}{2}\|100\rangle$
$\|001\rangle$	BA	$\frac{1}{2}(1+i)\|001\rangle+\frac{1}{2}(1-i)\|010\rangle$

$\|001\rangle$	BB	$\|010\rangle$
$\|001\rangle$	BC	$\frac{i}{2}\|001\rangle + \frac{1}{2}\|010\rangle + \frac{1}{2}(1-i)\|100\rangle$
$\|001\rangle$	CA	$\frac{1}{2}(1+i)\|001\rangle + \frac{1}{2}(1-i)\|100\rangle$
$\|001\rangle$	CB	$\frac{i}{2}\|001\rangle + \frac{1}{2}(1-i)\|010\rangle + \frac{1}{2}\|100\rangle$
$\|001\rangle$	CC	$\|100\rangle$

Table 2.2 Table of cases for Three-Qubit States with two gates

Let us take the example of all the three gates operated sequentially, once each, over the three qubits for all possible three-qubit separable input states (Table 1). For this instance of applications of the gates on three qubits, we have 216 instances.

$\|\psi_{in}\rangle$	Gate Combination	$\|\psi_{out}\rangle$
$\|000\rangle$	ABC	$\|000\rangle$
$\|000\rangle$	ACB	$\|000\rangle$
$\|000\rangle$	BCA	$\|000\rangle$
$\|000\rangle$	BAC	$\|000\rangle$
$\|000\rangle$	CBA	$\|000\rangle$
$\|000\rangle$	CAB	$\|000\rangle$
$\|001\rangle$	ABC	$\frac{1}{2}\|001\rangle + \frac{1}{4}(1-i)\|010\rangle + \frac{1}{4}(3-i)\|100\rangle$
$\|001\rangle$	ACB	$\frac{1}{2}\|001\rangle + \frac{1}{4}(3-i)\|010\rangle + \frac{1}{4}(1-i)\|100\rangle$
$\|001\rangle$	BCA	$\frac{1}{2}\|001\rangle + \frac{1}{2}\|010\rangle + \frac{1}{2}(1-i)\|100\rangle$
$\|001\rangle$	BAC	$-\frac{1}{4}(1-i)\|001\rangle + \frac{1}{4}(3-i)\|010\rangle + \frac{1}{2}\|100\rangle$
$\|001\rangle$	CBA	$\frac{1}{2}\|001\rangle + \frac{1}{2}(1-i)\|010\rangle + \frac{1}{2}\|100\rangle$
$\|001\rangle$	CAB	$-\frac{1}{4}(1-i)\|001\rangle + \frac{1}{2}\|010\rangle + \frac{1}{4}(3-i)\|100\rangle$
$\|010\rangle$	ABC	$\frac{1}{2}(1-i)\|001\rangle + \frac{1}{2}\|010\rangle + \frac{1}{2}\|100\rangle$
$\|010\rangle$	ACB	$\frac{1}{2}\|001\rangle - \frac{1}{4}(1-i)\|010\rangle + \frac{1}{4}(3-i)\|100\rangle$
$\|010\rangle$	BCA	$\frac{1}{4}(3-i)\|001\rangle - \frac{1}{4}(1-i)\|010\rangle + \frac{1}{2}\|100\rangle$
$\|010\rangle$	BAC	$\frac{1}{2}\|001\rangle + \frac{i}{2}\|010\rangle + \frac{1}{2}(1-i)\|100\rangle$
$\|010\rangle$	CBA	$\frac{1}{4}(1-i)\|001\rangle + \frac{1}{2}\|010\rangle + \frac{1}{4}(3-i)\|100\rangle$
$\|010\rangle$	CAB	$\frac{1}{4}(3-i)\|001\rangle + \frac{i}{2}\|010\rangle + \frac{1}{4}(1-i)\|100\rangle$
$\|011\rangle$	ABC	$-\frac{1}{4}(1-i)\|011\rangle + \frac{1}{4}(3-i)\|101\rangle + \frac{1}{2}\|110\rangle$
$\|011\rangle$	ACB	$\frac{i}{2}\|011\rangle + \frac{1}{2}\|101\rangle + \frac{1}{2}(1-i)\|110\rangle$
$\|011\rangle$	BCA	$\frac{i}{2}\|011\rangle + \frac{1}{4}(3-i)\|101\rangle + \frac{1}{4}(1-i)\|110\rangle$

$\|011\rangle$	BAC	$\frac{i}{2}\|011\rangle + \frac{1}{4}(1-i)\|101\rangle + \frac{1}{4}(3-i)\|110\rangle$
$\|011\rangle$	CBA	$-\frac{1}{4}(1-i)\|011\rangle + \frac{1}{2}\|101\rangle + \frac{1}{4}(3-i)\|110\rangle$
$\|011\rangle$	CAB	$\frac{i}{2}\|011\rangle + \frac{1}{2}(1-i)\|101\rangle + \frac{1}{2}\|110\rangle$
$\|100\rangle$	ABC	$\frac{1}{2}\|001\rangle + \frac{1}{4}(3-i)\|010\rangle - \frac{1}{4}(1-i)\|100\rangle$
$\|100\rangle$	ACB	$\frac{1}{2}(1-i)\|001\rangle + \frac{1}{2}\|010\rangle + \frac{i}{2}\|100\rangle$
$\|100\rangle$	BCA	$\frac{1}{4}(1-i)\|001\rangle + \frac{1}{4}(3-i)\|010\rangle + \frac{i}{2}\|100\rangle$
$\|100\rangle$	BAC	$\frac{1}{4}(3-i)\|001\rangle + \frac{1}{4}(1-i)\|010\rangle + \frac{i}{2}\|100\rangle$
$\|100\rangle$	CBA	$\frac{1}{4}(3-i)\|001\rangle + \frac{1}{2}\|010\rangle - \frac{1}{4}(1-i)\|100\rangle$
$\|100\rangle$	CAB	$\frac{1}{2}\|001\rangle + \frac{1}{2}(1-i)\|010\rangle + \frac{i}{2}\|100\rangle$
$\|101\rangle$	ABC	$\frac{1}{2}\|011\rangle + \frac{i}{2}\|101\rangle + \frac{1}{2}(1-i)\|110\rangle$
$\|101\rangle$	ACC	$\frac{1}{4}(3-i)\|011\rangle - \frac{1}{4}(1-i)\|101\rangle + \frac{1}{2}\|110\rangle$
$\|101\rangle$	BCA	$\frac{1}{2}\|011\rangle - \frac{1}{4}(1-i)\|101\rangle + \frac{1}{4}(3-i)\|110\rangle$
$\|101\rangle$	BAC	$\frac{1}{2}(1-i)\|011\rangle + \frac{i}{2}\|101\rangle + \frac{1}{2}\|110\rangle$
$\|101\rangle$	CBA	$\frac{1}{4}(3-i)\|011\rangle + \frac{i}{2}\|101\rangle + \frac{1}{4}(1-i)\|110\rangle$
$\|101\rangle$	CAB	$\frac{1}{4}(1-i)\|011\rangle + \frac{i}{2}\|101\rangle + \frac{1}{4}(3-i)\|110\rangle$
$\|110\rangle$	ABC	$\frac{1}{4}(3-i)\|011\rangle + \frac{1}{4}(1-i)\|101\rangle + \frac{i}{2}\|110\rangle$
$\|110\rangle$	ACB	$\frac{1}{4}(1-i)\|011\rangle + \frac{1}{4}(3-i)\|101\rangle + \frac{i}{2}\|110\rangle$
$\|110\rangle$	BCA	$\frac{1}{2}(1-i)\|011\rangle + \frac{1}{2}\|101\rangle + \frac{i}{2}\|110\rangle$
$\|110\rangle$	BAC	$\frac{1}{2}\|011\rangle + \frac{1}{4}(3-i)\|101\rangle - \frac{1}{4}(1-i)\|110\rangle$
$\|110\rangle$	CBA	$\frac{1}{2}\|011\rangle + \frac{1}{2}(1-i)\|101\rangle + \frac{i}{2}\|110\rangle$
$\|110\rangle$	CAB	$\frac{1}{4}(3-i)\|011\rangle + \frac{1}{2}\|101\rangle - \frac{1}{4}(1-i)\|110\rangle$
$\|111\rangle$	ABC	$\|111\rangle$
$\|111\rangle$	ACB	$\|111\rangle$
$\|111\rangle$	BCA	$\|111\rangle$
$\|111\rangle$	BAC	$\|111\rangle$
$\|111\rangle$	CBA	$\|111\rangle$
$\|111\rangle$	CAB	$\|111\rangle$

Table 2.3 Table of cases for Three-Qubit States

For four gates, we have 648 cases and associated states that are accessible. Hence, for k-gates, we have the following number of cases and associated output states, for all separable three qubit gates:

$$N_{acc_3} = 3^k \times 8 \tag{2.6}$$

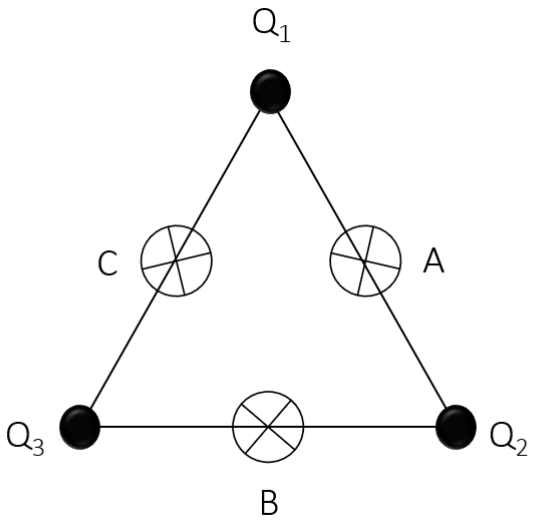


Fig. 2.1 Configuration for three qubit state $|123\rangle$ and $\sqrt{SWAP}$ gates $'A'$, $'B'$ and $'C'$

This result can be generalized for l-qubit separable input states:

$$N_{acc_l} = l^k \times 2^l \tag{2.7}$$

As can be seen, the problem grows exponentially with the number of qubits in the input (separable) states. The number of gates also scale this value exponentially. Certain cases are degenerate but the problem, all in all, grows exponentially with the number of qubits in the input state and the number of gates being operated with on the input state. As a result, this is a problem that cannot be treated numerically.

2.1.2 *SWAP* as a Permuting Operation

Permutation refers to the act of arranging (rearranging) all the elements of a (an) disordered (ordered) set into a certain order or sequence. For example, anagrams of the word 'CAT' ('CAT', 'CTA', 'ACT', 'ATC', 'TAC' and 'TCA') are permutations of the letters of the word 'CAT'.

There are a lot of ways to generate all $n!$ permutations of n elements. Over forty algorithms have been published during the past half a century for generating all the permutations of n elements [207–210]. Even though initially the relevance of permutation generation methods was for tackling computational problems where the elements are permutations such as the

assignment problem, given the presence of better techniques for tackling such problems now, the relevance of permutation-generation lies in their instructive role in illustrating certain fundamental computational concepts such as the relationship between counting, recursion and iteration [210].

The problem of permutation generation has certain inherent computational constraints including the number of permutations for large values of n elements and the time taken to compute them all by simple permutation enumeration. For example, the number of permutations for 15, 16 and 17 elements are 1307674368000, 20922789888000 and 355689428096000 respectively, and, for a a permutation generation program that produces a new permutation each microsecond, the time needed to compute all these permutations by permutation enumeration methods are 2 weeks, 8 months and 10 years respectively [210]! For this very reason, for most practical applications, an area of interest has been the development of *combinatorial search techniques* that are more efficient than permutation enumeration methods. Finding permutations based on exchanges of elements is one of the most efficient methods for permutation-generation [211, 210].

Two of the most famous permutation-generation algorithms using element exchanges are Steinhaus-Johnson-Trotter and Heap's algorithm. In this next section, we will briefly look into these algorithms.

Steinhaus-Johnson-Trotter Algorithm

Named after Hugo Steinhaus, Selmer Johnson and Hale Trotter, the Steinhaus-Johnson-Trotter algorithm generates all the permutations of n elements by swapping two adjacent elements of the sequence each time a new permutation has to be generated [212].

The algorithm has three primary steps, as follows,

> **Step 1**: Let x_i be the position where the value i is placed in permutation π For each i from 1 to n. If the order of the numbers from 1 to $i-1$ in the permutation π defines an even permutation, let
>
> $$y_i = x_i - 1 \tag{2.8}$$
>
> otherwise, let
>
> $$y_i = x_i + 1 \tag{2.9}$$

Step 2: Find the largest number i for which y_i defines a valid position in permutation π that contains a number smaller than i.

Step 3: Swap the values in positions x_i and y_i.

Heap's Algorithm

Proposed by B. R. Heap in 1963, the Heap's algorithm generates all possible permutations of n elements by generating every permutation from the previous one by simply interchanging a single pair of elements, leaving the other $n-2$ elements undisturbed [211, 210, 213]. The Heap's algorithm is simpler than the Steinhaus-Johnson-Trotter algorithm since it does not compute an offset for the pair of elements that are swapped.

The steps for the algorithm are as follows:

Suppose we have a permutation containing n different elements.

Step 1: First we set a counter (i) to 0.

Step 2: We initiatie a loop and perform the following steps repeatedly until $i = n$.

(2.a). We use the algorithm to generate the $(n-1)!$ permutations of the first $n-1$ elements. In each of these permutations, the last element is added to the end of the permutation.

(2.b). If n is odd, we switch the first element and the last element, while if n is even we switch the i^{th} element and the last element.

The counter is increased by one: $i \rightarrow i+1$ and the process is repeated in the loop.

We studied both these algorithms for defining our permutation matrices, especially for larger symmetric groups associated with higher number of qubits.

2.1.3 Transpositions, Cycles and Permutation Matrices

Since the swapping of adjacent elements is a specific manner of permuting elements, as best shown in the algorithms in the previous section, we expect the swap operation to be part of the *Permutation Group*.

Definition 2.1. A group G whose elements are permutations of a given set N is called the *permutation group*. The group operation for the *permutation group* is the composition of permutations in G.

The group of *all* permutations of a set N comprises the *symmetric group* of N and thus the *permutation group* of a set N is a subgroup of the *symmetric group* of set N. Permutation Groups and Symmetric Groups will be discussed at greater length in the section on *Analytic Methods*. If we relax our condition on the swap operation and go from swapping adjacent elements to swapping any two elements in the system, we have a numerical system that spans a larger section of the Hilbert Space. If this is further expanded to more number of elements being permuted, we move towards the general definition of the permutation group. A point of interest for us here, given the focus on *SWAP* and $SWAP^{1/n}$, is the manner in which a general permutation element can be expressed in terms of a *SWAP* operation. To look more closely at this, we will have to explore the idea of *transpositions*, the mathematical concept that realizes a *SWAP* operation among elements (qubits, in our study).

Definition 2.2. A *transposition* is an exchange of two elements of an ordered list with all the other elements staying the same. Therefore, a transposition is a permutation of two elements.

For example, the swapping of elements 2 and 5 in the list 123456 is a transposition to take it to list 153426. We can see that a transposition is what a *SWAP* fundamentally does. It transposes the qubits upon which it is operated. A general permutation is more than a transposition and can be expressed as a *cycle*.

Definition 2.3. A permutation cycle is a subset of a permutation whose elements exchange places with one another.

For example, for the original ordering $\{1,2,3,4\}$, a permutation 3-cycle (143) refers to the first element being replaced by the fourth, the fourth by the third, and the third by the first: $1 \to 4 \to 3 \to 1$, to give us the new ordering $\{3,2,4,1\}$. Cycles and transpositions are

closely linked in that we have a way to express one in terms of the other. We shall now state and prove a theorem that shows how every permutation (cycle) can be expressed as a product of transpositions.

Theorem 2.1. Every permutation of n elements can be expressed as a product of transpositions.

Proof. Let π be a permutation on a set A with n elements. Choosing an element $a_1^{(1)} \in A$ and let $a_2^{(1)} = \pi(a_1^{(1)})$, $a_3^{(1)} = \pi^2(a_1^{(1)})$ and so on till $a_1^{(1)} = \pi^{m_1}(a_1^{(1)})$ for some $m_1 \in \mathbb{N} \cup 0$. Since A is finite, $m_1 \leq n$. This gives us the first cycle

$$C_1 = (a_1^{(1)} a_2^{(1)} a_3^{(1)} ... a_{m_1}^{(1)}) \tag{2.10}$$

If $m < n$, then let us choose an element $a_1^{(2)} \in A$, which is not present in the first cycle. Let $a_2^{(2)} = \pi(a_1^{(2)})$, $a_3^{(2)} = \pi^2(a_1^{(2)})$ and so on till $a_1^{(2)} = \pi^{m_2}(a_1^{(2)})$ for some $m_2 \in \mathbb{N} \cup 0$. This gives us the second cycle

$$C_2 = (a_1^{(2)} a_2^{(2)} a_3^{(2)} ... a_{m_1}^{(2)}) \tag{2.11}$$

If $m_1 + m_2 < n$, then we continue with the construction of such disjoint cycles till we have $m_1 + m_2 + ... + m_t = n$ for some $t \in \mathbb{N}$, and then the permutation can be represented as a product of disjoint cycles:

$$\pi = (a_1^{(1)} a_2^{(1)} a_3^{(1)} ... a_{m_1}^{(1)})(a_1^{(2)} a_2^{(2)} a_3^{(2)} ... a_{m_2}^{(2)}) ... (a_1^{(t)} a_2^{(t)} a_3^{(t)} ... a_{m_t}^{(t)}) \tag{2.12}$$

Now suppose we have two permutation cycles: C_1 and C_2 on A. We assume that C_1 and C_2 *fix* the elements $a_i^{(f)}, f > 2, i \in \{1, 2, ..., m_f\}$. *Fixing* refers to the case where a permutation does not make changes when operating upon an element.

If we now taken an element $x = a_i^{(1)}, i \in \{1, 2, 3, ..., m_1\}$,

$$C_1 C_2(a_i^{(1)}) = C_1(C_2(a_i^{(1)})) = C_1(a_i^{(1)}) = a_{i+1}^{(1)}, a_{m_1+1}^{(1)} = a_1^{(1)} \tag{2.13}$$

$$C_2 C_1(a_i^{(1)}) = C_2(C_1(a_i^{(1)})) = C_2(a_{i+1}^{(1)}) = a_{i+1}^{(1)} \tag{2.14}$$

A similar case can be shown for $\{a_i^{(2)}\}, i \in \{1, 2, 3, ..., m_2\}$.

For $\{a_i^{(f)}\}, f > 2, i \in \{1,2,3,...,m_f\}$, when both the permutations leave the elements unchanged,

$$C_1C_2(a_i^{(f)}) = C_1(C_2(a_i^{(f)})) = C_1(a_i^{(f)}) = a_i^{(f)}, a_{m_f+1}^{(f)} = a_1^{(f)} \tag{2.15}$$

$$C_2C_1(a_i^{(f)}) = C_2(C_1(a_i^{(f)})) = C_2(a_i^{(f)}) = a_i^{(f)} \tag{2.16}$$

Using (18), (19), (20), (21), we can generalize to say that all disjoint cycles are commutative.

$$C_1C_2(x) = C_2C_1(x) \forall x \in A \tag{2.17}$$

Now, since

$$\pi = (a_1^{(1)}a_2^{(1)}a_3^{(1)}...a_{m_1}^{(1)})(a_1^{(2)}a_2^{(2)}a_3^{(2)}...a_{m_2}^{(2)})...(a_1^{(t)}a_2^{(t)}a_3^{(t)}...a_{m_t}^{(t)}) \tag{2.18}$$

and

$$(a_1^{(l)}a_2^{(l)}a_3^{(l)}...a_{m_l}^{(l)}) = (a_1^{(l)}a_{m_l}^{(l)})(a_1^{(l)}a_{m_l-1}^{(l)})...(a_1^{(l)}a_2^{(l)}), l \in \{1,2,...,t\} \tag{2.19}$$

we have,

$$\pi = (a_1^{(1)}a_{m_1}^{(1)})(a_1^{(1)}a_{m_1-1}^{(1)})...(a_1^{(1)}a_2^{(1)}).....(a_1^{(t)}a_{m_t}^{(t)})(a_1^{(t)}a_{m_t-1}^{(t)})...(a_1^{(t)}a_2^{(t)}) \tag{2.20}$$

The theorem is thereby proven. ■

A convenient representation of these permutations lies in permutation matrices. A permutation matrix [214] is a matrix that is obtained by permuting the rows of an $n \times n$ identity matrix according to some permutation of the numbers from 1 to n. Thus, every column and row contains just one 1 with 0s everywhere else. Every permutation has a unique permutation matrix corresponding to it.

The permutation matrices for transpositions represent *SWAP* operators between the elements (as qubits) that are being permuted. Due to this close link between permutation matrices and our operators of interest (*SWAP* and even the $SWAP^{1/n}$), we work on the idea that any permutation of these qubits can be represented by the permutation matrices.

Finding the permutation matrices for smaller number of elements is easy but doing so for higher number of elements (as in the case for higher number of qubits in our project) gets cumbersome. To resolve this numerical problem, we find an algorithm to find the permutation matrices for a general n-qubit quantum state using a bubble-sort method. For example, we start with the case of three qubits $\psi = |123\rangle$. The cycles that are possible for three qubits are

(), (12), (23), (13), (123) and (132). If one were to begin with a 8×8 identity matrix

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.21}$$

then by moving rows in a certain specific way, one can create the permutation matrices for these cycles.

(): Identity matrix remains unchanged.

(23):

$$P[k] \leftrightarrow P[k+1], k = 2,6 \tag{2.22}$$

(12):

$$P[k] \leftrightarrow P[k+2], k = 3,4 \tag{2.23}$$

(13):

$$P[k] \leftrightarrow P[k+3], k = 2,4 \tag{2.24}$$

(123):

$$P[2k] \rightarrow P[4+k], k = 1,2,3 \tag{2.25}$$

$$P[2k+1] \rightarrow P[1+k], k = 1,2,3 \tag{2.26}$$

(132):

$$P[1+k] \rightarrow P[2k+1], k = 1,2,3 \tag{2.27}$$

$$P[4+k] \rightarrow P[2k], k = 1,2,3 \tag{2.28}$$

Now let us look at specific cases that are permissible under the Young's Tableau criteria. For this, let us take the example of four qubits. For four qubit states $\psi = |1234\rangle$, we start with a 16×16 identity matrix, as previously for the case of three qubit states. The cycles that are possible for four qubits and are permissible by the Young's tableau criteria are (1)(2)(3)(4), (12)(3)(4), (13)(2)(4), (14)(2)(3), (12)(34), (13)(24), (123)(4), (124)(3), (134)(2) and (1234).

(): Identity matrix is left unchanged.

(12):

$$P[k] \leftrightarrow P[k-4], k = 9,10,11,12 \tag{2.29}$$

(13):

$$P[k] \leftrightarrow P[k-6], k = 9,10,13,14 \tag{2.30}$$

(14):

$$P[k] \leftrightarrow P[k-7], k = 9,11,13,15 \tag{2.31}$$

(12)(34):

$$P[k] \leftrightarrow P[k+1], k = 2,14 \tag{2.32}$$

$$P[k] \leftrightarrow P[k+4], k = 5,6,7,8 \tag{2.33}$$

(13)(24):

$$P[k] \leftrightarrow P[k+3], k = 2,7,12 \tag{2.34}$$

$$P[k] \leftrightarrow P[k+6], k = 3,8 \tag{2.35}$$

$$P[k] \leftrightarrow P[k+9], k = 4 \tag{2.36}$$

(123)(4):

$$P[k] \leftarrow P[k+6], k = 3,4 \tag{2.37}$$

$$P[k] \leftarrow P[k-2], k = 5,6 \tag{2.38}$$

$$P[k] \leftarrow P[k+4], k = 7,8 \tag{2.39}$$

$$P[k] \leftarrow P[k-4], k = 9,10 \tag{2.40}$$

$$P[k] \leftarrow P[k+2], k = 11,12 \tag{2.41}$$

(124)(3):

$$P[k] \leftarrow P[k+7], k = 2,4 \tag{2.42}$$

$$P[k] \leftarrow P[k-7], k = 15,13 \tag{2.43}$$

$$P[k] \leftarrow P[k-3], k = 5,7 \tag{2.44}$$

$$P[k] \leftarrow P[k+4], k = 6,8 \tag{2.45}$$

$$P[k] \leftarrow P[k-4], k = 9,11 \tag{2.46}$$

$$P[k] \leftarrow P[k+3], k = 10,12 \tag{2.47}$$

(134)(2):

$$P[k] \leftarrow P[k+7], k = 2,6 \tag{2.48}$$

$$P[k] \leftarrow P[k+7], k = 2,6 \tag{2.49}$$

$$P[k] \leftarrow P[k-1], k = 3,7 \tag{2.50}$$

$$P[k] \leftarrow P[k+6], k = 4,8 \tag{2.51}$$

$$P[k] \leftarrow P[k-6], k = 9,13 \tag{2.52}$$

$$P[k] \leftarrow P[k+1], k = 10,14 \tag{2.53}$$

$$P[k] \leftarrow P[k-7], k = 11,15 \tag{2.54}$$

(1234):

$$P[k] \leftarrow P[k+7], k = 2 \tag{2.55}$$

$$P[k] \leftarrow P[k-7], k = 15 \tag{2.56}$$

$$P[2k] \leftarrow P[k+7], k = 2,3,4,5,6,7 \tag{2.57}$$

$$P[2k+1] \leftarrow P[k], k = 1,2,3,4,5,6,7 \tag{2.58}$$

Let us look at the cases individually.

For a **2-cycle**, the idea is that one can understand exactly which swap is needed by looking at the placeholder index-values for the respective cycle. So for a cycle (ij) in an n-qubit state $|123...i...j...n\rangle$, we have the swap

$$P[k] \leftrightarrow P[k + (2^{n-i} - 2^{n-j})] \tag{2.59}$$

The next point is to look for which states have to be swapped for different kinds of cycles. The numbers over which the iteration will run will be determined by the value of the placeholder index of the qubit j. So for instance, an (ij) cycle will have the first 2^{4-j} vector states unchanged, the next 2^{4-j} states put into the aforementioned swap equation (65), and so on till $\frac{n}{2}$ after which it is symmetrically repeated. The distance between the vectors comprising the complementary set will be $2^{4-i} - 2^{4-j}$.

For cases where we have more than one 2-cycles simultaneously, the effects of each individual one add up. So, for instance if we have the cumulative cycle $(i_1 j_1)(i_2 j_2)$ and due to cycle $(i_1 j_1)$ we have a swap $a_1 \leftrightarrow b$, while due to cycle $(i_2 j_2)$ we have a

swap $b \leftrightarrow c_1$, then for the cumulative cycle, we will have the swap $a_1 \leftrightarrow c_1$.

Algorithm:

For an n-qubit state, we have the following algorithm for the finding of the various generators required in the Cayley tree for the system under consideration:

1. We define the identity matrix $P = I_{2^n \times 2^n}$

2. We find the matrix for the element (12), say T, by firstly initializing it with the P matrix defined above: $T = P$. We then carry out the following steps:

$$T[2^{n-2} + i] \leftrightarrow T[2^{n-1} + i], i = 1, 2, 3, ..., 2^{n-2} \tag{2.60}$$

This gives us the matrix T for the element (12).

3. We next find the matrix for the element (1234...n), say Q, by firstly initializing it with the P matrix defined above: $Q = P$. We then carry out the following steps to find the matrix itself.

$$P[j + i] \leftrightarrow P[2^{n-1} + i], j + i \leq 2^{n-1}, \tag{2.61}$$

for the j^{th} step.

As has been seen in this chapter previously, every additional qubit to be considered for a *SWAP*-based circuit makes the number of accessible states grow exponentially. As a result, even though we have devised a simplistic manner of generating random permutation matrices for swaps among various elements/qubits, we need to find a more systematic and standardized manner of analysing this problem. But before doing that, let us look at the concept of locus of accessible states.

2.2 Locus of Accessible States for Multiple Power-of-SWAP Gates

The locus of all the accessible quantum states that can be reached by the operation of multiple Power-of-SWAP gates is of primary interest to know the kind of quantum states that can

be reached from an arbitrary separable states, which are easier to prepare. This helps in optimally carrying out the quantum processing tasks, given separable state resources to begin with.

For the two-qubit case, let us begin with a state of the form

$$|\psi_{in}\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{2.62}$$

If we have a parameter $t \in [0,1]$ and the *SWAP*-gate is the unitary generated by the Heisenberg Hamiltonian for evolution time $t = 1$, then we can generate the fractional SWAP by doing the Hamiltonian evolution for time $t \in (0,1)$. For time steps of the form $t = 1/m, m \in \mathbb{Z}$, we obtain the so-called n^{th} Power-of-SWAP ($SWAP^{1/n}$) gates.

In the two-qubit case, let's fix a Power-of-SWAP circuit of depth m, such that for each $i = 1,\ldots,m$, we apply a $U_i = SWAP^{\gamma_i}$ with $\gamma_i = 1/n_i$ for $n_i \in \mathbb{Z}$. Let us look at only the subspace spanned by $\{|01\rangle, |10\rangle\}$. We have

$$|\psi_{in}\rangle \xrightarrow{U_m U_{m-1}\ldots U_1} \psi_f = \alpha'|00\rangle + \beta'|01\rangle + \gamma'|10\rangle + \delta'|11\rangle, \tag{2.63}$$

Since our unitaries are parity preserving, $\alpha' = \alpha, \delta' = \delta$. Now we can consider the inverse problem: fix the initial and final states, and a precision parameter $\varepsilon \in (0,1)$, and compute a sequence $n_1,\ldots,n_m$ such that $U(\Gamma) := U_m U_{m-1}\ldots U_1$ brings $|\psi_{in}\rangle$ within the ε-ball around $|\psi_f\rangle$, i.e, $||\psi_f\rangle - U|\psi_{in}\rangle| \leq \varepsilon$.

Noting that $U(\Gamma) = e^{i\Gamma H_{SWAP}}$, we can also first solve for the time parameter Γ and then obtain the sequence $\{n\}_i$. Let us do this for $\varepsilon = 0$. Taking the $|00\rangle, |11\rangle$ subspaces as invariant, we have the matrix equation

$$\frac{1}{2}\begin{bmatrix} 1+e^{i\pi\Gamma} & 1-e^{i\pi\Gamma} \\ 1-e^{i\pi\Gamma} & 1+e^{i\pi\Gamma} \end{bmatrix}\begin{pmatrix}\beta \\ \gamma\end{pmatrix} = \begin{pmatrix}\beta' \\ \gamma'\end{pmatrix}, \tag{2.64}$$

which we can solve for Γ to get the conditions (assuming $\alpha \neq \beta$)

$$e^{i\pi\Gamma} = \frac{2\beta' - (\beta+\gamma)}{\beta-\gamma} = -\frac{2\gamma' - (\beta+\gamma)}{\beta-\gamma}, \tag{2.65}$$

for which to have a solution, we require $\beta' + \gamma' = \beta + \gamma$.

For the **three-qubit** case, we have the operator of the form

$$U = exp(\alpha_{12}H_{12} + \alpha_{23}H_{23} + \alpha_{13}H_{13}) \tag{2.66}$$

where H_{ij} represents the hamiltonian for SWAP between i^{th} and j^{th} qubits.

So we have

$$U = exp\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha_{23}+\alpha_{13} & -\alpha_{23} & 0 & -\alpha_{13} & 0 & 0 & 0 \\ 0 & -\alpha_{23} & \alpha_{12}+\alpha_{23} & 0 & -\alpha_{12} & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha_{12}+\alpha_{13} & 0 & -\alpha_{12} & -\alpha_{13} & 0 \\ 0 & -\alpha_{13} & -\alpha_{12} & 0 & \alpha_{12}+\alpha_{13} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\alpha_{12} & 0 & \alpha_{12}+\alpha_{23} & -\alpha_{23} & 0 \\ 0 & 0 & 0 & -\alpha_{13} & 0 & -\alpha_{23} & \alpha_{13}+\alpha_{23} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.67}$$

Solving for this operator, we found conditions on the coefficients α_{12}, α_{23} and α_{13}. Since the Power-of-SWAP operators conserve Hamming weight, this symmetry allows us to consider the states with the same Hamming weight for the purposes of our analysis. Let us begin with Hamming weight 1 i.e. states that are spanned by $\{|001\rangle, |010\rangle, |100\rangle\}$. Before we move on to the conditions and considering $a = \alpha_{12}, b = \alpha_{23}, c = \alpha_{13}$, let us define the following variables (A, B and C):

$$A = \sqrt{a^2 + b^2 + c^2 - ab - ac - bc} \tag{2.68}$$

$$B = ab + bc + ac \tag{2.69}$$

$$C = a + b + c \tag{2.70}$$

We then have the mapping

$$U \begin{pmatrix} 0 \\ \alpha \\ \beta \\ 0 \\ \gamma \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ \alpha' \\ \beta' \\ 0 \\ \gamma' \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{2.71}$$

and the relations:

$$\begin{aligned}\alpha' = \{&\frac{b^2+c^2+(-a-A)(-a+A)}{3B} + \frac{(-ab+b^2-ac+c^2-bA-cA)e^{i(c-A)}}{3B-4C(C-A)+3(C-A)^2} \\ &+ \frac{(b^2+c^2+(b+c)(-a+A))e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\alpha \\ &+ \{\frac{1}{3} + \frac{(-b^2+ac+bA)e^{i(C-A)}}{3B-4C(C-A)-3(C-A)^2} + \frac{(-b^2+ac-bA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\beta \\ &+ \{\frac{1}{3} + \frac{(ab-c^2+cA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} + \frac{(ab-c^2-cA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\gamma \end{aligned} \quad (2.72)$$

$$\begin{aligned}\beta' = \{&\frac{1}{3} + \frac{(-b^2+ac+bA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} + \frac{(-b^2+ac-bA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\alpha \\ &+ \{\frac{a^2+b^2+(-c-A)(-c+A)}{3B} + \frac{(a^2+b^2-ac-bc-aA-bA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} \\ &+ \frac{(a^2+b^2+(a+b)(-c+A))e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\beta \\ &+ \{\frac{1}{3} + \frac{(-a^2+bc+aA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} + \frac{(-a^2+bc-aA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\gamma \end{aligned} \quad (2.73)$$

$$\begin{aligned}\gamma' = \{&\frac{1}{3} + \frac{(ab-c^2+cA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} + \frac{(ab-c^2-cA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\alpha \\ &+ \{\frac{1}{3} + \frac{(-a^2+bc+aA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} + \frac{(-a^2+bc-aA)e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\beta \\ &+ \{\frac{a^2+c^2+(-b-A)(-b+A)}{3B} + \frac{(a^2-ab-bc+c^2-aA-cA)e^{i(C-A)}}{3B-4C(C-A)+3(C-A)^2} \\ &+ \frac{(a^2+c^2+(a+c)(-b+A))e^{i(C+A)}}{3B-4C(C+A)+3(C+A)^2}\}\gamma \end{aligned} \quad (2.74)$$

These equations give the condition:

$$\alpha' + \beta' + \gamma' = \alpha + \beta + \gamma \quad (2.75)$$

This should also follow true for states with Hamming weight 2: $U \begin{pmatrix} 0 \\ 0 \\ 0 \\ \delta \\ 0 \\ \varepsilon \\ \nu \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ \delta' \\ 0 \\ \varepsilon' \\ \nu' \\ 0 \end{pmatrix}$ with the condition

$$\delta + \varepsilon + \nu = \delta' + \varepsilon' + \nu' \tag{2.76}$$

The result given above can be generalized to the case of higher-number of qubits. For any combination of Power-of-SWAP and general N-qubit input state of the form

$$|\psi\rangle = \alpha_0|000...00\rangle + \alpha_1|000...01\rangle + ... + \alpha_{2^N}|111...11\rangle \tag{2.77}$$

being transformed to

$$|\psi'\rangle = \beta_0|000...00\rangle + \beta_1|000...01\rangle + ... + \beta_{2^N}|111...11\rangle \tag{2.78}$$

we derive a condition for the coefficients of the vector basis states with the same Hamming weights.

Theorem 2.2. For the set of all coefficients associated with vector states with the same Hamming weight i as $\{\alpha^k_{(hw)^{(i)}}\}$ in the input quantum state, the set of all coefficients associated with vector states with the same Hamming weight $\{\beta^{k'}_{(hw)^{(i)}}\}$ in the output quantum state (here k and k' denote the indices of the coefficients in each such set), we have

$$\sum_k \alpha^k_{(hw)^{(i)}} = \sum_{k'} \beta^{k'}_{(hw)^{(i)}} \tag{2.79}$$

for any N-qubit case.

Proof. This proof will be divided into two parts:

(a) We first consider the case for the operation of Power-of-SWAP gates on distinct qubits, without any qubit being operated upon by more than one Power-of-SWAP gate. Then, we

can represent the resultant operator as

$$U = \prod_j (\otimes_i U^{(i,j)}_{SWAP_{1/n}}) \tag{2.80}$$

Here i refers to the i^{th} qubit and j refers to the j refers to the j^{th} step/application. Using the mixed product property of tensor products, we have

$$U = \otimes_i (\prod_j U^{(i)}_{SWAP_{1/n_j}}) \tag{2.81}$$

Now, we know that

$$\prod_j U^{(i)}_{SWAP_{1/n_j}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+e^{i\Sigma_j(\frac{1}{n_j})}) & \frac{1}{2}(1-e^{i\Sigma_j(\frac{1}{n_j})}) & 0 \\ 0 & \frac{1}{2}(1-e^{i\Sigma_j(\frac{1}{n_j})}) & \frac{1}{2}(1+e^{i\Sigma_j(\frac{1}{n_j})}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.82}$$

Studying the tensor product properties, we see that the sum of the elements in a row of the operator U equal 1. As a result, the theorem result follows from this.

(b) Let us take the case where the operators that can operate on common qubits. We can represent the operator

$$U_1 = U_{SWAP_{1/n_1}} \otimes U_{SWAP_{1/n_2}} \otimes ... \otimes U_{SWAP_{1/n_m}} \tag{2.83}$$

in compact form as

$$(U_1)_{r,c} = (S_m)_{r\%2^2+1,c\%2^2+1} (S_{m-1})_{\lfloor r/2^2 \rfloor, \lfloor c/2^2 \rfloor} ... (S_1)_{r/2^{2m},c/2^{2m}} \tag{2.84}$$

where r and c refer row and column indices respectively. S_k represents the k^{th} Power-of-SWAP gate and $\%$ denotes the modulo operation.

Now, if the operator (U_2) is one that has the first qubit undisturbed, and subsequent qubits operated upon by Power-of-SWAP gates. If we consider the case considered for U_1, we have even number of qubits and hence the last qubit will be left undisturbed in U_2. Then, the form of this operator is

$$U_1 = I_{2\times 2} \otimes U_{SWAP_{1/l_1}} \otimes U_{SWAP_{1/l_2}} \otimes ... \otimes U_{SWAP_{1/l_{m-1}}} \otimes I_{2\times 2} \tag{2.85}$$

where $I_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The compact form of this matrix can be written as

$$(U_2)_{r',c'} = (S_m)_{\lfloor r'/2 \rfloor \% 2^4+1, \lfloor c'/2 \rfloor \% 2^4+1} (S_{m-1})_{r' \% 2^3, c' \% 2^3} \ldots (S_1)_{r' \% 2^{2m+1}, c' \% 2^{2m+1}} \tag{2.86}$$

Now if we multiply operators U_1 and U_2 and simplify, we shall see that the sum of the rows of the resultant operator $U = U_1.U_2$ is always 1. This can be extended to more number of constituent operators. ■

This is a powerful theorem and result since it, along with the normalization condition, helps us determine the kinds of states that are derivable from the operation of just Power-of-SWAP gates on a general N-qubit state.

Having seen the locus of states accessible by our operators in a finite time, we see a certain sparseness in the distribution. The problem grows exponentially with the different orders of operation of the SWAP-based operators. The question is how to tackle this increasingly complex problem and not only determine the locus of accessible states but also the kinds of states that can be accessed.

The answer to the problem lies in *group theory*.

2.2.1 Invariant Subspaces

Even though the number of accessible states grows with each additional qubit added to the physical system, there are certain fundamental points that act as constraints on this ever-so-increasing set of states and keep them within specific subspaces of the Hilbert space. The concept of *invariant subspaces* has been an important one in operator theory and has played an important constraining role in such cases [215–217].

Definition 2.4. An *invariant subspace* of a linear transformation $T : V \to V$ is a subspace W of the vector space V that is preserved by T: $T(W) \subseteq W$.

As we saw on the section on the locus of accessible state using Power-of-SWAP gates, we have input states only going to certain, specific kinds of output states. This is because of the certain interesting characteristics of these operators and associated constraints on the kinds of states one can access with these operators operating on specific input states.

Parity Conservation: The *SWAP*, $\sqrt{SWAP}$ and the $SWAP^{\frac{1}{n}}$ have the interesting property that they conserve the parity of a quantum state, i.e. the number of $|0\rangle$s and $|1\rangle$s in the states are maintained. This is because of the structure of these operators. For instance, the Power-of-SWAP operator has the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+e^{i\pi/n}) & \frac{1}{2}(1-e^{i\pi/n}) & 0 \\ 0 & \frac{1}{2}(1-e^{i\pi/n}) & \frac{1}{2}(1+e^{i\pi/n}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.87}$$

A state with parity 0 ($|00\rangle$) goes to a state with parity 0($|00\rangle$) under the operation of a Power-of-SWAP gate, a state with parity 1 ($|01\rangle$/$|01\rangle$) goes to a state with parity 1($\frac{1}{2}(1+e^{i\pi/n})|01\rangle+\frac{1}{2}(1-e^{i\pi/n})|10\rangle$/$\frac{1}{2}(1-e^{i\pi/n})|01\rangle+\frac{1}{2}(1+e^{i\pi/n})|10\rangle$) under the operation of a Power-of-SWAP gate and a state with parity 2 ($|11\rangle$) goes to a state with parity 2($|11\rangle$) under the operation of a Power-of-SWAP gate. This is also true for multiple SWAP operators operating on multi-qubit states. Fundamentally, this is because of the fact that the *SWAP*-based operators do not cause any flip of qubits. This constraint on parity under operation by a *SWAP*-derivative gate creates subspaces with constant parities.

Even though this gives us a rough idea about the kinds of vectors that should be present in a certain invariant subspace, it does not tell us anything about the number of vectors that should comprise the basis for an invariant subspace.

Symmetry: The symmetries within the structure of the Power-of-*SWAP* operator causes us to have further constraints on the accessibility of states, starting with a specific input state. For instance, the symmetry of the operator for states $|01\rangle$ and $|10\rangle$ causes $|01\rangle+|10\rangle \rightarrow |01\rangle+|10\rangle$, irrespective of the value of n in $SWAP^{1/n}$. As a result, the perfectly symmetric Dicke state, for instance, always maps back on to itself, irrespective of the numbers or kinds of Power-of-SWAP gates used. This idea is explored further in the section on permutation symmetry in *Analytic Methods*.

For multiqubit states, the more the number of complementary states with respect to a Power-of-SWAP, lesser is the dimension of the subspace. For example, complementarity under action of Power-of-SWAP of qubits 1-2 ($\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{12}$) and 3-4 ($\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{34}$) in a six qubit state reduces the number of vectors needed to compose the invariant subspace than in the case of a state with only the 1-2 or 3-4 have a complementary state.

2.3 Analytic Methods

Sets of symmetries of an object that are closed under composition and under taking inverses are best addressed by what are known as *Groups*. For instance, the *Dihedral Group* D_{2n} is the group of symmetries of the regular n-sided polygon in a plane while the *Orthogonal Group* O(n) is the group of distance-preserving transformations that preserve a fixed point in a Euclidean space of dimension n. Some of these groups are used to describe symmetries in Physics. For example, the physical symmetry underlying special relativity can be expressed using the Poincaré groups while point groups are used to help understand symmetries in molecular chemistry.

The birth of *Group Theory* was intricately woven into the development of methods for finding solutions of polynomial equations of degree higher than four. The earliest work on this can be dated back to the late 1650s, in a work by Johannes Hudde. He worked on the theory of equations, and more particularly on the maxima and minima for a given equation. He gave an ingenious method to find multiple roots of an equation, which can be found in a letter entitled *Epistola secunda, de maximis et minimis* (1658), sent to the Dutch mathematician Franciscus van Schooten and published later as an appendix to his edition of Descartes's *La Géométrie*:

> *If in an equation two roots are equal and if it be multiplied by any arithmetical progression, i.e. the first term by the first term of the progression, the second by the second term of the progression, and so on: I say that the equation found by the sum of these products shall have a root in common with the original equation.*

Around a centure later, in 1740, Nicholas Saunderson noted that finding the quadratic factors of a biquadratic expression necessarily leads to an equation of degree six; an idea later elaborated by Le Sœur and Waring in the eighteenth century.

It was later in 1770 and 1771 that Joseph-Louis Lagrange formulated in his seminal papers the theory of resolvents that was a foundational stone for Galois theory as well. A *Resolvent* of an algebraic equation $f(x) = 0$ of degree n is an algebraic equation $g(y) = 0$, with coefficients that rationally depend on the coefficients of $f(x)$, such that if the roots of this equation are known, the roots of the given equation can be found by solving simpler equations of degrees not exceeding n. Lagrange was interested in understanding solutions of polynomials in several variables, and got the idea to study the behaviour of polynomials when the roots of

the equation are permuted. This led to what is known as Lagrange's Theorem [218]

> *If a function $f(x_1,...,x_n)$ of n variables is acted on by all n! possible permutations of the variables and these permuted functions take on only r values, then r is a divisior of n!.*

Lagrange's method of resolvents fails to give a general formula for solutions of equations of degree equal to or higher than five since it is found that the auxiliary equation involved has a degree that is higher than the original one. However, the significance of this method lies in the fact that it exhibits the formulas for solving equations of second, third and fourth degrees as manifestations of one overarching principle.

It was Évariste Galois who used the word *Group* when he developed Lagrange's theory. Galois found that if $\{r_1, r_2, ...r_n\}$ are the roots of an equation, there is always a group of permutations of the r's such that firstly, every function of the roots that remain invariable by the swapping of elements of the group is rationally known, and secondly (and conversely), every rationally determinable function of the roots remains invariant under the swapping of the elements of this group. Groups similar to such Galois groups are called permutation groups today. This was a concept that was investigated in particular by Augustin-Louis Cauchy, who formulated a number of important theorems in early group theory. Having worked on permutation groups, it was the British Mathematician Arthur Cayley who first defined the concept of *finite groups* in his publication *On the theory of groups, as depending on the symbolic equation* $\theta_n = 1$ (1854). Cayley's theorem [219] states that every group G is isomorphic to a subgroup of the symmetric group acting on G. The theorem considers any group as a permutation group of some underlying set.

Group theoretic concepts emerged in the nineteenth century in the domains of geometry and number theory. Group theory became an increasingly independent subject as it was popularized by the likes of Joseph Alfred Serret, Camille Jordan and Eugen Netto. Other group theorists of the 19th century were Joseph Bertrand, Charles Hermite, Ferdinand Georg Frobenius, Leopold Kronecker, Émile Mathieu, William Burnside, Leonard Eugene Dickson, Otto Hölder, Eliakim Hastings Moore, Peter Ludwig Mejdell Sylow and Heinrich Martin Weber. The convergence of the ideas of group theory in permutation groups, geometry and number theory into a uniform theory started with Camille Jordan's *Traité des substitutions et des équations algébriques* (1870) and von Dyck (1882) who first defined a *group* in the contemporary sense of the word. Jordan gathered all the applications of the mathematical

concept of *permutations* he could find, from number theory, algebraic geometry, function theory, and gave a unified presentation that included the works of Cauchy and Galois. In doing so, he made explicit the notions of homomorphism and isomorphism, and introduced the idea of solvable groups.

The abstract conception of group theory emerged slowly, extracting an idea that was relevant in multiple fields and that was common to permutation groups, transformation groups and abelian groups, each of which were formulated and developed independently over the seventeenth, eighteenth and nineteenth centuries. It took around a century from Lagrange's work in 1770 to Jordan's formulation of groups for the concept of *groups* to evolve. In 1854, Arthur Cayley gave the modern definition of group for the first time and it is with this that we shall like to conclude this historical journey of group theory

> *A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative.*

A group G is a set of elements alongwith an operation . that combines any two elements a and b to form a third element, $a.b$. To qualify as a group, the set and operation, (G, •), must satisfy the *Group Axioms*:

> **I.** Closure: $\forall\{a,b\} \in G \implies a.b \in G$
> **II.** Associativity: $\forall\{a,b,c\} \in G, (a.b).c = a.(b.c)$
> **III.** Identity Element: $\exists e \in G | \forall a \in G, e.a = a.e = a$
> **IV.** Inverse element: $\forall a \in G, \exists b \in G | a.b = b.a = e$. b is often denoted by a^{-1}.

A group G is called *Abelian* if the binary operation is commutative, i.e., $a.b = b.a$ for all $\{a,b\} \in G$.

In our project, we investigate and employ a particular kind of group called the permutation group, as discussed previously in the section on *Numerical Methods*. This group was first conceived when Lagrange was working on the Lagrange's theorem [220]. Interestingly, Lagrange did not prove Lagrange's theorem. The contemporary way of defining groups did not exist during his times. As discussed previously, Lagrange was interested in polynomial equations, and in understanding the existence and nature of the roots. What he actually ended

up proving was that if a polynomial in n variables has its variables permuted in all $n!$ ways, the number of different polynomials that are obtained is always a factor of $n!$. Since the permutations of n elements are actually a group (formally known as the *Symmetric Group*, which is used prominently in our thesis), the number of such polynomials is the index in the group of permutations of n elements of the subgroup H of permutations which preserve the polynomial. Hence, the size of H divides $n!$, which is the number of all permutations of n elements. This is just a particular case of what we now call the Lagrange's Theorem.

2.3.1 Permutation Symmetry, Parity and Conjugacy Classes

Groups were introduced and defined as a set with a binary operation which is closed. The group that we have been interested in for this project is the symmetric group [221, 222]. The symmetric group encapsulates the idea of permutation symmetry in the different kinds of permutation cycles within the structure of the group, and this idea is reflected in the invariance under group action on the basis of vector states associated with the group.

Definition 2.5. A permutation of a set S is a bijection on S and the set of all such functions, with respect to function composition, is a group called the *Symmetric Group* on S, denoted by S_n the symmetric group on n elements.

Example 2.1. Consider the symmetric group S_3 of permutations on 3 elements. It is given by

$$\begin{gathered} e : 123 \to 123 \text{ or } () \\ a : 123 \to 213 \text{ or } (12) \\ b : 123 \to 132 \text{ or } (23) \\ ba : 123 \to 312 \text{ or } (132) \\ ab : 123 \to 231 \text{ or } (123) \\ aba : 123 \to 321 \text{ or } (13) \end{gathered}$$

The notation (132) means that the permutation sends 1 to 3, 3 to 2, and 2 to 1. We can write a general permutation on m elements as $(i_1, ..., i_m)$ in what is called a *cycle notation*, and this permutation $(i_1, ..., i_m)$ is called an *m-cycle*. When m = 2, we obtain a *transposition*. A point to be noted here is that several different cycles can represent the same permutation. For instance,

$$(132) = (321) = (213) \tag{2.88}$$

and not every permutation is a cycle. For example, if we consider $1 \to 2, 2 \to 1, 3 \to 4, 4 \to 3$, this permutation is not a cycle but rather the product of two disjoint cycles: (12) and (34).

We say that two cycles $(i_1,...,i_s)$ and $(j_1,...,j_t)$ are disjoint if and only if

$$\{i_1,...,i_s\} \cap \{j_1,...,j_t\} = \emptyset \tag{2.89}$$

Such a decomposition of a permutation into product of disjoint cycles holds true in general. Every element of the symmetric group S_n can be expressed uniquely as a product of disjoint cycles, up to notational redundancy within each cycle, and ordering of the cycles. Furthermore, every *m-cycle* can be written as a product of transpositions.

The representations as a product of transpositions are not unique. For instance,

$$(2,5,3,6) = (2,6)(2,3)(2,5) = (5,2)(3,5)(6,3) = (1,7)(2,6)(2,3)(2,5)(1,7) \tag{2.90}$$

However, we can define an invariant of a permutation, called the *Parity* of the permutation.

Definition 2.6. (Parity) An element of the symmetric group S_n is said to be *even* if it can be expressed as a product of an even number of transpositions. Otherwise, it is said to be *odd*.

An important theorem relating to the parity of elements of the permutation group relates to the unique parity of every element in the group:

Theorem 2.3. For $n \geq 2$, every element of the symmetric group S_n has a unique parity, even or odd.

Proof. We will introduce an ordering on the permutations by calling the *switching number of a permutation* σ the number of ordered pairs (i, j) with $i < j$ but $\sigma(i) > \sigma(j)$. The important point to note here is that the switching number of a permutation is always an invariant. Let s be the switching number of permutation σ, and let τ be an arbitrary transposition: $\tau = (ij)$. Without loss of generality, we can assume that i comes before j in the permutation $\sigma(1),...,\sigma(n)$. By applying τ to σ, we switch i and j, and we now have

$$\begin{aligned}(1,2,...,\sigma^{-1}(i),...,\sigma^{-1}(j),...,n) &\xrightarrow{\sigma} (\sigma(1),\sigma(2),...,i,...,j,...,\sigma(n)) \\ &\xrightarrow{\tau} (\sigma(1),\sigma(2),...,\tau(i),...,\tau(j),...,\sigma(n))\end{aligned} \tag{2.91}$$

where the first vector is ordered, but not the second and the third.

To understand the effect of the transposition τ on the switching number of σ (we are computing the switching number of $\tau\sigma$ essentially and see how it differs from that of σ), we need to note that we are looking at all the ordered pairs $(k,l), k<l$, in $(1,2,...,n)$:

1. For the ordered pair $(\sigma^{-1}(i),\sigma^{-1}(j))$, upon applying σ there are two options *(a)* the ordering is preserved ($i<j$) and the switching number does not change; however when applying τ, the ordering is reversed, and thus $s\to s+1$. *(b)* the ordering is changed, but τ changes again the ordering, so that $s\to s-1$.

2. Let us now assume that $i<j$ (if not we can do the same with $j>i$). Then for every index l such $i<l<j$, we can look at the non-ordered pairs (i,l) and (l,j). It might be that $\sigma^{-1}(i)$ is either greater or smaller than $\sigma^{-1}(l)$, yielding one ordered pair or the other, and similarly for $\sigma^{-1}(j)$ and $\sigma^{-1}(l)$. Thus each ordered pair may or may not contribute to the switching number of τ, but after τ is applied, i and j are reversed, and thus, at once, both (i,l) and (l,j) are changed. Thus the switching number either increases by two, decreases by two, or does not change at all. We can write down the cases explicitly as follows:

$$(\sigma^{-1}(i),\sigma^{-1}(l)),(\sigma^{-1}(l),\sigma^{-1}(j)) \xrightarrow{\sigma} (i,l),(l,j) \xrightarrow{\tau} (j,l),(l,i), i<l<j \qquad (2.92)$$

thus the switching number of σ is t including no switch for these two pairs, and that of $\tau\sigma$ has two switches for these two pairs, thus is of $s+2$.

$$(\sigma^{-1}(i),\sigma^{-1}(l)),(\sigma^{-1}(j),\sigma^{-1}(l)) \xrightarrow{\sigma} (i,l),(j,l) \xrightarrow{\tau} (j,l),(i,l), i<l<j \qquad (2.93)$$

and the switching number of σ is here t including one switch for the second pair, and that of $\tau\sigma$ has one switch for the first pair, but none for the second, thus a total of s. The case $(\sigma^{-1}(l),\sigma^{-1}(i)),(\sigma^{-1}(l),\sigma^{-1}(j))$ also gives s, and lastly

$$(\sigma^{-1}(l),\sigma^{-1}(i)),(\sigma^{-1}(j),\sigma^{-1}(l)) \xrightarrow{\sigma} (l,i),(j,l) \xrightarrow{\tau} (l,j),(i,l), i<l<j \qquad (2.94)$$

has a switching number of s for σ including two switches for these two pairs, and $\tau\sigma$ has no switch, thus totalling $s-2$.

