Classical Simulation of Restricted Cluster State Quantum Circuits

Michael Garn

Department of Mathematics
Brunel University London

This dissertation is submitted for the degree of
Doctor of Philosophy

November 2023

Abstract

A fundamental open problem in quantum computing is to understand when quantum systems can or cannot be efficiently classically simulated. In this thesis, we study when cluster state quantum circuits with alternative input states (parameterised by a radius r) and measurements in the Z basis and XY-plane, can or cannot be efficiently classically simulated.

In the first part of this thesis, we study when such a system can be efficiently classically simulated. The main technical tool we consider is a generalised notion of separability in terms of cylindrical operators. We first show that if a CZ gate acts on cylindrical operators with radius r, then the output can be given a separable decomposition provided the radius of the cylindrical operators in the decomposition grows by a constant $\lambda > 0$. By combining this with a modified version of a previous algorithm, we find that this enables an efficient classical simulation algorithm that can sample from the output distribution to within additive error. We then use a coarse-graining approach to increase the range of input states that can be efficiently classically simulated. We then compute the equivalent of λ for arbitrary diagonal two-qubit gates. Lastly, we use alternative notions of entanglement to show that there are state spaces that can improve the region of input states that can be classically simulated.

In the second part, we examine potential obstacles that may arise when attempting to efficiently classically simulate an increased range of quantum input states. Using a percolation based approach, we show that if the input states are permitted with sufficient radius, then BQP can be supported and efficient classical simulation is unlikely. Furthermore, using conjectures about the polynomial hierarchy, we show that there is a threshold for which cluster states with alternative inputs cannot be efficiently classically simulated with multiplicative error.

Acknowledgements

I would like to first and foremost thank my supervisor, Shashank Virmani, for his invaluable support and guidance. His expertise, enthusiasm, and encouragement have been instrumental in guiding me through this PhD. I would also like to extend my thanks to Ilia Krasikov and Dalia Chakrabarty who have supported me through my PhD experience. I would like to thank my collaborators and friends, Sahar Atallah and David Tao, who have been involved in the projects that make up this PhD. I would also like to gratefully acknowledge the support of an EPSRC DTP award and a Prachi Dwivedi award, as well as an LMS Early Career Research Travel Grant and an IMA Small Grant Award.

I would like to acknowledge my friends Liam and Tom, who have been by my side since my first days as an undergraduate. I would like to express my gratitude to my parents and, of course, my brother Dominic for their continuous support and encouragement throughout my educational journey. Finally, special thanks go to Sophie for her continuous support, encouragement, and understanding that has been a constant source of motivation throughout this journey.

Table of contents

Chapter 1

Introduction

1.1 Overview

It is believed that quantum computers can potentially solve certain problems more efficiently than classical computers [1, 2]. However, it is not fully understood how and why these quantum algorithms provide a quantum speed-up. Finding the source of this speedup is an open problem, that is, what features of a quantum computation are necessary to provide an advantage over classical computations? This question can be answered by investigating when a quantum computer can or cannot be efficiently classically simulated. Moreover, what we mean is that if we restrict certain aspects of a quantum computation, can it be efficiently classically simulated? We will refer to these models of computing as restricted models of quantum computing. Restricted models of quantum computing can be useful as they allow us to probe the boundary between quantum and classical computation and, from a practical point of view, they can describe situations where there are experimental restrictions.

One way to address this question is to consider when can we efficiently classically simulate a quantum computation. A theorem that contributes towards answering this question is the celebrated Gottesman-Knill theorem [3]. It states that, quantum circuits, composed of Clifford gates and Pauli measurements, can be efficiently classically simulated. Subsequent research has also explored extensions to the Gottesman-Knill theorem, aiming to quantify and identify the resources that enable the full power of quantum computation [4, 5]. A widely studied feature of quantum computing, believed to contribute to its advantage over classical computing, is entanglement. It has been shown that in some settings, a lack of, or limited amount of entanglement can lead to efficient classical simulation algorithms [4, 6–8]. On the other hand, it has also been shown that weak amounts of entanglement can be sufficient for quantum computation [9, 10]. A useful way to investigate the feature of entanglement is

provided in the setting of measurement-based quantum computing [11, 12]. In this setting, entanglement is already present in the resource state, and operations are carried out in the form of measurements. In this thesis, we explore the computational power of such a model by considering a specified set of measurements and varying the input state. In particular, a key tool will be the notion of generalised entanglement [13, 14], which can be leveraged to enable a new type of classical simulation algorithm [15].

On the other hand, we can consider when a restricted model of quantum cannot be efficiently classically simulated. However, we currently have limited tools and methods for determining this. An approach to demonstrate classical intractability of a restricted model is to add certain features to it and show that it can nevertheless support universal quantum computation. This, in turn, makes it highly unlikely for the restricted model to be efficiently simulated classically. Another approach stemming from recent quantum supremacy experiments [16–18] has been developed, which can rule out efficient classical simulation of quantum computations based on widely believed complexity-theoretic conjectures [19–22]. Moreover, this approach has also been used to establish that some restricted models of quantum computing are hard to classically simulate [23–25]. Recent research in this direction has further focused on strengthening the conjectures and considering settings involving noise [26–29].

1.2 Organisation and Results of Thesis

This thesis is partly based on:

[30]: S. Atallah, M. Garn, S. Jevtic, Y. Tao, and S. Virmani, "Efficient classical simulation of cluster state quantum circuits with alternative inputs," arXiv preprint arXiv:2201.07655, 2022.

[31] S. Atallah, M. Garn, Y. Tao, and S. Virmani, "Classically efficient regimes in measurement based quantum computation performed using diagonal two qubit gates and cluster measurements," arXiv preprint arXiv:2307.01800, 2023.

In this thesis, we explore the computational power of cluster state quantum circuits with alternative inputs. In the first half of this thesis, we show that such a system can be efficiently classically simulated. In the second half, we examine potential obstacles that may arise when attempting to efficiently classically simulate an increased range of quantum input states. In further detail, this thesis is organised as follows.

In chapter 2, we begin by reviewing preliminary material. We then introduce measurement-based quantum computing (MBQC) and explain how it enables universal quantum computing. By modifying the inputs states to a typical MBQC scheme, we will see that we end up with a restricted model of quantum computation, which we refer to as a cluster state with alternative inputs. We then introduce the notion of generalised entanglement, which will serve as one of the main technical tools in this thesis. Lastly, we define what it means to simulate a quantum computation, before reviewing some important results in classical simulation.

In chapter 3, we study when a cluster state with alternative inputs can be efficiently classically simulated. The main tool that we will use is a generalised notion of entanglement. This notion allows for operators that return non-negative probabilities for the permitted measurements. Applying this notion to the cluster state systems we consider, where the permitted measurements are XY-plane and Z-basis measurements (i.e. measurements with projectors of the form: $(I+Z)/2$ and $(I+\cos\theta X+\sin\theta Y)/2$), allows us to consider operators that are drawn from cylindrically shaped state spaces. That is, we permit operators to be drawn from the following set:

$$\mathrm{Cyl}(r) := \{\rho | \rho = \rho^{\dagger}, \mathrm{Tr}\rho = 1, x^2+y^2 \leq r^2, z \in [-1,1]\}, \tag{1.1}$$

with $r \leq 1$, and where x,y,z are the Bloch expansion coefficients of ρ. In Sec.3.2.2, we present our first result that a CZ gate that acts on input operators that are drawn from cylinders of radius r, can be given a separable decomposition if the operators in the separable decomposition are drawn from cylinders of radius λr, with constant $\lambda > 0$. By combining this result with an existing classical algorithm (for systems that do not generate quantum entanglement) we develop a classical simulation algorithm based on cylinder radii growth. This provides lower bounds for regions of input cylinders, initialised with $r \leq 1/\lambda^D$, where D is the degree of the lattice, that can be efficiently classically simulated.

In chapter 4, we then focus on ways to improve and generalise our classical simulation algorithm. First, in Sec.4.2, we show that by considering a coarse graining approach, we can improve the bound on the parameter r that can be efficiently classically simulated. The idea of the approach is to partition the underlying lattice into blocks and treating each block as a single particle on a new lattice. Then by constructing separable decompositions over these blocks, we can analytically show that we can increase r for which we can efficiently classically simulate.

In Sec.4.3, we explicitly compute λ for any two-qubit diagonal gate, thus generalising and extending the result of Sec.3.2.2 beyond CZ gates. This result demonstrates that, for any finite-degree graph, a two-parameter family of pure entangled quantum states can be efficiently classically simulated within a non-trivial region for the permitted measurements. Consequently, for these systems, we are able to plot figures (see fig 4.6) that include regions that can be efficiently classically simulated. Note that the proof of this result uses similar techniques based on cylinder separability as in Sec.3.2.2.

The classical simulation methods presented so far are in the context of input state spaces that are cylinders. However, as we are ultimately only interested in simulating systems with quantum inputs, we may wonder whether it is possible to change our state spaces to obtain a greater range of quantum inputs that can be efficiently simulated classically. In Sec.4.4 we investigate this problem with linear programming methods. In Sec.4.4.4, we show that the range of r can be very slightly improved if one considers a state space (that we refer to as the Cylinder-Cone state space) that allows for variations in the height of the extremal points of that set. This demonstrates that the bounds on r are not tight, suggesting that there may be potential alternative methods that can expand the region of r that can be classically simulated.

In chapter 5, we examine potential obstacles that may arise when attempting to efficiently classically simulate an increased range of quantum input states. Moreover, we consider two approaches, based on percolation and quantum supremacy arguments, that potentially rule out efficient classical simulation for cluster state quantum circuits with input states of sufficient radius.

Using the first approach, based on percolation, we demonstrate in Sec.5.2.2 that a restricted cluster state on a degree 5 lattice, with input states of sufficient radius, can efficiently prepare a 2D cluster state. The underlying idea is that if the probability of successfully creating a $|+\rangle$ state on unmeasured qubits exceeds a threshold determined by the lattice's percolation thresholds, it becomes possible to implement a cluster state quantum computation.

The second approach is based on the quantum supremacy arguments [16], which show that if widely-believed complexity theoretic conjectures hold, then there cannot exist an efficient classical simulation algorithm. These arguments were developed in [19], in which it was show, that if IQP circuits could be weakly classically simulated up to multiplicative error, then this would cause the so-called polynomial hierarchy to collapse. Using similar arguments, we will show in Sec.5.3.2 that a cluster state on a degree 5 lattice, with input states

initialised with radii above $r_c = 0.3398$, cannot be classically simulated up to multiplicative error. As a next step, we would want to rule out efficient classical simulation of cluster states with alternative inputs under the more realistic notion of additive error. However, in this direction, we encountered challenges in applying previous existing methods [20, 21] and were unable to show this for the systems we were considering. Nevertheless, in Sec.5.3.3 we will briefly review the works of [32–34] that show how the approach has been adapted to cluster states with perfect inputs but with restrictions on the permitted measurements.

Chapter 2

Preliminaries

In this chapter, we will first introduce basic concepts from quantum information theory. In Sec.2.2 we will then give an overview of the principles of measurement-based quantum computing, followed by Sec.2.4 where we introduce a generalised notion of entanglement. Lastly, in Sec.2.5 we give an overview of classical simulation results that are relevant to the work within this thesis.

2.1 Mathematical Preliminaries

In this section, we briefly introduce key concepts and techniques in quantum information required for this thesis. Further details can be found in references, such as [35] and [36].

2.1.1 Quantum Mechanics: State Spaces, Evolution and Measurement

In quantum mechanics, a quantum system is represented by a state vector with unit norm, defined on a Hilbert Space $\mathscr{H} = \mathbb{C}^d$. That is, the usual d-dimensional complex space $\mathbb{C}^d$ endowed with an inner product. A simple quantum system that we will refer to is the quantum bit (qubit), which has a two-dimensional state space. The state of a qubit $|\psi\rangle \in \mathbb{C}^2$ can be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where $|0\rangle$, $|1\rangle$ are basis states, and α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Two possible states for a qubit are the states

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.2}$$

which correspond to the classical bits 0 and 1, respectively. The states $|0\rangle$ and $|1\rangle$ are referred to as computational basis states. State vectors denoted by $|\psi\rangle$ are commonly said to be pure states. When combining quantum systems, the state space of the composite system is the tensor product of the state spaces of the component systems. For example, the Hilbert space $\mathscr{H}_{AB}$ of two component Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_B$ is given by $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$. In the qubit case, supposing we have n qubits, the Hilbert space of the quantum system is $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2 \ldots \otimes \mathscr{H}_n$, where each $\mathscr{H}_i = \mathbb{C}^2$ is the component state space of each qubit.

The pure state description however, does not provide a complete description of quantum systems. More generally, the state of a quantum system can be a probabilistic mixture of pure states, called a mixed state. This is a more general description of a quantum system and is characterised by the density operator formalism. The density operator for the system is given by the equation:

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, \tag{2.3}$$

where $p_i \in [0,1]$ and $\sum_i p_i = 1$, and the $|\psi_i\rangle$ are pure states. Furthermore, the density operator ρ is Hermitian, and is in fact a non-negative operator, denoted $\rho \geq 0$, with unit trace. It can therefore be shown that ρ can be written as

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \tag{2.4}$$

where $\vec{r} = (r_x, r_y, r_z) \in \mathbb{R}^3$, and $\vec{\sigma}$ denotes the vector of Pauli matrices

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.5}$$

The property that ρ must be non-negative imposes the condition that $\|r\| \leq 1$. Note that if $r = (0,0,0)$, then this represents the maximally mixed state $\rho = I/2$.

The evolution of a (closed) quantum system is described by a unitary transformation. Let ρ denote the state of the system at time t_0, and ρ' represent its state at time t. These states are connected by a unitary operator U, that depends only on the times t_0 and t:

$$\rho' = U \rho U^\dagger, \tag{2.6}$$

where $U^\dagger$ is the Hermitian conjugate of U.

In quantum mechanics, a measurement has an incidence on the quantum system. That is to say, observing the system results in an interaction that makes the system no longer closed. The postulate, also known as Born's rule, provides a means to describe the effects of measurements on quantum systems. Quantum measurements are described by a set of measurement operators $\{M_m\}$ that satisfy the completeness equation:

$$\sum_m M_m^\dagger M_m = I. \tag{2.7}$$

The index m refers to the measurement outcomes that may occur. If the state of the quantum system is ρ immediately before the measurement, then the probability that the result m occurs is given by

$$p(m) = \mathrm{tr}\left(M_m^\dagger M_m \rho\right). \tag{2.8}$$

The post-measurement state is given by

$$\rho' = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\left(M_m^\dagger M_m \rho\right)}. \tag{2.9}$$

2.1.2 The Schmidt Decomposition and the PPT criterion

A bipartite pure state $|\psi\rangle \in \mathscr{H}_{AB}$ is said to be separable if it can be written as a product state,

$$|\psi\rangle = |\varphi_a\rangle \otimes |\varphi_b\rangle \tag{2.10}$$

for some $|\varphi_a\rangle \in \mathscr{H}_A$ and $|\varphi_b\rangle \in \mathscr{H}_B$. A state is said to be entangled if it is not a product state. Determining whether a given bipartite pure state is separable is a straightforward task that can be accomplished through the use of the Schmidt decomposition.

Theorem 2.1.1. *(Schmidt decomposition [35])*
If $|\psi\rangle$ is a pure state of a composite system, AB, then it can be given the decomposition

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle, \tag{2.11}$$

where $|i_A\rangle$,$|i_B\rangle$ are orthonormal states for systems A,B, respectively. The Schmidt coefficients λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$.

Proof. A proof of this can be found in [35]. □

The Schmidt decomposition allows us to determine whether a bipartite pure state $|\psi\rangle$ is separable. For example, it can be shown that the reduced states ρ_A and ρ_B are pure states if and only if $|\psi\rangle$ is a product state. Moreover, the state $|\psi\rangle$ is entangled if and only if it has a Schmidt rank greater than 1. On the other hand, checking separability of mixed states is not as straightforward as it is for pure states. A bipartite mixed state is said to be separable if it can be expressed as an ensemble of separable pure states:

$$\rho_{AB} = \sum_i p_i |\psi_i\rangle \langle\psi_i|_A \otimes |\varphi_i\rangle \langle\varphi_i|_B \tag{2.12}$$

$$= \sum_i p_i \rho_i^A \otimes \rho_i^B. \tag{2.13}$$

where p_i are non-negative probabilities that sum to 1, and ρ_i^A, ρ_i^B are density operators of the respective subsystems. Generally, testing whether a given state is separable is a challenging task [37, 38]. However, an efficient method for determining separability (in some systems) is the Positive Partial-Transpose (PPT) criterion [39, 40]. Specifically, a bipartite state ρ in a Hilbert space of dimension 2×2 (or 2×3) is separable if and only if its partial transpose is non-negative. That is, the PPT criterion states that if ρ_{AB} is separable, then

$$\rho_{AB}^{T_A} = (\mathscr{T} \otimes \mathrm{id})\rho_{AB} = \sum_i p_i \big(|\psi_i\rangle \langle\psi_i|_A\big)^T \otimes |\varphi_i\rangle \langle\varphi_i|_B \tag{2.14}$$

is non-negative, where $\mathscr{T}$ is the transpose map.

For states in higher dimensional Hilbert spaces, the PPT criterion is no longer a sufficient test for separability. This is because there exist entangled states in higher dimensions that are both positive and PPT. Therefore, while the PPT criterion can efficiently determine separability for systems of dimension 2×2 (or 2×3), it cannot be relied upon for all cases.

As a side note, it is important to point out that other approaches for determining separability do exist [41–44]. However, we will not make use of these methods. Instead, in section 4.4, we will use an approach based on linear programming.

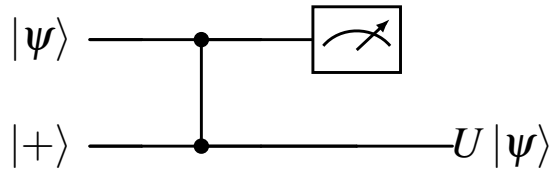


Fig. 2.1 Circuit demonstrating one-bit teleportation. This is achieved by performing a CZ gate on the input state $|\psi\rangle$ and $|+\rangle$, and then measuring the first qubit in the X-basis. This teleports the state $|\psi\rangle$ from the first qubit to the second and induces the operation $U = X^m H$, where m is either 0 or 1 depending on the measurement outcome. Note that if the measurement is a XY-plane measurement, then this instead induces the operation $U = X^m H U_Z$, where U_Z is the rotation operator about the Z-axis.

2.2 Measurement-Based Quantum Computation

In the quantum circuit model, an input state is first prepared, followed by the application of a unitary circuit (consisting of a sequence of gates), and the output is subsequently measured [35]. In this model, information is processed by manipulating the state of qubits through a sequence of unitary gates. An alternative universal model of quantum computation is measurement-based quantum computation (MBQC) [11, 12]. In MBQC, information is processed by first preparing an initial multiparty entangled state, and then performing measurements in a selected pattern. The measurements induce a non-unitary operation, which can nevertheless be used to simulate gates within the circuit model.

The key idea behind measurement-based quantum computation can be understood through the concept of one-bit teleportation [45, 46]. Consider the quantum circuit illustrated in figure 2.1, which is designed to "teleport" the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to another qubit. The teleportation scheme works as follows. The input state to the circuit is $|\psi\rangle|+\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Next, we apply a control-Z gate, denoted

$$CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|,$$

between the two qubits, resulting in:

$$\begin{aligned} CZ(|\psi\rangle|+\rangle) &= CZ(\alpha|0\rangle|+\rangle + \beta|1\rangle|+\rangle) && (2.15)\\ &= \alpha|0\rangle|+\rangle + \beta|1\rangle|-\rangle. && (2.16)\end{aligned}$$

Now, measuring the first qubit in the X-basis $\{|+\rangle, |-\rangle\}$ has the effect of projecting the second qubit onto the state

$$\alpha |+\rangle + (-1)^m \beta |-\rangle = HZ^m (\alpha |0\rangle + \beta |1\rangle), \tag{2.17}$$

where $H = |+\rangle\langle 0| + |-\rangle\langle 1|$ is the Hadamard gate and $m \in \{0,1\}$ is the measurement outcome. From this we can see that measuring the first qubit, has the effect of teleporting the state to the second qubit, up to a known unitary operation $HZ^m = X^m H$. Similarly, if instead we had measured the first qubit in the XY-plane, then the resultant unitary operation on the second qubit is $X^m H U_z$, where $U_z(\theta) = e^{-i\theta Z/2}$ is the rotation operator about the Z-axis. Note that the measurement in the XY-plane corresponds to a measurement in the X-basis transformed by a U_z rotation. This is illustrated in figure 2.1.

We will now see how through single qubit measurements we can implement an arbitrary single qubit rotation operation. To demonstrate this, we will introduce the 1D cluster state. The 1D cluster state, illustrated in figure 2.2, is created by initialising a chain of qubits in the $|+\rangle$ state and applying CZ gates between nearest neighbour qubits:

$$\prod_i^{n-1} CZ_{i,i+1} |+\rangle^{\otimes n}. \tag{2.18}$$

For example, if $n = 4$, then we have $CZ_{1,2}CZ_{2,3}CZ_{3,4} |+\rangle^{\otimes 4}$, which can be written explicitly as

$$|0\rangle|+\rangle|0\rangle|+\rangle + |1\rangle|-\rangle|0\rangle|+\rangle + |0\rangle|-\rangle|1\rangle|-\rangle + |1\rangle|+\rangle|1\rangle|-\rangle. \tag{2.19}$$

Repeating the procedure in figure 2.1, we perform XY-plane measurements on the first three qubits, leaving the state of the 4th qubit as

$$X^{m_3} H U_z(\theta_3) X^{m_2} H U_z(\theta_2) X^{m_1} H U_z(\theta_1) |+\rangle, \tag{2.20}$$

By standard commutation relations, this can be rewritten[1] as

$$X^{m_3} Z^{m_2} X^{m_1} H U_z[(-1)^{m_2}\theta_3] U_x[(-1)^{m_1}\theta_2] U_z[\theta_1] |+\rangle. \tag{2.21}$$

where $U_x(\theta) = e^{-i\theta X/2}$. It is known that a general rotation of a single qubit can be decomposed as $U_z(\alpha)U_x(\beta)U_z(\gamma)$, where α, β, γ are angles [35]. Therefore, this shows that

[1] Where we first use $X^m H = HZ^m$. Next, add in $H^2 = I$ to transform a Z-rotation into a X-rotation. And lastly, use commutations such as $XU_z(\theta) = U_z(-\theta)X$ to achieve the desired form.

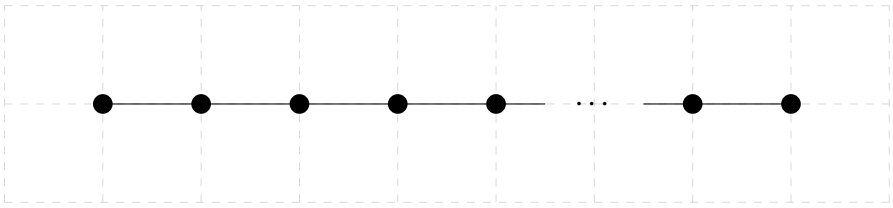


Fig. 2.2 The 1D cluster state is obtained by initialising $|+\rangle$ states on the nodes of the 1D lattice and applying CZ gates (depicted by edges) between nearest neighbour qubits.

through single qubit measurements, we can implement a unitary operator that implements any single qubit rotation [47]. Note that by adaptively choosing the measurement basis, we can ensure a deterministic computation. Furthermore, the Pauli corrections arising through measurements do not pose a problem, as they can be factored into the final result through classical post-processing.

Extending the above example, we can extend the concept of a 1D cluster state to a lattice of degree D. This is known as a graph state. A graph state is a pure-entangled state of n qubits, corresponding to a graph $G = \{E,V\}$ of n vertices. Every vertex $i \in V$ represents a qubit, and each edge $(i, j) \in E$ represents a CZ gate. The graph state, denoted as $|G\rangle$, is then given by:

$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes n}$$

where (i, j) represents pairs of neighbouring vertices in the lattice and $CZ_{i,j}$ is the controlled-Z gate applied to qubits i and j.

Note that in the literature, a cluster state is sometimes referred to as a graph state on a 2-dimensional lattice. Similar to the 1D cluster state example, on a 2D cluster state we can implement a sequence of 1 and 2 qubit gates by measuring selected qubits on the lattice [47]. If we allow for XY-plane and Z-basis measurements, then from the previous section, it is clear that we can implement arbitrary single qubit rotations. It is then straightforward to implement a two-qubit gate, such as a CZ or $CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$, as demonstrated in figure 2.3. Together, these operations, along with $H, U_Z(\theta)$, form a universal gate set, enabling cluster state quantum circuits to implement universal quantum computation.

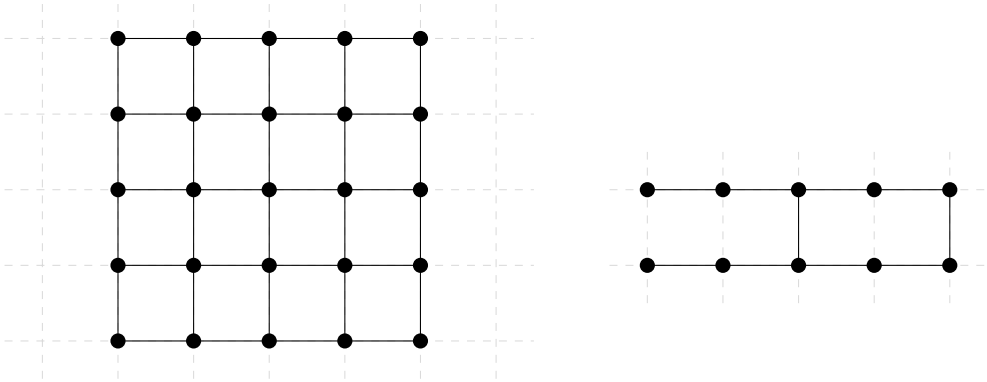


Fig. 2.3 The 2D cluster state is obtained by preparing qubits in the $|+\rangle$ state and placing them on the vertices of the 2D lattice (figure on the left), and interacting them with *CZ* gates connected by edges. The figure on the right is a brickwork state (of 5 columns, 2 rows). By performing measurements in the X-basis, the input qubits in the first column can be teleported from left to right. When a vertical *CZ* is encountered, the unitary acting on the qubits acquires a *CZ* gate.

2.3 Understanding Non-Classical Computation through Restricted Models of Quantum Computing

In the quantum circuit model, restrictions can be placed on the input states or permitted measurements, and it is common to restrict various aspects of the circuit, such as the circuit's structure (e.g. only allowing nearest neighbour gates), depth, or available gate set.

Placing such restriction on models of quantum computing can be useful as they allow us to explore the computational power between quantum and classical computations. By imposing restrictions on certain features of a quantum computation, we can potentially determine which features are necessary to retain full quantum computing power. From a more practical point of view, restricted models are useful as they can describe situations where there is an experimental limitation. We will now briefly introduce a well-known restricted model of quantum computing, known as Instantaneous Quantum Computation (IQP), that will be useful later on when discussing the quantum supremacy arguments.

The circuits used in Instantaneous Quantum Computation (IQP), are characterised by the restriction of using only commuting gates. This restricted model was initially introduced in [48] and further discussed in [19]. The structure of an IQP circuit is as follows: the input states are initialised as $|0\rangle^{\otimes n}$, and each gate in the circuit is diagonal in the X-basis. Specifically, the gates take the form:

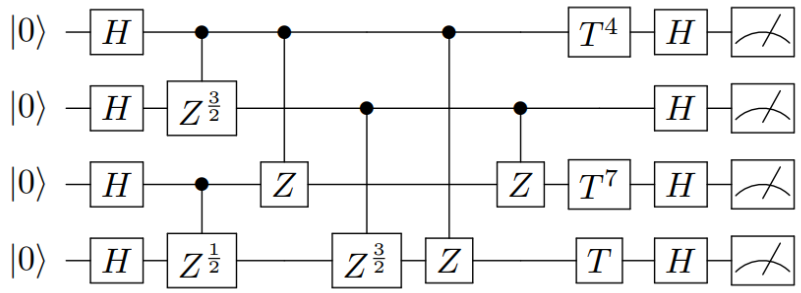


Fig. 2.4 Example an IQP circuit [21] where each qubit must begin and end with a Hadamard gate. The gates in-between are diagonal gates that commute and in principle can be applied simultaneously.

$$U = e^{i\theta\left(X_{i_1}\otimes\ldots\otimes X_{i_k}\right)}, \tag{2.22}$$

where θ is a parameter, and the subset $i_1,\ldots,i_k$ is permitted to act on $\mathcal{O}(n)$ lines of the circuit. Lastly, a computational basis measurement is performed on a specified set of output lines. An alternative description of an IQP circuit, as shown in figure 2.4, involves the insertion of $HH = I$ gates before and after the circuit. This modification results in the gates within the circuit being diagonal in the Z-basis. In subsequent work [19, 21, 49–52], the computational power of IQP circuits under different constraints has been explored. In [21], it was shown that IQP circuits, that consist of Z and CZ gates, together with a CCZ gate defined as

$$CCZ = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes CZ,$$

along with a layer of Hadamard gates at the beginning and end of the circuit, are hard to classically simulate.

