Quantum Computation Beyond the Unitary Circuit Model

Naïri Usher

A thesis submitted to

University College London

for the degree of

Doctor of Philosophy

Department of Physics and Astronomy

University College London

September 2016

I, Naïri Usher, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Signed: Date:

Publications

The majority of the work presented in this thesis contains materials from the following publications:

N. Usher, and D.E. Browne, *Noise in Measurement-Based Quantum Computing*, arXiv:1704.07298.

N. Usher, M.J. Hoban, and D.E. Browne, *Constructing Local Hamiltonians from Non-unitary Quantum Computation*, arXiv:1703.08118.

M.J. Hoban, J.J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D.E. Browne, *Measurement-Based Classical Computation*, Phys. Rev. Lett. **112**, 140505 (2014).

Acknowledgements

I am thankful for my time at UCL which has brought to me more than words can convey. First and foremost, I am thankful to Dan for having supported and guided me throughout my PhD with endless patience and kindness. I am truly grateful for his encouragement to explore and investigate questions I found interesting as well as for everything I had the chance to learn from him. I wish to thank my examiners Shashank and Sougato for having taken the time to read this thesis as well as for offering valuable feedback for its improvement. I was fortunate to collaborate with Matty, with whom I shared many both interesting and entertaining discussions, and I am thankful for his invaluable insights and encouragement. I am in particular thankful to Simone for his continued support and guidance. From my start at UCL, the quantum group meetings were a source of joy, each week introducing me to new ideas, and granting me the privilege of learning from exceptional people, and for this I am thankful to Dan, Fernando, Aram, Jonathan, Simone and Toby.

I have made many friends throughout both my time at UCL and travelling the world to conferences: to all those with whom I have shared coffees, drinks, dances and walks, thank you for enriching my life. I found within the physics department a space in which questions were always welcome, and I thank all those with whom I spent time discussing and debating all matter of ideas. I look back with a particular fondness to both my first ever summer school in Waterloo and a trip to Malawi, for which I am greatly thankful to Terry for the brilliant organisation and experience. The K_3 has been a bastion of sanity, and have proven themselves to be thoroughly solid vertices throughout all these adventures. Thank you to Chris for walking, benching and impromptu singing, and to Pete for his skill at fixing all things, endless laughter and activities. To my co-author and friend, Hussain, I am thankful for arguments, coffees and most of all, his kindness. To my friends Noor and Justin, I am grateful for your true friendship, and look forward to times yet to come. And finally, thank you to my mother, my friend, Victoria Gaspari, for showing me, ever since the day I was born, all the beauty and wonder to be discovered within the world.

Abstract

This thesis considers various paradigms of quantum computation in an attempt to understand the nature of the underlying physics. A standard approach is to consider unitary computation on pure input states, such that the outcome of the computation is determined by single computational basis measurement on the output state. It has been shown that there exists equivalent models of computation, such as measurement based quantum computing (MBQC), which provide insight into the role of entanglement and measurement. Furthermore, constraining or relaxing available resources can directly impacts the power of the computation, allowing one to gauge their role in the process.

Here, we first extend known constructions such as Matrix Product States, MBQC and the one-clean qubit model to a mixed state formalism, in an attempt to develop computational models where noise acting on the physical resources, as might be experienced in laboratory settings, may be mapped to logical noise on the computation. Next, we introduce Measurement-Based Classical Computing, an essentially classical model of computation, wherein the complexity hard wired into probability distributions generated via quantum means yields surprising non classical results. Finally, we consider postselection the ability to discard displeasing measurement outcomes and argue that it may be used in a tame way, which does not provide a dramatic increase in computational power. From here, we develop a new Hamiltonian, based on a circuit to Hamiltonian construction, presenting evidence of QMA-hardness.

Contents

List of Figures

Chapter 1

Introduction

1.1 Physics, Computation, Information

Since our earliest age, we watch and observe the world, instinctively seeking patterns and repetitions within the unknown that surrounds us. We learn to predict and thus to expect, and so we tame a world dancing to an elusive rhythm seemingly always beyond our grasp. We call a description of these processes an explanation and believe that to predict, is to understand. At times, sudden paradoxes appear to us unwitting observers, leaving us both troubled and determined to resolve the apparent discontinuity in our understanding. One might argue that it is precisely these paradoxes which force us to leap into uncharted territory in our attempt to resolve them. Often, the source of our errors lies within our assumptions—automatic beliefs we harbour about the world—the more seemingly trivial and obvious, the more treacherous in hindsight. It was in such an opaque atmosphere that, more than a century ago, the fields of both mathematics and physics were thrown into disarray, fundamental paradoxes shaking what had previously been thought to be solid ground. This predicament would only find its resolution with a complete overhaul of both their respective foundations.

At the turn of the twentieth century, the field of mathematics was subjected to a thorough investigation, the aim of which was to solidify its foundations, ultimately leading to what became known as the foundational crisis of mathematics [1, 2]. Spurred forward by the likes of Cantor's infinities and Russell's paradox, mathematicians from various schools of thought sought to develop a consistent and complete framework of mathematics, both powerful and intuitive in its structure. Of the three fundamentally opposed approaches which collided in this attempt, namely logicism [3], intuitionism [4] and formalism [5], it would be Hilbert's formalist approach which would emerge dominant. Today, we are barely aware of Russell's attempt at deriving for instance natural numbers from Grecian prepositional logic, or even less of Bouwer's belief that the human mind is ultimately our only source of knowledge, and that thus for instance proofs by contradiction are unsound.

The formalist goal was to derive a finite set of axioms alongside a finite set of simple rules,

from which the most complex of mathematical objects could be built (complete) whilst avoiding paradoxical statements (consistent). In 1928, Hilbert posed the Entscheidungsproblem [6], asking whether given a first-order logical expression one may determine whether it is universally valid, or equivalently, deductible from a given set of axioms. Three years later, in 1931, Gödel's first incompleteness theorem established that in any strong enough axiomatic framework, there would exist statements which although true were not provable. The final blow to this ideal would be dealt in 1936, independently by both Church [7] and Turing [8] who both realized and developed an abstract model capturing the mechanical notion of computation, which nonetheless could not compute every single function.

Yet, from this wreckage, a profound insight emerged: the computability of a function is independent of the formal framework used, a result known as the Church–Turing Thesis. Indeed, Turing's abstract model of computation, the Turing Machine still serves as the computational model of choice in computational complexity for the study of problems. This is a mechanical device built from an infinite piece of tape, a tape head which may read or write on the tape as well as move to the left or to the right. The behaviour of the tape head is dictated by its internal state, what we may think of as a list of contingency instructions, a program. In other words, the computation is broken down into a sequence of simple steps to be performed according to a given set of rules. The ground-breaking insight that a universal Turing Machine can simulate the behaviour of any Turing Machine—with polynomial overhead—spearheaded the creation of the fields of computation and information.

Nevertheless, it was shown that there existed functions which could *not* not be computed, such as for instance the halting problem. Here, given the description of a Turing machine and an input, one is asked to determine whether the machine eventually halts on an input. By using techniques akin to Cantor's diagonal argument, this was shown to be an uncomputable problem, whose undecidability stems from the fundamental impossibility of establishing a bijection between the number of Turing machines with the number of possible problems. Notwithstanding, this series of results heralded a new era of technological advancement, the age of computation, which would see human society radically change within the space of half a century.

Yet one might argue that this process of change truly originated in the seventeenth century, when the field of physics rapidly grew to encompass a plethora of physical phenomena in its insights and predictions. It was a time when Newton's laws of mechanics and a growing understanding of thermodynamics ignited the industrial revolutions and irretrievably altered the fabric of society. From trains to mills passing through steam power and mining, scientific progress affected all aspects of life, allowing man to automate tasks and harness the physical world to the realization of his ambitions. By the end of the nineteenth century, Maxwell and Faraday had successfully explained the phenomena of both electricity and magnetism, until then mysterious powers at play. Physics

emerged triumphant and man felt master of his world.

It started with unexpected experimental observations. The radiation spectrum of a black body, the behaviour of electrons on a metal surface exposed to light and the atomic spectra presented behaviour in stark conflict with that predicted from the established theories of yesterday. Planck realised that the first of these, resulting in the ultraviolet catastrophe, could be resolved if energy was treated as a discrete quantity. This simple mathematical assumption, formally known as quantization, was in conflict with the classical view of energy as a continuous quantity. With Einstein's seminal 1905 paper [9], what initially seemed to be a mere mathematical formality came to revolutionise our understanding and perception of physics at the atomic scale. Light was posited to consist of individual quanta—or photons—each carrying a discrete packet of energy, and thus a significant shift in our description of the world occurred. Later, the idea of quantization would be applied by Bohr to the atom, and yet again lead to more accurate theoretical predictions.

For centuries, if not millennia, the nature of matter has been subject to intense speculation and debate, alternating between being thought of as either a particle or a wave. With quantum theory, these two seemingly mutually exclusive characters were reunited, two sides of one and the same coin, matter exhibiting one behaviour or the other depending on the experiment at hand. Objects at the atomic and subatomic scale would be described by their wave function, as introduced by Schrödinger, and their dual aspects connected via the De Broglie wavelength.

Yet, the nature of the wave function remained mysterious, for it remained unclear as to whether it referred to a state of physical reality or a state of human knowledge. If a quantum system is measured, it allows for the outcome probabilities to be computed. Therein lies the information it can yield. Since then, the field of quantum foundations has grown in its attempt to propose a clear interpretation, although no consensus or resolution has been found to this day.

The EPR paper of 1935 [10] probed the question as to whether in the absence of measurement quantum systems nonetheless possess physical properties. Indeed, the intrinsically probabilistic quantum theory yields no information as to the state of the system prior to observation, and yet once a measurement is performed, a certain configuration of reality is witnessed. The term action at a distance was introduced in order to capture the process whereby this could take place. This raised questions as to the locality—objects separated in space should not instantaneously influence one another—as well as separability—each object has a reality—of the theory. Shortly after, Schrödinger introduced the term entanglement [11] in order to capture the notion of non-local correlations arising within a composite quantum system. Later, Bell would go on to show that these quantum correlations were stronger than classical correlations.

However surprising these ideas might have seemed, quantum theory provided an increasing amount of correct experimental predictions, and with time, its successes established it as an ac-

cepted model of reality at the atomic scale. Had a complete theory allowing us to calculate and predict the behaviour of small objects been achieved? A pivotal problem was soon encountered: when considering collections of objects—as opposed to individual particles or atoms—the nature of the correlations arising within the system were far more complex than what we were classically accustomed to. In order to model such composite systems, an exponential mathematical workspace was required, which in turn meant that to simulate its behaviour on a classical computer could require exponential time. This fundamental realization had as a consequence that, a priori, the mere description of a quantum system constitutes an intractable problem, leaving us unable to generically calculate and predict its properties or behaviour. Could it be that our understanding and technological advances had come to an unexpected grinding halt?

It was Feynman who, in 1982, realised that if a quantum system could not be simulated by a classical system due to the required resources growing exponentially with the system size, then perhaps a quantum system could be used in order to efficiently simulate *another* quantum system [12]. This raised the question of building a quantum computer [13], a computational device based not on the laws of classical physics, but of quantum physics, which was subsequently formalised and pioneered by Deutsch [14]. The field of quantum computing gained momentum, and in 1994, Shor proposed an algorithm for efficient prime factorization [15] with a polynomial run time on a quantum device, as opposed to its believed classical intractability. By harnessing the nature itself of quantum systems a new model of computation had been developed, and thus a novel prospect arose: could a quantum computer be strikingly, even exponentially, more powerful than a classical computer?

In the affirmative, this would mean that the laws of physics governing quantum systems could be utilised for greater computational power, and thus that it is perhaps precisely the classical intractability of quantum systems which could be leveraged for a speed-up. This would be a violation of the strong Church-Turing thesis [14] which asserts that any reasonable model of computation can be efficiently simulated by a Turing Machine, thus linking the notions of computation to that of the physical model.

Yet, we are faced with an important caveat: due to experimental challenges [16], no scalable universal quantum computer has to this day been buit: although significant advances have recently been made [17–19], the effect of noise remains a critical problem. Indeed, the traditional frameworks for both quantum computation and algorithms have been developed for noiseless physical systems. In practice, quantum systems are sensitive, and their interaction with the environment induces noise which must be contended with, via for instance quantum error correction codes to achieve fault tolerance [20–22]. Important research advances have meant that noise below a certain threshold may be tolerated in order for the system to simulate a noiseless computation. Nonetheless,

it remains that in practice, every stage of the computational process is affected by noise, damaging our knowledge of the physical states, the information they encode and the computation performed. Thus, between the promise of quantum computing and the challenges of experimental implementation, some might argue that this is a time similar to that of classical computing in the sixties, when the silicon chips which would lead to a revolution in hardware were yet to be discovered. Others, that these experimental obstacles are more than mere technical issues, and that perhaps there exists a fundamental restriction placed by nature on what we may compute and control. Nonetheless, competing groups throughout the world have been continuously making advances towards building a universal quantum computer, achieving significant milestones on the way.

And so a natural question arises: could currently available quantum technologies be somehow exploited in order to achieve quantum computational tasks which provide a speed-up over classical algorithms? In order for this to be successful, non-classical features of quantum systems would have to be harnessed and thus on a fundamental level, such an approach could allow us to determine what the quantum ingredient at the root of the speed-up is. In turn, this could shed light on the intrinsic difference between the nature of classical and quantum objects.

The world may thus be probed via two different paradigms: that of physics and that of computation. The first focuses our attention on material objects evolving according to physical laws, whereas the second shifts it to that of information being processed, each approach allowing us to study the world from a different perspective. Whereas one might initially believe this to be cause for tension, the deep connections between these two pictures soon yield a sense of complementarity. For indeed, computation requires physical resources to be performed and information is encoded onto systems, or as Landauer said "information is physical" [23]. Our understanding of the nature of the world lies perhaps not in picking one approach over another, but instead, in understanding their connections.

This thesis proposes to study quantum computation beyond the standard circuit model, with the fundamental motivation being the interplay between quantum physics and computation. In this introductory chapter we present crucial ideas from quantum physics in section 1.2, followed by quantum computation in section 1.3 and finally computational complexity in section 1.4. Next, in chapter 2, a model for noise in one-dimensional MBQC is developed, and subsequently used in order to study the mapping of physical errors acting on physical states to logical errors acting on the computation. In chapter 3, Measurement Based Classical Computing (MBCC) is introduced, which is an essentially classical model of computation, which allows for the role of adaptivity in MBQC to be investigated. Finally, in chapter 4, a novel family of Hamiltonian operators encoding non-unitary evolutions is presented and its complexity studied.