3. All the non-ordered pairs (k,l), where $l<i<j$ and $k<l$ or $k>l$, or $l>j>i$ and $k<l$ or $k>l$ do not induce any change in the switching number*s*, since by swapping i

and j, we do not change the ordering of the pairs.

This shows that given a permutation σ with switching number s, composing with one transposition always changes the parity of the switching number. However, since the switching number is invariant, this means that it always takes an even number of transpositions applied to σ to keep the same switching number. This establishes that the parity of any permutation is always either even or odd, but not both. ■

The set of even permutations forms a subgroup of the symmetric group S_n called the alternating group, denoted by A_n [223]. Note that if τ is an odd permutation, then the coset τA_n consists only of odd permutations, and conversely, if σ is an odd permutation, then $\tau^{-1}\sigma$ is even, so $\sigma \in \tau A_n$. This shows that $|A_n| = \frac{|S_n|}{2}$.

One of the simplest permutation groups is the symmetric group S_3. The group S_3 is the set of all permutations of three distinct, distinguishable objects, where each element corresponds to a particular permutation of the objects as per a given reference order. Since the first object can be put into any one of three positions, the second object into either of two positions that remain, and the last object can only be put into the remaining position, there are $3 \times 2 \times 1 = 6$ elements in the set:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tag{2.95}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tag{2.96}$$

In this notation, the top line represents the initial order of the objects and the bottom line represents the effect of the permutation. The composition law corresponds to performing successive permutations and is undertaken out by rearranging the objects according to the first permutation and then using this as the reference initial order to rearrange the objects as per the second permutation. A geometric realization of S_3 can be established by considering the symmetry transformations of an equilateral triangle (Fig 1). The elements a, b, and c correspond to reflections through lines which intersect the vertices at 3, 1, and 2, respectively, and d and f correspond to clockwise rotations of this triangle by $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$ radians, respectively. The effects of these transformations on the positions of the vertices of the equilateral triangle is identical with the corresponding elements of the symmetric group S_3 and there is a one-to-one correspondence between these transformations and the elements

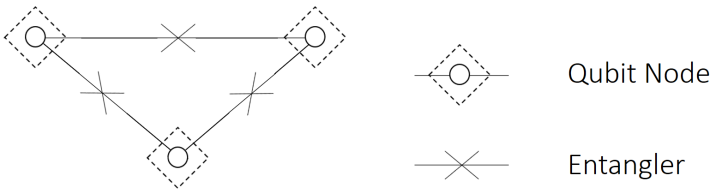


Fig. 2.2 Symmetry transformations of an equilateral triangle labelled by the corresponding elements of the symmetric group S_3

of the symmetric group. Also, this correspondence is preserved by the composition laws in the two groups. Two such groups that have the same algebraic structure are said to be *isomorphic* to one another and are said to be, for all purposes, identical.

Conjugacy Classes and Class Equation

Two elements a and b of a group G are *conjugate* if there is an element g in the group called the *conjugating element* such that

$$a = gbg^{-1} \tag{2.97}$$

Conjugation is an example of an *equivalence relation*, denoted by "$\equiv$", and is defined by the following conditions:

1. *Reflexivity*: $a \equiv a$
2. *Symmetry*: If $a \equiv b$, then $b \equiv a$
3. *Transitivity*: If $a \equiv b$ and $b \equiv c$, then $a \equiv c$

Let us check whether the conjugacy corresponds to an equivalence relation. We consider each of these conditions in turn. By choosing $g = e$ as the conjugating element, we have

$$a = eae^{-1} = a \tag{2.98}$$

This gives

$$a \equiv a \tag{2.99}$$

If $a \equiv b$, then $a = gbg^{-1}$, which we can rewrite as $g^{-1}ag = g^{-1}a(g^{-1})^{-1} = b$ so $b \equiv a$, with g^{-1} as the conjugating element.

Finally, to show transitivity, the relations $a \equiv b$ and $b \equiv c$ imply that there are elements

g_1 and g_2 such that $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$. Thus, $c = g_2 b g_2^{-1} = g_2 g_1 a g_1^{-1} g_2^{-1} = (g_2 g_1) a (g_2 g_1)^{-1}$ so c is conjugate to a with the conjugating element $g_1 g_2$. Therefore, conjugation fulfills the three conditions of an equivalency class.

One important consequence of equivalence is that it permits the assembly of classes: sets of equivalent quantities. In particular, a conjugacy class is the total set of elements that can be obtained from a given group element by conjugation operation. Group elements in the same conjugacy class have various common properties. For instance, all elements of the same class have the same order: Order n of an element a is the smallest integer such that $a^n = e$. An arbitrary conjugate b of a is $b = gag^{-1}$. Thus,

$$b^n = (gag^{-1})(gag^{-1})(gag^{-1}) = ga^n g^{-1} = geg^{-1} = e \tag{2.100}$$

Now that we have defined the equivalence properties of the conjugacy relations, let us look more closely at how these conjugacy relations constitute *conjugacy classes* that compose the set X. Let G be a finite group and X a set over which the action of G is defined. We shall again consider the conjugation ($X = G$), given by: $g.x = gxg^{-1}, x \in X$. Recall that orbits under this action are given by

$$B(x) = \{gxg^{-1}, g \in G\} \tag{2.101}$$

Let us notice that x always is in its orbit $B(x)$ (taking $g = 1$). Hence, if we have an orbit of size 1, this means that $gxg^{-1} = x \iff gx = xg$ and we get an element x in the center $Z(G)$ of G. Thus, elements that have an orbit of size 1 under the action by conjugation are elements of the center.

Recall that the orbits $B(x)$ partition X: $X = \sqcup B(x)$ where the disjoint union is over a set of representatives. We get

$$|G| = \sum |B(x)| = |Z(G)| + \sum |B(x)| = |Z(G)| + \sum [G : Stab(x)] \tag{2.102}$$

where the second equality is arrived at by splitting the sum between orbits with one element and orbits with at least two elements, while the third follows from the *Orbit-Stabilizer Theorem*. By remembering that $Stab(x) = C_G(x)$ when the action is the conjugation, we can

write

$$|G| = |Z(G)| + \sum [G : C_G(x)] \tag{2.103}$$

This formula is called the *class equation*.

Example 2.2. Consider the dihedral group D_4 of order 8:

$$D_4 = \{1, s, r, r^2, r^3, rs, r^2s, r^3s\}, s^2 = 1, r^4 = 1, srs = r^{-1} \tag{2.104}$$

We have that the center $Z(D_4)$ of D_4 is $\{1, r^2\}$. There are three conjugacy classes given by

$$\{r, r^3\}, \{rs, r^3s\}, \{s, r^2s\} \tag{2.105}$$

Thus

$$|D_4| = 8 = |Z(D_4)| + |B(r)| + |B(rs)| + |B(s)| \tag{2.106}$$

Representation of Groups

Consider finite groups G and G' with elements $\{e, a, b, ...\}$ and $\{e', a', b', ...\}$ and that may not be of the same order. Suppose there is a mapping ϕ between the elements of G and G' which preserves their composition rules: if $a' = \phi(a)$ and $b' = \phi(b)$, then

$$\phi(ab) = \phi(a)\phi(b) = a'b' \tag{2.107}$$

If the order of the two groups G and G' is the same, then this mapping ϕ is said to be an *isomorphism* and the two groups are said to be isomorphic to one another, denoted by $G \approx G'$.

If the order of the two groups is not the same, then the mapping is called a *homomorphism* and the two groups are homomorphic to one another. Hence, an isomorphism is a one-to-one correspondence between two groups, whereas a homomorphism is a many-to-one correspondence. An isomorphism is found to preserve the structure of the original group but due to a homomorphism, some of the structure of the original group is sometimes lost. For instance, as seen previously in this chapter, the symmetric group S_3 is isomorphic to the planar symmetry operations of an equilateral triangle.

Definition 2.7. A representation of dimension n of a group G is a homomorphism or isomorphism between the group of nonsingular $n \times n$ matrices with complex entries and the elements of G. The ordinary matrix multiplication is the composition law for such groups.

An isomorphic representation is named as a *faithful representation* and a homomorphic representation is called an *unfaithful representation*. As per this definition, if elements a and b of G are assigned matrices $D(a)$ and $D(b)$, then

$$D(a)D(b) = D(ab) \tag{2.108}$$

The nonsingular nature of the matrices is need since the inverses must be contained in the set.

Representations of groups are important in quantum mechanics for various reasons. Firstly, the eigenfunctions of a certain Hamiltonian transform under the symmetry operations of that Hamiltonian according to a particular representation of that group. Secondly, quantum mechanical operators are often written in terms of their matrix elements and so it is more convenient to write symmetry operations in a similar kind of matrix representation. Lastly, the algebra of matrices is usually simpler to carry out than abstract symmetry operations.

Reducible and Irreducible Representations

Given a matrix representation

$$\{D(e), D(a), D(b), ...\} \tag{2.109}$$

of an abstract group with elements $\{e, a, b, ...\}$, we can obtain a new set of matrices which also form a representation of the group by simply performing a transformation that is known as a equivalence, similarity or canonical transformation,

$$\{BD(e)B^{-1}, BD(a)B^{-1}, BD(b)B^{-1}, ...\} \tag{2.110}$$

Such (similarity) transformations arise quite naturally, for instance, in carrying out a change of basis for matrices. Hence, suppose one begins with the matrix equation $\mathbf{b} = A\mathbf{a}$ relating vectors **a** and **b** through a transformation A. Now if we wish to express this equation in a different basis which is obtained from the original basis by applying a transformation B, we can write

$$B\mathbf{b} = BA\mathbf{a} = BAB^{-1}B\mathbf{a} \tag{2.111}$$

so in the new basis, our equation becomes **b'** $= A'$**a'** where **b'** $= B\mathbf{b}$, **a'** $= B\mathbf{a}$, and $A' = BAB^{-1}$. A similarity transformation can therefore be rendered as a sequence of transformations involving, firstly, a transformation to the original basis (B^{-1}), then the transformation A, and

finally transforming back to the new basis (B).

Let us take the case where we have representations of dimensions m and n, and we construct a representation of dimension $m+n$ by forming block-diagonal matrices of the form:

$$\{\begin{pmatrix} D(e) & 0 \\ 0 & D'(e) \end{pmatrix}, \begin{pmatrix} D(a) & 0 \\ 0 & D'(a) \end{pmatrix}, \begin{pmatrix} D(b) & 0 \\ 0 & D'(b) \end{pmatrix}, ...\} \tag{2.112}$$

where $D(e), D(a), D(b), ...$ are n-dimensional representations and $D'(e), D'(a), D'(b), ...$ an m-dimensional representation of the group G. Each of these $m+n$-dimensional matrices created in this way is called a *direct sum* of the n- and m-dimensional component matrices. The direct sum is denoted by '$\oplus$' to distinguish it from the ordinary addition of two matrices. Hence, we can write the representation in equation (2.112) as

$$\{D(e) \oplus D'(e), D(a) \oplus D'(a), D(b) \oplus D'(b), ...\} \tag{2.113}$$

The representations that form this direct sum can be either identical or distinct, and the block-diagonal form can be continued indefinitely simply by incorporating additional representations in such diagonal blocks. However, we are simply reproducing the properties of the known representations in all such constructions. Thus, even though representations are a convenient way of associating matrices with group elements, the freedom we have in constructing representations, best seen in equation (2.112), does not readily help in demonstrating that these matrices embody any intrinsic characteristics of the group that they represent. To overcome this problem of nonuniqueness posed by representations that are related by similarity transformations we consider the trace of an $n \times n$ matrix A. The utility of the trace of a matrix representation stems from its invariance under similarity transformations

$$tr(A) = tr(BAB^{-1}) \tag{2.114}$$

The significance of this invariance is that, although there may be an infinite variety of representations related by similarity transformations, each such representation has the same trace. But using the trace alone does not resolve the problem of nonuniqueness of representations. To address this problem, we introduce the concept of an *irreducible representation*. Representations such as the one in equation (2.112) are called *reducible* since they are the direct sum of multiple representations. Representations that are not block diagonal but obtained from block-diagonal representations using similarity transformations are still deemed to be reducible because they are obtained from matrices which originally were in block form.

Definition 2.8. If the same equivalence (similarity) transformation transforms all of the matrices of a representation into the same block form, then such a representation is said to be *reducible*. Otherwise, the representation is said to be *irreducible*.

By definition, irreducible representations cannot be expressed in terms of any representations of lower dimensionality. As a result, one-dimensional representations are always irreducible.

We have seen that there is considerable flexibility in constructing group representations. We can restrict this freedom by showing that any representation can be expressed only in terms of unitary matrices. The following theorem allows us to think of group representations as proper and improper complex *rotations* since the property of unitarity, when applied to operators,since it enables changes of bases while preserving the orthogonality of bases.

Theorem 2.4. Every representation can be brought into unitary form by a similarity transformation.

Proof. Let $\{A_1, A_2, ..., A_{|G|}\}$ be a d-dimensional representation of a group G. From these matrices we can form a matrix H given by the sum

$$H = \sum_{\alpha=1}^{|G|} A_\alpha A_\alpha^\dagger \tag{2.115}$$

This matrix is Hermitian since

$$H^\dagger = \sum_{\alpha=1}^{|G|} (A_\alpha A_\alpha^\dagger)^\dagger = \sum_{\alpha=1}^{|G|} A_\alpha A_\alpha^\dagger = H \tag{2.116}$$

Now it is seen that any Hermitian matrix can be diagonalized by some unitary transformation U. Denoting the diagonalized form of H by D, we have $D = U^\dagger H U$,

$$D = \sum_{\alpha=1}^{|G|} U^\dagger A_\alpha A_\alpha^\dagger U = \sum_{\alpha=1}^{|G|} (U^\dagger A_\alpha U)(U^\dagger A_\alpha^\dagger U) = \sum_{\alpha=1}^{|G|} (U^\dagger A_\alpha U)(U^\dagger A_\alpha U)^\dagger \tag{2.117}$$

We use the notation $\bar{A}_\alpha = U^\dagger A_\alpha U$ and see that the diagonal elements of D are real,

$$D_{kk} = \sum_\alpha \sum_j (\bar{A}_\alpha)_{kj} (\bar{A}_\alpha^\dagger)_{jk} = \sum_\alpha \sum_j (\bar{A}_\alpha)_{kj} (\bar{A}_\alpha)_{kj}^* = \sum_\alpha \sum_j |(\bar{A}_\alpha)_{kj}|^2 \tag{2.118}$$

for $k = 1, 2, ..., d$, and positive, because the summation over j includes a diagonal element of the identity, which is a $d \times d$ unit matrix. Thus, the diagonal matrix $D^{1/2}$,

$$D^{1/2} = \begin{pmatrix} D_{11}^{1/2} & 0 & ... & 0 \\ 0 & D_{22}^{1/2} & ... & 0 \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ 0 & 0 & ... & D_{dd}^{1/2} \end{pmatrix} \tag{2.119}$$

and $D^{-1/2}$, given by a similar expression, have positive entries.

We now form the matrices

$$B_\alpha = D^{-1/2} \bar{A}_\alpha D^{1/2} \tag{2.120}$$

from which we obtain

$$B_\alpha^\dagger = (D^{-1/2} \bar{A}_\alpha D^{1/2})^\dagger = D^{1/2} \bar{A}_\alpha^\dagger D^{-1/2} \tag{2.121}$$

Now

$$B_\alpha B_\alpha^\dagger = (D^{-1/2} \bar{A}_\alpha D^{1/2})(D^{1/2} \bar{A}_\alpha^\dagger D^{-1/2}) = D^{-1/2} \bar{A}_\alpha D \bar{A}_\alpha^\dagger D^{-1/2} \tag{2.122}$$

Using the definition of D,

$$B_\alpha B_\alpha^\dagger = D^{-1/2} \sum_j \bar{A}_\alpha \bar{A}_\beta \bar{A}_\beta^\dagger \bar{A}_\alpha^\dagger D^{-1/2} = D^{-1/2} \sum_j (\bar{A}_\alpha \bar{A}_\beta)(\bar{A}_\alpha \bar{A}_\beta)^\dagger D^{-1/2} \tag{2.123}$$

Since the A_α are a representation of G, so are the $\bar{A}_\alpha$, since $UU^\dagger = I$ and $U^\dagger = U^{-1}$, leading to an equivalence $\bar{A}_\alpha^\dagger = U A_\alpha U^{-1}$. Hence, the product $\bar{A}_\alpha \bar{A}_\beta$ is another matrix $\bar{A}_\gamma$ in this representation. The sum over all β means that the set of $\bar{A}_\gamma$ obtained from these products contains the matrix corresponding to each group element only once.

$$B_\alpha B_\alpha^\dagger = D^{-1/2} \sum_\gamma \bar{A}_\gamma \bar{A}_\gamma^\dagger D^{-1/2} = D^{-1/2} D D^{-1/2} = I \tag{2.124}$$

Therefore, B_α, which are formed from the original representation using the similarity transformation

$$B_\alpha = D^{-1/2} U^{-1} A U D^{1/2} = (U D^{1/2})^{-1} A (U D^{1/2}) \tag{2.125}$$

are unitary representations of G. Thus, without loss of generality, we may always assume that a representation is unitary. ■

Properties of Irreducible Representations

The identification of whether a representation is reducible or not is a tedious task if it relies solely on the methods of linear algebra. In this section, the foundation for a more systematic approach to this question will be lay by deriving the fundamental theorem of representation theory known as the *Great Orthogonality Theorem*. The central role of this theorem in the applications of group theory to physical problems is due to the fact that it leads to simple criteria for determining irreducibility and provides a way to identify the number of inequivalent representations for a given group G.

The Great Orthogonality Theorem is based on two lemmas of Schur [224]. These lemmas are concerned with the properties of matrices that commute with the matrices of irreducible representations.

Great Orthogonality Theorem

The Schur's lemmas are restrictions on the form of matrices that commute with all the matrices of irreducible representations. The group property enables us to construct matrices that satisfy Schur's First and Second Lemmas, and this is the basis for the Great Orthogonality Theorem.

Theorem 2.5. (Great Orthogonality Theorem) Suppose $\{A_1, A_2, ..., A_{|G|}\}$ and $\{A'_1, A'_2, ..., A'_{|G|}\}$ are two inequivalent irreducible representationsof a group G that has elements $\{g_1, g_2, ..., g_{|G|}\}$ and have dimensionalities d and d', respectively. The matrices A_α and A'_α correspond to the element g_α in G. Then we see that

$$\sum_\alpha (A^*_\alpha)_{ij}(A'_\alpha)_{i'j'} = 0 \tag{2.126}$$

For elements of a single (unitary) irreducible representation,

$$\sum_\alpha (A^*_\alpha)_{ij}(A_\alpha)_{i'j'} = \frac{|G|}{d}\delta_{i,i'}\delta_{j,j'} \tag{2.127}$$

Proof. Considering the $d' \times d'$ matrix

$$M = \sum_{\alpha} A'_{\alpha} X A_{\alpha}^{-1} \tag{2.128}$$

where X is taken to be an arbitrary matrix with d' rows and d columns.

We pre-multiply M by the matrix A'_{β},

$$A'_{\beta} M = \sum_{\alpha} A'_{\beta} A'_{\alpha} X A_{\alpha}^{-1} = \sum_{\alpha} A'_{\beta} A'_{\alpha} X A_{\alpha}^{-1} A_{\beta}^{-1} A_{\beta} = \sum_{\alpha} A'_{\beta} A'_{\alpha} X (A_{\beta} A_{\alpha})^{-1} A_{\beta} \tag{2.129}$$

Since the A_{α} and A'_{α} form representations of G, the products $A_{\alpha}A_{\beta}$ and $A'_{\alpha}A'_{\beta}$ also are representation matrices A_{γ} and A'_{γ}, respectively.

$$A'_{\beta} M = \sum_{\gamma} A'_{\gamma} X A_{\gamma}^{-1} A_{\beta} = M A_{\beta} \tag{2.130}$$

We now consider the cases of equivalent and inequivalent representations individually:

Case 1: $d \neq d'$ or, if $d = d'$ and the representations are inequivalent. Schur's Second Lemma then implies that M must be the zero matrix. Using (2.128), we see that this requires

$$M'_{ii} = \sum_{\alpha} \sum_{jj'} (A'_{\alpha})_{ij} X_{jj'} (A_{\alpha}^{-1})_{j'i'} = 0 \tag{2.131}$$

We can rewrite this as

$$M'_{ii} = \sum_{jj'} X_{jj'} \sum_{\alpha} (A'_{\alpha})_{ij} (A_{\alpha}^{-1})_{j'i'} = 0 \tag{2.132}$$

Since X is arbitrary, each of its entries may be varied independently and arbitrarily without affecting the vanishing sum. The only way we can ensure that is to require that the coefficients of the $X_{jj'}$ vanish

$$\sum_{\alpha} (A'_{\alpha})_{ij} (A_{\alpha}^{-1})_{j'i'} = 0 \tag{2.133}$$

Since the representations are unitary, we have

$$\sum_{\alpha} (A'_{\alpha})_{ij} (A_{\alpha}^{*})_{j'i'} = 0 \tag{2.134}$$

This is the first part of the Great Orthogonality Theorem.

Case 2: $d = d'$ and the representations are equivalent. Then, according to Schur's First Lemma, $M = cI$, and so

$$M = \sum_{\alpha} A_\alpha X A_\alpha^{-1} = cI \tag{2.135}$$

Taking trace of this equation and using the cyclic property of the trace of a product of elements,

$$\begin{aligned} tr(cI) = cd = tr(\sum_{\alpha} A_\alpha X A_\alpha^{-1}) = \sum_{\alpha} tr(A_\alpha X A_\alpha^{-1}) = \sum_{\alpha} tr(X A_\alpha^{-1} A_\alpha) \\ = \sum_{\alpha} tr(X) = |G| tr(X) \end{aligned} \tag{2.136}$$

Simplifying these equations

$$c = \frac{|G|}{d} tr(X) \tag{2.137}$$

Using this in equation (2.135),

$$\frac{|G|}{d} tr(X) = \sum_{\alpha} A_\alpha X A_\alpha^{-1} \tag{2.138}$$

Expressing this in terms of the matrix elements,

$$\sum_{jj'} X_{jj'} [\sum_{\alpha} (A_\alpha)_{ij} (A_\alpha^{-1})_{j'i'}] = \frac{|G|}{d} \delta_{i,i'} \sum_{j} X_{jj} \tag{2.139}$$

This can be written as

$$\sum_{jj'} X_{jj'} [\sum_{\alpha} (A_\alpha)_{ij} (A_\alpha^{-1})_{j'i'} - \frac{|G|}{d} \delta_{i,i'} \delta_{j,j'}] = 0 \tag{2.140}$$

For any independent variation of the elements of matrix X, the coefficient of these elements in (2.140) must vanish

$$\sum_{\alpha} (A_\alpha)_{ij} (A_\alpha^{-1})_{j'i'} - \frac{|G|}{d} \delta_{i,i'} \delta_{j,j'} = 0 \tag{2.141}$$

Since the representation is unitary,

$$\sum_{\alpha} (A_\alpha)_{ij} (A_\alpha^{*})_{j'i'} - \frac{|G|}{d} \delta_{i,i'} \delta_{j,j'} = 0 \tag{2.142}$$

This is the second part of the Great Orthogonality Theorem.

We can combine the two statements of the Great Orthogonality Theorem as

$$\sum_{\alpha}(A^k_\alpha)_{ij}(A^{k'}_\alpha)^*_{i'j'} = \frac{|G|}{d}\delta_{i,i'}\delta_{j,j'}\delta_{k,k'} \tag{2.143}$$

This expression helps us to understand the motivation for calling this theorem the Great Orthogonality Theorem:

> Let us consider the matrix elements of the irreducible representations as elements in vectors in a space of dimensionality $|G|$:
>
> $$\mathbf{V}^k_{ij} = [(A^k_1)_{ij}, (A^k_2)_{ij}, ..., (A^k_{|G|})_{ij}] \tag{2.144}$$
>
> According to the Great Orthogonality Theorem, two such vectors are *orthogonal* if they differ in any one of the indices i, j or k, since (2.143) and (2.144) can be used to write
>
> $$\mathbf{V}^k_{ij}.\mathbf{V}^{k'}_{i'j'} = \frac{|G|}{d}\delta_{i,i'}\delta_{j,j'}\delta_{k,k'} \tag{2.145}$$
>
> In a $|G|$-dimensional space there are at most $|G|$ mutually orthogonal vectors. Now, suppose we have irreducible representations of dimensionalities $d_1, d_2, ...$ where the $d_k \geq 0, d_k \in \mathbb{Z}$. For the k representations, there are d_k choices for each of i and j, and there are d_k^2 matrix elements in each matrix of the representation. Summing over all the irreducible representations, we have
>
> $$\sum_k d_k^2 \leq |G| \tag{2.146}$$
>
> Hence, the order of the group acts as the upper bound for the number as well as the dimensionalities of the irreducible representations, and a finite group can have only a finite number of irreducible representations.

Example 2.3. For the symmetric group S_3, we have the order of the group $|G| = 6$. S_3 has two one-dimensional irreducible representations and one two-dimensional irreducible representation. Hence, using equation (2.146),

$$\sum_k d_k^2 = 1^2 + 1^2 + 2^2 = 6 \tag{2.147}$$

and so the Great Orthogonality Theorem tells us that there can be no additional distinct irreducible representations of S_3.

2.3.2 Characters and Character Tables

In the previous sections, we proved the orthogonality between the matrix elements corresponding to different irreducible representations of a group. However, for various applications of group theory, only the traces (within classes of group elements) called *characters* are required. An application, for instance, involves determining whether a given representation is reducible or not.

The mathematical machinery that is used to assemble the characters of the irreducible representations of a group is encapsulated in what are called *character tables*. The construction of character tables requires two types of input: the order of the group and the number of classes it contains. Orthogonality relations derived from the Great Orthogonality Theorem provide constraints on characters of various irreducible representations, which considerably simplifies the construction of character tables.

2.3.3 Orthogonality Relations of Characters

To begin with, we can show how the statement of the Great Orthogonality Theorem can be manipulated into an expression solely in terms of the characters of these representations. This will help us in establishing a sum rule between the number of irreducible representations and the number of classes in a group.

We begin by setting $i = j$ and $j' = i'$ in equation (2.143),

$$\sum_{\alpha}(A^k_\alpha)_{ii}(A^{k'}_\alpha)^*_{i'i'} = \frac{|G|}{d_k}\delta_{i,i'}\delta_{k,k'} \tag{2.148}$$

Summing over i and i' on the left-hand side of this equation, we obtain

$$\sum_{i,i'}\sum_{\alpha}(A^k_\alpha)_{ii}(A^{k'}_\alpha)^*_{i'i'} = \sum_{\alpha}[\sum_{i}(A^k_\alpha)_{ii}][\sum_{i'}(A^{k'}_\alpha)^*_{i'i'}] = \sum_{\alpha} tr(A^k_\alpha)tr(A^{k'}_\alpha)^* \tag{2.149}$$

Summing over i and i' on the right-hand side of this equation and considering that $\sum_i 1 = d_k$ for our system, we obtain

$$\sum_{i,i'} \frac{|G|}{d_k} \delta_{i,i'} \delta_{k,k'} = \frac{|G|}{d_k} \delta_{k,k'} \sum_i \sum_{i'} \delta_{i,i'} = \frac{|G|}{d_k} \delta_{k,k'} \sum_i 1 = |G| \delta_{k,k'} \tag{2.150}$$

Using equations (2.148), (2.149) and (2.150), we can therefore rewrite the Great Orthogonality Theorem as

$$\sum_\alpha tr(A_\alpha^k) tr(A_\alpha^{k'})^* = |G| \delta_{k,k'} \tag{2.151}$$

This expression can be re-written in a more useful form by noting that matrices corresponding to elements in the same conjugacy class have the same trace. Let us introduce the notation χ_α^k for the trace corresponding to all the elements of the α class of the kth irreducible representation. This is known as the *character of the class*. If there are $n\alpha$ elements in the class, then we can write the equation (2.151) in terms of characters as a sum over conjugacy classes

$$\sum_\alpha n_\alpha \chi_\alpha^k (\chi_\alpha^{k'})^* = |G| \delta_{k,k'} \tag{2.152}$$

The summation here goes from $\alpha = 1$ to $\alpha = C$ where C represents the number of conjugacy classes. This statement is also sometimes referred to as the statement for the ***Great Orthogonality Theorem of Characters***.

This theorem can be used to arrive at a relationship between the number of classes of a group and the number of irreducible representations. We can write equation (2.175) as

$$\sum_\alpha [(\frac{n_\alpha}{|G|})^{1/2} \chi_\alpha^k][(\frac{n_\alpha}{|G|})^{1/2} (\chi_\alpha^{k'})^*] = \delta_{k,k'} \tag{2.153}$$

Let us introduce the vector

$$(\tilde{\mathbf{C}})_k = |G|^{-1/2} (\sqrt{n_1} \chi_1^k, \sqrt{n_2} \chi_2^k, ..., \sqrt{n_C} \chi_C^k) \tag{2.154}$$

So we can write the orthogonality equation (2.176) for characters

$$(\tilde{\mathbf{C}})_k . (\tilde{\mathbf{C}})_k = \delta_{k,k'} \tag{2.155}$$

The vectors $(\tilde{\mathbf{C}})_k$ reside in a space whose dimension is the number of classes C in the group. Hence, the maximum number of a set of mutually orthogonal vectors in this space is C. These vectors are labelled by an index k that correspond to the irreducible representations of the

group. Thus,

Number of Irreducible Representations $\leq$ *Number of Conjugacy Classes*

It is also possible to obtain an orthogonality relation that has the roles of the irreducible representations and conjugacy classes reversed in comparison to that in the *Great Orthogonality Theorem of Characters* [1]:

$$\sum_{\alpha} \chi_{\alpha}^{k} (\chi_{\beta}^{k'})^{*} = \frac{|G|}{n_{\alpha}} \delta_{\alpha,\beta} \tag{2.156}$$

By following an analogous line of reasoning as above, we can deduce that this relation implies that the

Number of Irreducible Representations $\geq$ *Number of Conjugacy Classes*

Combined with the statement of the Great Orthogonality Theorem of Characters, we have the following theorem:

Theorem 2.6. The number of conjugacy classes of the group is equal to the number of irreducible representations of that group.

Example 2.4. The symmetric group S_3 has three conjugacy classes. Thus, there are three irreducible representations which consist of two one-dimensional representations and one two-dimensional representation.

Theorem 2.7. (Decomposition Theorem) The character χ_{α} for the α class of any representation can be written in terms of the corresponding characters of the irreducible representations of the group as

$$\chi_{\alpha} = \sum_{k} a_k \chi_{\alpha}^{k}, a_k = \frac{1}{|G|} \sum_{\alpha} n_{\alpha} (\chi_{\alpha}^{k})^{*} \chi_{\alpha} \tag{2.157}$$

Proof. The same similarity transformation brings all of the matrices of a reducible representation into the same block-diagonal form. In this form, the matrix A_{α} can be written as the direct sum of matrices A_j^k of irreducible representations.

Given that similarity transformations leave the trace invariant, we can write the charac-

ter χ_i of this reducible representation corresponding to the ith class as

$$\chi_\alpha = \sum_k a_k \chi_\alpha^k, a_k \geq 0, a_k \in \mathbb{Z} \tag{2.158}$$

We can now multiply both sides of this equation by $n_\alpha(\chi_\alpha^{k'})^*$, sum over α, and use the orthogonality relation (2.175),

$$\sum_\alpha n_\alpha (\chi_\alpha^{k'})^* \chi_\alpha = \sum_k a_k \sum_\alpha n_\alpha (\chi_\alpha^{k'})^* \chi_\alpha^k = \sum_k a_k |G| \delta_{k,k'} = |G| a_{k'} \tag{2.159}$$

Thus,

$$a_{k'} = \frac{1}{|G|} \sum_\alpha n_\alpha (\chi_\alpha^{k'})^* \chi_\alpha \tag{2.160}$$

so $a_{k'}$ is the projection of the reducible representation onto the k'th irreducible representation. Now, since the number of irreducible representations equals the number of classes, according to Theorem 2.8, the orthogonal vectors of characters span a space whose dimensionality is the number of classes, and so this decomposition is unique.

The *Decomposition Theorem* helps in reducing the task of determining the irreducible representations contained within a reducible representation to one of vector algebra. Unless a certain application requires the matrix-forms of the representations, we do not need to block-diagonalize a representation to identify its irreducible components.

We can follow a procedure similar to the one that was used to prove the Decomposition Theorem to derive a criterion to identify whether a representation is reducible or not. We begin with the decomposition (2.157), take its complex conjugate and consider that $a_k \in \mathbb{Z}$:

$$\chi_\alpha^* = \sum_k a_{k'} (\chi_\alpha^k)^* \tag{2.161}$$

We now take the product of (2.157) and (2.161), multiply by n_α, sum over α, and invoke (2.156),

$$\sum_\alpha n_\alpha \chi_\alpha \chi_\alpha^* = \sum_{k,k'} a_k a_{k'} \sum_i n_\alpha \chi_\alpha^k (\chi_\alpha^{k'})^* = \sum_{k,k'} a_k a_{k'} |G| \delta_{k,k'} = |G| \sum_k a_k^2 \tag{2.162}$$

Thus,

$$\sum_\alpha n_\alpha |\chi_\alpha|^2 = |G| \sum_k a_k^2 \tag{2.163}$$

If the representation *is* irreducible, then $a_k = 0$ for all a_k except the one corresponding to that irreducible representation, for which $a_k = 1$. If the representation is reducible, then there will be at least two of these coeeficient a_k which satisfy $a_k > 0, a_k \in \mathbb{Z}$. We can put these observations into making a simple criterion for reducibility:

1. If the representation is irreducible, then

$$\sum_{\alpha} n_\alpha |\chi_\alpha|^2 = |G| \tag{2.164}$$

2. If the representation is reducible, then

$$\sum_{\alpha} n_\alpha |\chi_\alpha|^2 > |G| \tag{2.165}$$

Example 2.5. A representation of the symmetric group S_3 is

$$e = d = f = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.166}$$

$$a = b = c = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix} \tag{2.167}$$

The notation here is given with reference to (2.95) and (2.96). There are three conjugacy classes of this group, e, a, b, c, and d, f, so we have $n_1 = 1, n_2 = 3, n_3 = 2$, respectively.

The characters corresponding to the three classes are found to be

$$\chi_1 = 2, \chi_2 = 0, \chi_3 = 2 \tag{2.168}$$

Now,

$$\sum_{i=1}^{3} n_i |\chi_i|^2 = 12 > 6 = |G|_{S_3} \tag{2.169}$$

Using the criterion formed earlier, this representation is reducible. To determine the irreducible components of this representation, we use the decomposition theorem. There are three irreducible representations of the symmetric group S_3:

The one-dimensional *identical representation*, with characters

$$\chi_1^1 = 1, \chi_2^1 = 1, \chi_3^1 = 1, \sum_{i=1}^{3} n_i |\chi_i^1|^2 = 6 = |G|_{S_3} \tag{2.170}$$

The one-dimensional *parity representation*, with characters

$$\chi_2^1 = 1, \chi_2^2 = -1, \chi_3^2 = 1, \sum_{i=1}^{3} n_i |\chi_i^2|^2 = 6 = |G|_{S_3} \tag{2.171}$$

The two-dimensional *coordinate representation*, with characters

$$\chi_1^3 = 2, \chi_2^3 = 0, \chi_3^3 = -1, \sum_{i=1}^{3} n_i |\chi_i^3|^2 = 6 = |G|_{S_3} \tag{2.172}$$

We now calculate the values of a_k using (2.163). These identify the *projections* of the characters of the reducible representation onto the characters of the irreducible representation. We obtain

$$a_1 = 1, a_2 = 1, a_3 = 0 \tag{2.173}$$

Hence, this particular reducible representation is composed of the *identical representation* and the *parity representation*, without any contribution from the two-dimensional *coordinate representation*. The block-diagonal form of this representation is

$$e = d = f = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.174}$$

$$a = b = c = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.175}$$

Character Tables

Character tables are fundamental to various applications of group theory, especially those involving the decomposition of reducible representations into their irreducible constituents. In this section, the construction of character tables for groups will be discussed with an emphasis on the example of the symmetric group S_3. For this, two types of information are used: sum rules for the number and dimensionalities of the irreducible representations, and orthogonality relations for the characters of these representations. A point to note here is that by convention, characters tables are displayed with the columns labelled by the classes and

the rows by the irreducible representation.

The first step in the construction of the character table is to observe that, since $|G|_{S_3} = 6$ and there are three conjugacy classes, there are three irreducible representations whose dimensionalities must satisfy

$$d_1^2 + d_2^2 + d_3^2 = 6 \tag{2.176}$$

The unique solution of this equation, for $d_i \geq 0, d_i \in \mathbb{Z}, i \in \{1,2,3\}$, is $d_1 = 1, d_2 = 1, d_3 = 2$. Thus, there are two one-dimensional and one two-dimensional irreducible representations.

In the character table for any group, quite a few entries can be made immediately. The *identical representation*, where all elements are equal to unity, is always a one-dimensional irreducible representation. Similarly, the characters that correspond to the unit element are equal to the dimensionality of that representation, since they are always calculated from the trace of the identity matrix with that dimensionality. Therefore, denoting by α, β, γ, and δ quantities that are to be determined, the character table for S_3 is:

S_3	$\{e\}$	$\{a,b,c\}$	$\{d,f\}$
Γ_1	1	1	1
Γ_2	1	α	β
Γ_3	2	γ	δ

where the Γ_i, where $i \in \{1,2,3\}$ for S_3, are the conventional labels for the irreducible representations.

The remaining entries are determined from the orthogonality relations for characters. Taking elements for Γ_1 and Γ_2 for the orthogonality relations,

$$1 + 3\alpha + 2\beta = 0 \tag{2.177}$$

Taking only the elements for Γ_2 for the orthogonality relations

$$1 + 3\alpha^2 + 2\beta^2 = 6 \tag{2.178}$$

Considering, the multiplication table for the symmetric group S_3,

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
f	f	b	c	a	e	d
d	d	c	a	b	f	e

This group multiplication table requires that

$$a^2 = e, b^2 = e, c^2 = e, d^2 = f \tag{2.179}$$

Since the one-dimensional representations must obey the multiplication table, these products imply that

$$\alpha^2 = 1, \beta^2 = \beta \tag{2.180}$$

Using (2.178) and (2.180),

$$\beta = 1 \tag{2.181}$$

Using (2.170) and (2.181),

$$\alpha = -1 \tag{2.182}$$

Using the orthogonality relation (2.156) between the columns of the character table,

$$1 + \alpha + 2\gamma = 0 \tag{2.183}$$

$$1 + \beta + 2\delta = 0 \tag{2.184}$$

Using the values of α and β from (2.181) and (2.182), respectively, in (2.183) and (2.184),

$$\gamma = 0, \delta = -1 \tag{2.185}$$

Thus, the complete character table of the symmetric group S_3 is

S_3	$\{e\}$	$\{a,b,c\}$	$\{d,f\}$
Γ_1	1	1	1
Γ_2	1	-1	1
Γ_3	2	0	-1

When character tables are compiled, a notation is used that reflects the fact that the elements of the group correspond to transformations on physical objects. The notation for the classes

of S_3 are as follows:

1. $\{e\} \rightarrow E$: The *identity* element

2. $\{a,b,c\} \rightarrow 3\sigma_v$: Reflection through vertical planes, where *vertical* stands for the planes that contain the axis of highest rotational symmetry. In the case of the symmetric group S_3, it is the z-axis. The $'3'$ refers to the fact that there are three elements in this class.

3. $\{d,f\} \rightarrow 2C_3$: Rotation by $\frac{2\pi}{3}$ radians, where the $'2'$ refers to there being two elements in this class. The notation C_3^2 is for rotations by $\frac{4\pi}{3}$ radians and so the *class* notation is only meant to indicate the type of operation. In general, C_n refers to rotations through $\frac{2\pi}{n}$ radians.

Several notations are also used for irreducible representations. One of the most common is to use

A for one-dimensional representations
E for two-dimensional representations
T for three-dimensional representations

Subscripts are used in the notation for the representations to distinguish multiple occurrences of irreducible representations of the same dimensionality. The character table for S_3 is denoted as that of the group C_{3v} as that components are interpreted as the planar symmetry operations of an equilateral triangle.

We can write the S_3 character table as

C_{3v}	E	$3\sigma_v$	$2C_3$
A_1	1	1	1
A_2	1	-1	1
E	2	0	-1

2.3.4 Representations of Symmetric Groups S_n

The symmetric group S_n on a finite set is the group whose elements are all permutation operations, which are defined as bijective functions from the set of n symbols to itself. The group operation is the composition of such permutation operations. There are various ways to denote the elements and their permutations of the symmetric group. For example, let

us say we have three balls Red (R), Blue (B) and Green (G), as shown in Figure 2. Then any permutation of these balls can be reached from an initial state, let's say RGB (linear arrangement of the balls).

There are various ways to denote the permutations of the elements of the symmetric group, as well:

1. *Square Parantheses* [...] denote the new ordering of elements. For example, [213](RGB) permutes the second ball to the first position, first ball to the second position and keeps the third ball as it is, giving us the new arrangement (GRB).

2. *Cylic notation*, represented by the round brackets (...), denotes the subgroups over which permutation takes place. For example, the case taken in the point above can be represented in cyclic notation as (12)(3). This tells us that the first and second balls swap places while the third one stays put.

This result can be generalized to a general symmetric group S_n. If we represent the elements of the general symmetric group S_n as $i_1, i_2, ..., i_k$, with all being different, the cyclic notation for the permutations can put as follows:

$$(i_1 i_2)(i_2 ... i_k) = \begin{cases} i_1 \to i_1 \to i_2 \\ i_2 \to i_3 \to i_3 \\ i_3 \to i_4 \to i_4 ... \\ i_k \to i_2 \to i_1 \end{cases} = (i_1 i_2 ... i_k) \tag{2.186}$$

$$(i_1 i_2 i_3)(i_3 ... i_k) = \begin{cases} i_1 \to i_1 \to i_2 \\ i_2 \to i_3 \to i_3 \\ i_3 \to i_4 \to i_4 ... \\ i_k \to i_3 \to i_1 \end{cases} = (i_1 i_2 ... i_k) \tag{2.187}$$

$$(i_1 ... i_k)(i_k i_1) = \begin{cases} i_1 \to i_k \to i_1 \\ i_2 \to i_2 \to i_3 \\ i_3 \to i_3 \to i_4 ... \\ i_k \to i_1 \to i_2 \end{cases} = (i_2 i_1 ... i_k) \tag{2.188}$$

$$(i_1...i_k)(i_k i_2 i_1) = \begin{cases} i_1 \to i_k \to i_1 \\ i_2 \to i_1 \to i_2 \\ i_3 \to i_3 \to i_4... \\ i_k \to i_2 \to i_3 \end{cases} = (i_3 i_1 i_2 ... i_k) \tag{2.189}$$

and so on. Due to the above relations (2.186) - (2.189), one can construct all the group

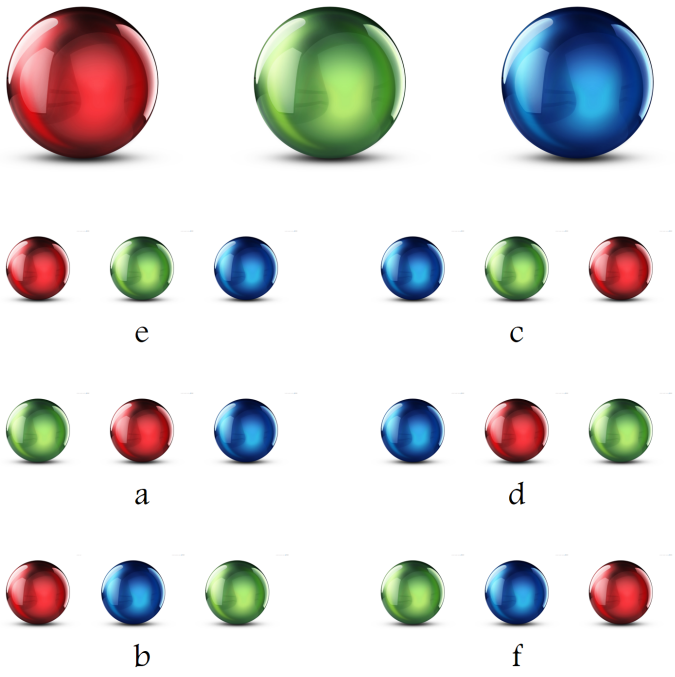


Fig. 2.3 Illustration of Symmetric Group S_3, corresponding to elements shown in Figure 1, using coloured balls

elements of S_n using only the transpositions $(12),(13),...,(1n),(23),...,(2n),....,(n-1,n)$. This can be further restricted to the set $\{(12)(23)(34),...,(n-1,n)\}$.

We can take the example of group S_4 to illustrate this point. We will be showing the relevance of the group S_4 for our cluster-state quantum computation model later in the thesis. This group can be formed using only the set $\{(12)(23)(34)\}$.

$$(13) = (12)(23)(12) \tag{2.190}$$

$$(14) = (12)(23)(12)(34)(12)(23)(12) \tag{2.191}$$

$$(24) = (23)(12)(34)(12)(23) \tag{2.192}$$

Interestingly, the product of all elements of the set of transpositions yields the following

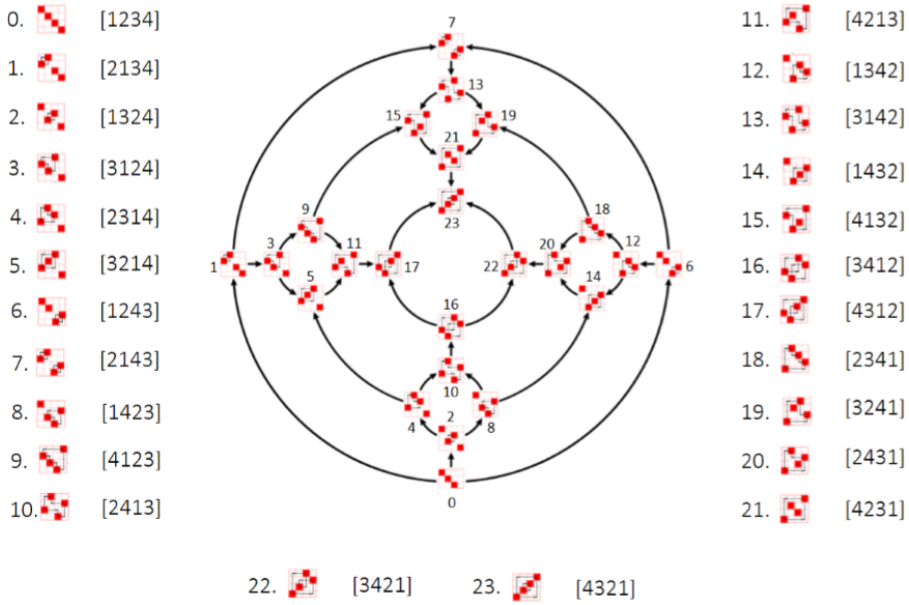


Fig. 2.4 Permutations represented by matrices for the symmetric group S_4. Here the red boxes for matrix-elements have a value of 1 while white boxes have value 0. The straight arrows between two permutations depict an inversion operation while a curved arrow depicts a rotation operation

group element of S_n:

$$(12)(23)(34)...(n-1,n) = (123....n) \tag{2.193}$$

It can be shown that the complete permutation group S_n can be generated by (12) and $(123...n)$.

Matrix Representations of Symmetric Group S_4

An n-dimensional matrix representation of a group element g of the group G is given by a transformation $D(g)$ of an n-dimensional, complex vector space V_n into itself

$$D(g) : V_n \to V_n \tag{2.194}$$

The matrix for $D(g)$ is known, once the transformation of the basis vectors $\hat{e}_i$ $(i = 1,2,...,n)$ of V_n is specified. In this section, we will look into an example of matrix representations of

symmetric groups, with an emphasis on S_4.

One can use the word representation for the vector associate with the S_4 group: ABCD. This can be written as

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = A \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + B \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + C \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + D \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{2.195}$$

An example of a symmetric group element is the transformation (12)(3)(4) which is given by

$$D^w(12) \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} \rightarrow \begin{pmatrix} B \\ A \\ C \\ D \end{pmatrix} \tag{2.196}$$

The element $D^w(12)$ is given by

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.197}$$

The various group elements are given by

$$D^w(I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.198}$$

$$D^w(12) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.199}$$

$$D^w(23) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.200}$$

$$D^w(132) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.201}$$

$$D^w(123) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.202}$$

$$D^w(13) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.203}$$

$$D^w(34) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.204}$$

$$D^w(12)(34) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.205}$$

$$D^w(243) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.206}$$

$$D^w(1432) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.207}$$

$$D^w(1243) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.208}$$

$$D^w(143) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.209}$$

$$D^w(234) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.210}$$

$$D^w(1342) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.211}$$

$$D^w(24) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.212}$$

$$D^w(142) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.213}$$

$$D^w(13)(24) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.214}$$

$$D^w(1423) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.215}$$

$$D^w(1234) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.216}$$

$$D^w(134) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.217}$$

$$D^w(124) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.218}$$

$$D^w(14) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.219}$$

$$D^w(1324) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.220}$$

$$D^w(14)(23) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.221}$$

2.3.5 Partitions and Young Tableau

The cyclic structure of a group element of S_n can be represented by a partition of n.

Definition 2.9. A partition of n is a set of positive integer numbers: $[\lambda_1, \lambda_2, ..., \lambda_k]$ with $\lambda_1 \geq \lambda_2 \geq \lambda_3 ... \geq \lambda_k$ and $\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_k = n$.

Considering the class structure of the symmetric group S_n, we see that the conjugacy classes are given by cycle structures and a particular conjugacy class is specified by giving the n numbers $\xi_1, \xi_2, ..., \xi_n$, where ξ_i is the number of i cycles in an element belonging to the conjugacy class.

Example 2.5. In the group S_6, for $(1426)(35) \in S_6$, $\xi_1 = 0, \xi_2 = 1, \xi_3 = 0, \xi_4 = 1, \xi_5 = 0, \xi_6 = 0$.

We can observe that $\sum_{i=1}^{n} i\xi_i = n$. The specification of a class of the symmetric group corresponds to the specification of a partition of n that can be defined by the construction:

$$\lambda_1 = \xi_1 + \xi_2 + ... + \xi_n \tag{2.222}$$

$$\lambda_2 = \xi_2 + ... + \xi_n \tag{2.223}$$

and so on, with $\lambda_n = \xi_n$.

For the case in *Example 2.5*,

$$\lambda_1 = 2 \tag{2.224}$$

$$\lambda_2 = 2 \tag{2.225}$$

$$\lambda_3 = 1 \tag{2.226}$$

$$\lambda_4 = 1 \tag{2.227}$$

$$\lambda_5 = 0 \tag{2.228}$$

$$\lambda_6 = 0 \tag{2.229}$$

and the sum of these numbers is six.

We use this correspondence in the inventing a graphical description to represent the partition of the symmetric group, known as *Young Diagrams*.

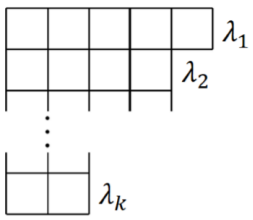


Fig. 2.5 Example of Young Diagram of the Symmetric Group S_k with λ_1 boxes in the first row, λ_2 boxes in the second row, and so on, as determined by the values of the partitions for a cyclic structure of a group element of S_n

Definition 2.10. A Young diagram is a figure of n boxes arranged in horizontal rows in the following way:

λ_1 boxes in the upper row
λ_2 boxes in the second row
...
λ_k boxes in the k-th and last row.

Illustration 2.1. The partitions and Young diagrams for the cyclic structures of the symmetric group S_4 are as follows

1. *Partition [4]*: The elements constituting this conjugacy class are (1234), (1243), (1324), (1342), (1423) and (1432) in cyclic notation.

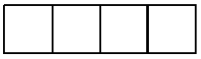


Fig. 2.6 Partition [4] of the symmetric group S_4 of four elements

In this class, none of the elements permute.

2. *Partition [31]*: The elements constituting this conjugacy class are (1)(234), (1)(243), (123)(4), (132)(4), (124)(3), (142)(3), (134)(2) and (143)(2). In this class, one of the

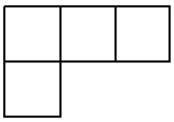


Fig. 2.7 Partition [31] of the symmetric group S_4 of four elements

elements permutes with one other element.

3. *Partition [22]*: The elements constituting this conjugacy class are (12)(34), (13)(24) and (14)(23). In this class, two of the elements permute with two other elements.

4. *Partition [211]*: The elements constituting this conjugacy class are (1)(2)(34), (1)(23)(4), (1)(24)(3), (12)(3)(4), (13)(2)(4) and (14)(2)(3). In this class, two of the elements permute with each other while two others remain unpermutated.

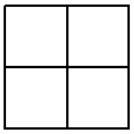


Fig. 2.8 Partition [22] of the symmetric group S_4 of four elements

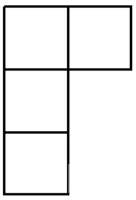


Fig. 2.9 Partition [211] of the symmetric group S_4 of four elements

5. *Partition [1111]*: The element constituting this conjugacy class is (1)(2)(3)(4). In this class, none of the elements permute.

Fig. 2.10 Partition [1111] of the symmetric group S_4 of four elements

It is observed that the Young diagrams for a given n classifies all the conjugacy classes of S_n. Since the conjugacy classes are related to the irreducible representations of a symmetric group, it is not surprising that these diagrams are also useful in identifying irreducible representations of S_n. There is found to be a $1:1$ correspondence between Young diagrams and irreducible representations of S_n. To define this irreducible representations, one requires what are known as *Young's Tableau*.

Definition 2.11. A Young tableau is a Young diagram in which the n boxes are filled with the numbers $1,...,n$, each number used only once.

For example, one of the Young tableau for S_4 is shown in Figure 2.11.

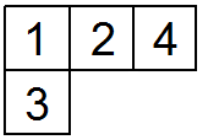


Fig. 2.11 Young Tableau for a [31] Irreducible Representation of the symmetric group S_4

Definition 2.12. A *standard Young tableau* is a Young tableau in which the numbers appear in ascending order within each row from left to right and within each column from top to bottom.

Example 2.6. For the S_4 group, we have the Young Tableau given in Figures 2.12 - 2.16.

There are many other interesting connections between Young tableaux and representations of S_n. One of this is as follows: Let us say that we have an irreducible representation in S_n and we want to find its induced representation in S_{n+1}. It is found that the induced representation is simply the direct sum of all the representations corresponding to the Young diagrams that are obtained by adding one new square to the original Young diagram at various points below or to the right of a pre-existing Young diagram element!

Example 2.7. The induced representation of the standard representation from S_3 to S_4 is shown in Figure 2.13. Similarly, the restricted representation (construction of the standard representation of a lower symmetric group from a higher symmetric Group, such as S_2 from S_3) can be obtained by removing one square from the Young diagram, as shown in Figure 2.14.

2.3.6 Structures of Irreducible Representation

Now that we have found a way to find the number of irreducible representations of the symmetric group using Young Tableau, it is important to explore a way to find the structure of the irreducible representations.