2.3.1 Cluster State Quantum Circuits with Alternative Inputs

The scheme that will be of focus in this work can be considered to be a restricted model of measurement-based quantum computation. As described in section 2.2, the typical cluster state scheme can be described in three stages. First, qubits are prepared in the $|+\rangle$ state, and placed at the vertices of a lattice. Second, CZ gates are performed on qubits connected by lattice edges. Finally, single qubit measurements are performed on the lattice. If the measurements are adaptive, and are in the Z-basis and the XY-plane, then it is known that this cluster state quantum computation can support universal quantum computation.

In this work, we will be interested in exploring the computational power of a cluster state computation, wherein we vary the initial state preparation step. Instead of initialising the inputs as $|+\rangle$ states, we will instead consider pure states of the form

$$|\theta\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle, \tag{2.23}$$

with angle θ, where we will be interested in the computational power of this scheme as we vary the angle θ. It is clear that if the input states are $|0\rangle$ or $|1\rangle$, then the CZ gates would act trivially, and this scheme can be efficiently classically simulated. On the other hand, if the input states are close to the equator. Then it has been shown that, through a measurement process that requires certain POVMs and reusing measured qubits, this scheme can support universal quantum computation [53, 54]. In the subsequent work, we will consider cluster state schemes that have inputs of the form (2.23) and destructive measurements (i.e. measured qubits cannot be reused) in the XY-plane and Z-basis.

2.4 Generalised Separability

The usual notion of quantum separability:

$$\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B, \tag{2.24}$$

where ρ_i^A and ρ_i^B are normalised and non-negative operators, is based on the established concept of a single particle quantum state space. In this thesis, we will be interested in modifying the single particle state space, departing from the usual quantum version and introducing a more generalised notion of entanglement.

The idea that the notion of entanglement can be generalised was introduced in [13, 55]. However, for the purposes of this work, we will consider a more concrete and narrower framework. Specifically, we will consider relaxing the requirement that ρ_j^A and ρ_j^B must be non-negative operators, and instead allow the local operators to be drawn from the dual set of permitted measurements. That is, let $\mathscr{M}$ be the set of single-particle measurement operators. Then the normalised dual set $\mathscr{M}^*$ of operators ρ to $\mathscr{M}$ is defined as:

$$\mathscr{M}^* = \{\rho \mid \mathrm{tr}[\rho] = 1, \mathrm{tr}[\rho M] \geq 0, \forall M \in \mathscr{M}\}. \tag{2.25}$$

In other words, the dual set $\mathscr{M}^*$ contains operators that, through the Born rule, yield positive probabilities for a given set of measurement operators. Using the definitions of [56, 57], we now define a generalised notion of separability.

Definition 2.4.1. *Consider a convex set of local operators $\mathscr{S}_A, \mathscr{S}_B$ acting on systems A,B, respectively. A bipartite state ρ_{AB} is $(\mathscr{S}_A, \mathscr{S}_B)$-separable if it can be given the decomposition*

$$\rho_{AB} = \sum_i p_i \tilde{\rho}_i^A \otimes \tilde{\rho}_i^B, \tag{2.26}$$

where p_i are non-negative and sum to 1, and $\tilde{\rho}_i^A, \tilde{\rho}_i^B$ are operators drawn from $\mathscr{S}_A$ and $\mathscr{S}_B$ respectively. We refer to $\mathscr{S}_A$ and $\mathscr{S}_B$ as the local state spaces.

To distinguish the usual quantum separable notion to the more generalised separable notion, we will usually emphasise this by referring to being quantum separable or separable w.r.t to the local state spaces in question.

In particular, we will consider definition 2.4.1 in the context where the operators are drawn from the dual set as defined in (2.25). It is important to point out that these operators can, in fact, be non-physical operators. However, by placing restrictions on the permitted measurements and managing any negatives that may potentially occur, these operators can still be used to enable efficient classical simulation algorithms [58, 15]. In particular, in chapter 3 we will make use of this framework in the context of cluster states. This will lead us to consider various state spaces and consider when these can be a given a generalised separable decomposition. Furthermore, as we will see later on when developing our classical simulation algorithm, of particular interest will be when the separable decompositions exhibit minimal growth w.r.t to the output state spaces.

2.5 Classical Simulation

2.5.1 Notions of Efficient Classical Simulation

Before reviewing the literature on classical simulation, it is necessary to define what it means to simulate a quantum computation. The notions described below are based on the definitions in [59].

There are two main established notions of classical simulation: strong simulation and weak simulation. Let $p(x)$ to be the probability distribution that describes the statistics of the measurement outcomes for a given quantum circuit. Then a strong simulation of a quantum circuit, requires that the simulator has to be able to compute the probability $p(x)$ to arbitrary accuracy for each measurement outcome x. It has been argued in the literature that such a notion is considered to be unnecessarily challenging form of classical simulation [60, 59] as a quantum computer would not simulate to multiplicative error. Instead, a more appropriate choice is considered to be that of weak simulation. In a weak simulation, the simulator has to be able to sample an outcome x according to a distribution $\tilde{p}(x)$ that approximates the target distribution $p(x)$. Within weak simulations, several different notions of approximation have been considered, two of which are multiplicative and additive approximations.

1. The approximate weak simulation is multiplicative, if for every x,

$$|\tilde{p}(x) - p(x)| \leq \varepsilon p(x), \tag{2.27}$$

   with fixed $\varepsilon > 0$.

2. The approximate simulation is additive if,

$$\sum_x |\tilde{p}(x) - p(x)| \leq \varepsilon, \tag{2.28}$$

   where ε is some small-fixed constant.

The notion of multiplicative approximation is considered to be a strict and unrealistic notion of simulation, and was used in early quantum supremacy type arguments [19, 24]. A weaker, more appropriate notion is that of additive approximation, which has been used as the standard in quantum supremacy type arguments to demonstrate hardness [20, 21].

2.5.2 Review of Classical Simulation

In this section, we will review classical simulation results that are relevant to the work within this thesis.

A key theorem in classical simulation results is the Gottesman-Knill theorem [3].

Theorem 2.5.1. *(Gottesman–Knill) A quantum computation involving only: state preparations in the computational basis, polynomial-sized circuits consisting of Clifford gates, and Pauli measurements, can be efficiently simulated on a classical computer.*

The Gottesman-Knill theorem describes a highly non-trivial class of computations that can generate highly entangled systems and demonstrate phenomena like quantum teleportation. Furthermore, by relaxing the constraints and allowing for one non-Clifford gate in the allowed gate set, such as a T gate[2], universal quantum computation can be restored [3]. To implement a T gate, one can introduce a resource called the "magic" state $|\psi\rangle = 2^{-1/2}(|0\rangle + e^{i\pi/4}|1\rangle)$. By using this magic state and constructing a T-gadget, which resembles a teleportation scheme, it is possible to incorporate a T gate into a Clifford circuit and thus restore universal quantum computing [61].

The Gottesman-Knill theorem provides a direction in which we can identify the resources required to lift a computation that can be efficiently classically simulated to one that that has the full power of quantum computation [60]. This raises the question of what other features and resources could be added to Clifford circuits to enable quantum computation. For example, Jozsa and Van den Nest [4] investigated whether Clifford circuits, when supplemented with various additional features such as general input product states, intermediate adaptive or non-adaptive measurements can be efficiently classically simulated, where different notions of simulation were considered. It is not straightforward to determine generally the extent to which restricted models of quantum computing can be efficiently classically simulated due to the plethora of models, resources, and features that can be considered. However, by exploring the computational power of restricted models of quantum computing, we can establish a boundary between classical and quantum computing. Two well-known restricted models are IQP [48, 19] and matchgate [62, 63] circuits. Nearest neighbour matchgate circuits encode the physics of non-interacting fermions [62, 63]. These circuits can be efficiently classically simulated, although the addition of the swap gate allows for universal quantum computation [64, 65]. IQP circuits are circuits that consist of gates that are all diagonal in the X-basis, and measurements are performed in the computational basis. The classical simulation of these circuits has been studied under a variety of notions and features, such as noisy circuits, circuit depth, and short/long-range interaction gates [49, 21, 50].

[2] $T = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$.

A feature of quantum computing that has been widely studied is entanglement. It has been demonstrated that without entanglement, a quantum pure state computation can be classically efficiently simulated [66]. Furthermore, if there is limited entanglement, one can use tensor network type approaches [67–69] to provide efficient classical simulations [6, 70, 7]. However, the computations permitted by the Gottesman-Knill theorem clearly allow for highly entangled systems, and yet can also be classically simulated. On the other hand, it has been shown that weak amounts of entanglement can, in fact, be sufficient for quantum computation, [9, 10]. One avenue for exploring the effect of entanglement on classical simulation is to consider a more general framework of entanglement, introduced in [13]. By utilising this more general notion, classical simulation methods have been developed that can simulate pure systems that are nevertheless quantum entangled [58, 30].

A useful way to investigate the feature of entanglement is provided in the setting of measurement based quantum computing [11, 12]. In this setting, the entanglement is already present in the resource state, and non-clifford operations are carried out in the form of adaptive measurements to enable universal quantum computation. By imposing restrictions on certain parts of an MBQC (measurement-based quantum computation) scheme, it has been demonstrated that even with limitations such as, only measuring in the XY-plane [71], or utilising entangling unitaries of the form $e^{-i\frac{\pi}{2^n}Z\otimes Z}$ [72], or employing lattices with specific degrees (e.g. a brickwork state [73]), the scheme supports universal quantum computation. Another aspect that one can restrict in an MBQC scheme it the input state. This has been explored in [54, 53], where it was shown that if the input states are sufficiently close to the equatorial state, a filtering operation can be employed that recovers universal quantum computation. Recent methods have been developed, known as quantum supremacy arguments, that prove that if classically computers can efficiently simulate quantum computers, then this would violate widely believed complexity theoretic conjectures [16]. This approach has been used to demonstrate that certain restricted models of computing cannot be efficiently simulated [19–21, 25, 74–80, 32, 33]. Recent research in this direction has also focused on tackling the outstanding conjectures required in this approach, as well as settings involving noise [26–29, 34, 50]. Therefore, these arguments provide a tool that can be used to potentially establish that a restricted model of quantum computing cannot be efficiently classically simulated.

Chapter 3

Classical Simulation of Cluster State Quantum Circuits with Alternative Inputs

3.1 Introduction

In the previous chapter, we saw that a cluster state computation in its original form is known to support universal quantum computation. However, what happens if the input state is replaced by a pure state of the form $\cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle$? The answer to this is not obvious even for small θ, as states that are locally close to product states can still support universal quantum computation [9]. In this chapter, we will develop an efficient classical simulation algorithm that can simulate a cluster state scheme with inputs that are "close enough" to diagonal in the computational basis.

3.1.1 Overview and Related Work

It has been demonstrated that with certain types of limited entanglement, a pure state quantum computation can be efficiently classically simulated [66, 6, 7]. However, the computations permitted by the Gottesman-Knill theorem allow for highly entangled systems, and yet can also be efficiently classically simulated. It has also been shown that weak amounts of entanglement can, in fact, be sufficient for universal quantum computation [9, 10]. An approach for exploring the effect of entanglement on classical simulation is to consider a more general framework of entanglement [13, 55] and, in some cases, one can develop efficient classical simulation methods that can simulate quantum computations that are entangled [58].

A useful approach to investigating the role of entanglement arises in measurement-based quantum computing. Consider the typical cluster state scheme, which can be described in

three stages. First, qubits are prepared in the $|+\rangle$ state, and placed at the vertices of a lattice. Second, CZ gates are performed on qubits connected by lattice edges. Finally, single qubit measurements are performed on the lattice. If the measurements are adaptive, and are in the Z-basis and the XY-plane, then it is known that this scheme can support universal quantum computation. If, however, the input qubits are prepared in the $|0\rangle$ or $|1\rangle$ state, then the CZ gates act trivially, generating no entanglement. On the other hand, if the input states are close enough to the equator, then it has been shown that, through a measurement process that requires certain POVMs, such schemes can support universal quantum computation [53, 54]. In this work, we will be interested in exploring the computational power of a cluster state computation, wherein we vary the initial state preparation step. Instead of initialising the input state as a $|+\rangle$ state, we will instead consider pure states of the form

$$|\theta\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle, \tag{3.1}$$

with angle θ. Throughout this thesis, we will consider cluster state schemes with inputs of the form (3.1), and measurements in the XY-plane and Z-basis that are destructive[1].

This chapter is organised as follows. In Sec.3.2.2 we present our main result, that the output of a CZ gate acting on two cylinder states can be given a separable decomposition provided that the cylinder radii in the decomposition grow sufficiently. Sec.3.3.2 combines this result with the Harrow and Nielsen algorithm (Sec.3.3.1) to obtain an efficient classical simulation algorithm based on cylinder radii growth. Note that in the next chapter, we consider ways to improve and extend our classical simulation algorithm.

Contributions

The results presented in chapter 3 and chapter 4 are based on [30] and [31]. My contributions to this work are as follows. In Sec.4.2.1 the numerical computations of l_1 and $\tilde{l}_1$ were independently performed by Y.Tao, M.Garn and S.Virmani in order to verify the results. The initial exploratory investigations of lemma 3.2.1 in Sec.3.2.2 were developed by my supervisor in the symmetric case, and the extension to the asymmetric case was first done by Y.Tao. The lemma 4.3.1 in Sec.4.3 was initially explored by S.Atallah. The curve in figure 4.5 was obtained partially numerically by S.Atallah based on theoretical investigations initiated by S.Virmani. These results were verified by M.Garn, and M.Garn and S.Virmani together derived equation (4.21) in lemma 4.3.1. In table 4.2, some of the numerical values were first computed by S.Atallah and then independently verified by M.Garn. Observation

[1] That is, we do not permit remeasuring qubits.

4.4.2 and figure 4.9 were done by M.Garn. The theoretical results, other than those above, were developed by my supervisor. The writing and all other discussion was done by myself under the guidance of my supervisor.

3.2 Obtaining a Generalised Separable Decomposition

3.2.1 Cylindrical State Spaces

In section 2.2, we described the typical cluster state scheme, where input qubits are initialised in the $|+\rangle$ state and CZ gates are applied to nearest neighbour qubits. The resultant state is a highly entangled multiparty pure state that cannot be given a separable decomposition:

$$\sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C \otimes \dots \tag{3.2}$$

where ρ_i^K are normalised non-negative local operators. Furthermore, if the qubits are measured adaptively in either the Z-basis or the XY-plane, then this scheme can implement universal quantum computation.

However, in section 2.4 we saw that it is possible to generalise this notion of entanglement by relaxing the requirement that the ρ_j^K must be non-negative operators. Indeed, we will consider this and instead permit operators that yield non-negative probabilities. That is, allowing the local operators to be drawn from the normalised dual set:

$$\mathscr{M}^* := \{\rho \mid \mathrm{tr}[\rho] = 1, \mathrm{tr}[\rho M] \geq 0, \forall M \in \mathscr{M}\}, \tag{3.3}$$

where $\mathscr{M}$ denotes the set of permitted single particle measurement operators. Now consider the cluster state scheme with permitted single particle measurements in the Z-basis and XY-plane. The projectors for these measurements are of the form:

$$I \pm Z \quad \text{and} \quad I \pm (\cos\theta X + \sin\theta Y)\,. \tag{3.4}$$

We will now see how the condition $\mathrm{tr}[\rho M] \geq 0$ places constraints on ρ. Consider an arbitrary ρ expanded in the Pauli basis,

$$\rho = \frac{1}{2}(I + xX + yY + zZ)\,, \tag{3.5}$$

with $x, y, z \in \mathbb{R}$. Taking the projectors $P_{X\pm} = (I \pm X)/2$ and calculating $\text{tr}[\rho P_{X\pm}] \geq 0$, imposes the condition that $|x| \leq 1$. Similarly, if we consider the projectors $P_{Y\pm} = (I \pm Y)/2$, this imposes the condition $|y| \leq 1$. By calculating $\text{tr}[\rho M]$ for the remaining measurements in (3.4), we find that $z \in [-1,1]$ and $x^2 + y^2 \leq r^2$. Therefore, the dual set for the permitted measurements (3.4), becomes a cylindrically shaped state space as illustrated figure3.1.

Definition 3.2.1. *A cylinder of radius r is defined as the following set of normalised operators:*

$$\text{Cyl}(r) := \{\rho | \rho = \rho^\dagger, Tr\rho = 1, x^2 + y^2 \leq r^2, z \in [-1,1]\} \tag{3.6}$$

where x, y, z are the Bloch expansion coefficients of ρ.

We will commonly refer to operators that are drawn from (3.6) as cylinder states. It is important to point out that the operators drawn from the cylinder state space contain states that are outside the Bloch sphere and, consequently, contain non-physical operators. However, by ensuring that $r \leq 1$, the operators in (3.6) will nevertheless return valid probabilities for measurements in the Z-basis and XY-plane. As we will see later in Sec.3.3.1, we will use this fact to develop an efficient classical simulation algorithm. It is also important to point out that the physical states $|\theta\rangle$ are examples of cylinder states. That is, the states in equation (3.1) can be expressed as a convex combination of cylinder states in (3.6), where the correspondence between θ and r is given by $r = \sin\theta$. Lastly, we provide an alternative definition for cylinder sets in terms of dephasing noise.

Definition 3.2.2. *A cylinder of radius r is defined as the following set of normalised operators:*

$$\text{Cyl}(r) := \{\rho | \rho = \rho^\dagger, Tr\rho = 1, \|\rho - \mathscr{D}_Z(\rho)\| \leq r\}, \tag{3.7}$$

where $\mathscr{D}_Z(\rho) = (1-p)\rho + pZ\rho Z$, with $p = 1/2$.

3.2.2 Cylindrical Separability based on Radii Growth

We have just introduced cylindrical state spaces, which arise in the context of cluster state quantum circuits when measurements are restricted to the XY-plane and Z-basis. The key

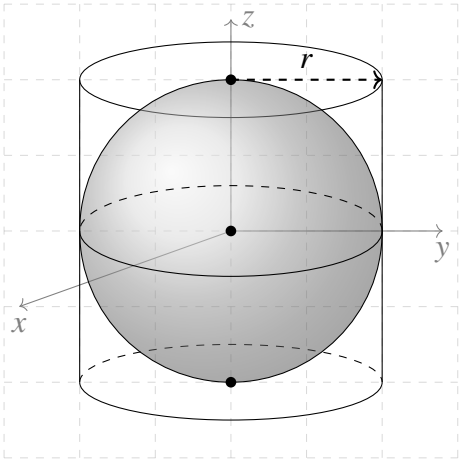


Fig. 3.1 This diagram illustrates a cylinder with $r = 1$ in the Bloch space, where the sphere represents the Bloch Sphere. The cylinders always extend the full height from $z = -1$ to $z = +1$, irrespective of radius. The unit cylinder with $r = 1$ is the normalised dual of the permitted measurements. That is the set of normalised operators that yield positive probabilities for the allowed measurements.

technical result that we will now show is that if a *CZ* gate acts on two cylindrical state spaces, the output can be given a separable decomposition with respect to two new cylindrical state spaces with larger radii.

Lemma 3.2.1. *Consider the set* $CZ(\mathrm{Cyl}(r_A) \otimes \mathrm{Cyl}(r_B))$ *of two qubit operators made by acting with a CZ gate on* $\mathrm{Cyl}(r_A) \otimes \mathrm{Cyl}(r_B)$. *Any operator in* $CZ(\mathrm{Cyl}(r_A) \otimes \mathrm{Cyl}(r_B))$ *can be written in the generalised separable form:*

$$\sum_i p_i \rho_i^A \otimes \rho_i^B \tag{3.8}$$

where $\rho_i^A \in \mathrm{Cyl}(R_A)$ *and* $\rho_i^B \in \mathrm{Cyl}(R_B)$ *if and only if:*

$$1 \geq \left(\frac{r_A}{R_A} + \frac{r_B}{R_B}\right)^2 + \left(\frac{r_A}{R_A}\right)^2 \left(\frac{r_B}{R_B}\right)^2. \tag{3.9}$$

We refer to an operator of the form of equation (3.8) as being $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$*-separable.*

Before starting the proof, we will first need to introduce some notation. Consider an operator ρ expanded in the Pauli basis. We will use the brackets "[...]", containing the Pauli expansion coefficients, to denote the operator ρ. For example, the bracket $[1, x, y, z]$

denotes the single particle operator $\rho = \frac{1}{2}(I + xX + yY + zZ)$. If ρ_{AB} is a two particle operator expanded in the Pauli basis as

$$\rho_{AB} = \frac{1}{4}\sum_{i,j}\rho_{i,j}\sigma_i \otimes \sigma_j, \tag{3.10}$$

where $\sigma_0 = I, \sigma_1 = \sigma_= X, \sigma_2 = Y, \sigma_3 = Z$ are the Pauli matrices, then we denote this operator as

$$\begin{bmatrix} \rho_{00} & \rho_{01} & \rho_{02} & \rho_{03} \\ \rho_{10} & \rho_{11} & \rho_{12} & \rho_{13} \\ \rho_{20} & \rho_{21} & \rho_{22} & \rho_{23} \\ \rho_{30} & \rho_{31} & \rho_{32} & \rho_{33} \end{bmatrix}. \tag{3.11}$$

Proof. Consider the two particle product state $\rho_A \otimes \rho_B$ where ρ_A, ρ_B are drawn from two cylinders with radii r_A and r_B respectively. The task is to determine whether the output of a CZ gate, acting on all such possible inputs, leads to a $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable state.

Suppose we have a CZ acting on any such input state ρ. As ρ can be expressed as a linear combination of extremal states and as the CZ is a linear operator, we see that if the output is separable for extremal inputs, then the output is separable for all inputs. Therefore, we only need to consider whether the output of a CZ acting on extremal state inputs is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable.

Next, we will show that we can further reduce the number of input states we need to consider by exploiting properties of the CZ gate and symmetries of cylindrical state spaces. Suppose that we have an explicit $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable decomposition:

$$CZ(\rho_A \otimes \rho_B) = \sum_i p_i \omega_A^i \otimes \omega_B^i \tag{3.12}$$

where $\omega_k^i \in \mathrm{Cyl}(R_k)$. Then we have the following observations.

1. Observe that any extremal input state $\rho_k \in \mathrm{Cyl}(r_k)$ can be expressed as $U_z^k([1, r_k, 0, \pm 1])$, where U_z^k is the rotation operator about the Z axis. Now using the fact that U_z^k commutes with the CZ and that cylinders are invariant under Z rotations, we have the $\mathrm{Cyl}(r_A), \mathrm{Cyl}(r_B)$-separable decomposition:

$$CZ\left(U_z^A(\rho_A) \otimes U_z^B(\rho_B)\right) = \sum_i p_i U_z^A\left(\omega_A^i\right) \otimes U_z^B\left(\omega_B^i\right).$$

This shows that the separable decomposition in equation (3.12) is invariant up to local Z rotations and we may restrict inputs to the form

$$[1, r_A, 0, \pm 1] \otimes [1, r_B, 0, \pm 1].$$

2. Notice that if the first input particle has $z_A = 1$ with the second input particle having $z_B = \pm 1$, and the output is separable:

$$CZ([1, r_A, 0, 1] \otimes [1, r_B, 0, \pm 1]) = \sum_i p_i \omega_A^i \otimes \omega_B^i,$$

then modifying the first input to have $z_A = -1$ gives another operator with a separable decomposition:

$$CZ([1, r_A, 0, -1] \otimes [1, r_B, 0, \pm 1]) = \sum_i p_i X \omega_A^i X^\dagger \otimes Z \omega_B^i Z^\dagger.$$

In this argument we could equally well have considered the second input instead, as the CZ is symmetric. This shows that input product states with asymmetric z-components[2] preserve (3.12) up to an $X \otimes Z$ or $Z \otimes X$ operation. Therefore, we only need to consider input states of the form $[1, r_k, 0, 1]$.

Following these observations, we have reduced the task to determining whether the output of a CZ gate, acting on one input extremum:

$$[1, r_A, 0, 1] \otimes [1, r_B, 0, 1] \tag{3.13}$$

is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable. Under the action of the CZ gate acting on inputs (3.13), we have

$$\begin{bmatrix} 1 & r_B & 0 & 1 \\ r_A & 0 & 0 & r_A \\ 0 & 0 & r_A r_B & 0 \\ 1 & r_B & 0 & 1 \end{bmatrix}. \tag{3.14}$$

If this corresponds to a $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable operator, then it can be given the decomposition, written as the outer product, as:

[2] That is, the first input particle has $z_A = 1$ and the second input particle has $z_B = -1$, or $z_A = -1$ and $z_B = 1$.

$$\sum_i p_i \begin{bmatrix} 1 \\ R_A\cos(\theta_i) \\ R_A\sin(\theta_i) \\ 1 \end{bmatrix} \begin{bmatrix} 1 & R_B\cos(\phi_i) & R_B\sin(\phi_i) & 1 \end{bmatrix}, \tag{3.15}$$

where the angles θ_i and ϕ_i indicate where on the top perimeter of the cylinder the local states lie. Setting equation (3.14) equal to (3.15), and left multiplying by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/R_A & 0 & 0 \\ 0 & 0 & 1/R_A & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.16}$$

and right multiplying by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/R_B & 0 & 0 \\ 0 & 0 & 1/R_B & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{3.17}$$

we see that equation (3.14) is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable if and only if

$$\begin{bmatrix} 1 & \frac{r_B}{R_B} & 0 & 1 \\ \frac{r_A}{R_A} & 0 & 0 & \frac{r_A}{R_A} \\ 0 & 0 & \frac{r_A r_B}{R_A R_B} & 0 \\ 1 & \frac{r_B}{R_B} & 0 & 1 \end{bmatrix} \tag{3.18}$$

is $\mathrm{Cyl}(1), \mathrm{Cyl}(1)$-separable.

We will now demonstrate that verifying whether (3.18) is $\mathrm{Cyl}(1), \mathrm{Cyl}(1)$-separable is equivalent to checking the usual quantum separability of a two-qubit quantum operator. First,

assume that the operator

$$\begin{bmatrix} 1 & \pm\frac{r_B}{R_B} & 0 & 0 \\ \pm\frac{r_A}{R_A} & 0 & 0 & 0 \\ 0 & 0 & \frac{r_A r_B}{R_A R_B} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{3.19}$$

has a quantum separable decomposition:

$$\sum_i p_i [1, x_A^i, y_A^i, z_A^i] \otimes [1, x_B^i, y_B^i, z_B^i]. \tag{3.20}$$

Given such a decomposition, and setting $z_A^i = 1$ and $z_B^i = 1$ for all i, we have that (3.18) is $\mathrm{Cyl}(1), \mathrm{Cyl}(1)$-separable because it has decomposition

$$\sum_i p_i [1, x_A^i, y_A^i, 1] \otimes [1, x_B^i, y_B^i, 1]. \tag{3.21}$$

Conversely, by taking any $\mathrm{Cyl}(1), \mathrm{Cyl}(1)$-separable decomposition for equation (3.18) and setting $z_A^i = 0$ and $z_B^i = 0$ for all i, we recover a quantum-separable decomposition for (3.19). Therefore, we have that (3.14) is $\mathrm{Cyl}(r_A), \mathrm{Cyl}(r_B)$-separable if and only if (3.19) corresponds to a positive and PPT operator, so we may apply the PPT criterion [39, 40].