1.2 Quantum Physics

Our perception of the world shifts with the object we behold. At times continuous, at others discrete, our model of reality depends on the task at hand. On one hand, our physical experience of space-time offers us the intuition that the world is continuous, that is, best described by the continuum of real numbers. On the other, discrete models have proven themselves to be both useful — from statistical mechanics to computation — and more simple to comprehend. That these two models are as yet unconnected and seem to point to two altogether different worlds is a perplexing question. It is precisely this chasm between discrete and continuous quantities, that is of natural versus real numbers, which was at the root of uncomputability, and which we shall yet again encounter within the framework of quantum theory.

Ultimately, as all physical theories, quantum theory seeks to model reality—or more specifically, an experiment—in order to provide the observer with accurate predictions of future observations. Henceforth, we shall choose to ignore the specifics of physical systems—that is, of the object—and instead consider a more abstract, high level picture, in that of its representation.

For example, a room may be lit by turning a switch and an integer can subsequently be associated with each of the room's states: 0 or 1 corresponding to whether the light is off or on. Here, we are not concerned with the particularities of the specific device providing us with light, be it a light bulb or a gas lamp, but instead with whether light is or is not present. Similarly, an atom may be in its lowest energy state or have absorbed a photon and thus be in a higher energy—or excited—state. These in turn can be associated with two orthonormal states $|0\rangle$ and $|1\rangle$, which are called computational basis states. In analogy with classical information theory, where a state 0 or 1 is a bit, we shall call such a 2-level quantum object a quantum bit—or a qubit—and more generally, a qudit for a d-level system.

Henceforth, we shall adopt an information theoretic approach to the treatment of quantum systems and abstract much of their physical detail. A state vector $|\psi\rangle$, the wavefunction, will provides us with a description of the quantum system. This is a vector belonging to a complex Hilbert space, which may be expressed as a linear combination $|\psi\rangle = \sum_{i=1}^{N} \alpha_i |\phi_i\rangle$ in an orthonormal basis $|\phi_i\rangle$, and where normalisation requires that $\sum_{i=1}^{N} |\alpha_i|^2 = 1$. For example, a single qubit may be expressed in the computational basis as $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, with $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

As we previously saw, quantum theory requires for certain physical quantities such as spin, angular momentum or energy to be discrete. The basis elements $|\phi_k\rangle$ in conjunction with some real eigenvalues λ_k define a Hermitian operator $\mathcal{O}$, called an observable: $\mathcal{O} = \sum_{k=1}^{N} \lambda_k |\phi_k\rangle\langle\phi_k|$. For example, this could refer to the energy of the system, where each basis element corresponds to an energy level, such as the ground and excited states $|E_0\rangle$ and $|E_1\rangle$ in the case of an atom. The eigenvalues and complex amplitudes then specify, via the Born rule, the probability of obtaining a specific outcome when the energy is measured.

But objects rarely, if ever, exist as isolated entities. Instead, these interact with different elements forming greater and more complex systems. Thus a composite system made of two parts $\mathcal{A}$ and $\mathcal{B}$—for example an atom and its environment—are combined via a tensor product and form a Hilbert space $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. As we shall see, the correlations present between these two subsystems will prove to be at the heart of quantum theory and computing. When we focus our attention on one of the subsystems, we lose valuable information contained within the correlations: in the words of Aristotle, "The whole is greater than the sum of its parts".

The aim of this section is to introduce some of the main ideas behind the framework of quantum theory [24]. First, in section 1.2.1, we consider the description of an isolated quantum system, and next, in section 1.2.2, we introduce Matrix Product States (MPS), which belong to the family of tensor network states. Next, we shall consider subsystems and see how these may be described in the mixed state formalism. The dynamics of both pure and mixed states will then be studied, before finally the pivotal role of measurement as the interface between quantum and classical information is discussed.

1.2.1 Quantum States

A system of n-qubits is described by its wave function $|\psi\rangle$, a normalised vector living within a complex Hilbert space $\mathcal{H}$ of dimension 2^n, which can be expressed as:

$$|\psi\rangle = \sum_{k=1}^{n} \sum_{i_k=0}^{1} \alpha_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle, \tag{1.1}$$

where $|i_1 \ldots i_n\rangle$ denotes the computational basis and $\alpha_{i_1 \ldots i_n} \in \mathbb{C}$ a complex coefficient. For ease of notation, this will henceforth be expressed:

$$|\psi\rangle = \sum_{i_1 \ldots i_n} \alpha_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle. \tag{1.2}$$

In order for the laws of probability to be conserved, it is required for the quantum state to be normalised, that is $|||\psi\rangle|| = \sqrt{\langle\psi|\psi\rangle} = 1$ and we thus have that: $\sum_{i=1} |\alpha_i|^2 = 1$.

The wavefunction belongs to a Hilbert space whose dimension grows exponentially with the number of qubits n. Thus, for it to be fully specified, an exponential number of terms is required: the mere description of an arbitrary quantum state is classically intractable, let alone the computation of its physical properties. Intuitively, this means that the complexity of an arbitrary state is high.

This is related to the nature of quantum correlations. Indeed, let us consider the global state $|\psi\rangle$ of n particles. In the case when each particle is completely uncorrelated with its neighbours, then its description is local and we can write that particle i is described by a state $|\phi_i\rangle$. The global state is then called a product state: $|\psi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$, where $|\phi_i\rangle$ is a valid state for $i = 1, \ldots, n$. Here,

the number of terms required to describe the state scales polynomially with the system size, akin to what we are classically accustomed to. On the contrary, if such a description can not be obtained, then the state is said to be entangled. This occurs when the state of each particle is correlated to at least another. An example of a two qubit entangled state is given by $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, one of the four entangled Bell states. In this case, the description of the system scales exponentially with its size.

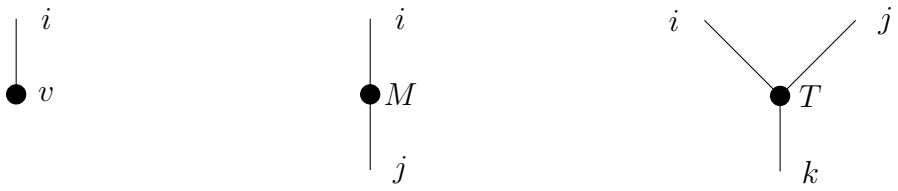
Ultimately, we are interested in quantum states which occur in nature. These are found to possess certain striking properties: for example, ground states of typical Hamiltonians are not of arbitrary complexity, plucked at random from the Hilbert space. Instead, such physical states seem to occupy a region of the Hilbert space with bounded complexity, and the question thus arises: is a typical quantum state a generic quantum state? Or, can we, by placing restrictions on correlations or geometry define families of states? In an attempt to answer these questions, we shall now introduce Matrix Product States (MPS). These belong to the more general class of tensor network states, and are one such example.

1.2.2 Tensor Network States: Matrix Product States

Tensors are mathematical objects commonly used in physics both as a computational tool and in order to represent and store the information pertaining to a system and its physical properties. Particularly used in the fields of many body and condensed matter physics, a tensor is a d-dimensional array $T_{i_1,\dots i_d}$, $d \in \mathbb{N}$. For example, a one-dimensional tensor corresponds to a vector v_i, $i \in \mathbb{N}$ and a two-dimensional tensor to a matrix M_{ij}, $i, j \in \mathbb{N}$. These can respectively be used to describe the state of a system and its evolution. In order to compute physical properties of a system, and calculate their evolution in time, we shall need to multiply tensors together, which effectively translates into contracting their relevant indices. This is a task whose hardness increases with the tensor dimension.

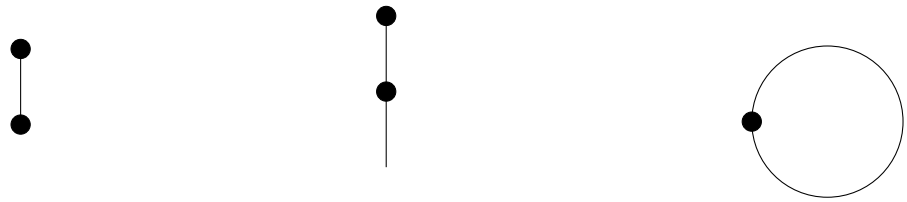
Tensors can be represented schematically, as illustrated in Fig. 1.1, where a dot represents the label of the tensor and each line corresponds to an index. For example, a scalar is a zero dimensional tensor, that is, a dot with no outgoing lines. In addition, operations between tensors can also be also diagrammatically represented, as shown in Fig. 1.2. These illustrate the way in which indices are contracted, and show the way in which tensors can be combined. The output of the calculation is thus determined by the new object formed, and its dimension by the number of emerging lines.

Tensor network states—such as Matrix Product States (MPS) [25] for one-dimensional objects or Projected Entangled Pair States (PEPS) and Multi-Scale Entanglement Renormalization Ansatz (MERA) in two-dimensions—refer to classes of quantum states which can be described using a tensor network. The dimension of the tensor network will depend on the complexity of the state, as for instance determined by the locality of its interactions or its entanglement.



(a) A vector v_i. (b) A matrix M_{ij}. (c) A tensor with three indices.

Figure 1.1: *Tensor networks.* Tensors of dimensions one, two and three are diagrammatically represented.



(a) The inner product between two vectors results in a scalar.

(b) The product between a matrix and vector yields a new vector.

(c) The trace of a matrix.

Figure 1.2: *Tensor network index contraction.*Operations on tensors result in the contraction of relevant indices.

Crucially, it has been shown that tensor network states offer good approximations to ground states of certain common physical Hamiltonians, as illustrated by the success of Density Matrix Renormalization Group (DMRG) numerical methods, which is a variational algorithm over MPS [26, 27]. Interestingly, any statement as to the structure of the ground state immediately tells us something about its parent Hamiltonian. This in turn allows us to connect features of Hamiltonians, such as an energy gap between the ground and excited state, with the decay rates of physical correlations.

In the following, we shall bring our attention to the MPS formalism, where the complex coefficients present in the state description will be expressed as a product of a polynomial number of matrices. The size of these matrices is determined by a parameter called the bond size or Schmidt rank, a quantity connected to the amount of bipartite entanglement present in the system. Vidal [28] showed that, when the size of these matrices is bounded, MPS states can be used to classically efficiently simulate slightly entangled quantum computation. In addition, these will be of particular use to us when studying Measurement-Based Quantum Computing (MBQC). We shall next introduce the Schmidt decomposition as it is at the heart of the representation.

The Schmidt Decomposition

How can the strength of the correlations present in a system be quantified? There exists a variety of different measures of entanglement [29]. First, we shall restrict ourselves to the simple case of bipartite entanglement. Here, the system of interest is partitioned into two, and the correlations between the two subsystems are considered. Formally, we consider a pure state $|\psi\rangle \in \mathcal{H}$, and partition the Hilbert space into two subspaces $\mathcal{H}_a$ and $\mathcal{H}_b$, each of respective dimension d_a and d_b, such that $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$. The Schmidt decomposition, stemming from the Singular Value Decomposition of linear algebra, tells us that there exists an orthonormal set of eigenvectors $\{|v_j\rangle\} \in \mathcal{H}_a$ and $\{|w_k\rangle\} \in \mathcal{H}_b$ such that we may write:

$$|\psi\rangle = \sum_{i=1}^{\chi} \lambda_i |v_i\rangle \otimes |w_i\rangle. \tag{1.3}$$

The scalars $\lambda_i \in \mathbb{R}^+$ are the positive, real Schmidt coefficients, which satisfy the two following conditions: $\lambda_i \geq 0$ and $\sum_i \lambda_i^2 = 1$. The Schmidt rank χ, where $1 \leq \chi \leq \min(d_a d_b)$, can thus be interpreted as a measure of the amount of bipartite entanglement present in the system. For example, in the case of a product state we have that $\chi = 1$.

If we discard—that is, trace out—the second system on $\mathcal{H}_b$, then we are left with the reduced state on the first subsystem $\mathcal{H}_a$, denoted here by $\rho_{\mathcal{A}} = \mathrm{Tr}_{\mathcal{B}}(|\psi\rangle\langle\psi|)$. It can easily be shown that its eigenvectors and eigenvalues are respectively given by the square of the Schmidt coefficients λ_i^2 and the Schmidt eigenvectors $|v_i\rangle$.

MPS from Schmidt Decomposition

We shall now reproduce the derivation of the formalism of MPS based on the Schmidt decomposition, as introduced by Vidal. The idea relies on performing successive partitions across a one-dimensional system, each time re-expressing the local description of the qubit in terms of the Schmidt basis. A one-dimensional system, shown in Fig. 1.3 consisting of n qubits placed on a

Figure 1.3: *One-dimensional system on a line.* A system of 7 qubits on a one-dimensional lattice.

line is generically described by its state vector:

$$|\psi\rangle = \sum_{i_1,\ldots,i_n} c_{i_1\ldots i_n} |i_1 \ldots i_n\rangle. \tag{1.4}$$

Each qubit is labelled from 1 to n, starting from the left, and we then perform a partition between the furthermost left qubit and the $n-1$ others, thus splitting the Hilbert space $\mathcal{H}$ into two subspaces $\mathcal{H}^{[1]}$ and $\mathcal{H}^{[2\ldots n]}$, where $\mathcal{H} = \mathcal{H}^{[1]} \otimes \mathcal{H}^{[2\ldots n]}$. A Schmidt decomposition is then performed across this partition:

$$|\psi\rangle = \sum_{\alpha_1}^{\chi_1} \lambda_{\alpha_1}^{[1]} |\Phi_{\alpha_1}^{[1]}\rangle \otimes |\Phi_{\alpha_1}^{[2\ldots n]}\rangle, \tag{1.5}$$

where $\lambda^{[1]}$ is a vector of dimension χ_1, containing the Schmidt coefficients. Next, the Schmidt eigenvectors are expanded in the computational basis: $|\Phi_{\alpha_1}^{[1]}\rangle = \sum_{i_1} \Gamma_{\alpha_1}^{[1]i_1} |i_1\rangle$, where $\Gamma_{\alpha_1}^{[1]}$, a tensor with two indices, may be viewed as the matrix of basis transformation. The state may thus be expressed as:

$$|\psi\rangle = \sum_{\alpha_1, i_1} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} |i_1\rangle \otimes |\Phi_{\alpha_1}^{[2\ldots n]}\rangle. \tag{1.6}$$