Irreps of Symmetric Group S_3

As has been discussed previously, the symmetric group S_3 can be analysed by looking at a triangular arrangement of elements ABC, wherein each element is equidistant from every

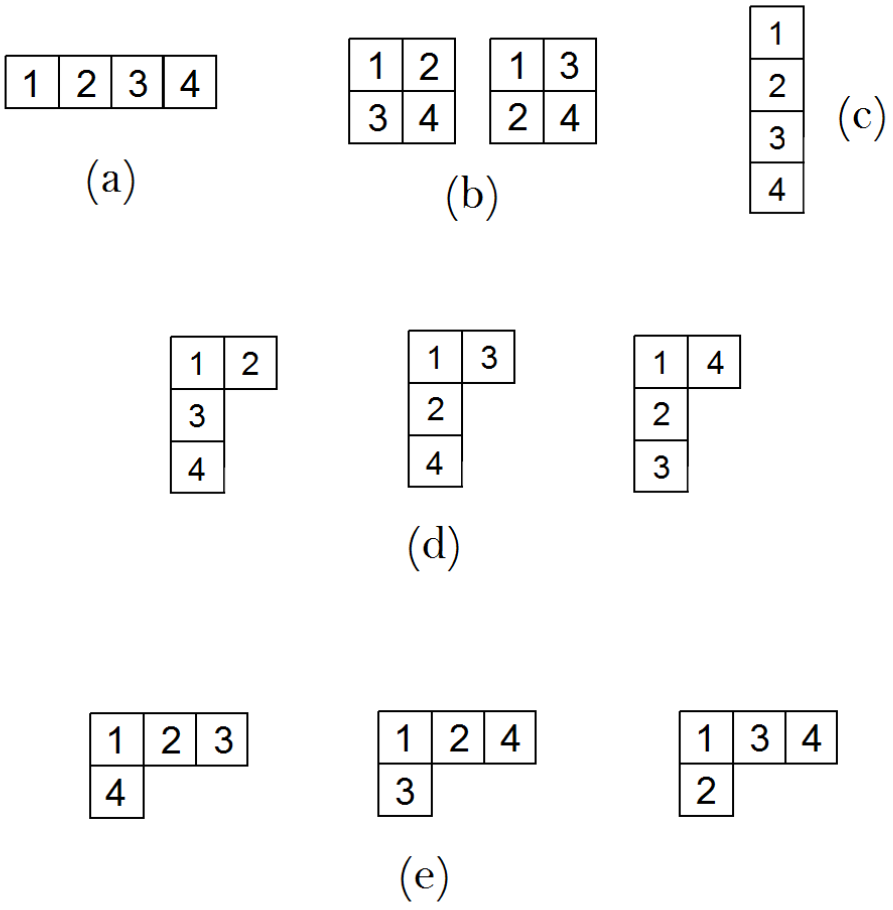


Fig. 2.12 Young Tableau of the symmetric group S_4 for (a) Partition [4], (b) Partition [22], (c) Partition [1111], (d) Partition [211] and (e) Partition [31]

other element. This equilateral triangle can be used to derive a set of matrix representations for S_3.

The representation $D^w(132)$: $D^w(132)ABC = BCA$ has an analogy to a rotation of this equilateral triangle by an angle of 120°. This transformation is given, in matrix form, as the rotation matrix for an angle of 120°.

$$R = \begin{pmatrix} cos\theta|_{\theta=120^\circ} & -sin\theta|_{\theta=120^\circ} \\ sin\theta|_{\theta=120^\circ} & cos\theta|_{\theta=120^\circ} \end{pmatrix} \tag{2.230}$$

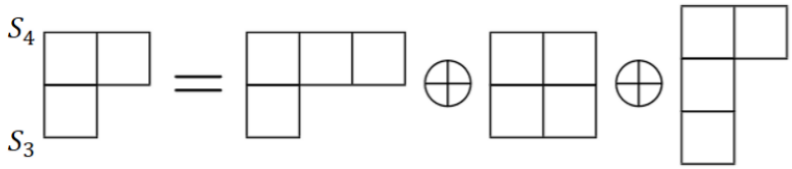


Fig. 2.13 Induced representation of the standard representation from S_3 to S_4

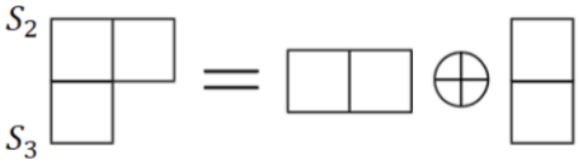


Fig. 2.14 Induced representation of the standard representation from S_3 to S_2

This simplifies to

$$R = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \tag{2.231}$$

The reflection operation around x-axis keeps the x-component of a point on the plane unchanged while the y-component of the point accumulates a phase of 180°.

$$P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.232}$$

This is equivalent to taking ABC to ACB. One can construct the various elements of the group from the transformations $\{I, P, R, R^2, PR, PR^2\}$ for S_3.

Irreps of the Symmetric Group S_n

A group has an infinite number of representations, in principle, even for a finite group like S_n. So, how can one organize the representations of such a group in an ordered manner? The answer to this question lies in the concepts of reducible and irreducible representations. Before going into the concept of reducibility of representations, let us consider the concept of the equivalence of representations

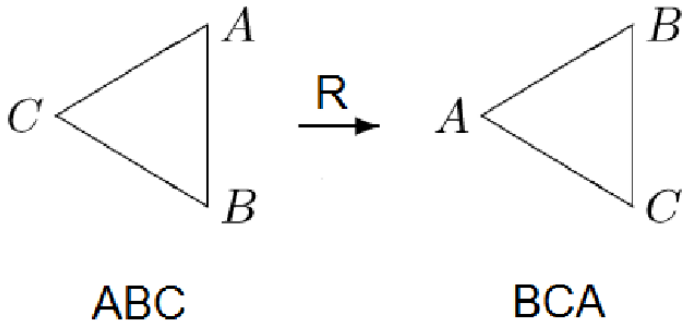


Fig. 2.15 Rotation by an angle of 120° brings elements A to position of C, C to position of B and B to position of A

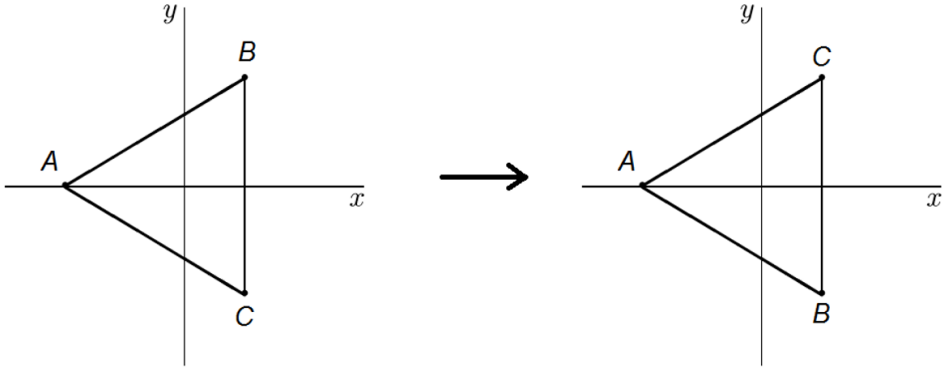


Fig. 2.16 Reflection around x-axis brings elements B to position of C, C to position of B, leaving the element A unaffected in this illustration

Let us consider two n-dimensional representations, $D^{(\alpha)}$ and $D^{(\beta)}$, of the group G. If there exists a non-singular $n \times n$ matrix S, such that for all group elements g we have

$$D^{(\alpha)}(g) = S^{-1} D^{(\beta)}(g) S \tag{2.233}$$

then the two representations $D^{(\alpha)}$ and $D^{(\beta)}$ are said to be equivalent.

Irreducible representations or irreps are the building blocks of representations of a group. All other representations can be constructed out of irreps. The dimensions for the irreps of a group, such as the symmetric groups S_n, can be found using Young Tableu. In doing so, we need to look into the concepts of *axial distance*, *hook length* and *hook product* of elements in Young Tableau.

Definition 2.13. (Yamanouchi Symbol) A Yamanouchi Symbol of a Young Tableau is a notation of its elements of the form $[y_1 y_2 ... y_n]$, where y_i represents the position of the element i in a Young Tableau and takes the value of the row in the Young Tableau in which the element i is placed.

Example 2.8. The Yamanouchi symbol for the Young Tableau in Figure 2.17 is [1212].

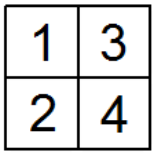


Fig. 2.17 Young Tableau of Symmetric Group S_4 with the associated Yamanouchi symbol being [1212]

Definition 2.9. The axial distance $\rho(M;x,y)$ between two boxes x and y of a standard Young tableau M (M represents the Yamanouchi symbol of the tableau), is the number of steps (horizontal and/or vertical) to get from x to y, where steps contribute:

$$\begin{cases} +1 for \downarrow or \leftarrow \\ -1 for \uparrow or \rightarrow \end{cases} \tag{2.234}$$

Definition 2.10. (Hooklength) The hook length $h(i,j)$ of a box (i,j) in a Young Tableau is one plus the sum of the number of boxes that are in the same row i to the right of it and the number of boxes in the same column j below it.

Example 2.9. The hooklength of the element with the black-dot in Figure 2.18 is 3.

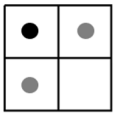


Fig. 2.18 Illustration for Hooklength: The hooklength of the box with the black dot is 3. The boxes with the grey-dots are in the same column or row as the box with the black dot

Definition 2.11. (Hook-Product) The product of hooklengths of all the boxes in a Young Tableau is called the Hook-Product.

Example 2.10. The hook-product of the Young Tableau in Figure 2.19 is 12.

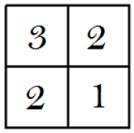


Fig. 2.19 Illustration for Hook-Product: The hook-product of the Young Tableau is $3 \times 2 \times 2 \times 1 = 12$

Definition 2.12. (Dimension of Irreducible Representations) In evaluating the irreps for a group, one needs to consider the dimension of an irrep given by $f[\mu]$, which is the number of possible standard Young tableaux for a given partition. The dimension $f[\mu]$ of an irrep of S_n corresponding to a Young diagram $[\mu]$ (where $[\mu]$ represents the corresponding partition of n) can be found from

$$f[\mu] = \frac{n!}{h[\mu]} \tag{2.235}$$

where $h[\mu]$ is the hook-product. The hookproduct $h[\mu]$ of the Young diagram belonging to the partition $[\mu]$, is the product of all numbers in its hook-table.

For the S_4 group, we have

$f[\mu]$ = 1 for the partition [4]
$f[\mu]$ = 3 for the partition [31]
$f[\mu]$ = 2 for the partition [22]
$f[\mu]$ = 3 for the partition [211]
$f[\mu]$ = 1 for the partition [1111]

Once the dimensions of these irreps have been found, we move on to finding the form of the irreps. For this, we employ the concept of Young's orthonormal forms, which are real and unitary. The irrep $[\mu]$ of S_n is defined in an $f[\mu]$-dimensional vector space $V^{[\mu]}$. In this, we use the orthonormal basis $\hat{e}_i^{\mu}$ where $i = 1,2,3,....,f[\mu]$

$$(\hat{e}_i^{[\mu]}, \hat{e}_j^{[\mu]}) = \delta_{ij} \tag{2.236}$$

To the index i of the basis vector we relate the Yamanouchi symbol M.

In terms of the basis vectors, one obtains the standard form for the matrix representation:

$$D^{[\mu]}((k,k+1))e^{[\mu]}_{M_1\ldots M_n} = (\rho(M_1\ldots M_n;k+1,k))^{-1}\hat{e}^{[\mu]}_{M_1\ldots M_n} + A\hat{e}^{[\mu]}_{M_1\ldots M_{k+1}M_k\ldots M_n} \tag{2.237}$$

where $A = \sqrt{1-(\rho(M_1\ldots M_n;k+1,k))^{-2}}$

Example 2.11. Let us look into the construction of irreducible representations of S_4 using the construction scheme mentioned above.

To begin with, let us take the following basis vectors:

$\hat{e}^{[1111]}_{1234}$ for the partition [1111]
$\hat{e}^{[211]}_{1123}$, $\hat{e}^{[211]}_{1213}$ and $\hat{e}^{[211]}_{1231}$ for the partition [211]
$\hat{e}^{[22]}_{1122}$ and $\hat{e}^{[22]}_{1212}$ for the partition [22]
$\hat{e}^{[31]}_{1112}$, $\hat{e}^{[31]}_{1121}$ and $\hat{e}^{[31]}_{1211}$ for the partition [31]
$\hat{e}^{[4]}_{1111}$ for the partition [4]

where

$$\hat{e}^{[211]}_{1123} = \hat{e}^{[31]}_{1112} = \begin{pmatrix}1\\0\\0\end{pmatrix}, \hat{e}^{[211]}_{1213} = \hat{e}^{[31]}_{1121} = \begin{pmatrix}0\\1\\0\end{pmatrix}, \hat{e}^{[211]}_{1231} = \hat{e}^{[31]}_{1211} = \begin{pmatrix}0\\0\\1\end{pmatrix} \tag{2.238}$$

$$\hat{e}^{[22]}_{1122} = \begin{pmatrix}1\\0\end{pmatrix}, \hat{e}^{[22]}_{1212} = \begin{pmatrix}0\\1\end{pmatrix} \tag{2.239}$$

Using equation (2.237), we can find the matrix representation for the generator transpositions (12), (23) and (34).

$D(12) = -1$ for [1111]

$$D(12) = \begin{pmatrix}1 & 0 & 0\\0 & -1 & 0\\0 & 0 & -1\end{pmatrix} \text{ for [211]}$$

$$D(12) = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \text{ for [22]}$$

$$D(12) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ for [31]}$$
$$D(12) = 1 \text{ for [4]}$$

$$D(23) = -1 \text{ for [1111]}$$
$$D(23) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ for [211]}$$
$$D(23) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \text{ for [22]}$$
$$D(23) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \text{ for [31]}$$
$$D(23) = 1 \text{ for [4]}$$

$$D(34) = -1 \text{ for [1111]}$$
$$D(34) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} \\ 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} \end{pmatrix} \text{ for [211]}$$
$$D(34) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ for [22]}$$
$$D(34) = \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ for [31]}$$
$$D(34) = 1 \text{ for [4]}$$

These are the fundamental representations of the S_4 group, which can be used to build various reducible representations.

2.3.7 Symmetric Group, Heisenberg Hamiltonian and $SWAP^{1/n}$ Quantum Operators

The Symmetric Group, by virtue of its relevance in multiple fields of mathematics and physics, is an important element of abstract algebra. Not only is it significant as the key building block in Galois Theory and the mathematical basis of the 100-vertices undirected graph called the Higman-Sims graph, but is also found to be associated to the all-important Heisenberg Hamiltonian in Physics. The Heisenberg exchange model is a many-body quantum model, which has has been applied to fields as varied as multipolar exchange interactions and high-temperature superconductivity.

In 1928, Werner Heisenberg proposed the (Heisenberg) model, noting that the internactions had a certain spin-free nature and the model had a symmetric-group character [2]. These two aspects have been of particular interest, particularly to the likes of the famous chemist F. A. Matsen. In 1971, he looked into the spin-free group-theoretic nature [3]. Later, alongwith Cosgrove and Picone, he also looked into a symmetric group-theoretic solution of a special, uniform interaction case of the model in 1971 [4], and relations to spin-correlations in 1975 [5].

Let us briefly follow Heisenberg and Matsen's view in seeking a symmetric-group algebraically motivated solution to the Heisenberg Hamiltonian, which for a collection of N doublet spin-1/2 sites, is given by

$$\mathbf{H} = \sum_P \mathbb{J}_P \mathbf{P} \tag{2.240}$$

where $\mathbf{P}$ is a permutation acting on the indices of the sites of the system and $\mathbb{J}_P$ is a coupling constant. Often, the non-zero $\mathbb{J}_P$ are assumed to be only for transpositions $P = ij$, which interchange the indices of nearest neighbour sites i and j. In the spin-space, the Dirac-identity

$$(ij) = 2\vec{S}_i.\vec{S}_j + \frac{1}{2} \tag{2.241}$$

may be used to express the hamiltonian in terms of the spin operators. Clearly, H is an element of the group algebra of the symmetric group S_n acting on the N spin indices. If we consider the unitary evolution operator U for the hamiltonian H obtained from equations (2.240) and (2.241) in the time-dependent case,

$$H(t) = \mathbb{J}_P(t)\vec{S}_i.\vec{S}_j \tag{2.242}$$

$$U_P(t) = \tau exp[-\frac{i}{\hbar}\int_0^t H(t')dt'] = \tau exp[-\frac{i}{\hbar}\int_0^t \mathbb{J}_P(t')\vec{S}_i.\vec{S}_j dt'] \tag{2.243}$$

For a constant interaction $\mathbb{J}_P(t) = J_0$ and time $\tau_s s.t. \frac{J_0\tau_s}{\hbar} = \pi mod(2\pi), U_P(\tau_s/2) = U_P(\tau_s)^{1/2}$ performing the so-called 'Square-Root-of-SWAP' gate, that is functionally given by,

$$\sqrt{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.244}$$

Given the pre-eminent position of this operator, it is interesting to note that this operator falls into the symmetric group S_n, just like the general Heisenberg Hamiltonian. Now, from our study of representations of (symmetric) groups earlier in this chapter, we know that any representation of $\sqrt{SWAP}$ can be decomposed into the irreducible representations of the symmetric group S_n. But for convenience, we will be using the reducible representation for the $SWAP = \sqrt{SWAP}\sqrt{SWAP}$ instead, which are the permutation matrices. This case of $\sqrt{SWAP}$ is extended to the case of $SWAP^{1/n}$ too.

Before moving further, let us see why the similarity transformation for the *SWAP* should work for the $SWAP^{1/n}$ as well:

Similarity Transformation for SWAP and $\sqrt{SWAP}$

By definition, we see that

$$U_{SWAP^{1/n}} = \frac{1+e^{i\pi/n}}{2}U_{SWAP} + \frac{1-e^{i\pi/n}}{2}I_{2^N\times 2^N} \tag{2.245}$$

where $I_{2^N\times 2^N}$ is a $2^N \times 2^N$ identity matrix. Premultiplying with S^{-1} and postmultiplying with S, we have

$$S^{-1}U_{SWAP^{1/n}}S = \frac{1+e^{i\pi/n}}{2}S^{-1}U_{SWAP}S + \frac{1-e^{i\pi/n}}{2}I_{2^N\times 2^N} \tag{2.246}$$

Since the linear combination of the block-form of U_{SWAP} and a a $2^N \times 2^N$ identity matrix maintains the block-form of J_1 albeit with possibly different matrix-elements, $J_2 = S^{-1}U_{SWAP^{1/n}}S$ has the same similarity transformation and the same set of magic-vectors.

The similarity transformation for *SWAP* and $SWAP^{1/n}$ are found to be the same. Hence, the magic vectors associated with the transformation are relevant for both operations.

$$J_1 = S^{-1} U_{SWAP} S \tag{2.247}$$

where J_1 is the block-form representation for the *SWAP* operation.

Having found that the similarity transformation for *SWAP* applies for $\sqrt{SWAP}$ operator, let us look at the reducible representations of the *SWAP* operator. For a general n-qubit system, we will have a vector of dimensional 2^n. The *SWAP* operator will swap the elements of each of vector-components. For example, a $SWAP_{12}|01101\rangle = |10101\rangle$, where the first and second qubits are swapped. This can be realized using a permutation matrix, which we investigated earlier in the chapter. A permutation matrix is a square binary matrix that has only one entry of 1 in each row and each column and 0s every where else. Each such matrix P represents a permutation of m elements and multiplied with another matrix, say A, results in permuting the rows (when pre-multiplying: PA) or columns (when post-multiplying: AP) of the matrix A.

Example 2.12. The permutation matrix P_π corresponding to the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$ is given by

$$P_\pi = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.248}$$

The three major properties of any permutation matrix are:

1. A permutation matrix is non-singular.

2. The determinant of a permutation matrix is always ± 1

3. A permutation matrix P_π always satisfies

$$P_\pi P_\pi^T = I \tag{2.249}$$

Now, that we have the reducible representations of a general *SWAP* operator in the form of the permutation matrices, our next task is to see how we could optimally find all the irreducible representations of the various cases. This is where the concepts of *Cayley Graphs* and *Cayley Trees* come in handy.

2.3.8 Cayley Graph and Cayley Tree

For a lower dimensional symmetric-group, finding the irreducible representations is easy but as we go to higher dimensions, the number of irreducible representations increases as well, making it a tedious task to find them. To make matters convenient, we have the concept of the *Cayley Graph*.

Definition 2.13. A Cayley graph, also known as a Cayley diagram, is a graph that encodes the abstract structure of a group.

Suppose that G is a group and X is a generating set. The Cayley graph $\Gamma = \Gamma(G,X)$ is a colored directed graph constructed as follows:

1. Each element $g \in G$ is assigned a vertex, which is part of the vertex set $V(\Gamma)$ of Γ, identified with G.

2. Each generator $x \in X$ is assigned a color c_x.

3. For any $g \in G$, $x \in X$, the vertices corresponding to the elements g and gx are joined by a directed edge of colour c_x. Thus the edge set $E(\Gamma)$ consists of pairs of the form (g, gx), with $x \in X$ providing the color.

The Cayley graph $\Gamma(G,X)$ depends on the choice of the set X of generators. For instance, if the generating set X has k elements then each vertex of the Cayley graph has k incoming and k outgoing directed edges.

2.3.9 From Separable States to Invariant Subspaces of the Symmetric Group

Having found a way to efficiently and quickly find the irreducible representations, and having obtained the reducible representations for the *SWAP* operator, we come to the fundamental problem of the thesis relating to the creation of quantum states (and the entanglement

therein): operating combinations of $SWAP^{1/n}$ gate to a separable quantum state and finding the output states and patterns of multipartite entanglement in them. Since the $SWAP^{1/n}$ is a Hamming-weight preserving operator, we will have invariant subspaces with vectors that are superpositions of states with the same Hamming weight.

The basic system we are working on comprises of a lattice of spin $\frac{1}{2}$ particles that are connected by edges with initially dormant $SWAP^{1/n}$ operators that can be switched on for generating entanglement between the elements. For understanding the kind of states we can obtain from the system, we will have to look into the group-theoretic aspects of the system using equivalence relations to find a similarity transformation that can transform the reducible representations for the *SWAP* operator and provide us with the magic-vector states for the $SWAP^{1/n}$ operator (since the similarity transformation for *SWAP* and $SWAP^{1/n}$ are the same).

Now, if P represents the permutation matrix for the system and T represents the block-diagonal form for the same, by equivalence,

$$P = STS^{-1} \tag{2.250}$$

where S is the similarity transformation for the reducible representation.

In our method, we have found the ways to determine the matrices P and T. Thus, from this information we can find S for an N-qubit case by solving the $N!$ simultaneous linear equations: $P_iS - ST_i = 0$, where i denotes a particular group element and $i = 1,2,3,...,N!$. A point to note here is that this does not give us a unique value of S and this has to be determined by imposing the unitarity condition on this matrix.

The magic-vectors for an operator under similarity-transformation is given by

$$V' = S^{-1}V \tag{2.251}$$

where V is the vector for the untransformed system and V' is the vector for the transformed system. This provides us with vector states that comprise a complete invariant subspace. Any state that preserves the permutation symmetry associated with the subspace can be expressed a linear superposition of the vectors comprising that subspace. It is found that for some states (and Hamming weights), there are more than one invariant subspace associated with these states. For instance, in the case of four qubits, there is a [31], [22] and [4] invariant subspaces associated with Hamming weight 2 (quantum states with two $|0\rangle$ and two $|1\rangle$). A point to

note here is that in terms of ascendancy of symmetries, for this case, $[4] > [31] > [22]$.... Hence, when an arbitrary state with this Hamming weight is given, one needs to see the highest symmetry of the state and accordingly choose the invariant subspace for it.

This approach is fairly comprehensive and complete, it relies heavily on conceptual tools like the *Cayley Tree*, which are not easily found for higher number of qubits. This leads to difficulty in finding the P_i and T_i matrices, and by extension, the S matrix. To get around this problem, we have explored and investigated an alternative approach using the nullspace approach.

2.4 Symmetric States and the Nullspace Approach

One of the fundamental properties of the $SWAP^\alpha$ gates are that they conserve Hamming weight of the representation. The number of $|0\rangle$s and $|1\rangle$s in a multiqubit state remain the same. This is a key to proposing an efficient algorithm for finding the vector states associated with the invariant subspaces for the $SWAP^\alpha$ gates.

Let us say we have the following families of n-qubit states:

$$W_i = PERM(|\underbrace{00..0}_{n-i}\underbrace{11...1}_{i}\rangle) \tag{2.252}$$

where PERM defines the permutation function for a given set of qubits.

There is no map, $f(U_{SWAP^\alpha})$ comprising of only $SWAP^\alpha$ that can take us from one such family W_i to another family W_j for $i \neq j$. This property can be used to define the set of basis vector-sets by starting with a completely symmetric state using all the vectors in the family W_i and then finding the nullspace vectors for the same. We have found an algorithm and realization of the same that can carry out quick and efficient generation of the vector-states for n-qubits under operation by $SWAP^\alpha$ gates.

Let V be the set of basis vectors corresponding to the 2^n dimensional Hilbert space of n-qubit system; V=$\{v_{\phi_0}, v_{\phi_1}, ..., v_{\phi_{n^2-1}}\}$. In order to decompose the 2^n x 2^n matrix representation of S_n to block diagonal form a transformation matrix R needs to be found. R is constructed by finding a new set of basis vectors, in which the representation is in block diagonal form. Let us call this new basis $X = \{x_1, x_2, .., x_{n^2}\}$ and define V_i, where $i \in [0, n]$), as the set of of vectors, corresponding to states with i 1_s.e.g. for n=2, $V_0 = \{v_{00}\}, V_1 = \{v_{01}, v_{10}\}, V_2 = \{v_{11}\}$.The

Power-of-SWAP operations do not change the number of 1_s in the quantum state, therefore each of V_i is invariant subspace, although not necessarily an irreducible one. Therefore, the task reduces to decomposing each of V_i. Also observe that the number of vector in V_i is given by:

$$|V_i| = \frac{n!}{(n-i)!} = \binom{n}{i} \tag{2.253}$$

A point to note here is that each $V_i = V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i}$ and $V_{i,j}$ is isomorphic to $V_{k,j}$ for any i, j, k. Here $V_{i,j}$ are irreducible invariant subspaces.

Algorithm

1. For $i = 0$ (and $i = n$), V_0 (V_n) has a single vector which is one-dimensional invariant subspace, corresponding to the trivial irrep.

2. For i=1, from equation (2.276), $|V_1| = n$, and $V_1 = V_{1,0} \bigoplus V_{1,1}$. Also $V_0 = V_{0,0}$ is isomorphic to $V_{1,0}$. Therefore $|V_{1,0}| = 1$ and $|V_{1,1}| = n-1$. The one element of $V_{1,0}$ can be written as the sum of all vectors in V_1, $\{\sum_{v \varepsilon V_1} v/\sqrt{n}\}$, and $V_{1,1}$ can be found by taking the orthogonal compliment of $V_{1,0}$ in V_1.

3. The case for i$\geq$2, becomes more interesting. We know that $V_i = V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i}$. Firstly $V_{i,i}$ and its orthogonal complement space in V_i, let us call it O, need to be determined. We also know that $|O|$=$|V_{i-1}|$ and$O$== $V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i-1}$.

4. To find O, a set of $\binom{n}{(i-1)}$ basis vectors $\{o_k\}$ need to be formed. The procedure to form this vectors is as follows:

   (a) Label the vectors in V_i by their corresponding quantum states. For instance, n=4, i=2, $V_1 = \{v_{0011}, v_{0101}, v_{0110}, ...\}$

   (b) Form all sets of length i of different numbers in the range $[1, n]$, and call them $\{s_k\}$. There will be

   (c) For each s_k form basis vector o_k by summing over all vectors of V_i which corresponds to states with 1_s at the positions s_k. For instance, for n=4, i=2, $o_1 = v_{0011} + v_{0101} + v_{1001}$, $o_2 = v_{0011} + v_{0110} + v_{1010}$,...

Once, all o_k are formed, O is known and $V_{i,i}$ can be formed by taking the orthogonal complement of O inside V_i. O is isomorphic to V_{i-1}. Therefore, O can be decomposed

in the same way as V_{i-1}.

5. By finding the basis vectors of the each $V_{i,j}$ the new basis X is determined and the transformation matrix R can be constructed by taking its columns to be the vectors of X.

In this manner, the vector states for any arbitrary symmetric group and qubit system can be used. We find that the number of invariant subspaces, N_{inv}, for an n-qubit system is given by:

$$N_{inv} = \begin{cases} \frac{1}{4}(n+2)^2, \text{if n is even} \\ \frac{1}{4}(n+1)(n+3), \text{if n is odd} \end{cases} \quad , n > 1 \tag{2.254}$$

The form of, and number of basis vectors comprising, an invariant subspace are related to a particular symmetry under permutations of the qubits. For instance, the three-qubit quantum state that is invariant under a *proper rotation* of all elements is $|\psi\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ and the conjugacy class related to $[3]$ comprises of only this vector.

If we have a quantum state of the form

$$|\psi\rangle = \sum_{PERM(i)} \alpha_i |\underbrace{00..0}_{k}\underbrace{11...1}_{n-k}\rangle_i \tag{2.255}$$

where i is an index related to each permutation of the qubits and the summation is over i, all the permutations of the qubits. We expect that for any value of k we have invariance under certain transpositions and their associated conjugacy classes. We find that we need to know about only specific conjugacy classes for each value of k, under which a state remains invariant. The transpositions related to the remaining conjugacy classes can be represented by the transpositions associated to this established set of conjugacy classes.

For even n and $k \leq \frac{n}{2}$, the relevant conjugacy classes are $\mathscr{C}^{(k)} = \{C_i^{(k)}\} = \{[n], [n-1,1], ..., [n-k,k]\}$, where the i is the index of the conjugacy classes for a fixed value of k. This is because the symmetries under transpositions $[n-(k+1), k+1], ..., [11..(\text{n times})]$ are encapsulated in the existing set C_i. An example of this is shown in Figure 2.20 for $k = 1$, where the $[n-2,2]$ is shown to be an instance of the permutation $[n]^{(\otimes 3)}$. For even n and $k > \frac{n}{2}$, the relevant conjugacy classes are $C_i^{(k)} = \{[n], [n-1,1], ..., [n-(n-k), n-k]\}$. Thus, there are $(n+1)$ basis vector-sets associated with the invariant subspace $[n]$, $(n-1)$ for $[n-1,1]$, $(n-3)$ for $[n-2,2]$ and so on till 1 set for $[\frac{n}{2}, \frac{n}{2}]$, with there being $\frac{n}{2}+1$ kinds of subspaces that are relevant. As a result, $N_{inv}^{(\text{even n})} = \frac{1}{2}(\frac{n}{2}+1)((n+1)+1) = \frac{1}{4}(n+2)^2$.

For odd n, we have conjugacy classes $C_i^{(k)} = \{[n],[n-1,1],...,[n-k,k]\}$ for $k \leq \frac{n-1}{2}$ and

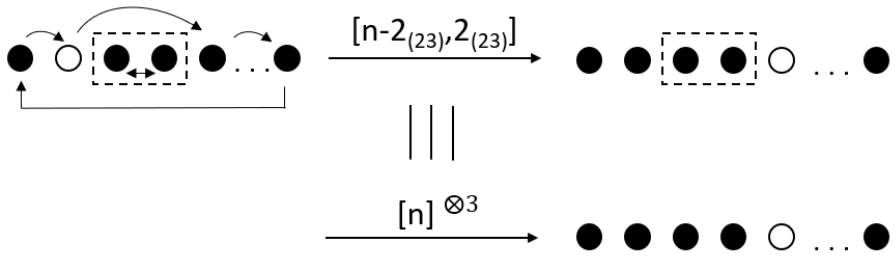


Fig. 2.20 Illustration of representation of permutation $[n-2,2]$ as an instance of the permutation $[n]^{(\otimes 3)}$ for $k = 1$

$C_i^{(k)} = \{[n],[n-1,1],...,[n-(n-k),n-k]\}$ for $k \geq \frac{n+1}{2}$. We have $(n+1)$ basis vector-sets associated with the invariant subspace $[n]$, $(n-1)$ for $[n-1,1]$, $(n-3)$ for $[n-2,2]$ and so on till 2 sets for $[\frac{n+1}{2},\frac{n-1}{2}]$, with there being $\frac{n-1}{2}+1$ kinds of subspaces that are relevant. As a result, $N_{inv}^{(\text{odd n})} = \frac{1}{2}(\frac{n-1}{2}+1)((n+1)+2) = \frac{1}{4}(n+1)(n+3)$.

In this manner, we use both numeric and analytic methods to study the quantum states in a system operated upon by a combination of Power-of-SWAP operators. In the next chapter, we will be looking at how this resource can be used, by studying the separability and entanglement characteristics of these states.

Chapter 3

Separability and Quantum Entanglement

"Quantum physics thus reveals a basic oneness of the universe."

— Erwin Schrödinger

Correlations between properties of particles or elements exist in a lot of physical systems. Be it spin correlations in quarks or orthographic correlations in astrophysics, these correlations provide a basis for describing the collective state of two or more particles in nature. In the quantum domain, we find a unique form of correlation that implies the existence of a state of a composite system, comprising of constituent elements, which cannot be written as a product of the states of individual subsystems. Originally called "*Verschränkung*" by Erwin Schrödinger, this phenomenon is today known as "entanglement" and was first studied by the trio of Einstein, Podolsky, and Rosen (EPR), and independently by Schrödinger. The 'spooky' feature of entanglement lies at the heart of quantum mechanics.

In this chapter, we will look into ways of characterizing this using two different approaches: one, using separability and the other using entanglement witnesses.

3.1 Separability

The problem of knowing how entangled a certain quantum state is, is of utmost importance before the entanglement within the quantum state can be used. This constitutes the entanglement characterization or *quantum separability problem*, which is of central importance

in quantum information theory [225–229]. Different kinds of entanglement can be used for different applications. Maximally entangled states can be used for applications such as teleportation [230] and remote state preparation [231] while partially entangled states are used for applications such as measurement-based quantum computation [162, 163, 165] and separable states are usually used as ancilla qubits in various quantum computing protocols [232, 233].

The separability problem for the bipartite case is well understood and an efficient computation method to determine separability is the Schmidt/Singular Value decomposition[234–236]. An N qubit pure state,

$$|\Psi\rangle = \sum_{n=0}^{2^N-1} a_n |n\rangle \tag{3.1}$$

is said to be separable under a particular bipartition if it can be written in the form,

$$|\Psi\rangle = \left|\Psi^A\right\rangle \otimes \left|\Psi^B\right\rangle. \tag{3.2}$$

If it cannot be written in this form then it is said to be entangled. The bipartitions of the system can be written as the various separability classes: $[s, N-s]$ denoting a general separability class formed of an s qubit sub-system and an $N-s$ qubit sub-system. Generally, there will be ${}^N C_s = \frac{N!}{s!(N-s)!}$ ways to arrange N qubits into a sub-system of size s.

The case of multipartite separability is more involved and has been shown to be NP-hard by Leonid Gurvits [237–239]. The exponential growth of the Hilbert Space causes the separability classes in the multipartite case to be more complex in form and structure. Not only do the number of separability classes for N qubits scale as the partition function for N elements, the manner in which these partitions can be filled by different combinations of elements (qubits) leads to there being a number of partitions for the same separability class. For example, the separability class [21] for three-qubits, where the first two qubits are entangled while the last qubit is separable, can have three cases: $[2_{12}1_3]$, $[2_{13}1_2]$ and $[2_{23}1_1]$. In the first case, qubit 3 is the separable qubit while in the second and third cases, the qubits 2 and 1 are separable respectively.

An N qubit state is said to be fully separable if it can be written in the form,

$$|\Psi\rangle = \prod_{\otimes i=1}^{N} (\alpha_0^{(i)} |0_i\rangle + \alpha_1^{(i)} |1_i\rangle) \tag{3.3}$$

where $\sqrt{|\alpha_0^{(i)}|^2+|\alpha_1^{(i)}|^2}=1$. The index (i) denotes the i^{th} qubit and it runs from 1 to N and the direct product runs over all N qubits. If a state is not separable in any subsystem of qubits then it is said to be *entangled*. Partially separable states are those in which there are two or more subsystems formed of many qubits. Where N is greater than 2, the bipartite separability described above is a particular instance of a partially separable state. A state is partially separable if it can be written in the form,

$$|\Psi\rangle = |\psi_1^{(a_1^{(1)},a_2^{(1)},...,a_{m_1}^{(1)})}\rangle \otimes |\psi_2^{(a_1^{(2)},a_2^{(2)},...,a_{m_2}^{(2)})}\rangle \otimes ... \otimes |\psi_n^{(a_1^{(n)},a_2^{(n)},...,a_{m_n}^{(n)})}\rangle \tag{3.4}$$

where $|\psi_l^{(a_1^{(l)},a_2^{(l)},...,a_{m_l}^{(l)})}\rangle$ denotes the l^{th} subsystem that has m_l qubits: $\{(a_1^{(l)},a_2^{(l)},...,a_{m_l}^{(l)})\}$, which are entangled among themselves and there are n subsystems. There will be $\frac{N!}{s_1!s_2!s_3!...}$ ways to arrange N qubits into the $[s_1,s_2,s_3,...]$ separability class. Due to symmetry, we introduce an additional factor of $\frac{1}{2}$ for every subsystem that is equal in size to another.

One of the most thorough methods to classify separability is the comparison method [240]. Each separability class has a standard form for the quantum states associated with it. Comparing a general state to this standard form is a good way to check if the state belongs to the separability class. Let us take the example of four-qubits to illustrate this method. A four-qubit state could be in one of five different separability classes: the [4] completely entangled class, the [31] separability class, the [22] separability class, the [211] separability class and [1111] completely separable class. The standard forms for these classes are as follows:

$$|\psi_{[1111]}\rangle = (a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b_2|1\rangle)(a_3|0\rangle + b_3|1\rangle)(a_4|0\rangle + b_4|1\rangle)$$

$$|\psi_{[211]}\rangle = (\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle)(a_3|0\rangle + b_3|1\rangle)(a_4|0\rangle + b_4|1\rangle)$$

$$|\psi_{[22]}\rangle = (\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle)(\beta_1|00\rangle + \beta_2|01\rangle + \beta_3|10\rangle + \beta_4|11\rangle)$$

$$\begin{aligned}|\psi_{[31]}\rangle = (\alpha_1|000\rangle + \alpha_2|001\rangle + \alpha_3|010\rangle + \alpha_4|011\rangle + \alpha_5|100\rangle + \alpha_6|101\rangle \\ + \alpha_7|110\rangle + \alpha_8|111\rangle) \times (a_4|0\rangle + b_4|1\rangle)\end{aligned}$$

Here any permutation of size 1 is expressed in terms of $\{a_i,b_i\}$ for the i^{th} qubit, while for higher dimensional cycles, the subsystems are expressed in terms of $\{\alpha_k\}$ where k is the decimal equivalent of Q in the qubit representation $|Q\rangle$ for which α_k is the multiplicative constant in the superposition for that susbsystem.

If we take a random quantum state, say the four-qubit W-state $|\psi\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$, and compare it to these standard forms, we can ascertain the specific separability class of the state. Since the W-state cannot be expressed in terms of any of the aforementioned separability classes, the state is completely entangled.

3.1.1 The Thread and Bead Model

Geometric tools like the Bloch representation of vectors can help us study separability conditions of quantum states. As part of my doctoral project, I have also looked into a certain new model of depicting and studying the separability of quantum states: the thread-and-bead model. In this model an arbitrary quantum system is represented in terms of threads and beads. Each state in the superposition in the system is represented by a single thread. Every qubit in these states has an associated bead: a 'single' bead for $|0\rangle$ and a 'double' bead for $|1\rangle$. The important property in this representation is that if two or more beads have the same nature ('single' or 'double'), they join together only for that bead. This is an effective way to see how separable a state is: the more it is connected in being 'beaded together', the more separable they are.

The interesting part about this approach is that more entangled these threads are, more separable are the corresponding states, and vice versa! Let us look at an illustration, in Figure 3.1. The primary problem with this approach that we found relates to the probability factors

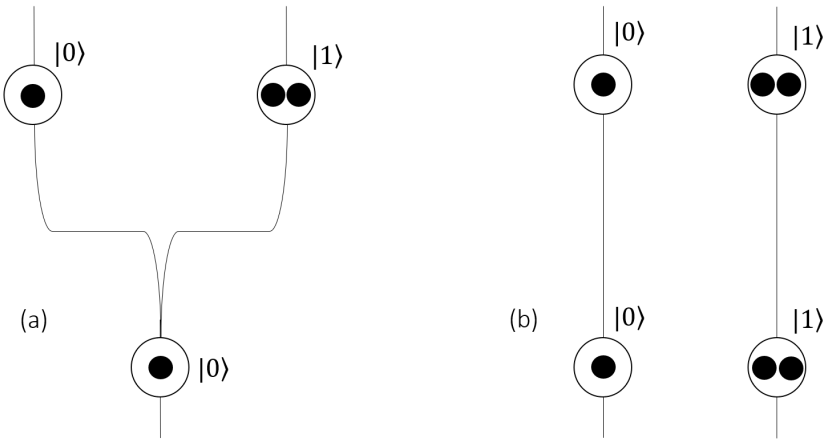


Fig. 3.1 Illustration of the Thread-and-Bead Model for two qubits: (a) separable state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ and (b) maximally entangled Bell-state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

associated with the beads. Entanglement depends significantly on these factors. A general

two-qubit state $\alpha|0\rangle + \beta|1\rangle$ does not have the same entanglement as state $\alpha'|0\rangle + \beta'|1\rangle$ for $\alpha \neq \alpha', \beta \neq \beta'$. To tackle this problem, we proposed a method of changing the girth of the thread associated with a superposition term depending on the probability factor. This helps in understanding not only the separability in quantum states, qualitatively, but also nuances of how entangled a quantum state is.

3.1.2 A Classical Approach to Separability

Separability testing is an NP-hard problem, in general [238, 227]. The difficulty within the problem can be seen if one attempts to solve the problem by a brute-force approach, for a fixed dimension. We end up seeing that, even for low dimensions, the problem quickly becomes intractable. Hence, more sophisticated methods are required for the same. As a result, the separability problem is quite an important subject of current research in quantum information theory.

There are two different classical methods we will be discussing in this section: the method of optimal separable approximation as given by Leinaas et al [241] and a partition-based classical algorithm that we have put forward.

Classical Separability Check using Optimal Separable Approximations

In their paper Leinaas et al [241] offer a numerical approach in an iterative manner, refining an estimated separable state towards the target quantum state to be tested, and checking if the target state can indeed be reached.

Let us assume that we have a test state ρ. Let ρ_s be a separable state such as a pure product state. We consider what is known as the direction from ρ_s to ρ, denoted by $\sigma = \rho - \rho_s$. In order to improve the estimate of the separable state ρ_s we look for a pure product state ρ_p that maximizes the scalar product

$$s = Tr[(\rho_p - \rho_s)\sigma] \tag{3.5}$$

or equivalently, maximizes $s' = Tr(\rho_p\sigma)$.

If $s > 0$, then it is possible to find a closer separable state ρ_s' by mixing in the product state ρ_p. This search for closer separable states is continued by iteration, either until no pure product state ρ_p can be found such that $s > 0$, which means that s is already the unique separable state closest to ρ, or until some other criterion for convergence is satisfied.

There are two mathematical sub-problems that have to be solved numerically in this algorithm and approach. The first problem is to find the pure product state maximizing the scalar product s'. The second problem is the quadratic programming problem, which lays out a method to find the convex combination of a finite number of pure product states which is closest to the given state ρ.

To approach the first sub-problem, we must note that a pure product state ρ_p has matrix elements of the form

$$\langle ij|\rho_p|kl\rangle = \phi_i \chi_j \phi_k^* \chi_l^* \tag{3.6}$$

where $\sum_i |\phi_i|^2 = \sum_j |\chi_j|^2 = 1$.

We would like to find complex coefficients ϕ_i and χ_j that maximize

$$s' = Tr(\rho_p \sigma) = \sum_{i,j,k,l} \phi_i^* \chi_j^* \sigma_{ij;kl} \phi_k \chi_l \tag{3.7}$$

The iteration scheme given below is found to be an efficient numerical method. It may not give a global maximum, but at least it gives a useful local maximum that may depend on a randomly chosen starting point.

The method is based on the observation that the maximum value of the variable s' is the maximal eigenvalue μ in the two linked eigenvalue problems

$$\sum_k A_{ik} \phi_k = \mu \phi_i, \sum_l B_{jl} \chi_l = \mu \chi_j \tag{3.8}$$

where

$$A_{ik} = \sum_{j,l} \chi_j^* \sigma_{ij;kl} \chi_l, B_{jl} = \sum_{i,k} \phi_i^* \sigma_{ij;kl} \phi_k \tag{3.9}$$

As a result, we may start with any arbitrary unit vector $|\chi\rangle = \sum_j \chi_j |j\rangle_B \in \mathscr{H}_B$ and compute the Hermitian matrix A. We compute the unit vector $|\phi\rangle = \sum_i \chi_i |i\rangle_A \in \mathscr{H}_A$ as an eigenvector of A with maximal eigenvalue, and then we use it to compute the Hermitian matrix B. Next, a new unit vector $|\chi\rangle$ is computed as an eigen-vector of B with maximal eigenvalue, and we keep iterating the procedure.

This scheme produces a non-decreasing sequence of values for the function s' that must converge to a certain maximum value. This is a local maximum at least, and there corresponds to

it at least one product vector $|\phi\rangle \otimes |\chi\rangle$ and product density matrix $\rho_p = (|\phi\rangle\langle\phi|) \otimes (|\chi\rangle\langle\chi|)$. If $s > 0$,the above construction of ρ_p implies that there exist separable states

$$\rho_s^{'} = (1-\lambda)\rho_s + \lambda\rho_p \tag{3.10}$$

with $0 < \lambda \leq 1$, closer to ρ than ρ_s is. However, it turns out to be inefficient to search only along the line segment from ρ_s to ρ_p for a better approximation to ρ. It is more efficient to append the new ρ_p to a list of product states ρ_{pk} found in previous iterations, and then minimize

$$F = Tr(\rho - \sum_{\lambda} \lambda_k \rho_{pk})^2 \tag{3.11}$$

which is a quadratic function of coefficients $\lambda_k \geq 0$ with $\sum_k \lambda_k = 1$. This quadratic programming problem is solved by adapting the conjugate gradient method. A given product matrix ρ_{pk} is thrown away if and only if the corresponding coefficient λ_k becomes zero when F is minimized. In practice, this means that we may construct several product states altogether, but only a limited number of those, typically less than 100 in the cases we have studied, are included in the final approximation s.

3.1.3 Partitioning Algorithm

This classical approach to studying separability relies on partitioning states and checking for separability in the various permutations for the separability class.

Algorithm:

1. For an n-qubit state, we start with the simplest separability class $[n-1,1]$ and initialize two registers of strings with $|0^{\otimes n-1}\rangle$ and $|0\rangle$ respectively.

2. We then select the first qubit as our '1' in $[n-1,1]$ and the remaining quantum state as '$n-1$'. We then store the first qubit of the first superposition state in the register and its corresponding remaining subsystem in the second register. We do the same for all the superposition states. If the entries for all the superposition states are the same in the second register then we say that the state is separable in '$[n-1_{234\ldots n}, 1_1]$'

3. We then select the second qubit as our '1' in $[n-1,1]$ and the remaining quantum state as '$n-1$', and carry out the same step as the last. We continue taking all the qubits individually for as '1' in '$[n-1,1]$.

4. We move to the next separability class $[n-2,2]$ and carry out the entire process for different permutations.

5. For multipartite separable states like '$[\alpha_1, \alpha_2, ...\alpha_k]$ for some positive integer k, we will need k different registers for the same process as mentioned in the steps above.

The culmination of the realization of this algorithm would be the determination of the exact separability class of the quantum state under consideration.

3.1.4 Quantum Correlations and Permutation Symmetries

Quantum entanglement has been closely linked to various kinds of symmetries in physics [242–246]. Entangled many-body systems [247–249] are subject to symmetries that play a major role in fields such as quantum information theory [250–255]. Symmetries can also help in determining the nature of entanglement present in these systems [256, 257]. We find that the connection between quantum non-locality and permutation symmetries, more specifically local permutability, can be used to characterize the non-local correlations between qubits.

A separable quantum state can be represented as

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes ... \otimes |\psi_n\rangle \tag{3.12}$$

for an n-partite separable state. Let us say that we have for each separable sub-system, a general expansion

$$|\psi_i\rangle = \sum_j \alpha_j^{(i)} |\psi_{i,j}\rangle \tag{3.13}$$

Now, if we define local permutation as a permutation operation on the i^{th} subsystem that shifts its constitutent k_i superposition terms by one place within the subsystem, keeping the rest of the system unchanged. Let us denote such a local permutation operator by U_i, and its action as

$$\begin{aligned} &|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes (\alpha_1^{(i)} |\psi_{i,1}\rangle + \alpha_2^{(i)} |\psi_{i,2}\rangle + ... + \alpha_{k_i}^{(i)} |\psi_{i,k_i}\rangle) \otimes ... \otimes |\psi_n\rangle \\ &\xrightarrow{U_i} |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes (\alpha_{k_i}^{(i)} |\psi_{i,k_i}\rangle + \alpha_1^{(i)} |\psi_{i,1}\rangle + ... + \alpha_{k_i-1}^{(i)} |\psi_{i,k_i-1}\rangle) \otimes ... \otimes |\psi_n\rangle \end{aligned} \tag{3.14}$$

As can be seen this local permutation operator on the i^{th} qubit keeps the state invariant for a separable state. We will look at two kinds of permutations in this section: firstly, when the

permutation is confined to the subspace of the subsystem Hilbert space that is spanned by the initial vectors within the subsystem of the state $|\psi\rangle$, and secondly, when the permutation is not confined and can access any part of the subsystem Hilbert Space.

Let us see what happens if we take an entangled state, with the example of the maximally entangled two-qubit Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and operate U_2:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{U_2} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3.15}$$

This clearly changes the state, taking it to another Bell state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. In this case, the permutation is over the confined subspace $\{|0\rangle, |1\rangle\}$ but since this also spans the entire one-qubit Hilbert Space, one can simply conclude that a local permutations changes the state if the state is an entangled state in two-qubits. Is this still the case for higher number of qubits?

Let us take the case of the three qubit W-state

$$\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \xrightarrow{U_{23}} \frac{1}{\sqrt{3}}(|000\rangle + |001\rangle + |110\rangle) \tag{3.16}$$

If we perform a general permutation within the confined subspace, as defined above, the permutation is confined to $\{00, 01, 10\}$, and the remaining subsystems do not remain invariant under such a transformation, in general, unless we have a trivial identity element, showing the non-separability of the W-state. In the latter case, where the permutation can be over the entire subspace Hilbert Space, this confinement is not present. In this section, we will look more closely at both these cases.

Local Permutation within a Confined Subspace

If we have a bipartite separable pure state $|\chi\rangle = |\phi\rangle \otimes |\psi\rangle$ with partitions $\varepsilon = \{\phi, \psi\}$, the aforementioned local permutation within a confined space can be realized using the operator:

$$U_{rs_{\varepsilon^{(k)}}} = \mathbb{I} \otimes \sum_i \frac{\langle \varepsilon_p^{(k)} | \chi \rangle}{\langle \varepsilon_i^{(k)} | \chi \rangle} |\varepsilon_p^{(k)}\rangle \langle \varepsilon_i^{(k)}| \tag{3.17}$$

where $\varepsilon_l^{(k)}$ represents the l^{th} vector-state in superposition within the k^{th} partition. In this operator, the $\varepsilon_i^{(k)}$ is being permuted to the $\varepsilon_p^{(k)}$ vector state. A point to note here is that there is an inherent cyclicity in this operator for this to work: the last term in superposition is permuted to the first, for a simple permutation operation that shifts all vector state by one to

the right in the superposition. If a state is separable in a particular partition, it is found that the operation of such an operator leaves the state invariant. We can generalize this idea to a more efficient operator that considers all permutations at once:

$$U'_{rs_\psi} = \mathbb{I} \otimes \sum_i \sum_j |\varepsilon_j^{(k)}\rangle\langle\varepsilon_i^{(k)}| \tag{3.18}$$

with the relative phases not being considered here, for convenience of representation.

It is found that formalism can be extended to the case of mixed states. An N-partite separable mixed state can be represented by the density matrix: $\rho = |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes ... \otimes |\psi_N\rangle\langle\psi_N|$. Operating with the operator U_{rs_ψ},

$$\begin{aligned} U_{rs_\psi}(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| \otimes ... \otimes |\psi_N\rangle\langle\psi_N|) \\ = (|\psi'_1\rangle\langle\psi_1| \otimes |\psi'_2\rangle\langle\psi_2| \otimes ... \otimes |\psi'_N\rangle\langle\psi_N|) \end{aligned} \tag{3.19}$$

where $|\psi'_i\rangle$ is the vector state that $|\psi_i\rangle$ is permuted into. For the bipartite case $\rho = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|$, this operation gives us

$$U_{rs_\psi}(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|\otimes) = |\phi\rangle\langle\psi| \otimes |\psi\rangle\langle\phi| \tag{3.20}$$

which gives us the familiar partial transpose form. A point to note here is that, unlike in the permutation of a pure state where the state was found to be invariant under this operation, the partial transpose of a density matrix of a separable state is not equal to the density matrix itself. However, they have certain common shared characteristic properties, such as the determinant and eigenspectrum, which can be used for characterization of separability. Now, let us look at two properties of matrices under partial transposition: their determinants and eigenspectra.

Statement 3.1. A state is separable if and only if the partial transpose of its density matrix has a non-negative determinant.

Proof. We know that a characteristic equation of a matrix A is given by

$$det(A - \lambda I) = (-1)^n(\lambda - \lambda_1)(\lambda - \lambda_2)...(\lambda - \lambda_n) \tag{3.21}$$

where I is the identity matrix of the same dimensions as A, λ is a variable and $\{\lambda_1, \lambda_2, ..., \lambda_n\}$ are the eigenvalues of the matrix A. Setting $\lambda = 0$,

$$det(A) = \lambda_1 \lambda_2 ... \lambda_n \tag{3.22}$$

Now, if we express $\rho = |\psi\rangle\langle\psi|$ and find its eigenvalues, corresponding to the eigenvector $|\phi\rangle$,

$$\langle\phi|\rho|\phi\rangle = \langle\phi|\psi\rangle\langle\psi|\phi\rangle = |\langle\phi|\psi\rangle|^2 \geq 0 \tag{3.23}$$

Using equations (3.19) and (3.20),

$$det(\rho) \geq 0 \tag{3.24}$$

For a general Kronecker Product $A \otimes B$ for n-dimensional A and m-dimensional B, where $A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$ and $B = \begin{pmatrix} b_{11} & b_{12} & ... & b_{1q} \\ b_{21} & b_{22} & ... & b_{2q} \\ ... & ... & ... & ... \\ b_{p1} & b_{p2} & ... & b_{pq} \end{pmatrix}$,

$$\begin{aligned} A \otimes B &= \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ ... & ... & ... & ... \\ a_{m1}B & a_{m2}B & ... & a_{mn}B \end{pmatrix} \\ &= \begin{pmatrix} B & 0 & 0 & ... & 0 \\ 0 & B & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & B \end{pmatrix} \begin{pmatrix} a_{11}I_q & a_{12}I_q & ... & a_{1n}I_q \\ a_{21}I_q & a_{22}I_q & ... & a_{2n}I_q \\ ... & ... & ... & ... \\ a_{m1}I_q & a_{m2}I_q & ... & a_{mn}I_q \end{pmatrix} \\ &= (I_m \otimes B)(A \otimes I_q) \end{aligned} \tag{3.25}$$

where I_q is the identity matrix of dimension q. For $m = n, p = q$, $A \otimes B = (I_m \otimes B)(A \otimes I_p)$. Now, considering the determinant of this Kronecker Product

$$det(A \otimes B) = det(I_m \otimes B) det(A \otimes I_p) = det(B)^p det(B)^m \tag{3.26}$$

If our density matrix is separable, it can be expressed as $\rho = \rho_1 \otimes \rho_2$ for an two-partite system. Taking the partial transpose over any one subsystem, say, the second subsystem, and

finding the determinant of the same using equation (3.23)

$$det(\rho_1 \otimes (\rho_2)^T) = det(\rho_1)^{d_2} det((\rho_2)^T)^{d_1} = det(\rho_1)^{d_2} det(\rho_2)^{d_1} = det(\rho_1 \otimes \rho_2) = det(\rho) \geq 0 \tag{3.27}$$

where d_i represents the dimensions of the density matrix of the i^{th} subsystem, and we have used the property that $det(A^T) = det(A)$ for any matrix A.■

Statement 3.2. A state is separable if and only if the partial transpose of its density matrix has only non-negative eigenvalues.