Explicitly verifying (3.19) is quantum separable, corresponds to checking that the minimal eigenvalues of the operator (3.19):

$$I + (\frac{r_A}{R_A} X \otimes I + I \otimes \frac{r_B}{R_B} X) + \frac{r_A r_B}{R_A R_B} Y \otimes Y \tag{3.22}$$

and its partial transpose

$$I + (\frac{r_A}{R_A} X \otimes I + I \otimes \frac{r_B}{R_B} X) - \frac{r_A r_B}{R_A R_B} Y \otimes Y \tag{3.23}$$

are non-negative. Notice however, that (3.22) and (3.23) are related by the unitary $X \otimes I$. Specifically, applying a X transformation on the first qubit of (3.22) gives (3.23), hence the eigenvalues of the two operators are equivalent.

To proceed, we will simplify the problem by applying a Hadamard unitary to both qubits of (3.23) to give

$$I+(\frac{r_A}{R_A}Z\otimes I+I\otimes\frac{r_B}{R_B}Z)-\frac{r_Ar_B}{R_AR_B}Y\otimes Y. \tag{3.24}$$

Expressing the above equation in the computation basis:

$$\begin{pmatrix} 1+f_A+f_B & 0 & 0 & f_Af_B \\ 0 & 1+f_A-f_B & -f_Af_B & 0 \\ 0 & -f_Af_B & 1-f_A+f_B & 0 \\ f_Af_B & 0 & 0 & 1-f_A-f_B \end{pmatrix}, \tag{3.25}$$

where we have defined $f_A := r_A/R_A$ and $f_B := r_B/R_B$. The eigenvalues can be worked out on the inner and outer block separately. Both blocks have positive trace, and the determinants of the inner and outer block are:

$$1-(f_A-f_B)^2-f_A^2f_B^2, \tag{3.26}$$
$$1-(f_A+f_B)^2-f_A^2f_B^2 \tag{3.27}$$

respectively. As $f_A, f_B \geq 0$, the lowest of these is the outer determinant (3.27). Therefore, if the outer determinant is non-negative the output will be $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable.

□

We will now discuss some implications of lemma 3.2.1. First, let us define the 'growth' factor ratios as

$$g_k := \frac{R_k}{r_k}. \tag{3.28}$$

Therefore, we can interpret the result of lemma 3.2.1 as stating that a *CZ* can be interpreted as a gate giving separable output, provided that the radii of the output spaces are sufficiently large relative to those of the input spaces. That is, provided that the growth factors satisfy

$$1 \geq \left(\frac{1}{g_A}+\frac{1}{g_B}\right)^2+\left(\frac{1}{g_A}\right)^2\left(\frac{1}{g_B}\right)^2. \tag{3.29}$$

If we consider the case in which the growth factors are symmetric, $g_A = g_B = g$, then condition (3.9) in lemma 3.2.1 reduces to

$$1-\frac{4}{g^2}-\frac{1}{g^4} \geq 0 \tag{3.30}$$

which can be solved to give:

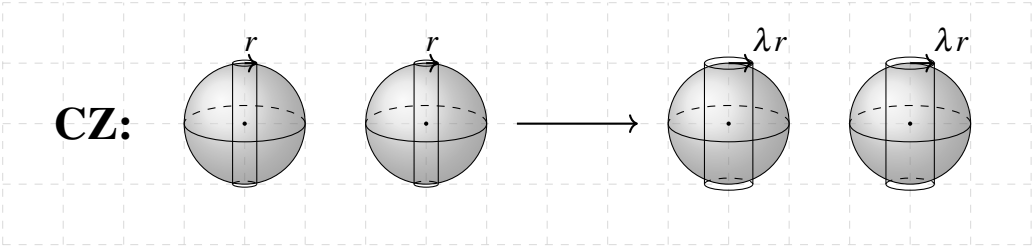


Fig. 3.2 This figure summarises the result of lemma 3.2.1 with symmetric growth factors λ. Applying a *CZ* operation to two input cylinders, the output can be given a separable decomposition with respect to cylindrical state spaces provided that the cylinder radius grows by $\lambda \approx 2.058$.

$$g \geq \lambda := \sqrt{\frac{1}{\sqrt{5}-2}} \approx 2.05817. \tag{3.31}$$

Therefore, in the case that the growth factors are symmetric, we see that as long as the radii of the output spaces are roughly twice the input radii, then the *CZ* can be considered a separable operation (see figure 3.2).

3.3 An Efficient Classical Simulation Algorithm

In this section, we describe the classical algorithm proposed by Harrow and Nielsen (HN) [8] for efficient simulation of noisy quantum systems that cannot generate entanglement. We then show that by combining this algorithm with the concept of cylinder separability, we obtain an efficient classical simulation algorithm based on the growth of cylinder radii. Moreover, the algorithm only requires modest changes to the HN algorithm to implement cylindrical state spaces.

3.3.1 The Harrow and Nielsen algorithm

The Harrow and Nielsen algorithm is an efficient classical simulation algorithm that can simulate a quantum computation where: the input is a product state, the circuit only contains non-entangling gates, and the output is obtained by performing local measurements.

The idea of the algorithm is to represent the global state of the system with variables that approximate the Bloch vector of each particle, up to l-bits of precision. And for every (separable) gate in the quantum circuit being simulated, the classical algorithm represents this through a gate simulation step.

In the gate simulation step, the algorithm takes as input, w.l.o.g states ρ_A and ρ_B, and through a brute force search constructs an approximation to the separable decomposition $\sum_i p_i \rho_i^A \otimes \rho_i^B$. The algorithm then samples i according to p_i, and for that i updates the Bloch vectors (up to l-bit precision) with corresponding ρ_i^A, ρ_i^B. Once all the gate simulation steps in the circuit have been carried out, the measurement outcomes are then sampled from the final product state. In [8], it was then shown that if l is of order $O(\log(\text{poly}(n)/\varepsilon))$, with n number of gates in the circuit, then the algorithm samples the quantum distribution to within ε in polynomial time.

We now describe in detail how the efficient classical simulation algorithm from [8] is performed.

Description of Variables

The method involves the use of valid three-dimensional real vectors $\vec{s}_j$ for $j = 1, \ldots, q(n)$, where $q(n)$ is a polynomial in n. Each $\vec{s}_j$ is said to be valid if: it is in the range $[-1, 1]$, specified to l bits of precision[3], and $|\vec{s}_j| \leq 1$. The notation $\vec{s} \equiv (\vec{s}_1, \ldots, \vec{s}_{q(n)})$ is used to denote the $3q(n)$-dimensional real vector containing all the $\vec{s}_j$ s as sub-vectors. The idea of the classical simulation is that the variables $\vec{s}$ will be used to represent the states $\rho(\vec{s})$:

$$\rho(\vec{s}) \equiv \frac{I + \vec{s}_1 \cdot \vec{\sigma}}{2} \otimes \ldots \otimes \frac{I + \vec{s}_{q(n)} \cdot \sigma}{2}. \tag{3.32}$$

The initial state of the quantum computer is assumed to be $|x\rangle$, where x has binary expansion $x_1 \ldots x_{q(n)}$. If $x_j = 0$, then set $\vec{s}_j = (0, 0, 1)$, while if $x_j = 1$, then set $\vec{s}_j = (0, 0, -1)$. To simulate a two-qubit[4] separable gate $\mathscr{E}$ acting on qubits A and B, we use the following gate simulation procedure. The procedure takes $\vec{s}$ as input and produces a $3q(n)$-dimensional vector $\vec{s}'$ as output. We then set $\vec{s} = \vec{s}'$ and repeat the procedure for each gate in the computation until we reach the final output value of $\vec{s}$.

The Gate Simulation Procedure

To simulate a two-qubit gate, we start with $\vec{s}$. Our goal is to find $\vec{s}_A^j$ and $\vec{s}_B^j$, and a probability distribution p_j, specified to l bits of precision. We want to satisfy the following inequality:

[3] To be fixed later in order to ensure the overall accuracy is at least ε.

[4] Note that we only need to consider simulating two-qubit gates as a single-qubit gate can be simulated as a two-qubit gate, where one qubit is acted on trivially.

$$D\left(\mathscr{E}\left(\frac{I+\vec{s}_A\cdot\vec{\sigma}}{2}\otimes\frac{I+\vec{s}_B\cdot\vec{\sigma}}{2}\right),\sum_j p_j\frac{I+\vec{s}_A^j\cdot\vec{\sigma}}{2}\otimes\frac{I+\vec{s}_B^j\cdot\vec{\sigma}}{2}\right)\leq c2^{-l}$$

where c is a constant that does not depend on $\mathscr{E}$,A or B. To do this, we use Carathéodory's theorem, which tells us that the separable, two-qubit state $\mathscr{E}\left(\frac{I+\vec{s}_A\cdot\vec{\sigma}}{2}\otimes\frac{I+\vec{s}_B\cdot\vec{\sigma}}{2}\right)$ can be written as:

$$\sum_j q_j\frac{I+\vec{t}_A^j\cdot\vec{\sigma}}{2}\otimes\frac{I+\vec{t}_B^j\cdot\vec{\sigma}}{2}$$

where q_j are probabilities, $\vec{t}_A^j,\vec{t}_B^j$ are real-three vectors satisfying $|\vec{t}_A^j|,|\vec{t}_B^j|\leq 1$, and there are at most 16 terms in the sum. We choose the p_j to be probabilities that are l-bit approximations to the q_j, and the $\vec{s}_A^j,\vec{s}_B^j$ to be valid vectors that approximate $\vec{t}_A^j,\vec{t}_B^3$ to l bits. This allows us to satisfy the inequality above. It is important to note that finding valid probabilities and vectors may require significant computational effort. While Carathéodory's theorem ensures the existence of such probabilities and vectors, finding them may not be a trivial task. The output of the procedure is a valid vector $\vec{s}'$, which is chosen with probability p_j. We construct the vectors $\vec{s}_A^j$ and $\vec{s}_B^j$ to approximate $\vec{t}_A^j$ and $\vec{t}_B^j$, which are real-three vectors satisfying certain conditions.

Simulating the Final Measurement

To simulate the final measurement, we start with a subset of qubits that are measured at the output of the quantum computation, denoted as S. For each qubit k in S, we let s_k^3 be the third component of the vector $\vec{s}_k$. To determine the measurement outcome for qubit k, we use the following probabilities: the measurement result is 0 with probability $\left(1+s_k^3\right)/2$, and it is 1 with probability $\left(1-s_k^3\right)/2$. By following this procedure, we obtain a distribution over possible outcomes, denoted as $\tilde{p}_x(y)$, where y is the outcome and x is the input to the quantum computation.

3.3.2 Efficient Classical Simulation based on Radii Growth

We will now show that the Harrow and Nielsen algorithm can be applied to our setting by considering the following minor modifications.

First, we modify the initialisation step by placing particles on the nodes of a regular graph, where the operators are drawn from the set $Cyl(r_i)$ with radii r_i. It was established in the previous section that the output of a CZ gate, acting on two cylinder states, can be

given a separable decomposition provided the output radii grow sufficiently. Therefore, in the gate simulation step, we replace r_i with $\lambda_i r_i$, where λ_i is the growth factor required to ensure separability. Moreover, for each CZ gate we perform a gate simulation step, resulting in the output remaining cylinder separable provided that the cylinder spaces $Cyl(r_i)$ are replaced with

$$\mathrm{Cyl}(\lambda_i^D r_i) \tag{3.33}$$

where D is the degree of the graph. Therefore, if we restrict the measurements to Z-basis measurements and XY-plane measurements, then we can use the cylinder separable description to sample the measurements efficiently. That is, if the initial qubits satisfy the condition:

$$||\rho_i - (\rho_i)_{\mathrm{diag}}|| \leq \frac{1}{\lambda^D}, \tag{3.34}$$

then the system can be efficiently simulated classically. This can be summarised in the following theorem.

Theorem 3.3.1. *If a quantum computation involves initialising n qubits in state ρ on the sites of a lattice, and interacting qubits joined by an edge with CZ gates, then if the states ρ satisfy:*

$$\|\rho - \rho_{diag}\| \leq \frac{1}{\lambda^D}, \quad \lambda := \sqrt{\frac{1}{\sqrt{5}-2}} \approx 2.05817 \tag{3.35}$$

where D is the maximum degree of any node, then measurements in the Z basis and the XY plane can be sampled classically to within additive error ε in $O(poly(n, \frac{1}{\varepsilon}))$ time.

3.4 Summary and Remarks

In this chapter, we have shown that computations made from cluster state circuits acting upon inputs close enough to computational basis states can be efficiently simulated classically. The main technical tool we considered was a generalised notion of separability. Specifically, we considered relaxing the requirement that the local operators ρ_j^K must be non-negative operators, and instead allowed the operators to be drawn from a set of operators that, through the Born rule, yield positive probabilities for a given set of measurement operators. Applying this to the permitted cluster measurements, we arrived at the notion of cylindrical state spaces.

Using this notion, we first proved that if a *CZ* gate acts on input operators that are drawn from cylinders of radius r, the output can be given a separable decomposition provided that the radius of the output cylinders in the decomposition grows by a constant $\lambda > 0$. By combining this with a modified version of Harrow and Nielsen's algorithm, we see that this enables an efficient classical simulation algorithm that can sample from the output distribution to within additive error. As a result, this provides examples of pure entangled quantum systems that can be efficiently classically simulated. We remark that the techniques on generalised separability presented in this chapter and in earlier work [15], could be potentially applied to other quantum systems (e.g. non-diagonal gates, and other restrictions on measurements) and therefore may enable efficient classical simulation algorithms.

Chapter 4

Classical Simulation: Improvements and Generalisations

4.1 Introduction

In Chapter 3, we showed that computations arising from cluster state quantum circuits acting upon inputs close enough to computational basis states can be efficiently classically simulated. Key to the classical simulation algorithm that was developed in chapter 3, is that for each CZ interaction, the radius r of the output operators in the separable decomposition must grow by λ. This requirement, coupled with the dual constraint, determines the values of r that can be efficiently simulated. In this chapter, we look at ways to improve and extend our classical simulation algorithm. Namely, we improve the regions of r that can be efficiently classically simulated by considering a coarse-graining approach and other alternative notions of separability. We also generalise and extend the result of Sec.3.2.2 beyond CZ gates, by computing the equivalent λ for any two-qubit diagonal gate.

4.1.1 Overview

In this chapter, we will focus on ways to improve and generalise our classical simulation algorithm. First, in Sec.4.2, we show that by considering a coarse graining approach, we can improve the bound on the parameter r that can be efficiently classically simulated. The idea of the approach is to partition the underlying lattice into blocks and treating each block as a single particle on a new lattice. Then by constructing separable decompositions over these blocks, we can analytically show that we can increase r for which we can efficiently classically simulate.

In Sec.4.3, we explicitly compute λ for any two-qubit diagonal gate, thus generalising and extending the result of Sec.3.2.2 beyond CZ gates. This result demonstrates that, for any finite-degree graph, a two-parameter family of pure entangled quantum states can be efficiently classically simulated within a non-trivial region for permitted measurements. Consequently, for these systems, we are able to plot figures (see fig 4.6) that include regions that can be efficiently classically simulated. Note that the proof of this result uses similar techniques based on cylinder separability as in Sec.3.2.2.

Next, we consider whether there are state spaces that maintain a separable decomposition with a lower growth rate than the cylinder state space. In sec.4.4, we investigate this for two state spaces, that we call the Protruding state space and the Cylinder-Cone state space. The main approach used in this section is to map a separability problem into a linear programming problem. In Sec.4.4.1, we find that the Protruding state space requires greater growth to maintain separability than the cylinder state space. However, in Sec.4.4.4, we find that for the Cylinder-Cone state space there is a very slight improvement in the growth required for maintaining a separable decomposition.

4.2 Coarse Graining

The classical simulation algorithm developed in section 3.3.2 has two conflicting requirements:

1. To maintain a cylinder separable decomposition, the input radii r_i must grow with each application of a CZ gate.

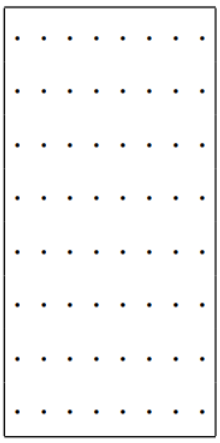
2. The input radii r_i must also satisfy the dual constraint, thus requiring that

$$\lambda_i^D r_i \leq 1,$$

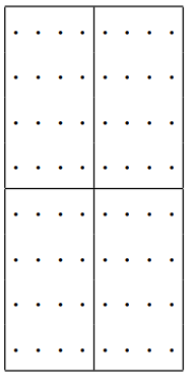
   where D is the maximum degree of the lattice and λ_i is the growth rate required to main a cylinder separable decomposition.

In this section, we will show that this trade-off can be better managed through a coarse-graining approach. We will explain this approach through an example.

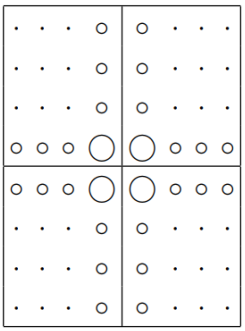
Consider a lattice of size 8×8, where each node of the lattice represents a particle that is drawn from $\mathrm{Cyl}(r)$, illustrated in figure 4.1a. We partition the lattice into 4×4 blocks of fixed size, see figure 4.1b. Next, apply the external CZ gates that connect particles between



(a) Initialise the 8×8 lattice.



(b) Partition the lattice into 4×4 blocks of fixed size.



(c) Apply the external CZ gates that connect particles between blocks.

Fig. 4.1 Example of Coarse Graining approach for a 8×8 lattice with 4×4 blocks. In this figure, each node represents a particle that is drawn from $\mathrm{Cyl}(r)$. The smaller circles represent particles drawn from $\mathrm{Cyl}(\lambda r)$ and the biggest from $\mathrm{Cyl}(\lambda^2 r)$.

blocks, see figure 4.1c. To maintain a separable decomposition, we require that the radius of each particle grows according to the number of external CZ gates applied to the qubit. The updated new state space of each block B, after undergoing the external CZ gates, is:

$$S'_B(r) := \bigotimes_{i=1}^{n} \mathrm{Cyl}(r_i). \tag{4.1}$$

Here, for each qubit i in the block, the radius r_i is determined by $r_i = r\lambda^{e_i}$, where e_i denotes the number of external CZ gates applied to that qubit. It should be noted that, prior to applying the internal CZ gates, each block B is separable with respect to these state spaces.

Lastly, for each block we apply the internal CZ gates, the resulting state space for each block is $S''_B(r)$. We define the maximum value of r for which S''_B is in dual as $r_{B,\max}$. We also denote the state space for a block B as $S_B := S''_B(r_{B,\max})$.

Comparing the Coarse-Grained and Fine-Grained approaches.

To understand the differences between the coarse-grained and the previous fine-grained approach, consider the last step of the procedure outlined above. In the fine-grained approach, the radii r were chosen such that the internal CZ gates satisfy two constraints: i) the block state space is in the dual of the measurements, ii) the output state has to be separable with

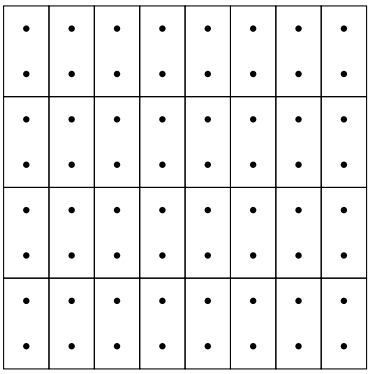


Fig. 4.2 Example of the coarse-graining approach, where a 8×8 lattice has been partitioned into blocks of two particles.

respect to an internal partition into $\mathrm{Cyl}(1)$ spaces. Note that the constraint i) is satisfied if ii) holds.

In contrast, the coarse-grained approach only imposes a single constraint, that the internal *CZ* gates keep the block state space in the dual of the measurements. We will see that this weaker requirement allows us to increase the r that we can classically simulate compared to the fine-grained approach.

Example. Blocks of 2 Cylinders

To demonstrate the difference in the approaches outlined above, we will consider a 2D square lattice partitioned into blocks of two particles, as shown in figure 4.2. Following the procedure, we apply the external *CZ* gates that connect particles between blocks. To maintain a separable decomposition, we require that the output radii must satisfy

$$r' = r\lambda^3, \tag{4.2}$$

for all particles not on the perimeter[1].

In the fine-grained approach, the remaining internal *CZ* gates would be applied within each block, resulting in the constraint

$$r \leq \frac{1}{\lambda^4} \tag{4.3}$$

[1]We exclude particles on the perimeter from the calculation, as their radii grow by λ or λ^2, leading to a weaker constraint on r.

However, in the coarse-approach, we only need to ensure that we do not get taken out of the dual. This means that, the output of a CZ gate acting on all extremal input cylinder states must only be in the dual of the measurements. Therefore, we have to calculate the maximum r', such that the output of a CZ gate acting on all possible extremal cylinder states, returns non-negative probabilities for the permitted measurements (Z basis and XY-plane measurements). Explicitly in appendix A.1, we show that $r' \leq 1/2$ and therefore equation (4.2) implies that

$$r \leq \frac{1}{2\lambda^3}. \tag{4.4}$$

Comparing this with the restriction on r of the fine-grained approach of (4.3), we see that coarse-graining improves the range of r for the case of 2-blocks.

Sequences obtained by increasing block size

We will now see that by increasing the block sizes further, we will only ever increase the region of r that can be classically simulated. Let B be a rectangular block with $H \times W$ qubits, where $H, W \geq 2$, which is embedded in a larger lattice. We will consider two ways of initialising the qubits in the block, illustrated in figure 4.3.

The first way is to initialise all states in an extremal cylinder state with radius r and $z = 1$ and apply the internal CZ gates. We denote the resultant operator describing this block as $\rho(B,r)$. The second way is to initialise the interior qubits in extremal cylinder states with radius r and $z = 1$. The states on the boundary of the block, are initialised in extremal cylinder states with a radius that grows according to the number of external CZ gates. We now apply the internal CZ gates within this block and denote the resultant operator as $\rho_\lambda(B,r)$.

We will be interested in when these operators are in the dual of the permitted measurements, and therefore it will be helpful to define the following quantities:

$$s(B) := \max\{r \mid \mathrm{Tr}[M\rho(B,r)] \geq 0, \forall M \in \mathscr{M}\} \tag{4.5}$$

and

$$s_\lambda(B) := \max\{r \mid \mathrm{Tr}[M\rho_\lambda(B,r)] \geq 0, \forall M \in \mathscr{M}\} \tag{4.6}$$

where $\mathscr{M}$ is the set of permitted measurements.

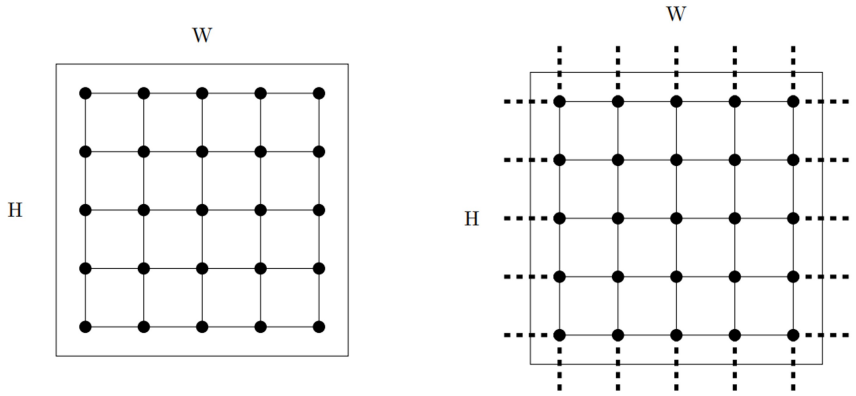


Fig. 4.3 Example of block operators $\rho(B,r)$ and $\rho_\lambda(B,r)$, where the block B is of size $H \times W$. The operator $\rho(B,r)$ describes the block on the left, where all states have been prepared in an extremal cylinder state with radius r and $z = 1$, and all internal CZ gates have been applied. The operator $\rho_\lambda(B,r)$ describes the block on the right, which is constructed as follows. The interior qubits are extremal cylinder states with radius r and $z = 1$. The states on the boundary of the block, are initialised in extremal cylinder states with a radius that grows according to the number of external CZ gates (denoted by dashed lines). Applying the internal CZ gates within this block results in the operator $\rho_\lambda(B,r)$.

At this point it is helpful to summarise how these quantities connect to the classical simulation algorithm presented in Sec.3.3.2. If there exists a block B for which $r \leq s_\lambda(B)$, then it is possible to efficiently classically simulate inputs from cylinders with radii r. However, if $r > s(B)$, then inputs from cylinders with a radius of r would result in negative probabilities, hence we cannot apply the classical simulation algorithm. Therefore, our goal is to identify blocks with large $s_\lambda(B)$ thereby allowing for greater range of r to be simulated. To aid in this task, we present the following lemma from [30].

Lemma 4.2.1. *Consider a region KL of qubits embedded in a larger lattice. Consider cutting the region into two disjoint subregions K and L (i.e. we remove the CZ gates joining these two regions). Then we have the following relationships. For any region F whatsoever:*

$$s(F) \geq s_\lambda(F) \tag{4.7}$$

For the region KL and its subregions K and L:

$$s(KL) \leq \min\{s(K), s(L)\} \tag{4.8}$$

$$s_\lambda(KL) \geq \min\{s_\lambda(K), s_\lambda(L)\} \tag{4.9}$$

In particular suppose that the two subregions K and L are identical (i.e. correspond to isomorphic graphs), then in that case we would have (writing $K = L$ to denote that the subregions are isomorphic):

$$s(LL) \leq s(L) \tag{4.10}$$
$$s_\lambda(LL) \geq s_\lambda(L) \tag{4.11}$$

Proof. For details of the proof see [30]. □

The usefulness of this result lies in its ability to help define sequences that emerge when blocks are combined in the coarse graining approach, hence capturing the efficient classical simulatability of r.

To see this, suppose we divide the 2D lattice into square blocks of size 2×2. To construct a sequence of larger blocks, we can start with a single 2×2 block B_1 and then recursively combine two copies of the previous block B_{n-1} to create the next block B_n. We can then define two sequences:

$$u_n = s(B_n), \tag{4.12}$$

which denotes the maximum r such that the operator $\rho(B_n, r)$ is positive w.r.t the permitted measurements. Similarly define

$$l_n = s_\lambda(B_n). \tag{4.13}$$

which denotes the maximum r such that the operator $\rho_\lambda(B_n, r)$ is positive w.r.t the permitted measurements. From lemma 4.2.1, we have that $u_n \geq l_n$, l_n is a non-decreasing sequence and u_n is a non-increasing sequence. To denote their limits, we use:

$$u := \lim u_n \tag{4.14}$$
$$l := \lim l_n. \tag{4.15}$$

Therefore, if input cylinders are drawn with r that satisfies $r < l$, then the system can be efficiently classically simulated. If the radii r exceed the upper limit u (i.e., $r > u$), then negative probabilities arise, and we cannot apply our classical simulation algorithm.

4.2.1 Numerical Results

Recall that the block operator $\rho(B,r)$ denotes the operator resulting from applying the internal CZ gates to all the cylinders in an arbitrary extremal cylinder state with radius r and $z=1$. And that $\rho_\lambda(B,r)$ denotes the operator resulting from applying the internal CZ gates within the block of cylinders in extremal cylinder states with radius r and $z=1$ on the interior qubits, while the qubits on the boundary of the rectangle are prepared in extremal cylinder states with a radius that grows according to the number of external CZ gates.

We make the observation that we can replace the cylinder states that do not have any external CZs acting on them with qubits from the Bloch sphere. This replacement allows us to define another sequence:

$$\tilde{l}_n = \tilde{s}_\lambda(B_n), \tag{4.16}$$

which denotes the maximum r such that the operator $\tilde{\rho}_\lambda(B_n,r)$ is positive w.r.t the permitted measurements. And the operator $\tilde{\rho}_\lambda(B_n,r)$ denotes the operator resulting from the right-hand side of figure 4.3, but where crucially the interior states are qubits (with radius r). We have numerically (see appendix A.2 for corresponding Matlab code) calculated $\tilde{l}_1$ for several block sizes, with the results presented in table 4.1. By considering cylinder input extrema of the form $(I+\alpha X+Z)/2$ and measurement projectors $(I-X)/2$, we find that (see figure 4.4) the sequence $\tilde{l}_1$ provides an improvement over l_1. This means that for $r \leq \tilde{l}_1$, there is slight improvement compared to l_1, in the range of inputs that can be efficiently classically simulated.