Next, we consider the space $\mathcal{H}^{[2\ldots n]}$, which we once again partition between the utmost left qubit and the $n-2$ remaining others: $\mathcal{H}^{[2\ldots n]} = \mathcal{H}^{[2]} \otimes \mathcal{H}^{[3\ldots n]}$. The first qubit is expressed in the computational basis, with an arbitrary state on the second subsystem: $|\Phi_{\alpha_1}^{[2\ldots n]}\rangle = \sum_{i_2} |i_2\rangle \otimes |\tau_{\alpha_1 i_2}^{[3\ldots n]}\rangle$. By considering the reduced density matrix on $\mathcal{H}^{[3\ldots n]}$, we may compute its eigenvectors $|\Phi_{\alpha_2}^{[3\ldots n]}\rangle$ and associated eigenvalues $\lambda^{[2]}$, and thus express the arbitrary state in this orthonormal basis: $|\tau_{\alpha_1 i_2}^{[3\ldots n]}\rangle = \sum_{\alpha_2} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} |\Phi_{\alpha_2}^{[3\ldots n]}\rangle$. The full state on n qubits may thus now be written:

$$|\psi\rangle = \sum_{i_1,\alpha_1,i_2,\alpha_2} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} |i_1 i_2\rangle |\Phi_{\alpha_2}^{[3\ldots n]}\rangle. \tag{1.7}$$

By repeating this process over successive partitions, the full state on n qubits is finally expressed as:

$$|\psi\rangle = \sum_{i_1,\alpha_1,\ldots i_n,\alpha_n} \Gamma_{\alpha_1}^{[1]i_1} \lambda_{\alpha_1}^{[1]} \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]} \ldots \Gamma_{\alpha_{n-1}\alpha_n}^{[n-1]} \lambda_{\alpha_n}^{[n-1]} \Gamma_{\alpha_n}^{[n]i_n} |i_1, \ldots, i_n\rangle. \tag{1.8}$$

The Schmidt coefficients λ_{α_k} may be absorbed in the tensors by defining $\tilde{\Gamma}_{\alpha_1}^{[1]i_1} = \lambda_{\alpha_1}^{[1]} \Gamma_{\alpha_1}^{[1]i_1}$, $\tilde{\Gamma}_{\alpha_n}^{[n]i_n} = \lambda_{\alpha_n}^{[n]} \Gamma_{\alpha_n}^{[n]i_n}$ and $\tilde{\Gamma}_{\alpha_1\alpha_2}^{[2]i_2} = \Gamma_{\alpha_1\alpha_2}^{[2]i_2} \lambda_{\alpha_2}^{[2]}$, which we then reorder:

$$|\psi\rangle = \sum_{\alpha_1, i_1 \ldots \alpha_n, i_n} \tilde{\Gamma}_{\alpha_n}^{[n]i_n} \tilde{\Gamma}_{\alpha_n\alpha_{n-1}}^{[n-1]i_{n-1}} \ldots \tilde{\Gamma}_{\alpha_1}^{[1]i_1} |i_1 \ldots i_n\rangle. \tag{1.9}$$

The indices α determine the dimension of the tensors: at each extremity the single index tensor corresponds to a vector and the $n-2$ others to matrices. By contracting the indices, we can write:

$$|\psi\rangle = \sum_{i_1 \ldots i_n} \tilde{\Gamma}^{[n]i_n} \tilde{\Gamma}^{[n-1]i_{n-1}} \ldots \tilde{\Gamma}^{[1]i_1} |i_1 \ldots i_n\rangle. \tag{1.10}$$

We thus now have an expression for the state of the n qubits, where each complex coefficient is given by the multiplication of n matrices. Each tensor depends not only a state i_k but also on the

lattice site k at which it acts, with $k = 1, \ldots, n$.

MPS from Projection

An alternative derivation of the MPS formalism can be obtained [25], where we now consider a system of n d-dimensional qudits placed on a ring-like structure and subject to nearest neighbour interactions and cyclic boundary conditions.

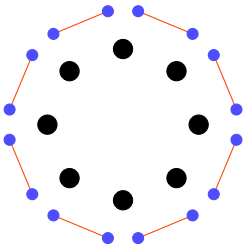


Figure 1.4: *One-dimensional system on a ring.* The black dots represent the real (physical) qubits, whereas the blue dots represent the two virtual qubits assigned to each qubit. The red line represents the maximally entangled bond between pairs of virtual qubits of adjacent real qubits.

Two virtual qudits of dimension D are then assigned to each real—or physical—qudit, with this dimension depending on the amount of entanglement present in the system. A maximally entangled bond is created between neighbouring virtual qudits of adjacent sites, resulting in the maximally entangled state:

$$|v\rangle = \sum_{\alpha=0}^{D-1} \frac{1}{\sqrt{D}} |\alpha, \alpha\rangle. \tag{1.11}$$

Next, the operator A is defined as a mapping from the two virtual qudits onto the real qubit:

$$A = \sum_{i=1}^{d} \sum_{\alpha,\beta=0}^{D-1} A_{i,\alpha,\beta} |i\rangle\langle\alpha, \beta|, \tag{1.12}$$

where $A_{i,\alpha,\beta}$ are complex coefficients. We can define the D-dimensional matrix acting at site k as $A_i^{[k]}$, and in the case where these are assumed to be site independent, an assumption known as translational invariance, the state of the n qubits on the ring can be expressed as:

$$|\psi\rangle = \sum_{i_1 \ldots i_N} \mathrm{Tr}(A[i_1]A[i_2] \ldots A[i_N]) |i_1, \ldots i_N\rangle. \tag{1.13}$$

If one of the bonds is broken, then this is equivalent to considering qubits placed on a line. The boundary conditions are no longer cyclic, and new suitable boundary conditions must be chosen,

which can be encoded as states $|L\rangle$ and $|R\rangle$, thus yielding the expression:

$$|\psi\rangle = \sum_{i_1 \ldots i_N} \langle R|A[i_N]A[i_{N-1}] \ldots A[i_1]|L\rangle |i_1, \ldots, i_N\rangle. \tag{1.14}$$

Further Insights

This procedure can be implemented for all states provided the dimension of the virtual qubits is large enough. Indeed, in the case of a highly entangled quantum state, the dimension of the auxiliary qubits will be required to also be high. This in turn means that the dimension of the matrices will be greater. In the case where these are of size poly(n), where n is the number of qubits, then the representation is said to be efficient.

Thus, the correlations present are mediated through the auxiliary space of dimension D. More generally, the pivotal role of quantum correlations has generated an approach for the study of quantum systems. In particular, the question as to whether entanglement grows as the volume or the boundary between two systems has motivated the study of Area Laws [30, 31], and leads us to question how information is propagated from one part of the system to another, as studied by Lieb-Robinson Bounds [32, 33].

1.2.3 Mixed States

We shall now shift our attention from the state of the whole—an isolated and thus uncorrelated system—to that of its parts. Indeed, systems typically interact with both the environment as well as other systems, and we can thus no longer model the system of interest as being isolated. In particular, the information pertaining to these interactions is described in terms of correlations: to understand the world we must not merely look at objects but also at the relations between these. More formally, we will consider the joint pure state of a system and its environment $\mathcal{H}_{syst} \otimes \mathcal{H}_{env}$. If we choose to focus solely on the state of the system, that is, to trace over the environment, information contained within the system-environment correlations will be lost, and this in turn will induce a certain classical uncertainty in our description.

When our state of knowledge is imperfect, that is if classical uncertainty is present, then we effectively believe the state of the system to be $|\psi_i\rangle$, with probability p_i, where $1 \leq i \leq k$, $p_i \geq 0$ and $\sum_i^k p_i = 1$, in order for probability to be conserved. The state is thus given by an ensemble description $\{p_i, |\psi_i\rangle\}$, which may be expressed as a convex combination:

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i|, \tag{1.15}$$

where ρ, the density operator, is a positive matrix of unit trace, that is $\rho \geq 0$ and $\mathrm{Tr}(\rho) = \sum_i p_i = 1$.

In the special case when the uncertainty is maximal, the state of knowledge is modelled by a uniform distribution. This results in the maximally mixed state on n qubits $\rho = \frac{1}{2^n}\mathbb{1}_n$, where $\mathbb{1}_n$ corresponds to the identity matrix for a space of dimension 2^n. For example, this would be the case if half of a Bell state were to be traced over.

For mixed states, the task of determining the properties of the system is more difficult than for pure states. For example, the notion of product state is no longer meaningful, and is thus replaced with that of a separable state [34], where a state is said to be separable if it can be expressed as:

$$\rho = \sum_i \lambda_i \rho_i^{[A]} \otimes \rho_i^{[B]}, \tag{1.16}$$

where the Hilbert space has been partitioned as $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and where $\sum_i \lambda_i = 1$. Next, we consider quantum evolution, in the case of both pure and mixed states.

1.2.4 Quantum State Evolution

We have until now considered the question as to how quantum systems can be modelled. But, systems rarely, if ever, remain static, instead evolving subject to forces and interactions with their environment, are modelled by the Hamiltonian operator.

Pure State Evolution

The evolution of a pure state $|\psi\rangle$ to a new pure state $|\psi'\rangle$ is characterised by a norm-preserving unitary operator U such that $UU^\dagger = U^\dagger U = \mathbb{1}$. The evolution of the system is given by the continuous Schrödinger equation:

$$i\hbar \frac{\partial \psi}{\partial t} = \hat{H}\psi. \tag{1.17}$$

Mixed State Evolution

More generally, the evolution of a quantum system from a mixed state ρ to ρ', is modelled by the superoperator ε. This is a mapping on the space of linear operators $\mathcal{L}(\mathcal{H})$ which implements $\rho' = \varepsilon(\rho)$. For this operation to have any physical meaning, that is, to output a valid quantum state we must demand it to satisfy certain properties. First, we require $\mathrm{Tr}(\rho') = 1$, which means that the map should preserve the trace. Secondly, the eigenvalues of the new state should be positive.

Interestingly, only requiring the mapping to be both trace-preserving and positive proves to be too weak a constraint. Indeed, for certain states, adjoining an ancillary system left untouched by the map can create a negative state, as seen with the partial transpose [35]. Instead, completely positivity is instead required, that is for $I_p \otimes \varepsilon : M_p \otimes M_n \to M_p \otimes M_m$ to be positive, or in other words $I_p \otimes \varepsilon$ to be positive for all p.

We have thus defined a CPTP map which is a convex map acting on the space of linear operators $\mathcal{L}(\mathcal{H})$. Such a map may be expressed in three different yet equivalent formalisms: the Kraus [36], Choi [37] and Stinespring [38] representations. The Kraus decomposition—also known as the operator-sum decomposition—is given by:

$$\varepsilon(\rho) = \sum_{j=1}^{|\tau|} K_j \rho K_j^\dagger, \tag{1.18}$$

where $\sum_{j=1} K_j^\dagger K_j = \mathbb{1}$ and $|\tau|$ denotes the number of terms in the sum. Note that when the summation is over a single term, this corresponds to unitary evolution. The Choi matrix provides an alternative representation:

$$C_\varepsilon = \sum_{i,j} |i\rangle\langle j| \otimes \varepsilon(|i\rangle\langle j|), \tag{1.19}$$

where the effect of the map on each basis element $|i\rangle\langle j|$ is calculated and stored within the Choi matrix, of rank $|\tau|$, fully determining the quantum operation.

Finally, we can add an ancillary state $|0\rangle^{\dim \mathcal{K}}$ from a Hilbert space $\mathcal{K}$ and perform a unitary operation on the joint system, before tracing over the system $\mathcal{K}$. This is known as the Stinespring representation and is expressed:

$$\varepsilon(\rho) = \mathrm{Tr}_{\mathcal{K}} U(\rho \otimes |0\rangle\langle 0|)U^\dagger, \tag{1.20}$$

where $\mathcal{K}$ denotes an ancillary Hilbert space of dimension $|\tau|$ and U is a unitary operator acting on the joint space $\mathcal{H} \otimes \mathcal{K}$. Thus, having studied both the representation of quantum states and their evolution, we finally consider the crucial link between classical and quantum worlds: measurement.

1.2.5 Measurement

Until now, our discussion has focused on introducing a theoretical model of systems at the atomic scale. We have seen that these no longer behave according to the laws of classical physics, and that a different model of reality is required. Ultimately though, we, as humans are macroscopic classical objects, and the observations we record are classical data. How does information pertaining to a quantum system get transformed into classical data? This transition is mediated via the process of measurement, whereby a classical observer—the experimentalist—interacts with a quantum system. The observer has a choice of measurement, and each measurement can probabilistically yield one of many outcomes.

First, we introduce projective measurements and observables, followed by their generalisation to Positive Operator-Valued Measurements (POVMs). Finally, we shall briefly discuss how the analysis of experimental data can yield insight into the question of locality via Bell's theorem.

Projective Measurements

Given a quantum state $|\psi\rangle$, we can measure the observable M, given by its spectral decomposition $M = \sum_k \lambda_k |v_k\rangle\langle v_k|$. This corresponds to the state $|\psi\rangle$ being projected onto one of the orthonormal subspaces P_k spanned by one of the eigenvectors $|v_k\rangle$. The outcome of the measurement will be one of the eigenvalues λ_k, which will occur with probability $p_k = |\langle v_k|\psi\rangle|^2$. When the outcome m is obtained, the state evolves to:

$$|\psi_m\rangle = \frac{P_m|\psi\rangle}{\sqrt{p_m}}. \tag{1.21}$$

We can interpret this result as the state $|\psi\rangle$ probabilistically evolving to state $|\psi_m\rangle$ via the measurement process. This is a process of different nature to the previously introduced unitary dynamics, where the outcome probabilities contain a priori information pertaining to the pre-measurement state $|\psi\rangle$.

Observables

The set of eigenvectors $|v_k\rangle$ and associated eigenvalues λ_k fully specify the observable M to be measured. A natural extension is to consider the new observable $UMU^\dagger$, which corresponds to the set of eigenvalues λ_k and eigenvectors $\{U|v_k\rangle\}$, where U is a unitary operator. The probability of obtaining a given outcome k has now been changed to $p'_k = |\langle v_m|U^\dagger|\psi\rangle|^2$. A mathematically equivalent yet physically distinct view of this would be to first apply the operator $U^\dagger$ to the state $|\psi\rangle$ and only then performing a measurement of the observable M.

POVMs

A generalisation of the projective measurements previously introduced are Positive Operator Valued Measurements (POVM). These are specified by a set of positive operators E_m which sum to the identity, that is $E_k \geq 0$ and $\sum_k E_k = \mathbb{1}$. Once the POVM has been applied and the outcome m has been obtained, the quantum state will have evolved to a new state ρ'_m with probability p_m given by:

$$p_m = \mathrm{Tr}(E_m \rho E_m^\dagger). \tag{1.22}$$

In the case when the POVM elements are orthogonal, that is $E_m E_n = \delta_{nm} E_m$, we then recover projective measurements.