Proof. Considering any general matrix A and using the characteristic polynomial of the transpose of the matrix,

$$det(A^T - \lambda I) = det((A - \lambda I)^T) = det(A - \lambda I) \tag{3.28}$$

where the symmetric property of the identity matrix has been used, besides the property that $det(M^T) = det(M)$ for a general matrix M. Thus, the characteristic polynomials of both A and A^T are the same. As a result, the eigenvalues of A^T and A are the same.

Using this result for a density matrix $\rho = \rho_1 \otimes \rho_2$, the partial transpose with respect to the second subsystem: $\rho_1 \otimes (\rho_2)^T$ preserves the eigenspectrum of ρ. Since the eigenvalues of ρ are non-negative, the eigenvalues of the partial transpose with respect to the i^{th} subsystem ρ^{T_i} are also non-negative. ■

This is actually the statement of the famous Partial Positive Transpose (PPT) condition [152], which is a necessary and sufficient condition for separability. Thus, we have, starting with the idea of permuting subsystem-states and partial transposition, independently reached a set of conditions that corroborate with a necessary and sufficient condition in the PPT criterion.

One of the key problems in contemporary quantum entanglement and separability characterization is in the realization of conceptual tools and maps, such as the partial transpose, in physical systems. Horodecki and Ekert [258] proposed the method known as structural physical approximation (SPA) which provides a way in which non-physical operations that can detect entanglement such as the partial transpose can be approximated systematically by physical operations. *Lim et al* [259] presented a practical scheme to realize a physical

approximation to the partial transpose.They did this using local measurements on individual quantum systems and classical communication.

Given this way of realizing the partial transpose, we have developed an algorithm for determining whether a state is entangled and thereafter which entanglement class it belongs to. The physical realization of the non-unitary operator that we use in this method would rely on local measurements and state preparation as well. This is something that we will not discuss beyond the theoretical formulation of the concept, in this project. Before going on to our algorithm, we will define an operator that will play a pivotal role in the algorithm:

Theorem 3.1. A multiqubit state $|\chi\rangle$, with M superposition states, has a bipartite separability in the partitions $\varepsilon^{(k)} = \{\phi, \psi\}$ for the form $|\chi\rangle = |\phi\rangle \otimes |\psi\rangle$ if after the operation of the operator $U_{rs_{\varepsilon^{(k)}}}$ (where $\varepsilon^{(k)}$ represents the partition that has the separable qubits)

$$U_{rs_{\varepsilon^{(k)}}} = \mathbb{I} \otimes \sum_i |\frac{\langle \varepsilon_{i+1}^{(k)} | \chi \rangle}{\langle \varepsilon_i^{(k)} | \chi \rangle}| \, |\varepsilon_{i+1}^{(k)}\rangle \langle \varepsilon_i^{(k)}| \tag{3.29}$$

the state maps back onto itself. $|\varepsilon_i^{(k)}\rangle$ represents the i^{th} superposition state in the $\varepsilon^{(k)}$ partition.

Proof. Let us take the composite quantum system:

$$|\chi\rangle = |\phi\rangle \otimes |\psi\rangle \tag{3.30}$$

where

$$|\phi\rangle = \sum_{i=1}^{m} \alpha_i |\phi_i\rangle \tag{3.31}$$

$$|\psi\rangle = \sum_{j=1}^{n} \beta_j |\psi_j\rangle \tag{3.32}$$

Considering the operator U_{rs} for the subsystem $|\psi\rangle$:

$$U_{rs_{|\psi\rangle}} = \mathbb{I} \otimes \sum_i |\frac{\langle \psi_{i+1} | \chi \rangle}{\langle \psi_i | \chi \rangle}| \, |\psi_{i+1}\rangle \langle \psi_i| \tag{3.33}$$

An important point here is that there is a certain cyclicity in the indices. So, this operator takes the n^{th} state to the first superposition vector-state.

Thus, the action of this operator is given by

$$|\chi\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_i\beta_j|\phi_i\rangle \otimes |\psi_j\rangle \xrightarrow{U_{rs_{|\psi\rangle}}} \sum_{i=1}^{m}\sum_{j=1}^{n-1} \alpha_i\beta_{j+1}|\phi_i\rangle \otimes |\psi_{j+1}\rangle + \sum_{i=1}^{m} \alpha_i\beta_1|\phi_i\rangle \otimes |\psi_1\rangle \tag{3.34}$$

In effect, this gives back the same state as in equation (3.30).

If the coefficients (physically, the relative phases) for each of the superposition vector-states are not considered, then the operator becomes a local permutation operator for the particular subsystem ψ, with

$$U = \mathbb{I} \otimes P_\psi \tag{3.35}$$

where P_ψ is the permutation operator over partition ψ given by a permutation matrix of dimensions $2^k \times 2^k$ where k is the number of qubits in ψ.

We find that the concept of superposition of operators gives us an efficient method to realize all possible permutations all once. This is done with $U = \sum_t \mathbb{I} \otimes P_\psi^t$ where P_ψ^t is a distinct permutation operator. So, we can present this idea in a different way by defining a new V_{rs_ψ} operator such that,

$$V_{rs_\psi} = \mathbb{I} \otimes \sum_i \sum_j |\varepsilon_j^{(k)}\rangle\langle\varepsilon_i^{(k)}| \tag{3.36}$$

Here we are not considering the relative phases but the relevant corrections can be added if the phases are considered. Then the operation of V_{rs_ψ} on $|\chi\rangle$ generates every cyclic permutation at once. More correctly, V_{rs_ψ} generates multiple copies of every cyclic permutation since there will still be cases where $|\psi_i\rangle \neq |\psi_j\rangle$.

If a state $|\psi\rangle$ is considered as an m qubit state with its superposition states the various $|\psi_i\rangle$ states, then the operator V_{rs_ψ} may be considered to be an outer product of the form

$$V_{rs_\psi} = tr_\phi|\chi\rangle\langle\chi| \tag{3.37}$$

Determination of closure after these permutation operations could be achieved in a variety of ways:

1. If we carry out $M-1$ sequential permutation operations, we will have a newly generated set of states: $\{|\chi_1'\rangle, |\chi_2'\rangle, ..., |\chi_{M-1}'\rangle\}$, where $|\chi_i'\rangle$ denotes the state after the

i^{th} iteration. This can be compared to the original after each permutation operation. A possible test is that if the inner product

$$\langle \chi_i' | \chi \rangle \neq 0$$

for even one iteration, the state is not closed under that partition.

2. A speed-up may be possible by using certain quantum operations. Considering the most general symmetric N-qubit state with 2^N superposition states,

$$|N\rangle = \frac{1}{\sqrt{2^N}}((|0\rangle + |1\rangle)^{\otimes N}) \tag{3.38}$$

We can then use the given state $|\chi\rangle$, without consideration of relative phases, to form the state $|\chi_-\rangle = |N\rangle - |\chi\rangle$, which contains every N qubit superposition state not present in $|\chi\rangle$. It is then reasonable to state to reason that if a new state is generated after a permutation operation then $|\langle \chi | \chi_- \rangle| \neq 0$ and the state is not closed. If a state is closed under a particular partition of the system then

$$|\langle \chi_- | V_{rs_\psi} | \chi \rangle| = 0 \tag{3.39}$$

3. If two copies of the same state $|\chi\rangle$ are taken and the *Quantum Roll-Slot Operator* V_{rs_ψ}, which was jointly proposed with Mr. N.B. Devlin of Cavendish Laboratory, is used on one copy, we have the states $|\chi'\rangle = V_{rs_\psi}|\chi\rangle$ and $|\chi\rangle$. A point to be noted here is that the relative phases are not considered in this case. These states can now be compared to see whether the new state is the same as the reference state. Quantum state comparison relies on measurements based on projections and Positive-Operator Valued Measures (POVMs). But before moving on to studying about these, a fundamental theorem regarding state comparison must be mentioned [260–263]

> ***Theorem 3.2.*** No quantum measurement can unambiguously confirm when two quantum systems have been prepared in the same state when each system is prepared in some unknown pure state. It is only possible to detect when the states of the two systems are different, with a certain probability.

> ***Proof.*** The most general kind of quantum measurement, with N possible outcomes, is described by a set of positive operators π_k, where $k = 1, ..., N$ and $\sum_k \pi_k = \mathbb{I}$. These operators form a set of positive, operator-valued measures

(POVMs), each of which corresponds to a particular measurement outcome.

Let the initial state of the system be represented by the density operator ρ, then the probability of obtaining the result 'k' is

$$P(k|\rho) = Tr(\rho\pi_k) \tag{3.40}$$

A state-comparison measurement will have three possible outcomes and, thus, three corresponding POVMs: π_y that corresponds to the states being the same, π_n that corresponds to the states being different and $\pi_?$ that corresponds to the outcome being inconclusive. The natural space for these operators is the Hilbert Space of pairs of quantum particles. The requirements of the measurement impose the following conditions:

$$\langle\psi| \otimes \langle\psi|\pi_n|\psi\rangle \otimes |\psi\rangle = 0 \tag{3.41}$$

$$\langle\psi| \otimes \langle\phi|\pi_y|\psi\rangle \otimes |\phi\rangle = 0, |\langle\psi|\phi\rangle < 1 \tag{3.42}$$

for all physically realisable states $|\psi\rangle, |\phi\rangle$ of the systems that are being considered. These conditions make sure that the measurements never give erroneous results.

Now let us take the trace of the POVM π_y and express this in terms of an orthonormal product basis $\{|x_i\rangle \otimes |x_j\rangle\}$:

$$Tr(\pi_y) = \sum_{i,j} \langle x_i| \otimes \langle x_j|\pi_y|x_i\rangle \otimes |x_j\rangle = \sum_i \langle x_i| \otimes \langle x_i|\pi_y|x_i\rangle \otimes |x_i\rangle \tag{3.43}$$

Now, let us take two other alternative orthonormal basis sets: $\{|y_j\rangle\}$ and $\{|z_k\rangle\}$ for the subsystem state spaces. The sets $\{|y_j\rangle\}$ and $\{|z_k\rangle\}$ are taken to have no common elements. Since hese are basis sets, we may write

$$|x_i\rangle = \sum_j U_{ij}|y_j\rangle = \sum_k V_{ik}|z_k\rangle \tag{3.44}$$

where U_{ij} and V_{ik} are unitary transformations. If we substitute these expressions into equation (3.43), using the bases $\{|y_j\rangle\}$ and $\{|z_k\rangle\}$ for the first and second

subsystems respectively, we find

$$Tr(\pi_y) = \sum_{ijkj'k'} U^*_{ij'} V^*_{ik'} U_{ij} V_{ik} \langle y_{j'}| \otimes \langle z_{k'}|\pi_y|y_j\rangle \otimes |z_k\rangle \tag{3.45}$$

Using the Cauchy-Schwarz Inequality for the square of the modulus of the tensor-product terms in the sum above, we have

$$|\langle y_{j'}| \otimes \langle z_{k'}|\pi_y|y_j\rangle \otimes |z_k\rangle|^2 \leq \langle y_{j'}| \otimes \langle z_{k'}|\pi_y|y_{j'}\rangle \otimes |z_{k'}\rangle \langle y_j| \otimes \langle z_k|\pi_y|y_j\rangle \otimes |z_k\rangle = 0 \tag{3.46}$$

Since the modulus-squares cannot be less than 0, all the terms in the sum in equation (3.45) will be equal to zero.

$$Tr(\pi_y) = 0 \tag{3.47}$$

Since the only positive operator with zero trace is the zero operator,

$$\pi_y = 0 \tag{3.48}$$

Thus, it is **impossible to confirm unambiguously and with non-vanishing probability that two quantum systems have been prepared in the same state**, without any knowledge of their initial states.

We are therefore led to consider a two-outcome measurement with corresponding POVMs π_n and $\pi_?$. With such measurements we would be able to determine if the states of both quantum systems are different, at most.

Equation (3.41) implies that the support of the operator π_n is a subspace of the antisymmetric subspace: $\frac{(|i\rangle\otimes|j\rangle - |j\rangle\otimes|i\rangle)}{\sqrt{2}}$, where $1 \leq i < j \leq D$ for a D-dimensional Hilbert Space. Since for any bipartite tensor-product state, we have $D(D-1)/2$ antisymmetric states, we can represent the POVM π_n as

$$\pi_n = \sum_{\mu=1}^{D(D-1)/2} t_\mu |t_\mu\rangle\langle t_\mu| \tag{3.49}$$

for some states $|t_\mu\rangle$ that form an orthonormal basis for the antisymmetric subspace, and some real, nonnegative coefficients t_μ with $0 \leq t_\mu \leq 1$. The maximum probability of any pair of different states giving rise to an 'n' (not same state)

result is attained when all $t_\mu = 1$, which implies that the optimal POVM element for detecting any differences between the states of the two quantum systems is when π_n is the projector onto the perfectly antisymmetric subspace.

Now, since $\sum_k \pi_k = 1$ and $P_{anti} + P_{symm} = 1$, where P_{anti} and P_{symm} are projectors onto the antisymmetric and symmetric subspaces respectively, we have

$$\pi_? = 1 - \pi_y - \pi_n = 1 - \pi_n = 1 - P_{anti} = P_{symm} \tag{3.50}$$

Thus, the POVM $\pi_?$ that is responsible for inconclusive results is equal to the projector onto the perfectly symmetric subspace, P_{symm}.

This concludes the important point of optimizing the measurements so that the probability of detecting a difference between two quantum states can attain its maximum possible value. □

Thus, given the states $|\chi'\rangle = V_{rs_\psi}|\chi\rangle$ and $|\chi\rangle$, we can find out using POVMs whether they are different. If so, then the state is not separable in the partition under consideration.

These methods can be generalized to the multipartite case. Let us consider a particular partition of an n-partite quantum state into an $[\alpha_1, \alpha_2, \alpha_3, ..., \alpha_L]$ separability class. Then $|\chi\rangle$ can be written as

$$|\chi\rangle = \sum_{i=1}^{M} \prod_{\otimes j=1}^{L} |\psi_i^j\rangle \tag{3.51}$$

We can then define the set of $n-1$ operators

$$U_{\psi_1} = P_{\psi_1} \otimes \mathbb{I}_{\psi_2} \otimes \mathbb{I}_{\psi_3} ... \tag{3.52}$$

$$U_{\psi_2} = \mathbb{I}_{\psi_1} \otimes P_{\psi_2} \otimes \mathbb{I}_{\psi_3} \tag{3.53}$$

$$U_{\psi_3} = \mathbb{I}_{\psi_1} \otimes \mathbb{I}_{\psi_2} \otimes P_{\psi_3} \otimes ... \tag{3.54}$$

and so on, where P_α is the permutation operator on the partition α. If we apply this sequentially in a total of $(M-1)^{n-1}$ steps, we generate every permutation of the quantum system required. Generalising the quantum permutation operator defined in equation (3.37)

to the case applicable to an n-partite system, we have

$$V_{rs_\psi} = \prod_{k=1}^{L}(\sum_i \sum_j |\psi_k^j\rangle\langle\psi_k^j|)$$

This operator permutes all subsystems over all possible states all at once. This is not as useful as the operator permuting only one subsystem locally. For a specific subsystem, we can define the operator

$$\begin{aligned} U_i &= tr_{\psi_i}|\chi\rangle\langle\chi| \\ &= \sum_j \sum_{j'} (|\psi_1^j\rangle|\psi_2^j\rangle...|\psi_{i-1}^j\rangle|\psi_{i+1}^j\rangle...|\psi_L^j\rangle)(\langle\psi_1^{j'}|\langle\psi_2^{j'}|...\langle\psi_{i-1}^{j'}|\langle\psi_{i+1}^{j'}|...\langle\psi_L^{j'}|) \end{aligned} \quad (3.55)$$

we find that one operation is required to carry out all $(M-1)^{n-1}$ permutation operations at once. To test for the closure of a particular i^{th} partition for a given separability class, we check if

$$\langle\chi'|U_i|\chi\rangle = 0 \quad (3.56)$$

If this is true, then the state is separable in the i^{th} partition.

Hybrid Permutation-Based Algorithm for Separability Analysis

Even with the speed-up possible with the elements and concepts presented in the last section, the problem of the presence of a large number of possible partitions possible for each separability class remains. This can be further optimized and made quicker using a combination of quantum and classical steps for a comprehensive hybrid algorithm for determining the particular separability class *and* partition for a quantum state.

Step 1: *Determining the possible separability classes given a superposition state*

Beginning with J, the number of superposition states in the system, we can find it's prime factors, preferably using a quantum algorithm like Shor's algorithm [9]

$$J = J_{\alpha_1} J_{\alpha_2} J_{\alpha_3} ... \quad (3.57)$$

where J_{α_i} is the number of superposition states for the partition α_i. If J is a prime number, this factorisation would be either be the case for the completely entangled state $[N]$ or the state is $[1, N-1]$ separable. There will be instances where this step of prime factorisation of J does not significantly reduce the number of separability classes

within this method. This informs us about the kind of separability classes possible for quantum qubit state. We can further reduce the possibilities of partitions that the state can have. For a single qubit to be separable, the number of $|1\rangle$ for that qubit within the superposition is found to be 0, J or $\frac{J}{2}$.

Theorem 3.3. For a particular qubit $|q\rangle$ in a quantum state to be separable, the sum of the number of vector-states in superposition that have $|q\rangle = |1\rangle$ must be 0, J or $\frac{J}{2}$.

Proof. Let us say we have α of the superposition states having $|0\rangle$ for the qubit being considered while β of the superposition states have $|1\rangle$ for the the qubit considered, with the total number of superposition states being J. Let us say that the quantum state is a tensor product of three sections: $|\Psi_1\rangle$, $|q_i\rangle$ and $|\Psi_2\rangle$, where $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are the subsystems of the state besides the separable i^{th} qubit, with n_1 and n_2 qubits in them respectively. Let $|\Psi_1\rangle$ and $|\Psi_2\rangle$ be superposition of J_1 and J_2 vector-states respectively. We need not discuss the separability of these subsystems, though we know that $n_1 + n_2 + 1 = N$, where N is the total number of qubits.

We can represent the state as

$$|\psi\rangle = |\Psi_1\rangle(\alpha|0\rangle + \beta|1\rangle)_i|\Psi_2\rangle, \sqrt{|\alpha|^2 + |\beta|^2} = 1 \tag{3.58}$$

There can be three cases now: $\{\alpha \neq 0, \beta \neq 0\}$, $\{\alpha = 0, \beta \neq 0\}$ and $\{\alpha \neq 0, \beta = 0\}$. In the first case, the total number of superposition terms are $J = 2J_1J_2$ while the number of terms with $|q\rangle = |1\rangle$ are J_1J_2. Thus in this case, the number of terms with $|q\rangle = |1\rangle$ is $\frac{J}{2}$. In the second and third cases, the number of terms with $|q\rangle = |1\rangle$ are 0 and J respectively. Thus, we see that

$$S \in \{0, J, \frac{J}{2}\} \tag{3.59}$$

for the separable qubit □

This is just a specific case of a more general pattern. if a qubit is part of a larger n_α qubit subsystem for the partition α, then the number of $|1\rangle$'s for that i^{th} qubit is

$$N_i^{(1)} = \frac{x}{J_\alpha} J, 0 \geq x \leq J_\alpha \tag{3.60}$$

where J_α are the number of superposition states in the partition α. The qubit is trivially separable if $x = 0$ or $x = J_\alpha$. Since J_α can only take values in the range $1 \geq J_\alpha \leq 2^{n_\alpha}$, this limits the set of qubits which be part of a separable n_α qubit subsystem. The condition that we can have for this qubit to be part of separable n_α qubit subsystem is

$$N_i^{(1)} = \frac{x}{J_\alpha} J^2 \tag{3.61}$$

Step 3: We shall now look at which of the separability classes and partitions a state lies in. For this, we will define what we call the *Trace-Space Coordinates*:

$$Q_i^{(\alpha)} = \begin{cases} |1\rangle, U_{rs_{\alpha_{(i)}}} |\chi\rangle \text{ is closed} \\ |0\rangle, U_{rs_{\alpha_{(i)}}} |\chi\rangle \text{ is not closed} \end{cases} \tag{3.62}$$

where α refers to a particular separability class and (i) refers to the particular permutation or instance of this. So, if the placeholder values for each qubit is given from right-to-left, as per convention, we will assign the index i accordingly, depending on the larger of the bipartitions.

For example, for the three qubit case and $[21]$ separability, we take the '$2'$ qubits and assign $i = 1$ for $[23,1]$, $i = 2$ to $[12,3]$ and $i = 3$ to $[13,2]$.

We then find all the coordinates this way and then assign relative phases to the coordinates for the same separability class and add the states to form a sum L^α. We then use positive-operator valued measure (POVMs) with basis-states based on these relative phases.

So, for instance, for the three qubit states, we have the separability classes $[3]$, $[21]$ and $[111]$. However, the trace-method works only for bipartitions and thus we will only have cases for $[21]$ with $i = 1$ for $[23,1]$, $i = 2$ to $[12,3]$ and $i = 3$ to $[13,2]$. Let us say we have the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |100\rangle)$, we have $Q_1^{([21])} = |0\rangle, Q_2^{([21])} = |1\rangle$ and $Q_3^{([21])} = |0\rangle$. Thus, the relative-phase based construction would be of the form:

$L^{[21]} = Q_1^{([21])} + e^{i\phi_1} Q_2^{([21])} + e^{2i\phi_1} Q_3^{([21])} = |0\rangle + e^{i\phi_1}|1\rangle + e^{2i\phi_1}|0\rangle$. This can be determined using POVMs with basis vectors: $|v_{k\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{ik\phi_\alpha}|1\rangle$ where ϕ_α denotes the separability class specific phase factor.

This completely describes the separability class and partition that a particular state falls into.

Permutations across subspace Hilbert Space for Detection of Entanglement

Permutation of qubits within the Hilbert Space of subspaces and correlations in a quantum state are found to have a connection that has been explored extensively in the past [251, 264, 265]. We find that permutations of qubits can characterize entanglement. In the previous subsections, we looked at how permutations within a confined subspace can be helpful in characterizing separability. In this subsection, we will analyse how permutations can act as entanglement witnesses. For a general separable mixed quantum state

$$\rho = \sum_k p_k |\phi_1^{(k)}\rangle\langle\phi_1^{(k)}| \otimes |\phi_2^{(k)}\rangle\langle\phi_2^{(k)}| \otimes ... \otimes |\phi_N^{(k)}\rangle\langle\phi_N^{(k)}| \tag{3.63}$$

We know that a general permutation can expressed as a product of transpositions or 2-cycles $T_{i,j}$. For instance, a three element permutation $(123) = (12)(13)$. Let us look at the expectation value of such an operator on a mixed quantum state,

$$\begin{aligned}\langle T_{i,j}\rangle = Tr(T_{i,j}\rho) = Tr(\sum_k p_k |\phi_1^{(k)}\rangle\langle\phi_1^{(k)}| \otimes ... |\phi_j^{(k)}\rangle\langle\phi_i^{(k)}| \otimes |\phi_i^{(k)}\rangle\langle\phi_j^{(k)}| ... \otimes |\phi_N^{(k)}\rangle\langle\phi_N^{(k)}|) \\ = p_k |\langle\phi_1^{(k)}\rangle|^2 ... |\langle\phi_i^{(k)}|\phi_j\rangle|^2 ... |\langle\phi_N^{(k)}\rangle|^2 \geq 0\end{aligned} \tag{3.64}$$

Thus for a separable state, the expectation value of $\langle T_{i,j}\rangle$ is positive or zero, and if $\langle T_{i,j}\rangle < 0$, then the state is entangled. This idea can be extended to higher dimensions using the idea that any permutation can be written as a transposition of elements (qubits). It then naturally follows that

$$\frac{\langle T_{i_1,j_1}\rangle}{|\langle T_{i_1,j_1}\rangle|^2} + \frac{\langle T_{i_2,j_2}\rangle}{|\langle T_{i_2,j_2}\rangle|^2} + ... \frac{\langle T_{i_S,j_S}\rangle}{|\langle T_{i_S,j_S}\rangle|^2} = -A \tag{3.65}$$

where A relates to the A cycle being investigated, T_{i_l,j_l} denotes the transposition operator for the l^{th} transposition between qubits i_l and j_l, and the system is entangled over the qubits covered by this permutation A-cycle. While every state that satisfies this condition is non-separable, not all entangled states satisfy this condition.

For instance, the W-state $\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ gives a value of 3. In fact, all the

higher dimensional N-qubit W-states give a value of N for the measure in equation (3.65). These states that are also known as Dicke states [266, 267] have perfect permutation symmetry, besides being maximally entangled. Thus, we see that though transpositions and permutations can help us with characterizing entanglement in certain cases, in some cases, they do not give us a good idea of the entanglement of a quantum state.

3.2 Quantum Principal Component Analysis and Filtering

In statistics, there is often a need to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables. This is best accomplished by the procedure called *Principal Component Analysis (PCA)* that uses an orthogonal transformation to convert a certain data-set into its so-called principal components. In their seminal paper, Lloyd et al [268] extended this idea to the quantum domain with the *Quantum Principal Component Analysis*. Usually, the properties of an unknown quantum state, given multiple copies of the state, are revealed using measurements of different observables and the subsequent analysis of the measurement results statistically. Thus, in state tomography techniques, the state usually plays a passive role, as an entity to only be measured. However, using Quantum Principal Component Analysis (qPCA), this analysis can be done with an active role played by the unknown quantum state itself!

Given many copies of a quantum system represented by the density matrix ρ, it is now known to be possible to perform the unitary transformation $e^{-i\rho t}$. This can be carried out using yet another application of the *SWAP* operator, which will be explored further. In this section, I extend this recently found conceptual tool of Quantum Principal Component Analysis (qPCA) to a hitherto unexplored area: separability and entanglement, with the help of Peres' separability criterion for density matrices [152].

Suppose we have n copies of the density matrix $\rho = |\psi\rangle\langle\psi|$ for a quantum state. Let us consider having another density matrix $\sigma = |\phi\rangle\langle\phi|$ and the quantum *SWAP* operator S.

$$\begin{aligned} tr_P(e^{-\imath S\Delta t}(\rho\otimes\sigma)e^{\imath S\Delta t}) &= tr_P((cos(S\Delta t)-\imath sin(S\Delta t))(\rho\otimes\sigma)(cos(S\Delta t)+\imath sin(S\Delta t))) \\ = tr_P((1-\frac{(S\Delta)^2}{2!}t+...)-\imath(S\Delta t+\frac{(S\Delta)^3}{3!}+...))(\rho\otimes\sigma)(1-\frac{(S\Delta)^2}{2!}t+...)+\imath(S\Delta t+\frac{(S\Delta)^3}{3!}+...))) \end{aligned} \tag{3.66}$$

The partial trace operation is over the first variable. Since $S^2 = \mathbb{I}$, this expression can be written as

$$tr_P(S^2(1-\frac{(\Delta)^2}{2!}t+...)-\imath S(\Delta t+\frac{(\Delta)^3}{3!}+...)(\rho\otimes\sigma)((1-\frac{(\Delta)^2}{2!}t+...)+\imath S(\Delta t+\frac{(\Delta)^3}{3!}+...)))$$
$$= tr_P((cos(\Delta t)-\imath S sin(\Delta t))(\rho\otimes\sigma)(cos(\Delta t)+\imath S sin(\Delta t))) \quad (3.67)$$

Simplifying this equation, we get

$$tr_P(cos^2(\Delta t)\rho\otimes\sigma + sin^2(\Delta t)S\rho\otimes\sigma S - \imath sin(\Delta t)cos(\Delta t)(S\rho\otimes\sigma - \rho\otimes\sigma S))$$
$$= tr_P(cos^2(\Delta t)\rho\otimes\sigma + sin^2(\Delta t)\sigma\otimes\rho - \imath sin(\Delta t)cos(\Delta t)(|\phi\rangle\langle\psi|\otimes|\psi\rangle\langle\phi| - |\psi\rangle\langle\phi|\otimes|\phi\rangle\langle\psi|))$$
$$= cos^2(\Delta t)\sigma + sin^2(\Delta t)\rho - \imath sin(\Delta t)cos(\Delta t)[\rho,\sigma] = \sigma - \imath\Delta t[\rho,\sigma] \quad (3.68)$$

where an infinitesmal time period is taken and higher order terms are neglected in the last step. Repeated application of (3.63-3.65) with n copies of ρ allows us to construct $e^{-i\rho n\Delta t}\sigma e^{i\rho n\Delta t}$. Thus, repeatedly performing infinitesimal swap operations on $\rho\otimes\sigma$ allows us to construct the unitary operator $e^{-i\rho t}$.

One of the major applications of density matrix exponentiation is that is allows us to find the eigenvectors and eigenvalues of an unknown density matrix. Such a quantum phase algorithm uses conditional applications of $e^{-i\rho t}$ for varying times t to implement: $|\psi\rangle|0\rangle \rightarrow \sum_i \psi_i|\chi_i\rangle|\tilde{r}_i\rangle$, where $|\chi_i\rangle$ are the eigenvectors of ρ and $|\tilde{r}_i\rangle$ are the corresponding eigenvalues. Now, if we were to consider the partial transposition of ρ and feed into this system, a check on the eigenvalue bin is enough to see if the state is separable. Since a necessary condition for separability is that the partial transposition of ρ has only non-negative eigenvalues, $|\tilde{r}_i\rangle$ will have positive entries only, for a separable state.

Separability Filter using qPCA

This methodology can also be used to devise a filter. Let us say that the two states fed into the qPCA process constitute the same quantum state in a tensor product: $\tau = \rho\otimes\sigma$, then partially tracing out this matrix with respect to various partitions and qubits in the system can either give rise to an exponentiation, in case of a separable state, or else not. Whether the exponentiation is successful or not can be thereafter tested by trying to find the eigen-spectrum of constituents of the state, as in the previous section. This gives us a filter using infinitesmal operation of the swap operator for knowing if a state is separable or not.

3.3 Quantum Entanglement

Separability and entanglement are two sides of the same coin. One is negation of the other and vice versa. In this chapter, we have studied and devised tests and conceptual tools for observing separability in states. In this section, we will investigate entanglement characterization. As discussed previously, in the early part of the twentieth century, the world of physics encountered a new ('spooky') form of correlations between particles, hitherto unseen in the realm of classical physics: *entanglement*. Entanglement is a phenomenon that occurs when systems of particles are generated or interact in such a way that the quantum state of each particle cannot be described independently of the state of the others, even when the particles are spatially separated by large distances! Measurements of physical properties of the constituents of such systems are found to be correlated. It was only after the turn of the millenium that it was found that *entanglement* happens to be a subset of a larger concept: *quantum discord* [269–273]. Quantum discord is a measure of the non-classical correlations between two subsystems of a quantum system. Interestingly, although separability implied the absence of entanglement, it does not imply the absence of quantum correlations altogether, as seen in the case of some mixed separable states [274].

3.3.1 $SWAP^{1/n}$ as an Entanglement Witness

In our formalism of quantum computation, we have used the $SWAP^{1/n}$ gate for generation of entanglement in physical systems. It is interesting to see that these operators can also be used to characterize entanglement. In the previous section, we saw how transpositions and permutations can be used for entanglement characterization. A partial swap or permutation is also a good conceptual tool for characterizing quantum correlations. We investigate this for the case of two qubits.

We define the entanglement witness

$$W = Tr(U_{SWAP^{1/n}}|\psi\rangle\langle\psi|) \tag{3.69}$$

This entanglement witness relies on the symmetry of the Power-of-SWAP operator to give us distinct results for the cases of entangled and separable states.

To see the action of this entanglement witness, let us consider a basic two-qubit state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{3.70}$$

with $\sqrt{|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2}=1$. The action of the Power-of-SWAP operator leads to

$$U_{SWAP^{1/n}}|\psi\rangle = \alpha|00\rangle+\beta(\frac{1}{2}(1+e^{i\pi/n})|01\rangle+\frac{1}{2}(1-e^{i\pi/n})|10\rangle) \\ +\gamma(\frac{1}{2}(1-e^{i\pi/n})|01\rangle+\frac{1}{2}(1+e^{i\pi/n})|10\rangle)+\delta|11\rangle \quad (3.71)$$

and the entanglement witness yields

$$W = Tr\begin{pmatrix} \alpha\alpha^* & \alpha\beta^* & \alpha\gamma^* & \alpha\delta^* \\ B\alpha^* & B\beta^* & B\gamma^* & B\delta^* \\ C\alpha^* & C\beta^* & C\gamma^* & C\delta^* \\ \delta\alpha^* & \delta\beta^* & \delta\gamma^* & \delta\delta^* \end{pmatrix} \quad (3.72)$$

where

$$B = \beta\frac{1}{2}(1+e^{i\pi/n})+\gamma\frac{1}{2}(1-e^{i\pi/n}) \quad (3.73)$$

$$C = \gamma\frac{1}{2}(1+e^{i\pi/n})+\beta\frac{1}{2}(1+e^{i\pi/n}) \quad (3.74)$$

Evaluating the trace in equation (3.69) gives

$$W = |\alpha|^2+(|\beta|^2+|\gamma|^2)(\frac{1}{2}(1+e^{i\pi/n})+(\beta\gamma^*+\gamma\beta^*)\frac{1}{2}(1-e^{i\pi/n}))+|\delta|^2 \\ = 1-(1-|\alpha|^2-|\delta|^2-2Re(\beta\gamma^*)(\frac{1-e^{i\pi/n}}{2}) \\ \leq 1-(1-|\alpha|^2-|\delta|^2-2|\beta||\gamma|)(\frac{1-e^{i\pi/n}}{2}) \quad (3.75)$$

using the triangular inequalities for complex numbers. We see that for this entanglement witness, the value for the completely separable and maximally entangled states are exactly the same. Thus, this cannot be used as the entanglement witness.

We next look at a more complex structure of the entanglement witness: $U_{SWAP^{1/n_1}}(\sigma_x \otimes I_{2\times 2})U_{SWAP^{1/n_2}}$. Taking the expectation value shows us that this entanglement witness vanishes for both separable as well as maximally entangled states. Thus, this cannot be used as an entanglement witness either.

The problem in both cases is that the structure of the Power-of-SWAP gates is not symmetric for the presence of maximally entangled states comprising of $|00\rangle/|11\rangle$ and $|01\rangle/|10\rangle$. This problem can be solved by adding a term to the Power-of-SWAP. Looking at this problem

theoretically and searching for an appropriate addition, we came across the choice of the following operator:

$$W = Tr((U_{SWAP^{1/n}} - (\sigma_x \otimes \sigma_x))|\psi\rangle\langle\psi|) \tag{3.76}$$

A point to note here is that there could be variants of this operator that can be considered.

Let us see what it gives for a standard two-qubit state of the form mentioned in equation (3.55).

$$\begin{aligned} W &= (\alpha\alpha^* - \delta\alpha^*) + (\frac{1+e^{i\pi/n}}{2})(\beta^*\beta - \gamma\beta^*) \\ &\quad + (\frac{1+e^{i\pi/n}}{2})(-\beta\gamma^* + \gamma^*\gamma) + (-\alpha\delta^* + \delta\delta^*) \\ &= (|\alpha|^2 + |\delta|^2 - 2Re(\alpha^*\delta)) + (\frac{1+e^{i\pi/n}}{2})(|\beta|^2 + |\gamma|^2 - 2Re(\beta^*\gamma)) \\ &\leq (|\alpha|^2 + |\delta|^2 - 2|\alpha||\delta|) + (\frac{1+e^{i\pi/n}}{2})(|\beta|^2 + |\gamma|^2 - 2|\beta||\gamma|) \end{aligned} \tag{3.77}$$

For the various conditions and cases, we have state-dependent values and hence this is an instance of device-dependent entanglement witness using the $SWAP^{1/n}$. For the maximally entangled states we have

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \rightarrow W \leq (|\alpha| - |\delta|)^2 < 1 \tag{3.78}$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \rightarrow W \leq (\frac{1+e^{i\pi/n}}{2})(|\beta| - |\gamma|)^2 < (\frac{1+e^{i\pi/n}}{2}) \tag{3.79}$$

using the point that the maximum value of $(|\alpha| - |\delta|)^2 = (|\beta| - |\gamma|)^2 = 1$, which can be determined by defining a function in terms of the normalization condition for these variables in these cases.

For the completely separable states, we have

$$|\psi\rangle = |00\rangle \rightarrow W = 1 \tag{3.80}$$

$$|\psi\rangle = |11\rangle \rightarrow W = 1 \tag{3.81}$$

$$|\psi\rangle = |01\rangle \rightarrow W = (\frac{1+e^{i\pi/n}}{2}) \tag{3.82}$$

$$|\psi\rangle = |10\rangle \rightarrow W = (\frac{1+e^{i\pi/n}}{2}) \tag{3.83}$$

For any other general case, we find intermediate conditions for the entanglement witness proposed here. It is pertinent to point out that for separable states that are not one of the cases mentioned in (3.80)-(3.83), we have $W > 0$.

For the case of $e^{i\pi/n} = -1$, which is the case when the operator is just the *SWAP* operator, we get the results mentioned by Wang et al [275]. Looking at the steps, cases and derivation done above, we can posit a theorem

Theorem 3.4. If the expectation value of $(U_{SWAP^{1/n}} - (\sigma_x \otimes \sigma_x)$, given by

$$W = Tr((U_{SWAP^{1/n}} - (\sigma_x \otimes \sigma_x))|\psi\rangle\langle\psi|) \tag{3.84}$$

on all separable states is larger than or equal to zero, then the inequality

$$W < 0 \tag{3.85}$$

gives us a sufficient condition for quantum states to be entangled.

This operator can be constructed using the exchange interaction, along with the operation of local single qubit rotation (σ_x) on both qubits simultaneously. This formalism can be extended to the case of multiqubit states but this would require sequential testing of an ensemble of copies of the quantum state with the aforementioned operator on various pairs of qubits. This is a tedious process for multiple qubits (which has been done for the case of three and four qubits), particularly in the case of the vector states that we have found for higher dimensional states. As a result, for further characterization of the entanglement in these states, we use established conceptual tools in the next couple of sections in this chapter.

3.3.2 Characterization of Multipartite Entanglement

Multipartite entanglement has been a subject of quite some interest, due to its application in evaluating how good a quantum resource-state is for various quantum information processing tasks. Multipartite entanglement has been studied over the years using a number of conceptual tools: witness operators [276], negativity [277], geometric measures [226], multipartite concurrences [278, 279] and entanglement entropy [249]. In this section, we study and apply certain geometrical and algebraic measures of entanglement on our states. We also

evaluate a function-oriented characterization of entanglement that directly informs us of the appropriateness of a quantum state for a quantum information processing task.

Geometrical Measure of Entanglement

The geometric measure of entanglement is an effective means of quantifying entanglement in multipartite states. For a system $|\psi\rangle$ comprising of N subsystems, the full corresponding Hilbert Space $\mathbb{H}$ is given by $\mathbb{H}_1 \otimes \mathbb{H}_2 \otimes ... \otimes \mathbb{H}_N$, and the geometric measure of entanglement is given by

$$G = min[||(|\psi\rangle - |\phi\rangle)||] \tag{3.86}$$

where $|\phi\rangle$ denotes the set of all possible separable states in this Hilbert Space. For the purposes of the project, we have looked into various kinds of norms for this definition. One important kind of norm that we used for this analysis is the Hilbert-Schmidt norm: $||A|| = Tr(A^\dagger A)$. For our states, we have found the geometric measure of entanglement. The measures for the three- qubit vector-states are given below, while those for higher dimensions are given in the appendix.

Vector State	G	Nearest Separable State
$\|\psi_1^{(3)}\rangle$	0.605811	$-\|010\rangle$
$\|\psi_2^{(3)}\rangle$	0.765367	$\|001\rangle$
$\|\psi_3^{(3)}\rangle$	0.605811	$-\|101\rangle$
$\|\psi_4^{(3)}\rangle$	0.765367	$\|110\rangle$
$\|\psi_5^{(3)}\rangle$	0	$\|000\rangle$
$\|\psi_6^{(3)}\rangle$	0.919402	$\|001\rangle/\|010\rangle/\|100\rangle$
$\|\psi_7^{(3)}\rangle$	0.919402	$\|011\rangle/\|110\rangle/\|101\rangle$
$\|\psi_8^{(3)}\rangle$	0	$\|111\rangle$

Table 3.1 Geometric Measure of Entanglement and Nearest Separable States of the three-qubit Vector States of the Symmetric Group S_3

As is expected, the maximally entangled states have larger distances from their nearest completely separable neighbours, while the separable states, understandably, have vanishing distance.

Wei et al [226] gave another measure relating to the geometric characterization of entanglement. Even though the concept of *distance* has a clear geometric meaning, it is useful to define a characterizing variable that is an entanglement monotone (a quantity that never

increases on average under *Local (quantum) Operations and Classical Communication (LOCC)*). The quantity

$$E = 1 - sup_{|\phi\rangle} \langle\psi|\phi\rangle^2 \tag{3.87}$$

If we look at the geometric measure G defined above,

$$G = \sqrt{|(|\psi\rangle - |\phi\rangle)|^2} = \sqrt{2 - 2\langle\psi|\phi\rangle} = \sqrt{2(1 - \sqrt{1 - (1 - \langle\psi|\phi\rangle^2)})} \tag{3.88}$$

This gives us

$$G = \sqrt{2(1 - \sqrt{1 - (1 - E)})} \tag{3.89}$$

However, our interest has been in seeing how these states can be used for various applications in quantum information processing. As a result, we defined a utilitarian extension to this definition

$$E = 1 - sup_{|\phi\rangle \in K} \langle\phi|\mathbb{L}|\psi\rangle^2 \tag{3.90}$$

where the set K, instead of being the set of all separable states, is the set of all resource states for specific quantum information tasks. The operator $\mathbb{L}$ represents a LOCC that can be operated on our resource state, if needed, to bring them as close to the resource states as possible. This extension was proposed by us since there might be situations where a certain quantum state is required in a particular quantum information task but it may be difficult to establish this state between distant parties. Instead, states generated naturally in our system could be more easily established with little cost. For such cases, the lessening of this 'deficiency' in the resource, as given by E, can be used as a measure of the replaceability of the required state by one of our vector states. Let us look at this idea for some popular quantum information processing tasks, taking the case of four-qubit vector states.

Distance E of our Resource States for Quantum Teleportation, Superdense Coding and Quantum Information Splitting:

For three-qubit states, we have the GHZ-like states mentioned by Prakash et al [280] as the resources used for teleporting arbitrary quantum states. If we take as that our reference set, we see that the value of E is 0.25, with the vector state from our states being the maximally entangled W-states. This is understandable since the greater the entanglement in a state, the greater is the teleportation potential of the state. For a higher number of qubits, the higher the value of G, the higher will be the teleportation potential and therefore lower the value of E, as has been checked for quantum states with higher numbers of qubits as well, by us. An interesting point here is that addition of our basis vector-states can reduce this

distance further. In the case of three-qubits, taking a state of the form $|\psi\rangle = \frac{1}{2}|\psi_5\rangle + \frac{\sqrt{3}}{2}|\psi_7\rangle$ or $|\psi\rangle = \frac{1}{2}|\psi_8\rangle + \frac{\sqrt{3}}{2}|\psi_6\rangle$ gives us the value $E_t = 0$.

This same understanding applies to applications like superdense coding and quantum information splitting (with associated E_{sc} and E_{qis}) respectively) as well, where maximally entangled states are preferred. Thus we can generalize, using equation (3.74), and say

$$E_t = E_{sc} = E_{qis} = (1 - \frac{G^2}{2})^2 \tag{3.91}$$

This can be understood as the greater the distance of a resource state from the nearest separable neighbour, the smaller is its potential to be a resource for teleportation or superdense coding.

However, since $SWAP^{1/n}$ preserves the number of $|0\rangle$s and $|1\rangle$s in a state, this segregation is not optimal, and rather a superposition of a number of vector states would be more useful, as mentioned above. Thus we would like to extend our definition here to

$$E = 1 - sup_{|\phi\rangle \in K, |\psi_i\rangle \in F} [\langle \phi | (\sum_i \mathbb{L}_i |\psi_i\rangle)]^2 \tag{3.92}$$

where the set K is the set of all resource states optimal for a quantum information task while F is the set of all vector states that we have found. The LOCC $\mathbb{L}_i$ operates on state $|\psi\rangle_i$. Thus this becomes an optimization problem given a set of resource-states.

Distance E of our Resource States for Cluster State Quantum Computation:

For cluster state quantum computation, the resources needed are partially entangled quantum states. This case is more interesting since the state can neither be completely separable nor maximally entangled. Our four-qubit vector state $|\psi_{11}\rangle$ has distance $E = 0$ from standard resource state: $|\psi\rangle = -\frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)$ when operated upon by $I \otimes \sigma_x \otimes I \otimes \sigma_x$, where σ_x is the Pauli X matrix. Interestingly this state has distance $E = 1$ for quantum teleportation, quantum information splitting and superdense coding. Thus, the point to note here is that because the resource-states for different applications have different entanglement requirements, the E of the same state for different applications are also different.

In this way, we define a functional, utilitarian definition of entanglement witness.

Algebraic Methods for Entanglement Characterization

Two of the prominent entanglement measures that have been used widely have been the tangle and concurrence, which have a connection with the idea of the hyperdeterminant of the quantum state.

The 'residual entanglement' or 'tangle' of an N-qubit state is defined as

$$\tau(\psi) = 2|\sum a_{\alpha_1\alpha_2\ldots\alpha_n} a_{\beta_1\beta_2\ldots\beta_n} a_{\gamma 1\gamma_2\ldots\gamma_n} a_{\delta_1\delta_2\ldots\delta_n} \times \varepsilon_{\alpha_1\beta_1}\varepsilon_{\alpha_2\beta_2}\ldots\varepsilon_{\alpha_{n-1}\beta_{n-1}}\varepsilon_{\gamma_1\delta_1}\varepsilon_{\gamma_2\delta_2}\ldots\varepsilon_{\gamma_{n-1}\delta_{n-1}}\varepsilon_{\alpha_n\gamma_n}\varepsilon_{\beta_n\delta_n}| \quad (3.93)$$

where the a terms are the coefficients in the standard basis $|\psi\rangle = \sum_{i_1\ldots i_N} a_{i_1 i_2\ldots i_N}|i_1 i_2\ldots i_N\rangle$ and $\varepsilon_{10} = -\varepsilon_{01} = 1$ and $\varepsilon_{00} = \varepsilon_{11} = 0$.

This measure is defined so that

1. $0 \leq \tau(\psi) \leq 1$
2. $\tau(\psi) = 0$ for separable states.
3. $\tau(\psi) = 1$ for maximally entangled states.
4. $\tau(\psi)$ is invariant under qubit permutations and local unitary operations.

Tangle of Three-Qubit States

The tangle for three-qubit states is defined as:

$$\begin{aligned}\tau(\psi) = 4|&a_{011}^2 a_{100}^2 + a_{010}^2 a_{101}^2 + a_{001}^2 a_{110}^2 + a_{000}^2 a_{111}^2 - 2a_{001}a_{011}a_{110}a_{100} \\ &+ 4a_{001}a_{010}a_{111}a_{100} - 2a_{000}a_{011}a_{111}a_{100} - 2a_{010}a_{011}a_{101}a_{100} - 2a_{001}a_{010}a_{101}a_{110} \\ &+ 4a_{000}a_{011}a_{101}a_{110} - 2a_{000}a_{010}a_{101}a_{111} - 2a_{000}a_{001}a_{110}a_{111}| \quad (3.94)\end{aligned}$$

We find the tangle for our three-qubit vector states. This itself shows the problem with the tangle. For maximally entangled, separable as well as partially entangled states, the tangle value vanishes. It is not as good a witness, based on the conditions associated with it for different kinds of entanglement.

This can be refined and corrected by studying the manner in which the various kinds of states contribute to the tangle. We create a functionally useful witness that we call the '*engle*'.

Vector State	τ
$\|\psi_1^{(3)}\rangle$	0
$\|\psi_2^{(3)}\rangle$	0
$\|\psi_3^{(3)}\rangle$	0
$\|\psi_4^{(3)}\rangle$	0
$\|\psi_5^{(3)}\rangle$	0
$\|\psi_6^{(3)}\rangle$	0
$\|\psi_7^{(3)}\rangle$	0
$\|\psi_8^{(3)}\rangle$	0

Table 3.2 Tangle of the three-qubit Vector States of the Symmetric Group S_3

Before moving to the definition of the witness, we would like to prove a result:

Statement 3.3: The maximum value of $f(x_1,x_2,x_3,...,x_N) = x_1x_2x_3x_4...x_N$ is obtained when $x_1 = x_2 = x_3 = ... = x_N$.

Proof. We have the function

$$f(x_1,x_2,x_3,...,x_N) = x_1x_2x_3x_4...x_N \tag{3.95}$$

and the normalization condition $x_1^2 + x_2^2 + ... + x_N^2 = 1$

Let us use the concept of constrained maximization and define

$$g(x_1,x_2,...,x_N) = x_1x_2x_3x_4...x_N - \lambda(x_1^2 + x_2^2 + ... + x_N^2 - 1) \tag{3.96}$$

For the maxima of this equation, we have

$$\frac{\delta g}{\delta x_1} = \frac{\delta g}{\delta x_2} = ... = \frac{\delta g}{\delta x_N} = 0 \tag{3.97}$$

This gives us the conditions:

$$x_2x_3x_4...x_N = 2\lambda x_1 \tag{3.98}$$

$$x_1x_3x_4...x_N = 2\lambda x_2 \tag{3.99}$$

...

$$x_1x_2x_3x_4...x_{N-1} = 2\lambda x_N \tag{3.100}$$

Solving these equations we obtain the condition

$$x_1 = x_2 = x_3 = ... = x_N \tag{3.101}$$

for the maxima of the function. ■

Using this concept, we know that the product of coefficients of quantum states would be maximum when they are equal, which corresponds to the maximally entangled case. Keeping this in mind, we define a modification of the 'tangle' for the three-qubit states as

$$\zeta(\psi) = |2a_{000}a_{111} - 3\sqrt{3}a_{001}a_{010}a_{100} - 3\sqrt{3}a_{011}a_{101}a_{110}| \tag{3.102}$$

A point to note here is that this entanglement witness is best suited for systems where states with different Hamming weight do not mix, as in the case of the physical system that we are studying.

For our three-qubit vector states, we find

Vector State	ζ
$\|\psi_1^{(3)}\rangle$	$\frac{1}{\sqrt{2}}$
$\|\psi_2^{(3)}\rangle$	0
$\|\psi_3^{(3)}\rangle$	$\frac{1}{\sqrt{2}}$
$\|\psi_4^{(3)}\rangle$	0
$\|\psi_5^{(3)}\rangle$	0
$\|\psi_6^{(3)}\rangle$	1
$\|\psi_7^{(3)}\rangle$	1
$\|\psi_8^{(3)}\rangle$	0

Table 3.3 Modified Tangle of the three-qubit Vector States of the Symmetric Group S_3

We define the this modification for the four qubits as

$$\zeta(\psi) = |2a_{0000}a_{1111} - 16a_{0001}a_{0010}a_{0100}a_{1000} - 16a_{0111}a_{1011}a_{1101}a_{1110} - 216|a_{0011}a_{0101}a_{0110}a_{1001}a_{1010}a_{1100}| \tag{3.103}$$

For our four-qubit vector states,

The problem with this modification is that the terms need all the quantum states with

Vector State	ζ
$\|\psi_1^{(3)}\rangle$	$\frac{1}{3}$
$\|\psi_2^{(3)}\rangle$	0
$\|\psi_3^{(3)}\rangle$	0
$\|\psi_4^{(3)}\rangle$	1
$\|\psi_5^{(3)}\rangle$	$\frac{1}{2}$
$\|\psi_6^{(3)}\rangle$	0
$\|\psi_7^{(3)}\rangle$	$\frac{1}{3}$
$\|\psi_8^{(3)}\rangle$	0
$\|\psi_9^{(3)}\rangle$	0
$\|\psi_{10}^{(3)}\rangle$	$\frac{1}{2}$
$\|\psi_{11}^{(3)}\rangle$	0
$\|\psi_{12}^{(3)}\rangle$	0
$\|\psi_{13}^{(3)}\rangle$	1
$\|\psi_{14}^{(3)}\rangle$	1
$\|\psi_{15}^{(3)}\rangle$	1
$\|\psi_{16}^{(3)}\rangle$	0

Table 3.4 Modified Tangle of the four-qubit Vector States of the Symmetric Group S_4

the same Hamming weight to be present, for giving a value of this witness. However, we know that there can be entangled states with lesser than that number, such as $|\psi\rangle = \frac{1}{\sqrt{3}}(|0011\rangle + |0110\rangle + |1001\rangle)$.

To overcome this problem and define an entanglement witness that provides information about entanglement for states with the same Hamming weight, we define a new entanglement witness called 'engle' as

$$\zeta(\tau) = \frac{1}{(1-\frac{1}{N_{P_n}})^{N_{P_n}}}(\prod_i(1 - |a_i|^2))f(\prod_S(\sum_j|T_{|S\rangle_1,|S\rangle_j} - T_{|S_r\rangle_1,|S_r\rangle_j}|)) \quad (3.104)$$

where n represents the number of $|1\rangle$ qubits and

$$T_{|S\rangle_i,|S\rangle_j} = 1 \text{ if } |S\rangle_i - |S\rangle_j = |0\rangle \text{ or } 0 \text{ otherwise.} \quad (3.105)$$

The function $f : f(x) = 1 \forall x \neq 0; f(x) = 0, x = 0$. $|S\rangle_i$ is a subsystem of the i^{th} superposition term in a state, with their being N superposition terms, while $|S_r\rangle_i$ denotes the remainder

subsystem of the quantum state.

In this quantity, there are two parts of the witness: $\prod_i (1 - \frac{|a_i|}{N})$ and $f(\prod_S (\sum_j |T_{|S\rangle_1,|S\rangle_j} - T_{|S_r\rangle_1,|S_r\rangle_j}|))$. The former tells us about the amount of entanglement, using the symmetry considerations and Statement 3.1, while the latter removes cases that are separable.

Let us test this for our five qubit vector-states, as tabulated in Table 3.5. Looking at the table, we can see that this newly defined measure is a good tool to not only study the separability but also the entanglement using symmetry considerations. The natural extension to this concept would deal with the situation when states with different Hamming weight are evaluated, and this comprises the *Further Work* based on this project.