Block sizes	l_1	$\tilde{l}_1$
3×3	0.0795	0.0799
3×4	0.0822	0.0828
4×4	0.0851	0.0859
4×5	0.0868	0.0877
5×5	0.0885	0.0895
5×6	0.0895	0.0909
6×6	0.0906	0.0917
6×7	0.0913	0.0924

Table 4.1 This table compares the values of l_1 and $\tilde{l}_1$ for different block sizes. l_1 and $\tilde{l}_1$ denote the maximum r such that the operators $\rho_\lambda(B_n,r)$, $\tilde{\rho}_\lambda(B_n,r)$, respectively, are positive w.r.t the permitted measurements.

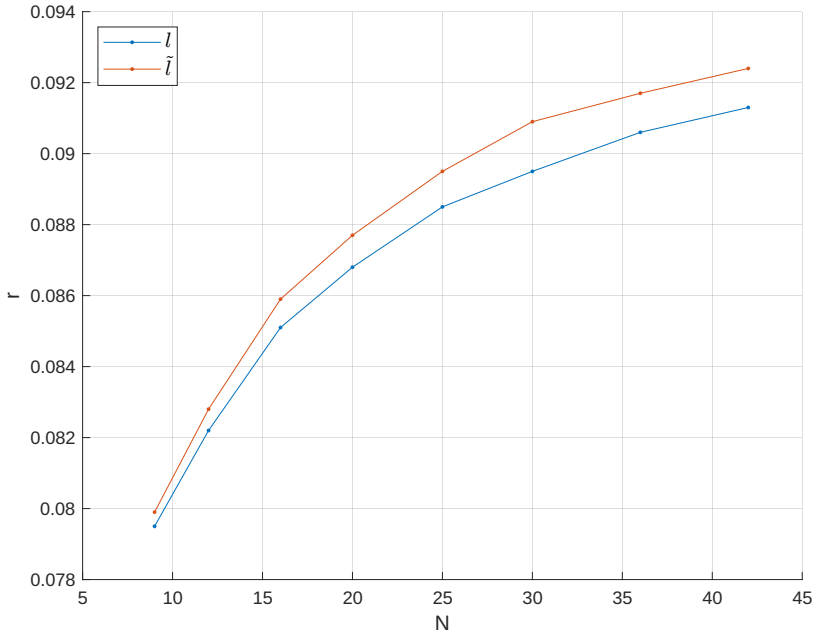


Fig. 4.4 This figure shows the sequences l_1 and $\tilde{l}_1$ for different block sizes. On the x-axis, the value N denotes the product of the width and height of each block, as given in table 4.1. The sequences were calculated using cylinder input extrema of the form $(I+\alpha X+Z)/2$ and measurement projectors $(I-X)/2$.

4.3 Maintaining Cylinder Separability under a Controlled-Phase Gate

In Sec. 3.2.2, the key result was that a CZ can be interpreted as a gate giving separable output, provided that (3.9) is satisfied. In this section, we consider generalising the result of lemma emma 3.2.1 in Sec.3.2.2, to arbitrary 2-qubit gates that are diagonal in the computational basis:

$$e^{i\varphi_1}|00\rangle\langle 00| + e^{i\varphi_2}|01\rangle\langle 01| + e^{i\varphi_3}|10\rangle\langle 10| + e^{i\varphi_4}|11\rangle\langle 11|, \tag{4.17}$$

where $0 \leq \varphi_i \leq 2\pi$. In fact, it can be easily verified that this gate is equivalent to a controlled phase gate up to local Z-rotations. To see this, as a first step, we can remove the parameter φ_1 in equation (4.17) by introducing a global phase. Next, we act with local Z-rotations, with angles γ_1 and γ_2 resulting in:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i(\varphi_2-\varphi_1-\gamma_2)} & 0 & 0 \\ 0 & 0 & e^{i(\varphi_3-\varphi_1-\gamma_1)} & 0 \\ 0 & 0 & 0 & e^{i(\varphi_4-\varphi_1-\gamma_1-\gamma_2)} \end{pmatrix}, \tag{4.18}$$

By setting $\gamma_1 = \varphi_3 - \varphi_1$ and $\gamma_2 = \varphi_2 - \varphi_1$, the resultant gate is of the form of a controlled-phase gate:

$$V_\varphi = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\varphi}|11\rangle\langle 11|, \tag{4.19}$$

where $\varphi = \varphi_4 + \varphi_1 - \varphi_2 - \varphi_3$.

The generalisation of the result in Section 3.2.2 is of interest due to its connections to existing literature on measurement-based quantum computing, where previous works have considered the computational power of using cylinder measurements and two-qubit gates that are diagonal in the computational basis [9, 50, 72]. Examples include weighted graph states (using a combination of CZ and controlled-phase gates V_φ with $\varphi = \pi/2$) [9], and parity-phase graph states [72], which have been shown to be capable of preparing universal resource states. On the other hand, in [21], it was shown that IQP circuits that have restrictions on the diagonal gates are still classically hard to simulate.

Lemma 4.3.1. *Consider the set $V_\varphi(\mathrm{Cyl}(r_A)\otimes\mathrm{Cyl}(r_B))$ of two qubit operators made by a controlled-phase gate V_φ, with $0 \le \varphi \le \pi$, acting on $\mathrm{Cyl}(r_A)\otimes\mathrm{Cyl}(r_B)$. Any operator in $V_\varphi(\mathrm{Cyl}(r_A)\otimes\mathrm{Cyl}(r_B))$ can be written in the generalised separable form:*

$$\sum_i p_i \rho_i^A \otimes \rho_i^B \tag{4.20}$$

where $\rho_i^A \in \mathrm{Cyl}(R_A)$ and $\rho_i^B \in \mathrm{Cyl}(R_B)$ if and only if:

$$\left(1+f_A^4\right)\left(1+f_B^4\right) - 2\left(f_A^2+f_B^2\right) + 2\cos\varphi\left(2-f_A^2-f_B^2\right)f_A^2 f_B^2 \ge 0, \tag{4.21}$$

where $f_A := r_A/R_A$ and $f_B := r_B/R_B$.

Proof. The task we consider is the following. Suppose a controlled-phase gate V_φ acts on a two particle product state $\rho_A \otimes \rho_B$, where ρ_A, ρ_B are cylinders states with radii r_A and r_B respectively. Our goal is to establish whether the output is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable. Before proceeding with the proof, we remark that at $\varphi = 0$, the entangling gate becomes

the identity and the output is trivially separable. Therefore, we will only need to consider $0 < \varphi \leq \pi$. It should be noted that this proof uses similar ideas to the proof of lemma 3.2.1 in Sec. 3.2.2.

As V_φ is a linear operator, we can use the same reasoning as used in the proof of lemma 3.2.1 to restrict our analysis to only consider whether the output from all extremal input states is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable. Furthermore, we will now show that we can reduce the number of input states we need to consider by exploiting properties of the controlled-phase gate and the symmetry of cylindrical state spaces.

Indeed, suppose that we have an explicit $\mathrm{Cyl}(r_A), \mathrm{Cyl}(r_B)$-separable decomposition:

$$V_\varphi(\rho_A \otimes \rho_B) = \sum_i p_i \omega_A^i \otimes \omega_B^i, \tag{4.22}$$

where $\omega_k^i \in \mathrm{Cyl}(R_k)$. Then we find we have the following observations.

1. Observe that any extremal input state $\rho_k \in \mathrm{Cyl}(r_k)$ can be expressed as $U_z^k([1, r_k, 0, \pm 1])$, where U_z^k is the rotation operator about the Z axis. Since U_z^k commutes with V_φ and cylinders are invariant under Z rotations, we have the $\mathrm{Cyl}(r_A), \mathrm{Cyl}(r_B)$-separable decomposition:

$$V_\varphi(U_z^A(\rho_A) \otimes U_z^B(\rho_B)) = \sum_i p_i U_z^A(\omega_A^i) \otimes U_z^B(\omega_B^i),$$

where $\omega_k^i \in \mathrm{Cyl}(R_k)$. This shows that the decomposition (4.22) is invariant up to local Z-rotations, and we may restrict inputs to the form

$$[1, r_A, 0, \pm 1] \otimes [1, r_B, 0, \pm 1].$$

2. If both inputs have $z = -1$, then the input extrema:

$$([1, r_A, 0, -1] \otimes [1, r_B, 0, -1]),$$

can be expressed as

$$X^A \otimes X^B([1, r_A, 0, 1] \otimes [1, r_B, 0, 1]).$$

Next, applying the identity $V_\varphi(X \otimes X) = (X \otimes U_Z X) V_\varphi$ to the input and using (4.22), we obtain another separable decomposition:

$$V_\varphi\left(X^A(\rho_A)\otimes X^B(\rho_B)\right)=\sum_i p_i X\omega_A^i X^\dagger\otimes U_z^B\left(X\omega_B^i X^\dagger\right),$$

where U_z^B is a Z-rotation with angle φ. This shows that if $z_A=z_B=-1$, this is equivalent to determining when the output from input extremum $z_A=z_B=1$ are separable. Therefore, we do not need to check the input $[1,r_A,0,-1]\otimes[1,r_B,0,-1]$.

3. Next, consider input states of the form

$$[1,r_A,0,1]\otimes[1,r_B,0,-1]$$

and

$$[1,r_A,0,-1]\otimes[1,r_B,0,1].$$

As V_φ is symmetric between the two input states, we can switch the control and target state, therefore we need only consider one input extremum where the z-components are not the same.

4. At this stage, we have managed to reduce the inputs we need to consider to

$$[1,r_A,0,1]\otimes[1,r_B,0,\pm1].$$

However, we will find it convenient to consider one input extremum $\left[1,r_{A/B},0,1\right]$ but with two possible transformations. Suppose V_φ acts on inputs

$$([1,r_A,0,1]\otimes[1,r_B,0,-1]),$$

then it is easy to verify that this equivalent to

$$V_{-\varphi}([1,r_A,0,1]\otimes[1,r_B,0,1]),$$

where we have used the identity $V_\varphi(I\otimes X)=(I\otimes X)V_{-\varphi}$. We will later find that having this alternative expression will make it easy to see the equivalence to $V_{-\varphi}$ acting on $[1,r_A,0,1]\otimes[1,r_B,0,1]$.

In summary, the observations have reduced the task to determining whether the output of V_φ and $V_{-\varphi}$ acting on one input extremum:

$$([1,r_A,0,1]\otimes[1,r_B,0,1]) \tag{4.23}$$

is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable.

To begin with, we consider V_φ acting on (4.23). This operator can be expressed in the Pauli basis as

$$\begin{bmatrix} 1 & r_B & 0 & 1 \\ r_A & r_A r_B(\cos(\varphi)+1)/2 & r_A r_B \sin(\varphi)/2 & r_A \\ 0 & r_A r_B \sin(\varphi)/2 & r_A r_B(1-\cos(\varphi))/2 & 0 \\ 1 & r_B & 0 & 1 \end{bmatrix}. \tag{4.24}$$

If the above equation is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable then it can be given the decomposition

$$\sum_i p_i \begin{bmatrix} 1 \\ R_A\cos(\theta_i) \\ R_A\sin(\theta_i) \\ 1 \end{bmatrix} \begin{bmatrix} 1 & R_B\cos(\phi_i) & R_B\sin(\phi_i) & 1 \end{bmatrix}. \tag{4.25}$$

Setting equation (4.24) equal to (4.25), and left multiplying by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/R_A & 0 & 0 \\ 0 & 0 & 1/R_A & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.26}$$

and right multiplying by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/R_B & 0 & 0 \\ 0 & 0 & 1/R_B & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{4.27}$$

we arrive at the following expression:

$$\begin{bmatrix} 1 & f_B & 0 & 1 \\ f_A & f_A f_B(\cos(\varphi)+1)/2 & f_A f_B \sin(\varphi)/2 & f_A \\ 0 & f_A f_B \sin(\varphi)/2 & f_A f_B(1-\cos(\varphi))/2 & 0 \\ 1 & f_B & 0 & 1 \end{bmatrix} = \sum_i p_i \begin{bmatrix} 1 \\ \cos(\theta_i) \\ \sin(\theta_i) \\ 1 \end{bmatrix} [1, \cos(\phi_i), \sin(\phi_i), 1], \tag{4.28}$$

where we have simplified notation by defining $f_A := r_A/R_A$ and $f_B := r_B/R_B$. The above equation states that the operator (4.24) is $\mathrm{Cyl}(R_A), \mathrm{Cyl}(R_B)$-separable if and only if (4.28) is

$\mathrm{Cyl}(1),\mathrm{Cyl}(1)$-separable.

We will now see that determining whether the LHS of (4.28) is $\mathrm{Cyl}(1),\mathrm{Cyl}(1)$-separable is equivalent to checking quantum separability of a two qubit quantum operator. First, suppose that we have the quantum separable decomposition

$$\begin{bmatrix} 1 & f_B & 0 & 0 \\ f_A & f_A f_B(\cos(\varphi)+1)/2 & f_A f_B \sin(\varphi)/2 & 0 \\ 0 & f_A f_B \sin(\varphi)/2 & f_A f_B(1-\cos(\varphi))/2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \sum_i p_i [1, x_A^i, y_A^i, z_A^i] \otimes [1, x_B^i, y_B^i, z_B^i]. \tag{4.29}$$

As (4.29) is quantum separable, it is quantum separable where the local terms of the RHS of (4.29) have $z_A^i = z_B^i = 0$, for all i. Now given such a decomposition, by setting $z_A^i = z_B^i = 1$ for all i, it then follows that

$$\sum_i p_i [1, x_A^i, y_A^i, 1] \otimes [1, x_B^i, y_B^i, 1] \tag{4.30}$$

is a $\mathrm{Cyl}(1),\mathrm{Cyl}(1)$-separable decomposition for

$$\begin{bmatrix} 1 & f_B & 0 & 1 \\ f_A & f_A f_B(\cos(\varphi)+1)/2 & f_A f_B \sin(\varphi)/2 & f_A \\ 0 & f_A f_B \sin(\varphi)/2 & f_A f_B(1-\cos(\varphi))/2 & 0 \\ 1 & f_B & 0 & 1 \end{bmatrix}. \tag{4.31}$$

Conversely, suppose now that (4.31) has a $\mathrm{Cyl}(1),\mathrm{Cyl}(1)$-separable decomposition, given by 4.30). By setting $z_A^i = z_B^i = 0$, for all i in (4.30) we find that we can recover the LHS of (4.28) thereby giving a quantum separable decomposition. Therefore, we have established that the LHS of (4.28) is $\mathrm{Cyl}(1),\mathrm{Cyl}(1)$-separable if and only if the operator

$$\begin{bmatrix} 1 & f_B & 0 & 0 \\ f_A & f_A f_B(\cos(\varphi)+1)/2 & f_A f_B \sin(\varphi)/2 & 0 \\ 0 & f_A f_B \sin(\varphi)/2 & f_A f_B(1-\cos(\varphi))/2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.32}$$

is quantum separable. In order for the operator (4.32) to be quantum separable, it must be both positive and a PPT operator. The partial transpose of (4.32) with respect to particle A is

$$\begin{bmatrix} 1 & f_B & 0 & 0 \\ f_A & f_A f_B(\cos(\varphi)+1)/2 & f_A f_B \sin(\varphi)/2 & 0 \\ 0 & -f_A f_B \sin(\varphi)/2 & -f_A f_B(1-\cos(\varphi))/2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{4.33}$$

At this point, it is easy to see the equivalence of determining the eigenvalues of (4.32) if instead we had used $V_{-\varphi}$. To see this, notice that cosine is an even function and the sine terms would acquire a change of sign, therefore this operator would be related to (4.33) by a $I \otimes X$ transformation and would have the same eigenvalues. Furthermore, equations (4.32) and (4.33) can be interconverted by the unitary $X \otimes I$. Hence, the eigenvalues of the two operators are equivalent, and we only need to check the minimum eigenvalues of one of these operators, say (4.32). This operator can be expressed in the computational basis as

$$\begin{pmatrix} 1 & f_B & f_A & f_A f_B e^{-i\varphi} \\ f_B & 1 & f_A f_B & f_A \\ f_A & f_A f_B & 1 & f_B \\ f_A f_B e^{i\varphi} & f_A & f_B & 1 \end{pmatrix} \tag{4.34}$$

We now need to determine when (4.34) is a non-negative operator. To start with, note that (4.34) can be expressed as

$$(I + f_A X) \otimes (I + f_B X) + f_A f_B (e^{-i\varphi} - 1) |00\rangle \langle 11| + f_A f_B (e^{i\varphi} - 1) |11\rangle \langle 00|. \tag{4.35}$$

Furthermore, to simplify notation we set $f_A f_B (e^{i\varphi} - 1) = c e^{i\gamma}$, where c is real and non-negative. Thus, the above equation can be rewritten as

$$(I + f_A X) \otimes (I + f_B X) + c \left(e^{-i\gamma} |00\rangle \langle 11| + e^{i\gamma} |11\rangle \langle 00| \right). \tag{4.36}$$

To show that (4.36) is non-negative, we will have to consider three cases.

i) The first case is if $f_A > 1$ and/or $f_B > 1$. Suppose that (4.32) is separable, then it is straightforward to show that the expected value $X \otimes I$ is greater than 1, which is impossible for a separable quantum state.

ii) The second is if $f_A = 1$ and/or (by symmetry) $f_B = 1$. Suppose $f_A = 1$ then the term $(I + f_A X) \otimes (I + f_B X)$ in (4.36) has at least two zero eigenvalues, with eigenstates $|--\rangle$ and $|-+\rangle$. We may compute

$$\langle -+ | c \left(e^{i\gamma} |00\rangle \langle 11| + c e^{-i\gamma} |11\rangle \langle 00| \right) |-+\rangle = -\frac{c}{2} \cos(\gamma) \tag{4.37}$$

and

$$\langle --| c\left(e^{i\gamma}|00\rangle\langle 11| + ce^{-i\gamma}|11\rangle\langle 00|\right)|--\rangle = \frac{c}{2}\cos(\gamma). \tag{4.38}$$

Therefore, as long as $c\cos(\gamma) \neq 0$ either (4.37) or (4.38) will be negative. The only way $c\cos(\gamma) = 0$ is if V_φ is the identity, which we do not need to consider as the output would be trivially separable. Additionally, we also do not need to consider $f_A = 0$ and/or $f_B = 0$ as this would also lead to the output being trivially separable. This means that if $f_A = 1$ and/or (by symmetry) $f_B = 1$, then we have at least one negative eigenvalue and the output is not separable.

iii) The third case is if $f_A, f_B < 1$. Suppose that we add and subtract $c\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)$ to (4.36), we then have

$$\begin{aligned}(I + f_A X)\otimes(I + f_B X) + c\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) \\ -c\left(|00\rangle\langle 00| + |11\rangle\langle 11| - e^{-i\gamma}|00\rangle\langle 11| - e^{i\gamma}|11\rangle\langle 00|\right).\end{aligned} \tag{4.39}$$

Observe that (4.39) can be considered to be a sum of two operators. The top line in (4.39) is a positive-definite operator, while the bottom line is an operator with eigenvalues of $(0,0,0,-2c)$. We denote these operators as P and R, respectively.

To proceed, we shall make use of the Weyl inequalities [81], which assert that if R, P are $n \times n$ Hermitian matrices, and $\{\lambda_i(R)\}_{i=1}^n$, $\{\lambda_i(P)\}_{i=1}^n$ and $\{\lambda_i(R+P)\}_{i=1}^n$ denote the sets of eigenvalues of R, P, and $R+P$, in decreasing order, then

$$\lambda_i(R) + \lambda_n(P) \leq \lambda_i(R+P) \leq \lambda_i(R) + \lambda_1(P), \tag{4.40}$$

for $1 \leq i \leq n$. Additionally, it follows that if P is positive-definite, then $\lambda_i(R) < \lambda_i(R+P)$, for all i.

Therefore, by noting that P and R are Hermitian and P is a positive-definite operator, the application of the Weyl inequalities yield the following inequalities

$$0 < \lambda_1(R+P) \tag{4.41}$$
$$0 < \lambda_2(R+P) \tag{4.42}$$
$$0 < \lambda_3(R+P) \tag{4.43}$$
$$-2c < \lambda_4(R+P). \tag{4.44}$$

Consequently, for the case of $f_A, f_B < 1$, these inequalities show that (4.34) has three strictly positive eigenvalues and at most 1 negative eigenvalue $\lambda_4(R+P)$. Under the assumption that $f_A, f_B < 1$, we have that (4.34) is non-negative if and only if its determinant:

$$\left(1+f_A^4\right)\left(1+f_B^4\right) - 2\left(f_A^2+f_B^2\right) + 2\cos\varphi\left(2-f_A^2-f_B^2\right)f_A^2 f_B^2 \tag{4.45}$$

is non-negative. Moreover, for $f_A, f_B < 1$, the non-negativity of the determinant becomes necessary and sufficient as a test for cylinder separability.

□

In appendix A.3 we explicitly show how to calculate the determinant of (4.34). We will now focus on the implications of lemma 4.3.1 and discuss what the result means for the growth rate. Recall that the growth factors, denoted as $g_i := R_i/r_i$, represent the factor by which the radii of the output state space need to increase for the controlled-phase operation to be cylinder separable. If we impose a symmetric growth rate restriction $f = f_A = f_B$, the determinant given by (4.45) simplifies to:

$$\left(1-f^2\right)\left[\left(1-f^2\right)^3 + 4(\cos\varphi - 1)f^4\right]. \tag{4.46}$$

Therefore, in the symmetric case ($R_A = R_B$), the condition in lemma 4.21 simplifies and any operator in $V_\varphi(\mathrm{Cyl}(r)\otimes\mathrm{Cyl}(r))$ can be given the separable decomposition:

$$\sum_i p_i \rho_i^A \otimes \rho_i^B,$$

where $\rho_i^A, \rho_i^B \in \mathrm{Cyl}(R)$ if and only if:

$$\left(1-\frac{r^2}{R^2}\right)^3 + 4(\cos\varphi - 1)\left(\frac{r}{R}\right)^4 \geq 0. \tag{4.47}$$

By numerically varying φ we can determine the required growth rate g for the controlled-

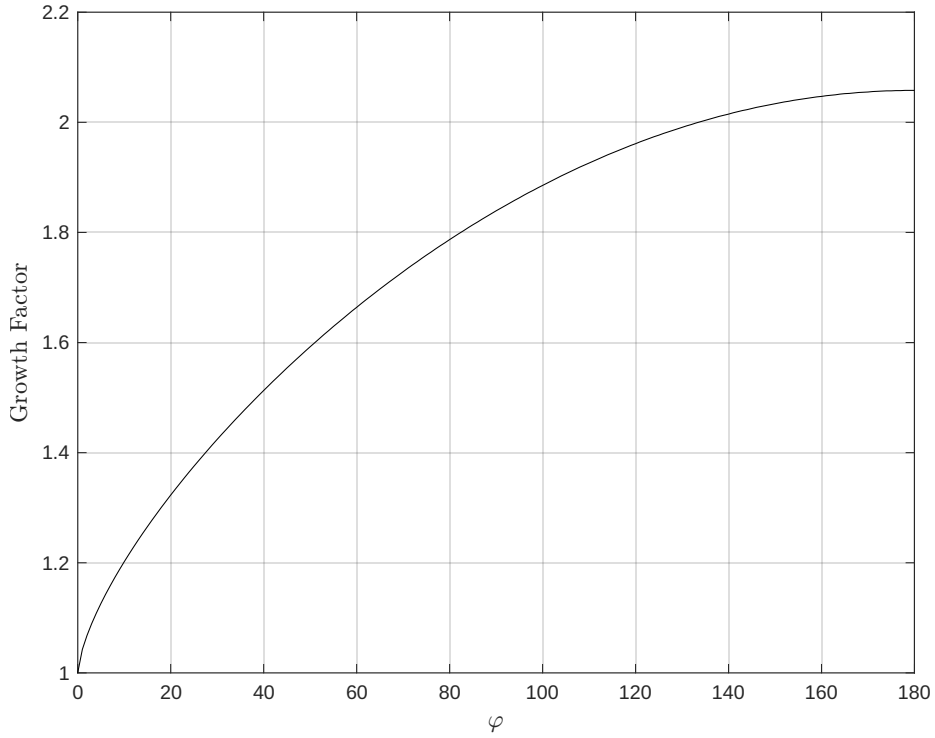


Fig. 4.5 This figure displays the growth factor g, as φ varies from 0 to π. The growth factor is the factor by which the output state space radii is required to increase for the controlled-phase operation to be considered a separable operation.

phase operation to be separable. This is shown in figure 4.5. At $\varphi = 0$ the controlled-phase gate performs the identity gate and the output state space is trivially separable, hence in figure 4.5 the growth factor is 1 (i.e., requiring no growth in the output radii to maintain separability). When $\varphi = \pi$, the controlled-phase gate becomes a CZ operation and the maximum growth rate 2.058 is attained. We can also consider a region of pure input states, of the form $(I + \sin(\theta)X + \cos(\theta)Z)/2$, that can be efficiently classically simulated. Instead of r, we use the polar angle $\theta = \sin^{-1}(r)$ that a pure state of radius r would make with the z-axis. In figure 4.6 we have plotted the polar angle θ against φ, showing for a given value of φ, when the system is classically efficiently simulatable.

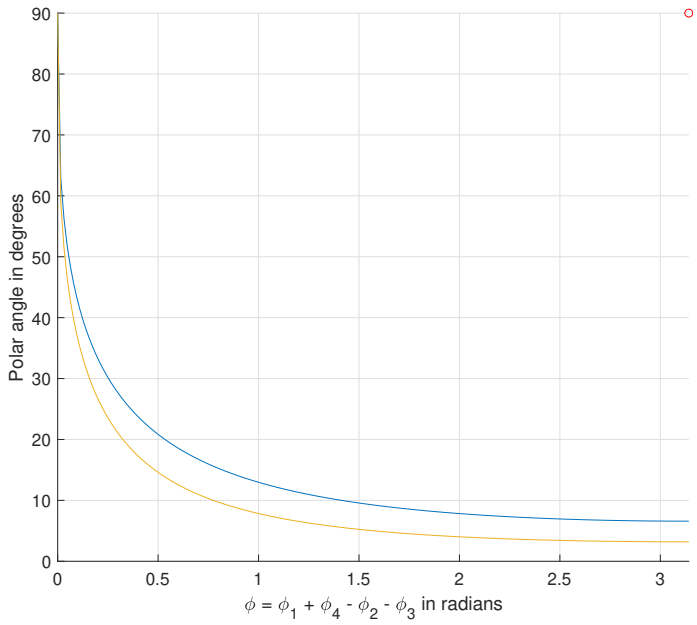


Fig. 4.6 This is a plot of the polar angle θ against φ. The point (φ,θ) represents the pure states one gets by placing states $(I+\sin(\theta)X+\cos(\theta)Z)/2$ on the nodes of a graph and interacting them with arbitrary two-qubit diagonal gates $e^{i\varphi_1}|00\rangle\langle 00|+e^{i\varphi_2}|01\rangle\langle 01|+e^{i\varphi_3}|10\rangle\langle 10|+e^{i\varphi_4}|11\rangle\langle 11|$ such that $\varphi=\varphi_4+\varphi_1-\varphi_2-\varphi_3$. The upper curve corresponds to lattices of degree $D=3$ and the lower curve corresponds to lattices of degree $D=4$. In each case for a given value of φ the system is classically efficiently simulatable. Note that the red dot in the top right-hand corner indicates the ideal cluster state.

4.4 Obtaining a Separable Decomposition via Linear Programming

In this chapter so far, we have constructed an efficient classical simulation algorithm based on cylinder separability. The key result that allows this is that for $\rho^A,\rho^B\in \mathrm{Cyl}(r)$ we have the following decomposition:

$$CZ(\rho_A\otimes\rho_B)=\sum_i p_i\omega_A^i\otimes\omega_B^i, \tag{4.48}$$

where $\omega_i^A,\omega_i^B\in\mathrm{Cyl}(R)$ such that $g\cdot r=R$, where $g=2.058$. Furthermore, from the dual constraint, the output radii R must also satisfy the condition $g^D r\leq 1$, where D is the degree of the lattice. However, one can consider whether there are state spaces that are "better" (i.e. can be shown to be separable w.r.t a lower growth rate than the cylinder), and allow for a

greater range of r to be classically simulated.

In this section, we investigate this possibility by introducing two state spaces, where key will be to convert a separability problem into a linear programming problem. In Sec.4.4.1 we will first introduce a state space that we call the Protruding state space, illustrated in figure 4.7. By converting to a linear program, we find in Sec.4.4.3 that the Protruding state space requires greater growth to maintain separability than the cylinder state space. Secondly, in Sec.4.4.4 we introduce a cylinder-cone state space, depicted in figure 4.8. For this state space, we find that there is a very slight improvement in the growth required for maintaining a separable decomposition.