An alternative characterization is given by Naimark's theorem. Here, an ancillary system is coupled to the system of interest. They both then undergo unitary evolution, before a joint projective measurement is performed, and finally, the ancillary system is traced out. It can be shown that this is equivalent to implementing a POVM directly onto the system of interest.

Quantum Signatures

Questions as to the nature of the quantum states remain, to this day, unanswered. From a practical standpoint, we prepare quantum states, measure them and, by repeating these procedures, collect data. These in turn can be used in order to test our model of the underlying physical process.

From this operational perspective, Bell investigated correlations present in a composite quantum system [39]. The model he sought to test was whether quantum theory could allow for a local hidden variable model. Bell's theorem showed that the statistics obtained crossed out the possibility of a local hidden variable, a phenomenon known as non-locality [40]. Similarly, contextuality tells us that the measurement outcomes we obtain are dependent on other measurements performed alongside it. This means that variables do not have prefixed values, which are simply revealed by a measurement. Thus, the relation between entanglement, non-locality and contextuality is a rich field of current research.

This thus concludes the introduction to quantum states, evolution and measurements. We now have the necessary tools in order to approach the question of whether quantum systems can be utilised in order to perform computation.

1.3 Quantum Computing

Computation is the process whereby an input x is transformed into an output y. By encoding the information within a physical system and by evolving it via a finite sequence of operations, the desired output state may be obtained, thus yielding the solution to the problem we wish to solve.

Is there a connection between the nature of the system embedding the computation, and the nature of the computation itself? The answer would seem to be *yes*, for the many features and properties of quantum mechanics—such as its exponential workspace—can be exploited in order to perform a more powerful computation [15].

But what is the origin of this quantum speed-up? What features of quantum mechanics can be exploited by an algorithm in order to outperform its classical counterpart? These are but some of the many questions which lie at the heart of research into quantum computing. For example, by studying the role of correlations in computation it has been shown that a necessary component of any quantum speed-up is multipartite entanglement scaling with the system size [41, 42].

In order to build a quantum computer, we need a theoretical model of computation—a framework—which will allow us to model and understand the interplay between the physical system and the encoded information. The circuit model of quantum computation [43, 44] is the standard framework within which quantum computing and quantum algorithms has been studied [45]. Its premise is the transformation of a "simple" quantum state—in the sense that it may either be classically efficiently

described or experimentally prepared in a laboratory—to a more complex quantum state via the application of a unitary operator. The output of the computation is determined by a computational basis measurement on a set of qubits. Thus, we are ultimately constrained to accessing a classical multi-bit string, sampled from the associated probability distribution. This highlights the following crucial limitation of quantum computing: although the information processing is quantum in nature, we, as classical entities, can only ever access classical information obtained via measurement.

Could an alternative model of computation yield new insight into these questions? Measurement Based Quantum Computing (MBQC) [46–51] is an alternative computational scheme, which, although equivalent in power to the circuit model, offers new insight by highlighting the role of quantum correlations and measurement. Alternatively, by placing restrictions on the available resources, alternative models of computation [52–54] can be obtained and their power analysed. This approach allows the connection between physical systems and computational power to be probed, thus fine tuning our understanding of non-classicality.

Thus, the benefits of quantum computing are two-fold. First, the study of computational power as a function of available resources allows for the structure of the underpinning physical system to be studied and probed. Secondly, the increase in computational power offers us the possibility of developing new technologies, with potential application to a broad spectrum of disciplines. Thus, over the past decade, quantum computing has emerged as a rich field of direct relevance to both fundamental and technological questions [55].

1.3.1 The Quantum Circuit Model

The quantum circuit is the model of quantum computation most commonly used in the study of quantum computing and quantum algorithms. In the following, we shall introduce the framework, by considering the quantum circuit model as the analogue of the classical circuit model. We shall then discuss some of the key results illustrating the novel nature of computation at play, such as in the one-bit teleportation protocol.

The Classical Circuit Model

The quantum circuit model can be viewed as the quantum analogue of the classical circuit model. Classically, a circuit takes as input a finite n-bit string x and outputs a finite m-bit string y, each encoding information represented in binary form. The circuit thus implements a Boolean function $f : \{0,1\}^n \to \{0,1\}^m$, where $y = f(x)$. There exists countably many such functions. For instance, in the case where the output is a single bit, there exists 2^{2^n} such functions, and thus an exponential number of corresponding circuits.

Each of these circuits will be built by using a finite number of gates chosen from a finite gate

set. For example, the AND, OR and NOT gates form a universal gate set for classical computation, that is, any circuit can be built from these. Finally, one notes that an important feature of classical computing is that information can be copied by using a FANOUT gate.

Qubits

In quantum computing, information is encoded in a qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, where $\alpha_i \in \mathbb{C}, i = 0, 1$ and $\sum_i |\alpha_i|^2 = 1$. This is the quantum analogue of a classical bit, and can be geometrically represented in the Bloch sphere picture, as illustrated in Figure 1.5. Here, the quantum state is represented by a three dimensional state vector, where the orthonormal axes correspond to the eigenvectors of the Pauli operators:

$$X = \sigma_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \sigma_{10} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad iY = ZX = \sigma_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

and where we introduce the following notation for the identity operator:

$$I = \sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.23}$$

Of particular subsequent interest will be states lying within the equatorial plane of the Bloch sphere, which are given by:

$$|s_k\rangle = \frac{|0\rangle + (-1)^k e^{i\phi}|1\rangle}{\sqrt{2}}, \tag{1.24}$$

and which form an orthonormal pair of states, with $k \in \{0, 1\}$.

Quantum Gates

In contrast with classical computation, unitary evolution is a reversible process, requiring the input and output to be of the same size. Thus an n-qubit quantum state will evolve to a new n-qubit quantum state via a continuous evolution. For example, in the case of a single qubit, the evolution corresponds to a rotation by an angle θ around an axis $\vec{n} = (n_x, n_y, n_z)$ in the Bloch sphere:

$$R_{\vec{n}}(\theta) = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}} = \cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}, \tag{1.25}$$

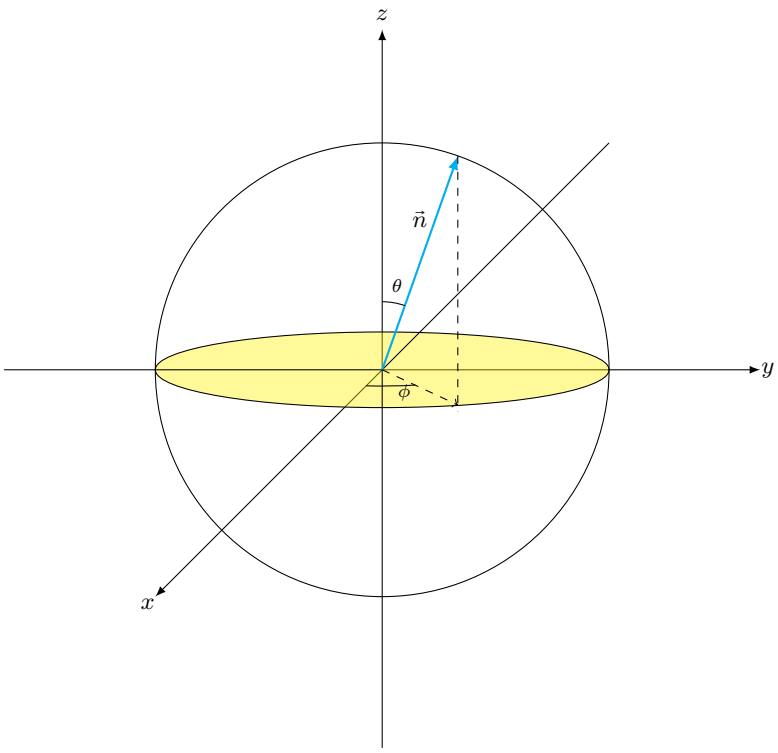


Figure 1.5: *Bloch sphere.* The Bloch sphere, where the equatorial plane has been highlighted in yellow, provides a geometric representation of a single qubit.

where $\vec{\sigma}$ is a vector of Pauli operators (X, Y, Z). For example, a rotation around the Z axis by an angle ϕ can be expressed as:

$$R_{\vec{z}}(\phi) = \begin{pmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{i\frac{\phi}{2}} \end{pmatrix}, \tag{1.26}$$

which, up to a global phase corresponds to the Pauli phase gate:

$$S_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \tag{1.27}$$

and in the case where $\phi = \pi/2$ we obtain:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{1.28}$$

Thus, for example, states in the equatorial plane can be obtained by first applying a Hadamard gate to a computational basis state, followed by a rotation around the Z axis by an angle ϕ, that is, $|s_k\rangle = R_z(\phi)H|k\rangle$. In the case when $\phi = 0$, we recuperate the eigenstates of X, and when $\phi = \pi/2$, the eigenstates of Y.

Unitary Evolution

Thus, when evolution is unitary, there exists a continuum of possible transformations. In contrast, a realistic model of computation is implemented by the application of gates picked from a finite gate set, $\mathcal{G}$. That is, a countable number of quantum circuits may be implemented, and thus arbitrary unitary evolution can only ever be approximated. Formally, a quantum gate set $\mathcal{G}$ is said to be universal [56] if for any arbitrary n-qubit gate U, we have that:

$$\forall \varepsilon > 0, \quad \|U - U_{g_1} \dots U_{g_L}\| \leq \varepsilon, \tag{1.29}$$

where U_{g_i} denotes the gate g_i acting on $k \leq n$ qubits, with identity on the $(n-k)$ remaining qubits. Thus, $U_{g_1} \dots U_{g_L}$ corresponds to the unitary evolution which, in practice, we aim to implement, and, as such, has been the subject of extensively study [44, 57–62].

The Solovay-Kitaev Theorem (and algorithm) [63] provides the guarantee that $L = O(\log^2 \frac{1}{\varepsilon})$, and that thus by using a polynomial number of gates $L = O(\text{poly}(N))$, any arbitrary evolution may be approximated with exponential accuracy $\varepsilon = \frac{1}{2^N}$.

For example, the Toffoli gate, which maps the state $|a, b, c\rangle$ to $|a, b, c \oplus ab\rangle$, taken with the Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1.30}$$

form one such universal gate set. Another such example is the set consisting of the controlled-Z entangling operator:

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \tag{1.31}$$

taken with the Hadamard gate H and single qubit rotations $R_z(\theta)$ around the Z axis of the Bloch sphere, that is, we have $\mathcal{G} = \{CZ, H, R_z(\theta)\}$.

The Circuit Model

The quantum circuit model was the first model of quantum computation developed, mirroring classical circuits with bits replaced by qubits and logic gates by unitary gates. The computation takes as input an n-bit string x, and is given access to a polynomial number of qubits initialised in the $|0\rangle$ state to which a poly(n)-qubit unitary operator U_x is applied. Then, a set of N qubits are finally measured in the computational basis, yielding an N-bit output string y. The output of the compu-

tation is thus an N =poly(n) classical bit string y, a single sample over an exponential 2^N possible outcomes, each of which occurs with probability P$[Y = y]$.

For example, the simple circuit depicted in Fig. 1.6 prepares a a maximally entangled two-qubit state—a Bell state—as an output. There are four such Bell states $|B_{ij}\rangle$ which form an orthonormal basis for a Hilbert space of dimension two, where: $|B_{ij}\rangle = (\mathbb{1} \otimes X^i Z^j)|B_{00}\rangle$ or alternatively $|B_{ij}\rangle = (Z^j X^i \otimes \mathbb{1})|B_{00}\rangle$ for $i, j \in \{0, 1\}$ and where $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

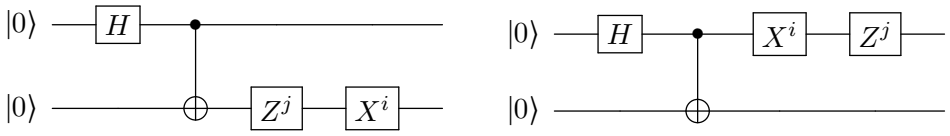


Figure 1.6: *Circuit for Bell state preparation.* Both of these circuits equivalently result in an entangled Bell state $|B_{ij}\rangle$ being prepared.

Unitary Operators in the Pauli Basis

The set of linear operators $\mathcal{L}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ forms a vector space, with an inner product defined by $\langle A, B\rangle$ = tr$(A^\dagger B)$, where $A, B \in \mathcal{L}(\mathcal{H})$. Any single qubit unitary operator can be decomposed in the Pauli basis as:

$$U = \sum_{j,k} u_{jk}\sigma_{jk}, \tag{1.32}$$

where u_{jk} = Tr$(U\sigma_{jk})$.

We can define the Pauli group $\mathcal{P}_1$ on a single qubit as:

$$\mathcal{P}_1 = \{\pm i^k \sigma_{mn} | m, n, k = 0, 1\}, \tag{1.33}$$

where the coefficients ± 1 and $\pm i$ ensure group closure. This forms a non-abelian group for the multiplication operation, and consists of the common Pauli operators, up to a phase factor. The Pauli group is a subgroup of the Clifford group $\mathcal{C}_1$, which consists of the set of operators which transform an element of the Pauli group to an element of the Pauli group under conjugation:

$$\mathcal{C}_1 = \{U | U\sigma_{jk}U^\dagger = \sigma_{j'k'}\}. \tag{1.34}$$

For instance, the Hadamard gate H is an element of the Clifford group as $HXH = Z$ and $HZH = X$, as well as Pauli operators themselves (e.g. $XZX = -X$).

More generally, the n-qubits Pauli group $\mathcal{P}_n$ is the n-fold tensor products of $\mathcal{P}_1$, which forms a

basis for n-qubit operators. For example, a generalised n-qubit rotation around the Z axis is given by:

$$U_z = \prod_{\vec{m}\in\mathbb{F}_2^n} e^{i\frac{\theta_{\vec{m}}}{2}Z[\vec{m}]}, \tag{1.35}$$

where $\vec{m} = (m_1, \ldots, m_n)$ denotes an n-bit string and $\sigma[\vec{k}] = \sigma_1^{k_1} \otimes \ldots \otimes \sigma_n^{k_n}$. There exists 2^n terms in the product (including $\vec{m} = (0, \ldots, 0)$ the null vector which simply adds a global phase to the state).

Algorithms

Over the past two decades, various quantum algorithms exhibiting a speed-up over their classical counterpart have been developed. These have covered a wide variety of problems, from questions in number theory with applications to cryptography to useful optimisation problems. Complete reviews of these algorithms exist and the reader is referred to these for more a complete discussion [64–68].