Vector State	ζ
$\|\psi_1^{(5)}\rangle$	0.857299
$\|\psi_2^{(5)}\rangle$	0.888698
$\|\psi_3^{(5)}\rangle$	0
$\|\psi_4^{(5)}\rangle$	0
$\|\psi_5^{(5)}\rangle$	0
$\|\psi_6^{(5)}\rangle$	0.857299
$\|\psi_7^{(5)}\rangle$	0.888698
$\|\psi_8^{(5)}\rangle$	0
$\|\psi_9^{(5)}\rangle$	0
$\|\psi_{10}^{(5)}\rangle$	0
$\|\psi_{11}^{(5)}\rangle$	0.497137
$\|\psi_{12}^{(5)}\rangle$	0
$\|\psi_{13}^{(5)}\rangle$	0
$\|\psi_{14}^{(5)}\rangle$	0
$\|\psi_{15}^{(5)}\rangle$	0.989633
$\|\psi_{16}^{(5)}\rangle$	0.975028
$\|\psi_{17}^{(5)}\rangle$	0.0.957635
$\|\psi_{18}^{(5)}\rangle$	0
$\|\psi_{19}^{(5)}\rangle$	0.497137
$\|\psi_{20}^{(5)}\rangle$	0
$\|\psi_{21}^{(5)}\rangle$	0
$\|\psi_{22}^{(5)}\rangle$	0
$\|\psi_{23}^{(5)}\rangle$	0.989633
$\|\psi_{24}^{(5)}\rangle$	0.975028
$\|\psi_{25}^{(5)}\rangle$	0.957635
$\|\psi_{26}^{(5)}\rangle$	0
$\|\psi_{27}^{(5)}\rangle$	0
$\|\psi_{28}^{(5)}\rangle$	1
$\|\psi_{29}^{(5)}\rangle$	1
$\|\psi_{30}^{(5)}\rangle$	1
$\|\psi_{31}^{(5)}\rangle$	1
$\|\psi_{32}^{(5)}\rangle$	0

Table 3.5 Engle of the four-qubit Vector States of the Symmetric Group S_5

Chapter 4

Quantum Computation using $SWAP^{1/n}$ Gates

Quantum Computation is the manipulation of quantum resources and quantum entanglement therein for the purposes of realizing an information processing task. Historically, the circuit-based model of quantum computation and measurement-based model of quantum computation have been the most popular. These arise from the key concepts of evolution and measurement of a quantum particle or system.

The $SWAP^{1/n}$ gate is a powerful tool for carrying out quantum computation, due to its ubiquity in physical systems such as those with exchange interactions. We have seen that the locus of states accessible using these gates is restricted to a certain subspace of the Hilbert space. As a result, it is understood that not all states are accessible by only using the $SWAP^{1/n}$ gate.

In this chapter, we will be looking at how to realize quantum computation using the $SWAP^{1/n}$ as the key cornerstone of this discussion.

4.1 Circuit-based Quantum Computers using $SWAP^{1/n}$ Gates

In the realm of quantum information, a quantum circuit model of quantum computation is one wherein a computation is a sequence of quantum gates. These quantum gates are reversible transformations on a quantum register, a system comprising multiple qubits. The key paradigm shift, going from classical computation to quantum computation is the presence of reversible (quantum) logic gates. These logic gates, in contrast to classical logic gates,

are always reversible due to them being a form of reversible function known as a unitary mapping. These mappings preserve the Hermitian inner product and a general n-qubit (reversible) quantum gate is a unitary mapping U from the Hilbert space of n-qubits onto itself. The pertinent point to be addressed here is regarding the number of quantum gates and resources required that can optimally approximate any quantum computation.

4.1.1 Universal Gate Set with $SWAP^{1/n}$

A set of universal quantum gates is a set of quantum gates that can, in a finite sequence of gates from this set, replicate any arbitrary unitary operation that may be possible on a quantum computer [70, 281–283, 69]. For physical systems with exchange interaction, universal quantum gates have been constructed with encoded qubits [25, 284], while the Loss-Divincenzo Quantum Computer relies on the $\sqrt{SWAP}$ and single-qubit gates [115]. As part of this project, we see that this can be extended to the case of any general Power-of-SWAP $SWAP^{1/n}$. Before doing this, let us look at some of the existing sets of universal quantum gates:

1. Hadamard Gate: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, the Phase-Shift gate for angle $\frac{\pi}{4}$: $R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ and the CNOT gate: $U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ comprise a universal quantum gate set. Single qubit rotation gates: $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and CNOT gate: $U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, can also be used to implement an arbitrary unitary operation on n qubits and therefore constitute a universal gate set[285].

2. The Ising Gate: $U_{XX_\phi} = \begin{pmatrix} 1 & 0 & 0 & -ie^{i\phi} \\ 0 & 1 & -i & 0 \\ 0 & -i & 1 & 0 \\ -ie^{-i\phi} & 0 & 0 & 1 \end{pmatrix}$ and the Phase-Shift gate:

$R_\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varepsilon} \end{pmatrix}$ constitute a universal gate set [286].

DiVincenzo and Loss [115] showed that the $\sqrt{SWAP}$ gate is universal with single-qubit rotations. This universality is derived in terms of the relation of the $\sqrt{SWAP}$ gate with the classical XOR gate, which can be realized using the CNOT gate in the realm of quantum information processing [287]. This leads us to believe that a generalized case (of any general Power-of-SWAP can comprise a universal gate set too).

The first step in defining a universal gate set using $SWAP^\alpha$ is to realize that no such set can be made purely out of $SWAP^\alpha$ gates since these gates preserve Hamming weight of the quantum state representation. If we allow single qubit unitary operations, let us see the lowest number of $SWAP^\alpha$ that are required to carry this out. Given this symmetry of the $SWAP^\alpha$ gates, the cases we look into are: $A_1|00\rangle + B_1|11\rangle \rightarrow A_2|00\rangle + B_2|11\rangle, |A_1|^2 + |B_1|^2 = |A_2|^2 + |B_2|^2 = 1$ and $C_1|01\rangle + D_1|10\rangle \rightarrow C_2|01\rangle + D_2|10\rangle, |C_1|^2 + |D_1|^2 = |C_2|^2 + |D_2|^2 = 1$. However, how is this possible if the $SWAP^\alpha$ gate leaves the states $|00\rangle$ and $|11\rangle$ unchanged? This can be done by using a qubit-flip gate on one of the qubits:

$$U_1 = U_{SWAP^{\alpha_1}}(\sigma_x \otimes I_{2\times 2})U_{SWAP^{\alpha_2}} = \begin{pmatrix} 0 & \frac{1-e^{i\pi\alpha_2}}{2} & \frac{1+e^{i\pi\alpha_2}}{2} & 0 \\ \frac{1-e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{1+e^{i\pi\alpha_1}}{2} \\ \frac{1+e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{1-e^{i\pi\alpha_1}}{2} \\ 0 & \frac{1+e^{i\pi\alpha_2}}{2} & \frac{1-e^{i\pi\alpha_2}}{2} & 0 \end{pmatrix} \tag{4.1}$$

The $SWAP^\alpha$ also has a fixed accessibility of states, as mentioned previously in this paper. Since the sum of the coefficients for vectors with the same Hamming weight add to the same value over an operation of $SWAP^\alpha$ gates, states that do not follow this rule cannot be accessed. To begin with, two Bell-states differing by a relative phase of $e^{i\pi}$ cannot be inter-converted using $SWAP^\alpha$ gates. This can, however, be achieved using a phase-flip operator on a single qubit, say the second qubit.

$$U_2 = U_1(I_{2\times 2} \otimes \sigma_z) = \begin{pmatrix} 0 & \frac{-1+e^{i\pi\alpha_2}}{2} & \frac{1+e^{i\pi\alpha_2}}{2} & 0 \\ \frac{1-e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{-1-e^{i\pi\alpha_1}}{2} \\ \frac{1+e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{-1+e^{i\pi\alpha_1}}{2} \\ 0 & \frac{-1-e^{i\pi\alpha_2}}{2} & \frac{1-e^{i\pi\alpha_2}}{2} & 0 \end{pmatrix} \tag{4.2}$$

Even though this brings in the extreme case of $|\psi_{\pm}\rangle \rightarrow |\psi_{mp}\rangle$ and $|\phi_{\pm}\rangle \rightarrow |\phi_{mp}\rangle$, there are lots of other states that should be accessible using a general two qubit unitary gate. This greater independence is seen to come from the application of yet another $SWAP^{\alpha}$ gate:

$$U_3 = U_2 U_{SWAP^{\alpha_3}} = \begin{pmatrix} 0 & \frac{e^{i\pi\alpha_2}-e^{i\pi\alpha_3}}{2} & \frac{e^{i\pi\alpha_2}+e^{i\pi\alpha_3}}{2} & 0 \\ \frac{1-e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{-1-e^{i\pi\alpha_1}}{2} \\ \frac{1+e^{i\pi\alpha_1}}{2} & 0 & 0 & \frac{-1+e^{i\pi\alpha_1}}{2} \\ 0 & \frac{-e^{i\pi\alpha_2}-e^{i\pi\alpha_3}}{2} & \frac{-e^{i\pi\alpha_2}+e^{i\pi\alpha_3}}{2} & 0 \end{pmatrix} \tag{4.3}$$

This along with local unitary operations $\{K_i, L_i\}$, where the index i denotes the qubit being operated on, should be able to implement any general two-qubit quantum gate. Hence, in the most general form, any two qubit quantum gate can be realized by the expansion

$$(K_1 \otimes K_2)(U_{SWAP^{\alpha_1}}(\sigma_x \otimes I_{2\times 2})U_{SWAP^{\alpha_2}}(I_{2\times 2} \otimes \sigma_z) \times U_{SWAP^{\alpha_3}})(L_1 \otimes L_2) \tag{4.4}$$

Any circuit with two-qubit and single-qubit gates can thus be constructed using the $SWAP^{\alpha}$ gate, alongwith single-qubit unitary operations. This can be presented as a Theorem.

Theorem 4.1. Any unitary operation $U \in SU(4)$ acting on two qubits can be realized using only three $SWAP^{1/n}$ gates, along with single-qubit unitary gates.

Proof. Kraus et al [288] showed that an arbitrary unitary transformation $U \in SU(4)$ can be decomposed into

$$U = (K_A \otimes K_B)e^d(L_A \otimes L_B) \tag{4.5}$$

where

$$d = -i(\sum_k h_k \sigma_k \otimes \sigma_k), k = 1,2,3 \tag{4.6}$$

and

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.7}$$

with $\frac{\pi}{4} \geq h_1 \geq h_2 \geq h_3 \geq 0$ since it is seen that the maximal amount of entanglement created by e^d is symmetric around $\frac{\pi}{4}$, and $\frac{\pi}{2}$-periodic in h_1, h_2 and h_3.

Considering the matrix form of d' ($= id$) using equations (4.5), (4.6) and (4.7),

$$
\begin{aligned}
d' &= \begin{pmatrix} h_3 & 0 & 0 & h_1-h_2 \\ 0 & -h_3 & h_1+h_2 & 0 \\ 0 & h_1+h_2 & -h_3 & 0 \\ h_1-h_2 & 0 & 0 & h_3 \end{pmatrix} \\
&= \begin{pmatrix} h_3 & 0 & 0 & h_1-h_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ h_1-h_2 & 0 & 0 & h_3 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -h_3 & h_1+h_2 & 0 \\ 0 & h_1+h_2 & -h_3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
&= (h_3+h_1-h_2)|\psi_+\rangle\langle\psi_+| + (h_3-h_1+h_2)|\psi_-\rangle\langle\psi_-| \\
&+ (-h_3+h_1+h_2)|\phi_+\rangle\langle\phi_+| + (-h_3-h_1-h_2)|\phi_-\rangle\langle\phi_-| \\
&= A_{\psi_+}|\psi_+\rangle\langle\psi_+| + A_{\psi_-}|\psi_-\rangle\langle\psi_-| + A_{\phi_+}|\phi_+\rangle\langle\phi_+| + A_{\phi_-}|\phi_-\rangle\langle\phi_-| \quad (4.8)
\end{aligned}
$$

where $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. By the property of exponentiation of matrices, we have

$$
e^d = e^{-id'} = e^{-iA_{\psi_+}}|\psi_+\rangle\langle\psi_+| + e^{-iA_{\psi_-}}|\psi_-\rangle\langle\psi_-| + e^{-iA_{\phi_+}}|\phi_+\rangle\langle\phi_+| + e^{-iA_{\phi_-}}|\phi_-\rangle\langle\phi_-| \quad (4.9)
$$

A point to note here is the effect of $SWAP^{1/n}$ on the Bell basis:

$$U_{SWAP^{1/n}}|\psi_+\rangle = |\psi_+\rangle \quad (4.10)$$

$$U_{SWAP^{1/n}}|\psi_-\rangle = |\psi_-\rangle \quad (4.11)$$

$$U_{SWAP^{1/n}}|\phi_+\rangle = |\phi_+\rangle \quad (4.12)$$

$$U_{SWAP^{1/n}}|\phi_-\rangle = e^{i\pi/n}|\phi_-\rangle \quad (4.13)$$

and the effect of single-qubit rotations:

$$(\sigma_x \otimes \mathbb{I}_{2\times 2})|\psi_+\rangle = |\phi_+\rangle, (\sigma_x \otimes \mathbb{I}_{2\times 2})|\phi_+\rangle = |\psi_+\rangle \quad (4.14)$$

$$(\sigma_x \otimes \mathbb{I}_{2\times 2})|\psi_-\rangle = -|\phi_-\rangle, (\sigma_x \otimes \mathbb{I}_{2\times 2})|\phi_-\rangle = -|\psi_-\rangle \quad (4.15)$$

$$(\mathbb{I}_{2\times 2} \otimes \sigma_x)|\psi_+\rangle = |\phi_+\rangle, (\mathbb{I}_{2\times 2} \otimes \sigma_x)|\phi_+\rangle = |\psi_+\rangle \quad (4.16)$$

$$(\mathbb{I}_{2\times 2} \otimes \sigma_x)|\psi_-\rangle = |\phi_-\rangle, (\mathbb{I}_{2\times 2} \otimes \sigma_x)|\phi_-\rangle = |\psi_-\rangle \quad (4.17)$$

$$(\sigma_z \otimes \mathbb{I}_{2\times 2})|\psi_+\rangle = |\psi_-\rangle, (\sigma_z \otimes \mathbb{I}_{2\times 2})|\psi_-\rangle = |\psi_+\rangle \quad (4.18)$$

$$(\sigma_z \otimes \mathbb{I}_{2\times 2})|\phi_+\rangle = |\phi_-\rangle, (\sigma_z \otimes \mathbb{I}_{2\times 2})|\phi_-\rangle = |\phi_+\rangle \tag{4.19}$$

$$(\mathbb{I}_{2\times 2} \otimes \sigma_z)|\psi_+\rangle = |\psi_-\rangle, (\mathbb{I}_{2\times 2} \otimes \sigma_z)|\psi_-\rangle = |\psi_+\rangle \tag{4.20}$$

$$(\mathbb{I}_{2\times 2} \otimes \sigma_z)|\phi_+\rangle = -|\phi_-\rangle, (\mathbb{I}_{2\times 2} \otimes \sigma_z)|\phi_-\rangle = -|\phi_+\rangle \tag{4.21}$$

Thus, due to equations (4.10)-(4.21), application of distinct $SWAP^{1/n}$ along with single-qubit rotations can give independent phases for each of the Bell-basis states. We can now write equation (4.22) as

$$\begin{aligned} e^d &= e^{-iA_{\phi_+}}(|\phi_+\rangle\langle\phi_+| + e^{-iA_{\phi_-}+iA_{\phi_+}}|\phi_-\rangle\langle\phi_-| + e^{-iA_{\psi_+}+iA_{\phi_+}}|\psi_+\rangle\langle\psi_+| + e^{-iA_{\psi_-}+iA_{\phi_+}}|\psi_-\rangle\langle\psi_-|) \\ &= e^{-i(h_3-h_1-h_2)}(|\phi_+\rangle\langle\phi_+| + e^{2i(h_1+h_2)}|\phi_-\rangle\langle\phi_-| \\ &\quad + e^{2i(h_2-h_3)}|\psi_+\rangle\langle\psi_+| + e^{2i(h_1-h_3)}|\psi_-\rangle\langle\psi_-|) \end{aligned} \tag{4.22}$$

We can write the matrix form for convenience,

$$\begin{aligned} e^d &= e^{-i(h_3-h_1-h_2)} \begin{pmatrix} e^{2i(h_2-h_3)} + e^{2i(h_1-h_3)} & 0 & 0 & e^{2i(h_2-h_3)} - e^{2i(h_1-h_3)} \\ 0 & 1+e^{2i(h_1+h_2)} & 1-e^{2i(h_1+h_2)} & 0 \\ 0 & 1-e^{2i(h_1+h_2)} & 1+e^{2i(h_1+h_2)} & 0 \\ e^{2i(h_2-h_3)} - e^{2i(h_1-h_3)} & 0 & 0 & e^{2i(h_2-h_3)} + e^{2i(h_1-h_3)} \end{pmatrix} \\ &= e^{-i(h_3-h_1-h_2)} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1+e^{2i(h_1+h_2)} & 1-e^{2i(h_1+h_2)} & 0 \\ 0 & 1-e^{2i(h_1+h_2)} & 1+e^{2i(h_1+h_2)} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ &\quad + e^{-i(h_3-h_1-h_2)} \begin{pmatrix} e^{2i(h_2-h_3)} + e^{2i(h_1-h_3)} & 0 & 0 & e^{2i(h_2-h_3)} - e^{2i(h_1-h_3)} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ e^{2i(h_2-h_3)} - e^{2i(h_1-h_3)} & 0 & 0 & e^{2i(h_2-h_3)} + e^{2i(h_1-h_3)} \end{pmatrix} \end{aligned} \tag{4.23}$$

Observing these matrices, and noting some properties of tensor product of Pauli-matrices that we studied and that are relevant for this section:

$$(I \otimes \sigma_x) \begin{pmatrix} A & B & c & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix} (I \otimes \sigma_x) \rightarrow \begin{pmatrix} F & E & H & G \\ B & A & D & C \\ N & M & P & O \\ J & I & L & K \end{pmatrix} \tag{4.24}$$

$$(I\otimes\sigma_x\sigma_z)\begin{pmatrix} A & B & C & D\\ E & F & G & H\\ I & J & K & L\\ M & N & O & P\end{pmatrix}(I\otimes\sigma_x\sigma_z)\rightarrow\begin{pmatrix} -F & E & -H & G\\ B & -A & D & -C\\ -N & M & -P & O\\ J & -I & L & -K\end{pmatrix} \tag{4.25}$$

leads us to a $SWAP^{1/n}$-matrix based form,

$$\begin{aligned} e^d = e^{-i(h_3-h_1-h_2)}(&SWAP^{2(h_1+h_2)/\pi}+(I\otimes\sigma_x)SWAP^{2(h_2-h_3)/\pi}(I\otimes\sigma_x)\\ &-(I\otimes\sigma_x\sigma_z)SWAP^{2(h_1-h_3)/\pi}(I\otimes\sigma_x\sigma_z)) \end{aligned} \tag{4.26}$$

However, this is not suitable for construction in a circuit model, which is usually used to sequential application of gates and therefore a multiplication instead of addition of unitary operators. By observing the matrix form in equation (4.23) we can see that there is a manner of constructing a decomposition of e^d in terms of a product of operators:

$$\begin{aligned} e^d &= e^{-i(h_3-h_1-h_2)}(SWAP^{2(h_1+h_2)/\pi}\times(I\otimes\sigma_x)SWAP^{2(h_1-h_3)/\pi}(I\otimes\sigma_x)\\ &\qquad\times(I\otimes\sigma_x\sigma_z)SWAP^{2(h_2-h_3)/\pi}(I\otimes\sigma_x\sigma_z))\\ &= e^{-i(h_3-h_1-h_2)}(SWAP^{2(h_1+h_2)/\pi}\times(I\otimes\sigma_x)SWAP^{2(h_1-h_3)/\pi}\\ &\qquad\times(I\otimes\sigma_z)SWAP^{2(h_2-h_3)/\pi}(I\otimes\sigma_x\sigma_z)) \end{aligned} \tag{4.27}$$

since $(I\otimes\sigma_x)\times(I\otimes\sigma_x\sigma_z)=(I\otimes\sigma_z)$. We further simplified this by observing the property that $(\sigma_z\otimes\sigma_z)SWAP^{1/n}(\sigma_z\otimes\sigma_z)$ for any Power-of-SWAP,

$$\begin{aligned} e^d &= e^{-i(h_3-h_1-h_2)}(SWAP^{2(h_1+h_2)/\pi}\times(I\otimes\sigma_x)SWAP^{2(h_1-h_3)/\pi}\\ &\qquad\times(I\otimes\sigma_z)(\sigma_z\otimes\sigma_z)SWAP^{2(h_2-h_3)/\pi}(\sigma_z\otimes\sigma_z)(I\otimes\sigma_x\sigma_z))\\ &= e^{-i(h_3-h_1-h_2)}(SWAP^{2(h_1+h_2)/\pi}\times(I\otimes\sigma_x)SWAP^{2(h_1-h_3)/\pi}\\ &\qquad\times(\sigma_z\otimes I)SWAP^{2(h_2-h_3)/\pi}(\sigma_z\otimes\sigma_x)) \end{aligned} \tag{4.28}$$

This, along with local unitary operations K_1,K_2,L_1,L_2 in equation (4.5), can reconstruct any two qubit unitary operation. This proves that $SWAP^{1/n}$ with single qubit unitary gates constitutes a universal gate set. ■

4.2 Invariant Subspace-based Quantum Computers using $SWAP^{1/n}$

Quantum computers are able to solve certain problems more efficiently than possible conventional classical computer [137, 289, 69, 290, 285, 291]. Quantum algorithms have been realized on multiple quantum computing platforms, many of which are specifically customised in hardware to implement a particular algorithm or execute a computational task.

The three most important sections of a quantum computer are: high-fidelity initialization of the input quantum state, detection by measurement of the output quantum state at the individual qubit level and control of operations by interactions between qubits. In the previous section, we have defined universality of a set of quantum gates comprising the $SWAP^{1/n}$ and quantum single-qubit rotation gates. This is sufficient for universal quantum computation. Later in the chapter, we will be discussing qudit-based quantum computing and cluster state quantum computing using $SWAP^{1/n}$ gates. In this section, we present our findings of a model of quantum computing that uses encoded quantum states as resource and that belong to the invariant subspaces of the symmetric group.

Divincenzo et al [25] defined an encoded quantum computation model based on encoding three physical qubits in one logical qubit. For the case of qubits operated upon by the exchange interaction, we can have a different model of encoding and quantum computation that exploits the (permutation) symmetry of the system. For instance, for the three-qubit case, we can consider the invariant subspace [21] and Hamming weight 1,

$$\alpha|1\rangle + \beta|2\rangle \xrightarrow{U} \alpha'|1\rangle + \beta'|2\rangle \tag{4.29}$$

where U is an operation based on the symmetry of the invariant subspace.

If one were to start with a state that is a superposition of vectors within an invariant subspace and operate on it with an operator that abides by that symmetry, then the resultant output state willl remain in the invariant subspace. The selection of invariant subspace depends on the number of vector states we want as our basis. This directly relates to the dimensionality of the invariant subspace.

Let us look at the kinds of initializations, operation and measurements that are required for

this model of quantum computing.

Initialization: Ideally an input quantum state for a quantum computer is separable. However, in this model of invariant subspace-based quantum computation, the input state must respect the symmetry of the invariant subspace. As a result, the input state can be the vector state, of the invariant subspace selected, which is closest to a separable state. For instance, for three-qubit states with the invariant subspace [21] and Hamming weight 1, a good input state would be $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |100\rangle)$.

Operations: The operations that can be applied on the vector-state are selected based on the symmetry of the invariant subspace. Firstly, we look at all the Young's Tableaux for the invariant subspace. Thereafter, we decompose the cycle-structure into transpositions and apply associated $SWAP^{1/n}$ on the vector state. The selection of the Power-of-SWAP depends on the output state that is required.

Measurements: The measurement basis for the invariant-subspace based quantum computing model comprises the m vector-states in the invariant subspace

$$V = \{V_1, V_2, ..., V_m\} \tag{4.30}$$

Theoretically, this measurement can be carried out by projection operators onto the vector states.

To truly understand the scope of this quantum computation model, let us look at the realization of a few-qubit cases. We do this by firstly looking at the evaluation of the invariant subspaces and associated vector-states, and then present the manner in which invariant-subspace based quantum computation can be realized in these cases.

4.2.1 Three-Qubit Quantum Computer

The simplest quantum computer that can be constructed, which has more than one $SWAP^{1/n}$ involved, is a three-qubit quantum computer. The initial state of this system can be any of

the following

$$\psi_n = \begin{pmatrix} |000\rangle \\ |001\rangle \\ |010\rangle \\ |011\rangle \\ |100\rangle \\ |101\rangle \\ |110\rangle \\ |111\rangle \end{pmatrix} \tag{4.31}$$

The underlying symmetry of the system is described by the S_3 symmetric group. We have previously discussed the character table and the irreducible representations of this group in Chapter 2. Using these elements and conceptual tools, it is found that the [21] and [3] partitions of the S_3 group, for the three-qubit states, are the relevant partitions for our systems.

For this system, the invariant subspace-vector states are found to be as follows

$$|\psi_1\rangle = \frac{1}{\sqrt{6}}(|001\rangle + |100\rangle) - \sqrt{\frac{2}{3}}|010\rangle \tag{4.32}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |100\rangle) \tag{4.33}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{6}}(|011\rangle + |110\rangle) - \sqrt{\frac{2}{3}}|101\rangle \tag{4.34}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(-|011\rangle + |110\rangle) \tag{4.35}$$

$$|\psi_5\rangle = |000\rangle \tag{4.36}$$

$$|\psi_6\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100) \tag{4.37}$$

$$|\psi_7\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |110\rangle + |101) \tag{4.38}$$

$$|\psi_8\rangle = |111\rangle \tag{4.39}$$

Now, states $|\psi_1\rangle$ - $|\psi_2\rangle$ and $|\psi_3\rangle$ - $|\psi_4\rangle$ constitute the first and second families of states, respectively, for our three-qubit case.

$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_1\rangle \rightarrow |\psi_1\rangle \tag{4.40}$$

$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_2\rangle \rightarrow i|\psi_2\rangle \tag{4.41}$$

$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_3\rangle \rightarrow |\psi_3\rangle \tag{4.42}$$

$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_4\rangle \rightarrow i|\psi_4\rangle \tag{4.43}$$

This result is expected since this is a family of states that remains invariant under a [21] partition transformation, up to a global phase.

The states $|\psi_5\rangle$, $|\psi_6\rangle$, $|\psi_7\rangle$ and $|\psi_8\rangle$ compose the families: 3, 4, 5 and 6 respectively. For all these families (3, 4, 5 and 6), the state remains invariant under all possible permutations of the entanglers: $R_{swap} \otimes I$, $I \otimes R_{swap}$ and $(R_{swap} \otimes I) \times (I \otimes R_{swap})$. This is expected for the [111] case. It is also valid for the [3] partition case, which refers to no intermixing of the states.

Within each family of states, we find a hierarchy based on the classification put forward by Dür et al [292]. In Family 1, the state $|\psi_1\rangle$ falls in the W-class of states. Using the transformation

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \tag{4.44}$$

we can obtain the standard W-state: $|\psi_W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

The other state in Family 1 lies in the $A-BC$ seperable class in the same classification. It is a partially seperable state of the form:

$$|\psi_2\rangle = |0\rangle_2 \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{13} \tag{4.45}$$

The same is true for Family 2 as well, after the application of an $X^{\otimes 3}$ gate, where X represents the σ_x pauli matrix operation.

The states $|\psi_5\rangle$ and $|\psi_8\rangle$ are $A-B-C$ seperable states according to Dür's classification, while $|\psi_6\rangle$ and $|\psi_7\rangle$ belong to the W-class, with the latter being so under an application of $X^{\otimes 3}$.

Thus the states are neatly arranged into the following chart:

$$\begin{pmatrix} \frac{1}{\sqrt{2}}\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&-2\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\rightarrow W-Class \\ A-BC \\ X^{\otimes 3}\rightarrow\frac{1}{\sqrt{2}}\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&-2\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\rightarrow W-Class \\ X^{\otimes 3}\rightarrow A-BC \\ A-B-C \\ W-class \\ X^{\otimes 3}\rightarrow W-class \\ A-B-C \end{pmatrix} \tag{4.46}$$

Although, this gives us a neat way of arranging the elements and their classes, it is the seperable product states that we are interested in, due to the ease of preparation of such states as input states. States of the form

$$\sqrt{2}|\psi_1\rangle - |\psi_6\rangle = -\sqrt{3}|010\rangle \tag{4.47}$$

$$\sqrt{2}|\psi_3\rangle - |\psi_7\rangle = -\sqrt{3}|101\rangle \tag{4.48}$$

can be considered in this regard. We see that upon application of an entangler combination, the aforementioned states in equations (18) and (19) produce states that are linear superpositions of the 2-dimensional subgroup and the relevant one-dimensional subgroup mentioned above.

For example, operating with $R_{Swap}\otimes I_{2\times 2}$ on $|010\rangle$ gives

$$\psi_{(\sqrt{SWAP}\otimes I_{2\times 2})|010\rangle} = \frac{1}{2}(1+i)|010\rangle + \frac{1}{2}(1-i)|100\rangle = A|\psi_1\rangle + B|\psi_2\rangle + C|\psi_6\rangle \tag{4.49}$$

It is found that

$$A = \frac{1}{2\sqrt{3}}(1-i) - \frac{1}{\sqrt{6}}(1+i), B = -\frac{1}{2\sqrt{2}}(1-i), C = \frac{1}{\sqrt{6}}(1-i) + \frac{1}{6}(1+i) \tag{4.50}$$

States $|\psi_1\rangle$ and- $|\psi_2\rangle$ and $|\psi_3\rangle$ - $|\psi_4\rangle$constitute the first and second families of states, respectively, for our three-qubit case.

$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_1\rangle \rightarrow |\psi_1\rangle \tag{4.51}$$
$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_2\rangle \rightarrow i|\psi_2\rangle \tag{4.52}$$
$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_3\rangle \rightarrow |\psi_3\rangle \tag{4.53}$$
$$((R_{swap})_{13} \otimes (I_{2\times 2})_2)|\psi_4\rangle \rightarrow i|\psi_4\rangle \tag{4.54}$$

This result is expected since this is a family of states that remains invariant under a [21] partition transformation, up to a global phase.

The states $|\psi_5\rangle$, $|\psi_6\rangle$, $|\psi_7\rangle$ and $|\psi_8\rangle$ compose the families: 3, 4, 5 and 6 respectively. For all these families (3, 4, 5 and 6), the state remains invariant under all possible permutations of the entanglers: $R_{swap} \otimes I$, $I \otimes R_{swap}$ and $(R_{swap} \otimes I) \times (I \otimes R_{swap})$. This is expected for the [111] case. It is also valid for the [3] partition case, which refers to no intermixing of the states.

Within each family of states, we find a hierarchy based on the classification put forward by Dür et al [292]. In Family 1, the state $|\psi_1\rangle$ falls in the W-class of states. Using the transformation

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \tag{4.55}$$

we can obtain the standard W-state: $|\psi_W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

The other state in Family 1 lies in the $A - BC$ separable class in the same classification. It is a partially separable state of the form:

$$|\psi_2\rangle = |0\rangle_2 \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{13} \tag{4.56}$$

The same is true for Family 2 as well, after the application of an $X^{\otimes 3}$ gate, where X represents the σ_x pauli matrix operation.

The states $|\psi_5\rangle$ and $|\psi_8\rangle$ are $A - B - C$ separable states according to Dür's classification, while $|\psi_6\rangle$ and $|\psi_7\rangle$ belong to the W-class, with the latter being so under an application of

$X^{\otimes 3}$.

Thus the states are neatly arranged into the following chart:

$$\begin{pmatrix} \frac{1}{\sqrt{2}}\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&-2\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\rightarrow W-\text{Class} \\ \text{A-BC} \\ X^{\otimes 3}\rightarrow\frac{1}{\sqrt{2}}\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&-2\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\rightarrow W-\text{Class} \\ X^{\otimes 3}\rightarrow A-BC \\ \text{A-B-C} \\ W-\text{class} \\ X^{\otimes 3}\rightarrow W-\text{class} \\ \text{A-B-C} \end{pmatrix} \tag{4.57}$$

Although, this gives us a neat way of arranging the elements and their classes, it is the separable product states that we are interested in, due to the ease of preparation of such states as input states. States of the form

$$\sqrt{2}|\psi_1\rangle - |\psi_6\rangle = -\sqrt{3}|010\rangle \tag{4.58}$$

$$\sqrt{2}|\psi_3\rangle - |\psi_7\rangle = -\sqrt{3}|101\rangle \tag{4.59}$$

can be considered in this regard. We see that upon application of an entangler combination, the aforementioned states in equations (18) and (19) produce states that are linear superpositions of the 2-dimensional subgroup and the relevant one-dimensional subgroup mentioned above.

For example, operating with $R_{Swap}\otimes I_{2\times 2}$ on $|010\rangle$ gives

$$\begin{aligned}\psi_{(\sqrt{SWAP}\otimes I_{2\times 2})|010\rangle} &= \frac{1}{2}(1+i)|010\rangle + \frac{1}{2}(1-i)|100\rangle \\ &= A|\psi_1\rangle + B|\psi_2\rangle + C|\psi_6\rangle \end{aligned} \tag{4.60}$$

It is found that

$$A = \frac{1}{2\sqrt{3}}(1-i) - \frac{1}{\sqrt{6}}(1+i), B = -\frac{1}{2\sqrt{2}}(1-i), C = \frac{1}{\sqrt{6}}(1-i) + \frac{1}{6}(1+i) \tag{4.61}$$

It is thus found that a higher-dimensional unit of information, based on the vectors in the invariant subspace, have properties that makes it evolve in a specific way. For instance, the one-dimensional irrep vectors remain unchanged with the operation of any combination of $SWAP^{1/n}$ gates, while higher dimensional irreps evolve within their invariant subspace.

4.2.2 Four-Qubit Quantum Computer

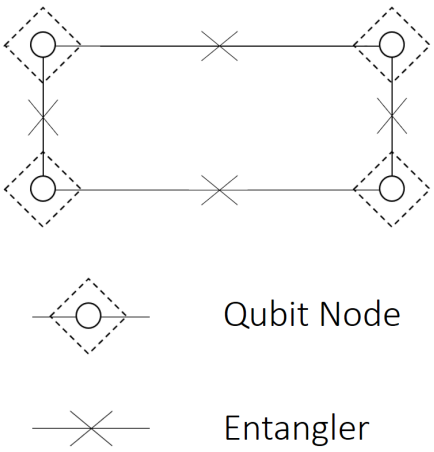


Fig. 4.1 Four-Qubit Quantum Computer

For the S_4 group, we have

$f[\mu] = 1$ for the partition [4]
$f[\mu] = 3$ for the partition [31]
$f[\mu] = 2$ for the partition [22]
$f[\mu] = 3$ for the partition [211]
$f[\mu] = 1$ for the partition [1111]

Let us take the following basis vectors:

$\hat{e}^{[1111]}_{1234}$ for the partition [1111]
$\hat{e}^{[211]}_{1123}$, $\hat{e}^{[211]}_{1213}$ and $\hat{e}^{[211]}_{1231}$ for the partition [211]
$\hat{e}^{[22]}_{1122}$ and $\hat{e}^{[22]}_{1212}$ for the partition [22]
$\hat{e}^{[31]}_{1112}$, $\hat{e}^{[31]}_{1121}$ and $\hat{e}^{[31]}_{1211}$ for the partition [31]
$\hat{e}^{[4]}_{1111}$ for the partition [4]

where

$$\hat{e}^{[211]}_{1123} = \hat{e}^{[31]}_{1112} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \hat{e}^{[211]}_{1213} = \hat{e}^{[31]}_{1121} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \hat{e}^{[211]}_{1231} = \hat{e}^{[31]}_{1211} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{4.62}$$

$$\hat{e}^{[22]}_{1122} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \hat{e}^{[22]}_{1212} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{4.63}$$

Using (44), we can find the matrix representation for the generator transpositions (12), (23) and (34).

$$D(12) = -1 \text{ for } [1111]$$
$$D(12) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ for } [211]$$
$$D(12) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ for } [22]$$
$$D(12) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ for } [31]$$
$$D(12) = 1 \text{ for } [4]$$

$$D(23) = -1 \text{ for } [1111]$$
$$D(23) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ for } [211]$$
$$D(23) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \text{ for } [22]$$
$$D(23) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \text{ for } [31]$$
$$D(23) = 1 \text{ for } [4]$$

$$D(34) = -1 \text{ for } [1111]$$

$$D(34) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} \\ 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} \end{pmatrix} \text{ for [211]}$$

$$D(34) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ for [22]}$$

$$D(34) = \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ for [31]}$$

$D(34) = 1$ for [4]

Now we have to find the block form for a general 16×16 representation of S_4. For this we must investigate the character table of S_4. The Character Table for D_8 is given by

Representation	()	(12)(34)	(12)	(1234)	(123)	
Trivial Representation [4]	1	1	1	1	1	α
Sign Representation [1111]	1	1	-1	-1	1	β
Degree 2 Representation [22]	2	2	0	0	-1	γ
Degree 3 (Standard) Representation [31]	3	-1	1	-1	0	δ
Degree 3 Standard $\otimes$ Sign Representation [211]	3	-1	-1	1	0	ε

For the 16×16 representation, the trace is 16 for (), 4 for (12)(34), 8 for (12), 2 for (1234) and 4 for (123). We can now solve for the number of irreps of each kind in the block form of the permutation matrices.

$$\alpha + \beta + 2\gamma + 3\delta + 3\varepsilon = 16 \tag{4.64}$$

$$\alpha + \beta + 2\gamma - \delta - \varepsilon = 4 \tag{4.65}$$

$$\alpha - \beta + \delta - \varepsilon = 8 \tag{4.66}$$

$$\alpha - \beta - \delta + \varepsilon = 2 \tag{4.67}$$

$$\alpha + \beta - \gamma = 4 \tag{4.68}$$

Solving these equations, we have

$$\varepsilon = 0, \delta = 3, \alpha = 5, \beta = 0, \gamma = 1 \tag{4.69}$$

Table 4.1 : States, Transformations and Entanglement Families for Four-Qubit States

State	Transformations	Family
$\|1\rangle$	$\sigma_x^{\otimes 2} \otimes I_{2\times 2}^{\otimes 2}$ and $I_{2\times 2}^{\otimes 3} \otimes i\frac{\sqrt{3}}{2}\begin{pmatrix} -\frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix}$	L_{ab_3}
$\|2\rangle$	-	ABC-D seperable
$\|3\rangle$	-	ABC-D seperable
$\|4\rangle$	$I_{2\times 2}^{\otimes 3} \otimes \sigma_z$ with $a=\frac{1}{\sqrt{6}}, b=\sqrt{\frac{2}{3}}, c=0, d=\frac{1}{\sqrt{6}}$	G_{abcd}
$\|5\rangle$	$\sigma_z \otimes I_{2\times 2}^{\otimes 3}$ with $a=\frac{1}{2}, b=-\frac{1}{2}, c=-\frac{1}{2}, d=\frac{3}{2}$	G_{abcd}
$\|6\rangle$	$I_{2\times 2} \otimes \sigma_z \otimes I_{2\times 2}^{\otimes 2}$ with $a=\frac{1}{2}, b=\frac{1}{2}, c=\frac{1}{2}, d=-\frac{1}{2}$	G_{abcd}
$\|7\rangle$	$I_{2\times 2}^{\otimes 2} \otimes \sigma_x^{\otimes 2}$ and $I_{2\times 2}^{\otimes 3} \otimes i\frac{\sqrt{3}}{2}\begin{pmatrix} 1 & 0 \\ 0 & -\frac{1}{3} \end{pmatrix}$	L_{ab_3}
$\|8\rangle$	-	ABC-D seperable
$\|9\rangle$	-	ABC-D seperable
$\|10\rangle$	-	$G_{abcd}(a=\frac{1}{2\sqrt{3}}, b=\frac{3}{2\sqrt{3}}, c=-\frac{1}{2\sqrt{3}}, d=-\frac{1}{2\sqrt{3}})$
$\|11\rangle$	$\sigma_x \otimes I_{2\times 2} \otimes \sigma_x \otimes I_{2\times 2}$ and $I_{2\times 2}^{\otimes 2} \otimes \sigma_z^{\otimes 2}$	$G_{abcd}(a=\frac{1}{2}, b=\frac{1}{2}, c=-\frac{1}{2}, d=\frac{1}{2})$
$\|12\rangle$	$I_{2\times 2} \otimes \sigma_x^{\otimes 2} \otimes I_{2\times 2}$	$L_{abc_2}(a=0, b=0, c=0)$
$\|13\rangle$	$I_{2\times 2}^{\otimes 2} \otimes \sigma_x^{\otimes 2}$	$L_{ab_3}(a=0, b=0)$
$\|14\rangle$	$\sigma_x^{\otimes 2} \otimes I_{2\times 2}^{\otimes 2}$	$G_{abcd}(a=\frac{1}{2}, b=1, c=0, d=\frac{1}{2})$
$\|15\rangle$	$\sigma_x^{\otimes 2} \otimes I_{2\times 2}^{\otimes 2}$	$L_{ab_3}(a=0, b=0)$
$\|16\rangle$	$\sigma_x \otimes I_{2\times 2}^{\otimes 2} \otimes \sigma_x$	$L_{abc_2}(a=0, b=0, c=0)$

The symmetric group S_4 for our system has the orthogonal vectors as given in Appendix 1, which correspond to the relevant irreps for the four-qubit case.

As per Verstraete et al [293], a four qubit state can be entangled in nine different ways:

$$G_{abcd} = \frac{a+d}{2}(|0000\rangle + |1111\rangle) + \frac{a-d}{2}(|0011\rangle + |1100\rangle) + \frac{b+c}{2}(|0101\rangle + |1010\rangle) + \frac{b-c}{2}(|0110\rangle + |1001\rangle)$$

$$L_{abc_2} = \frac{a+b}{2}(|0000\rangle + |1111\rangle) + \frac{a-b}{2}(|0011\rangle + |1100\rangle) + c(|0101\rangle + |1010\rangle) + |0110\rangle$$

$$L_{a_2b_2} = a(|0000\rangle + |1111\rangle) + b(|0101\rangle + |1010\rangle) + |0110\rangle + |0011\rangle$$

$$L_{ab_3} = a(|0000\rangle + |1111\rangle) + \frac{a+b}{2}(|0101\rangle + |1010\rangle) + \frac{a-b}{2}(|0110\rangle + |1001\rangle) + \frac{i}{\sqrt{2}}(|0001\rangle + |0010\rangle + |0111\rangle + |1011\rangle)$$

$$L_{a_4} = a(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) + (i|0001\rangle + |0110\rangle - i|1011\rangle)$$

$$L_{a_2 0_{3\oplus 1}} = a(|0000\rangle + |1111\rangle) + (|0011\rangle + |0101\rangle + |0110\rangle)$$

$$L_{0_{5\oplus 3}} = |0000\rangle + |0101\rangle + |1000\rangle + |1110\rangle$$

$$L_{0_{7\oplus 1}} = |0000\rangle + |1011\rangle + |1101\rangle + |1110\rangle$$

$$L_{0_{3\oplus 1}0_{3\oplus 1}} = |0000\rangle + |0111\rangle$$

The states obtained for our system can be put into the various families of states with certain transformations as in Table 4.1.

The families $\{|1\rangle, |2\rangle, |3\rangle\}$, $\{|4\rangle, |5\rangle, |6\rangle\}$, $\{|7\rangle, |8\rangle, |9\rangle\}$, $\{|10\rangle, |11\rangle\}$, $\{|12\rangle\}$, $\{|13\rangle\}$, $\{|14\rangle\}$, $\{|15\rangle\}$ and $\{|16\rangle\}$ are the vectors that are associated to the different irreps for the group. These subsets comprise families of four-qubit states. The first and third families have a vanishing tangle while the second and fourth have a tangle of 1.

4.2.3 Five-Qubit Quantum Computer

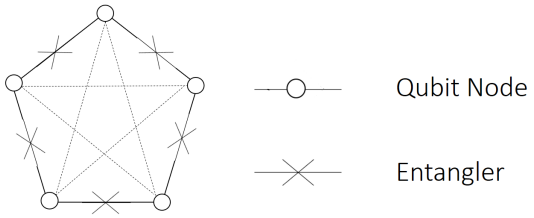


Fig. 4.2 Five-Qubit Quantum Computer

For the S_5 group, we have For the S_5 group, we have

$f[\mu] = 1$ for the partition [5]
$f[\mu] = 4$ for the partition [41]
$f[\mu] = 4$ for the partition [2111]
$f[\mu] = 6$ for the partition [311]
$f[\mu] = 5$ for the partition [32]
$f[\mu] = 5$ for the partition [221]
$f[\mu] = 1$ for the partition [11111]

Let us take the following basis vectors:

$\hat{e}^{[11111]}_{12345}$ for the partition [11111]
$\hat{e}^{[211]}_{1123}$, $\hat{e}^{[211]}_{1213}$ and $\hat{e}^{[211]}_{1231}$ for the partition [211]
$\hat{e}^{[22]}_{1122}$ and $\hat{e}^{[22]}_{1212}$ for the partition [22]
$\hat{e}^{[31]}_{1112}$, $\hat{e}^{[31]}_{1121}$ and $\hat{e}^{[31]}_{1211}$ for the partition [31]
$\hat{e}^{[4]}_{1111}$ for the partition [4]

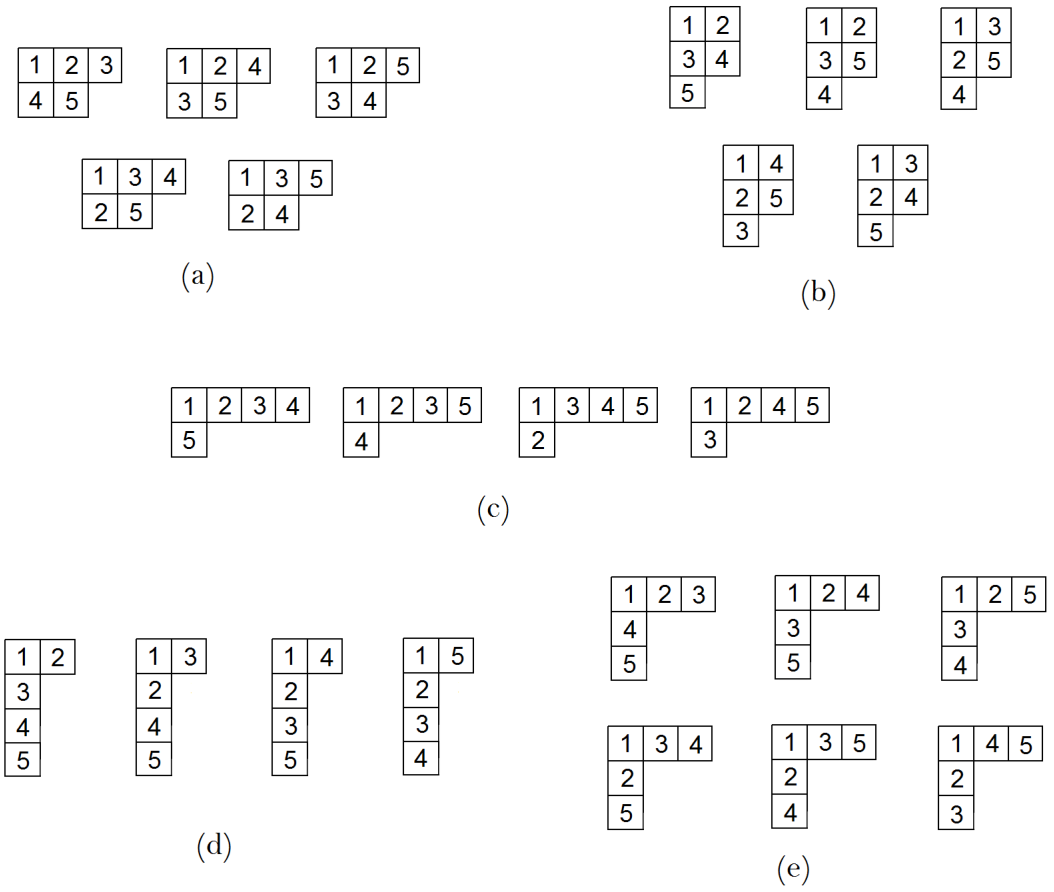


Fig. 4.3 Young Tableau of the Symmetric Group S_5 for (a) Partition [32], (b) Partition [221], (c) Partition [41], (d) Partition [2111] and (e) Partition [311]

Now we have to find the block form for a general 32×32 representation of S_5. For this we must investigate the character table of S_5.

For the 32×32 representation, the trace is 32 for $\{\}$

We can now solve for the number of irreps of each kind in the block form of the permutation matrices.

$$\alpha + \beta + 4\gamma + 4\delta + 5\varepsilon + 5\nu + 6\sigma = 32 \tag{4.70}$$

$$\alpha - \beta + 2\gamma - 2\delta + \varepsilon - \nu = 16 \tag{4.71}$$

$$\alpha + \beta + \varepsilon + \nu - 2\sigma = 8 \tag{4.72}$$

Representation	()	(12)	(12)(34)	(123)	(123)(45)	(12345)	(1234)	
Trivial	1	1	1	1	1	1	1	α
Sign	1	-1	1	1	-1	1	-1	β
Standard	4	2	0	1	-1	-1	0	γ
Sign $\times$ Standard	4	-2	0	1	1	-1	0	δ
5 $\times$ 5 Irrep	5	1	1	-1	1	0	-1	ε
5 $\times$ 5 Irrep	5	-1	1	-1	-1	0	1	ν
Exterior Square of Standard	6	0	-2	0	0	1	0	σ

Table 4.2 Character Table for the Symmetric Group S_5

$$\alpha+\beta+\gamma+\delta-\varepsilon-\nu=8 \tag{4.73}$$

$$\alpha-\beta-\gamma+\delta+\varepsilon-\nu=4 \tag{4.74}$$

$$\alpha+\beta-\gamma-\delta+\sigma=2 \tag{4.75}$$

$$\alpha-\beta-\varepsilon+\nu=4 \tag{4.76}$$

Solving these equations, we have

$$\alpha=6,\beta=0,\gamma=4,\delta=0,\varepsilon=2,\nu=0,\sigma=0 \tag{4.77}$$

The Invariant Subspace Vectors for S_5:

The symmetric group S_5 for our system has the orthogonal vectors that emerge from the block form, as given in the Appendix 1. We now analyze which are the various seperable and entangled states that can be formed of the linear combination of such states.

4.2.4 Six-Qubit Quantum Computer

The Character Table for the group S_6 is given by the Table 4.3. In the table, S.E.P.St. means Second Exterior Power of Standard and T.E.P.St. means Third Exterior Power of Standard.

The character value of each cycle type is as follows:

Cycle {}: 64
Cycle {(12)}: 32

Cycle $\{(123456)\}$: 2
Cycle $\{(12345)\}$: 4
Cycle $\{(123)\}$: 16
Cycle $\{(1234)\}$: 8
Cycle $\{(123)(45)\}$: 8
Cycle $\{(12)(34)\}$: 16
Cycle $\{(12)(34)(56)\}$: 8
Cycle $\{(123)(456)\}$: 4
Cycle $\{(1234)(56)\}$: 4

The relevant equations to be solved to find the relevant blocks in the block form are as follows:

$$\alpha+\beta+5\gamma+5\delta+5\nu+5\mu+10\varepsilon+10\sigma+9\kappa+9\zeta+10\tau=64 \tag{4.78}$$

$$\alpha-\beta+3\gamma-3\delta-\nu+\mu+2\varepsilon-2\sigma-3\kappa+3\zeta=32 \tag{4.79}$$

$$\alpha-\beta-\gamma+\delta+3\nu-3\mu-2\varepsilon+2\sigma-3\kappa+3\zeta=8 \tag{4.80}$$

$$\alpha+\beta+2\gamma+2\delta-\nu-\mu+\varepsilon+\sigma-2\tau=16 \tag{4.81}$$

$$\alpha+\beta-\gamma-\delta+2\nu+2\mu+\varepsilon+\sigma-2\tau=4 \tag{4.82}$$

$$\alpha+\beta+\gamma+\delta+\nu+\mu-2\varepsilon-2\sigma+\kappa+\zeta=16 \tag{4.83}$$

$$\alpha-\beta+\gamma-\delta+\nu-\mu+\kappa-\zeta=8 \tag{4.84}$$

$$\alpha+\beta-\gamma-\delta-\nu-\mu+\kappa+\zeta=4 \tag{4.85}$$

$$\alpha-\beta-\nu+\mu-\varepsilon+\sigma=8 \tag{4.86}$$

$$\alpha-\beta-\gamma+\delta+\varepsilon-\sigma=2 \tag{4.87}$$

$$\alpha+\beta-\kappa-\zeta+\tau=4 \tag{4.88}$$

Solving for the variables, we find

$$\alpha=7 \tag{4.89}$$

$$\gamma=5 \tag{4.90}$$

$$\mu=1 \tag{4.91}$$

$$\zeta=3 \tag{4.92}$$

Rep.	()	(12)	(12)(34)(56)	(123)	(123)(456)	(12)(34)	(1234)	(1234)(56)	(123)(45)	(123456)	(12345)	
Trivial	1	1	1	1	1	1	1	1	1	1	1	α
Sign	1	-1	-1	1	1	1	-1	1	-1	-1	1	β
Standard	5	3	-1	2	-1	1	1	-1	0	-1	0	γ
St. $\times$ Sign	5	-3	1	2	-1	1	-1	-1	0	1	0	δ
5D Irrep (2)	5	-1	3	-1	2	1	1	-1	-1	0	0	ν
5D Irrep (3)	5	1	-3	-1	2	1	-1	-1	1	0	0	μ
S.E.P.St.	10	2	-2	1	1	-2	0	0	-1	1	0	ε
T.E.P.St.	10	-2	2	1	1	-2	0	0	1	-1	0	σ
Rep. (9)	9	-3	-3	0	0	1	1	1	0	0	-1	κ
Rep. (10)	9	3	3	0	0	1	-1	1	0	0	-1	ζ
Rep. (11)	16	0	0	-2	-2	0	0	0	0	0	1	τ
	64	**32**	**8**	**16**	**4**	**16**	**8**	**4**	**8**	**2**	**4**	

Table 4.3 Character Table for the Symmetric Group S_6

$$\beta, \delta, \nu, \varepsilon, \sigma, \kappa, \tau = 0 \tag{4.93}$$

This means we have three nine-dimensional blocks, six five-dimensional block and seven one-dimensional blocks in the block form of the entangler combinations.

For the S_6 group, we have the partitions shown in Figures 4.8 - 4.18.