4.4.1 The Protruding State Space

To begin to answer whether there are state spaces which maintain a separable decomposition with lower radius growth than that of cylinders, we have the following result from [31], to help us.

Consider two sets S_A and S_B that represent the local state spaces for particles A and B, respectively. Each state space is represented by a compact set of Bloch vectors $[x,y,z]$, where $z = \pm 1$ and $x, y \neq 0$. Suppose that we act with a CZ gate on $S_A \otimes S_B$, then we need to find the minimum required radius growth R for $CZ(S_A \otimes S_B)$ to be S_A, S_B-separable. If such a value of R exists, we denote the optimum value of R as R^*. We can now state the (adapted) lemma from [31].

Lemma 4.4.1. *Consider compact sets (S_A, S_B) such that $R^*(S_A, S_B)$ exist. Assume that the sets contain a Bloch vector of the form $[x,y,\pm 1]$ for some $x, y \neq 0, 0$.Then the cylinders can only have a lower value of R^*, the radial growth needed to maintain separability when acted on by a CZ.*

Taking into account this observation, we can limit our attention to state spaces that have a single point at both the top and bottom, as well as shapes that exhibit rotational symmetry about the z-axis. One state space that satisfies these observations is what we refer to as the Protruding state space.

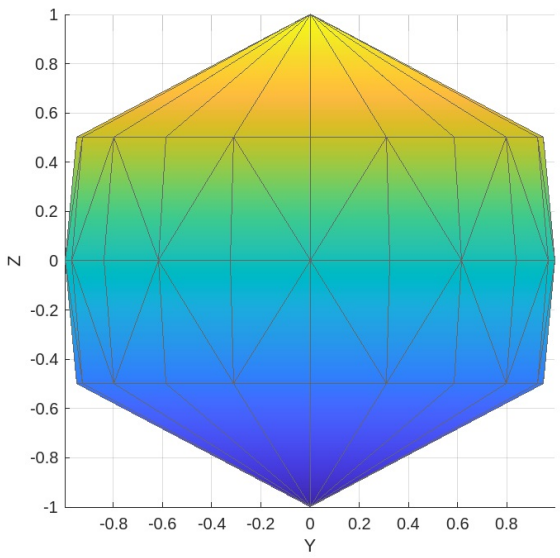


Fig. 4.7 This figure illustrates the Protruding state space in the YZ plane with $r = 1$, $\zeta = 0.1$ and $h = 0.5$. The parameter θ has been discretised with 20 points around the XY plane.

Definition 4.4.1. *The Protruding State Space, denoted $\mathscr{P}(r,h,\zeta)$, is defined to be the convex hull of operators with Bloch vectors*

$$\{(0,0,\pm 1),(r\cos\theta, r\sin\theta, 0),(r\omega\cos\theta, r\omega\sin\theta, \pm h)\}, \tag{4.49}$$

where $\theta \in [0,2\pi]$ and $\omega = \sqrt{1-h^2}(1+\zeta)$. We will consider varying parameters $\zeta \in \mathbb{R}$ and $h \in [0,1]$.

In equation (4.49), the Bloch vector $(0,0,\pm 1)$ describes the states from the top and bottom of the state space, while the states that lie on the XY-plane with radius r are given by $(r\cos\theta, r\sin\theta, 0)$. Additionally, the states that lie in between are given by $(r\omega\cos\theta, r\omega\sin\theta, \pm h)$, with angle θ, ω is the protrusion parameter, and h denotes the height. When $\zeta = 0$ and $r = 1$, the vector $(r\omega\cos\theta, r\omega\sin\theta, \pm h)$ corresponds to a point on the Bloch sphere. In the following, we will vary ζ leading to state spaces that extend beyond the surface of the Bloch sphere, figure 4.7. Notice that if $\omega > 1$ then the state space is a non-convex set. Conversely, if $\zeta \leq (1-h^2)^{-1/2} - 1$, then the state space remains a convex set.

4.4.2 A Linear Programming Approach to the Separability Problem

Consider a two particle product state $\rho_A \otimes \rho_B$, where $\rho_A, \rho_B \in \mathscr{P}(r,h,\zeta)$. We would like to determine whether the output of a CZ, acting on all such possible inputs, can be given the separable decomposition:

$$\sum_i p_i \omega_A^i \otimes \omega_B^i, \tag{4.50}$$

where $\omega_k^i \in \mathscr{P}(r,h,\zeta)$. We will show, through state vectorisation[2], that determining whether the output can be given a separable decomposition can be transformed into a linear programming problem. Before we proceed, we will briefly define a linear programming problem and introduce some terminology. A comprehensive introduction to linear programming can be found in [82].

Definition 4.4.2. *[82] A problem is a said to be a general linear program if it has the form*

$$\begin{array}{ll} \text{minimise} & c^T x \\ \textit{subject to} & Ax \preceq b \\ & A_{eq} x = b_{eq}, \end{array} \tag{4.51}$$

where $A \in \mathbb{R}^{m\times n}$, $A_{eq} \in \mathbb{R}^{p\times n}$, and the objective linear function C and the constraint functions are affine.

The minimisation of $c^T x$ is subject to a linear inequality and a linear equality, where $\preceq$ denotes componentwise inequality. A feasible solution to a linear program is a solution that satisfies all the above constraints. An optimal solution to a linear program is the feasible solution with the smallest objective function value.

Returning to the task at hand, we are given a two particle state ρ_{AB} and would like to determine if the following decomposition holds:

$$\rho_{AB} = \sum_i x_i \rho_i^A \otimes \rho_i^B, \tag{4.52}$$

where ρ_i^A, ρ_i^B are local operators and x_i is a probability distribution. The key idea is to represent equation (4.52) in terms of a linear inequality and equality satisfying (4.51). To do

[2]Representing each state in terms of a column vector containing its Pauli expansion coefficients.

this, express the LHS side of (4.52) in the Pauli basis:

$$\rho_{AB} = \frac{1}{4}\sum_{i,j}\rho_{i,j}\sigma_i \otimes \sigma_j, \tag{4.53}$$

where σ_i, σ_j are the Pauli matrices and $\rho_{i,j}$ are expansion coefficients. Then we can represent ρ_{AB} as a 16 element column vector:

$$b_{eq} = (\rho_{1,1}, \rho_{1,2}, \ldots, \rho_{4,3}, \rho_{4,4})^T. \tag{4.54}$$

Similarly, we can vectorise the output state space, the RHS of (4.52), by creating a matrix A_{eq} that represents the convex hull of product states $\rho_i^A \otimes \rho_i^B$ in vectorised form:

$$A_{eq} = \begin{pmatrix} g_1 & g_2 & \cdots & g_D \end{pmatrix}. \tag{4.55}$$

Here, each g_i is a 16×1 column vector that contains the Pauli expansion coefficients of an extremal product state. Therefore, A_{eq} will a matrix of dimension $16 \times D$, where D is the cardinality of the convex hull, i.e. the number of extremal product states of the output state space. Next, we need to ensure that $x_i \geq 0$ since it represents a probability distribution. To impose this condition, we make use of the inequality in (4.51) and set

$$A = \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}, \quad \text{and} \quad b = (0, 0, \cdots, 0)^T, \tag{4.56}$$

where A is a $D \times D$ dimensional matrix and b is a $D \times 1$ column vector. Therefore, we have expressed (4.52) as a linear equality in equation (4.51). Furthermore, we have used the linear inequality in (4.51) to impose the condition that the probability distribution must be non-negative.

Finally, we can set the objective function to be arbitrary, such as a zero vector, as we are not concerned about minimising the objective function. Instead, we would like to determine whether the linear programming problem has a feasible solution. If there exists a feasible solution, then we have determined that (4.51) holds.

4.4.3 LP-Based Separable Decompositions for Protruding States

Previously, we showed that testing for a separability decomposition can be transformed into a linear programming problem. We will now apply this approach to Protruding state spaces, determining the required radius growth to achieve separable output with respect to these state spaces. We will first show that with similar reasoning as used in Sec.3.9 (and Sec.4.3), we can reduce the number of input states we need to consider by using properties of the *CZ* gate and the symmetries of the state spaces.

Recall the set of extremal states of $\mathscr{P}(r,h,\zeta)$ are described by the Bloch vectors

$$\{(0,0,\pm 1),(r\cos\theta,r\sin\theta,0),(r\omega\cos\theta,r\omega\sin\theta,\pm h)\}. \tag{4.57}$$

The task is to determine whether the output of a *CZ*, acting on all such possible inputs, can be given a separable decomposition if the operators in the separable decomposition are drawn from $\mathscr{P}(R,h,\zeta)$.

Following the same line of reasoning as used in Sec.3.2.2 we can decrease the number of input extrema that must be considered. Clearly, input states of the form $[1,0,0,\pm 1]$ do not need to be considered as the *CZ* acts trivially on them. Secondly, as local Z-rotations commute with the *CZ* gate and the fact that $\mathscr{P}(r,h,\zeta)$ is invariant under Z-rotations, we only need to consider inputs states with a fixed angle, for convenience we consider $\theta = 0$. Furthermore, by the same argument as used in the proof lemma emma 3.2.1, we do not need to consider the states with z-component $-h$. Lastly, for convenience we will take the input radius $r = 1$, therefore the output radius R will be the growth rate as $g = R/r$. In summary, we can reduce the number of input states we need to consider to states of the form:

$$\begin{aligned} &[1,1,0,0]\otimes[1,1,0,0],\\ &[1,1,0,0]\otimes[1,\omega,0,0.5],\\ &[1,\omega,0,0.5]\otimes[1,\omega,0,0.5]. \end{aligned} \tag{4.58}$$

We now need to determine when the output of a *CZ* gate acting on every input extrema (4.58) is $\mathscr{P}(r,h,\zeta)$-separable. For each input extrema in (4.58) we proceed with the subsequent procedure, previously described in Sec.4.4.

Step 1: Without loss of generality, consider $[1,1,0,0]\otimes[1,1,0,0]$. Expressing the output of the *CZ* gate acting on this input in the Pauli basis:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{4.59}$$

This allows us to easily note the non-zero Pauli coefficients and form the vector representing our input state:

$$b_{eq} = (1,0,0,0,0,0,0,1,1,0,0,1,0,0,1,0,0)^T, \tag{4.60}$$

with $\rho_{11} = \rho_{2,4} = \rho_{3,3} = \rho_{4,2} = 1$.

Step 2: To form the matrix A_{eq}, we discretise the single particle output state space $\mathscr{P}(r,h,\zeta)$ by selecting a finite number of θ values, $\theta \in 0, N, 2N, \ldots, 2\pi - N$, where N is a non-zero interval in terms of π. Then, we use the Pauli expansion coefficients of the extremal product states to create each column vector of A_{eq}. We can then represent the single particle state space of each particle A, B as a matrix, where each column contains the Pauli coefficients of an extremal product state:

$$S^{A/B} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & \cdots & 1 & \cdots \\ 0 & 0 & R & \cdots & R\omega & \cdots & R\omega & \cdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots \\ 1 & -1 & 0 & \cdots & h & \cdots & -h & \cdots \end{pmatrix}, \tag{4.61}$$

where $\omega = \sqrt{1-h^2}(1+\zeta)$. The first two columns contain the Pauli coefficients of $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, respectively. Starting from the third column, these are the states, of the form $[1, R\cos\theta, R\sin\theta, 0]$, that lie on the XY plane. The remaining matrix entries denote states that have height $\pm h$, these are the states of the form $[1, R\omega\cos\theta, R\omega\sin\theta, h]$. In total, the matrix $S^{A/B}$ will be of dimension $4 \times (2 + 6\pi/N)$. Note that the parameter we will be varying to determine if the output from the CZ is separable is R. The matrix A_{eq} can now be constructed to represent the output state space:

$$A_{eq} = S^A \otimes S^B,$$

where A_{eq} is a $16 \times D$ dimensional matrix, where $D = (2+6\pi/N)^2$. Lastly, we impose the condition that the probability distribution must be non-negative by setting A and b as in (4.56), where A is of size $D \times D$ and b is a D-dimensional column vector.

Step 3: The problem of finding a separable decomposition has now been transformed into a linear programming problem. By increasing the radii R of the output state space and running the linear program, we can check for a feasible solution. If the linear program does not return a feasible solution, we increase the value of R, and repeat the linear program with the new value of R. If the linear program does return a feasible solution, then we record the value of R.

Step 4: Repeat Steps 1-3 for the remaining input extrema. The minimum growth rate g required for $\mathscr{P}(R,h,\zeta)$-separability is the largest value of R that yields a feasible solution for each input extrema.

The results from running this procedure are summarised by the following observation and presented in table 4.2. In appendix A.5, we provide an example that clarifies this process.

Observation 4.4.1. *Any operator $CZ(\rho_A \otimes \rho_B)$, where ρ_A, ρ_B are drawn from $\mathscr{P}(r,h,\zeta)$ with $h \in [0,0.8]$ and $\zeta = \{0, 0.1, 1.1\}$, can be given a generalised separable decomposition*

$$\sum_i p_i \rho_i^A \otimes \rho_i^B, \tag{4.62}$$

where $\rho_i^A, \rho_i^B \in \mathscr{P}(R,h,\zeta)$, if $R \geq (2.415)r$.

4.4.4 The Cylinder-Cone State Space

Previously, we showed that cylindrical state spaces require a radius growth of 2.058 to maintain a separable decomposition. Using numerical methods, we then investigated whether Protruding state spaces required a lower growth rate to maintain a separable decomposition. However, we found that this was not true, as Protruding state spaces require at least a radius growth of 2.415.

In this section, we now look at a variation of the previous problem, where instead of Protruding state spaces, we consider state spaces that we call the Cylinder-Cone (CC) state

Height	ζ	XY-points	R
0.1	0	6	2.488
		10	2.432
		15	2.436
		20	2.415
0.1	0.1	6	2.484
		10	2.429
		15	2.439
		20	2.415
0.1	1.1	6	2.484
		10	2.429
		15	2.439
		20	2.415
0.2	0	6	2.458
	0	10	2.429
	0	15	2.438
	0	20	2.415
0.2	0.1	6	2.464
	0.1	10	2.438
	0.1	15	2.442
	0.1	20	2.415
0.2	1.1	6	2.464
	1.1	10	2.438
	1.1	15	2.442
	1.1	20	2.415
0.3	0	6	2.459
	0	10	2.433
	0	15	2.437
	0	20	2.415
0.3	0.1	6	2.476
	0.1	10	2.45
	0.1	15	2.437
	0.1	20	2.415
0.3	1.1	6	2.476
	1.1	10	2.45
	1.1	15	2.437
	1.1	20	2.415
0.4	0	6	2.465
	0	10	2.436
	0	15	2.441
	0	20	2.415
0.4	0.1	6	2.500
	0.1	10	2.448
	0.1	15	2.441
	0.1	20	2.415
0.4	1.1	6	2.5
	1.1	10	2.448
	1.1	15	2.441
	1.1	20	2.415

Height	ζ	XY-points	R
0.5	0	6	2.468
	0	10	2.442
	0	15	2.433
	0	20	2.415
0.5	0.1	6	2.507
	0.1	10	2.434
	0.1	15	2.424
	0.1	20	2.415
0.5	1.1	6	2.528
	1.1	10	2.434
	1.1	15	2.424
	1.1	20	2.415
0.6	0	6	2.484
	0	10	2.447
	0	15	2.435
	0	20	2.415
0.6	0.1	6	2.515
	0.1	10	2.447
	0.1	15	2.435
	0.1	20	2.415
0.6	1.1	6	2.528
	1.1	10	2.447
	1.1	15	2.435
	1.1	20	2.415
0.7	0	6	2.503
	0	10	2.447
	0	15	2.435
	0	20	2.415
0.7	0.1	6	2.528
	0.1	10	2.452
	0.1	15	2.437
	0.1	20	2.415
0.7	1.1	6	2.528
	1.1	10	2.452
	1.1	15	2.437
	1.1	20	2.415
0.8	0	6.0	2.528
	0	10.0	2.434
	0	15.0	2.424
	0	20.0	2.415
0.8	0.1	6.0	2.528
	0.1	10.0	2.452
	0.1	15.0	2.425
	0.1	20.0	2.415
0.8	1.1	6.0	2.528
	1.1	10.0	2.452
	1.1	15.0	2.425
	1.1	20.0	2.415

Table 4.2 This table shows that the output of a CZ acting on operators drawn from $\mathscr{P}(r,h,\zeta)$ with $r = 1$, remains separable w.r.t operators drawn from $\mathscr{P}(R,h,\zeta)$. Here ζ is a function of the protrusion parameter $\omega = \sqrt{1-h^2}(1+\zeta)$, XY-points denote the number of points θ has been discretised into, and R is the output radius. This shows that Protruding state spaces require radius growth 2.415 to maintain separability, which is greater than the cylinder state space growth 2.058.

space, illustrated in figure 4.8. The motivation for CC state spaces is that they contain cylinder states but crucially allowing for variations in the height of the extremal points of the set, see figure 4.8. By considering CC state spaces and using the numerical methods described in Sec.4.4, we will show that we can very slightly improve the range of r that we can efficiently classically simulate.

Definition 4.4.3. *The Cylinder-Cone State Space, denoted $S_{CC}(r,h)$, is defined to be the convex hull of operators with Bloch vectors*

$$\{(0,0,\pm 1),(r\cos\theta, r\sin\theta, \pm h)\}, \tag{4.63}$$

where $\theta \in [0,2\pi]$ and $r,h \in [0,1]$.

The CC state space with $h = 0.6$ and $r = \sqrt{1-h^2}$ is illustrated in figure 4.8. We will investigate the effects of changing the parameters r and h such that we obtain states that are not confined to the surface of the Bloch sphere. If, however, we impose the condition that $r = \sqrt{1-h^2}$ then the states with Bloch vector $(r\cos\theta, r\sin\theta, \pm h)$ describe a pure state from the Bloch sphere. Additionally, notice that if we set $h = 1$ and allow r to vary, then the CC state space is equivalent to the cylinder state space.

Let us now recall some information from Sec.3.2.2 on cylinder state spaces. As a first step, it was shown that a CZ operation on two input cylinders can be given a separable decomposition with respect to cylindrical state spaces, provided that the output cylinder radii grow by $g_C \approx 2.05817$. Repeating this, and imposing the dual constraint, the output radii R_{out} must satisfy the condition $g_C^D r_{in} \leq 1$, where D is the degree of the lattice and r_{in} denotes the radius with which the particle was initialised in. For example, if $D = 1$, this imposes a condition on the input radius: $r_{in} \leq 0.486$. Similarly, if $D = 2$ then $r_{in} \leq 0.236$, and $D = 3$ leads to $r_{in} \leq 0.115$.

Let us now consider a similar problem, where we will vary the first step and instead ask for CC-separability. Thereafter, we will use the usual notion of cylinder-separability, leading to conditions on r_{in}. More precisely, we wish to determine the radius growth $g_{cc} = R/r$ such that the decomposition

$$CZ(\rho_A \otimes \rho_B) = \sum_i p_i \omega_A^i \otimes \omega_B^i, \tag{4.64}$$

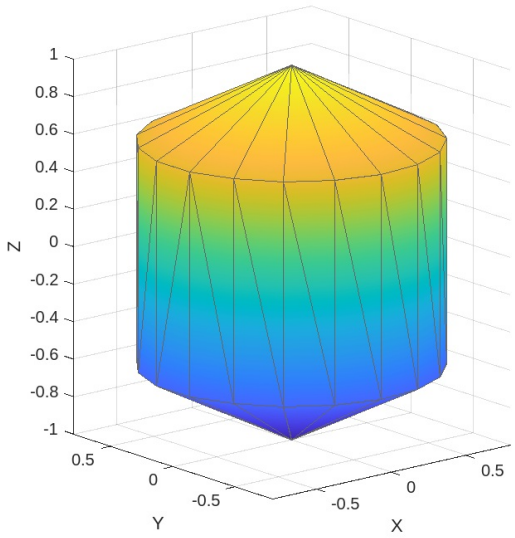


Fig. 4.8 This figure illustrates the Cylinder-Cone State space with $h = 0.6$ and $r = \sqrt{1-h^2}$. The parameter θ has been discretised with 20 points around the XY-plane. Notice that if $h = 1$ and r is non-zero then the CC state space is equivalent to the cylinder state space.

holds, where $\rho_k^i \in S_{CC}(r,h)$ with $r = \sqrt{1-h^2}$, and $\omega_k^i \in S_{CC}(R,1)$. Notice that the input operators from S_{CC} lie on the surface of the Bloch sphere, but the output operators in the decomposition have $H = 1$ and therefore are cylinders with radii R, this is illustrated in figure 4.10. To determine the radius growth g_{CC}, we will use the approach previously used in Sec.4.4.2, transforming the separability problem into a linear programming problem. We find that (4.64) holds for input radius $r = r_{in}$ and output radius $R = R_{out}$ with growth factor g_{CC} as shown in figure 4.9. From this figure we can make the following observation.

Observation 4.4.2. *Let $S_{CC}(r,h)$ and* Cyl(r) *denote the Cylinder-Cone (CC) state space and the Cylinder state space, respectively. Consider a CZ gate that acts on input operators that are drawn from $S_{CC}(r,h)$:*

$$CZ\left(\rho_A \otimes \rho_B\right), \tag{4.65}$$

where $\rho^A, \rho^B \in S_{CC}(r,h)$ with $r = \sqrt{1-h^2}$. Then the output can be given a separable decomposition if the operators in the decomposition are drawn from $S_{CC}(R,1)$, where $R = g_{CC} \cdot r$, and with

$$g_{CC}(r) < g_C. \tag{4.66}$$

Here, $g_{CC}(r)$ denotes the radius growth required to be separable w.r.t the output state space $S_{CC}(R,1)$, and $g_C \approx 2.058$ is the growth rate required to maintain cylinder separability.

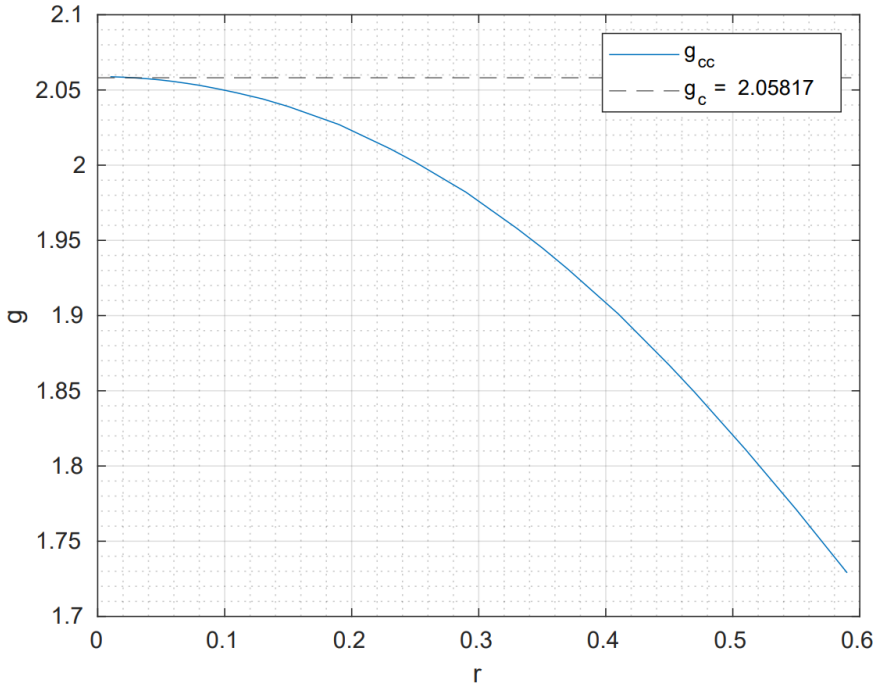


Fig. 4.9 This figure shows the growth rate $g_{CC} = R/r$, required for the output given by (4.64) to be separable with respect to operators drawn from $S_{CC}(R,1)$. We find that the g_{CC} growth rate is lower than the growth rate g_c required for cylinder separability.

This observation is based on figure 4.9. Furthermore, if we additionally impose the dual constraint that $R \leq 1$, we find approximately that $r_{in} \leq 0.57$ and the output will still be $S_{CC}(R,1)$-separable. In comparison, to maintain a separable decomposition with cylindrical state spaces, we would require that $r_{in} \leq 0.485$. This suggests that CC state spaces allow for an increase in the range of r that can efficiently classically simulated.

Let us now combine observation 4.4.2 with lattices of degree D. Consider placing qubits at the nodes of a degree D lattice such that each particle i is initialised from within $S_{CC}(r,h)$ where $r = \sqrt{1-h^2}$. Next, w.l.o.g consider applying a CZ gate to two of the qubits. Using observation 4.4.2, the output remains $S_{CC}(R,1)$-separable, provided that we grow the radius by a factor g_{CC}. Note that the particles on the lattice are now cylinders with radius $g_{CC}r_{in}$. After applying the remaining $D-1$ CZ gates, in order for the output to remain separable, the

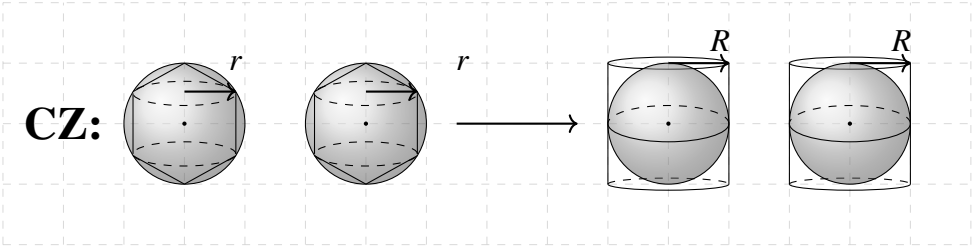


Fig. 4.10 When applying a CZ gate to two cylinder-cone states with $r = \sqrt{1-h^2}$, the output can be given a separable decomposition with respect to operators drawn from $S_{CC}(R,1)$, these output operators are cylinder states with radii R. Note that the cylinder-cone growth rate is $g_{CC} = R/r$.

output radius must grow to $R_{out} = (g_{CC})(g_C^{D-1})r_{in}$. Altogether, this can be represented by the map:

$$S_{CC}(r,h) \to \mathrm{Cyl}(\mathrm{g_{CC}} \cdot \mathrm{r}) \to \mathrm{Cyl}(\mathrm{g_{CC}} \cdot \mathrm{g_C} \cdot \mathrm{r}) \to \ldots \to \mathrm{Cyl}\left(\mathrm{g_{CC}} \cdot \mathrm{g_C^{D-1}} \cdot \mathrm{r}\right) \tag{4.67}$$

where the arrow denotes that the output is separable w.r.t to that set. For example, the output of a CZ gate acting on two operators drawn from $S_{CC}(r,h)$ is separable w.r.t to operators drawn from $S_{CC}(g_{CC} \cdot r, 1)$. Furthermore, in the first arrow, we have used the fact that being $S_{CC}(R,1)$-separable is equivalent to being Cyl(R)-separable. Lastly, from the cylinder dual constraint, we require that the final output radius satisfies

$$R_{out} = (g_{CC})(g^{D-1})r_{in} \leq 1. \tag{4.68}$$

Using (4.68), one can then calculate explicit bounds on r_{in} for different D. For example, if $D = 3$ then equation (4.68) leads to $r_{in} \leq 0.1153$. In comparison, if the initialised qubits were drawn only from cylindrical state spaces, we would end up with the constraint $g_C^3 r_{in} \leq 1$, implying that each $r_{in} \leq 0.1147$. These results suggest there is a very slight improvement in the range of r that we can classically efficiently simulate if CC state spaces are considered. Notably, we remark that these results suggest that the bounds on r derived for cylinder separability appear not to be tight. Therefore, there may be potential other methods that can increase the region of r that can be classically simulated.

4.5 Summary and Remarks

In summary, we showed that the output of an arbitrary 2-qubit diagonal gate acting on operators drawn from cylinders of radius r, can be given a separable decomposition if (4.21) holds. This result can be combined with the Harrow and Nielsen algorithm in Sec.3.3.2 to develop a new type of classical simulation algorithm based on cylinder radii separability. We remark that the techniques presented here have the potential to be applied to other quantum systems (e.g. non-diagonal gates, and other restrictions on measurements). We further saw that we can improve the range of r that can be classically simulated by considering a coarse graining approach. Lastly, by considering a Cylinder-Cone state space, we demonstrated that the bounds on r are not tight, suggesting that there may be potential alternative methods that can expand the region of r that can be classically simulated. Whilst our approach uses a linear programming approach, one could explore whether other numerical methods could be applied, such as in [41–44].