Here, we note that typically, the idea is to first build a classical circuit implementing a function f, which is called the oracle box. Next, two registers are prepared: the first containing n qubits initialised in the $|0\rangle^{\otimes n}$ state and the second containing a single qubit $|0\rangle$. Then, n Hadamard gates are applied to the first register, which will yield an equal superposition over all n qubit computational basis states $\frac{1}{2^{\frac{n}{2}}}\sum_{i_i\ldots i_n}|i_1\ldots i_n\rangle|0\rangle$. Now, the oracle box function is called and applied to the first register, with its output stored in the second register:

$$\frac{1}{2^{\frac{n}{2}}}\sum_{i_i\ldots i_n}|i_1\ldots i_n\rangle|f(i_1\ldots i_n)\rangle. \tag{1.36}$$

It would thus seem that in a single time step we have computed the outputs of a function on an exponential numbers of inputs. Of course, the catch is that a measurement will have to be performed on the output state, thus destroying the superposition. In other words, as classical entities, we are restricted with regards to the information we may access.

Nonetheless, various powerful algorithms have been devised, such as Shor's algorithm which achieves an exponential speed-up by using the Quantum Fourier Transform to solve prime factorisation, or the Deutsch-Jozsa Algorithm [69] which answers in a single query the question of determining whether a function is constant or balanced given the promise that one of these is true.

Another example of quantum algorithm is Grover's Search, which performs database queries with a quadratic speed-up. Here, we have a list of N objects, which shall each be labelled by an n bit string, that is $N = 2^n$ indexed items. We next pick an item $x \in \{0, \ldots, N-1\}$ and ask whether is is a marked item. In the case where there are M marked items, the algorithm runs in time $\mathcal{O}(\sqrt{\frac{N}{M}})$. More recently, a quantum algorithm considering systems of linear equations was devised

[70], which sparked the nascent field of quantum machine learning. Thus, quantum algorithms have been developed for a wide breadth of applications, with the feature of a polynomial or exponential speed-up. We shall next consider certain elements of quantum computation which are significantly different to classical computation.

Quantum Teleportation

Quantum teleportation allows for an arbitrary, unknown, quantum state to be teleported from one system to another. In this process, the information is not being merely copied—impossible from the No Cloning Theorem [71, 72]—but actually transmitted, hence lending it the name of teleportation.

In order to achieve this, we need to have access to a Bell state, which is the quantum resource state shared between the two parties, Alice and Bob. Indeed, the entanglement present can be utilised as a resource in order to create a communication channel, and thus for information to be transmitted.

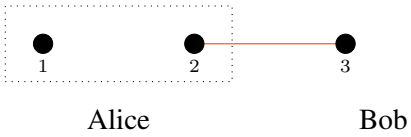


Figure 1.7: *Teleportation.* Alice is in possession of the two leftmost qubits (labelled 1 and 2), on which she shall perform a Bell measurement (illustrated with the dotted box), whilst Bob has the qubit on the right (labelled 3). The qubits 2 and 3 are the entangled resource state, which is a pure Bell state.

Alice and Bob share a pure entangled Bell state $|B_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$. In addition, Alice is in possession of a single qubit in an arbitrary state $|\psi\rangle = \sum_u \alpha_u |u\rangle$. The resulting total system is thus in the joint state $|\psi\rangle \otimes |B_{00}\rangle$, with the first two qubits belonging to Alice, and the last one to Bob, as depicted in Fig. 1.7.

First, as the set of four orthonormal Bell states $|B_{ij}\rangle = (\mathbb{1} \otimes X^i Z^j)|B_{00}\rangle$ for $i, j \in \{0, 1\}$ forms a basis for a Hilbert space of dimension two, we can express any two-qubit computational basis state as:

$$|ij\rangle = \frac{1}{\sqrt{2}} \sum_k (-1)^{ik} (\mathbb{1} \otimes X^{i \oplus j} Z^k)|B_{00}\rangle. \tag{1.37}$$

We now write the joint state of the system on the first two qubits which belong to Alice in the Bell basis, and leave Bob's qubit in the computational basis:

$$\frac{1}{2} \sum_u \sum_k \alpha_u (-1)^{uk} (\mathbb{1} \otimes X^{u+i} Z^k)|B_{00}\rangle \otimes |i\rangle = \frac{1}{2} \sum_u \sum_k \alpha_u (-1)^{uk} |B_{u \oplus i, k}\rangle \otimes |i\rangle. \tag{1.38}$$

Next, the first two qubits are measured in the Bell basis, and let s, t be the outcome of the measurement, with $P_{st} = |B_{st}\rangle\langle B_{st}|$ denote the projector onto the Bell state $|B_{st}\rangle$, with $s, t \in \{0, 1\}$. The system is now in the state $\frac{1}{2}\sum_u \sum_k \alpha_u (-1)^{uk} P_{st}|B_{u\oplus i,k}\rangle \otimes |i\rangle$. As the set of Bell states is orthogonal, a non-zero result occurs only if we have $s = u \oplus i$ and $t = k$. Explicitly if $s = 0$ then $i = u$ and $j = v$, and if $s = 1$ then $i = u \oplus 1$ and $j = v \oplus 1$. These conditions may be succinctly expressed as: $X^s|u\rangle = |i\rangle$ and $X^s|v\rangle = |j\rangle$, which leads to the system being in the state:

$$\frac{1}{4}\sum_{u,v} \alpha_{uv}(-1)^{(u+v)t} P_{st} \otimes X^s|u\rangle\langle v|X^s. \tag{1.39}$$

Finally, this equation can be rearranged and shown to be equivalent to:

$$\frac{1}{4}\sum_{u,v} \alpha_{uv} P_{st} \otimes X^s Z^t|u\rangle\langle v|Z^t X^s = \frac{1}{4} P_{st} \otimes X^s Z^t|\psi\rangle\langle\psi|Z^t X^s. \tag{1.40}$$

Thus, we have that the unknown input state has been transferred from qubit one to qubit three, with the application of potential additional Pauli operators depending on the measurement outcomes s and t. We can thus interpret this protocol as a communication channel transferring information from qubit one to qubit three, with the application of some additional Pauli operators depending on the measurement outcome.

One Bit Teleportation

The one-bit teleportation protocol [73] is a seemingly simple quantum circuit which nonetheless captures key features of quantum systems. Here, we are given an arbitrary single qubit state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ as well as an ancillary qubit initialised in the $|0\rangle$ state. First, a Hadamard gate is applied to the ancilla, which transforms it to the $|+\rangle$ state. Next, the two qubits are entangled via a controlled-Z operator. Finally, a Hadamard is applied to the first qubit which is subsequently measured in the computational basis, as illustrated in Fig. 1.8.

If the measurement outcome is denoted by m, then the state on the second qubit can easily be shown to be $\frac{1}{2}X^m H|\psi\rangle$. Thus, the unknown state $|\psi\rangle$ has been transmitted onto the second qubit, with an additional Hadamard gate and, depending on the random measurement outcome, a potential Pauli X.

This circuit may thus be viewed as applying a quantum channel ε, as shown in Fig.1.9 to the unknown input state:

$$\varepsilon(|\psi\rangle\langle\psi|) = \frac{1}{2}\sum_m X^m H|\psi\rangle\langle\psi|HX^m. \tag{1.41}$$

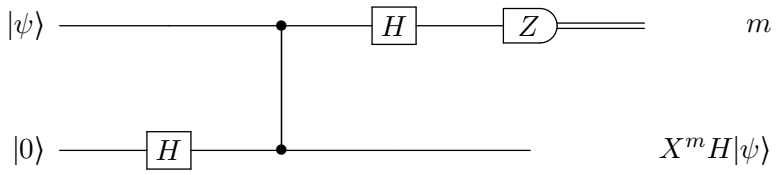


Figure 1.8: *One bit teleportation.* The circuit transfers an unknown state $|\psi\rangle$ from the first to the second qubit, with the additional application of a Hadamard gate and random Pauli operator depending on the measurement outcome m.

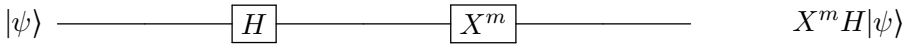


Figure 1.9: *One bit teleportation as a quantum channel.* The circuit implementing the one-bit teleportation protocol can alternatively be represented as a quantum channel acting on the input state.

In the case where the measurement outcome is $m = 0$, we can interpret this process as deterministically implementing a Hadamard gate. This case shall henceforth be known as a Hadamard Gadget, as illustrated in Figure 1.10.

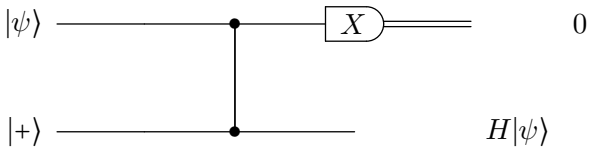


Figure 1.10: *Hadamard gadget.* In the special case when the measurement outcome $m = 0$ occurs, the one bit teleportation protocol results in a Hadamard gate being applied to the arbitrary input state $|\psi\rangle$.

This procedure allows the entanglement present in the circuit to be utilised as a quantum channel in order to transfer information from one part of the system to another. In the next section, we shall consider a universal model of computation whereby measurements and entanglement are directly exploited in order to implement an algorithm.

1.3.2 Measurement Based Quantum Computing

Measurement based quantum computing (MBQC) [46–51] is an alternative quantum computing scheme to the circuit model. Here, the computation exploits the correlations present in an entangled resource state and the nature of measurement in order to implement a given algorithm. In the

following section, we shall review this model as well as some some of its key results.

Connection to One Bit Teleportation

The one bit teleportation protocol yielded the insight that correlations existing in an entangled state can be exploited, and that measurements can implement operators on the unmeasured qubits, with additional by-product operators due to random nature of measurements. These ideas will be encountered again in MBQC, with in addition an efficient scheme for dealing with the random errors.

The scheme proceeds in two steps: first, an entangled universal resource state is prepared. Next, local measurements are performed sequentially, where the choice of qubit and bases—determined by a classical device—depend both on the algorithm to be implemented and the previous measurement outcomes. Thus, the computation is now split into a quantum component and classical post-processing. This hybrid quantum-classical model thus highlights the role played by quantum processes in the computation.

An Alternative Model of Computation

Although MBQC is equivalent to the circuit model in terms of computational power, it nonetheless offers new insights on both theoretical and experimental fronts. Here, the correlations present in a quantum state are explicitly used in order to perform the computation via measurements, and thus allows us to probe the role of entanglement in computation. The quantum algorithm to be implemented determines the choice and order of measurement bases, and is conditioned on previous measurement outcomes (a dependence referred to as adaptive).

As we shall see, a certain amount of computation can be delegated to a classical computer, thus rendering the role of quantum computation in a potential speed up more crystalline. It has indeed been conjectured that any efficient polynomial time quantum algorithm can be implemented with $O(\log n)$ quantum layers interspersed with polynomial time classical computations, as illustrated by Shor's algorithm which contains both quantum and classical components. Finally, one should note that the ability to perform certain measurements synchronously yields a great amount of parallelizability and thus efficiency.

Measurement Bases and Unitary Operators

We previously discussed the one bit teleportation protocol, where an arbitrary state $|\psi\rangle$ is entangled with a $|+\rangle$ state and then measured in the X basis. This results in the state of the first qubit being teleported onto the second qubit, with a Hadamard gate and a potential Pauli operator applied depending on the measurement outcome.

First, it is to be noted that if, in general, the observable $UZU^\dagger$ is measured, then this is effectively equivalent to applying $U^\dagger$ to the state followed by a computational basis measurement. Thus, a measurement of the observable $U_z(\theta)XU_z^\dagger(\theta)$, as shown in Fig. 1.11, effectively applies a rotation around the Z axis by angle $-\theta$ to the state before measurement, since $U_z(\theta)^\dagger = U_z(-\theta)$. As this gate commutes with the controlled-Z operator, one may view this as a teleportation from the first qubit on to the second of the state $U_z^\dagger|\psi\rangle$, as illustrated in Fig. 1.12. Thus, measurements of the observable $U_z(\theta)XU_z^\dagger(\theta)$ allow for the implementation of arbitrary rotations on the input state.

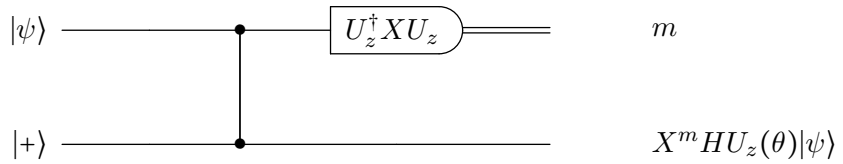


Figure 1.11: *Measurement in the equatorial plane of the Bloch sphere.* By performing a measurement of the observable $U_z^\dagger XU_z$, the operators $HU_z(\theta)$ are applied to the input state, with a potential random Pauli error X depending on the measurement outcome m.

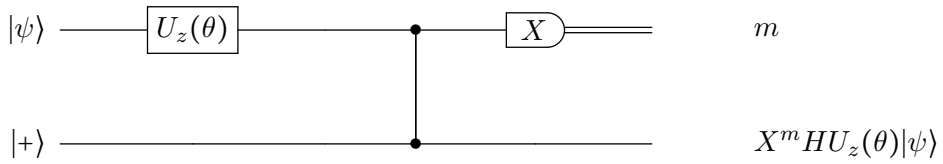


Figure 1.12: *Measurement in the X basis.* An alternative is to apply a Z rotation to the input state, and perform a measurement in the X basis. This procedure will result in the state $X^m HU_z(\theta)|\psi\rangle$ being transmitted.

Previously, in the circuit model, measurements were restricted to project onto computational basis states. Now, in MBQC, such observables corresponds to measurements projecting onto states lying in the equatorial plane of the Bloch sphere:

$$|s(\phi)_k\rangle = \frac{|0\rangle + (-1)^k e^{i\phi}|1\rangle}{\sqrt{2}} = e^{i\frac{\phi}{2}}U_z(\phi)H|k\rangle = e^{i\frac{\phi}{2}}Z^k U_z(\phi)H|0\rangle. \tag{1.42}$$

Euler's decomposition states that any arbitrary rotation can be be decomposed as three consecutive rotations around the two orthogonal axes: $U = U_z(\alpha)U_x(\beta)U_z(\gamma)$, which under Clifford conjugation can be shown to reduce to rotation around a single axis Z interspersed with Hadamard gates : $U = U_z(\alpha)HU_z(\beta)HU_z(\gamma)$. By performing measurements in the equatorial plane and in the X basis, we are thus able to respectively implement arbitrary rotations around the Z axis

and Hadamard gates, up to random by by-product operators and thus achieve universal single qubit rotations.