For the S_6 group, we have

$f[\mu]$ = 1 for the partition [6]
$f[\mu]$ = 5 for the partition [51]
$f[\mu]$ = 10 for the partition [3111]
$f[\mu]$ = 10 for the partition [411]
$f[\mu]$ = 9 for the partition [42]
$f[\mu]$ = 16 for the partition [321]
$f[\mu]$ = 5 for the partition [33]
$f[\mu]$ = 5 for the partition [222]
$f[\mu]$ = 9 for the partition [2211]
$f[\mu]$ = 5 for the partition [21111]
$f[\mu]$ = 1 for the partition [111111]

Let us take the following basis vectors:

$\hat{e}^{[111111]}_{123456}$ for the partition [111111]

$\hat{e}^{[33]}_{111222}$, $\hat{e}^{[33]}_{121212}$, $\hat{e}^{[33]}_{112122}$, $\hat{e}^{[33]}_{121122}$ and $\hat{e}^{[33]}_{112212}$ for the partition [33]

$\hat{e}^{[51]}_{121111}$, $\hat{e}^{[51]}_{11211}$, $\hat{e}^{[51]}_{111211}$, $\hat{e}^{[51]}_{111121}$ and $\hat{e}^{[51]}_{111112}$ for the partition [51]

$\hat{e}^{[222]}_{112233}$, $\hat{e}^{[222]}_{121233}$, $\hat{e}^{[222]}_{123123}$, $\hat{e}^{[222]}_{121323}$ and $\hat{e}^{[222]}_{112323}$ for the partition [222]

$\hat{e}^{[21111]}_{112345}$, $\hat{e}^{[21111]}_{121345}$, $\hat{e}^{[21111]}_{123145}$, $\hat{e}^{[21111]}_{123415}$ and $\hat{e}^{[21111]}_{123451}$for the partition [21111]

$\hat{e}^{[42]}_{111122}$, $\hat{e}^{[42]}_{111212}$, $\hat{e}^{[42]}_{111221}$, $\hat{e}^{[42]}_{112112}$, $\hat{e}^{[42]}_{112121}$, $\hat{e}^{[42]}_{121112}$, $\hat{e}^{[42]}_{121121}$, $\hat{e}^{[42]}_{121211}$ and $\hat{e}^{[42]}_{112211}$ for the partition [42]

$\hat{e}^{[2211]}_{112234}$, $\hat{e}^{[2211]}_{123412}$, $\hat{e}^{[2211]}_{121234}$, $\hat{e}^{[2211]}_{121342}$, $\hat{e}^{[2211]}_{121324}$, $\hat{e}^{[2211]}_{123142}$, $\hat{e}^{[2211]}_{123124}$, $\hat{e}^{[2211]}_{112342}$ and $\hat{e}^{[2211]}_{112324}$ for the partition [2211]

$\hat{e}^{[321]}_{111223}$, $\hat{e}^{[321]}_{112123}$, $\hat{e}^{[321]}_{112213}$, $\hat{e}^{[321]}_{112231}$, $\hat{e}^{[321]}_{121123}$, $\hat{e}^{[321]}_{121213}$, $\hat{e}^{[321]}_{123112}$, $\hat{e}^{[321]}_{111232}$, $\hat{e}^{[321]}_{112312}$, $\hat{e}^{[321]}_{112321}$, $\hat{e}^{[321]}_{121123}$, $\hat{e}^{[321]}_{123121}$, $\hat{e}^{[321]}_{121312}$, $\hat{e}^{[321]}_{121321}$, $\hat{e}^{[321]}_{121132}$ and $\hat{e}^{[321]}_{121231}$ for the partition [321]

$\hat{e}^{[3111]}_{111234}$, $\hat{e}^{[3111]}_{112134}$, $\hat{e}^{[3111]}_{112314}$, $\hat{e}^{[3111]}_{112341}$, $\hat{e}^{[3111]}_{121134}$, $\hat{e}^{[3111]}_{121314}$, $\hat{e}^{[3111]}_{121341}$, $\hat{e}^{[3111]}_{123114}$, $\hat{e}^{[3111]}_{123141}$ and $\hat{e}^{[3111]}_{123411}$ for the partition [3111]

$\hat{e}^{[411]}_{111123}$, $\hat{e}^{[411]}_{123111}$, $\hat{e}^{[411]}_{121311}$, $\hat{e}^{[411]}_{121131}$, $\hat{e}^{[411]}_{121113}$, $\hat{e}^{[411]}_{112311}$, $\hat{e}^{[411]}_{112131}$, $\hat{e}^{[411]}_{112113}$, $\hat{e}^{[411]}_{111231}$ and $\hat{e}^{[411]}_{111213}$for the partition [411]

$\hat{e}^{[6]}_{111111}$ for the partition [6]

where

$\hat{e}^{[33]}_{111222} = \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[33]}_{112122} = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[33]}_{112212} = \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$, $\hat{e}^{[33]}_{121122} = \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$, $\hat{e}^{[33]}_{121212} = \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$ for the partition [33]

$\hat{e}^{[51]}_{111112} = \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[51]}_{111121} = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[51]}_{111211} = \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$, $\hat{e}^{[51]}_{112111} = \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$, $\hat{e}^{[51]}_{121111} = \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$ for the partition [51]

$\hat{e}^{[222]}_{112233} = \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[222]}_{112323} = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[222]}_{121233} = \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$, $\hat{e}^{[222]}_{121323} = \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$, $\hat{e}^{[222]}_{123123} = \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$ for the partition [222]

$\hat{e}^{[21111]}_{112345} = \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[21111]}_{121345} = \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[21111]}_{123145} = \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$, $\hat{e}^{[21111]}_{123415} = \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$, $\hat{e}^{[21111]}_{123451} = \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$ for the partition [21111]

$\hat{e}^{[42]}_{111122} = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{111212} = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{111221} = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{112112} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{112121} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{112211} = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{121112} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{121121} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}$, $\hat{e}^{[42]}_{121211} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix}$ for the partition [42]

$\hat{e}^{[2211]}_{112234} = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[2211]}_{112324} = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[2211]}_{112342} = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[2211]}_{121234} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[2211]}_{121324} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}$, $\hat{e}^{[2211]}_{121342} = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$,

$$\begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}, \hat{e}^{[2211]}_{123124} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}, \hat{e}^{[2211]}_{123142} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix}, \hat{e}^{[2211]}_{123412} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix} \text{ for the partition } [42]$$

$$\hat{e}^{[321]}_{111223} = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} =$$

$$\begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix},$$

$$\hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix}, \hat{e}^{[321]}_{111223} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}$$

for the partition [321]

$$\hat{e}^{[3111]}_{111234} = \begin{pmatrix} 1\\0\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{112134} = \begin{pmatrix} 0\\1\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{112314} = \begin{pmatrix} 0\\0\\1\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{112341} = \begin{pmatrix} 0\\0\\0\\1\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{121134} = \begin{pmatrix} 0\\0\\0\\0\\1\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{121314} =$$

$$\begin{pmatrix} 0\\0\\0\\0\\0\\1\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{121341} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\1\\0\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{123114} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\1\\0\\0 \end{pmatrix}, \hat{e}^{[3111]}_{123141} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\1\\0 \end{pmatrix}, \hat{e}^{[3111]}_{123411} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\0\\1 \end{pmatrix} \text{ for the partition}$$

[3111]

$$\hat{e}^{[411]}_{111123} = \begin{pmatrix} 1\\0\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[411]}_{111213} = \begin{pmatrix} 0\\1\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[411]}_{111231} = \begin{pmatrix} 0\\0\\1\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[411]}_{112113} = \begin{pmatrix} 0\\0\\0\\1\\0\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[411]}_{112131} = \begin{pmatrix} 0\\0\\0\\0\\1\\0\\0\\0\\0\\0 \end{pmatrix}, \hat{e}^{[411]}_{112311} =$$

$$\begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}, \hat{e}^{[411]}_{121113} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}, \hat{e}^{[411]}_{121131} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}, \hat{e}^{[411]}_{121311} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix}, \hat{e}^{[411]}_{123111} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix} \text{ for the partition } [411]$$

For our system, the relevant blocks are of the dimensions one, five and nine. We can find the matrix representation for the generator transpositions (12).

$$D^{[111111]}(12) = -1$$
$$D^{[6]}(12) = 1$$

Since we need one-dimensional irreps with character value 1, the relevant irrep is that for the [6] partition.

$$D^{[33]}(12) = \begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&-1&0\\0&0&0&0&-1\end{pmatrix}$$

$$D^{[51]}(12) = \begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&-1\end{pmatrix}$$

$$D^{[222]}(12) = \begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&-1&0&0\\0&0&0&-1&0\\0&0&0&0&-1\end{pmatrix}$$

$$D^{[222]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

We see that the trace of these matrices gives us the relevant partition corresponding to our character table categories. Since we need five five-dimensional irreps with trace 3 and one five-dimensional irrep with trace 1, the relevant partitions are [51] and [33] respectively.

$$D^{[42]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[2211]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Since the nine-dimensional irrep we need has a character value of +3, the relevant partition is [42].

We now find the elements D(23), D(34), D(45) and D(56) for the relevant partitions.

We begin with [6]:

$$D^{[6]}(12) = 1$$
$$D^{[6]}(23) = 1$$

$$D^{[6]}(34) = 1$$
$$D^{[6]}(45) = 1$$
$$D^{[6]}(56) = 1$$

We consider [33]:

$$D^{[33]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[33]}(23) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & -\frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

$$D^{[33]}(34) = \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 & 0 & 0 \\ \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[33]}(45) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$D^{[33]}(56) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

We consider [51]:

$$D^{[51]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[51]}(23) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$D^{[51]}(34) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ 0 & 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D^{[51]}(45) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{4} & \frac{\sqrt{15}}{4} & 0 & 0 \\ 0 & \frac{\sqrt{15}}{4} & \frac{1}{4} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D^{[51]}(56) = \begin{pmatrix} -\frac{1}{5} & \frac{\sqrt{24}}{5} & 0 & 0 & 0 \\ \frac{\sqrt{24}}{5} & \frac{1}{5} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We consider [42]:

$$D^{[42]}(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[42]}(23) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

$$D^{[42]}(34) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & 0 & \frac{\sqrt{8}}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{3} & 0 & \frac{\sqrt{8}}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{8}}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{\sqrt{8}}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$D^{[42]}(45) = \begin{pmatrix} -\frac{1}{4} & \frac{\sqrt{15}}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{\sqrt{15}}{4} & \frac{1}{4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$D^{[42]}(56) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Now, the permutation $D(123456) = D(12)D(13)D(14)D(15)D(16)$. We can find these constituent two-element forms for the relevant partitions:

Now,

$$D^{[5]}(13) = D^{[5]}(12)D^{[5]}(23)D^{[5]}(12)$$
$$D^{[5]}(14) = D^{[5]}(13)D^{[5]}(34)D^{[5]}(13)$$
$$D^{[5]}(15) = D^{[5]}(14))D^{[5]}(45)D^{[5]}(14)$$
$$D^{[5]}(16) = D^{[5]}(15))D^{[5]}(56)D^{[5]}(15)$$

Invariant Subspace Vectors for S_6:

The symmetric group S_6 for our system has the following orthogonal vectors that emerge from the block form, as given in Appendix 1.

4.2.5 Higher Multiqubit States

We find the vector states for the higher multiqubit states as well, based on the *Nullspace Approach*, mentioned in Chapter 2. The cases to the n-qubit case can be generalized using the application of Ross's breaking of the Hilbert Space based on the symmetry under parity for the $SWAP^{1/n}$ gates.

The circuit-based model of quantum computing may be the most popular at the moment, but it has sources of error (relating to gate operations, noise and leakage errors) that do not make it the most reliable. The encoded quantum computation models are one step further towards more resilience and robustness against these errors due to the symmetry properties of the states. However, the formalism that is most highly regarded for this aspect is the cluster-state model of quantum computation. Formulated by Raussendorf [163], this model relies on single qubit measurements and hence is also called the measurement-based model of quantum computing. In the next section, we look at how the exchange interaction and $SWAP^{1/n}$ gates can be used to realize cluster-state quantum computing.

4.3 Cluster State Quantum Computation

Cluster states can be generated using $SWAP^{1/n}$ gates. Tanamoto et al [294] showed that this could be done for $\sqrt{SWAP}$ and *iSWAP* gates. We get to similar results independently, using numerical and analytical methods, and go on to define a 'dynamical' model of cluster state quantum computation.

Cluster states are pure quantum states [163] defined on two-level systems arranged on a cluster-lattice. This cluster is a *connected* subset of a simple cubic lattice Z_d in d$\geq$1 dimensions.

The cluster states $|\phi_{cluster}\rangle$ obey the set of eigenvalue equations

$$M^{(a)}|\phi_{cluster_m}\rangle = (-1)^{m_a}|\phi_{cluster}\rangle \tag{4.94}$$

with the correlation operators

$$M^{(a)} = \sigma_x^{(a)} \otimes \sigma_z^{(b)} \tag{4.95}$$

Here, b $\in$ nbgh(a), the set of all neighboring lattice sites of a, and $\{cluster_m\}$:=$\{m_a \in \{0,1\}|$ a $\in$ Cluster$\}$ is a set of binary parameters which specify the cluster state.

4.3.1 $SWAP^{1/n}$-based Model of Cluster State Quantum Computation

One of the fundamental differences that a $SWAP^{1/n}$ model has with the usual CPHASE-based Raussendorf model of cluster quantum computation is that neighboring interactions generally do not commute: $[H_{i,i-1}, H_{i,i+1}] \neq 0$, as discussed previously, unlike the CPHASE gate:

$$U_{CPHASE} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{4.96}$$

which does. As a result, we have, for the evolution operator, $e^{-iHt} \neq \prod_{ij} e^{-iH_{i,j}t}$. For creating cluster states using such non-commutative interactions, pairwise bonding between the qubits is needed. So, for an n-dimensional qubit array, cluster states can only be generated in $2n$ steps: firstly, two-qubit cluster states are constructed by performing exchange interactions between pairs of nearest neighbor qubits. These qubit pairs are thereafter connected to each other using another set of such operations, and a one-dimensional chain (cluster state) is created. Afterwards, these chains can be connected in various ways to give more complex structures, such as two-dimensional clusters and ladder clusters. A point to remember here is that to reach the standard cluster-state form, as formulated by Raussendorf, single qubit rotation gates are required. Even though it is possible to have a modified $U_\phi U_\psi$-based cluster state model, where U_ϕ and U_ψ are measurement gates along an arbitrary angle, it is more convenient to change all bases to a standard form of two-qubit cluster states:

$$|\psi\rangle_C^2 = (|0\rangle_1|-\rangle_2 + |1\rangle_1|+\rangle_2) \tag{4.97}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. This realization can be carried out using a simple sequence of steps.

Algorithm

Part I: Generating the two-qubit cluster states

1. We start with a state

$$|\psi_{in}\rangle = |+\rangle_1|-\rangle_2 \tag{4.98}$$

2. We apply a general $SWAP^{1/n}$:

$$U_{SWAP^{1/n}}|\psi_{in}\rangle \rightarrow |0\rangle(|0\rangle - e^{i\pi/n}|1\rangle) + e^{i\pi - i\pi/n}|1\rangle(|0\rangle + e^{i\pi/n}|1\rangle) \tag{4.99}$$

3. We use the following composite operator:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{-i\pi/n} & 0 & 0 \\ 0 & 0 & e^{-i\pi/n} & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{4.100}$$

to obtain the state $|\psi\rangle_C^2$.

Part II: Creating larger cluster states

1. Let us start with the simple case of connecting two qubit-pairs with the states of the cluster states C_{12} and $|+\rangle_3$:

2. We apply the $SWAP^{1/n}$ gate between qubits 2 and 3. This gives the state:

$$|\psi_o\rangle = (|000\rangle + e^{i\pi/n}|001\rangle - e^{i\pi/n}|010\rangle - |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \tag{4.101}$$

3. We then operate with the operator:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{-i\pi/n} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -e^{-i\pi/n} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.102}$$

to obtain the cluster state:

$$|\psi\rangle_C^3 = (|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle) \tag{4.103}$$

This method can be extended for higher numbers of qubits.

As can be seen, a general $SWAP^{1/n}$ has the problem of the need for the use of a non-local operator at the end to 'clean up' the state to get the cluster state finally. This is, however, not the case for *iSWAP*:

$$U_{iSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.104}$$

This gate can be realized by taking $J_x = J_y = J, J_z = 0$ and $t = \frac{\pi}{8J}$ in the exchange interaction $H = Js_1.s_2$. Let us see how this affects the creation of cluster states for quantum computation.

$$|+\rangle_1|-\rangle_2 \xrightarrow{iSWAP\times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}} |0\rangle|-\rangle + |1\rangle|+\rangle \tag{4.105}$$

For three qubits,

$$(|0\rangle|-\rangle + |1\rangle|+\rangle)|+\rangle_3 \xrightarrow{I\otimes iSWAP} |+\rangle_1|0\rangle_3(|0\rangle + i|1\rangle)_2 - i|-\rangle_1|1\rangle_3(|0\rangle - i|1\rangle)_2 \tag{4.106}$$

Applying a Phase-Shift Gate $R_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ on the third qubit, we get

$$|\psi\rangle_C^3 = (|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle) \tag{4.107}$$

If we take two cluster pairs C_{12} and C_{34}: $|\psi\rangle_{C_{12}}^2 = (|0\rangle|-\rangle + |1\rangle|+\rangle)_{12}$ and $|\psi\rangle_{C_{34}}^2 = (|0\rangle|-\rangle + |1\rangle|+\rangle)_{34}$ and apply a $SWAP^{1/n}$ gate on qubits 2 and 3, we have

$$|\psi\rangle_{C_{12}}^2|\psi\rangle_{C_{34}}^2 \xrightarrow{I_{2\times2}\otimes iSWAP_{23}\otimes I_{2\times2}} (|0\rangle|0\rangle|+\rangle|-\rangle + i|0\rangle|1\rangle|-\rangle|+\rangle + |1\rangle|0\rangle|-\rangle|-\rangle + i|1\rangle|1\rangle|+\rangle|+\rangle) \tag{4.108}$$

where $I_{2\times2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This shows a very interesting property: the resultant cluster state is 'twisted' and there seems to be a C_{1324} cluster. This trend is found by us to continue for higher numbers of qubits too.

4.3.2 Dynamical Cluster State Quantum Computation Model

The exchange interaction, which is used to realize $SWAP^{1/n}$ gates, often takes place between moving qubits, such as electrons trapped in a surface acoustic wave. For such qubits, it is only natural to define a dynamical model of cluster state quantum computation.

The basic element of the dynamical cluster state model, much as in the static cluster state quantum computation, is the lattice of points that represent the physical qubits (Figure 4.7), moving in a certain direction. We define the conventional direction of motion for this lattice to be towards the right. These can be realized with fermions or bosons, depending on the kind of physical system being considered. For the cases discussed already, for the static cluster state quantum computation, these could be phonons, photons or ions, among other possibilities. In the figure, one can see two kinds of basis elements, with the second (Figure 4.20 (b)) being just a selectively time-delayed version of the first orientation (a). Such time-delayed basis are useful for creating highly entangled cluster states, as worked on by *Yokoyama et al* [60]. These qubits are independently initialized to a certain input basis set. This initialization is intricately linked to the kind of entangling operation and stage one has for the setup. Some of the possible initialization basis and their corresponding entanglers are mentioned below:

Entangler	**Input States**
CPHASE	$\|\pm\rangle$
Root-of-SWAP	Alternating $\|0/1\rangle$
CNOT	$\|0/1\rangle$ and $\|\pm\rangle$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

The entangler is the element in the circuit which facilitates generation of the entanglement used in cluster state quantum computation. For example, a combination of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|0\rangle$ gives us the bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$when the former is used as the control and the latter as the target qubit in a CNOT operation. In the case of the Root-of-SWAP entangler, one can use an antiferromagnetic configuration with alternating spins to realize the initialization discussed in the table above. A similar configuration can also be used for a general $SWAP^{1/n}$ entangler.

For the dynamical cluster state model, one can have an interesting characteristic feature of

the architecture, known as *state hopping*, as shown in Figure 4.21. One can introduce a state anywhere on the cluster-lattice and displace it in any direction in the rectangular structure using σ_x and σ_z measurements. σ_z measurements essentially remove a qubit from the cluster while σ_x measurements provide a 'wire', a conduit, for the passage of information from an arbitrary state to another location. Upon measuring the original location in the σ_x basis, one can receive the original state in the new location (up to corrective operations). Measurements of observables σ_z effectively remove the respective lattice qubit(s) from the cluster-state. Such a measurement projects the cluster state ϕ_C into the tensor product $|A\rangle \otimes |\psi\rangle$. Here, $|A\rangle$ is a product state in the computational basis, and $|\psi\rangle$ the state of the remaining unmeasured qubits. In our model, to implement measurements, as in the static cluster state quantum computation model, we have the measuring elements to the right of the entanglers. The right-most end of the lattice is measured first. As a result, the information flow is from the right to left. Hence, initializing an input register, as shown in Figure 4.21, or even the basis states for a particular gate or algorithmic operation on the right-most column of the physical qubits, helps to obtain the result further into the cluster, using a combination of projective measurements and state-hopping. Now that we have laid the fundamental theoretical ground for further discussion, we would like to introduce the idea of circuit segment concatenation. In this model, we consider three primary segments of the circuit: initiation of physical qubits in the *Input* (I) stage, generation of entanglement in the *Entanglement-Generation* (E) stage and finally the *Read-out* (R) stage.

The Readout (R) stage can be made of time-sequenced array of read-out elements, as shown below, in Figure 4.24, wherein the yellow elements are the active readout elements.

4.3.3 Deutsch Josza Algorithm

One of the most famous algorithms in the history of quantum information processing has been the Deutsch Josza algorithm. In this section, I will be describing a new way to do this using a particular cluster state generated by our physics system:

$$|\psi\rangle = \frac{1}{2}(|0101\rangle + |0011\rangle + |1100\rangle - |1010\rangle) \tag{4.109}$$

The Deutsch Jozsa algorithm is an algorithm to distinguish between two classes of two-bit binary functions: $f : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}$. The two classes are the constant functions, in which all input values get mapped to the same output value (either 0 or 1), and the balanced functions in which exactly half the inputs get mapped to 0, while the other half get mapped to 1.

In my implementation scheme, measurements on each qubit has a definite outcome for the algorithm. Qubits 1 and 3 are used as the query and ancillary qubits $|x\rangle|y\rangle$ for $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$. Qubit 2 and the steps associated with it act as the oracle qubit. Qubit 4 helps in projecting Qubit 3 to the final state that shall implement the algorithm. One has two different categories of this implementation: one for balanced functions and the other for the constant function.

Measuring qubits in $\{|+\rangle,|-\rangle\}_1, \{|+\rangle,|-\rangle\}_2, \{|0\rangle,|1\rangle\}_3, \{|0\rangle,|1\rangle\}_4$ (where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$), we have the state

$$\begin{aligned}|\psi_{DJ_C}\rangle = &|+\rangle|+\rangle|1\rangle|1\rangle + |-\rangle|+\rangle|1\rangle|1\rangle + |+\rangle|+\rangle|0\rangle|1\rangle + |-\rangle|+\rangle|0\rangle|1\rangle \\ &- |+\rangle|+\rangle|1\rangle|0\rangle + |-\rangle|+\rangle|1\rangle|0\rangle + |+\rangle|+\rangle|0\rangle|0\rangle - |-\rangle|+\rangle|0\rangle|0\rangle + |+\rangle|-\rangle|1\rangle|1\rangle \\ &+ |-\rangle|-\rangle|1\rangle|1\rangle - |+\rangle|-\rangle|0\rangle|1\rangle - |-\rangle|-\rangle|0\rangle|1\rangle - |+\rangle|-\rangle|1\rangle|0\rangle + |-\rangle|-\rangle|1\rangle|0\rangle \\ &- |+\rangle|-\rangle|0\rangle|0\rangle + |-\rangle|-\rangle|0\rangle|0\rangle \end{aligned} \quad (4.110)$$

Based on the measurement of the disentangler - Qubit 2, and the projective measurement of Qubit 4, one finds that irrespective of the input $|x\rangle$ qubit, the output is the same. This is the implementation of the *constant function*.

Measuring qubits in $\{|i+\rangle,|i-\rangle\}_1, \{|i+\rangle,|i-\rangle\}_2, \{|+\rangle,|-\rangle\}_3, \{|+\rangle,|-\rangle\}_4$ (where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|i\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ gives us the output

$$\begin{aligned}&\frac{i}{2\sqrt{2}}(|i-\rangle|i-\rangle|+\rangle|+\rangle + |i-\rangle|i-\rangle|-\rangle|-\rangle + |i-\rangle|i+\rangle|-\rangle|+\rangle + |i-\rangle|i+\rangle|+\rangle|-\rangle \\ &\quad + (-|i+\rangle|i+\rangle|+\rangle|+\rangle - |i+\rangle|i+\rangle|-\rangle|-\rangle - |i+\rangle|i-\rangle|-\rangle|+\rangle - |i+\rangle|i-\rangle|+\rangle|-\rangle))_{1234}\end{aligned} \quad (4.111)$$

For the Qubit $2-4$ combinations, one gets a balanced function output.

4.4 Indefinite Causal Order and Functional Quantum Computing

In classical computing and programming, we have object-oriented and functional models of information processing. While the former deals with the manipulation of elements and

resources using operators, the latter relates to the changing of operators to realize a certain computation. Classical functional computing relies on what is known as λ-calculus [295], which treats functions and data as the same type of objects. It allows for the computation of both functions of data as well as functions of functions.

This idea can be extended to the realm of quantum information processing too. The idea of quantum combs has been used for this purpose [296, 297], as have models based on quantum λ calculus [298, 299]. The switch-based model of functional quantum computing [300] is the realization that we are most interested in. In our project, we extended the idea from being a control-qubit-based model to a control-qudit-based model.

The model takes as its inputs a set of N quantum operators $U_0, U_1, ..., U_{N-1}$, a control qudit $|d\rangle_C$ and a register of input qubits. In our model, we consider that each operator is applied just once and we encode the operator in the N-qubit control qudit as follows:

$$|0\rangle_d = |000...0\rangle_d = |1234...(N-1)(N)\rangle_e \tag{4.112}$$

$$|1\rangle_d = |000...1\rangle_d = |1234...(N)(N-1)\rangle_e \tag{4.113}$$

$$|2\rangle_d = |000..10\rangle_d = |1234...(N-1)(N-2)(N)\rangle_e \tag{4.114}$$

...

$$|N!\rangle_d = |111...1\rangle_d = |(N)(N-1)...3421\rangle_e \tag{4.115}$$

The encoding, marked by $|\rangle_e$ shows the sequence of the operators as well. The model coherently orders the quantum operators based on the value of the control-qudit, thereby creating a meta-operator, a superposition of many different sequential orderings of the same set of operators, which is then applied to the input qubit. Let us call this entire operation O_{SWAP} and let us take an illustration of this using the simple example of two operators U_1 and U_2. We will then have the control qudit in the states $|0\rangle_d = |12\rangle_e$ and $|1\rangle_d = |21\rangle_e$, which have the following action on the operators:

$$|0\rangle_d U_1 U_2 = U_1 U_2 \tag{4.116}$$

$$|1\rangle_d U_1 U_2 = U_2 U_1 \tag{4.117}$$

For a control qudit $|c\rangle = \alpha|0\rangle_d + \beta|1\rangle_d$ and an input state $|\psi\rangle$,

$$O_{SWAP}|c\rangle(U_1U_2)|\psi\rangle = \alpha|0\rangle_d + \beta|1\rangle_d(U_1U_2)|\psi\rangle \\ = \alpha|0\rangle_d U_1U_2|\psi\rangle + \beta|1\rangle_d U_2U_1|\psi\rangle \quad (4.118)$$

This is an extremely useful tool for a multi-operator lattice-configuration such as the one we have developed for our model of cluster state quantum computation. Instead of restructuring the gates manually or even using gate-potentials in a synchronized manner, we can simply use the appropriate control-qudit to do the same.

4.5 Qudit-Based Quantum Computation using $SWAP^{1/n}$ Quantum Operator

Quantum gates that are universal for binary quantum logic operations belong to a family of unitary transforms are seen to be described by three parameters, and this arises out of the idea that up to an overall phase factor, any two dimensional unitary matrix can be written as

$$U_2(\lambda,\nu,\phi) = \begin{pmatrix} cos\lambda & -e^{i\nu}sin\lambda \\ e^{i(\phi-\nu)}sin\lambda & e^{i\phi}cos\lambda \end{pmatrix} \quad (4.119)$$

expressed in the basis states $|0\rangle$ and $|1\rangle$. The three parameters are usually taken to be irrational multiples of π and each other. This this allows even a single gate in to generate all single-qubit transforms by repeated application. However, we find it to be more useful to consider these three parameters as arbitrary variables, with U_2 representing a family of gates that can be realized by an appropriate choice of three physical controls. One of the properties of U_2 is that it can transform any known state of a qubit to $|1\rangle$: $\alpha|0\rangle + \beta|1\rangle \xrightarrow{Z_2} |1\rangle$. U_2 also contains the phase gate X_2 that alters the phase of $|1\rangle$ without affecting $|0\rangle$: $|1\rangle \xrightarrow{X_2} e^{i\phi}|1\rangle, |0\rangle \xrightarrow{X_2} |0\rangle$. Using these two transformation properties of U_2, the two-qubit gates that are universal for quantum logic take the form

$$A_2[U_2] = \begin{pmatrix} I_2 & 0 \\ 0 & U_2 \end{pmatrix} \quad (4.120)$$

The family of gates $A_2[U_2]$ is universal for binary quantum logic. A unitary transform on any number of qubits can be simulated by repeated application of these gates on just two qubits at any one given time.

We can generalize this to the multivalued case. We define Z_d as a family of d-dimensional

transforms that maps a known single-qudit state to $|d-1\rangle$: $\alpha_1|0\rangle+\alpha_2|0\rangle+...+\alpha_{d-1}|d-1\rangle \xrightarrow{Z_d} |d-1\rangle$. Similarly, we define the d-dimensional phase gate X_d as a function that does the following: $|d-1\rangle \xrightarrow{X_d} e^{i\phi}|d-1\rangle, |q\rangle \xrightarrow{X_d} |q\rangle, q \neq d-1$. We can now define the multivalued analog of $A_2[U_2]$ as

$$A_2[U_d] = \begin{pmatrix} I_{d^2-d} & 0 \\ 0 & U_d \end{pmatrix} \tag{4.121}$$

For our system, we devise a very simple way to do this. We will present the formalism using a state with Hamming weight 1 for n-qubits. This can be generalized to other states with different Hamming weights. We define the state $|d-1\rangle$ as the n-qubit W-state:

$$|d-1\rangle = |N-1\rangle\frac{1}{\sqrt{N}}(-|00...01\rangle+|00...010\rangle+...+|100...0\rangle) \tag{4.122}$$

Now we define the other states by introducing a relative phase of $e^{i\pi}$in front of each of the superposition states one-by-one, so as to obtain

$$|N-2\rangle = \frac{1}{\sqrt{N}}(|00...01\rangle+|00...010\rangle-|00..0100\rangle+...+|100...0\rangle) \tag{4.123}$$

...

$$|0\rangle = \frac{1}{\sqrt{N}}(|00...01\rangle+|00...010\rangle+...-+|010...00\rangle-|100...0\rangle) \tag{4.124}$$

In this formalism, we will use the property that $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) \xrightarrow{SWAP^{1/n}} \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle), \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \xrightarrow{SWAP^{1/n}} e^{i\pi/n}\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$. A point to note here is that even though we could have constructed N logical qubits, we only constructed $N-1$. This was because the definition of X_d, as we do it below, does not allow the consideration of the state: $\frac{1}{\sqrt{N}}(|00...01\rangle-|00...010\rangle+|00..0100\rangle+...+|100...0\rangle)$ for the properties of X_d to hold true.

We define the Z_d operator as an inverse map, based on the linear combination of vectors considered and

$$X_d = I_2 \otimes I_2 \otimes ... \otimes I_2 \otimes U_{SWAP^{1/n}} \tag{4.125}$$

This allows us to construct the gate $A_2[U_d]$ and therefore do universal qudit quantum computation using our system.

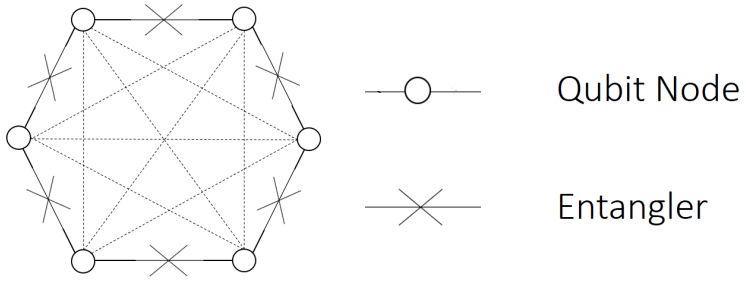


Fig. 4.4 Six-Qubit Quantum Computer

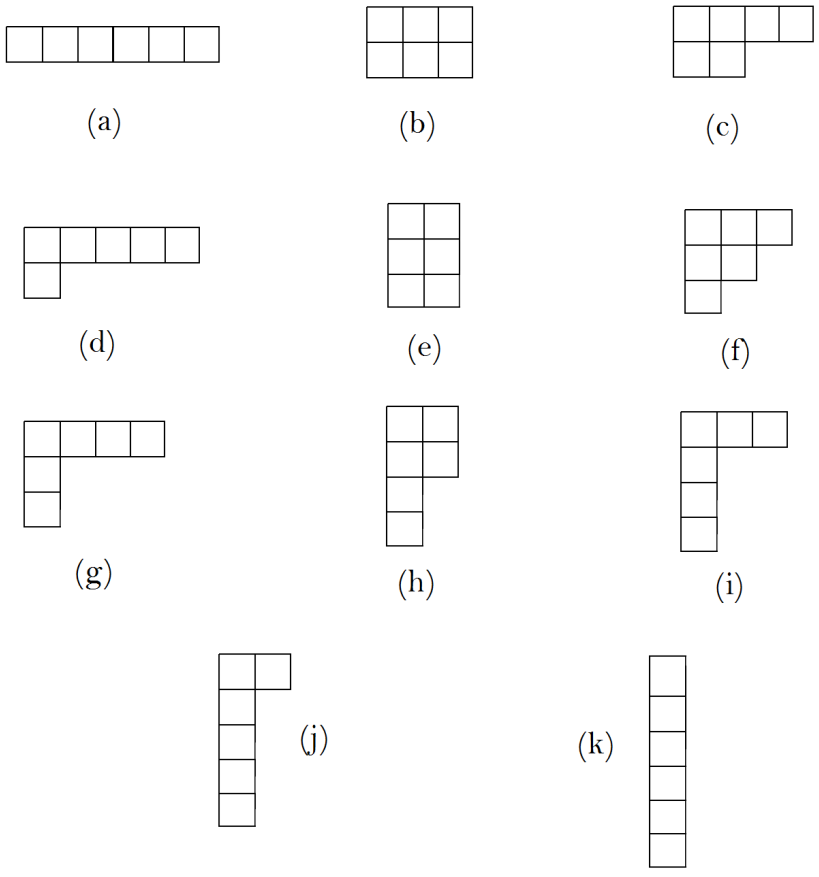


Fig. 4.5 Young's Diagram associated with S_6 Symmetric Group, for (a) Partition [6], (b) Partition [33], (c) Partition [42], (d) Partition [51], (e) Partition [222], (f) Partition [321], (g) Partition [411], (h) Partition [2211], (i) Partition [3111], (j) Partition [21111] and (k) Partition [111111]

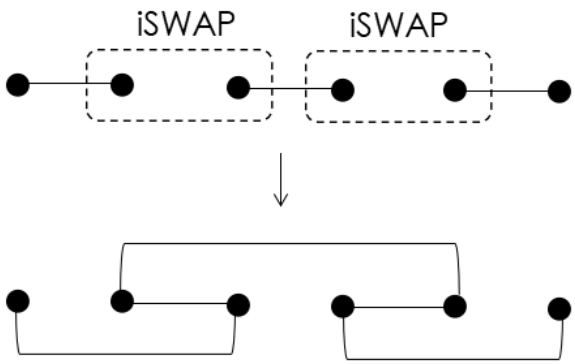


Fig. 4.6 Application of the iSWAP gate between cluster-pairs leads to a 'twisted' resultant cluster state

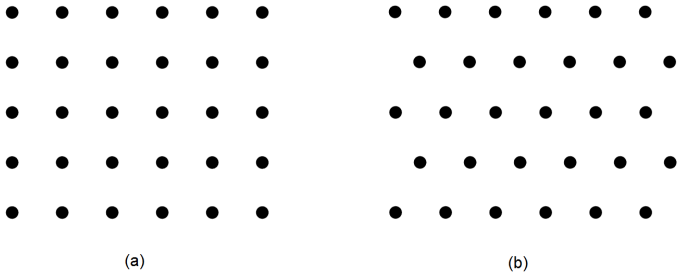


Fig. 4.7 Physical Basis for Dynamical Cluster State Quantum Computation. (b) is the configuration where every even-numbered row is moving at a speed variant with that of the odd-number rows, unlike in (a), where each row moves at the same speed

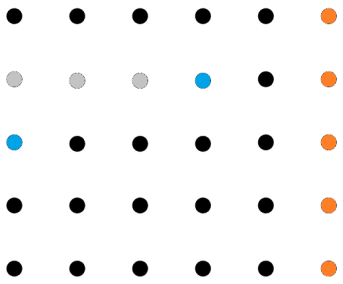


Fig. 4.8 Characteristics of a Dynamical Cluster State Quantum Computation Circuit. Input register (in orange) and state-hopping mechanism (in blue with intermediate physical qubits in grey) are two such interesting aspects of this model

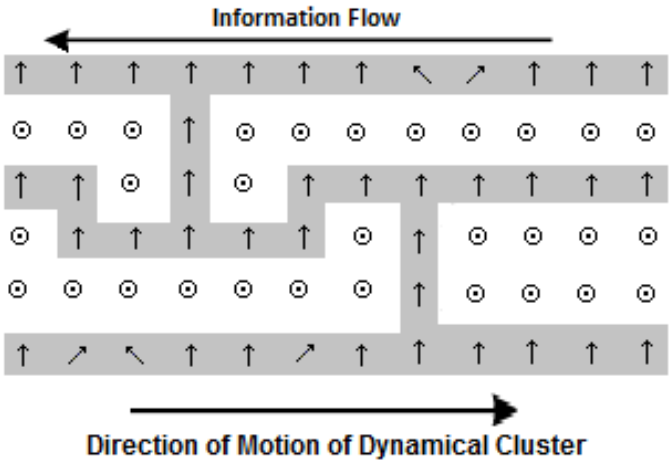


Fig. 4.9 Dynamical Cluster State Quantum Computation. The $\odot$ represents measurement in σ_z basis while the arrows represent measurements in the σ_x basis. The σ_z basis measurements remove the elements from the lattice while a chain of σ_x measurements creates an information-carrying 'wire'

Fig. 4.10 Generalized Circuit for Dynamical Cluster State Quantum Computation has three primary elements: the cluster input that constitutes the physical basis for the creation of the cluster state, the 'entangler' that creates entanglement between the various elements of the cluster and the readout section that measures elements in the cluster to enact the various quantum computation operations and algorithms on the cluster

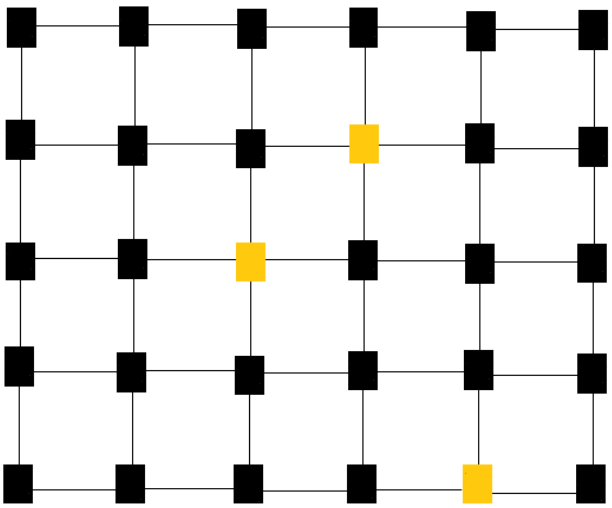


Fig. 4.11 Readout Elements. The Yellow Elements are active while the Black Elements are inactive. With a combination of active and inactive read-out elements, one can enact a quantum computation operation

Chapter 5

Decoherence-free Subspaces, Quantum Communication and Quantum Memory

"Quantum computation is...nothing less than a distinctly new way of harnessing nature."

— David Deutsch

Having established the significance of quantum entanglement, ways of generating and characterizing it, the most important step in the realm of quantum computation is the application of quantum entanglement in quantum information processing. The vector states associated with the $SWAP^{1/n}$ gates belong to a number of families and classes of quantum states, be it maximally entangled states (like the Dicke States) or partially entangled states (like Cluster States). Each of these families and states have the potential to be used for different kinds of quantum information processing tasks.

In this chapter, some of the key tasks will be investigated. This includes Decoherence-Free Subspaces (DFS), Cluster State Quantum Computation, Quantum Key Distribution (QKD) and Quantum Communication protocols, using the states found as part of this project.

5.1 Decoherence-Free Subspaces

A decoherence-free subspace is a subspace of Hilbert space of a system that remains invariant to non-unitary dynamics [161, 88, 301]. The system is kept decoupled from the environment and therefore its evolution is completely unitary. Decoherence-free subspaces can be characterized as a special class of quantum error correcting codes (QECC), as shall be highlighted later in this chapter. These subspaces isolate quantum information and thereby

prevent destructive or noisy interactions with the system's environment. These subspaces are an important conceptual and physical tool in quantum information, and are found to be useful when coherent control of a quantum system is required. Loss of coherence of quantum systems is called decoherence and takes place due to the interaction of a quantum system with uncontrollable degrees of freedom of the environment of the system. Since quantum computers cannot be truly and entirely isolated from their environment and thereby information can be lost due to decoherence, the study of decoherence-free subspaces is of utmost important for the implementation of quantum computation in the real world.

As per the definition of *Decoherence-free subspaces* [88], if we consider the dynamics of a system S coupled to a bath B and let the system evolve unitarily under the combined system-bath Hamiltonian

$$H = H_S \otimes I_B + I_S \otimes H_B + H_I \tag{5.1}$$

where H_S and H_B are the system and bath Hamiltonians respectively. I_S and I_B are the identity operator on the system and bath respectively. The last term in the hamiltonian denotes the interaction Hamiltonian

$$H_I = \sum_{\alpha=1} S_\alpha \otimes B_\alpha \tag{5.2}$$

where S_α and B_α act solely on the system and bath respectively.

The evolution in a subspace $\widetilde{\mathscr{H}}$ of the system Hilbert space $\mathscr{H}$ is unitary for all possible bath states iff

1. The following condition holds true

$$S_\alpha|\psi\rangle = a_\alpha|\psi\rangle, a_\alpha \in \mathbb{C} \tag{5.3}$$

for all states $|\psi\rangle$ that span $\widetilde{\mathscr{H}}$ and for every operator S_α in H_I.

2. Interaction operators S and B are decoupled initially.

3. $H_S|\psi\rangle$ has no overlap with states in the subspace that is orthogonal to $\widetilde{\mathscr{H}}$.

Then the subspace $\widetilde{\mathscr{H}}$ is called a decoherence-free subspace of $\mathscr{H}$.

To illustrate the idea of decoherence-free subspaces, let us take the example of one of the key

quantum gates in this project: the $\sqrt{SWAP}$ quantum gate in the interaction Hamiltonian for the idea of Decoherence-free subspaces,

$$H_{AB} = (|0\rangle\langle 0|) \otimes (|0\rangle\langle 0|) + (|1\rangle\langle 1|) \otimes (|1\rangle\langle 1|) + \frac{1}{2}(1+i)(|0\rangle\langle 0|) \otimes (|1\rangle\langle 1|) + \frac{1}{2}(1+i)(|1\rangle\langle 1|) \otimes (|0\rangle\langle 0|) + \frac{1}{2}(1-i)(|1\rangle\langle 0|) \otimes (|0\rangle\langle 1|) + \frac{1}{2}(1-i)(|0\rangle\langle 1|) \otimes (|1\rangle\langle 0|) \tag{5.4}$$

These terms can be written in the form

$$H_{AB} = \sum_{\alpha} t_{\alpha} A_{\alpha} B_{\alpha}, t_{\alpha} \in \mathbb{C} \tag{5.5}$$

We have $A_{\alpha} = \{|0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 1|, |1\rangle\langle 0|\}$, and the eigenvectors for A_{α} are $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. If we take these as our vectors $|\gamma_i\rangle$, and our single qubit operators as $H_A/H_B = \sum_k f_k \hat{\sigma}_k, f_k \in \mathbb{C}$, we see that the single qubit operators operating on the eigenvectors keeps them in the same 'good' subspace. Thus, the decoherence-free subspace for two qubits for the $\sqrt{SWAP}$ is given by

$$DFS_{\sqrt{SWAP}_2} = Span\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\} \tag{5.6}$$

Using these calculations for any power of $SWAP$, we can see that this is the DFS for all such systems. The reason this works for two qubits is because $|00\rangle \xrightarrow{\sqrt{SWAP}} |00\rangle$, $|11\rangle \xrightarrow{\sqrt{SWAP}} |11\rangle$ and $Span\{|01\rangle, |10\rangle\} \xrightarrow{\sqrt{SWAP}} Span\{|01\rangle, |10\rangle\}$.

Now, if we take the system A to be one with the operation of the $\sqrt{SWAP}$, connected to a 'bath' with an error-generating operator, we have a three-dimensional decoherence-free subspace

$$DFS_{\sqrt{SWAP}}(2) = Span\{|00\rangle\} \tag{5.7}$$

$$DFS_{\sqrt{SWAP}}(0) = Span\{|11\rangle\} \tag{5.8}$$

$$DFS_{\sqrt{SWAP}}(1) = Span\{|01\rangle, |10\rangle\} \tag{5.9}$$

This follows through for higher number of qubits (and other Powers-of-SWAP gates) as well, since the $\sqrt{SWAP}$ has a symmetry under parity. For an N-qubit case, the space spanned by vectors with the same number of $|0\rangle$'s and $|1\rangle$'s is decoherence-free. We can look at this at greater detail using elements of the Spin-Boson Model [302, 303, 301].

In this model, N spins form system A and a bosonic field forms the 'bath' system B. We have a hamiltonian of the form

$$H = \sum_{i=1}^{N} \sum_{k} (g_{i,k}^{+} \sigma_i^{+} \otimes b_k + g_{i,k}^{-} \sigma_i^{-} \otimes b_k^{\dagger} + g_{i,k}^{z} \sigma_i^{z} \otimes (b_k + b_k^{\dagger})) \tag{5.10}$$

where $\{\sigma_i^{+} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_i^{-} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_i^{z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\}$ are Pauli operators acting on the i^{th} spin, b_k ($b_k^{\dagger}$) is an annihilation (creation) operator for the k^{th} bosonic mode, and $g_{i,k}^{\alpha}$ are coupling constants. The Hamiltonian above describes a general interaction between a system of spins and a 'bath' of bosons, exchanging energy through the terms $g_{i,k}^{+} \sigma_i^{+} \otimes b_k + g_{i,k}^{-} \sigma_i^{-} \otimes b_k^{\dagger}$, and changing phase through the $g_{i,k}^{z} \sigma_i^{z} \otimes (b_k + b_k^{\dagger})$ term. As it stands this hamiltonian does not support a decoherence-free subspace: there are $3N$ A_α operators when comparing to Eq. (5.5), the N triples of local $sl(2)$ algebras $\{\sigma^{+}, \sigma^{-}, \sigma^{z}\}$, each acting on a single qubit, and therefore having a two-dimensional irrep. The overall action of the total Lie algebra is represented by the irreducible N-fold tensor product of all local two-dimensional irreps, which means that there are no one-dimensional irreps. This violates equation (5.10), since that condition is required for any index α , and thus this hamiltonian has no decoherence-free subspace.

This is no longer the case when a permutation symmetry is imposed on the system-bath interaction,

$$g_{i,k}^{\alpha} = g_k^{\alpha} \tag{5.11}$$

This is often called the *collective decoherence* case. We can now define the Hamiltonian as

$$H = \sum_{\alpha} A_\alpha \otimes B_\alpha \tag{5.12}$$

where $A_\alpha = \sum_{i=1}^{N} \sigma_i^{\alpha}$, $B_+ = g_k^{+} b_k$, $B_- = g_k^{-} b_k^{\dagger}$ and $B_z = g_k^{z}(b_k + b_k^{\dagger})$. The important part is that now the A_α form a global $sl(2)$ angular momentum algebra: $[A_+, A_-] = A_z$ and $[A_z, A_\pm] = 2A_\pm$. This forms a highly reducible $2^N \times 2^N$ representation formed by the action of the A_α operators on all N qubits at once. Since $sl(2)$ is a semisimple Lie algebra, Eq. (5.10) tells us that the decoherence-free subspace for this system is made up of those states $|\psi\rangle$ that satisfy

$$A_\alpha |\psi\rangle = 0 \forall \alpha \tag{5.13}$$

These are states with zero total angular momentum, the 'singlets' of the $sl(2)$ Lie algebra. Their explicit form is well known for the case $N = 2$, in which case there is only one singlet:

$$|\psi\rangle_2 = |s\rangle_{12} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{5.14}$$

where the notation $|s_{12}\rangle$ denotes a 'singlet state of qubits 1 and 2'. It is easy to see that the state

$$|\psi_N\rangle = \otimes_{m=1}^{N/2} |s\rangle_{2m-1,2m} \tag{5.15}$$

is in the N-qubit decoherence-free subspace and there are no decoherence-free subspace states for N. The method of Young tableaux can be used to derive the dimensionality formula: $\frac{N!}{h}$, where N is the number of elements and h is the hookproduct of the elements.

$$dim[DFS(N)] = \frac{N!}{(\frac{N}{2}+1)!\frac{N}{2}!} \tag{5.16}$$

If we look at the encoding efficiency ε of the decoherence-free subspace and using Stirling's approximation for factorials,

$$\varepsilon = \frac{log_2 dim[DFS(N)]}{N} = log_2\left(\frac{1}{(\frac{1}{2}+\frac{1}{N})^{\frac{1}{2}})(\frac{N}{2}+1)^{\frac{1}{N}})\sqrt{\frac{1}{2}}}\right) \xrightarrow{n\to\infty} log_2(2) = 1 \tag{5.17}$$

There are a lot of ways to calculate the singlet states for arbitrary N. We could do this by using group representation theory, using linear algebra or by using angular momentum addition rules. Let us consider the case of $N = 4$. The dimensionality formula yields $dim[DFS(4)] = 2$, meaning that this decoherence-free subspace encodes one logical qubit. One of the states is $|0_L\rangle = |s\rangle_{12} \otimes |s\rangle_{34}$. The second state that is orthogonal to the first must be a combination of the triplet states $|t_-\rangle = |00\rangle$, $|t_+\rangle = |11\rangle$ and $|t_0\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. The combination

$$|1_L\rangle = \frac{1}{\sqrt{3}}(|t_-\rangle_{12} \otimes |t_+\rangle_{34} - |t_0\rangle_{12} \otimes |t_0\rangle_{34} + |t_+\rangle_{12} \otimes |t_-\rangle_{34}) \tag{5.18}$$

has total $J = 0$ and is the second logical qubit. In this manner one can construct total $J = 0$ states for progressively, given the dimensions of the logical qubits, higher N.

For two qubits, we see that the subspace spanned by $\{|00\rangle, |11\rangle, \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\}$ is decoherence free when we have $S_\alpha = SWAP^{1/n}$ in equation (5.2). The case for higher number of qubits is a little more complex, as can be seen for the three-qubit case: if we take a

general state with a definite Hamming weight, say $\beta|001\rangle + \gamma|010\rangle + \delta|100\rangle; \beta, \gamma, \delta \in \mathbb{C}$ that has Hamming weight 1, this is not invariant under the application of a general interaction hamiltonian satisfying the aforementioned conditions. For example, $\beta|001\rangle + \gamma|010\rangle + \delta|100\rangle \xrightarrow{\sqrt{SWAP}\otimes I_{2\times 2}} \beta|001\rangle + (\frac{1}{2}(\gamma+\delta) + \frac{i}{2}(\gamma-\delta))|010\rangle + (\frac{1}{2}(\gamma+\delta) + \frac{i}{2}(-\gamma+\delta))|100\rangle \neq c(\beta|001\rangle + \gamma|010\rangle + \delta|100\rangle) \exists c \in \mathbb{C}$. We thus see that having a general state with the same Hamming weight is not invariant under a general interaction hamiltonian, even if all the coefficients for the vectors in a superposition are equal. We see that the DFS for such states, given any general $SWAP^{1/n}$-based system hamiltonian, are specifically the W-states:

$$DFS_0 = \{|000\rangle\} \tag{5.19}$$

$$DFS_1 = \{\frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)\} \tag{5.20}$$

$$DFS_2 = \{\frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle)\} \tag{5.21}$$

$$DFS_3 = \{|111\rangle\} \tag{5.22}$$

where DFS_i denotes decoherence-free subspace with Hamming weight i.

For the purposes of universal quantum computation, as in the case for qudit-based quantum computation and invariant-subspace based quantum computation, the fundamental qubits are encoded qubits that are known as logical qubits. These qubits are encoded in clusters formed by constituents of a decoherence-free subspace. In this formalism, two types of gates are needed:

1. Gates that perform operations within a Decoherence-Free Subspace

2. Gates that link two or more Decoherence-Free Subspace clusters (which encode logical qubits)

5.1.1 Stabilizers for Decoherence-Free Subspaces

As mentioned in the last section, we would like to find a set of universal gates for computation based on decoherence-free subspaces, with an emphasis on the exchange interaction and the associated $SWAP^{1/n}$. In order to identify such a set of fault-tolerant gates, we can reframe the definition of a decoherence-free subspaces into a *stabilizer formalism*. We define the *Decoherence-free Subspace stabilizer* $\mathscr{S}$ as a set of operators O_γ which act as identity on the

Decoherence-free subspace states

$$O_\gamma|\psi\rangle = |\psi\rangle \forall O_\gamma \in \mathscr{S} \tag{5.23}$$

if and only if the state $|\psi\rangle$ is in a decoherence-free subspace. Here γ is an index that can be discrete or continuous, while $\mathscr{S}$ forms a finite set or group.

A general error process can be described by Kraus operator-sums [83]:

$$\rho \to \sum_\mu A_\mu \rho A_\mu^\dagger \tag{5.24}$$

These (Kraus) operators A_μ can be expanded in a basis ε_i of 'errors', which exist in two types:

(i) Errors that anticommute with stabilizer codes in $\mathscr{S}$ and require active correction.

(ii) Errors that constitute the stabilizer $\varepsilon_i \in \mathscr{S}$ and do not affect the code.

Quantum Error Correction Codes (QECC) are designed primarily to deal with the first kind of errors but they can also be regarded as decoherence-free subspaces for the errors that are part of their stabilizers. Conversely, decoherence-free subspaces are designed to tackle errors of the second type but can be used as Quantum Error Correction Codes against type (i) errors.

Using equation (5.3), we can write $(S_\alpha - a_\alpha)|\psi\rangle = 0$. A general case could have a summation over the index: $\sum_\alpha (S_\alpha - a_\alpha)|\psi\rangle = 0$. Taking the exponent of this operator and operating on the state,

$$exp[\sum_\alpha (S_\alpha - a_\alpha I)]|\psi\rangle = |\psi\rangle \tag{5.25}$$

This is the condition given in equation (5.22). But instead of equating the two, we introduce a parameter p_α such that

$$O(\overrightarrow{p}) = exp[\sum_\alpha (S_\alpha - a_\alpha I)p_\alpha]|\psi\rangle = |\psi\rangle \tag{5.26}$$

Thus a natural link between decoherence-free subspaces, stabilizers and quantum error correction codes emerges.

Coming back to the question of allowed gates, going by this stabilizer picture, we have to identify gates that take code words to code words and that transform the stabilizer into

itself. Let $|\psi\rangle \in \widetilde{\mathscr{H}}$ and $O(\overrightarrow{p})|\psi\rangle = |\psi\rangle$. For an allowed gate, the associated operation U must be in this subspace $\widetilde{\mathscr{H}}$ as well: $O(\overrightarrow{p}')(U|\psi\rangle) = (U|\psi\rangle)$. This can be re-written as:

$$UO(\overrightarrow{p}')U^{\dagger}|\psi\rangle = |\psi\rangle = O[\overrightarrow{p}'(\overrightarrow{p})]|\psi\rangle \tag{5.27}$$

where $[\overrightarrow{p}'(\overrightarrow{p})]$ denotes a functional of $\overrightarrow{p}$ and $O[\overrightarrow{p}'(\overrightarrow{p})]$ must cover $\mathscr{S}$. Daniel Gottesman [304] showed that if $\mathscr{S}$ is a unitary group then the set of allowed operations is the normalizer of $\mathscr{S}$.

We note that so far we have required only that the action of the gate-operator must preserve the subspace at the conclusion of the gate operation. There is no condition on this during the duration of the gate operation. *Bacon et al* [88] proposed a stronger requirement that the state of the system must stay inside the decoherence-free subspace during the entire operation time of the gate. Rewriting the composite operator in equation (5.26) and considering a general time-dependent case:

$$U(t)O(\overrightarrow{p}') = O[\overrightarrow{p}'(\overrightarrow{p})]U(t) \tag{5.28}$$

Since quantum gate-operators are realized using hamiltonians H: $U = e^{-iHt}$, we use this idea in equation (5.28), differentiate with respect to time and evaluate at time $t = 0$,

$$HO(\overrightarrow{p}') = O[\overrightarrow{p}'(\overrightarrow{p})]H \tag{5.29}$$

This gives us a sufficient condition for the generating Hamiltonian for a gate-operator to keep the state at all times entirely within the decoherence-free subspace that was first given by *Bacon et al* [88].