Chapter 5

Obstacles to Classically Simulating Restricted Cluster States

5.1 Introduction

In the preceding chapters, we developed a classical simulation method, based on cylinder separability. However, these cylindrical state spaces contain non-physical operators, and we are ultimately only interested in simulating systems with quantum inputs. This raises the question whether it is possible to find state spaces that allow for a greater range of quantum inputs to be efficiently simulated classically. This was to some extent explored in Sec. 4.4. However, one might wonder whether other types of classical simulation algorithms, apart from ours, that can efficiently simulate a greater range of quantum input states. For example, input states that are contained in the Bloch sphere but with a higher radius. In this chapter, we discuss potential obstacles that such endeavours may encounter. Specifically, we examine two approaches, based on percolation and quantum supremacy type arguments, that potentially rule out efficient classical simulation.

5.1.1 Overview and Related Work

One approach to demonstrate the classical intractability of a restricted model is to show that it can nevertheless support universal quantum computation. In Sec.5.2.2, we employ percolation-type arguments to show that a restricted cluster state on a degree 5 lattice, with inputs of sufficient radius, can efficiently prepare a 2D cluster state. Note that in this setting, we continue to restrict to destructive Z basis and XY-plane measurements. Consequently, it is highly unlikely that this scheme can be efficiently classically simulated. The underlying idea

is that if the probability of successfully creating a $|+\rangle$ state on unmeasured qubits exceeds a threshold determined by the lattice percolation thresholds, then it becomes possible to implement a 2D cluster state and hence can support universal quantum computation. This idea of using percolation type arguments in MBQC stems from [83–85] and has also been applied in several restricted settings [9, 53, 54], wherein imperfect graph states are usually measured locally (e.g. undergo a filtering operation) such that universal quantum computation is recovered.

The second approach is based on the quantum supremacy arguments [16]. Generally speaking, these arguments prove that if widely-believed complexity theoretic conjectures hold then there cannot exist an efficient classical simulation algorithm. These arguments were developed in [19], in which they show that if IQP circuits could be weakly classically simulated up to multiplicative error, then this would cause the so-called polynomial hierarchy to collapse, considered to be unlikely. That is, a classical algorithm cannot efficiently sample from a distribution $p(x)$ that approximates the quantum output distribution $q(x)$ such that

$$|p(x) - q(x)| \leq \varepsilon q(x), \tag{5.1}$$

is satisfied for every x and any fixed $\varepsilon > 0$. Key in the arguments of [19], is to show that IQP circuits with postselection[1] can simulate universal quantum circuits with postselection. In Sec.5.3.2, we apply this approach to restricted cluster state circuits on a degree 5 lattice. In contrast to the percolation approach, in which we have to carefully consider the outcome probabilities, we will instead be given the ability to postselect on measurement outcomes. We then show that if the input states are initialised with radii above a critical threshold of approximately $r_c = 0.3398$, then through postselection and a recursion type argument, we can implement a perfect 2D cluster state on the remaining sublattice. Then, by the arguments in [19], this is sufficient to show that a restricted cluster state cannot be simulated up to multiplicative error. This straightforward approach has been widely used in several results to rule out classical simulation for various restricted models of quantum computing [23–25].

However, a multiplicative error simulation is considered to be a highly accurate and unrealistic notion of simulation. Ideally, we would want to show that restricted cluster states

[1] Postselection is a theoretical tool, where one can post-select (ability to selectively measure and condition on specific outcomes) on exponentially unlikely measurement outcomes [86].

cannot be simulated under the more realistic notion of additive error:

$$\sum_x |p(x) - q(x)| \leq \varepsilon, \tag{5.2}$$

where ε is the error parameter. To rule out such a simulation, an approach was developed that uses results from computational complexity theory to connect the hardness of sampling and the hardness of computing output probabilities [20, 21]. This approach has been used to rule out efficient classical simulation up to additive error of various types of quantum computing [50, 25, 87, 76, 74–80, 32–34]. As we will discuss later on, the key difficulty is showing that the quantum architecture demonstrates certain properties, namely anticoncentration and average-case hardness. However, we have not been able to do this for the systems considered in this work. Nevertheless, in Sec.5.3.3 we will review how this has been achieved in an MBQC setting [32–34] (see also [78–80]) and towards the end of this section, we will explain the difficulties encountered in trying to adapt these ideas to our scenario.

Contributions

The results presented in this section are based on [30]. My contributions to this work are as follows. Sec.5.2.2 was done by M.Garn. The computations in Sec.5.3.2 were done separately by Y.Tao and M.Garn. The connections between these computations and polynomial hierarchy quantum supremacy arguments were explored by M.Garn. The writing and all other discussion was done by myself under the guidance of my supervisor

5.2 Universality of Cluster States with Alternative Inputs

5.2.1 Percolation Methods

Percolation theory provides a framework for understanding the behaviour of connected structures, in which the connections between nodes can be probabilistically present or absent. In the context of quantum computing, we can consider an "imperfect" cluster state, where each node is missing with probability $1-p$ and present with a probability p. It has been shown in certain cases that if the value of p exceeds a lattice percolation threshold p_c, the imperfect cluster state can still support universal quantum computation.

These ideas were developed in [83–85], and in particular the latter work presented an explicit polynomial-time algorithm that, for $p > p_c$, an imperfect cluster state can be efficiently reduced to the 2D cluster state using local Y and Z-basis measurements. These

percolation arguments have subsequently been applied in several similar settings [9, 53, 54]. To demonstrate how to apply these ideas, we will consider an explicit example provided in [54], in which they considered a deformed cluster state,

$$|dC_{N\times N}\rangle = \left(\frac{2}{1+\lambda^2}\right)^{N^2/2} \Lambda^{\otimes N^2} |C_{N\times N}\rangle\,, \tag{5.3}$$

where $\Lambda = \mathrm{diag}(1,\lambda)$ is the local deformation parameter, with $\lambda \in [0,1]$. These are exactly the type of states that we consider in this chapter, but with the slight variation that our states are parametrised by θ rather than λ. They proceed by applying a local filtering operation. That is, performing local two-outcome measurements (that are diagonal in the computational basis) on each qubit, described by the measurement operators:

$$\left\{\Lambda^{-1} = \lambda\,|0\rangle\langle 0| + |1\rangle\langle 1|\,, \quad \overline{\Lambda^{-1}} = \sqrt{1-\lambda^2}\,|0\rangle\langle 0|\right\}. \tag{5.4}$$

If the outcome of the measurement is Λ^{-1}, then the deformation effect is successfully undone, and we recover a $|+\rangle$ on the node with probability

$$p = \frac{2\lambda^2}{1+\lambda^2}. \tag{5.5}$$

Whereas, if the outcome is $\overline{\Lambda^{-1}}$, the qubit is projected onto $|0\rangle$. This corresponds to a deletion of the lattice node with the attached edges (i.e. a hole on the lattice). Therefore, if $p > p_c$, then by [85], the deformed cluster state (with holes) is a universal resource for quantum computation.

In the subsequent subsection, we will apply these methods to our setting of restricted cluster with alternative inputs. The key difference in our model is that we do not permit remeasuring of qubits and additionally only allow Z basis and XY-plane measurements. Despite these limitations, we will show that a restricted cluster state with inputs with high enough radius can support universal quantum computation.

5.2.2 Preparing Universal Resources via Cluster Measurements

In this section, we demonstrate that a restricted cluster state on a degree 5 lattice, with inputs of sufficient radius, can efficiently prepare a 2D cluster state. The method is straightforward and illustrated in figure 5.1. A linear chain is attached vertically to the 2D lattice with the goal of preparing a single $|+\rangle$ state on each node of the lattice. The linear chain is constructed

from ancilla qubits initialised with certain specified angles, which are then measured in the X-basis. If the probability of successfully creating a $|+\rangle$ state on unmeasured qubits exceeds a threshold determined by the lattice percolation thresholds on the unmeasured lattice, cluster state quantum computation can be implemented.

Observation 5.2.1. *Consider a lattice of degree 5, as shown in figure 5.1, if the input quantum pure states are drawn from within* $\mathrm{Cyl}(r_{max})$ *with* $r_{max} = 0.84$ *one can create a perfect 2D Cluster State efficiently on one subset of the qubits by measuring the other qubits.*

Instead of describing the inputs in terms of r will now use a quantum pure state description, as the inputs are taken from the surface of the Bloch sphere. The initial product state on the $n \times m$ lattice is

$$|\psi_{n\times m}\rangle = \bigotimes_{i=1}^{N} (\cos(\phi_i/2)\,|0\rangle + \sin(\phi_i/2)\,|1\rangle)\,, \tag{5.6}$$

where the index i denotes the qubit site, $N = nm$ is the total number of qubits on the lattice and $0 \leq \phi_i \leq \phi_{max}$. A CZ gate is then applied to each edge on the lattice. Note the correspondence between the radius and angle is given by $r = |\sin\phi|$. The fidelity with the usual perfect cluster state is then $\prod_i^N (\frac{1+\sin\phi_i}{2})$, and the perfect cluster state is recovered when $\phi_i = \pi/2$. If the input qubits were not $|+\rangle$ states, this is not an ideal cluster state. However, one can show that by attaching and measuring at most three ancilla qubits to each qubit (see figure 5.1), we can probabilistically prepare $|+\rangle$ 2D cluster states suitable for quantum computation. The starting lattice (including the ancilla qubits) is hence the degree 5 graph illustrated in figure 5.1. To see how to perform universal quantum computation, consider the following sequence of operations.

1. Prepare two ancilla qubits $|\phi_1\rangle$ and $|\phi_2\rangle$, where $|\phi_j\rangle = \cos(\phi_j/2)\,|0\rangle + \sin(\phi_j/2)\,|1\rangle$, $\phi_j \in (0, 2\pi)$ and the index j denotes the qubit. Additionally, for technical reasons we impose the condition that $\phi_1 + \phi_2 = \frac{\pi}{2}$.

2. Apply a CZ gate between ancilla qubits 1 and 2 and measure the 1st qubit in the X-basis. If the outcome $x_1 = 1$ is obtained, which occurs with probability $p_{x_1}(1) = \frac{1}{2}(1 - \sin\phi_1 \cos\phi_2)$, the post-measurement state of qubit 2 is

$$\begin{aligned} |\phi_2'\rangle = &\frac{[\cos(\phi_1/2) - \sin(\phi_1/2)]\cos(\phi_2/2)}{\sqrt{1-\sin\phi_1\cos\phi_2}}\,|0\rangle \\ &+ \frac{[\cos(\phi_1/2) + \sin(\phi_1/2)]\sin(\phi_2/2)}{\sqrt{1-\sin\phi_1\cos\phi_2}}\,|1\rangle\,. \end{aligned} \tag{5.7}$$

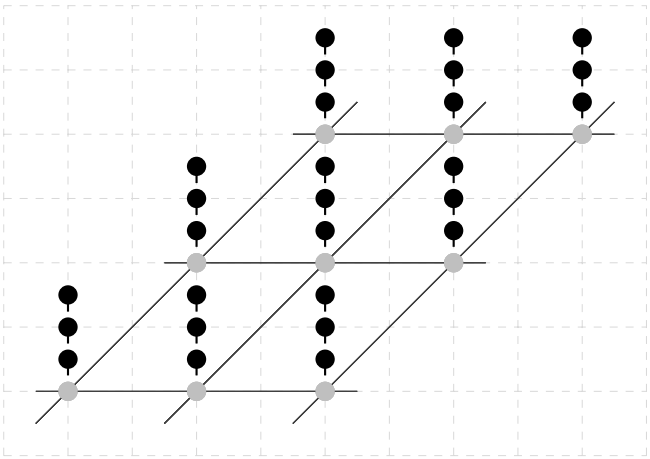


Fig. 5.1 This diagram illustrates how to prepare a single $|+\rangle$ state on a 2D lattice via a linear chain. The linear chain, attached vertically to the 2D lattice, is built from ancilla qubits that are initialised with certain specified angles, which are then measured in the X-basis.

Therefore, if we pick $\phi_1 + \phi_2 = \frac{\pi}{2}$, the post-measurement state $|\phi_2'\rangle$ becomes a $|+\rangle$ state.

3. If the outcome $x_1 = 0$ is obtained, which occurs with probability $p_{x_1}(0) = \frac{1}{2}(1 + \sin\phi_1 \cos\phi_2)$, the post-measurement state of qubit 2 is

$$|\phi_2'\rangle = \frac{[\cos(\phi_1/2) + \sin(\phi_1/2)]\cos(\phi_2/2)}{\sqrt{1+\sin\phi_1\cos\phi_2}}|0\rangle + \frac{[\cos(\phi_1/2) - \sin(\phi_1/2)]\sin(\phi_2/2)}{\sqrt{1+\sin\phi_1\cos\phi_2}}|1\rangle . \tag{5.8}$$

That is, $|\phi_2\rangle$ has undergone a rotation about the Y axis toward the $|0\rangle$ state.

If the outcome $x_1 = 1$ is obtained, then we have successfully produced a $|+\rangle$ state which is placed on the lattice. If the wrong outcome $x_1 = 0$ is obtained, then we initialise another ancilla qubit $|\phi_3\rangle$, such that $\phi_2' + \phi_3 = \frac{\pi}{2}$, where ϕ_2' is the angle of the post-measurement state of qubit 2. We then proceed to repeat the above procedure. That is, we apply a CZ gate between qubits 2 and 3, and measure qubit 2 in the X basis. Similarly, if the outcome $x_2 = 1$ is obtained, with probability $p_{x_2}(1) = \frac{1}{2}(1 - \sin\phi_2' \cos\phi_3)$, then the post-measurement state of qubit 3 is $|+\rangle$. If outcome $x_2 = 0$ is obtained, which occurs with probability $p_{x_2}(0) = \frac{1}{2}(1 + \sin\phi_2' \cos\phi_3)$, then the post-measurement state of qubit 3 is $|\phi_3'\rangle$. By repeating this method, we can calculate the probability that the lattice site will be occupied by a $|+\rangle$ state. For example, repeating the method for three ancilla qubits, the probability is

$$p_{site} = p_{x_1}(1) + p_{x_1}(0)\left[p_{x_2}(1) + p_{x_2}(0)p_{x_3}(1)\right]. \tag{5.9}$$

In the case that a $|+\rangle$ has not been successfully prepared on the lattice by the ancilla chain, we measure the final qubit in the Z basis. This projects the qubit into the $|0\rangle$ (or $|1\rangle$) state which corresponds to creating a hole on the lattice, i.e. we have removed a vertex and edges from the cluster state. According to the percolation threshold $p_c = 0.5927\ldots$, if $p_{site} > p_c$ then by [85] we can construct an efficient LOCC algorithm that creates a perfect cluster state from a 2D cluster state with holes. We find that by attaching and measuring three ancilla qubits, with angles $\phi_1 = 0.18\pi$, $\phi_2 = 0.32\pi$ and $\phi_3 = 0.31\pi$, we can prepare a $|+\rangle$ state on the lattice with probability 0.73 which is above the percolation threshold p_c. The maximum angle required $\phi_2 = 0.32\pi$ corresponds to $r_{max} = 0.84$. Therefore, we can prepare a $|+\rangle$ state with probability above the percolation threshold p_c, with three ancilla that are drawn from within $\mathrm{Cyl}(r_{max})$ with $r_{max} = 0.84$.

5.3 Quantum Supremacy Arguments

5.3.1 Multiplicative Error Simulation

In this section, we present the arguments by Bremner, Jozsa, and Shepherd [19] on the hardness of simulating IQP circuits up to multiplicative error. They showed that, if IQP circuits could be efficiently classically simulated up to multiplicative error, then this would contradict widely believed complexity-theoretic conjectures, i.e. the so-called non-collapse of the polynomial hierarchy (PH), the details of which are outside the scope of this thesis. Briefly, however, the polynomial hierarchy is a hierarchy of complexity classes that builds upon the classes P and NP. At the bottom is P and NP in levels zero and one, respectively. The second level includes the class $\mathrm{NP}^{\mathrm{NP}}$, representing problems solvable in NP with access to an NP oracle. Higher levels are then defined by nesting these classes. For a more thorough description, see [88, 89].

The motivation behind these results stems from the challenge of demonstrating differences between quantum and classical computing. The starting points is to consider boosting the power of both quantum and classical computing with postselection. In this context, postselection refers to a circuit that includes not only an output register but also an additional disjoint register known as the postselection register. The output distribution of the output register is then conditioned on the outcome of the postselection register. We refer to these circuits as post-selected circuits. The proof in [19] is a proof by contradiction, where it

is first assumed that the output probability distributions generated by IQP circuits can be weakly classically simulated up to a multiplicative error. Next, it is shown that post-selected IQP circuits (PostIQP) can simulate any post-selected universal quantum circuit (PostBQP). Finally, in combination with the results of Aaronson [86], this leads to the collapse of the PH, considered to be unlikely.

This approach has been applied to various models of restricted quantum computing to rule out classical simulation up to multiplicative error [23–25]. The key step in applying this approach is to show that the restricted model of computation can implement universal quantum computation with postselection. This is demonstrated by the following lemma 5.3.1 in the context of IQP circuits. It then follows that, if the output distribution of IQP circuits could be classically weakly simulated, then it can be shown that PostIQP in contained in PostBPP (where BPP is the class of decision problems that can be efficiently solved by polynomial-size circuits with bounded error probability). In combination with lemma 5.3.1, this shows that PostBPP = PostBQP. However, using a result by Aaronson [86], it can then be shown that the polynomial hierarchy is contained in $\mathrm{P}^{\mathrm{PostBQP}}$ (i.e. class of problems that can be solved in polynomial time using a classical computer augmented with the ability to make queries to a postBQP oracle). However, as $\mathrm{P}^{\mathrm{PostBPP}}$ is contained in the third level of polynomial hierarchy, it follows that the polynomial hierarchy is contained in the third level, this considered to be unlikely and is referred to as the polynomial hierarchy collapsing.

In the next section, we will apply this approach to restricted cluster states to rule out a multiplicative error simulation.

Lemma 5.3.1. *[19] PostIQP = PostBQP*

Proof. This proof is taken from [19]. Since IQP circuits are a subclass of universal quantum circuits, it follows that post-selected universal quantum circuits can implement post-selected IQP circuits. To prove the reverse inclusion, it is necessary to show that post-selected IQP circuits can implement post-selected universal quantum circuits.

Let us consider an arbitrary quantum circuit with inputs $|0\rangle \dots |0\rangle$ and gates drawn from the universal gate set H, Z, CZ, P, where $P = \mathrm{e}^{i(\pi/8)Z}$. Next, we add $HH = I$ to the beginning and end of the circuit on each line. Therefore, each line now begins and ends with a H gate, and is acted on by gates from the set H, Z, CZ, P. This is almost of the form of an IQP circuit,

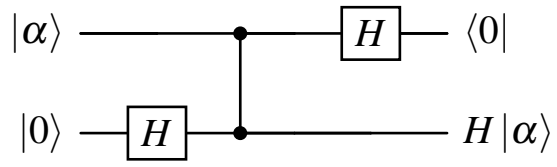


Fig. 5.2 This circuit gadget is designed to simulate the effect of an internal H gate within post-selected IQP circuits. To achieve this, an ancilla qubit is introduced, a CZ gate is then applied between the two qubits, after which the first qubit is measured and post-selected on the $|0\rangle$ outcome.

as in figure 2.4. The only gate not permitted in IQP circuits is the internal H gate. However, every internal H gate can be implemented with the use of the Hadamard gadget, as shown in figure 5.2. Note that in this construction, the ancillary qubit line begins and ends with a Hadamard gate and the resulting circuit will be of the form of an IQP circuit. Therefore, this shows that any post-selected quantum circuit can be implemented by a post-selected IQP circuit. □

5.3.2 Hardness of Classically Simulating Restricted Cluster States with Multiplicative Error

Having established that IQP circuits cannot be simulated up to multiplicative error, based on complexity-theoretic conjectures, we will similarly show that a restricted cluster state on a degree 5 lattice cannot be classically simulated up to multiplicative error. More specifically, we will consider a cluster state on a 2D lattice, where each node has a 1D-chain of qubits attached to it. The main tool then is to use post-selection to implement a perfect 2D cluster state on the sublattice and by the arguments of [19] this is sufficient to rule out a multiplicative simulation.

The technical result that we will now show is that through post-selection, the 1D-chain (illustrated in figure 5.3) with input states $|\theta\rangle$, where θ is above a threshold θ_c, can indeed prepare a $|+\rangle$ state.

Consider a 1D-chain of n qubits, where each qubit i is prepared in the same state

$$|\theta_i\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle\,, \tag{5.10}$$

with $0 < \theta < \pi/2$. We then consider applying the CZ gate between nearest neighbour qubits and performing local X-basis measurements on qubits 1 to $n-1$, post-selecting on the

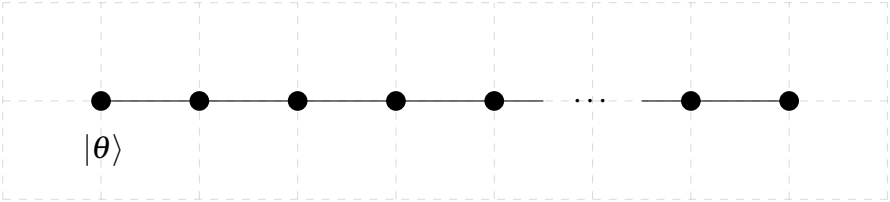


Fig. 5.3 1D-chain of n qubits. If the input states are initialised in the state $|\theta\rangle$, with angle θ above a threshold θ_c, then by applying nearest-neighbour CZ gates, measuring $n-1$ qubits in the X-basis from left to right, and post-selecting on the outcome corresponding to the projector $(I-X)/2$, the remaining n-th qubit can be prepared in the $|+\rangle$ state.

outcome corresponding to the $(I-X)/2$ measurement operator. This sequence of steps is illustrated in figure 5.3. A straightforward calculation shows that the nth qubit is projected onto the (unnormalised) state

$$|\theta_n'\rangle = \alpha_n |0\rangle + \beta_n |1\rangle , \tag{5.11}$$

where $\alpha_n = \cos(\theta/2)(\alpha_{n-1} - \beta_{n-1})$ and $\beta_n = \sin(\theta/2)(\alpha_{n-1} + \beta_{n-1})$. This is in the form of a linear recursion relation and can be rewritten as

$$|\theta_n'\rangle = T^{n-1} |\theta_n\rangle \tag{5.12}$$

$$= T^{n-1} \left[\cos(\theta/2) |0\rangle + \sin(\theta/2) |1\rangle\right], \tag{5.13}$$

where

$$T = \begin{pmatrix} \cos(\theta/2) & -\cos(\theta/2) \\ \sin(\theta/2) & \sin(\theta/2) \end{pmatrix}. \tag{5.14}$$

We now wish to express the state $|\theta_n'\rangle$ in terms of the eigenvalues and eigenvectors of T. The eigenvalues of T are

$$\lambda_{1,2} = \frac{1}{2}\left(\cos(\theta/2) + \sin(\theta/2) \pm \sqrt{1 - 3\sin(\theta)}\right), \tag{5.15}$$

and the corresponding eigenvectors are

$$|v_1\rangle = \begin{pmatrix} \frac{\cos(\theta/2)}{\cos(\theta/2) - \lambda_1} \\ 1 \end{pmatrix} \tag{5.16}$$

and

$$|v_2\rangle = \begin{pmatrix} \frac{\cos(\theta/2)}{\cos(\theta/2)-\lambda_2} \\ 1 \end{pmatrix}, \tag{5.17}$$

respectively. Therefore, we can now express the solution of the recursion (5.13) as

$$|\theta_n'\rangle = T^{n-1}(c_1|v_1\rangle + c_2|v_2\rangle) \tag{5.18}$$

$$= c_1\lambda_1^{n-1}|v_1\rangle + c_2\lambda_2^{n-1}|v_2\rangle. \tag{5.19}$$

The constants c_1 and c_2 can be explicitly calculated by setting $|\theta\rangle = c_1|v_1\rangle + c_2|v_2\rangle$, and the second equality follows as $|v_1\rangle$, $|v_2\rangle$ are eigenvectors of T (see appendix A.6 for details).

Now that we have solved the recursion relation, we can now analyse the behaviour of (5.19) as a function of θ. Note that the eigenvalues $\lambda_{1,2}$ provide important information about the behaviour of this recursion, determining the form of expression of (5.19), as well as its long-term behaviour with n. Therefore, we first observe that when $\sin\theta_c = 1/3$, equation (5.19) is undefined and the solution to the recursion does not exist. As a result, we will consider two separate cases: when the initial angle $\theta < \theta_c$, and when $\theta > \theta_c$.

If the initial angle θ is less than θ_c, then $|\lambda_1| > |\lambda_2|$. This means as n increases, $|\theta_n'\rangle$ will converge to $|v_1\rangle$. Let us now consider the behaviour of $|v_1\rangle$, in particular the amplitude of $|0\rangle$ in (5.16), which can be expressed as

$$\frac{2\cos(\theta/2)}{\cos(\theta/2) - \sin(\theta/2) - \sqrt{1-3\sin(\theta)}}. \tag{5.20}$$

This is a decreasing function of θ, with its minimum attained as θ approaches θ_c, with a value of approximately 2.14. This means that a n increases, (5.19) will converge to the state $|v_1\rangle$ and attain its maximum angle as θ approaches θ_c.

If the initial angle θ is greater than θ_c, then $|\lambda_1|, |\lambda_2|$ are complex with $|\lambda_1| = |\lambda_2|$. Now consider expressing λ_1, λ_2 as $r_\omega e^{i\omega}, r_\omega e^{-i\omega}$, respectively. Using these expressions for $\lambda_{1,2}$, and rewriting (5.19) in the computational basis, we have

$$r_\omega e^{i\omega m}\left[\left(\frac{c_1\cos(\theta/2)}{\cos(\theta/2)-\lambda_1} + \frac{c_2\cos(\theta/2)e^{-2i\omega m}}{\cos(\theta/2)-\lambda_2}\right)|0\rangle + \left(c_1 + c_2e^{-2i\omega m}\right)|1\rangle\right] \tag{5.21}$$

where $m = n-1$ denotes the number of qubits that are measured in the 1D-chain. In appendix A.7, we then show that if $\theta > \theta_c$ then the magnitudes of the amplitudes of $|0\rangle$ and $|1\rangle$ can be

equal which shows that the output of the recursion can indeed yield a $|+\rangle$ state.

We will now explain how this recursion argument can be used to show that a restricted cluster state can with postselection implement a perfect cluster state on a 2D lattice. Consider an initial 1D-chain of length n, attached to an underlying 2D lattice. Now if the initialised states are prepared with an angle θ above the critical threshold θ_c, then, for sufficiently large n, by post-selecting on the outcome corresponding to the projector $(I-X)/2$ and utilising the just-presented recursion argument, we can purify to a $|+\rangle$ state on the underlying 2D lattice. A consequence of the above result is that when $\theta > \theta_c$, the restricted cluster state of degree 5 can, through postselection, implement a perfect 2D cluster state, and hence postselected universal quantum computation. Consequently, according to the arguments in [19], if the output probability distributions generated by the restricted cluster states could be weakly classically simulated with multiplicative error, then would lead to the collapse of the Polynomial Hierarchy.

5.3.3 Additive Error Simulation and Cluster States

In Sec.5.3.2, we showed that a restricted cluster state (with inputs states prepared above $r_c = 0.3398$) cannot be efficiently classically simulated with multiplicative error. However, as a multiplicative error simulation is an unrealistic notion of simulation, we would ideally like to show that we can rule out an additive error simulation. Techniques have been developed in the literature for converting multiplicative error obstacles to classical simulation into additive error obstacles to classical simulation [20, 21]. However, we have not been able to do this for the systems considered in this work. Nevertheless, in this section, we will review how this conversion is achieved in other MBQC scenarios. Towards the end of this section, we will explain the difficulties encountered in trying to adapt these ideas to our scenario. Our starting point is to briefly review parts of the works of [32–34]), which considered cluster states with perfect inputs but with restrictions to *non-adaptive XY*-plane measurements, as opposed to the adaptive measurements required for quantum computation. We will then discuss how this links with the approaches of [20, 21] to make quantum supremacy claims in certain MBQC scenarios.