Finally, we note that a standard measurement of the Z observable destroys the correlations between the measured qubit and its neighbours, potentially adding a phase Z^k to the adjacent qubits depending on the measurement outcome k, $\frac{1}{\sqrt{2}}|k\rangle \otimes Z^k|+\rangle$. Thus, having studied the connection between measurement bases and unitary evolution, we next discuss the general computational scheme for MBQC.

The Scheme

The computation scheme proceeds as follows: first, an entangled state serving as a substrate for the computation is prepared [74, 75]. It generically depends on the algorithm to be implemented: an associated graph is classically generated, according to which the resource state is built by placing qubits initialised in the $|+\rangle$ state at the vertices, and implementing the entangling two qubit controlled-Z operation between connected vertices. A cluster state refers to a special class of graph states, where the underlying graph is a two-dimensional geometric lattice, as illustrated in Fig. 1.13 and in Fig. 1.14 for one-dimensional case.

One may thus alternatively simply generate a cluster state of large enough dimension, and perform additional Z measurements on it in order to obtain the appropriate graph state, as these will simply destroy the entangling bond between the measured qubit and its neighbours. Next, single qubit measurements are performed of the observables Z, X and $U_z(\theta)XU_z(-\theta)$, corresponding to measurements in either the computational basis or in the equatorial plane of the Bloch sphere. The resulting measurement outcomes specify the next qubit to be measured and its bases. We proceed

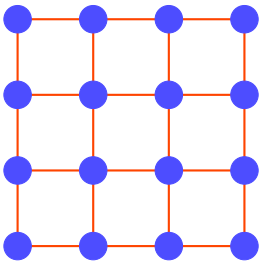


Figure 1.13: *Two-dimensional cluster state.* The blue dots represent qubits initialised in the $|+\rangle$ state placed on a two-dimensional lattice, with in red the entangling bonds acting between adjacent qubits.

in such a fashion until the end of the computation, when the desired sequence of unitary gates will

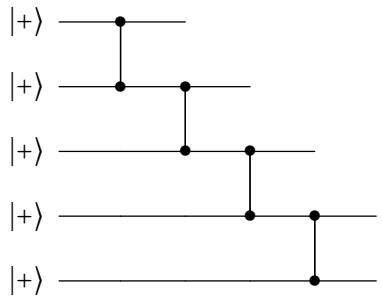


Figure 1.14: *One-dimensional cluster state.* The circuit prepares a one-dimensional cluster state, by applying a controlled-Z gate to pairs of adjacent qubits.

have effectively thus been implemented, up to some additional Pauli operators Z or X occurring due to the randomness of measurement.

At the end of the computation, we are left with an entangled state on the remaining unmeasured qubits, known as the readout state. As the computation has progressed, the correlations in the cluster state have been destroyed, and may no longer be used in order to implement a new algorithm. For this, a new cluster state will have to be prepared and the process will start over. It is this irreversibility of the computation which lends the name of One Way Computation to the paradigm of MBQC.

Correlations

What can be said of the correlations present in the resource state? This question has been studied, and it has been shown that the cluster state is said to be universal as by measuring any subset of its qubits any state may be obtained. In other words, the correlations present are strong enough to serve as reservoir, as opposed to other, one might say weaker, classes of quantum states. For instance, if no Bell inequality violations are observed then only convex combinations of linear functions of input bits can be achieved, as opposed to the more general class of linear computations [76].

By-product Operators

Finally, we must address the issue of the unwanted Pauli operators applied due to the randomness of the measurement outcome. Throughout the computation, random Pauli operators are interspersed throughout the unitary operations implemented via measurement. This is why the measurements are adaptive, and we can thus compensate for the randomness via the choice of measurement bases. In addition, as every single gate we have seen until now belonged to the Clifford group, and we can thus commute the undesired by-product operators to the end of the computation, which are then dealt with as classsical post processing.

MBQC in the MPS Framework

In section 1.2.2, the formalism of Matrix Product States (MPS) was introduced in order to represent one-dimensional quantum states. Crucially, we saw that this description was efficient provided the amount of bipartite entanglement present in the system was bounded.

Furthermore, the formalism of MPS offers an intuitive framework for the study of MBQC schemes on a one-dimensional lattice, highlighting both the role of measurement in the computation and that of the resource state [77–82]. Indeed, in MBQC a unitary operator is implemented by performing a sequence of measurements along of the Pauli observables as well as onto the equatorial plane of the Bloch sphere.

From equation 1.14, a one-dimensional n-qubit cluster state can be represented as an MPS:

$$|\psi\rangle = \sum_{i_1 \ldots i_n} \langle 0|A[i_n]A[i_{n-1}] \ldots A[i_1]|+\rangle |i_1, \ldots, i_n\rangle, \tag{1.43}$$

with logical operators $A[k] = H|k\rangle\langle k|$ and boundary conditions $|L\rangle = |+\rangle$ and $|R\rangle = |0\rangle$. When a qubit is measured in an orthonormal basis $|v_k\rangle$, the logical operator associated to the site in question undergoes the following mapping:

$$A[v_k] = \sum_i \langle v_k|i\rangle A[i]. \tag{1.44}$$

Thus, by sequentially measuring the qubits, starting with the first, logical operators are applied to the boundary condition, and the computation can thus be studied within the correlation space. For example, if the measurement of the first qubit results in the logical operator A_1, and similarly the measurement of the second qubit in A_2, then the updated description of the system is given by:

$$|\psi\rangle = \sum_{i_3 \ldots i_n} \langle R|A[i_N] \ldots A[i_3]|L'\rangle |\psi_1\rangle |\psi_2\rangle |i_3, \ldots, i_N\rangle, \tag{1.45}$$

where the boundary condition has evolved to $|L'\rangle = A_2 A_1 |L\rangle$. Thus, we can say that the measurements induces a virtual computation in the correlation space, as depicted in Fig.1.15. It is important to note that although the logical operators A_i are proportional to unitary operators, they are not unitary operators themselves.

In the case of one-dimensional MBQC, the boundary condition starts in the $|+\rangle$ state, and evolves via measurement throughout the computation. First, if a computational basis measurement is performed resulting in outcome m, then the logical operator evolves to $A[m] = H|m\rangle\langle m|$. Thus, if for example the first qubit is measured in this basis, then the boundary condition is updated to $Z^m|+\rangle$.

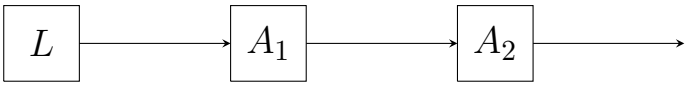


Figure 1.15: *MPS evolution.* The processing of logical operator in MPS. The input state is in state $|L\rangle$ at the start of the computation. As the first qubit is measured, its logical operator evolves to A_1, and as the second qubit is measured, its logical operator evolves to A_2. Thus the input state is processed as the computation goes along.

When the qubit is measured in the X basis resulting in outcome $|x_k\rangle$, then the logical operator evolves to:

$$A[x_k] = \sum_{i_j} \langle x_k|i_j\rangle A[i_j] = \frac{1}{\sqrt{2}} HZ^k, \tag{1.46}$$

and similarly a measurement in the Y basis resulting in outcome $|y_k\rangle$ results in the logical operator evolving to $A[y_k] = \frac{1}{\sqrt{2}} HZ^k$. Finally, when a measurement onto the equatorial plane of the Bloch sphere is performed resulting in outcome $|s_k\rangle$, the logical operator is mapped to $A[s_k] = \sum_{i_j} \langle s_k|i_j\rangle A[i_j]$. By substituting an expression for the basis state we obtain $A[s_k] = \sum_{i_j} \langle +|Z^k e^{i\frac{\phi}{2}Z}|i_j\rangle A[i_j]$, which further can be written as $A[s_k] = \sum_{i_j} \frac{1}{\sqrt{2}} e^{i(-1)^{i_j}\frac{\phi}{2}} (-1)^{i_j k} A[i_j]$. Thus, we finally have in the case of an equatorial basis measurement, the logical operator has evolved to:

$$A[s_k] = \frac{1}{\sqrt{2}} HZ^k e^{i\frac{\phi}{2}Z}. \tag{1.47}$$

We have thus introduced two distinct models of computation, the unitary circuit model and MBQC, which although different are equivalent in terms of computational power. But, the question now arises as to how can we assess and measure computational power? In order to answer this question, we shall next turn our attention to the field of computational complexity theory.

1.4 Computational Complexity

The world is in a state of continual change and evolution, wherein nature performs computational tasks of unimaginable complexity. Collections of atoms and molecules continuously interact with one another, their configuration changing over time until a state of equilibrium is reached. Yet, for us, the problem of modelling the dynamics of many-body systems and computing their properties is hard. The origin of this complexity is unclear, although its root may lie within the correlations present in the system. In order for this question to be studied, a framework capable of connecting both physical and computation is required, which is given by computational complexity [83, 84]. Here, the approach is to primarily consider problems with yes-or-no answers, and to answer these questions, we are given access to a machine M alongside a set of resources R.

First, we must ask how to quantify the hardness of a problem. A simple answer would be by how long it takes us to solve it: what is quick, we call easy, and what takes time, hard. A similar

approach is adopted by complexity theory, where the variable is the input size n, and where the question is to determine the time scaling with input size. For example, adding the numbers 3 and 5 is very easy but adding two nine digit numbers, only slightly harder. On the other hand, factoring 15 is easy, whereas factoring a nine digit number is now significantly harder. Thus, the scaling of computational time with input size captures the hardness of a given problem.

Thus, our goal is to determine the worst case run time $\mathcal{O}(f(n))$ with input size n. Here, we adopt the Big-O notation, where a function $g(n)$ is said to be $\mathcal{O}(f(n))$ if there exists constants n_0 and c such that $|g(n)| < c|f(n)|$, $\forall n > n_0$, thus placing an upper bound on the function $g(n)$. The computation is said to be efficient when the function $f(n)$ is typically a polynomial or logarithmic function. Complexity theory thus concerns itself with worst case run times, a behaviour which may not be representative of a typical instance, but which nonetheless is useful and insightful.

In the following, we shall first introduce key concepts of complexity theory in section 1.4.1, as well as the main complexity classes relevant to this thesis in section 1.4.2. Next, in section 1.4.3, the k-LOCAL HAMILTONIAN problem is presented, an important problem providing a link between the fields of physics and computer science. Finally, the tool of postselection is introduced in section 1.4.4, before efficient classical simulations of quantum computations is discussed in section 1.4.5.

1.4.1 The Language of Computational Complexity

First, we shall formally introduce different classes of problems which can be considered. Next, we shall look at the various models of computation and resources we have access to in order to solve these.

Problems

The first distinction we can make is by looking at whether the output of the computation is a single bit or a multi-bit string. The simplest class of problems we can consider are those with yes-or-no answers, which are called decision problems and which correspond to the case of a single output bit. For example, we can ask questions such as "Is x a prime number?", a problem known as primality testing. Here, the input is an n-bit string $x \in \{0,1\}^n$, and thus some of these inputs will cause the computation to output a 1, and others a 0. An alternative formulation is to think of the set of accepting strings, called a language, $\mathcal{L} \subseteq \{0,1\}^*$ and to determine whether the input belongs to that set, that is whether $x \in \mathcal{L}$.

Until now, we have assumed the computation to be defined on all inputs. By relaxing this condition, we can define promise problems, where we require the guarantee that the input is either a *yes*-instance or a *no*-instance, that is $x \in \mathcal{L}_{yes} \cup \mathcal{L}_{no}$, where $\mathcal{L}_{yes} = \{x \subset \{0,1\}^*\}$, and $\mathcal{L}_{no} = \{x \subset \{0,1\}^*\}$ are such that $\mathcal{L}_{yes} \cap \mathcal{L}_{no} = \varnothing$.

Furthermore, optimisation problems constitute an important class of problems due to their breadth of application. Here, the output of the computation is a numerical value. For example, we could ask what is the shortest tour in a graph or what is the minimum energy of a system. If we allow for approximation, these can then be transformed into decision problems, whereby we ask questions such as "Does there exist a tour with length less than k?". By repeating this procedure for ever decreasing values of k, an approximate solution can thus be obtained.

Finally, in the case of sampling problems we are given a probability distribution $\{p_1, \ldots, p_N\}$, $0 \leq p_i \leq 1$, $\sum_{i=1}^{N} = 1$ with $N = 2^n$ and asked to sample from it. That is, there are N possible outputs y_i, $1 \leq i \leq N$, each corresponding to an n-bit string, and the goal is to output y_i with probability p_i.

Turing Machines

A Turing Machine is an abstract model of computation. This is a mechanical device consisting of a tape-head and an infinite piece of tape. The tape-head can read the symbols written on the tape, move both to the left and right, and write a symbol from a finite alphabet on the tape. The behaviour of the tape head is dictated by its internal state, which is a list of instructions, and thus upon input x, the machine implements a sequence of steps. This process stops if the machine reaches the halting state, an accepting state or a rejecting state, where the output of the computation will respectively either be a string, a 1 or a 0.

If at each move the Turing Machine can evolve in a probabilistic way—for example, based on the outcome of an unbiased coin flip—then it is called a Probabilistic Turing Machine. As we shall see, randomness can thus be viewed as a resource, which can then utilized in the design of algorithms.

Finally, we can extend the model of computation we consider by looking at a Non-Deterministic Turing Machine. Here, a computation taking n time steps to complete could correspond to any one of 2^n possible computations, with each path resulting in an output bit. For a given input x, some of these will lead to a 1, others to a 0, and we can define the function $f(x)$ as the number of accepting paths minus the number of rejecting paths on input x, which is known as a GapP function. Thus, by setting different criteria for a computation to be accepting or rejecting on input x, different models of computation can be defined, as we shall see in the next section.

Circuit Families and the Uniformity Condition

In practice, the implementation of an algorithm requires a circuit C_n to be constructed, where n is the size of the input. Such a circuit will be made of a finite set of gates acting on an input of fixed size. A problem is said to be solved, if we can solve it for all input sizes n, and we shall thus choose to consider families of circuits $\{C_n\}_{n\geq 1}$. In order to construct this circuit, its description is required. This is in itself a non-trivial task, which will itself be the output of another algorithm. This

is modelled by saying that, for a given input x, there exists a Turing Machine which can provide us with a polynomial size poly(n) description of the circuit in polynomial time poly(n). This is known as the uniformity condition, and guarantees that the task of constructing the circuit does not encode the solution to a highly difficult problem in itself.