5.1.2 Decoherence-Free Subspaces for Exchange Interaction

Let us consider the dynamics of N interacting spins that are collectively coupled to an environment with each spin experiencing the same interaction with its environment. We can then write $S_\alpha = \sum_i \sigma_\alpha^{(i)}$ with $\sigma_\alpha^{(i)}$ denoting operation on the i^{th} qubit. If we expand these operators, they look like the following for an N-qubit case:

$$S_x = \sigma_x \otimes I_{2\times 2} \otimes ... \otimes I_{2\times 2} + I_{2\times 2} \otimes \sigma_x \otimes ... \otimes I_{2\times 2} + ... + I_{2\times 2} \otimes I_{2\times 2} \otimes ... \otimes \sigma_x \tag{5.30}$$

$$S_y = \sigma_y \otimes I_{2\times 2} \otimes ... \otimes I_{2\times 2} + I_{2\times 2} \otimes \sigma_y \otimes ... \otimes I_{2\times 2} + ... + I_{2\times 2} \otimes I_{2\times 2} \otimes ... \otimes \sigma_y \tag{5.31}$$

$$S_z = \sigma_z \otimes I_{2\times 2} \otimes ... \otimes I_{2\times 2} + I_{2\times 2} \otimes \sigma_z \otimes ... \otimes I_{2\times 2} + ... + I_{2\times 2} \otimes I_{2\times 2} \otimes ... \otimes \sigma_z \tag{5.32}$$

For the condition $S_\alpha|\psi\rangle = a_\alpha|\psi\rangle, a_\alpha \in \mathbb{C}$ to hold true for each of these forms of S, we must have states that will give a global and not local phase across the superposition in the operators S_x, S_y and S_z. This is only possible if $|\psi\rangle = |+\rangle \otimes |+\rangle \otimes ... \otimes |+\rangle$ or $|-\rangle \otimes |-\rangle \otimes ... \otimes |-\rangle$ for the operator of the form in equation (5.29), $|\psi\rangle = |+\rangle_y \otimes |+\rangle_y \otimes ... \otimes |+\rangle_y$ or $|-\rangle_y \otimes |-\rangle_y \otimes ... \otimes |-\rangle_y$ for the operator of the form in equation (5.30), and $|\psi\rangle = |0\rangle_y \otimes |0\rangle_y \otimes ... \otimes |0\rangle_y$ or $|1\rangle_y \otimes |1\rangle_y \otimes ... \otimes |1\rangle_y$ for the operator of the form in equation (5.31), where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. These can never be simultaneously true. As a result,

$$S_\alpha|\psi\rangle = 0 \tag{5.33}$$

Using equation (5.33) in equation (5.26),

$$O(\overrightarrow{p}) = exp[\sum_\alpha (S_\alpha - a_\alpha I)p_\alpha]|\psi\rangle = exp[\sum_\alpha (-a_\alpha I)p_\alpha]|\psi\rangle \tag{5.34}$$

If we now consider the hamiltonian for the exchange interaction: $E|a\rangle|b\rangle \rightarrow |b\rangle|a\rangle$, we see that

$$O(\overrightarrow{p})E = exp[\sum_\alpha (-a_\alpha I)p_\alpha]E = E \times exp[\sum_\alpha (-a_\alpha I)p_\alpha] = E \times O(\overrightarrow{p}) \tag{5.35}$$

Thus, given the result in equation (5.29), the operator given by the exchange interaction preserves the decoherence-free subspace for a 'collective decoherence' model. The smallest number of physical qubits that gives a fully encoded Decoherence-free Subspace qubit is found to be four [88]. Let us take this case, and consider the states with zero angular momentum:

$$|0\rangle_L = \frac{1}{2}(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle) \tag{5.36}$$

$$|1\rangle_L = \frac{1}{\sqrt{3}}(|00\rangle \otimes |11\rangle - \frac{1}{2}(|01\rangle + |10\rangle) \otimes (|01\rangle + |10\rangle) + |11\rangle \otimes |00\rangle) \tag{5.37}$$

Let us now look at the effect of the operation of the various exchange interactions E_{ij}, where the i^{th} and j^{th} qubits are being exchanged.

$$E_{12}|0\rangle_L \rightarrow -|0\rangle_L, E_{12}|1\rangle_L \rightarrow |1\rangle_L \tag{5.38}$$

Due to the symmetry of the logical basis states, E_{34} has the same effect. Looking at the operation, we can define an encoded $\bar{Z}$ operator:

$$\bar{Z} = -E_{12} = -E_{34} \tag{5.39}$$

For defining a similar $\bar{X}$ operator: $\bar{X}|0\rangle_L \rightarrow |1\rangle_L, \bar{X}|1\rangle_L \rightarrow |0\rangle_L$ is not as straightforward since no one exchange interaction seems to provide the solution. Therefore, before moving forward with trying to define this composite operator, let us look at some other cases for the exchange interaction:

$$\begin{aligned} E_{13}|0\rangle_L \rightarrow \frac{1}{2}(|0101\rangle - |1100\rangle - |0011\rangle + |1010\rangle) = \frac{1}{2}|0\rangle_L - \frac{\sqrt{3}}{2}|1\rangle_L, \\ E_{13}|1\rangle_L \rightarrow \frac{1}{\sqrt{3}}(|1001\rangle - \frac{1}{2}(|0101\rangle + |1100\rangle + |0011\rangle + |1010\rangle) + |0110\rangle) \\ = -\frac{\sqrt{3}}{2}|0\rangle_L - \frac{1}{2}|1\rangle_L \end{aligned} \quad (5.40)$$

Again, due to the symmetry of the states, the case for E_{24} gives the same results. Using operators E_{12} and E_{13} (or E_{34} and E_{24}), we can define the $\bar{X}$ operator

$$\bar{X} = -\frac{1}{\sqrt{3}}E_{12} - \frac{2}{\sqrt{3}}E_{13} = -\frac{1}{\sqrt{3}}E_{34} - \frac{2}{\sqrt{3}}E_{24} \quad (5.41)$$

The ability to implement these primary logical operations is sufficient to implement any gate in $SU(2)$ on the encoded qubits, by using the Euler angle reconstruction (about any two orthogonal axes):

$$exp(-i\omega(\vec{n}.\vec{\sigma})/2) = exp(-i\beta\sigma_z/2)exp(-i\theta\sigma_y/2)exp(-i\alpha\sigma_z/2) \quad (5.42)$$

the resulting rotation is given by the angle ω about the direction specified by the unit vector n, both of which are functions of α, β and θ. Mapping $(\sigma_x, \sigma_y, \sigma_z) \rightarrow (\bar{X}, \bar{Y}, \bar{Z})$, we can construct any element of SU(2) in the encoded space by turning on and off the appropriate exchange interaction.

For two qubit gates, we have to construct slightly more complex combinations of gates. Let us start with the controlled-Phase shift gate (CPHASE). The idea is to introduce a phase for the last case and not for any of the others. With some clever usage of the exchange interactions, this can be done:

$$(-E_{12} - E_{56})(-E_{12} - E_{56} - 2I) \quad (5.43)$$

This gives us a phase only for the case for $|11\rangle_L$. The CPHASE gate has been previously realized in a different manner by *Bacon et al* [88] using the operators: $h_1 = [E_{26}, E_{12} + E_{25}] + [E_{15}, E_{12} + E_{16}], h_2 = \sum_{j=5}^{8}(E_{1j} + E_{2j})$ and $c = \frac{1}{32}[h_1, (h_2, h_1)]$. As can

be seen, our operator is a lot simpler in construction.

The CNOT gate can be realized similarly using two logical qubits. We find the form of this operator in the encoded space to be

$$\frac{1}{\sqrt{3}}(I-E_{12})(-E_{56}-2E_{57}) \tag{5.44}$$

The CNOT gate has been realized previously with two logical qubits comprising of three physical qubits as well by *DiVincenzo et al* [25].

Thus, one can obtain a fault-tolerant universal set of gates using just the exchange interaction.

5.1.3 Fault-Tolerant Preparation, Non-Destructive Ancilla-Based Measurement and Decoding of Encoded States

The $|0\rangle_L$ can be easily constructed by preparing two pairs of qubits in the singlet state. The other Decoherence-free subspace states, such as $|1\rangle_L$, can be obtained by applying the appropriate operation, in the encoded space, to $|0\rangle_L$. To verify that a state has been correctly prepared and to decode the state, we need fault-tolerant measurements in the encoded basis $|0\rangle_L$, $|0\rangle_L$.

By measuring $\{\sigma_x^1, \sigma_x^2, \sigma_z^3, \sigma_z^4\}$ on the physical qubits, we can distinguish the logical qubits. However, this operation destroys the *Decoherence-free Subspace* state. We can resolve this problem by using ancilla qubits in the process. For instance, to perform a fault tolerant and non-destructive measurement of $\bar{Z}$, we initialize the ancilla qubits to the state

$$|\psi_{anc}\rangle = |0\rangle_L \tag{5.45}$$

Thereafter, we perform an encoded CNOT gate between the decoherence-free subspace state $|\psi_q\rangle$ and the ancilla qubits:

$$|x_q, y_{anc}\rangle \xrightarrow{\bar{CNOT}} |x_q, (x_q + y_{anc}) mod 2\rangle \tag{5.46}$$

This encoded CNOT gate can be constructed either by using the universal gates defined earlier in this section or the direct implementation of a logical CNOT gate. If we now perform a destructive measurement on the ancilla qubits, we obtain a nondestructive measurement of $\bar{Z}$. We can prevent possible uncontrolled error propagation due to an incorrectly prepared ancilla

by preparing multiple $|0\rangle_L$ ancillas and applying $C\bar{N}OT$ gates between the Decoherence-free subspace states to be measured and each ancilla. Along with majority voting this provides a fault-tolerant method for measuring $\bar{Z}$. This method can also be used to verify that a state $|0\rangle$ has been prepared correctly and in a fault-tolerant manner.

5.1.4 Error in Implementation of $SWAP^{1/n}$ Gates

Let us say that our operator for a certain quantum computing task is a specific $SWAP^{1/n_1}$ and there is error due to imperfect realization of the same, say due to incorrect timing of operation, potentially giving rise to an arbitrary $SWAP^{1/n'}$ operator with $n_1 \neq n'$. For states $|00\rangle/|11\rangle$, the state remains unchanged for both the operator and source of noise. The same goes for the Bell-basis with Hamming weight, except for a global phase in the singlet state. Thus there is an inherent robustness against imperfect realization of $SWAP^{1/n}$ gate using the concept of decoherence-free subspaces. In this section, we briefly saw how exchange interaction leads to change in entanglement pattern of the states. This concept can be used, as entanglement swapping, for other tasks in quantum information processing, such as quantum communication.

5.2 Quantum Entanglement Swapping using $SWAP^{1/n}$ and Quantum Repeaters

In the realm of quantum information processing, entanglement swapping plays a major role in helping generate entanglement in remote particles. Let us say we start with the n-qubit state

$$|\psi_{in}\rangle = |010101...01\rangle \tag{5.47}$$

Now if we have pairs of qubits locally made to undergo exchange interaction, we shall get a series of entangled pairs. If the operator is the $\sqrt{SWAP}$ and we have even number of qubits, we will have

$$|\psi_{int}\rangle = (\frac{1}{2}(1+i)|01\rangle + \frac{1}{2}(1-i)|10\rangle)...(\frac{1}{2}(1+i)|01\rangle + \frac{1}{2}(1-i)|10\rangle) \tag{5.48}$$

Thus, we have qubit pairs 12, 34, 56, 78, ... , (n-1,n). We found that if we now use exchange interaction on the pairs 23, 45, 67, 89,...,(n-2,n-1), and then perform single qubit measurements on all qubits from qubits 2 to n-1, we invariably entangle qubits 1 and n. Interestingly, due to the symmetric way in which the state decomposition over vector states takes place, the entanglement between qubits 1 and n is always maximal! Thus, using such smaller

units (pairs) of entangled qubits, we can generate maximal entanglement over more complex structures and longer distances. Using this, we have found a variant of the conventional quantum repeater protocol by using exchange interaction instead of projective measurements.

Even though both Bell-measurements (as used in conventional repeater protocols) and realization of exchange interaction (as in our model) have associated errors, our protocol is particularly useful for systems that give rise to the exchange interaction, such as in spin-systems and quantum dots. The maximally entangled state formed in our protocol between qubits 1 and n can be used for various quantum information processing tasks. This is particularly useful for quantum communication protocols.

5.3 Quantum Communication Protocols

Quantum communication is the process of transferring an arbitrary quantum state from one place to another. One of its most important applications is Quantum Key Distribution (QKD), which is very important in quantum cryptography. Traditionally photonic systems have been the most popular for the realization of quantum communication. For the simple exchange of quantum information between the elements of a quantum information processing system over small distances, spin dynamics can help in realizing quantum communication protocols.

5.3.1 A Stationary-Qubit Communication Model

One of the most popular communication models in classical communication is the bus-based model. In this model, the bus/register is the primary unit of information processing and information is mediated between buses using flying bits. In the world of quantum information processing, this has traditionally been done by carrier particles such as photons. As part of our project, we observed the short-range and yet effective mediation done by the exchange interaction in spin-systems. In our stationary-qubit model, we have an integrated computing-and-communication system. Each computation unit comprises of an array of spins being driven through channels, such as electrons driven by surface acoustic waves in semiconductor heterostructures, and made to interact at specific locations in the system.

This leads to rapid development of entanglement in this computing unit. Now, we have a bunch of particles in an intermediate unit that is kept away from the computing unit, until

they are required for mediating in the communication protocol. When this is so required, one particle from the computing bus-unit interacts with the 'flying' qubit, which subsequently interacts with other 'flying qubits' and finally with another computing bus-unit (and its qubits). In this manner, information is transferred from one computing bus-unit to another. A simple model in this case would be one where there are a finite number of 'flying' qubits, say one, for instance. Let us tag this qubit as F_1. Let there be a target qubit in a second bus-unit, tagged B_2. Let the 'flying' qubit F_1 and bus-qubit B_2 be initialized to $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. If the state on the qubit from the first bus (let us call it B_1) that is interacting with the flying qubit is in the state $|\psi_{B_1}\rangle = \alpha|0\rangle + \beta|1\rangle$, and we operate two distinct Power-of-SWAP gates between $|\psi\rangle$ and F_1, and between F_1 and B_2, we have

$$\begin{aligned}|\psi_{B_1F_1B_2}\rangle = \frac{1}{2}(&|0\rangle|0\rangle(\alpha|0\rangle + (\alpha(+)_2 + \alpha(+)_1(-)_2 + \beta(-)_1(-)_2)|1\rangle)\\ &+|0\rangle|1\rangle((\alpha(-)_2 + \alpha(+)_1(+)_2 + (-)_1(+)_2)|0\rangle + (\alpha(+)_1 + \beta(-)_1)|1\rangle)\\ &+|1\rangle|0\rangle((\alpha(-)_1 + \beta(+)_1)|0\rangle + (\alpha(-)_1(+)_2 + \beta(+)_1(+)_2 + \beta(-)_1)|1\rangle)\\ &+|1\rangle|1\rangle((\alpha(-)_1(-)_2 + \beta(+)_1(-)_2 + \beta(+)_1)|0\rangle + \beta|1\rangle)) \quad (5.49)\end{aligned}$$

where $(\pm)_i = \frac{1}{2}(1 \pm e^{i\pi/n_i})$

This model, however, has some associated problems: firstly, the tuning of the interaction for the 'flying' qubits has to be very precise and localized to the area around a qubit in a manner that does not affect or influence the other 'flying' qubits. As can be seen from the form of the state, there needs to be a great degree of control for this communication protocol. Secondly, errors could also arise with greater numbers of such interactions.

5.3.2 Communication using a Chain of Stationary Spins

A natural extension that could take place would be if the interactions between the qubits in a chain are non-changing and not controllable, and we cannot apply any control fields to the qubits. Such systems where a large collection of spin are permanently coupled can be found in bulk materials. These mutual interactions of spins makes them either tend towards being aligned or anti-aligned with respect to each other, resulting in phenomena such as anti-ferromagnetism. The term *spin chain* describes a large class of materials wherein the spins are arranged in a one-dimensional lattice and are permanently coupled to each other (with the interaction strength decreasing with distance usually). In the spin-chain model, we extend the communication model from the single qubit as initially defined to a collection of 'flying' qubits that transmit a certain amount of information.

We start our protocol with the initialization of the spin chain, say with all the states in the state $|0\rangle$

$$|\psi\rangle = |000000...0\rangle \tag{5.50}$$

We choose the couplings between the qubits in the exchange interaction

$$H = \sum_{i,j} J s_i.s_j \tag{5.51}$$

in such a manner that initialization of the spin chain to such a state is easy. For instance, if in the exchange interaction, we take the coupling constant such that $J < 0$, we get the case of the ferromagnets, where the ground state in a magnetic field has all the spins oriented in the direction of this external field. Much like in the case of the single qubit mentioned above, in this slightly more involved protocol, a user Alice places an arbitrary quantum state at one end of the spin chain.

Let us say that Alice is on the N^{th} site and Bob is on an arbitrary site b on the site. For instance, if Alice's state is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, then the state of the spin chain is

$$|\psi_{in}\rangle = \frac{1}{\sqrt{2}}(|000..0\rangle + |000..01\rangle) \tag{5.52}$$

The natural evolution of this spin-chain leads to the state propagating as well being dispersed along the chain. Let us define the states

$$|\psi_1\rangle = |1000..0\rangle \tag{5.53}$$

$$|\psi_2\rangle = |0100..0\rangle \tag{5.54}$$

...

$$|\psi_N\rangle = |000..01\rangle \tag{5.55}$$

Due to the Hamming-weight preserving symmetry of the exchange interaction, as discussed previously, the state $|\psi_{in}\rangle$ can only evolve into a superposition of the various $|\psi_i\rangle$ as defined above and $|0000...00\rangle$. As a result, the state of the spin changes at various points in the chain and also at Bob's end. Bob now has to choose an appropriate time to obtain a state that is as close to Alice's state as possible,

$$|\psi_{bob}\rangle = \frac{1}{\sqrt{2}}(|000..00\rangle + |\psi_b\rangle) \tag{5.56}$$

The state of the spin at the site b will, in general, be a mixed state. The resultant output state can be obtained by the partial tracing off of all the spins at the other sites. We find the final output state by evolving the initial state defined in equation (5.22),

$$|\psi_{out}\rangle = \langle\phi|e^{-iHt}(\frac{1}{\sqrt{2}}(|000..00\rangle + |\psi_N\rangle))|\phi\rangle \tag{5.57}$$

where $|\phi\rangle$ are all possible N qubit states. Practically, in this example, only states with Hamming weight one will remain. The mixed state density matrix is given by

$$\rho = Tr_{123..(N-1)}|\psi_{out}\rangle\langle\psi_{out}| \tag{5.58}$$

The transition amplitude depends on the factor $\langle b|e^{-iHt}|N\rangle$.

5.4 Quantum Memory using $SWAP^{1/n}$ Gates

Computation, without memory, is not as optimal and efficient, and quantum computation is no different in the case of most algorithms and information processing tasks. This is particularly required in the context of quantum communication, and a way to realize this, which follows from the previous discussion on quantum communication protocols using a medium that has constant coupling constant that is always operational, has been formulated by us, as part of this project.

Let us take the simple case of a system that has three components: the qubit(s) to be stored

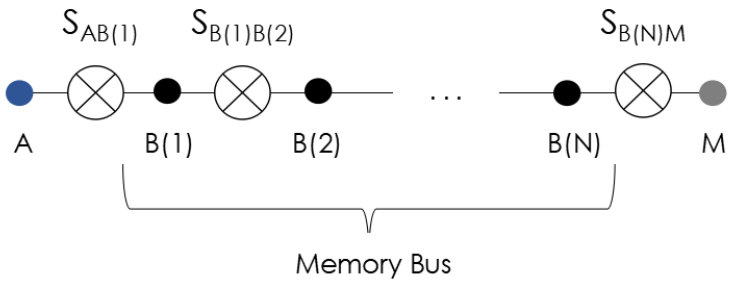


Fig. 5.1 Illustration of linear Quantum Memory using $SWAP^{1/n}$ with one input and output qubit, along with an N-qubit memory bus

(Q_A at location 'A' in Figure 5.1), the 'memory bus' and the qubit(s) in which the information

is to be stored (Q_M at location 'M' in Figure 5.1). The simplest example would be when the memory-bus is initialized to the state

$$|\psi_M\rangle = |000...00\rangle \tag{5.59}$$

Let us have the initial states of qubits Q_A and Q_M as: $|\psi_A\rangle = |1\rangle$ and $|\psi_M\rangle = |0\rangle$. An important point to note here is that though the couplings $S_{B(i)B(j)}, i \neq j$ are operational always, the $SWAP^{1/n}$-based couplings $S_{AB(1)}$ and $S_{B(N)M}$ are operated only when required.

We begin our protocol by switching on the couplings $S_{AB(1)}$ and $S_{B(N)M}$. Due to the Hamming-weight symmetry of the $SWAP^{1/n}$, the evolution of the states based on the couplings leads to a superposition of states with the same Hamming weight. We can select the couplings and time such that we reach a state as close to the quantum state:

$$|\psi_{AB(1)B(2)...B(N)M} = |000...001\rangle \tag{5.60}$$

The simplest case in this is when the quantum-bus is represented by a single qubit. If we begin with switching on the coupling between Q_A and the memory-bus, keeping the coupling between the memory-bus and Q_B switched off. One can realize the *SWAP* gate by continuous operation of the coupling giving a state $|\psi_{AB(1)}\rangle = |01\rangle$. We now shut off the coupling $S_{AB(1)}$ and switch on the one between the memory and the qubit Q_B. The *SWAP* gate is realized and state transferred to Q_B, completing the protocol.

More complicated circuits and systems can be implemented, including those with multiple storage qubits attached to the memory-bus. In the example shown in Figure 5.2, we can start with the state $|\psi_{A(1)A(2)B(1)B(2)B(3)B(4)M(1)M(2)}\rangle = |11000000\rangle$. Using appropriate coupling and time of interaction, we can reach the state $|\psi_{A(1)A(2)B(1)B(2)B(3)B(4)M(1)M(2)}\rangle = |00000011\rangle$, which completes the protocol.

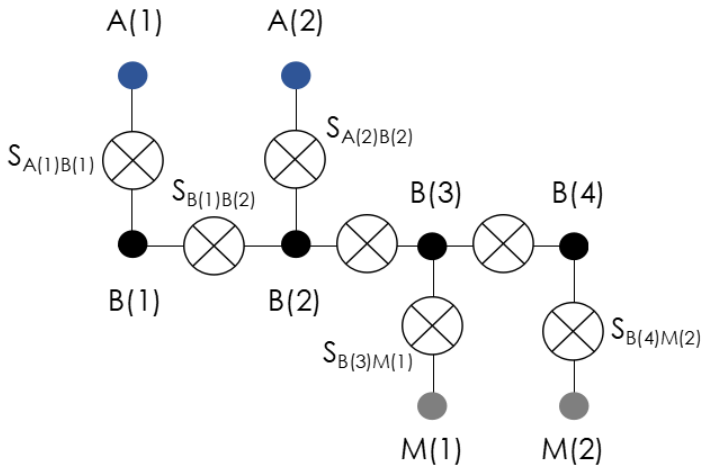


Fig. 5.2 Illustration of branched Quantum Memory using $SWAP^{1/n}$ with two input and two output qubits, along with a four-qubit memory bus

Chapter 6

Conclusion

In this project, we have worked on the generation, characterization and application of quantum entanglement using the $SWAP^{1/n}$ Operator, realized with the Heisenberg Hamiltonian. The Heisenberg Hamiltonian is ubiquitous in nature and where, on one hand, the $SWAP$ operator (which can be realized using the exchange interaction) is largely ineffective in generating entanglement, on the other hand, the partial $SWAP$ operators - the $SWAP^{1/n}$ gates are found to be efficient in entanglement generation, with the $\sqrt{SWAP}$ having the highest entangling power among all Power-of-$SWAP$s.

For the generation of entanglement, we have looked into numerical as well as analytic methods, supported by simulations of the physical systems, to generate vector states using the $SWAP^{1/n}$ Operator. The central question that was tackled in this phase of the project was regarding the kinds of quantum states that are accessible by just the application of the $SWAP^{1/n}$ gates on a general quantum state. The approach to resolve this central problem was firstly done using numerics and algorithms like Heap's algorithm. Since multiple $SWAP^{1/n}$ Operators are non-commutative in general, the problem assumes a complicated structure, and given the expontential scaling of the complexity of the problem with the addition of qubits, numerical approaches were found to be inefficient for higher number of qubits in the quantum system.

Having seen that numerical methods could not help us solve this problem beyond a point, we began employing group-theoretic methods to tackle this problem. This was done after seeing that the group of multiple $SWAP^{1/n}$ gates is isomorphic to the Symmetric Group S_n. The vector states for the groups for three, four, five and six qubits were found using the Cayley-tree formalism as well as the null-space formalism. General trends were found and some of the characteristics of higher-dimensional vector-states were highlighted, including

the presence of one-dimensional invariant subspaces that were spanned by the W-states/Dicke states. We also evaluated the number of invariant subspaces, the symmetry properties of vectors spanning them as well as entanglement patterns in each subspace for the cases of few-qubit systems as well as larger systems.

The characterization of the entanglement generated in these systems was done using tests for separability as well as those for entanglement. For the former, we looked into three distinct ways of tackling the problem: a graphical method of separability characterization, the classical approach to separability and the use of permutations and permutation symmetries to characterize separability. The 'thread-and-bead' model is a simple graphical method that we proposed to easily gauge the separability 'nodes' as they emerged for the various cases analysed using this method.

The classical approach to study separability including the comparison method and partitioning algorithm, both of which were found to be comprehensive methods of analysing separability. Lastly, local permutations within confined subspaces and in the entire Hilbert Space were found to yield interesting entanglement witnesses and tests for separability. In this section, we then looked at the entanglement characterization using three tools: $SWAP^{1/n}$ operator itself as an entanglement witness, application-based 'distance' measures and the 'engle' that was created to overcome the problems faced by traditional algebraic entanglement witnesses such as the tangle and concurrence. The application-based 'distance' measures we based on quantum information tasks such as quantum teleportation and communication protocols, while the idea of the 'engle' was based on the symmetry within entangled states.

The application of the entanglement generated was in three-major areas. We studied and independently devised ways to realized quantum computation using the exchange interaction and the $SWAP^{1/n}$ gate. This included the circuit-based model, the cluster-state model, the qudit-based model, the functional model and the decoherence-free subspaces based model of quantum computing using $SWAP^{1/n}$. A few vital changes in these models included a more comprehensive approach to devising the cluster-state model for exchange interaction, beginning with group-theoretic ideas, and moving from a qubit-based to a qudit-based model for functional quantum computing.

We looked closely into the creation of decoherence-free subspaces using exchange interaction, including looking at the possibility of faulty realization of $SWAP^{1/n}$ gates that would leave the decoherence-free subspaces unaffected. These subspaces provided us with a robust and

noise-proof resource for quantum information processing. We also studied the concept of entanglement swapping using $SWAP^{1/n}$ operator that was shown to be useful for the purposes of realizing quantum repeaters and quantum communication protocols. Last but not the least, we devised a simple model for quantum memory based on the exchange interaction and $SWAP^{1/n}$, so as to be used with the other elements devised and studied in this project, thereby completing a set of basic quantum information processing elements using the exchange interaction and $SWAP^{1/n}$ gates.

Thus, using the concept of entanglement generated by $SWAP^{1/n}$ Operator, we have explored certain key, relevant ideas related to entanglement and quantum information processing. A possible future direction of study, extending this work could be in contributing more to the entanglement characterization and looking at the various other applications of the entanglement generated in such systems, such as in quantum cryptography.

References

[1] Rafael N Alexander, Pei Wang, Niranjan Sridhar, Moran Chen, Olivier Pfister, and Nicolas C Menicucci. One-way quantum computing with arbitrarily large time-frequency continuous-variable cluster states from a single optical parametric oscillator. *Physical Review A*, 94(3):032327, 2016.

[2] John von Neumann. Zusätze zur arbeit "zur operatorenmethode...". *Annals of Mathematics*, 33(4):789–791, 1932.

[3] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[4] Erwin Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23(48):807–812, 1935.

[5] John S Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447, 1966.

[6] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Physical review letters*, 49(25):1804, 1982.

[7] Paul G Kwiat, Philippe H Eberhard, Aephraim M Steinberg, and Raymond Y Chiao. Proposal for a loophole-free bell inequality experiment. *Physical Review A*, 49(5):3209, 1994.

[8] Paul G Kwiat, Edo Waks, Andrew G White, Ian Appelbaum, and Philippe H Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2):R773, 1999.

[9] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[10] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4):2738, 1995.

[11] Charles H Bennett and David P DiVincenzo. Quantum information and computation. *Nature*, 404(6775):247–255, 2000.

[12] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325, 1997.

[13] David P DiVincenzo and Daniel Loss. Quantum computers and quantum coherence. *Journal of Magnetism and Magnetic Materials*, 200(1):202–218, 1999.

[14] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56(2):1201, 1997.

[15] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 63–68. ACM, 1998.

[16] Gilles Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003.

[17] Bala Kalyanasundaram and Georg Schnitger. Communication complexity and lower bounds for sequential computation. In *Informatik*, pages 253–268. Springer, 1992.

[18] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 358–367. ACM, 1999.

[19] Andris Ambainis, Leonard J Schulman, Amnon Ta-Shma, Umesh Vazirani, and Avi Wigderson. The quantum communication complexity of sampling. *SIAM Journal on Computing*, 32(6):1570–1585, 2003.

[20] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[21] David A Meyer. Quantum strategies. *Physical Review Letters*, 82(5):1052, 1999.

[22] Jens Eisert, Martin Wilkens, and Maciej Lewenstein. Quantum games and quantum strategies. *Physical Review Letters*, 83(15):3077, 1999.

[23] Lior Goldenberg, Lev Vaidman, and Stephen Wiesner. Quantum gambling. *Physical Review Letters*, 82(16):3356, 1999.

[24] Andrew M Steane, Wim van Dam, et al. Physicists triumph at guess my number. *Physics Today*, 53(2):35–39, 2000.

[25] David P DiVincenzo, Dave Bacon, Julia Kempe, Guido Burkard, and K Birgitta Whaley. Universal quantum computation with the exchange interaction. *Nature*, 408(6810):339, 2000.

[26] Yu A Pashkin, T Yamamoto, O Astafiev, Yasunobu Nakamura, DV Averin, and JS Tsai. Quantum oscillations in two coupled charge qubits. *Nature*, 421(6925):823–826, 2003.

[27] Tsuyoshi Yamamoto, Yu A Pashkin, Oleg Astafiev, Yasunobu Nakamura, and Jaw-Shen Tsai. Demonstration of conditional gate operation using superconducting charge qubits. *Nature*, 425(6961):941–944, 2003.

[28] LD Contreras-Pulido and R Aguado. Entanglement between charge qubits induced by a common dissipative environment. *Physical Review B*, 77(15):155420, 2008.

[29] Leo P Kouwenhoven, DG Austing, and Seigo Tarucha. Few-electron quantum dots. *Reports on Progress in Physics*, 64(6):701, 2001.

[30] MV Gurudev Dutt, L Childress, L Jiang, E Togan, J Maze, F Jelezko, AS Zibrov, PR Hemmer, and MD Lukin. Quantum register based on individual electronic and nuclear spin qubits in diamond. *Science*, 316(5829):1312–1316, 2007.

[31] Bjorn Trauzettel, Denis V Bulaev, Daniel Loss, and Guido Burkard. Spin qubits in graphene quantum dots. *Nature Physics*, 3(3):192–196, 2007.

[32] William F Koehl, Bob B Buckley, F Joseph Heremans, Greg Calusine, and David D Awschalom. Room temperature coherent control of defect spin qubits in silicon carbide. *Nature*, 479(7371):84–87, 2011.

[33] Muhandis Shiddiq, Dorsa Komijani, Yan Duan, Alejandro Gaita-Ariño, Eugenio Coronado, and Stephen Hill. Enhancing coherence in molecular spin qubits via atomic clock transitions. *Nature*, 531(7594):348–351, 2016.

[34] I Chiorescu, Y Nakamura, CJP Ma Harmans, and JE Mooij. Coherent quantum dynamics of a superconducting flux qubit. *Science*, 299(5614):1869–1871, 2003.

[35] I Chiorescu, P Bertet, K Semba, Y Nakamura, CJPM Harmans, and JE Mooij. Coherent dynamics of a flux qubit coupled to a harmonic oscillator. *Nature*, 431(7005):159–162, 2004.

[36] JB Majer, FG Paauw, ACJ Ter Haar, CJPM Harmans, and JE Mooij. Spectroscopy on two coupled superconducting flux qubits. *Physical review letters*, 94(9):090501, 2005.

[37] Gui-Lu Long and Yang Sun. Efficient scheme for initializing a quantum register with an arbitrary superposed state. *Physical Review A*, 64(1):014303, 2001.

[38] AM Stoneham, AJ Fisher, and PT Greenland. Optically driven silicon-based quantum gates with potential for high-temperature operation. *Journal of Physics: Condensed Matter*, 15(27):L447, 2003.

[39] Xiaodong Xu, Yanwen Wu, Bo Sun, Qiong Huang, Jun Cheng, DG Steel, AS Bracker, D Gammon, C Emary, and LJ Sham. Fast spin state initialization in a singly charged inas-gaas quantum dot by optical cooling. *Physical review letters*, 99(9):097401, 2007.

[40] M Veldhorst, CH Yang, JCC Hwang, W Huang, JP Dehollain, JT Muhonen, S Simmons, A Laucht, FE Hudson, KM Itoh, et al. A two-qubit logic gate in silicon. *Nature*, 526(7573):410–414, 2015.

[41] Konstantinos G Lagoudakis, Peter L McMahon, Kevin A Fischer, Shruti Puri, Kai Müller, Dan Dalacu, Philip J Poole, Michael E Reimer, Val Zwiller, Yoshihisa Yamamoto, et al. Initialization of a spin qubit in a site-controlled nanowire quantum dot. *New Journal of Physics*, 18(5):053024, 2016.

[42] I Malajovich, JM Kikkawa, DD Awschalom, JJ Berry, and N Samarth. Coherent transfer of spin through a semiconductor heterointerface. *Physical review letters*, 84(5):1015, 2000.

[43] I Malajovich, JJ Berry, N Samarth, and DD Awschalom. Persistent sourcing of coherent spins for multifunctional semiconductor spintronics. *Nature*, 411(6839):770–772, 2001.

[44] Jani Tuorila, Matti Partanen, Tapio Ala-Nissila, and Mikko Möttönen. Efficient protocol for qubit initialization with a tunable environment. *npj Quantum Information*, 3(1):27, 2017.

[45] Vladimir B Braginsky, Vladimir Borisovich Braginsky, and Farid Ya Khalili. *Quantum measurement*. Cambridge University Press, 1995.

[46] G Nogues, A Rauschenbeutel, S Osnaghi, M Brune, JM Raimond, and S Haroche. Seeing a single photon without destroying it. *Nature*, 400(6741):239–242, 1999.

[47] GJ Pryde, JL O'Brien, AG White, SD Bartlett, and TC Ralph. Measuring a photonic qubit without destroying it. *Physical review letters*, 92(19):190402, 2004.

[48] DB Hume, T Rosenband, and David J Wineland. High-fidelity adaptive qubit detection through repetitive quantum nondemolition measurements. *Physical review letters*, 99(12):120502, 2007.

[49] P Neumann. P. neumann, j. beck, m. steiner, f. rempp, h. fedder, pr hemmer, j. wrachtrup, and f. jelezko, science 329, 542 (2010). *Science*, 329:542, 2010.

[50] BR Johnson, MD Reed, AA Houck, DI Schuster, Lev S Bishop, E Ginossar, JM Gambetta, L DiCarlo, L Frunzio, SM Girvin, et al. Quantum non-demolition detection of single microwave photons in a circuit. *Nature Physics*, 6(9):663–667, 2010.

[51] Lucio Robledo, Lilian Childress, Hannes Bernien, Bas Hensen, Paul FA Alkemade, and Ronald Hanson. High-fidelity projective read-out of a solid-state spin quantum register. *Nature*, 477(7366):574–578, 2011.

[52] Sergio O Valenzuela, William D Oliver, David M Berns, Karl K Berggren, Leonid S Levitov, and Terry P Orlando. Microwave-induced cooling of a superconducting qubit. *Science*, 314(5805):1589–1592, 2006.

[53] MD Reed, BR Johnson, AA Houck, L DiCarlo, JM Chow, DI Schuster, L Frunzio, and RJ Schoelkopf. Fast reset and suppressing spontaneous emission of a superconducting qubit. *Applied Physics Letters*, 96(20):203110, 2010.

[54] BE King, CS Wood, CJ Myatt, QA Turchette, D Leibfried, WM Itano, C Monroe, and DJ Wineland. Cooling the collective motion of trapped ions to initialize a quantum register. *Physical Review Letters*, 81(7):1525, 1998.

[55] X-D Cai, Christian Weedbrook, Z-E Su, M-C Chen, Mile Gu, M-J Zhu, Li Li, Nai-Le Liu, Chao-Yang Lu, and Jian-Wei Pan. Experimental quantum computing to solve systems of linear equations. *Physical review letters*, 110(23):230501, 2013.

[56] Alistair J Brash, Luis MPP Martins, Feng Liu, John H Quilter, Andrew J Ramsay, Maurice S Skolnick, and Anthony M Fox. High-fidelity initialization of long-lived quantum dot hole spin qubits by reduced fine-structure splitting. *Physical Review B*, 92(12):121301, 2015.

[57] Jonathan D Mar, Jeremy J Baumberg, Xiulai Xu, Andrew C Irvine, and David A Williams. Ultrafast high-fidelity initialization of a quantum-dot spin qubit without magnetic fields. *Physical Review B*, 90(24):241303, 2014.

[58] Neil A Gershenfeld and Isaac L Chuang. Bulk spin-resonance quantum computation. *science*, 275(5298):350–356, 1997.

[59] David G Cory, Amr F Fahmy, and Timothy F Havel. Ensemble quantum computing by nmr spectroscopy. *Proceedings of the National Academy of Sciences*, 94(5):1634–1639, 1997.

[60] Michel Brune, E Hagley, J Dreyer, X Maitre, A Maali, Ch Wunderlich, JM Raimond, and S Haroche. Observing the progressive decoherence of the "meter" in a quantum measurement. *Physical Review Letters*, 77(24):4887, 1996.

[61] Wojciech Hubert Zurek. Decoherence and the transition from quantum to classical—revisited. In *Quantum Decoherence*, pages 1–31. Springer, 2006.

[62] Laura Mazzola, Jyrki Piilo, and Sabrina Maniscalco. Sudden transition between classical and quantum decoherence. *Physical review letters*, 104(20):200401, 2010.

[63] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern physics*, 76(4):1267, 2005.

[64] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.

[65] Serge Haroche. Entanglement, decoherence and the quantum/classical boundary. *Physics today*, 51(7):36–42, 1998.

[66] Cass A Sackett, David Kielpinski, Brian E King, Christopher Langer, Volker Meyer, Christopher J Myatt, M Rowe, QA Turchette, Wayne M Itano, David J Wineland, et al. Experimental entanglement of four particles. *Nature*, 404(6775):256–259, 2000.

[67] David A Kokorowski, Alexander D Cronin, Tony D Roberts, and David E Pritchard. From single-to multiple-photon decoherence in an atom interferometer. *Physical review letters*, 86(11):2191, 2001.

[68] Chung-Chieh Cheng and MG Raymer. Long-range saturation of spatial decoherence in wave-field transport in random multiple-scattering media. *Physical review letters*, 82(24):4807, 1999.

[69] David P DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015, 1995.

[70] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995.

[71] Debbie W Leung, Isaac L Chuang, Fumiko Yamaguchi, and Yoshihisa Yamamoto. Efficient implementation of selective recoupling in heteronuclear spin systems using hadamard matrices. *arXiv preprint quant-ph/9904100*, 1999.

[72] JI Cirac. Ji cirac and p. zoller, phys. rev. lett. 74, 4091 (1995). *Phys. Rev. Lett.*, 74:4091, 1995.

[73] Chris Monroe, DM Meekhof, BE King, Wayne M Itano, and David J Wineland. Demonstration of a fundamental quantum logic gate. *Physical review letters*, 75(25):4714, 1995.

[74] Anders Sørensen and Klaus Mølmer. Quantum computation with ions in thermal motion. *Physical review letters*, 82(9):1971, 1999.

[75] Emanuel Knill, Raymond Laflamme, and Wojciech H Zurek. Resilient quantum computation. *Science*, 279(5349):342–345, 1998.

[76] A Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[77] John Preskill. Reliable quantum computers. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 454, pages 385–410. The Royal Society, 1998.

[78] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error rate. *arXiv preprint quant-ph/9906129*, 1999.

[79] Emanuel Knill. Quantum computing with realistically noisy devices. *Nature*, 434(7029):39, 2005.

[80] Andrew M Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793, 1996.

[81] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[82] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek. Perfect quantum error correcting code. *Physical Review Letters*, 77(1):198, 1996.

[83] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.

[84] JM Taylor, H-A Engel, W Dür, A Yacoby, CM Marcus, P Zoller, and MD Lukin. Fault-tolerant architecture for quantum computation using electrically controlled semiconductor spins. *Nature Physics*, 1(3):177–183, 2005.

[85] G Waldherr, Y Wang, S Zaiser, M Jamali, T Schulte-Herbrüggen, H Abe, T Ohshima, J Isoya, JF Du, P Neumann, et al. Quantum error correction in a solid-state hybrid spin register. *Nature*, 506(7487):204–207, 2014.

[86] M Hebbache. Study of a quantum cnot logic gate with electron spins of diamond impurities. *Solid State Communications*, 194:20–24, 2014.

[87] Jonathan Roberts. *Using imperfect semiconductor systems for unique identification*. Springer, 2017.

[88] Dave Bacon, Julia Kempe, Daniel A Lidar, and KB Whaley. Universal fault-tolerant quantum computation on decoherence-free subspaces. *Physical Review Letters*, 85(8):1758, 2000.

[89] Howard M Wiseman and Gerard J Milburn. *Quantum measurement and control*. Cambridge university press, 2009.

[90] H Dieter Zeh. On the interpretation of measurement in quantum theory. *Foundations of Physics*, 1(1):69–76, 1970.

[91] Norwood Russell Hanson. Copenhagen interpretation of quantum theory. *American Journal of Physics*, 27(1):1–15, 1959.

[92] John Archibald Wheeler and Wojciech Hubert Zurek. *Quantum theory and measurement*. Princeton University Press, 2014.

[93] Jeff S Lundeen, Brandon Sutherland, Aabid Patel, Corey Stewart, and Charles Bamber. Direct measurement of the quantum wavefunction. *Nature*, 474(7350):188–191, 2011.

[94] Yakir Aharonov, David Z Albert, and Lev Vaidman. How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100. *Physical review letters*, 60(14):1351, 1988.

[95] NWM Ritchie, J Greg Story, and Randall G Hulet. Realization of a measurement of a "weak value". *Physical review letters*, 66(9):1107, 1991.

[96] Lijian Zhang, Animesh Datta, and Ian A Walmsley. Precision metrology using weak measurements. *Physical review letters*, 114(21):210801, 2015.

[97] Wen-Jie Zou, Yu-Huai Li, Shu-Chao Wang, Yuan Cao, Ji-Gang Ren, Juan Yin, Cheng-Zhi Peng, Xiang-Bin Wang, and Jian-Wei Pan. Protecting entanglement from finite-temperature thermal noise via weak measurement and quantum measurement reversal. *Physical Review A*, 95(4):042342, 2017.

[98] Zi-Huai Zhang, Geng Chen, Xiao-Ye Xu, Jian-Shun Tang, Wen-Hao Zhang, Yong-Jian Han, Chuan-Feng Li, and Guang-Can Guo. Ultrasensitive biased weak measurement for longitudinal phase estimation. *Physical Review A*, 94(5):053843, 2016.

[99] WB Gao, A Imamoglu, H Bernien, and R Hanson. Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields. *Nature Photonics*, 9(6):363, 2015.

[100] Emre Togan, Yiwen Chu, AS Trifonov, Liang Jiang, Jeronimo Maze, Lilian Childress, MV Gurudev Dutt, Anders Søndberg Sørensen, PR Hemmer, Alexander S Zibrov, et al. Quantum entanglement between an optical photon and a solid-state spin qubit. *Nature*, 466(7307):730, 2010.

[101] Kristiaan De Greve, Leo Yu, Peter L McMahon, Jason S Pelc, Chandra M Natarajan, Na Young Kim, Eisuke Abe, Sebastian Maier, Christian Schneider, Martin Kamp, et al. Quantum-dot spin–photon entanglement via frequency downconversion to telecom wavelength. *Nature*, 491(7424):421, 2012.

[102] WJ Munro, AM Stephens, SJ Devitt, KA Harrison, and Kae Nemoto. Quantum communication without the necessity of quantum memories. *Nature Photonics*, 6(11):777, 2012.

[103] WB Gao, Parisa Fallahi, Emre Togan, Javier Miguel-Sánchez, and Atac Imamoglu. Observation of entanglement between a quantum dot spin and a single photon. *Nature*, 491(7424):426, 2012.

[104] WB Gao, P Fallahi, E Togan, A Delteil, YS Chin, J Miguel-Sanchez, and A Imamoğlu. Quantum teleportation from a propagating photon to a solid-state spin qubit. *Nature communications*, 4:2744, 2013.

[105] JR Schaibley, AP Burgers, GA McCracken, L-M Duan, PR Berman, DG Steel, AS Bracker, D Gammon, and LJ Sham. Demonstration of quantum entanglement between a single electron spin confined to an inas quantum dot and a photon. *Physical review letters*, 110(16):167401, 2013.

[106] Hannes Bernien, Bas Hensen, Wolfgang Pfaff, Gerwin Koolstra, MS Blok, Lucio Robledo, TH Taminiau, Matthew Markham, DJ Twitchen, Lilian Childress, et al. Heralded entanglement between solid-state qubits separated by three metres. *Nature*, 497(7447):86, 2013.

[107] Wolfgang Pfaff, BJ Hensen, Hannes Bernien, Suzanne B van Dam, Machiel S Blok, Tim H Taminiau, Marijn J Tiggelman, Raymond N Schouten, Matthew Markham, Daniel J Twitchen, et al. Unconditional quantum teleportation between distant solid-state quantum bits. *Science*, 345(6196):532–535, 2014.

[108] H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[109] Juan Ignacio Cirac, Peter Zoller, H Jeff Kimble, and Hideo Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Physical Review Letters*, 78(16):3221, 1997.

[110] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[111] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023, 2008.

[112] L-M Duan and HJ Kimble. Scalable photonic quantum computation through cavity-assisted interactions. *Physical review letters*, 92(12):127902, 2004.

[113] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[114] Jeremy L O'brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687, 2009.

[115] Daniel Loss and David P DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57(1):120, 1998.

[116] Rutger Vrijen, Eli Yablonovitch, Kang Wang, Hong Wen Jiang, Alex Balandin, Vwani Roychowdhury, Tal Mor, and David DiVincenzo. Electron-spin-resonance transistors for quantum computing in silicon-germanium heterostructures. *Physical Review A*, 62(1):012306, 2000.

[117] Wolfgang Harneit. Fullerene-based electron-spin quantum computer. *Physical Review A*, 65(3):032322, 2002.

[118] JM Elzerman, R Hanson, LH Willems Van Beveren, B Witkamp, LMK Vandersypen, and Leo P Kouwenhoven. Single-shot read-out of an individual electron spin in a quantum dot. *nature*, 430(6998):431, 2004.

[119] Bruce E Kane. A silicon-based nuclear spin quantum computer. *nature*, 393(6681):133, 1998.

[120] Jonathan A Jones, Vlatko Vedral, Artur Ekert, and Giuseppe Castagnoli. Geometric quantum computation using nuclear magnetic resonance. *Nature*, 403(6772):869, 2000.

[121] John JL Morton, Alexei M Tyryshkin, Richard M Brown, Shyam Shankar, Brendon W Lovett, Arzhang Ardavan, Thomas Schenkel, Eugene E Haller, Joel W Ager, and SA Lyon. Solid-state quantum memory using the 31 p nuclear spin. *Nature*, 455(7216):1085, 2008.

[122] Gavin K Brennen, Carlton M Caves, Poul S Jessen, and Ivan H Deutsch. Quantum logic gates in optical lattices. *Physical Review Letters*, 82(5):1060, 1999.

[123] Tommaso Calarco, U Dorner, Paul S Julienne, Carl J Williams, and Peter Zoller. Quantum computations with atoms in optical lattices: Marker qubits and molecular interactions. *Physical Review A*, 70(1):012306, 2004.

[124] Immanuel Bloch. Quantum coherence and entanglement with ultracold atoms in optical lattices. *Nature*, 453(7198):1016, 2008.

[125] Lev B Ioffe, Vadim B Geshkenbein, Mikhail V Feigel'Man, Alban L Fauchere, and Gianni Blatter. Environmentally decoupled sds-wave josephson junctions for quantum computing. *Nature*, 398(6729):679, 1999.

[126] Lara Faoro, Jens Siewert, and Rosario Fazio. Non-abelian holonomies, charge pumping, and quantum computation with josephson junctions. *Physical review letters*, 90(2):028301, 2003.

[127] Alexandre Blais, Ren-Shou Huang, Andreas Wallraff, Steven M Girvin, and R Jun Schoelkopf. Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. *Physical Review A*, 69(6):062320, 2004.

[128] Shi-Liang Zhu, ZD Wang, and Paolo Zanardi. Geometric quantum computation and multiqubit entanglement with superconducting qubits inside a cavity. *Physical review letters*, 94(10):100502, 2005.

[129] Kurt Gödel. Russell's mathematical logic. *1944*, pages 123–153, 1944.

[130] Alonzo Church. Analysis of data when the response is a curve. *Technometrics*, 8(2):229–246, 1966.

[131] AM Turing. Computing machinery and intelligence. *Brian Physiology and Psychology*, page 213, 1995.

[132] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[133] Charles H Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology*, pages 267–275. Springer, 1983.

[134] Charles H Bennett and Gilles Brassard. An update on quantum cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 475–480. Springer, 1984.

[135] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[136] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557, 1992.

[137] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400(1818):97–117, 1985.

[138] Rodney J Baxter. One-dimensional anisotropic heisenberg chain. *Annals of Physics*, 70(2):323–337, 1972.

[139] Xiaoguang Wang and Paolo Zanardi. Quantum entanglement and bell inequalities in heisenberg spin chains. *Physics Letters A*, 301(1-2):1–6, 2002.

[140] Cyrus F Hirjibehedin, Christopher P Lutz, and Andreas J Heinrich. Spin coupling in engineered atomic structures. *Science*, 312(5776):1021–1024, 2006.

[141] Rajiv RP Singh and David A Huse. Ground state of the spin-1/2 kagome-lattice heisenberg antiferromagnet. *Physical Review B*, 76(18):180407, 2007.

[142] Simeng Yan, David A Huse, and Steven R White. Spin-liquid ground state of the s= 1/2 kagome heisenberg antiferromagnet. *Science*, page 1201080, 2011.

[143] P Samarasekara. A solution of the heisenberg hamiltonian for oriented thick ferromagnetic films. *Chinese Journal of Physics*, 44(5):377–386, 2006.

[144] Christian Kollmar and Olivier Kahn. A heisenberg hamiltonian for intermolecular exchange interaction: Spin delocalization and spin polarization. *The Journal of chemical physics*, 98(1):453–472, 1993.

[145] Guido Burkard, Daniel Loss, and David P DiVincenzo. Coupled quantum dots as quantum gates. *Physical Review B*, 59(3):2070, 1999.

[146] Simon C Benjamin and Sougato Bose. Quantum computing with an always-on heisenberg interaction. *Physical review letters*, 90(24):247901, 2003.

[147] CHW Barnes, JM Shilton, and AM Robinson. Quantum computation using electrons trapped by surface acoustic waves. *Physical Review B*, 62(12):8410, 2000.

[148] Richard Jozsa. Quantum effects in algorithms. In *Quantum Computing and Quantum Communications*, pages 103–112. Springer, 1999.

[149] Reinhard F Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277, 1989.

[150] Lluís Masanes, Yeong-Cherng Liang, and Andrew C Doherty. All bipartite entangled states display some hidden nonlocality. *Physical review letters*, 100(9):090403, 2008.

[151] Pawel Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333–339, 1997.

[152] Asher Peres. Collective tests for quantum nonlocality. *Physical Review A*, 54(4):2685, 1996.

[153] Maciej Lewenstein and Anna Sanpera. Separability and entanglement of composite quantum systems. *Physical review letters*, 80(11):2261, 1998.

[154] Sinisa Karnas and Maciej Lewenstein. Separable approximations of density matrices of composite quantum systems. *Journal of Physics A: Mathematical and General*, 34(35):6919, 2001.

[155] M Horodecki. M. horodecki, p. horodecki, and r. horodecki, phys. lett. a 223, 1 (1996). *Phys. Lett. A*, 223:1, 1996.

[156] CW Gardiner and P Zoeller. Quantum noise springer-verlag. *Berlin, Heidelberg, New York*, 1991.

[157] Wojciech H Zurek. The environment, decoherence, and the transition from quantum to classical. In *Quantum Gravity And Cosmology-Proceedings Of The Xxii Gift International Seminar On Theoretical Physics*, page 117. World Scientific, 1992.

[158] Maximilian A Schlosshauer. *Decoherence: and the quantum-to-classical transition*. Springer Science & Business Media, 2007.

[159] Aashish A Clerk, Michel H Devoret, Steven M Girvin, Florian Marquardt, and Robert J Schoelkopf. Introduction to quantum noise, measurement, and amplification. *Reviews of Modern Physics*, 82(2):1155, 2010.

[160] Erich Joos, H Dieter Zeh, Claus Kiefer, Domenico JW Giulini, Joachim Kupsch, and Ion-Olimpiu Stamatescu. *Decoherence and the appearance of a classical world in quantum theory*. Springer Science & Business Media, 2013.

[161] Daniel A Lidar, Isaac L Chuang, and K Birgitta Whaley. Decoherence-free subspaces for quantum computation. *Physical Review Letters*, 81(12):2594, 1998.

[162] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[163] Robert Raussendorf, Daniel E Browne, and Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical review A*, 68(2):022312, 2003.

[164] Robert Raussendorf and Jim Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Physical review letters*, 98(19):190504, 2007.

[165] Hans J Briegel, David E Browne, Wolfgang Dür, Robert Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19, 2009.

[166] P Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 486–494. IEEE, 1999.

[167] F Diedrich, JC Bergquist, Wayne M Itano, and DJ Wineland. Laser cooling to the zero-point energy of motion. *Physical Review Letters*, 62(4):403, 1989.

[168] JP Home, MJ McDonnell, DM Lucas, G Imreh, BC Keitch, DJ Szwer, NR Thomas, SC Webster, DN Stacey, and AM Steane. Deterministic entanglement and tomography of ion–spin qubits. *New Journal of Physics*, 8(9):188, 2006.

[169] Dietrich Leibfried, Brian DeMarco, Volker Meyer, David Lucas, Murray Barrett, Joe Britton, Wayne M Itano, B Jelenković, Chris Langer, Till Rosenband, et al. Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature*, 422(6930):412, 2003.

[170] Nicolas C Menicucci. Temporal-mode continuous-variable cluster states using linear optics. *Physical Review A*, 83(6):062314, 2011.