Let us begin by considering a typical cluster state scheme on a 2D lattice with n rows and m columns. The resource state is prepared by initialising $|+\rangle$ states on the vertices of the lattice, followed by applying CZ gates on the edges. Typically, the next step in MBQC schemes is to adaptively measure the resource state to implement deterministic computation, as seen in section 2.2. However, by performing random non-adaptive measurements, we

can effectively translate the standard MBQC scheme into one in which the last column of n qubits has effectively undergone a random quantum circuit [32, 34]. To see this, consider performing XY-plane measurements on $m-1$ columns of the lattice, with the measurement angle being uniformly chosen at random, then this is equivalent to a random circuit of the form $C_{m,\theta} = L^{m-1} \cdots L^2 \cdot L^1$, where each circuit 'layer' L^k is of the form

$$L^k = \left(\prod_{i=n}^{n} H_i\right)\left(\prod_{i=1}^{n-1} CZ_{i,i+1}\right)\left(\prod_{i=1}^{n} e^{\mathrm{i}\tilde{\theta}_i^k Z_i}\right). \tag{5.22}$$

It is convenient to note that the output distribution observed on the last column of qubits, conditioned on the measurement outcomes on the $m-1$ columns of qubits, of the $n \times m$ lattice can be expressed as

$$q(x) = q(x_R|x_L)q(x_L) = |\langle x_R|C_{m,\theta}|\psi\rangle|^2 q(x_L), \tag{5.23}$$

where $|\psi\rangle = |+\rangle^{\otimes n}$, and $x_L \in \{0,1\}^{(m-1)n}$, $x_R \in \{0,1\}^n$, denote the outcomes obtained from measuring the first $m-1$ columns and the last column, respectively. Therefore, we can see that by performing random non-adaptive measurements, the 2D cluster state generates a family of quantum circuits $\{C_{m,\theta}\}$. This allows us to exploit the following result of [21]:

Theorem 5.3.1. *(Adapted from [21]) Let $\{C_{m,\theta}\}$ be a family of quantum circuits such that C1 and C2 below are true. If it is possible to efficiently classically sample from a distribution $p(x)$ that approximates the quantum output distribution $q(x)$ of every circuit $C \in \{C_{m,\theta}\}$ to additive error, i.e. such that*

$$\sum_x |p(x) - q(x)| \leq \varepsilon, \tag{5.24}$$

then the Polynomial Hierarchy would collapse to its third level.

This means, that if the measurements in the cluster state scheme are chosen in the right way, such that C1. and C2. are true, then by the approach of [21] we can end up with a distribution on the last column that cannot be efficiently classically simulated up to additive error. We will now briefly discuss the proof of [21] that establishes theorem 5.3.3.

The proof in [21], is a proof by contradiction, where it is assumed that there exists an efficient classical algorithm, which for any $C \in \{C_{m,\theta}\}$, can sample from a probability distribution which approximates the output probability distribution $q(x)$ up to additive error. Then, by using Stockmeyer's theorem [90], it can be shown that there is an algorithm (contained

in the third level of the PH) that can compute the value of $q(x)$, for any outcome x, approximately up to multiplicative error on a sizeable fraction of the circuits C. A key ingredient in this argument is a property known as anticoncentration. Informally, this property ensures that the output distribution of a random quantum circuit is reasonably spread out. One of the key technical insights in [21] was showing that this property of anticoncentration holds for the families of IQP circuits considered.

The next step in this argument is to invoke a computational complexity assumption on approximately computing the value of $q(x)$ up to multiplicative error. It is known that the problem above is #P-hard in the worst-case (i.e. for specific circuits and measurements outcomes)[51], the authors of [21] now conjecture that this problem is #P-hard on average. If this conjecture is true, then the existence of an efficient additive error sampling algorithm would imply a collapse of the PH.

Therefore, to establish theorem 5.3.3 using the approach of [21], one typically needs to demonstrate the following properties:

C1. The output distribution of $\{C_{m,\theta}\}$ anticoncentrates. This has been demonstrated for the family of IQP circuits in [21].

C2. It is #P-hard to approximate the output probability $q(x)$ up to multiplicative error for a suitable fraction of the circuit instances. This has not been shown, but it is known to hold in the worse-case [51], which supports the conjecture.

This approach has been used to rule out efficient classical simulation up to additive error of various types of quantum computing, [91, 21, 50, 74, 75, 25, 87] and additionally has been adapted to MBQC settings [76–78, 32–34]. In particular, it was shown in [32–34] that a cluster state with perfect inputs but with restrictions to non-adaptive XY-plane measurements can be mapped to an ensemble of random circuits, where i) each circuit is sampled with uniform probability, and ii) each circuit has a straightforward structure, containing layers of CZ, H, and U_Z gates. Furthermore, it was demonstrated in [34] that such as system satisfies the anticoncentration property. However, in order to rule out efficient classical simulation up to additive error, the average-case complexity property still needs to be established.

In comparison, we have not been able to apply the approach of [21] to rule out classical simulation up to additive error of cluster states with alternative inputs. This is because we encounter challenges in understanding how the random circuit ensemble, generated from measuring the cluster state with alternative inputs, changes with the input radii. Furthermore,

the circuits generated in the ensemble are non-unitary circuits, and therefore it is unclear how existing arguments (e.g. demonstrating anticoncentration) can be applied.

5.4 Summary and Remarks

In this chapter, we examined potential obstacles that may arise when attempting to efficiently classically simulate an increased range of quantum input states.

In particular, we considered two approaches, based on percolation and quantum supremacy arguments, that potentially rule out efficient classical simulation for cluster state quantum circuits with input states of sufficient radius. The first approach uses percolation-type arguments to demonstrate that a restricted cluster state on a degree 5 lattice, with input states of sufficient radius, can efficiently prepare a 2D cluster state. The underlying idea is that if the probability of successfully creating a $|+\rangle$ state on unmeasured qubits exceeds a threshold determined by the lattice's percolation thresholds, it becomes possible to implement a cluster state quantum computation. For a degree 5 lattice, we find that allowing for input states with approximately $r \leq 0.84$, we can still prepare a universal 2D cluster state. We remark that this approach can potentially be improved and extended. For example, by utilising all permitted cluster measurements rather than only using X-basis measurements or by altering the lattice configuration, it may be possible to prepare a $|+\rangle$ state from the 1D-chain using input states with lower values of r. Additionally, there are alternative strategies to consider beyond simply preparing a $|+\rangle$ state, for example, one could consider directly implementing a universal gate set by measuring the resource state.

In the second approach, we attempt to apply quantum supremacy-type arguments to rule out classical simulation of restricted cluster states. We showed that if the input states are initialised with radii above a critical threshold of approximately $r_c = 0.3398$, then through postselection and a recursion type argument, we can implement a perfect 2D cluster state on the remaining sublattice. Then by the standard arguments in [19], this is sufficient to show that a restricted cluster state cannot be simulated up to multiplicative error. However, the aim was to rule out classical simulation of restricted cluster states with additive error. Unfortunately, we have not been able to do this for the cluster state with alternative inputs. Nevertheless, we reviewed how the approach in [21] can be adapted to MBQC scenarios [32–34] and briefly discussed the difficulties in adapting the approach to our scenario.

Chapter 6

Summary and Conclusion

A fundamental aim in quantum computing to understand when quantum systems can or cannot be efficiently classically simulated. In this thesis, we studied when cluster state quantum circuits with alternative inputs and measurements in the Z basis and XY-plane, can or cannot be efficiently classically simulated.

In the first part of this thesis (chapter 3 and chapter 4), we studied when such a system can be efficiently classically simulated. The main technical tool we considered was a generalised notion of separability. Specifically, we considered relaxing the requirement that the local operators ρ_j^K must be non-negative operators, and instead allowed the operators to be drawn from a set of operators that, through the Born rule, yield positive probabilities for a given set of measurement operators. Applying this to the permitted cluster measurements, we arrived at the notion of cylindrical state spaces. Using this notion, we first proved that if a CZ gate acts on input operators that are drawn from cylinders of radius r, the output can be given a separable decomposition provided that the radius of the output cylinders in the decomposition grows by a constant $\lambda > 0$. By combining this with a modified version of Harrow and Nielsen's algorithm, we see that this enables an efficient classical simulation algorithm that can sample from the output distribution to within additive error. As a result, this provides examples of pure entangled quantum systems that can be efficiently classically simulated. In the future, we hope that the techniques of generalised separability can further be applied to enable efficient classical simulation algorithms [15] of other quantum systems (e.g. non-diagonal gates, and other restrictions on measurements).

In chapter 4, we then moved onto ways to improve and extend our classical simulation algorithm. First, we improved the bound on the parameter r in our classical simulation algorithm by considering a coarse-graining approach. Next, we demonstrated that the result

of lemma 3.2.1 can be generalised to hold for any two-qubit gate that is diagonal in the computational basis. Lastly, we showed that there are choices of state space that can increase the size of the classically efficient regime. In particular, we considered a state space that we call the cylinder-cone state space. Via linear programming, we showed that the output of a CZ gate acting on cylinder-cone states can be given a generalised separable decomposition and hence very slightly improves the range of r that can be efficiently classically simulated. This suggests that the bounds on r are not tight, and there may be potential alternative methods that can increase the region of r that can be classically simulated.

In the second part of this thesis (chapter 5), we examined potential obstacles that may arise when attempting to efficiently classically simulate an increased range of quantum input states. Using a percolation based approach, we showed that a restricted cluster state on a degree 5 lattice, with input states of sufficient radius, we can efficiently prepare a universal 2D cluster state, and therefore efficient classical simulation is unlikely. We remark that this approach can potentially be improved, for example, by utilising all permitted cluster measurements rather than only using X-basis measurements. Next, by using conjectures about the polynomial hierarchy, we showed that there is a threshold for which cluster states with alternative inputs cannot be efficiently classically simulated with multiplicative error. This approach uses postselection and a recursion type argument to show that the restricted cluster state can nevertheless implement any post-selected universal quantum circuit. However, the notion of a multiplicative simulation is unrealistic, and we would ideally like to show that a cluster state with alternative inputs cannot be simulated with additive error. Unfortunately, we have not been able to do this. Nevertheless, we reviewed how the approach in [21] has been adapted to MBQC scenarios [32–34] and we briefly discussed the difficulties in adapting the approach to our scenario. As such, ruling out classical simulation of cluster states with alternative inputs of sufficient r, is still an open problem that would be worthy to explore in future work.

We will now briefly summarise the results from this thesis for the regions of states that can and cannot be efficiently classically simulated. Recall the key result in Sec.3.3.2, where it was shown that a quantum computation that involves: i) initialising n qubits in the state ρ, satisfying $\|\rho - \rho_{diag}\| \leq 1/\lambda^D$, where $\lambda = 2.05817$ and D is the maximum degree of the lattice, ii) performing CZ gates between adjacent qubits, iii) and only allowing measurements in the Z-basis and XY-plane, can be efficiently classically simulated. In table 6.1, we have computed the value $1/\lambda^D$ for different degree lattices. From Sec.4.2, using a coarse graining approach (on a degree 4 lattice), numerical results suggest that inputs with $r \leq 0.0913$ can be

D	3	4	5	6
$1/\lambda^D$	0.1147	0.0557	0.0271	0.0132

Table 6.1 This table shows the values of $1/\lambda^D$ for different degree D lattices.

efficiently classically simulated. With the modifications discussed in Sec.4.2.1, this can be further improved to $r \leq 0.0924$. Lastly, we saw that using an alternative notion of separability (i.e. w.r.t to cylinder-cone state spaces), we can also improve the range of r that we can be efficiently classically simulated, where specifically for degree 3 lattices we have that $r \leq 0.1153$. On the other hand, in Sec.5.2.2, it was shown that allowing for states with $r \geq 0.84$ on degree 5 lattices enables universal quantum computation and, consequently, rules out efficient classical simulation. Additionally, in Sec.5.3.2, on a degree 5 lattice we ruled out efficient classical simulation up to multiplicative error for $r > 0.3398$.

Lastly, we remark that the numerics on coarse-graining in Sec.4.2.1 could be taken further, e.g. by considering larger blocks. Furthermore, in these numerics, we conjectured that projectors of the form $(I-X)/2$ and input extrema$(I+\alpha X+Z)/2$ return the maximum r for which these systems return positive probabilities. In the future, one could aim to prove this conjecture. Additionally, in Sec.4.4, for some of the state spaces considered, one could try to understand if analogues of the PPT criterion or entanglement witnesses could be applied. In Sec.4.4.4, one could also explore improvements to the cylinder-cone result. For example, rather than requiring the output state space to be cylinders, one could consider cylinder-cone states (with height < 1) or some other alternative state space.

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[3] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Physical Review A*, vol. 70, no. 5, p. 052328, 2004. Publisher: APS.

[4] R. Jozsa and M. Van Den Nest, "Classical simulation complexity of extended clifford circuits," *Quantum Information & Computation*, vol. 14, no. 7&8, pp. 633–648, 2014. Publisher: Rinton Press, Incorporated Paramus, NJ.

[5] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, "Simulation of quantum circuits by low-rank stabilizer decompositions," *Quantum*, vol. 3, p. 181, 2019. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften.

[6] G. Vidal, "Efficient classical simulation of slightly entangled quantum computations," *Physical review letters*, vol. 91, no. 14, p. 147902, 2003. Publisher: APS.

[7] I. L. Markov and Y. Shi, "Simulating quantum computation by contracting tensor networks," *SIAM Journal on Computing*, vol. 38, no. 3, pp. 963–981, 2008. Publisher: SIAM.

[8] A. W. Harrow and M. A. Nielsen, "Robustness of quantum gates in the presence of noise," *Physical Review A*, vol. 68, no. 1, p. 012308, 2003. Publisher: APS.

[9] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, "Measurement-based quantum computation beyond the one-way model," *Physical Review A*, vol. 76, no. 5, p. 052315, 2007. Publisher: APS.

[10] M. V. D. Nest, "Universal quantum computation with little entanglement," *Physical Review Letters*, vol. 110, Feb. 2013.

[11] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical review letters*, vol. 86, no. 22, p. 5188, 2001. Publisher: APS.

[12] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Physical review A*, vol. 68, no. 2, p. 022312, 2003. Publisher: APS.

[13] H. Barnum, E. Knill, G. Ortiz, R. Somma, and L. Viola, "A subsystem-independent generalization of entanglement," *Physical Review Letters*, vol. 92, no. 10, p. 107902, 2004. Publisher: APS.

[14] H. Barnum, E. Knill, G. Ortiz, and L. Viola, "Generalizations of entanglement based on coherent states and convex sets," *Physical Review A*, vol. 68, no. 3, p. 032308, 2003. Publisher: APS.

[15] N. Ratanje and S. Virmani, "Exploiting non-quantum entanglement to widen applicability of limited-entanglement classical simulations of quantum systems," *arXiv preprint arXiv:1201.0613*, 2012.

[16] A. W. Harrow and A. Montanaro, "Quantum computational supremacy," *Nature*, vol. 549, no. 7671, pp. 203–209, 2017. Publisher: Nature Publishing Group UK London.

[17] A. P. Lund, M. J. Bremner, and T. C. Ralph, "Quantum sampling problems, BosonSampling and quantum supremacy," *npj Quantum Information*, vol. 3, no. 1, p. 15, 2017. Publisher: Nature Publishing Group UK London.

[18] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, and others, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019. Publisher: Nature Publishing Group.

[19] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy," in *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 467, pp. 459–472, Royal Society, Feb. 2011. ISSN: 14712946 Issue: 2126.

[20] S. Aaronson and A. Arkhipov, "The Computational Complexity of Linear Optics," *Theory OF Computing*, vol. 9, no. 4, pp. 143–252, 2013.

[21] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-case complexity versus approximate simulation of commuting quantum computations," *Physical review letters*, vol. 117, no. 8, p. 080501, 2016. Publisher: APS.

[22] S. Aaronson and L. Chen, "Complexity-Theoretic Foundations of Quantum Supremacy Experiments," in *32nd Computational Complexity Conference*, p. 1, 2017.

[23] T. Morimae, K. Fujii, and J. F. Fitzsimons, "Hardness of classically simulating the one-clean-qubit model," *Physical review letters*, vol. 112, no. 13, p. 130502, 2014. Publisher: APS.

[24] E. Farhi and A. W. Harrow, "Quantum supremacy through the quantum approximate optimization algorithm," *arXiv preprint arXiv:1602.07674*, 2016.

[25] M. Yoganathan, R. Jozsa, and S. Strelchuk, "Quantum advantage of unitary Clifford circuits with magic state inputs," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 475, May 2019. Publisher: Royal Society Publishing.

[26] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, "On the complexity and verification of quantum random circuit sampling," *Nature Physics*, vol. 15, no. 2, pp. 159–163, 2019. Publisher: Nature Publishing Group UK London.

[27] A. M. Dalzell, N. Hunter-Jones, and F. G. Brandão, "Random quantum circuits transform local noise into global white noise," *arXiv preprint arXiv:2111.14907*, 2021.

[28] A. Bouland, B. Fefferman, Z. Landau, and Y. Liu, "Noise and the frontier of quantum supremacy," Feb. 2021.

[29] A. Deshpande, P. Niroula, O. Shtanko, A. V. Gorshkov, B. Fefferman, and M. J. Gullans, "Tight bounds on the convergence of noisy random circuits to the uniform distribution," *PRX Quantum*, vol. 3, no. 4, p. 040329, 2022. Publisher: APS.

[30] S. Atallah, M. Garn, S. Jevtic, Y. Tao, and S. Virmani, "Efficient classical simulation of cluster state quantum circuits with alternative inputs," *arXiv preprint arXiv:2201.07655*, 2022.

[31] S. Atallah, M. Garn, Y. Tao, and S. Virmani, "Classically efficient regimes in measurement based quantum computation performed using diagonal two qubit gates and cluster measurements," *arXiv preprint arXiv:2307.01800*, 2023.

[32] J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, and J. Eisert, "Architectures for Quantum Simulation Showing a Quantum Speedup," *Physical Review X*, vol. 8, p. 021010, Apr. 2018.

[33] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, "Anticoncentration theorems for schemes showing a quantum speedup," *Quantum*, vol. 2, p. 65, May 2018. arXiv:1706.03786 [cond-mat, physics:math-ph, physics:quant-ph].

[34] J. Haferkamp, D. Hangleiter, A. Bouland, B. Fefferman, J. Eisert, and J. Bermejo-Vega, "Closing gaps of a quantum advantage with short-time Hamiltonian dynamics," *Physical Review Letters*, vol. 125, p. 250501, Dec. 2020. arXiv:1908.08069 [quant-ph].

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2011.

[36] J. Preskill, "Lecture notes for ph219/cs219: Quantum information," *Accesible via http://theory.caltech.edu/~preskill/ph229/*, 2023.

[37] L. Gurvits, "Classical deterministic complexity of Edmonds' problem and quantum entanglement," in *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pp. 10–19, 2003.

[38] S. Gharibian, "Strong NP-hardness of the quantum separability problem," *Quantum Information & Computation*, vol. 10, no. 3 & 4, 2010.

[39] A. Peres, "Separability criterion for density matrices," *Physical Review Letters*, vol. 77, no. 8, p. 1413, 1996. Publisher: APS.

[40] M. Horodecki, P. Horodecki, and R. Horodecki, "On the necessary and sufficient conditions for separability of mixed quantum states," *Phys. Lett. A*, vol. 223, no. 1, 1996. Publisher: Citeseer.

[41] P. A. Parrilo, A. C. Doherty, and F. M. Spedalieri, "Entanglement witnesses and semidefinite programming," in *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, vol. 4, pp. 4575–4580, IEEE, 2002.

[42] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Complete family of separability criteria," *Physical Review A*, vol. 69, no. 2, p. 022308, 2004. Publisher: APS.

[43] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Detecting multipartite entanglement," *Physical Review A*, vol. 71, no. 3, p. 032333, 2005. Publisher: APS.

[44] A. C. Doherty, "Entanglement and the shareability of quantum states," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, p. 424004, 2014. Publisher: IOP Publishing.

[45] M. A. Nielsen, "Cluster-state quantum computation," *Reports on Mathematical Physics*, vol. 57, no. 1, pp. 147–161, 2006. Publisher: Elsevier.

[46] X. Zhou, D. W. Leung, and I. L. Chuang, "Methodology for quantum logic gate construction," *Physical Review A*, vol. 62, no. 5, p. 052316, 2000. Publisher: APS.

[47] R. Jozsa, "An Introduction to Measurement Based Quantum Computation," in *Quantum Information Processing*, pp. 137–158, IOS Press, 2006.

[48] D. Shepherd and M. J. Bremner, "Temporally unstructured quantum computation," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 465, pp. 1413–1439, May 2009. Publisher: Royal Society.

[49] X. Ni and M. Van den Nest, "Commuting quantum circuits: efficiently classical simulations versus hardness results," *Quantum Information & Computation*, vol. 13, no. 1-2, pp. 54–72, 2013. Publisher: RINTON PRESS, INC.

[50] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Achieving quantum supremacy with sparse and noisy commuting quantum computations," *Quantum*, vol. 1, p. 8, 2017. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften.

[51] K. Fujii and T. Morimae, "Commuting quantum circuits and complexity of Ising partition functions," *New Journal of Physics*, vol. 19, p. 033003, Mar. 2017. Publisher: IOP Publishing.

[52] A. Montanaro, "Quantum circuits and low-degree polynomials over F2," *Journal of Physics A: Mathematical and Theoretical*, vol. 50, Jan. 2017. Publisher: Institute of Physics Publishing.

[53] S. D. Barrett, S. D. Bartlett, A. C. Doherty, D. Jennings, and T. Rudolph, "Transitions in the computational power of thermal states for measurement-based quantum computation," *Physical Review A*, vol. 80, no. 6, p. 062328, 2009. Publisher: APS.

[54] C. E. Mora, M. Piani, A. Miyake, M. V. D. Nest, W. Dür, and H. J. Briegel, "Universal resources for approximate and stochastic measurement-based quantum computation," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 81, Apr. 2010.

[55] R. Somma, H. Barnum, G. Ortiz, and E. Knill, "Efficient solvability of Hamiltonians and limits on the power of some quantum computational models," *Physical review letters*, vol. 97, no. 19, p. 190501, 2006. Publisher: APS.

[56] H. Anwar, S. Jevtic, O. Rudolph, and S. Virmani, "Generalised versions of separable decompositions applicable to bipartite entangled quantum states," *New Journal of Physics*, vol. 21, no. 9, p. 093031, 2019. Publisher: IOP Publishing.

[57] H. Anwar, S. Jevtic, O. Rudolph, and S. Virmani, "Smallest state spaces for which bipartite entangled quantum states are separable," *New Journal of Physics*, vol. 17, no. 9, p. 093047, 2015. Publisher: IOP Publishing.

[58] N. Ratanje and S. Virmani, "Generalized state spaces and nonlocality in fault-tolerant quantum-computing schemes," *Physical Review A*, vol. 83, no. 3, p. 032309, 2011. Publisher: APS.

[59] H. Pashayan, S. D. Bartlett, and D. Gross, "From estimation of quantum probabilities to simulation of quantum circuits," *Quantum*, vol. 4, p. 223, 2020. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften.

[60] M. Van den Nest, "Classical Simulation of Quantum Computation, the Gottesmann-Knill theorem, and Slightly Beyond," *Quantum Information & Computation*, vol. 10, no. 3-4, pp. 258–271, 2010.

[61] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," *Physical Review A*, vol. 71, p. 22316, June 2005.

[62] L. G. Valiant, "Quantum computers that can be simulated classically in polynomial time," in *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pp. 114–123, 2001.

[63] B. M. Terhal and D. P. DiVincenzo, "Classical simulation of noninteracting-fermion quantum circuits," *Physical Review A*, vol. 65, no. 3, p. 032325, 2002. Publisher: APS.

[64] R. Jozsa and A. Miyake, "Matchgates and classical simulation of quantum circuits," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 464, no. 2100, pp. 3089–3106, 2008. Publisher: The Royal Society London.

[65] M. Hebenstreit, R. Jozsa, B. Kraus, and S. Strelchuk, "Computational power of matchgates with supplementary resources," *Physical Review A*, vol. 102, no. 5, p. 052604, 2020. Publisher: APS.

[66] R. Jozsa and N. Linden, "On the role of entanglement in quantum-computational speed-up," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 459, no. 2036, pp. 2011–2032, 2003. Publisher: The Royal Society.

[67] U. Schollwöck, "The density-matrix renormalization group," *Reviews of modern physics*, vol. 77, no. 1, p. 259, 2005. Publisher: APS.

[68] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, "Matrix product state representations," *arXiv preprint quant-ph/0608197*, 2006.

[69] F. Verstraete, M. M. Wolf, D. Perez-Garcia, and J. I. Cirac, "Criticality, the area law, and the computational power of projected entangled pair states," *Physical review letters*, vol. 96, no. 22, p. 220601, 2006. Publisher: APS.

[70] N. Yoran and A. J. Short, "Classical simulation of limited-width cluster-state quantum computation," *Physical review letters*, vol. 96, no. 17, p. 170503, 2006. Publisher: APS.

[71] A. Mantri, T. F. Demarie, and J. F. Fitzsimons, "Universality of quantum computation with cluster states and (X, Y)-plane measurements," *Scientific Reports 2017 7:1*, vol. 7, pp. 1–7, Feb. 2017. Publisher: Nature Publishing Group.

[72] A. Kissinger and J. v. d. Wetering, "Universal MBQC with generalised parity-phase interactions and Pauli measurements," *Quantum*, vol. 3, p. 134, Apr. 2019. Publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften.

[73] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pp. 517–526, IEEE, 2009.

[74] T. Morimae, "Hardness of classically sampling the one-clean-qubit model with constant total variation distance error," *Physical Review A*, vol. 96, Oct. 2017. Publisher: American Physical Society.

[75] A. Bouland, J. F. Fitzsimons, and D. E. Koh, "Quantum advantage from conjugated Clifford circuits," in *Proceedings of the 33rd Computational Complexity Conference (CCC2018). DOI*, vol. 10, 2017.

[76] X. Gao, S.-T. Wang, and L.-M. Duan, "Quantum supremacy for simulating a translation-invariant ising spin model," *Physical review letters*, vol. 118, no. 4, p. 040502, 2017. Publisher: APS.

[77] J. Miller, S. Sanders, and A. Miyake, "Quantum supremacy in constant-time measurement-based computation: A unified architecture for sampling and verification," *Physical Review A*, vol. 96, Dec. 2017. Publisher: American Physical Society.

[78] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham, "Efficient quantum pseudorandomness with simple graph states," *Physical Review A*, vol. 97, no. 2, p. 022333, 2018. Publisher: APS.

[79] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham, "Efficient approximate unitary t-designs from partially invertible universal sets and their application to quantum speedup," May 2019.

[80] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham, "On unitary t-designs from relaxed seeds," *Entropy*, vol. 22, p. 92, Jan. 2020. Publisher: MDPI AG.

[81] H. Weyl, "Das asymptotische Verteilungsgesetz der Eigenwerte linearer partieller Differentialgleichungen (mit einer Anwendung auf die Theorie der Hohlraumstrahlung)," *Mathematische Annalen*, vol. 71, pp. 441–479, Dec. 1912. Publisher: Springer-Verlag.

[82] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[83] M. V. D. Nest, A. Miyake, W. Dür, and H. J. Briegel, "Universal resources for measurement-based quantum computation," *Physical Review Letters*, vol. 97, p. 150504, Oct. 2006. Publisher: American Physical Society.

[84] K. Kieling, T. Rudolph, and J. Eisert, "Percolation, renormalization, and quantum computing with nondeterministic gates," *Physical Review Letters*, vol. 99, p. 130501, Sept. 2007. Publisher: American Physical Society.

[85] D. E. Browne, M. B. Elliott, S. T. Flammia, S. T. Merkel, A. Miyake, and A. J. Short, "Phase transition of computational power in the resource states for one-way quantum computation," *New Journal of Physics*, vol. 10, p. 023010, Feb. 2008. Publisher: IOP Publishing.

[86] S. Aaronson, "Quantum computing, postselection, and probabilistic polynomial-time," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2063, pp. 3473–3482, 2005. Publisher: The Royal Society London.

[87] M. Oszmaniec, N. Dangniam, M. E. Morales, and Z. Zimborás, "Fermion sampling: a robust quantum computational advantage scheme using fermionic linear optics and magic input states," *PRX Quantum*, vol. 3, no. 2, p. 020328, 2022. Publisher: APS.