Complexity Classes and Complete Problems

A complexity class C can now be defined by considering a specific model of computation, a well-defined criteria of acceptance and rejection, and finally by bounding the available resources, namely time and space. If a problem can be decided in a given class it is then said to belong to it.

Moreover, sometimes solving one specific problem can allow for another seemingly unrelated problem to be solved. This is achieved by way of a reduction, which is a transformation mapping an input x to the first problem into an input $R(x)$ of the second problem. Crucially, the output of the second problem will now correspond to the output of the first problem. The important point is to now ensure that the algorithm implementing the mapping is not in itself a complex task, and thus it is typically required to run in polynomial time, thus yielding what is called a polytime reduction. Sometimes, a more stringent requirement can be demanded, whereby the algorithm is demanded to run in logarithmic space, thus yielding a logarithmic reduction.

A problem is thus said to be hard for a class C if all the problems in C may be reduced to it via a specified reduction. That is, by solving it all the problems in the corresponding class can also be solved. A complete problem is one that is both in the complexity class and hard for it, and such problems are of particular interest as these capture the complexity of the entire class.

Finally, an oracle O allows for any problem in the class O to be immediately solved in a single time step. We can thus define the complexity class C^{O}, which corresponds to the complexity class C with access to an oracle O. This is of course an unrealistic model of computation, which will allow for very powerful complexity classes to be developed. This thus concludes a brief introduction to the language of complexity theory, and in the next section some common complexity classes will be defined and discussed.

1.4.2 Complexity Classes

We shall first introduce the most common classical complexity classes as well as their complete problems, before looking at how both randomness and then communication can be used in order to solve problems. Then, we shall consider how a quantum resources can be exploited in order to perform computation. Finally, the PCP theorem and its quantum analogue the QPCP conjecture are briefly discussed.

P and NP

The first class we introduce captures the class of problems which are easy to solve on a classical computer. Polytime P is the class of problems which may be solved in polynomial time by a deterministic Turing Machine with acceptance and rejection criteria defined as follows:

$$x \in \mathcal{L}, \quad \mathrm{P}[1] = 1, \tag{1.48}$$

$$x \notin \mathcal{L}, \quad \mathrm{P}[1] = 0, \tag{1.49}$$

where $\mathrm{P}[k]$ is the probability that the output bit is $k \in \{0, 1\}$. For example, the problem of primality testing is in P [85]. A problem is said to be P-complete if it is in P as well as hard for P under logarithmic space reduction. There exist many P-complete problems [86], such as for example Linear Programming. Here, given a matrix A and a vector $\vec{b}$, we are asked to find the rational vector of unknowns $\vec{x}$ such that $A\vec{x} \leq \vec{b}$ and where for a given cost vector $\vec{c}$ the quantity $\vec{c}^{\top}\vec{x}$ is maximised, .

Next, we can imagine being given access to some additional information which can be used in the computation. For instance, given a number (the input) and a set of prime numbers (the proof), we can be asked to verify whether these form a set of prime factors for the given number. Thus, such classes of questions can be thought of as verification problems.

More formally, we are given access to a Non-Deterministic Turing Machine for which the conditions of acceptance and rejection are defined as follows: if the input is a yes-instance, then there must exist at least one computational path which causes the machine to accept. If it is a no-instance, then every single computational path must reject. Alternatively, we can think of the accepting computational path as providing a proof that the input belongs to the language. This is a string of polynomial length which we shall denote by m. In contrast, for no-instances, no such proof exists.

Thus, the class Non-deterministic Polytime NP is defined as:

$$x \in \mathcal{L} \quad \exists m \text{ s.t.} \quad \mathrm{P}[1] = 1, \tag{1.50}$$

$$x \notin \mathcal{L} \quad \forall m \text{ s.t.} \quad \mathrm{P}[1] = 0, \tag{1.51}$$

where m is the proof bit-string of length $|x|$ =poly(n).

For example, the satisfiability problem, k-SAT is not only in NP, but also NP-complete. This is a constraint satisfaction problem, where we are given n literals $x_1, \ldots, x_n$ and m clauses $C_1 \ldots C_m$, each involving the conjunction of at most k variables x_i or their negation $\bar{x}_i$. The question is to determine whether the conjunction of all these clauses evaluates to true or false. For example, for 3-SAT we could have the following clauses: $C_1 = x_1 \vee x_2 \vee \bar{x}_3$ which evaluates to false if $x_1 = 0$, $x_2 = 0$ and $x_3 = 1$. Given a set of m such clauses, we need to establish whether there exists an

assignment which causes every single cause to evaluate to true.

From the Cook-Levin Theorem [87, 88], we have that 3-SAT is NP-complete. If the formula is satisfiable, then the satisfying assignment constitutes a proof of this which can easily be checked. If, on the other hand, no assignment can cause the formula it to evaluate to true, then at least one clause is not satisfied. In this case, whatever assignment is given will cause the formula to evaluate to false.

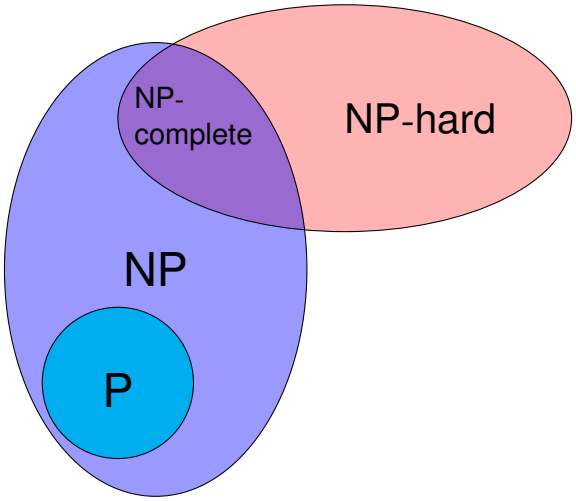


Figure 1.16: *Relationship between complexity classes P and NP.* The complexity class P is contained within NP, with NP-complete problems being in both in NP and NP-hard.

The complexity class NP is of particular importance as it contains the decision versions of many interesting optimisation problems, and the relationships between P and NP is depicted in Fig. 1.16. For instance, the associated optimization problem to k-SAT is the problem MAXSAT, where we now wish to know what is the maximum number of clauses which may be satisfied. This is NP-hard, and is a harder problem to solve than than k-SAT.

Thus, the complexity class NP is related to many important optimisation problems such as the TRAVELLING SALESMAN problem, where we are given a graph and asked to find the smallest tour which goes through each vertex, or INDEPENDENT SET, where for a given a graph the maximum set of vertices which are independent, that is, where no two vertices are adjacent, is to be determined. The decision version of both of these problems are NP-complete. Finally, we note that the famous problem of GRAPH ISOMORPHISM is in NP although not NP-complete.

Counting Problems

Until now, we have exclusively considered decision problems, where the question was to determine whether there existed a solution to a given problem. Next, we consider the class of counting problems which may be associated with a decision problem. Here, we are interested in determining how many solutions exists to a given problem. Clearly, this is a more complex question as solving the counting version of an NP-complete would immediately allow for any NP problem to be determined.

More formally, this allows for the complexity class #P to be defined as the following [83, 84, 89]. A function $f : \{0,1\}^* \to \mathbb{N}$ is said to be in #P if there exists a polynomial time Turing Machine M such that for all x we have that $f(x) = |\{y = \text{poly}(n) : M(x,y) = 1\}|$. This is reminiscent of the class NP where given a NDTM, the question was whether there existed a path which caused the TM to accept, and where now the question is how many of these paths cause the machine to accept.

For example, instead of asking whether there exists a satisfying assignment to k-SAT, we can now ask how many satisfying assignments there are, thus defining the problem #SAT, which is #P-complete. Another interesting problem which is #P-complete is PERMANENT [90], where given a matrix A of dimension $n \times n$ where each entry is either a 0 or 1, we are asked to calculate its permanent, $\text{perm}(A) = \sum_{\sigma \in S_n} \sum_{i=1}^{n} A_{i\sigma(i)}$, where S_n is the symmetric group over n.

The Polynomial Hierarchy: A Generalisation of P and NP

Next we consider the Polynomial Hierarchy PH, an infinite tower of complexity classes where each level corresponds to complexity classes of increasing in power and which exploit the power of oracles. This is a generalisation of the classes P and NP, and refers to a family of classes which are consensually believed to be distinct and which are defined as follows:

$$\Sigma_{i+1} = \mathsf{NP}^{\Sigma_i}, \tag{1.52}$$

$$\Pi_{i+1} = \mathsf{coNP}^{\Sigma_i}. \tag{1.53}$$

The ground level of the hierarchy is given by $\Sigma_0 = \Pi_0 = \mathsf{P}$, which corresponds to problems which have efficient classical algorithms. Next, at the first level we find the class $\Sigma_1 = \mathsf{NP}^{\mathsf{P}} = \mathsf{NP}$ and its complement $\Pi_1 = \mathsf{coNP}^{\mathsf{P}} = \mathsf{coNP}$, which corresponds to problems whose *no*-instances have polynomial sized checkable proofs. Thus, as we have gone up a level in the tower, the computational power has increased. Also, one notes that the belief that $\mathsf{P} \neq \mathsf{NP}$ implies that the ground and first level of the polynomial hierarchy are distinct.

At the second level, we find the classes $\Sigma_2 = \mathsf{NP}^{\mathsf{NP}}$ and $\Pi_2 = \mathsf{NP}^{\mathsf{coNP}}$. Here, the class $\mathsf{NP}^{\mathsf{NP}}$ is defined by given the class NP access to an NP oracle, and thus these problems can now be solved in a

single time step. The third level of the polynomial hierarchy thus has an even greater computational power than the second.

We can thus define successive complexity classes, where each level has increasing computational power. An important assumption of complexity theory is that these levels are distinct. If from the nth level onwards, the classes were to be equal, then we would say that the polynomial hierarchy collapses to the n^{th} level. For example, if P = NP then the polynomial hierarchy would collapse to the ground level. For future use, we shall formally define this as our first hypothesis:

Hypothesis 1. The k + 1th level of the polynomial hierarchy is distinct from the kth level for any integer k.

Until now, we have considered models of computation where no error might occur. We shall next extend these definitions to encompass randomness as a resource.

Randomness as a Resource: BPP and PP

Imagine you are trying to solve a problem, and are offered access to a fair coin: do you believe this might help you? If yes, then that would mean randomness is a valuable resource which can be exploited in order to create powerful algorithms. Exploiting randomness in the computation can be modelled by providing the Turing Machine with a set of uniform random bits. The computation will now evolve in a probabilistic manner, and thus an error on the output might occur.

The resulting complexity class is called Bounded Error Polynomial time, BPP, which is the analogue of P but with bounded error $\varepsilon = 1/3$ on output:

$$x \in \mathcal{L}, \quad \mathrm{P}[1] \geq 2/3, \tag{1.54}$$

$$x \notin \mathcal{L}, \quad \mathrm{P}[1] \leq 1/3. \tag{1.55}$$

More generally, the error probability could be any arbitrary constant bounded below one half, $0 \leq \varepsilon < \frac{1}{2}$. By repeating the algorithm and taking a majority vote on the outputs, the probability of making an error can approach zero. This can be shown by applying the Chernhoff-Hoeffding bound [83], where we get that by choosing a number of repetitions $n = \mathcal{O}(\frac{1}{\varepsilon^2})$, we can detect the correct output with good confidence. Thus, even if the error was given by $\varepsilon = \frac{1}{2} + \frac{1}{\mathrm{poly}(n)}$, then when x is a yes-instance a majority vote can be taken by performing a polynomial number of trials. On the other hand, if $\varepsilon = \frac{1}{2} + 2^{-n}$, then an exponential number of trials would be required in order for a majority vote to be taken, which is infeasible. Hence, the complexity class BPP captures the class of computation where an error can occur on the output, but where by running it a polynomial number of times and taking a majority vote the correct output may be obtained with good confidence. It is clear that P $\subseteq$ BPP, and it is currently conjectured although not proven that BPP $\subseteq$ P.

Until now, the error probability was bounded by an inverse polynomial in the input size. We now consider relaxing this, and we thus define the semantic class Probabilistic Polytime PP as the unbounded version of BPP:

$$\text{if } x \in \mathcal{L}, \quad \mathrm{P}[1] > \frac{1}{2}, \tag{1.56}$$

$$\text{if } x \notin \mathcal{L}, \quad \mathrm{P}[1] \leq \frac{1}{2}. \tag{1.57}$$

We have that the bounded version BPP is believed to be contained within PP, although the converse should not be true. Indeed, in PP, the error can depend on the input, whereas previously it was constant. Thus, we can imagine a scenario where the probability of acceptance and rejection are respectively $\frac{1}{2} + \frac{1}{2^n}$ and $\frac{1}{2} - \frac{1}{2^n}$, thus growing exponentially closer. In particular, Toda showed that PP is as hard as the polynomial hierarchy, or more precisely that the polynomial hierarchy is contained in the class P^{PP} [91].

The complete problem for PP is MAJSAT. Here, as in k-SAT, we are given the conjunction of a collection of clauses acting on k or less of the n variable, and the question is now to determine whether the majority of the possible 2^n assignments satisfy this expression or not. Intuitively, we can see this is a hard problem from the following argument: as the algorithm runs in polynomial time, each of the possible computational paths will be of polynomial length. As these may be of different lengths (thus making it an unbalanced or variable path length version of BPP), it must be standardised such that all paths have the same length $p(n)$. There thus exists a total of $2^{p(n)}$ different computational paths, leading either to a 1 or 0. We need to determine whether $\frac{2^{p(n)}}{2} + 1$ or more paths accept, the absolute worst case scenario occurring when, for a yes-instance, exactly $\frac{2^{p(n)}}{2} + 1$ accept and $\frac{2^{p(n)}}{2} - 1$ reject. So the difference between the number of accepting and rejecting paths will be of 2 paths, which translates into a probability of $\frac{2}{2^n} = \frac{1}{2^{n-1}}$. This is the error which will occur in the worst case, and as we can see it decreases exponentially with n.

Next, we shall consider the case of how communication can be used in order to help us solve problems. This can be thought of as having access to some additional information.

Interactive Proofs: IP, MA, AM

Until now, we have considered scenarios where we are given access to a Turing Machine as well as a set of uniform random, and asked to solve a given problem upon input x. Thus, the only information we had access to was the input itself. We now ask whether communication can help us with this computational task. More specifically, we imagine receiving additional information from a powerful interlocutor, which if correct, could be used.