[171] Shota Yokoyama, Ryuji Ukai, Seiji C Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nature Photonics*, 7(12):982, 2013.

[172] Moran Chen, Nicolas C Menicucci, and Olivier Pfister. Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb. *Physical review letters*, 112(12):120505, 2014.

[173] Pei Wang, Moran Chen, Nicolas C Menicucci, and Olivier Pfister. Weaving quantum optical frequency combs into continuous-variable hypercubic cluster states. *Physical Review A*, 90(3):032325, 2014.

[174] L-M Duan, MD Lukin, J Ignacio Cirac, and Peter Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413, 2001.

[175] Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165, 2007.

[176] Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7):nphys629, 2007.

[177] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[178] Gui-Lu Long and Xiao-Shu Liu. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, 65(3):032302, 2002.

[179] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, 2004.

[180] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[181] Harry Buhrman, Wim van Dam, Peter Høyer, and Alain Tapp. Multiparty quantum communication complexity. *Physical Review A*, 60(4):2737, 1999.

[182] Časlav Brukner, Marek Żukowski, Jian-Wei Pan, and Anton Zeilinger. Bell's inequalities and quantum communication complexity. *Physical review letters*, 92(12):127901, 2004.

[183] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long. Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, 71(4):044305, 2005.

[184] Wang Tie-Jun, Li Tao, Du Fang-Fang, and Deng Fu-Guo. High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement. *Chinese Physics Letters*, 28(4):040305, 2011.

[185] SJ Van Enk, Juan I Cirac, and Peter Zoller. Ideal quantum communication over noisy channels: a quantum optical implementation. *Physical Review Letters*, 78(22):4293, 1997.

[186] Jürgen Brendel, Nicolas Gisin, Wolfgang Tittel, and Hugo Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

[187] S Tanzilli, W Tittel, H De Riedmatten, H Zbinden, P Baldi, M DeMicheli, Da B Ostrowsky, and N Gisin. Ppln waveguide for quantum communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2):155–160, 2002.

[188] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, 68(4):042317, 2003.

[189] A Kuzmich, WP Bowen, AD Boozer, A Boca, CW Chou, L-M Duan, and HJ Kimble. Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles. *Nature*, 423(6941):731, 2003.

[190] Alessandro Romito, Rosario Fazio, and C Bruder. Solid-state quantum communication with josephson arrays. *Physical Review B*, 71(10):100501, 2005.

[191] Lilian Childress, JM Taylor, Anders Søndberg Sørensen, and MD Lukin. Fault-tolerant quantum communication based on solid-state photon emitters. *Physical review letters*, 96(7):070504, 2006.

[192] Sougato Bose. Quantum communication through spin chain dynamics: an introductory overview. *Contemporary Physics*, 48(1):13–30, 2007.

[193] Jian-Wei Pan, Christoph Simon, Časlav Brukner, and Anton Zeilinger. Entanglement purification for quantum communication. *Nature*, 410(6832):1067, 2001.

[194] Marco Lucamarini and Stefano Mancini. Secure deterministic communication without entanglement. *Physical review letters*, 94(14):140501, 2005.

[195] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum secure direct communication with quantum memory. *Physical review letters*, 118(22):220501, 2017.

[196] Michael J Biercuk, Hermann Uys, Aaron P VanDevender, Nobuyasu Shiga, Wayne M Itano, and John J Bollinger. Optimized dynamical decoupling in a model quantum memory. *Nature*, 458(7241):996, 2009.

[197] David Kielpinski, V Meyer, MA Rowe, CA Sackett, Wayne M Itano, C Monroe, and David J Wineland. A decoherence-free quantum memory using trapped ions. *Science*, 291(5506):1013–1015, 2001.

[198] Werner Heisenberg. Zur theorie des ferromagnetismus. *Zeitschrift für Physik*, 49(9-10):619–636, 1928.

[199] Erhard Scholz. Introducing groups into quantum theory (1926–1930). *Historia mathematica*, 33(4):440–490, 2006.

[200] Eugene P Wigner. On representations of certain finite groups. *American Journal of Mathematics*, 63(1):57–63, 1941.

[201] Eugene Paul Wigner. *Symmetries and Reflections: Scientific Essays of Eugene P. Wigner*. Ox Bow Press, 1979.

[202] Eugene Wigner. *Group theory: and its application to the quantum mechanics of atomic spectra*, volume 5. Elsevier, 2012.

[203] FA Matsen and David J Klein. Spin-free quantum chemistry. ix. aggregate theory of polyelectronic systems. *The Journal of Physical Chemistry*, 75(12):1860–1866, 1971.

[204] FA Matsen, JG Cosgrove, and JM Picone. Spin-free quantum chemistry. xiv. the infinite interaction range model for ferromagnetism. *International Journal of Quantum Chemistry*, 7(6):1077–1090, 1973.

[205] FA Matsen and TL Welsher. Spin-free quantum chemistry. xvi. spin correlation. *International Journal of Quantum Chemistry*, 9(1):171–188, 1975.

[206] S Balakrishnan and R Sankaranarayanan. Entangling characterization of swap 1/ m and controlled unitary gates. *Physical Review A*, 78(5):052305, 2008.

[207] Derrick H Lehmer. Teaching combinatorial tricks to a computer. In *Proc. Sympos. Appl. Math. Combinatorial Analysis*, volume 10, pages 179–193, 1960.

[208] RJ Ord-Smith. Generation of permutation sequences: part 1. *The Computer Journal*, 13(2):152–155, 1970.

[209] RJ Ord-Smith. Generation of permutation sequences: Part 2. *The Computer Journal*, 14(2):136–139, 1971.

[210] Robert Sedgewick. Permutation generation methods. *ACM Computing Surveys (CSUR)*, 9(2):137–164, 1977.

[211] BR Heap. Permutations by interchanges. *The Computer Journal*, 6(3):293–298, 1963.

[212] Katsuhisa Yamanaka. Permutation enumeration. *Encyclopedia of Algorithms*, pages 1–7, 2008.

[213] W Lipski. More on permutation generation methods. *Computing*, 23(4):357–365, 1979.

[214] Eric W Weisstein. Permutation matrix. 2002.

[215] Israel Gohberg, Peter Lancaster, and Leiba Rodman. *Invariant subspaces of matrices with applications*, volume 51. Siam, 1986.

[216] Heydar Radjavi and Peter Rosenthal. *Invariant subspaces*. Courier Corporation, 2003.

[217] Henry Helson. *Lectures on invariant subspaces*. Academic press, 2017.

[218] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990.

[219] Morton Hamermesh. *Group theory and its application to physical problems*. Courier Corporation, 2012.

[220] Margaret A Armstrong. Lagrange's theorem. In *Groups and Symmetry*, pages 57–60. Springer, 1988.

[221] G de B Robinson. On the representations of the symmetric group. *American Journal of Mathematics*, pages 745–760, 1938.

[222] Bruce E Sagan. *The symmetric group: representations, combinatorial algorithms, and symmetric functions*, volume 203. Springer Science & Business Media, 2013.

[223] Derek JS Robinson. *A Course in the Theory of Groups*, volume 80. Springer Science & Business Media, 2012.

[224] Walter Greiner and Berndt Müller. *Quantum mechanics: symmetries*. Springer Science & Business Media, 2012.

[225] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Mixed-state entanglement and quantum communication. In *Quantum information*, pages 151–195. Springer, 2001.

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

[227] Sevag Gharibian. Strong np-hardness of the quantum separability problem. *arXiv preprint arXiv:0810.4507*, 2008.

[228] J Sperling and W Vogel. Multipartite entanglement witnesses. *Physical review letters*, 111(11):110503, 2013.

[229] Jean-Daniel Bancal. Device-independent witnesses of genuine multipartite entanglement. In *On the Device-Independent Approach to Quantum Physics*, pages 73–80. Springer, 2014.

[230] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[231] Charles H Bennett, David P DiVincenzo, Peter W Shor, John A Smolin, Barbara M Terhal, and William K Wootters. Remote state preparation. *Physical Review Letters*, 87(7):077902, 2001.

[232] Toby S Cubitt, Frank Verstraete, W Dür, and J Ignacio Cirac. Separable states can be used to distribute entanglement. *Physical review letters*, 91(3):037902, 2003.

[233] Christian Peuntinger, Vanessa Chille, Ladislav Mišta Jr, Natalia Korolkova, Michael Förtsch, Jan Korger, Christoph Marquardt, and Gerd Leuchs. Distributing entanglement with separable states. *Physical review letters*, 111(23):230506, 2013.

[234] Barbara M Terhal and Paweł Horodecki. Schmidt number for density matrices. *Physical Review A*, 61(4):040301, 2000.

[235] Dagmar Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43(9):4237–4251, 2002.

[236] J Sperling and W Vogel. Necessary and sufficient conditions for bipartite entanglement. *Physical Review A*, 79(2):022318, 2009.

[237] Leonid Gurvits and Howard Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Physical Review A*, 66(6):062311, 2002.

[238] Leonid Gurvits and Howard Barnum. Separable balls around the maximally mixed multipartite quantum states. *Physical Review A*, 68(4):042312, 2003.

[239] Leonid Gurvits. Classical deterministic complexity of edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 2003.

[240] Crispin HW Barnes. Understanding entanglement. *Quantum Information Minor Option*, pages 3–5, 2108.

[241] Jon Magne Leinaas, Jan Myrheim, and Eirik Ovrum. Geometrical aspects of entanglement. *Physical Review A*, 74(1):012313, 2006.

[242] Olav F Syljuåsen. *Physical Review A*, 68(6):060301, 2003.

[243] Gregg Jaeger, Alexander V Sergienko, Bahaa EA Saleh, and Malvin C Teich. *Physical Review A*, 68(2):022318, 2003.

[244] Gabriel Bester, Alex Zunger, and J Shumway. *Physical Review B*, 71(7):075325, 2005.

[245] Ari M Turner, Yi Zhang, and Ashvin Vishwanath. *Physical Review B*, 82(24):241102, 2010.

[246] Luca Tagliacozzo and Guifre Vidal. *Physical Review B*, 83(11):115127, 2011.

[247] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. Entanglement in many-body systems. *Reviews of modern physics*, 80(2):517, 2008.

[248] Petar Jurcevic, Ben P Lanyon, Philipp Hauke, Cornelius Hempel, Peter Zoller, Rainer Blatt, and Christian F Roos. Quasiparticle engineering and entanglement propagation in a quantum many-body system. *Nature*, 511(7508):202–205, 2014.

[249] Rajibul Islam, Ruichao Ma, Philipp M Preiss, M Eric Tai, Alexander Lukin, Matthew Rispoli, and Markus Greiner. Measuring entanglement entropy in a quantum many-body system. *Nature*, 528(7580):77–83, 2015.

[250] Géza Tóth and Otfried Gühne. Entanglement and permutational symmetry. *Physical review letters*, 102(17):170503, 2009.

[251] Damian JH Markham. Entanglement and symmetry in permutation-symmetric states. *Physical Review A*, 83(4):042332, 2011.

[252] Robert Hübener, Matthias Kleinmann, Tzu-Chieh Wei, Carlos González-Guillén, and Otfried Gühne. Geometric measure of entanglement for symmetric states. *Physical Review A*, 80(3):032324, 2009.

[253] Artur Barasiński and Mateusz Nowotarski. Quantifying entanglement properties of qudit mixed states with incomplete permutation symmetry. *Physical Review A*, 95(4):042333, 2017.

[254] Manuel Calixto, Octavio Castaños, and Elvira Romera. Entanglement and quantum phase diagrams of symmetric multi-qubit systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2017(10):103103, 2017.

[255] Gururaj Kadiri and S Sivakumar. Permutation symmetry and entanglement in multipartite quantum states of unequal subsystem dimensions. *arXiv preprint arXiv:1702.04948*, 2017.

[256] T Eggeling and RF Werner. Separability properties of tripartite states with $u \otimes u \otimes u$ symmetry. *Physical Review A*, 63(4):042111, 2001.

[257] Géza Tóth and Otfried Gühne. Separability criteria and entanglement witnesses for symmetric quantum states. *Applied Physics B*, 98(4):617–622, 2010.

[258] Pawel Horodecki. P. horodecki and a. ekert, phys. rev. lett. 89, 127902 (2002). *Phys. Rev. Lett.*, 89:127902, 2002.

[259] Hyang-Tag Lim, Yong-Su Kim, Young-Sik Ra, Joonwoo Bae, and Yoon-Ho Kim. Realizing physical approximation of the partial transpose. In *Advances in Photonics of Quantum Computing, Memory, and Communication V*, volume 8272, page 82720J. International Society for Optics and Photonics, 2012.

[260] Stephen M Barnett, Anthony Chefles, and Igor Jex. Comparison of two unknown pure quantum states. *Physics Letters A*, 307(4):189–195, 2003.

[261] Dominique Spehner. Quantum correlations and distinguishability of quantum states. *Journal of Mathematical Physics*, 55(7):075211, 2014.

[262] Tao Zhou. Success probabilities for universal unambiguous discriminators between unknown pure states. *Physical Review A*, 89(1):014301, 2014.

[263] Emily Adlam and Adrian Kent. Knowledge-concealing evidencing of knowledge about a quantum state. *Physical review letters*, 120(5):050501, 2018.

[264] AK Rajagopal and RW Rendell. Robust and fragile entanglement of three qubits: Relation to permutation symmetry. *Physical Review A*, 65(3):032328, 2002.

[265] SJ Van Enk. The joys of permutation symmetry: Direct measurements of entanglement. *arXiv preprint arXiv:0902.2007*, 2009.

[266] Robert Prevedel, Gunther Cronenberg, Mark S Tame, Mauro Paternostro, Philip Walther, Mu-Seong Kim, and Anton Zeilinger. Experimental realization of dicke states of up to six qubits for multiparty quantum networking. *Physical review letters*, 103(2):020503, 2009.

[267] Bernd Lücke, Jan Peise, Giuseppe Vitagliano, Jan Arlt, Luis Santos, Géza Tóth, and Carsten Klempt. Detecting multiparticle entanglement of dicke states. *Physical review letters*, 112(15):155304, 2014.

[268] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631, 2014.

[269] Harold Ollivier and Wojciech H Zurek. Quantum discord: a measure of the quantumness of correlations. *Physical review letters*, 88(1):017901, 2001.

[270] Animesh Datta, Anil Shaji, and Carlton M Caves. Quantum discord and the power of one qubit. *Physical review letters*, 100(5):050502, 2008.

[271] Shunlong Luo. Quantum discord for two-qubit systems. *Physical Review A*, 77(4):042303, 2008.

[272] Borivoje Dakić, Vlatko Vedral, and Časlav Brukner. Necessary and sufficient condition for nonzero quantum discord. *Physical review letters*, 105(19):190502, 2010.

[273] Shunlong Luo and Shuangshuang Fu. Geometric measure of quantum discord. *Physical Review A*, 82(3):034302, 2010.

[274] Paolo Giorda and Matteo GA Paris. Gaussian quantum discord. *Physical review letters*, 105(2):020503, 2010.

[275] Guang-Ming Zhang and Xiaoguang Wang. Spin swapping operator as an entanglement witness for quantum heisenberg spin-s systems. *Journal of Physics A: Mathematical and General*, 39(26):8515, 2006.

[276] Mohamed Bourennane, Manfred Eibl, Christian Kurtsiefer, Sascha Gaertner, Harald Weinfurter, Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera. Experimental detection of multipartite entanglement using witness operators. *Physical review letters*, 92(8):087902, 2004.

[277] Guifré Vidal and Reinhard F Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, 2002.

[278] Rafał Demkowicz-Dobrzański, Andreas Buchleitner, Marek Kuś, and Florian Mintert. Evaluable multipartite entanglement measures: Multipartite concurrences as entanglement monotones. *Physical Review A*, 74(5):052303, 2006.

[279] Zhi-Hao Ma, Zhi-Hua Chen, Jing-Ling Chen, Christoph Spengler, Andreas Gabriel, and Marcus Huber. Measure of genuine multipartite entanglement with computable lower bounds. *Physical Review A*, 83(6):062325, 2011.

[280] Hari Prakash and Ajay K Maurya. Quantum teleportation using entangled 3-qubit states and the 'magic bases'. *Optics Communications*, 284(20):5024–5030, 2011.

[281] David Elieser Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. *Proc. R. Soc. Lond. A*, 449(1937):669–677, 1995.

[282] Yaoyun Shi. Both toffoli and controlled-not need little help to do universal quantum computation. *arXiv preprint quant-ph/0205115*, 2002.

[283] Jean-Luc Brylinski and Ranee Brylinski. Universal quantum gates. In *Mathematics of Quantum Computation*, pages 117–134. Chapman and Hall/CRC, 2002.

[284] Michael Hsieh, Julia Kempe, Simon Myrgren, and K Birgitta Whaley. An explicit universal gate-set for exchange-only quantum computation. *Quantum Information Processing*, 2(4):289–307, 2003.

[285] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[286] Jonathan A Jones. Robust ising gates for practical quantum computation. *Physical Review A*, 67(1):012317, 2003.

[287] Ferdinand Schmidt-Kaler, Hartmut Häffner, Mark Riebe, Stephan Gulde, Gavin PT Lancaster, Thomas Deuschle, Christoph Becher, Christian F Roos, Jürgen Eschner, and Rainer Blatt. Realization of the cirac–zoller controlled-not quantum gate. *Nature*, 422(6930):408, 2003.

[288] B Kraus and JI Cirac. Optimal creation of entanglement using a two-qubit gate. *Physical Review A*, 63(6):062309, 2001.

[289] Seth Lloyd. A potentially realizable quantum computer. *Science*, 261(5128):1569–1571, 1993.

[290] Isaac L Chuang and Yoshihisa Yamamoto. Simple quantum computer. *Physical Review A*, 52(5):3489, 1995.

[291] N David Mermin. *Quantum computer science: an introduction*. Cambridge University Press, 2007.

[292] Wolfgang Dur, Guifre Vidal, and J Ignacio Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62(6):062314, 2000.

[293] Frank Verstraete, Jeroen Dehaene, Bart De Moor, and Henri Verschelde. Four qubits can be entangled in nine different ways. *Physical Review A*, 65(5):052112, 2002.

[294] Tetsufumi Tanamoto, Yu-xi Liu, Xuedong Hu, and Franco Nori. Efficient quantum circuits for one-way quantum computing. *Physical review letters*, 102(10):100501, 2009.

[295] HP Barendregt. Lambda calculi with types, handbook of logic in computer science (vol. 2): background: computational structures, 1993.

[296] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Quantum circuit architecture. *Physical review letters*, 101(6):060401, 2008.

[297] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009.

[298] André Van Tonder. A lambda calculus for quantum computation. *SIAM Journal on Computing*, 33(5):1109–1135, 2004.

[299] Peter Selinger and Benoit Valiron. A lambda calculus for quantum computation with classical control. *Mathematical Structures in Computer Science*, 16(3):527–552, 2006.

[300] Timothy M Rambo, Joseph B Altepeter, Prem Kumar, and G Mauro D'Ariano. Functional quantum computing: An optical approach. *Physical Review A*, 93(5):052321, 2016.

[301] Daniel A Lidar and K Birgitta Whaley. Decoherence-free subspaces and subsystems. In *Irreversible quantum dynamics*, pages 83–120. Springer, 2003.

[302] Anthony J Leggett, SDAFMGA Chakravarty, AT Dorsey, Matthew PA Fisher, Anupam Garg, and W Zwerger. Dynamics of the dissipative two-state system. *Reviews of Modern Physics*, 59(1):1, 1987.

[303] Paolo Zanardi. Dissipative dynamics in a quantum register. *Physical Review A*, 56(6):4445, 1997.

[304] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127, 1998.

Chapter 7

Appendix 1: Vectors States

We find the vector states for the various number of qubits in our systems.

7.1 Three-Qubit Vector States

For this system, the magic-vector states are found to be as follows

$$|\psi_1\rangle = \frac{1}{\sqrt{6}}(|001\rangle + |100\rangle) - \sqrt{\frac{2}{3}}|010\rangle \tag{7.1}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |100\rangle) \tag{7.2}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{6}}(|011\rangle + |110\rangle) - \sqrt{\frac{2}{3}}|101\rangle \tag{7.3}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(-|011\rangle + |110\rangle) \tag{7.4}$$

$$|\psi_5\rangle = |000\rangle \tag{7.5}$$

$$|\psi_6\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100) \tag{7.6}$$

$$|\psi_7\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |110\rangle + |101) \tag{7.7}$$

$$|\psi_8\rangle = |111\rangle \tag{7.8}$$

7.2 Four-Qubit Vector States

$$|1\rangle = \frac{1}{2\sqrt{3}}(|0111\rangle + |1011\rangle + |1101\rangle) - \frac{\sqrt{3}}{2}|1110\rangle \tag{7.9}$$

$$|2\rangle = -\frac{\sqrt{2}}{\sqrt{3}}|0111\rangle + \frac{1}{\sqrt{6}}(|1011\rangle + |1101\rangle) \tag{7.10}$$

$$|3\rangle = -\frac{1}{\sqrt{2}}(|1011\rangle - |1101\rangle) \tag{7.11}$$

$$|4\rangle = \frac{1}{\sqrt{6}}(-|0011\rangle - |0101\rangle + |0110\rangle - |1001\rangle + |1010\rangle + |1100\rangle) \tag{7.12}$$

$$|5\rangle = \frac{1}{\sqrt{3}}(\frac{1}{2}|0011\rangle + \frac{1}{2}|0101\rangle + |0110\rangle - |1001\rangle - \frac{1}{2}|1010\rangle - \frac{1}{2}|1100\rangle) \tag{7.13}$$

$$|6\rangle = \frac{1}{2}(|0011\rangle - |0101\rangle + |1010\rangle - |1100\rangle) \tag{7.14}$$

$$|7\rangle = -\frac{\sqrt{3}}{2}|0001\rangle + \frac{1}{2\sqrt{3}}(|0010\rangle + |0100\rangle + |1000\rangle) \tag{7.15}$$

$$|8\rangle = \frac{1}{\sqrt{6}}(|0010\rangle + |0100\rangle) - \frac{\sqrt{2}}{\sqrt{3}}|1000\rangle \tag{7.16}$$

$$|9\rangle = \frac{1}{\sqrt{2}}(|0010\rangle - |0100\rangle) \tag{7.17}$$

$$|10\rangle = \frac{1}{\sqrt{3}}(\frac{1}{2}|0011\rangle + \frac{1}{2}|0101\rangle - |0110\rangle - |1001\rangle + \frac{1}{2}|1010\rangle + \frac{1}{2}|1100\rangle) \tag{7.18}$$

$$|11\rangle = \frac{1}{2}(|0011\rangle - |0101\rangle - |1010\rangle + |1100\rangle) \tag{7.19}$$

$$|12\rangle = |0000\rangle \tag{7.20}$$

$$|13\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \tag{7.21}$$

$$|14\rangle = \frac{1}{\sqrt{6}}(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle) \tag{7.22}$$

$$|15\rangle = \frac{1}{2}(|0111\rangle + |1011\rangle + |1101\rangle + |1110\rangle) \tag{7.23}$$

$$|16\rangle = |1111\rangle \tag{7.24}$$

7.3 Five-Vector Vector States

$$|1\rangle = \frac{1}{3\sqrt{2}}(-|00111\rangle - |01011\rangle + |01101\rangle + |01110\rangle - |10011\rangle + |10101\rangle + |10110\rangle + |11001\rangle + |11010\rangle) - \frac{1}{\sqrt{2}}(|11100\rangle) \quad (7.25)$$

$$|2\rangle = \frac{1}{6}(|01011\rangle - |01101\rangle + |10011\rangle - |10101\rangle) + \frac{1}{3}(-|00111\rangle + |01110\rangle + |10110\rangle + |11001\rangle - 2|11010\rangle) \quad (7.26)$$

$$|3\rangle = \frac{1}{\sqrt{3}}(-|00111\rangle - |11001\rangle) + \frac{1}{2\sqrt{3}}(|01011\rangle + |01101\rangle + |10011\rangle + |10101\rangle) \quad (7.27)$$

$$|4\rangle = \frac{1}{\sqrt{3}}(|01110\rangle + |10110\rangle) + \frac{1}{2\sqrt{3}}(-|01011\rangle - |01101\rangle + |10011\rangle + |10101\rangle) \quad (7.28)$$

$$|5\rangle = \frac{1}{2}(-|01011\rangle + |01101\rangle + |10011\rangle - |10101\rangle) \quad (7.29)$$

These states $\{|1\rangle, |2\rangle, |3\rangle, |4\rangle and |5\rangle\}$ form the first family of vector states associated to S_5 symmetric group.

$$|6\rangle = \frac{1}{3\sqrt{2}}(|00101\rangle + |00110\rangle + |01001\rangle + |01010\rangle - |01100\rangle + |10001\rangle + |10010\rangle - |10100\rangle - |11000\rangle) - \frac{1}{\sqrt{2}}(|00011\rangle) \quad (7.30)$$

$$|7\rangle = \frac{1}{3}(-2|00101\rangle + |00110\rangle + |01001\rangle + |10001\rangle - |11000\rangle) + \frac{1}{6}(-|01010\rangle + |01100\rangle - |10010\rangle + |10100\rangle) \quad (7.31)$$

$$|8\rangle = \frac{1}{\sqrt{3}}(-|00110\rangle - |11000\rangle) + \frac{1}{2\sqrt{3}}(|01010\rangle + |01100\rangle + |10010\rangle + |10100\rangle) \quad (7.32)$$

$$|9\rangle = \frac{1}{\sqrt{3}}(-|01001\rangle + |10001\rangle) + \frac{1}{2\sqrt{3}}(|01010\rangle + |01100\rangle - |10010\rangle - |10100\rangle) \quad (7.33)$$

$$|10\rangle = \frac{1}{2}(-|01010\rangle + |01100\rangle + |10010\rangle - |10100\rangle) \quad (7.34)$$

These states $\{|6\rangle,|7\rangle,|8\rangle,|9\rangle and|10\rangle\}$ form the second family of vector states associated to S_5 symmetric group.

$$|11\rangle = \frac{1}{2\sqrt{5}}(|00010\rangle + |00100\rangle + |01000\rangle + |10000\rangle) - \frac{2}{\sqrt{5}}|00001\rangle \tag{7.35}$$

$$|12\rangle = \frac{1}{2\sqrt{3}}(|00100\rangle + |01000\rangle + |10000\rangle) - \frac{\sqrt{3}}{2}|00010\rangle \tag{7.36}$$

$$|13\rangle = \frac{1}{\sqrt{6}}(|01000\rangle + |10000\rangle) - \sqrt{\frac{2}{3}}|00100\rangle \tag{7.37}$$

$$|14\rangle = \frac{1}{\sqrt{2}}(-|01000\rangle + |10000\rangle) \tag{7.38}$$

These states $\{|11\rangle,|12\rangle,|13\rangle and|14\rangle\}$ form the third family of vector states associated to S_5 symmetric group.

$$\begin{aligned}|15\rangle = \frac{1}{2}\sqrt{\frac{3}{5}}(-|00011\rangle - |00101\rangle - |01001\rangle - |10001\rangle) \\ + \frac{1}{\sqrt{15}}(|00110\rangle + |01010\rangle + |01100\rangle + |10010\rangle + |10100\rangle + |11000\rangle)\end{aligned} \tag{7.39}$$

$$\begin{aligned}|16\rangle = -\frac{1}{2}|00011\rangle + \frac{1}{3}(-|00110\rangle - |01010\rangle + |01100\rangle - |10010\rangle + |10100\rangle + |11000\rangle) \\ + \frac{1}{6}(|00101\rangle + |01001\rangle + |10001\rangle)\end{aligned} \tag{7.40}$$

$$\begin{aligned}|17\rangle = \frac{1}{3\sqrt{2}}(|01001\rangle + |01010\rangle - |01100\rangle + |10001\rangle + |10010\rangle - |10100\rangle) \\ + \frac{\sqrt{2}}{3}(-|00101\rangle - |00110\rangle + |1100\rangle)\end{aligned} \tag{7.41}$$

$$|18\rangle = \frac{1}{\sqrt{6}}(-|01001\rangle - |01010\rangle - |01100\rangle + |10001\rangle + |10010\rangle + |10100\rangle) \tag{7.42}$$

These states $\{|15\rangle,|16\rangle,|17\rangle and|18\rangle\}$ form the fourth family of vector states associated to S_5 symmetric group.

$$|19\rangle = \frac{1}{2\sqrt{5}}(|01111\rangle + |10111\rangle + |11011\rangle + |11101\rangle) - \frac{2}{\sqrt{5}}|11110\rangle \tag{7.43}$$

$$|20\rangle = \frac{1}{2\sqrt{3}}(|01111\rangle + |10111\rangle + |11011\rangle) - \frac{\sqrt{3}}{2}|11101\rangle \tag{7.44}$$

$$|21\rangle = \frac{1}{\sqrt{6}}(|01111\rangle + |10111\rangle) - \sqrt{\frac{2}{3}}|11011\rangle \tag{7.45}$$

$$|22\rangle = \frac{1}{\sqrt{2}}(|01111\rangle - |10111\rangle \tag{7.46}$$

These states $\{|19\rangle, |20\rangle, |21\rangle and |22\rangle\}$ form the fifth family of vector states associated to S_5 symmetric group.

$$|23\rangle = \frac{1}{\sqrt{15}}(|00111\rangle + |01011\rangle + |01101\rangle + |10011\rangle + |10101\rangle + |11001\rangle) + \frac{1}{2}\sqrt{\frac{3}{5}}(-|01110\rangle - |10110\rangle - |11010\rangle - |11100\rangle) \tag{7.47}$$

$$|24\rangle = \frac{1}{3}(|00111\rangle + |01011\rangle - |01101\rangle + |10011\rangle - |10101\rangle - |11001\rangle) + \frac{1}{6}(|01110\rangle + |10110\rangle + |11010\rangle) - \frac{1}{2}|11100\rangle \tag{7.48}$$

$$|25\rangle = \frac{1}{3\sqrt{2}}(-|01011\rangle + |01101\rangle + |01110\rangle - |10011\rangle + |10101\rangle + |10110\rangle) + \frac{\sqrt{2}}{3}(|00111\rangle - |11001\rangle - |11010\rangle) \tag{7.49}$$

$$|26\rangle = \frac{1}{\sqrt{6}}(|01011\rangle + |01101\rangle + |01110\rangle - |10011\rangle - |10101\rangle - |10110\rangle) \tag{7.50}$$

These states $\{|23\rangle, |24\rangle, |25\rangle and |26\rangle\}$ form the sixth family of vector states associated to S_5 symmetric group.

$$|27\rangle = |00000\rangle \tag{7.51}$$

$$|28\rangle = \frac{1}{\sqrt{5}}(|00001\rangle + |00010\rangle + |00100\rangle + |01000\rangle + |10000\rangle) \tag{7.52}$$

$$|29\rangle = \frac{1}{\sqrt{10}}(|00011\rangle + |00101\rangle + |00110\rangle + |01001\rangle + |01010\rangle + |01100\rangle + |10001\rangle + |10010\rangle + |10100\rangle + |11000\rangle) \tag{7.53}$$

$$|30\rangle = \frac{1}{\sqrt{10}}(|00111\rangle + |01011\rangle + |01101\rangle + |01110\rangle + |10011\rangle + |10101\rangle + |10110\rangle + |11001\rangle + |11010\rangle + |11100\rangle) \quad (7.54)$$

$$|31\rangle = \frac{1}{\sqrt{5}}(|01111\rangle + |10111\rangle + |11011\rangle + |11101\rangle + |11110\rangle) \quad (7.55)$$

$$|32\rangle = |11111\rangle \quad (7.56)$$

7.4 Six-Qubit Vector States

$$|1\rangle = -\sqrt{\frac{3}{5}}|000011\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|000101\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|000110\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|001001\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|001010\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|010001\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|010010\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|100001\rangle + \frac{1}{4}\sqrt{\frac{3}{5}}|100010\rangle + \frac{1}{2\sqrt{15}}(-|001100\rangle - |010100\rangle - |011000\rangle - |100100\rangle - |101000\rangle - |110000\rangle) \quad (7.57)$$

$$|2\rangle = -\frac{3}{4}|000101\rangle + \frac{1}{4}(|000110\rangle + |001001\rangle + |010010\rangle + |100001\rangle) + \frac{1}{12}(-|001010\rangle - |010010\rangle - |100010\rangle) + \frac{1}{6}(|001100\rangle + |010100\rangle - |011000\rangle + |100100\rangle - |101000\rangle - |110000\rangle) \quad (7.58)$$

$$|3\rangle = \frac{1}{\sqrt{2}}(-|000110\rangle) + \frac{1}{3\sqrt{2}}(|001100\rangle + |001100\rangle + |010010\rangle + |010100\rangle - |011000\rangle + |100010\rangle + |100100\rangle - |101000\rangle - |110000\rangle) \quad (7.59)$$

$$|4\rangle = \frac{1}{\sqrt{2}}(-|001001\rangle) + \frac{1}{3\sqrt{2}}(|001010\rangle + |001100\rangle - |110000\rangle) + \frac{1}{2\sqrt{2}}(|010001\rangle + |100001\rangle) + \frac{1}{6\sqrt{2}}(-|010010\rangle - |010100\rangle + |011000\rangle - |100010\rangle - |100100\rangle + |101000\rangle) \quad (7.60)$$

$$|5\rangle = \frac{1}{3}(-2|001010\rangle + |001100\rangle + |010010\rangle + |100010\rangle - |110000\rangle) + \frac{1}{6}(-|010100\rangle + |011000\rangle - |100100\rangle + |101000\rangle) \quad (7.61)$$

$$|6\rangle = \frac{1}{\sqrt{3}}(-|001100\rangle - |110000\rangle) + \frac{1}{2\sqrt{3}}(|010100\rangle + |011000\rangle + |100100\rangle + |101000\rangle) \quad (7.62)$$

$$|7\rangle = \frac{1}{2}\sqrt{\frac{3}{2}}(-|010001\rangle + |100001\rangle) + \frac{1}{2\sqrt{6}}(|010010\rangle + |010100\rangle + |011000\rangle - |100010\rangle - |100100\rangle - |101000\rangle) \quad (7.63)$$

$$|8\rangle = \frac{1}{\sqrt{3}}(-|010010\rangle + |100010\rangle) + \frac{1}{2\sqrt{3}}(|010100\rangle + |011000\rangle - |100100\rangle - |101000\rangle) \quad (7.64)$$

$$|9\rangle = \frac{1}{2}(-|010100\rangle + |011000\rangle + |100100\rangle - |101000\rangle) \quad (7.65)$$

This forms the first family of 9 vectors.

$$|10\rangle = \frac{1}{2}\sqrt{\frac{3}{10}}(-|000111\rangle - |001011\rangle - |010011\rangle - |011100\rangle - |100011\rangle - |101100\rangle - |110100\rangle - |111000\rangle) + \frac{1}{\sqrt{30}}(|001101\rangle + |001110\rangle + |010101\rangle + |010110\rangle + |011001\rangle + |011010\rangle + |100101\rangle + |100110\rangle + |101001\rangle + |101010\rangle + |110001\rangle + |110010\rangle) \quad (7.66)$$

$$|11\rangle = \frac{1}{2\sqrt{2}}(-|000111\rangle - |111000\rangle) + \frac{1}{3\sqrt{2}}(-|001101\rangle + |001110\rangle - |010101\rangle + |010110\rangle + |011001\rangle - |011010\rangle - |100101\rangle + |100110\rangle + |101001\rangle - |101010\rangle + |110001\rangle - |110010\rangle) + \frac{1}{6\sqrt{2}}(|001011\rangle + |010011\rangle + |011100\rangle + |100011\rangle + |101100\rangle + |110100\rangle) \quad (7.67)$$

$$|12\rangle = \frac{1}{2}(-|000111\rangle - |111000\rangle) + \frac{1}{6}(|001011\rangle + |001101\rangle - |001110\rangle + |010011\rangle + |010101\rangle - |010110\rangle - |011001\rangle + |011010\rangle + |011100\rangle + |100011\rangle + |100101\rangle - |100110\rangle - |101001\rangle + |101010\rangle + |101100\rangle - |110001\rangle + |110010\rangle + |110100\rangle) \quad (7.68)$$

$$|13\rangle = \frac{1}{3}(-|001011\rangle - |001101\rangle + |001110\rangle + |110001\rangle - |110010\rangle - |110100\rangle) + \frac{1}{6}(|010011\rangle + |010101\rangle - |010110\rangle - |011001\rangle + |011010\rangle + |011100\rangle + |100011\rangle + |100101\rangle - |100110\rangle - |101001\rangle + |101010\rangle + |101100\rangle) \quad (7.69)$$

$$|14\rangle = \frac{\sqrt{2}}{3}(-|001011\rangle - |110100\rangle) + \frac{1}{3\sqrt{2}}(|001101\rangle - |001110\rangle + |010011\rangle + |011100\rangle + |100011\rangle + |101100\rangle - |110001\rangle + |110010\rangle) + \frac{1}{6\sqrt{2}}(-|010101\rangle + |010110\rangle + |011001\rangle - |011010\rangle - |100101\rangle + |100110\rangle + |101001\rangle - |101010\rangle) \quad (7.70)$$

$$|15\rangle = \frac{1}{\sqrt{6}}(|001101\rangle - |001110\rangle - |110001\rangle - |110010\rangle) + \frac{1}{2\sqrt{6}}(|010101\rangle + |010110\rangle + |011001\rangle + |011010\rangle + |100101\rangle + |100110\rangle + |101001\rangle + |101010\rangle) \quad (7.71)$$

$$|16\rangle = \frac{1}{2\sqrt{3}}(-|010011\rangle - |010101\rangle + |010110\rangle - |011001\rangle + |011010\rangle + |011100\rangle + |100011\rangle + |100101\rangle - |100110\rangle + |101001\rangle - |101010\rangle - |101100\rangle) \quad (7.72)$$

$$|17\rangle = \frac{1}{\sqrt{6}}(-|010011\rangle + |011100\rangle + |100011\rangle - |101100\rangle) + \frac{1}{2\sqrt{6}}(|010101\rangle - |010110\rangle + |011001\rangle - |011010\rangle - |100101\rangle + |100110\rangle - |101001\rangle + |101010\rangle) \quad (7.73)$$

$$|18\rangle = \frac{1}{2\sqrt{2}}(-|010101\rangle - |010110\rangle + |011001\rangle + |011010\rangle + |100101\rangle + |100110\rangle - |101001\rangle - |101010\rangle) \quad (7.74)$$

These nine vectors form the second family for S6.

$$|19\rangle = \frac{1}{4}\sqrt{\frac{3}{5}}(-|011101\rangle - |011110\rangle - |101101\rangle - |101110\rangle - |110101\rangle - |110110\rangle - |111001\rangle - |111010\rangle) + \frac{1}{2\sqrt{15}}(|001111\rangle + |010111\rangle + |011011\rangle + |100111\rangle + |101011\rangle + |110011\rangle) + \sqrt{\frac{3}{5}}|111100\rangle \quad (7.75)$$

$$|20\rangle = \frac{1}{4}(-|011110\rangle - |101110\rangle - |110110\rangle - |111001\rangle + 3|111010\rangle) + \frac{1}{6}(|001111\rangle + |010111\rangle - |011011\rangle + |100111\rangle - |101011\rangle - |110011\rangle) + \frac{1}{12}(|011101\rangle + |101101\rangle + |110101\rangle) \quad (7.76)$$

$$|21\rangle = \frac{1}{3\sqrt{2}}(|001111\rangle + |010111\rangle - |011011\rangle - |011101\rangle + |100111\rangle - |101011\rangle - |101101\rangle - |110011\rangle - |110101\rangle) + \frac{1}{\sqrt{2}}|111001\rangle \quad (7.77)$$

$$|22\rangle = \frac{1}{\sqrt{2}}|110110\rangle + \frac{1}{2\sqrt{2}}(-|011110\rangle - |101110\rangle) + \frac{1}{3\sqrt{2}}(|001111\rangle - |110011\rangle - |110101\rangle) + \frac{1}{6\sqrt{2}}(-|010111\rangle + |011011\rangle + |011101\rangle - |100111\rangle + |101011\rangle + |101101\rangle) \quad (7.78)$$

$$|23\rangle = \frac{1}{3}(|001111\rangle - |011101\rangle - |101101\rangle - |110011\rangle + 2|110101\rangle) + \frac{1}{6}(-|010111\rangle + |011011\rangle - |100111\rangle + |101011\rangle) \quad (7.79)$$

$$|24\rangle = \frac{1}{\sqrt{3}}(|001111\rangle + |110011\rangle) + \frac{1}{2\sqrt{3}}(-|010111\rangle - |011011\rangle - |100111\rangle - |101011\rangle) \quad (7.80)$$

$$|25\rangle = \frac{1}{2}\sqrt{\frac{3}{2}}(-|011110\rangle + |101110\rangle) + \frac{1}{2\sqrt{6}}(|010111\rangle + |011011\rangle + |011101\rangle - |100111\rangle - |101011\rangle - |101101\rangle) \quad (7.81)$$

$$|26\rangle = \frac{1}{2\sqrt{3}}(|010111\rangle + |011011\rangle - |100111\rangle - |101011\rangle) + \frac{1}{\sqrt{3}}(-|011101\rangle + |101101\rangle) \quad (7.82)$$

$$|27\rangle = \frac{1}{2}(|010111\rangle - |011011\rangle - |100111\rangle + |101011\rangle) \quad (7.83)$$

These nine vectors form the third family for S6.

$$|28\rangle = \frac{1}{2}(-|000111\rangle + |111000\rangle) + \frac{1}{6}(|001011\rangle + |001101\rangle + |001110\rangle + |010011\rangle + |010101\rangle + |010110\rangle - |011001\rangle - |011010\rangle - |011100\rangle + |100011\rangle + |100101\rangle + |100110\rangle - |101001\rangle - |101010\rangle - |101100\rangle - |110001\rangle - |110010\rangle - |110100\rangle) \quad (7.84)$$

$$|29\rangle = \frac{\sqrt{2}}{3}(|001011\rangle + |110100\rangle) + \frac{1}{3\sqrt{2}}(|001101\rangle + |001110\rangle + |010011\rangle - |011100\rangle + |100011\rangle - |101100\rangle - |110001\rangle - |110010\rangle) + \frac{1}{6\sqrt{2}}(-|010101\rangle - |010110\rangle + |011001\rangle + |011010\rangle - |100101\rangle - |100110\rangle - |101001\rangle + |101010\rangle) \quad (7.85)$$

$$|30\rangle = \frac{1}{\sqrt{6}}(-|001101\rangle + |001110\rangle - |110001\rangle + |110010\rangle) + \frac{1}{2\sqrt{6}}(|010101\rangle - |010110\rangle + |011001\rangle - |011010\rangle + |100101\rangle - |100110\rangle + |101001\rangle - |101010\rangle) \quad (7.86)$$

$$|31\rangle = \frac{1}{\sqrt{6}}(|010011\rangle - |011100\rangle + |100011\rangle + |101100\rangle) + \frac{1}{2\sqrt{6}}(|010101\rangle + |010110\rangle + |011001\rangle + |011010\rangle - |100101\rangle - |100110\rangle - |101001\rangle - |101010\rangle) \quad (7.87)$$

$$|32\rangle = \frac{1}{2\sqrt{2}}(-|010101\rangle + |010110\rangle + |011001\rangle - |011010\rangle + |100101\rangle - |100110\rangle - |101001\rangle + |101010\rangle) \quad (7.88)$$

These five vectors form the fourth family for S6.

$$|33\rangle = -\sqrt{\frac{5}{6}}|00001\rangle + \frac{1}{\sqrt{30}}(|000010\rangle + |000100\rangle + |001000\rangle + |010000\rangle + |100000\rangle) \quad (7.89)$$

$$|34\rangle = \frac{1}{2\sqrt{5}}(|000100\rangle + |001000\rangle + |010000\rangle + |100000\rangle) - \frac{2}{\sqrt{5}}|000010\rangle \quad (7.90)$$

$$|35\rangle = -\frac{\sqrt{3}}{2}|000100\rangle + \frac{1}{2\sqrt{3}}(|001000\rangle + |010000\rangle + |100000\rangle) \quad (7.91)$$

$$|36\rangle = -\sqrt{\frac{2}{3}}|001000\rangle + \frac{1}{\sqrt{6}}(|010000\rangle + |100000rangle) \quad (7.92)$$

$$|37\rangle = \frac{1}{\sqrt{2}}(|100000\rangle - |010000\rangle) \quad (7.93)$$

This forms the fifth family for S6.

$$|38\rangle = \sqrt{\frac{2}{15}}(-|000011\rangle - |000101\rangle - |001001\rangle - |010001\rangle - |100001\rangle) + \frac{1}{\sqrt{30}}(|000110\rangle + |001010\rangle + |001100\rangle + |010010\rangle + |010100\rangle + |011000\rangle + |100010\rangle + |100100\rangle + |101000\rangle + |110000\rangle) \quad (7.94)$$

$$|39\rangle = \frac{1}{\sqrt{5}}|000011\rangle + \frac{1}{4\sqrt{5}}(|000101\rangle - 3|000110\rangle + |001001\rangle - 3|001010\rangle + |010001\rangle - 3|010010\rangle + |100001\rangle - 3|100010\rangle) + \frac{1}{2\sqrt{5}}(|001100\rangle + |010100\rangle + |011000\rangle + |100100\rangle + |101000\rangle + |110000\rangle) \quad (7.95)$$

$$|40\rangle = \frac{\sqrt{3}}{4}(-|000101\rangle - |000110\rangle) + \frac{1}{4\sqrt{3}}(|001001\rangle + |001010\rangle + |010001\rangle + |010010\rangle + |100001\rangle + |100010\rangle) + \frac{1}{2\sqrt{3}}(-|001100\rangle - |010100\rangle + |011000\rangle - |100100\rangle + |101000\rangle + |110000\rangle)) \quad (7.96)$$

$$|41\rangle = \frac{1}{\sqrt{6}}(-|001001\rangle - |001010\rangle - |001100\rangle + |110000\rangle) + \frac{1}{2\sqrt{6}}(|010001\rangle + |010010\rangle + |010100\rangle - |011000\rangle + |100001\rangle + |100010\rangle + |100100\rangle - |101000\rangle) \quad (7.97)$$

$$|42\rangle = \frac{1}{2\sqrt{2}}(-|010001\rangle - |010010\rangle - |010100\rangle - |011000\rangle + |100001\rangle + |100010\rangle + |100100\rangle + |101000\rangle) \quad (7.98)$$

This forms the sixth family of S6.

$$|43\rangle = \frac{1}{2\sqrt{5}}(-|000111\rangle - |001011\rangle - |001101\rangle + |001110\rangle - |010011\rangle - |010101\rangle + |010110\rangle - |011001\rangle + |011010\rangle + |011100\rangle - |100011\rangle - |100101\rangle + |100110\rangle - |101001\rangle + |101010\rangle + |101100\rangle - |110001\rangle + |110010\rangle + |110100\rangle + |111000\rangle) \quad (7.99)$$

$$|44\rangle = \frac{1}{2}\sqrt{\frac{3}{10}}(-|000111\rangle - |001011\rangle - |010011\rangle + |011100\rangle - |100011\rangle + |101100\rangle + |110100\rangle + |111000\rangle) + \frac{1}{\sqrt{30}}(|001101\rangle - |001110\rangle + |010101\rangle - |010110\rangle + |011001\rangle - |011010\rangle + |100101\rangle - |100110\rangle + |101001\rangle - |101010\rangle + |110001\rangle - |110010\rangle) \quad (7.100)$$

$$|45\rangle = \frac{1}{2\sqrt{2}}(-|000111\rangle + |111000\rangle) + \frac{1}{3\sqrt{2}}(-|001101\rangle - |001110\rangle - |010101\rangle - |010110\rangle + |011001\rangle + |011010\rangle - |10010\rangle - |100110\rangle + |101001\rangle + |101010\rangle + |110001\rangle + |110010\rangle) + \frac{1}{6\sqrt{2}}(|001011\rangle + |010011\rangle - |011100 + |100011\rangle - |101100\rangle - |110100\rangle) \quad (7.101)$$

$$|46\rangle = \frac{1}{3}(-|001011\rangle - |001101\rangle - |001110\rangle + |110001\rangle + |110010\rangle + |110100\rangle)$$
$$+ \frac{1}{6}(|010011\rangle + |010101\rangle + |010110\rangle - |011001\rangle - |011010\rangle - |011100\rangle + |100011\rangle$$
$$+ |100101\rangle + |100110\rangle - |101001\rangle - |101010\rangle - |101100\rangle) \quad (7.102)$$

$$|47\rangle = \frac{1}{2\sqrt{3}}(-|010011\rangle - |010101\rangle - |010110\rangle - |011001\rangle - |011010\rangle - |011100\rangle$$
$$+ |100011\rangle + |100101\rangle + |100110\rangle + |101001\rangle + |101010\rangle + |101100\rangle) \quad (7.103)$$

This forms the seventh family of S6.

$$|48\rangle = \sqrt{\frac{2}{15}}(-|011110\rangle - |101110\rangle - |110110\rangle - |111010 - |111100\rangle)$$
$$+ \frac{1}{\sqrt{30}}(|001111\rangle + |010111\rangle + |011011\rangle + |011101\rangle + |100111\rangle + |101011\rangle$$
$$+ |101101\rangle + |110011\rangle + |110101\rangle + |111001\rangle) \quad (7.104)$$

$$|49\rangle = \frac{1}{2\sqrt{5}}(|001111\rangle + |010111\rangle + |011011\rangle + |100111\rangle + |101011\rangle + |110011\rangle)$$
$$+ \frac{1}{4\sqrt{5}}(-3|011101\rangle + |011110\rangle - 3|101101\rangle + |101110\rangle - 3|110101\rangle$$
$$+ |110110\rangle - 3|111001\rangle + |111010\rangle) - \frac{1}{\sqrt{5}}|111100\rangle \quad (7.105)$$

$$|50\rangle = \frac{1}{2\sqrt{3}}(|001111\rangle + |010111\rangle - |011011\rangle + |100111\rangle - |101011\rangle - |110011\rangle)$$
$$+ \frac{1}{4\sqrt{3}}(|011101\rangle + |011110\rangle + |101101\rangle + |101110\rangle + |110101\rangle + |110110\rangle)$$
$$+ \frac{\sqrt{3}}{4}(-|111001\rangle - |111010\rangle) \quad (7.106)$$

$$|51\rangle = \frac{1}{\sqrt{6}}(|001111\rangle - |110011\rangle - |110101\rangle - |110110) + \frac{1}{2\sqrt{6}}(-|010111\rangle + |011011\rangle + |011101\rangle + |011110\rangle - |100111\rangle + |101011\rangle + |101101\rangle + |101110\rangle) \quad (7.107)$$

$$|52\rangle = \frac{1}{2\sqrt{2}}(|010111\rangle + |011011\rangle + |011101\rangle + |011110\rangle - |100111\rangle - |101011\rangle - |101101\rangle - |101110\rangle) \quad (7.108)$$

This forms the eighth family of S6.

$$|53\rangle = \frac{1}{\sqrt{30}}(|011111\rangle + |101111\rangle + |110111\rangle + |111011\rangle + |111101\rangle) - \sqrt{\frac{5}{6}}|111110\rangle \quad (7.109)$$

$$|54\rangle = \frac{1}{2\sqrt{5}}(|011111\rangle + |101111\rangle + |110111\rangle + |111011\rangle) - \frac{2}{\sqrt{5}}|111101\rangle \quad (7.110)$$

$$|55\rangle = \frac{1}{2\sqrt{3}}(|011111\rangle + |101111\rangle + |110111\rangle) - \frac{\sqrt{3}}{2}|111011\rangle \quad (7.111)$$

$$|56\rangle = \frac{1}{\sqrt{6}}(|011111\rangle + |101111\rangle) - \sqrt{\frac{2}{3}}|110111\rangle \quad (7.112)$$

$$|57\rangle = \frac{1}{\sqrt{2}}(|011111\rangle - |101111\rangle) \quad (7.113)$$

This forms the ninth family of S6.

$$|58\rangle = |000000\rangle \quad (7.114)$$

$$|59\rangle = \frac{1}{\sqrt{6}}(|000001\rangle + |000010\rangle + |000100\rangle + |001000\rangle + |010000\rangle + |100000\rangle) \quad (7.115)$$

$$|60\rangle = \frac{1}{2\sqrt{5}}(|000111\rangle + |001011\rangle + |001101\rangle + |001110\rangle + |010011\rangle + |010101\rangle + |010110\rangle + |011001\rangle + |011010\rangle + |011100\rangle + |100011\rangle + |100101\rangle + |100110\rangle + |101001\rangle + |101010\rangle + |101100\rangle + |110001\rangle + |110010\rangle + |110100\rangle + |111000\rangle) \quad (7.116)$$

$$|61\rangle = \frac{1}{\sqrt{15}}(|001111\rangle + |010111\rangle + |011011\rangle + |011101\rangle + |011110\rangle + |100111\rangle + |101011\rangle + |101101\rangle + |101110\rangle + |110011\rangle + |110101\rangle + |110110\rangle + |111001\rangle + |111010\rangle + |111000\rangle) \quad (7.117)$$

$$|62\rangle = \frac{1}{\sqrt{6}}(|011111\rangle + |101111\rangle + |110111\rangle + |111011\rangle + |111101\rangle + |111110\rangle) \quad (7.118)$$

$$|63\rangle = \frac{1}{\sqrt{15}}(|000011\rangle + |000101\rangle + |000110\rangle + |001001\rangle + |001010\rangle + |001100\rangle + |010001\rangle + |010010\rangle + |010100\rangle + |011000\rangle + |100001\rangle + |100010\rangle + |100100\rangle + |101000\rangle + |110000\rangle) \quad (7.119)$$

$$|64\rangle = |111111\rangle \quad (7.120)$$

Chapter 8

Appendix 2: Distance Measures and Nearest Separable Neighbours

The values of the distance measure and the nearest separable states for our four-qubit vector states are as follows:

Vector State	G	Nearest Separable State
$\|\psi_1^{(4)}\rangle$	0.517638	-$\|1110\rangle$
$\|\psi_2^{(4)}\rangle$	0.605811	-$\|0111\rangle$
$\|\psi_3^{(4)}\rangle$	0.765367	-$\|1101\rangle$
$\|\psi_4^{(4)}\rangle$	1.087889	-$\|0011\rangle$/-$\|0101\rangle$/$\|0110\rangle$/-$\|1001\rangle$/$\|1010\rangle$/$\|1100\rangle$
$\|\psi_5^{(4)}\rangle$	0.919402	$\|0110\rangle$/-$\|1001\rangle$
$\|\psi_6^{(4)}\rangle$	1	$\|0011\rangle$/-$\|0101\rangle$/$\|1010\rangle$/-$\|1100\rangle$
$\|\psi_7^{(4)}\rangle$	0.517638	$\|0001\rangle$
$\|\psi_8^{(4)}\rangle$	0.605811	-$\|1000\rangle$
$\|\psi_9^{(4)}\rangle$	0.765367	$\|0010\rangle$
$\|\psi_{10}^{(4)}\rangle$	0.919402	-$\|0110\rangle$/-$\|1001\rangle$
$\|\psi_{11}^{(4)}\rangle$	1	$\|0011\rangle$/-$\|0101\rangle$/-$\|1010\rangle$/$\|1100\rangle$
$\|\psi_{12}^{(4)}\rangle$	0	$\|0000\rangle$
$\|\psi_{13}^{(4)}\rangle$	1	$\|0001\rangle$/$\|0010\rangle$/$\|0100\rangle$/$\|1000\rangle$
$\|\psi_{14}^{(4)}\rangle$	1.087889	$\|0011\rangle$/$\|0101\rangle$/$\|0110\rangle$/$\|1001\rangle$/$\|1010\rangle$/$\|1100\rangle$
$\|\psi_{15}^{(4)}\rangle$	1	$\|0111\rangle$/$\|1011\rangle$/$\|1101\rangle$/$\|1110\rangle$
$\|\psi_{16}^{(4)}\rangle$	0	$\|1111\rangle$