[88] S. Arora and B. Barak, *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[89] C. H. Papadimitriou, "Computational complexity," in *Encyclopedia of computer science*, pp. 260–265, 2003.

[90] L. Stockmeyer, "On approximation algorithms for# P," *SIAM Journal on Computing*, vol. 14, no. 4, pp. 849–861, 1985. Publisher: SIAM.

[91] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pp. 333–342, 2011.

Appendix A

Appendix

A.1 Coarse Graining 2-Block Calculation

Observation A.1.1. *The maximum value of r' such that the output of*

$$CZ\left(\left[1, r'\cos\left(\theta_A\right), r'\sin\left(\theta_A\right), \pm 1\right] \otimes \left[1, r'\cos\left(\theta_B\right), r'\sin\left(\theta_B\right), \pm 1\right]\right) \tag{A.1}$$

is non-negative for all allowed measurements (Z basis and XY-plane measurements), is $r' = 1/2$. Moreover, for all allowed measurements, non-negative probabilities are obtained if and only if $r' \leq 1/2$.

Proof. We will first make some observations that simplify this problem.

1. Consider the probability

$$\mathrm{Tr}\left(\mathrm{M_A} \otimes \mathrm{M_B} \rho\right), \tag{A.2}$$

where M_A and M_B are measurement operators and ρ is the output state of (A.1). By the cyclicity of the trace, we may consider the CZ acting on the measurement operators $(M_A \otimes M_B$. If either M_A or M_B is a Z-basis measurement, the CZ gate would act trivially. Hence, we would have a product of measurements and no negative probabilities can occur. Therefore, we can restrict our analysis to measurements in the XY plane and exclude measurements in the Z-basis.

2. Suppose, w.lo.g that the second input has $z = -1$ on the given cylinder. This can be described as a $z = 1$ input with an X operator applied to it. Using the identity

$CZ(I\otimes X) = (Z\otimes X)CZ$, we can pull the X through the CZ. Therefore, we would have $(Z\otimes X)$ acting on the measurement operators, however these are just new XY plane or Z-basis measurements. Thereby, showing that we need only consider inputs with $z = 1$.

3. Lastly, consider XY-plane measurements of the form $\cos(\theta)X + \sin(\theta)Y$, which is equivalent to a local Z-rotation acting on a projector of the form $I - X$. Now, again by using the cyclicity of the trace and the fact that CZ commutes with local Z rotations, we would end up with another cylinder extremal state but with a different XY plane angle. Therefore, we may restrict to measurements $I - X$.

We have now simplified the problem to computing the maximum r' such that the output of a CZ gate acting on

$$\left(\left[1, r'\cos(\theta_A), r'\sin(\theta_A), 1\right] \otimes \left[1, r'\cos(\theta_B), r'\sin(\theta_B), 1\right]\right) \tag{A.3}$$

is non-negative for measurement projectors

$$\frac{I-X}{2} \otimes \frac{I-X}{2}. \tag{A.4}$$

Therefore, the probability of getting this outcome is:

$$1 - r'\cos(\theta_A) - r'\cos(\theta_B) + r'^2\sin(\theta_A)\sin(\theta_B) \tag{A.5}$$

$$= \left(1 - r'\cos(\theta_A)\right)\left(1 - r'\cos(\theta_B)\right) - r'^2\cos(\theta_A - \theta_B). \tag{A.6}$$

When $\theta_A = \theta_B = 0$, the condition simplifies to $1 - 2r' \geq 0$, which implies that $r' \leq 1/2$. However, for $0 \leq r' \leq 1/2$, this is the minimal possible value. This can be seen from (A.6), which is always greater than or equal to $(1 - r')(1 - r') - r'^2 = 1 - 2r'$. Therefore, (A.6) is non-negative for all measurements and inputs if and only if $r' \leq 1/2 = r_{2block,\max}$. □

A.2 Matlab Code for Coarse-Graining

```
% Numerical_measuring_MxN_lattice_cylinders on
% a N column and M row lattice
% Output: returns r s.t output probabilities are negative
% for measurement (I-X)/2

% Pauli Operators
```

```
I = eye(2); X = [0 1;1 0]; Z=[1 0;0 -1];

%% 1. initialisation Stage

% Input Columns N, Row M (N,M>1)
N = 3;
M = 3;

% Input height h as a matrix, radius r as a matrix (e.g., plus states r=1s, h=0s)
h = ones(M,N);
r = ones(M,N);

% Loop for values of x corresponding to radius r
for x=0.06:0.00001:0.5
    tic
    % Set radius R = to x value (i.e., increasing radius value for each loop)
    R=x;

    % Set lambda values for corner and edge
    lambda = 1/(sqrt(sqrt(5)-2));
    r_corner = R * lambda * lambda; % corner radius
    r_edge = R * lambda; % edge radius

    % For loop for edge and corner radii
    for i=1:N
        for j=1:M
            r(j,i) = r_edge;
            % Handle corners
            if i==1 && j==1 || i==N && j==1 || i==1 && j==M || i==N && j==M
                r(j,i) = r_corner;

            end
        end
    end

    % For loop for middle radii
    for i=2:N-1
        for j=2:M-1
            r(j,i) = R; %middle qbit has radius r
        end
    end

    % Loop to change the height of middle qubits to sqrt(1-R^2)
    for i=2:N-1
```

```
    for j=2:M-1
        h(j,i) = sqrt(1-R^2); % middle qubit has radius r
    end
end

% Initialise first layer of qubits, first column A
A = 1;
for i=1:1:M
    A1 = 0.5*(I+r(i,1)*X+h(i,1)*Z);
    A = kron(A,A1);
end

%Create measurement operators, I-X on layer A, Identity on B
P0 = 0.5*(I-X);
P=1;
for i=1:1:M
    P = kron(P,P0); % measurement operators 1-X on Layer A
end
for i=1:1:M
    P = kron(P,I); % measurement operators I on Layer B
end

%% 2. Main body: loop that CZs & measures layers
for j=2:1:N
    j;
    % Step 1: CZs on layer A
    CZ_A = 1;
    for i=1:1:M-1
        CZ_A =CZ_A*CZ_function(M,i,i+1);% e.g. if M = 3 -> require 2 CZs
    end
    A = CZ_A*A*CZ_A;

    %Step 2. Create global state psi of layer A and B & do CZs
    B = 1;
    for i=1:1:M
        B1 = 0.5*(I+r(i,j)*X+h(i,j)*Z);
        B = kron(B,B1);
    end

    psi = kron(A,B); % state of layer A and B

    % Step 3: Measure layer A and store prob
    CZ_all = 1;
    for i=1:1:M
```

```
        i;
        CZ_all = CZ_all*CZ_function(2*M,i,i+M);
    end
    psi = CZ_all*psi*CZ_all;

    %3. Measure layer A and store prob
    p(j-1) = trace(P*psi); %prob of Layer
    p_psi = P*psi*P/p(j-1);

    %%Step 4: partial trace over layer A
    %Input state of 2 layers
    % No. M (layer A to trace out, M is number of qubits)
    B = MG_partial_trace_mx2(p_psi,M);
    A = B;
end

%% 3. Final round of measurements and total prob
%Final CZ layer
CZ_A = 1;
for i=1:1:M-1
    CZ_A =CZ_A*CZ_function(M,i,i+1);%e.g. if M = 3 -> requrie 2 CZs
end
psi = CZ_A*A*CZ_A;%final state before measured

% Final measurement operators
P=1;
for i=1:1:M
    P = kron(P,P0); % measurement operators 1-X on Layer A
end
p(N) = trace(P*psi);

%total probability
total =1;
for k=1:N
    total = total*p(k);
end

%% 4. plot numerical
if total <0
    %if total prob < 0 then display
    format long
    [x,total] %radius and probability

    answer = ['At r = ', num2str(x),' get negative probability of ',num2str(tot
```

```
            disp(answer)
            %Return command: i.e. if total prob < 0 then STOP script
            toc
            return
        else
            disp(['no neg prob for r = ', num2str(x), ' continuing loop...'])
            toc
        end
    end
disp(['script finished, no negative probabilities found'])
```

A.3 Calculation of Determinant

In this appendix, we will show that the determinant of the matrix

$$\begin{pmatrix} 1 & f_B & f_A & f_A f_B e^{-i\varphi} \\ f_B & 1 & f_A f_B & f_A \\ f_A & f_A f_B & 1 & f_B \\ f_A f_B e^{i\varphi} & f_A & f_B & 1 \end{pmatrix} \tag{A.7}$$

can be expressed as

$$= \left(f_A^4+1\right)\left(f_B^4+1\right) - 2(f_A^2+f_B^2) - 2f_A^2 f_B^2 \cos\varphi \left(f_A^2+f_B^2-2\right). \tag{A.8}$$

The determinant of (A.7) can be found by taking the cofactor expansion along the first column:

$$\begin{aligned} &1\begin{vmatrix} 1 & f_A f_B & f_A \\ f_A f_B & 1 & f_B \\ f_A & f_B & 1 \end{vmatrix} - f_B \begin{vmatrix} f_B & f_A & f_A f_B e^{-i\varphi} \\ f_A f_B & 1 & f_B \\ f_A & f_B & 1 \end{vmatrix} \\ &+ f_A \begin{vmatrix} f_B & f_A & f_A f_B e^{-i\varphi} \\ 1 & f_A f_B & f_A \\ f_A & f_B & 1 \end{vmatrix} - f_A f_B e^{i\varphi} \begin{vmatrix} f_B & f_A & f_A f_B e^{-i\varphi} \\ 1 & f_A f_B & f_A \\ f_A f_B & 1 & f_B \end{vmatrix}. \end{aligned}$$

By calculating the 3 by 3 determinant in each term, we have

$$\begin{aligned} &f_A^2 f_B^2 - (f_A^2+f_B^2) + 1 + f_B e^{-i\varphi}\left(-f_A^2 f_B^3 + f_A^2 f_B + e^{i\varphi} f_B^3 - e^{i\varphi} f_B\right) \\ &\quad + f_A e^{-i\varphi}\left(-f_A^3 f_B^2 + e^{i\varphi} f_A^3 + f_A f_B^2 - e^{i\varphi} f_A\right) - f_A^2 f_B^2\left(-f_A^2 f_B^2 + e^{i\varphi}(f_A^2+f_B^2) - 2e^{i\varphi} + 1\right). \end{aligned}$$

This can now be simplified to give equation (A.8):

$$\begin{aligned}
&f_A^2 f_B^2 - (f_A^2 + f_B^2) + 1 + f_A^4 + f_B^4 - (f_A^2 + f_B^2) + f_A^2 f_B^2 e^{-i\varphi}(2 - f_A^2 - f_B^2) \\
&\qquad - f_A^2 f_B^2 \left(-f_A^2 f_B^2 + e^{i\varphi}(f_A^2 + f_B^2) - 2e^{i\varphi} + 1\right) \\
&= 1 + f_A^4 f_B^4 + f_A^4 + f_B^4 - 2(f_A^2 + f_B^2) + f_A^2 f_B^2 (2 - f_A^2 - f_B^2) e^{-i\varphi} - f_A^2 f_B^2 (f_A^2 + f_B^2 - 2) e^{i\varphi} \\
&= 1 + f_A^4 f_B^4 + f_A^4 + f_B^4 - 2(f_A^2 + f_B^2) + 2 f_A^2 f_B^2 \cos\varphi (2 - f_A^2 - f_B^2) \\
&= 1 + f_A^4 f_B^4 + f_A^4 + f_B^4 - 2(f_A^2 + f_B^2) - 2 f_A^2 f_B^2 \cos\varphi \left(f_A^2 + f_B^2 - 2\right) \\
&= \left(f_A^4 + 1\right)\left(f_B^4 + 1\right) - 2(f_A^2 + f_B^2) - 2 f_A^2 f_B^2 \cos\varphi \left(f_A^2 + f_B^2 - 2\right).
\end{aligned}$$

A.4 Matlab Code To Determine Growth Rate of Cylinder-Cone Separability

In this appendix, we present the code used to calculate the growth rate $g_{CC} = R/r$ in fig.4.9. As can be seen in the code, we used an increment of 0.0001 for g. However, for $r \leq 0.1$ we used an increment of 0.00001.

```
% LinearProgram_for_CC_separability
% The code calculates the growth rate for a cylinder cone to be separable
% w.r.t to cylinders, using different values of r and plots the results.

% Initialise variables
plot_r = [];
plot_g = [];
j = 1;

% Loop through different values of r
for r = 0.01:0.001: 0.6

    h = sqrt(1-(r*r)); % Calculate h based on the current value of r

    % Loop through different values of g
    for g = 1.5:0.00001:2.1

        R = g*r; %Calculate R based on the current value of r and g

        %% 1. Input state space: elongted cone varying radius
        va = [1;r;0;h];    vb = [1;r;0;h];
```

```
coef = kron(va,vb);
large_CZ = [
    1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0  0  0  0  0  1  0  0;
    0  0  0  0  0  0  0  0  0  0  0  0  0  0  1  0;
    0  0  0  1  0  0  0  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  1  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0  0  1  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0 -1  0  0  0  0  0  0;
    0  0  0  0  1  0  0  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0  0  0  1  0  0  0  0;
    0  0  0  0  0  0 -1  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  1  0  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  1  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0  0  0  1  0  0  0  0;
    0  1  0  0  0  0  0  0  0  0  0  0  0  0  0  0;
    0  0  1  0  0  0  0  0  0  0  0  0  0  0  0  0;
    0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1];

% create beq representing the input state acted on with a CZ
beq = large_CZ*coef;

%% 2. Create output state space: cylinder states with unit height
inc = 18; %discretisation parameter of points around XY-plane
i = 0;

for ha = [1,-1]
    for x = 0:inc:359.99
        i = i+1;
        G1(:,i) = [1;R*cosd(x);R*sind(x);ha];
    end
end

Aeq = kron(G1,G1);% Calculate matrix Aeq representing output state space

%% 3. Run Linear program
[numRows,numCols] = size(Aeq); % Get dimensions of Aeq matrix
A = -1*eye(numCols); % Constraint that xi's >= 0
b = zeros(numCols,1); % Ax <= b
f = zeros(numCols,1); % Set objective function to zero

% Run linear program, checking feasibility
%supress no constraints found
options = optimoptions('linprog','Display','none');
```

```
        x = linprog(f,A,b,Aeq,beq,[],[],options);

        if isempty(x) == 0 % If x is non-empty, a feasible solution exists
            R
            break
        end
    end
    % Calculate growth factor
    plot_r(j) = r;
    plot_g(j) = g;
    j = j+1;
end

% Plot results
plot(plot_r,plot_g)
yline(2.058,'--') % Plot cylinder growth rate
legend('g_{cc}','g_c = 2.05817')
xlabel('r')
ylabel('g')
grid on
```

A.5 Determining Separability for Protruding State Spaces via Linear Programming

This is an example with $\zeta = 0.1$ and $h = 0.5$ to demonstrate the process described in Sec.4.4.1.The task is to determine if $CZ(\rho_A \otimes \rho_B)$, where ρ_A, ρ_B are drawn from $\mathscr{P}(r,h,\zeta)$, is separable w.r.t $\mathscr{P}(r,h,\zeta)$. We now employ the arguments discussed in Sec.4.4.1 to reduce the number of input states we need to consider:

$$\begin{aligned} [1,1,0,0] \otimes [1,1,0,0], \\ [1,1,0,0] \otimes [1,\omega,0,0.5], \\ [1,\omega,0,0.5] \otimes [1,\omega,0,0.5]. \end{aligned} \tag{A.9}$$

Our objective is to determine when the output of a CZ gate acting on every input extrema in (A.9) is $\mathscr{P}(r,h,\zeta)$-separable. We begin by considering the single input extrema: $[1,1,0,0] \otimes [1,1,0,0]$. Expressing the action of the CZ gate on this input in the Pauli we have:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{A.10}$$

Noting the non-zero Pauli coefficients, we can form the vector representing our input state:

$$b_{eq} = (1,0,0,0,0,0,0,1,1,0,0,1,0,0,1,0,0)^T, \tag{A.11}$$

with $\rho_{11} = \rho_{2,4} = \rho_{3,3} = \rho_{4,2} = 1$. Our next step is to construct the matrix A_{eq}, where each column vector contains the Pauli expansion coefficients of an extremal product state.To achieve this, we discretise the single-particle state space $\mathscr{P}(r,h,\zeta)$ by selecting a finite set of θ values. Here, we consider $\theta = 0, \frac{\pi}{3}, \frac{2\pi}{3}, \ldots, \frac{5\pi}{3}$, which leads to a 4×20 matrix for the single-particle state space of particles A and B:

$$S^{A/B} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & \cdots & 1 & \cdots \\ 0 & 0 & R & \cdots & R\omega & \cdots & R\omega & \cdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots \\ 1 & -1 & 0 & \cdots & h & \cdots & -h & \cdots \end{pmatrix}, \tag{A.12}$$

where $\omega = \frac{11\sqrt{3}}{20}$. The first two columns contain the Bloch vector coefficients of $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, respectively. Starting from the third column, these are the states that lie on the XY plane. The remaining matrix entries denote states that have height $\pm 1/2$, where the Bloch vector coefficients of x and y are given by $R\omega\cos\theta$ and, $R\omega\sin\theta$ respectively. Recall, the parameter we will be varying to determine if the output is separable is R. We can now form the matrix A_{eq} that represents the output state space:

$$A_{eq} = S^A \otimes S^B,$$

where A_{eq} is a 16×400 dimensional matrix. Furthermore, we impose the condition that the probability distribution must be non-negative by setting A and b as in (4.56), where A is of size $D \times D$ and b is a D-dimensional column vector, with $D = 400$.

We have now transformed the problem of finding a separable decomposition into a Linear Programming problem. By increasing the parameter R, that is, the radii R of the output state

space, we can run the linear program to check for a feasible solution. In this example, the linear program returns a feasible solution at $R = 2.331$. We now repeat the above procedure with the second pair of input extrema in (A.9). We find that this returns a feasible solution at $R = 2.398$. Lastly, we repeat the procedure with the last input extrema in (A.9), finding a feasible solution at $R = 2.507$. Therefore, we can conclude a CZ that acts on any operators drawn from $\mathscr{A}(r, 0.5, 0.1)$ can be given a separable decomposition if the operators in the separable decomposition are drawn from $\mathscr{P}(R, 0.5, 0.1)$, where $R \geq 2.507r$.

A.6 Explicit Solution to the Recursion Relation

In this appendix, we solve the recursion relation leading to equation (5.19). The eigenvalues of

$$T = \begin{pmatrix} \cos(\theta/2) & -\cos(\theta/2) \\ \sin(\theta/2) & \sin(\theta/2) \end{pmatrix} \tag{A.13}$$

can be straightforwardly found:

$$\lambda_{1,2} = \frac{\cos(\theta/2) + \sin(\theta/2) \pm \sqrt{1 - 3\sin(\theta)}}{2}. \tag{A.14}$$

The eigenvectors of T can be found using standard row reduction techniques. For λ_1 we have:

$$T - \lambda_1 I_2 = \begin{pmatrix} a - \lambda_1 & -\cos(\theta/2) \\ b & b - \lambda_1 \end{pmatrix} \xrightarrow{R_1 : \frac{1}{a-\lambda_1} R_1} \begin{pmatrix} 1 & \frac{-a}{a-\lambda_1} \\ b & b - \lambda_1 \end{pmatrix} \tag{A.15}$$

$$\xrightarrow{R_2 : R_2 - bR_1} \begin{pmatrix} 1 & \frac{-a}{a-\lambda_1} \\ 0 & 0 \end{pmatrix}, \tag{A.16}$$

where we have set $a = \cos(\theta/2)$ and $b = \sin(\theta/2)$. The eigenvector corresponding to λ_1 is therefore

$$|v_1\rangle = \begin{pmatrix} \frac{a}{a-\lambda_1} \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{2\cos\left(\frac{\theta}{2}\right)}{\sqrt{2}\cos\left(\frac{\theta}{2}+\frac{\pi}{4}\right) - \sqrt{1-3\sin(\theta)}} \\ 1 \end{pmatrix}. \tag{A.17}$$

Similarly, the eigenvector corresponding to λ_2 is

$$|v_2\rangle = \begin{pmatrix} \frac{a}{a-\lambda_2} \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{2\cos\left(\frac{\theta}{2}\right)}{\sqrt{2}\cos\left(\frac{\theta}{2}+\frac{\pi}{4}\right)+\sqrt{1-3\sin(\theta)}} \\ 1 \end{pmatrix}. \tag{A.18}$$

We now express (5.19) in terms of the eigenvalues λ_1, λ_2 and corresponding eigenvectors $|v_1\rangle, |v_2\rangle$ of T:

$$|\theta_n'\rangle = T^{n-1}(c_1|v_1\rangle + c_2|v_2\rangle) \tag{A.19}$$

$$= c_1\lambda_1^{n-1}|v_1\rangle + c_2\lambda_2^{n-1}|v_2\rangle. \tag{A.20}$$

Lastly, c_1, c_2 can be found by setting $|\theta\rangle = c_1|v_1\rangle + c_2|v_2\rangle$:

$$\begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix} = c_1 \begin{pmatrix} \frac{\cos(\theta/2)}{\cos(\theta/2)-\lambda_1} \\ 1 \end{pmatrix} + c_2 \begin{pmatrix} \frac{\cos(\theta/2)}{\cos(\theta/2)-\lambda_2} \\ 1 \end{pmatrix} \tag{A.21}$$

which can be solved to find that

$$c_1 = \frac{\cos(\theta) - \sin(\theta) + 2\sin\left(\frac{\theta}{2}\right)\sqrt{1-3\sin(\theta)} - 1}{4\sqrt{1-3\sin(\theta)}}, \tag{A.22}$$

$$c_2 = \frac{\sin(\theta) - \cos(\theta) + 2\sin\left(\frac{\theta}{2}\right)\sqrt{1-3\sin(\theta)} + 1}{4\sqrt{1-3\sin(\theta)}}. \tag{A.23}$$

A.7 Purifying the Output of the Recursion to a $|+\rangle$ State

In this appendix, we show that if $\theta > \theta_c$, the output of the recursion can yield a $|+\rangle$ state on the end of the 1D-chain.

Suppose that $\theta > \theta_c$, then we have that $|\lambda_1| = |\lambda_2|$, and $|c_1| = |c_2|$. We can rewrite λ_1 and λ_2 in their polar forms as $\lambda_1 = r_\omega e^{i\omega}$ and $\lambda_2 = r_\omega e^{-i\omega}$. Now, using these expressions for $\lambda_{1,2}$ we can rewrite (5.19) in the computation basis:

$$|\theta_n'\rangle = c_1\lambda_1^{n-1}|v_1\rangle + c_2\lambda_2^{n-1}|v_2\rangle \tag{A.24}$$

$$= r_\omega e^{i\omega m}\left(c_1|v_1\rangle + c_2 e^{-2i\omega m}|v_2\rangle\right) \tag{A.25}$$

$$= r_\omega e^{i\omega m}\left[\left(\frac{c_1\cos(\theta/2)}{\cos(\theta/2)-\lambda_1} + \frac{c_2\cos(\theta/2)e^{-2i\omega m}}{\cos(\theta/2)-\lambda_2}\right)|0\rangle + \left(c_1 + c_2 e^{-2i\omega m}\right)|1\rangle\right], \tag{A.26}$$

where $m = n-1$. Our aim is now to show that, for $\theta > \theta_c$, the magnitudes of the amplitudes of $|0\rangle$ and $|1\rangle$ can be equal:

$$\left| \frac{c_1 \cos(\theta/2)}{\cos(\theta/2) - \lambda_1} + \frac{c_2 \cos(\theta/2) e^{-2i\omega m}}{\cos(\theta/2) - \lambda_2} \right| = \left| c_1 + c_2 e^{-2i\omega m} \right| \tag{A.27}$$

This can be rewritten as

$$\left| \frac{c_1 \cos(\theta/2)}{\cos(\theta/2) - \lambda_1} + \frac{c_2 \cos(\theta/2) e^{-2i\omega m}}{\cos(\theta/2) - \lambda_2} \right| - \left| c_1 + c_2 e^{-2i\omega m} \right| = 0. \tag{A.28}$$

To show that the above equation can be satisfied, for different values of m we have numerically calculated the output of the recursion, presented in fig.A.1. This figure suggests that for $\theta > \theta_c$ the output of the recursion $|\theta_n'\rangle$ can indeed yield a $|+\rangle$ state as the corresponding output angle $\theta' = \pi/2$ can be attained. For clarity in fig.A.1, we have plotted the radius rather than angle of the state, i.e. $r_{in} = |\sin\theta|$ and $r_{out} = |\sin\theta'|$.

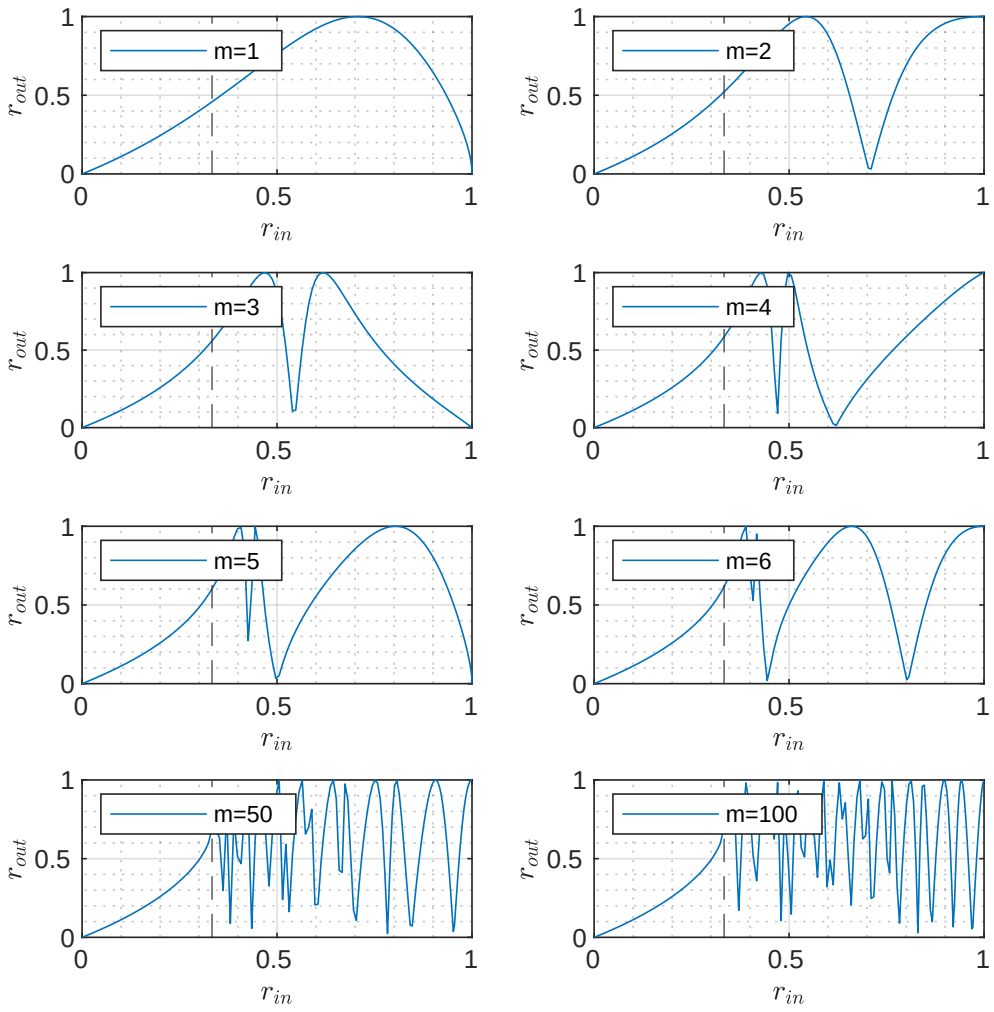


Fig. A.1 This figure depicts the recursion output for different values of m. The horizontal axis is the radius corresponding to the input angle (i.e. $r_{in} = |\sin\theta|$) and the vertical axis is the radius corresponding to the angle of the output state ($r_{out} = |\sin\theta'|$). The vertical dotted black line is the critical threshold $\sin\theta_c = 1/3$. The figure suggests that when $\theta > \theta_c$, the recursion output $|\theta'_n\rangle$ can yield a $|+\rangle$ state.