This situation is modelled by Arthur-Merlin games, where Arthur is a creature with polynomially

bounded computational power wishing to solve a given problem, and Merlin is an all powerful magician. They are both given access to the input x, and they can send each other messages of polynomial length. One round of communication corresponds to Arthur flipping his coins, sending a question to Merlin, and then in turn receiving an answer. A protocol with a constant number k of communication is called $\mathsf{AM[k]}$. It was shown that $\mathsf{AM[k]} = \mathsf{AM}[2]$ [92], where $\mathsf{AM}[2]$ is referred to as AM. If, on the other hand, the number of rounds depends on the input size n, then we have the powerful class $\mathsf{AM[poly(n)]}$, which corresponds to the class of interactive proofs systems, IP. This is an extremely powerful class, as we have that $\mathsf{IP} = \mathsf{PSPACE}$, where PSPACE corresponds to the problems which can be solved in polynomial space.

An alternative protocol exploiting communication would be for Merlin to send a message to Arthur upon receiving the input. This is thus a single message protocol and results in the class MA and which is defined as follows:

$$x \in \mathcal{L} \quad \exists m \quad \mathrm{P}[1] \geq 1 - \varepsilon, \tag{1.58}$$

$$x \notin \mathcal{L} \quad \forall m \quad \mathrm{P}[1] \leq \varepsilon, \tag{1.59}$$

where m is a classical bit string size of polynomial size $|m|$ =poly(n) and where the error probability ε is one again bounded below one half. As Arthur has access to randomness in order to perform the computation, this class can be viewed as the probabilistic analogue of NP. It thus contains both NP and consequently BPP. On the other hand, it can be seen as a special case of $\mathsf{AM}[3]$ and is thus contained in AM.

We have thus seen how first randomness could be exploited throughout the computation and then how communication could increase computational power. We now consider how exploiting features of quantum mechanics can be done, and find quantum analogues of many of the classes previously defined.

Quantum Resources: BQP and QMA

Finally, we now consider the power of quantum computation, whereby quantum states undergo unitary evolution before a final single qubit measurement is performed. In analogue with a classical Turing Machine, a Quantum Turing Machine (QTM) can be defined, which can then be used in order to introduce various quantum complexity classes [93].

As the output of the computation results from a measurement, which is a probabilistic process, a wrong answer might be obtained, which will result in a bounded error analogous to that seen in BPP. Thus, we define the class of decision problems which can be decided on a quantum device as

the class Bounded error Quantum Polytime, BQP [94]:

$$x \in \mathcal{L}, \quad \mathrm{P}[1] \geq 1 - \varepsilon, \tag{1.60}$$

$$x \notin \mathcal{L}, \quad \mathrm{P}[1] \leq \varepsilon, \tag{1.61}$$

where the error tolerance is given by $0 \leq \varepsilon < \frac{1}{2}$. As in the case of BPP, the computation can be repeated a polynomial number of times in order to amplify the output probabilities.

It is easy to see that both P and BPP are contained in BQP. Although it is believed that BQP is a powerful class, it is nonetheless contained within PP [95]. Finally, it is interesting to note that BQP is low for PP, illustrating the power of PP.

We next consider the role of communication when used in a quantum setting. Until now, complexity classes have been defined in terms of Turing Machines. Henceforth, we shall adopt a description in terms of circuit families $\{C_n\}_{n\geq 1}$, where n denotes the input size. We thus now consider the quantum analogue of the class MA, by looking at the class of problems which may be verified on a quantum computer given access to quantum advice. The complexity class QMA [96, 97] is the quantum analogue of MA, where we are now given a quantum state as a proof and a quantum computer in order to verify it. A promise problem $\mathcal{L}$ is in QMA if, on input x, there exists a polynomial classical algorithm that computes a function $x \mapsto Z(x)$, where $Z(x)$ is a description of a quantum circuit family realising an operator $U_x : \mathcal{B}^{\otimes N_x} \to \mathcal{B}^{\otimes N_x}$ such that:

$$x \in \mathcal{L} \quad \exists |\zeta\rangle \in \mathcal{B}^{\otimes m_x} \quad \mathrm{P}[1] \geq 1 - \varepsilon, \tag{1.62}$$

$$x \notin \mathcal{L} \quad \forall |\zeta\rangle \in \mathcal{B}^{\otimes m_x} \quad \mathrm{P}[1] \leq \varepsilon, \tag{1.63}$$

where once again the error probability is required to be bounded below one half, $0 \leq \varepsilon < \frac{1}{2}$.

The complete problem for the class QMA is the k-LOCAL HAMILTONIAN PROBLEM, which is discussed in detail in section 1.4.3. Here, we are given a Hamiltonian operator $H = \sum_{i=1}^{M} H_i$, where the individual terms H_i are Hermitian and k-local, and asked to determine whether the ground state energy is below a value $a \in \mathbb{R}$ or greater than a value $b \in \mathbb{R}$, where we are promised that the gap $b - a = \frac{1}{\mathrm{poly}(n)}$ scales as an inverse polynomial with the system size. This problem is of particular relevance as it connects the field of computational complexity to that of condensed matter physics.

Thus, we have seen that various complexity classes of varying computational power can be defined, as shown in Fig. 1.17. Finally, we briefly mention the PCP theorem and the research conducted towards understanding its quantum analogue.

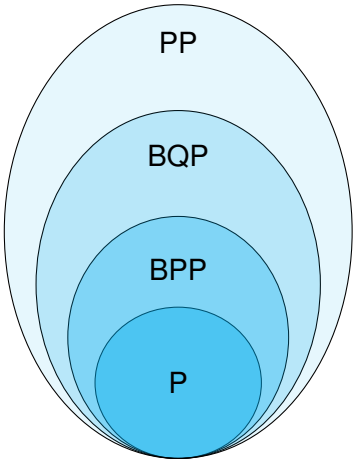


Figure 1.17: *A hierarchy of complexity classes.* The complexity class P is believed to be equal to BPP. In turn, this is contained in the quantum equivalent BQP, which is believed to be more powerful. Finally, these are all contained in the powerful semantic class PP, which is the unbounded error version of BPP.

The PCP Theorem and QPCP conjecture

The PCP, Probabilistically Checkable Proofs, theorem is an important result of classical complexity theory, dealing with hardness of approximation [98, 99]. Here, approximate solutions are sought for optimisation problems. For instance, we previously established that it was NP-hard to determine whether a 3-SAT formula is satisfiable or not, that is, to distinguish between the case when there exists a satisfying assignment from the case where all assignments are unsatisfying. For example, given a 3-SAT formula, one clause excludes one out of the $2^3 = 8$ possible assignments. It is thus satisfied with probability $\frac{7}{8}$, and the expectation value of the fraction of clauses satisfied is thus $\frac{7}{8}$. The PCP theorem states that it is NP-hard to do better than this. More precisely, it states that even if we are guaranteed that the expression is either satisfiable or most of the clauses are unsatisfiable, then it nonetheless remains NP-hard to distinguish between these two cases.

The Quantum PCP conjecture [100], QPCP is an attempt to derive a similar cornerstone result for the field of quantum approximation. Here, the problem considered is to approximate the ground state energy of a Hamiltonian operator. An important result towards the development of the QPCP conjecture is the No Low-Energy Trivial States (NLTS) conjecture, which tells us there are Hamiltonians that have non-trivial low energy states [101]. Here, a non-trivial state is one that can is generated by a low depth circuit, and yet is highly entangled.

Next, we look at the k-LOCAL HAMILTONIAN problem in greater detail, which is the complete problem for the class QMA. We will first consider its physical relevance, before discussing Kitaev's proof of QMA-completeness.

1.4.3 The k-LOCAL HAMILTONIAN Problem

The energy of a system, an important quantity in physics, is captured by its Hamiltonian operator. In the following, motivated by considerations stemming from condensed matter theory, we consider how physical systems can be connected to computation through the k-LOCAL HAMILTONIAN problem, which has been shown to be QMA-complete.

The Hamiltonian Operator

The dynamics of a quantum system are governed, via the Schrödinger equation, by the system's Hamiltonian operator H. This operator captures not only the interactions present between the particles, but also with their environment. For instance, the matrix representation of the Hamiltonian for a system comprising of n qubits is of exponential dimension 2^n, with a priori no symmetry or structure to be exploited. Thus, the Hamiltonian is an intuitively complex operator, which in turn places a fundamental limitation on our capacity to understand quantum systems.

For indeed, the eigenvectors and associated eigenvalues of the Hamiltonian correspond to respectively the energy states the system can adopt and its associated energy. It is thus a hermitian positive operator, whose spectrum is of critical importance to the fields of both physics and chemistry. Of particular interest is the smallest energy eigenvalue—the ground state energy E_0—which the system can adopt. For example, when a system is cooled down towards absolute zero, its energy will decrease as it tends towards the ground state.

Thus, we wish to compute the eigenvalues and eigenvectors of a matrix of exponential dimension, which is a hard task. Even though useful numerical methods have been devised, there exists as yet no efficient algorithm which efficiently computes these properties for matrices of arbitrary dimension. However useful heuristic methods might be, the question remains as to wherein lies the origin of this complexity.

Local Hamiltonians

The concept of locality is at the heart of physics. For example, many quantum objects have been successfully modelled by spins on a lattice subject to nearest neighbour interactions and local external fields. By both limiting the range of interaction and by pinning the qubits to the lattice, the problem at hand is considerably simplified, thus allowing it to be studied in more depth. Furthermore, the assumption of geometric locality is a constraint which not only simplifies the problem, but also roots it back into physical observation.

In the following, we shall adopt a different notion of locality. Here, a Hamiltonian operator will be said to be k-local if, for a system of n qubits, it can be expressed as a sum of a polynomial number of terms, where each term of the sum will itself be a Hamiltonian, this time acting on at most k of

qubits. Thus, the Hamiltonian operator itself may be highly non-local, even though it is made up of individually local terms.

Hamiltonians and Computation

It was Feynman who first had the fundamental insight that the Hamiltonian of a system could encode the discrete time evolution of a quantum state. The system starts in an initial state $|\psi_0\rangle$ at time step 0, and evolves to $|\psi_L\rangle$ via a sequence of intermediate states $|\psi_i\rangle$, where $i = 0, \ldots, L$. The idea is to construct a Hamiltonian operator whose zero eigenvalue eigenvectors correspond to these correct computational states.

More precisely, it will consist of two Hamiltonians: one associated with the system of interest $\mathcal{H}_{system}$ and one tracking discrete time, a clock register $\mathcal{H}_{clock}$. We can think of this as a pointer particle moving to the left or to the right of a one-dimensional lattice. For L time steps, we would thus require $L+1$ qubits. For example, if the particle hops to a site to the right, this models the clock transition from time step t to $t+1$. As quantum evolution is reversible, the particle will be allowed to also move to the to the left, thus effectively reversing time.

Thus, the history state $|\eta\rangle$ can now be introduced, which corresponds to a uniform superposition over all correct evolution states:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{i=0}^{L} |\psi_i\rangle \otimes |i\rangle, \tag{1.64}$$

and which will have to be contained in the kernel of the constructed Hamiltonian.

Hamiltonians and Satisfiability

Thus, we wish to define a Hamiltonian for which correct computational states are ground states. In the case of a frustration free Hamiltonian, the null states must be zero eigenvectors of each individual term, thus resulting in a Hamiltonian with zero ground state energy. This is reminiscent of the 3-SAT problem we previously introduced in the context of NP-completeness, for which a satisfying assignment had to satisfy every single clause. And indeed, the satisfiability problem can be connected to the Hamiltonian construction.

This is achieved by associating a projector with each unsatisfying assignment. By choosing to interpret it as a Hamiltonian operator, any unsatisfying configuration will then incur an energy penalty. For example, for the clause $x_1 \vee x_2 \wedge x_3$, the assignments 001 and 000 are unsatisfying, and lie within the subspace spanned by the projector $P = |000\rangle\langle 000| + |001\rangle\langle 001|$. In turn, a Hamiltonian operator can be associated with this, and the question is thus to determine whether there exists a ground state of zero energy, that is, simultaneously satisfying all projectors. This case of a frustration

free k-LOCAL HAMILTONIAN is known as k-QSAT and corresponds to the direct quantum analogue of k-SAT [102].

More generally, the problem MAX-k-SAT asks us to determine what is the assignment which satisfies the maximum number of clauses of a k-SAT formula. Here, we are no longer given the guarantee that all clauses are simultaneously satisfiable. The k-LOCAL HAMILTONIAN problem is its quantum analogue, and we shall now formally define it.

Formal Problem Statement

The k-LOCAL HAMILTONIAN problem was introduced by Kitaev [45], and generalises these ideas by taking into account the quantum nature of systems. Formally:

Definition 1. *The k-LOCAL HAMILTONIAN is the following: given a k-local operator $H = \sum_{i=1}^{r} H_i$, where $r = \mathcal{O}(n)$, $H_i^\dagger = H_i$, $||H_i|| \leq \mathcal{O}(1)$ and two real numbers $0 \leq a \leq b$ such that the promise gap $\delta = b - a$ closes polynomially with the system size $\delta > \frac{1}{O(n)}$, then:*

$$\text{if } x \in \mathcal{L}_{yes}: \quad \lambda_1(H) < a \quad ,\exists|\xi\rangle, \quad \langle\xi|H|\xi\rangle < a, \tag{1.65}$$

$$\text{if } x \in \mathcal{L}_{no}: \quad \lambda_1(H) > b \quad \forall|\xi\rangle, \quad \langle\xi|H|\xi\rangle > b. \tag{1.66}$$

It was shown the the k-LOCAL HAMILTONIAN problem, for $k = \mathcal{O}(1)$, is QMA-complete [103, 104], that is, it captures the complexity of the entire class of problems which can be verified by a quantum computer.

Theorem 1. *The k-LOCAL HAMILTONIAN problem is* QMA*-complete.*

More specifically, it was shown to be QMA-complete for $k = 5$, which was later improved to $k = 3$ [104] and then $k = 2$ [103]. The development of the k-LOCAL HAMILTONIAN problem and its proof of QMA-completeness spear-headed the field of Hamiltonian complexity [105–108], wherein a complexity theoretic approach is adopted in order to understand the nature and structure of ground states. For example, one may consider additional assumptions in the hope of rendering the problem both more physical and tractable, as for example stoquastic Hamiltonians, a problem shown to be MA-complete [109]. For a comprehensive review, we refer the reader to [110].

Core Idea

The fundamental idea captured by the k-LOCAL HAMILTONIAN problem is that if there exists a ground state with low energy, then providing a quantum computer with an efficient description of both the ground state and the Hamiltonian will allow us to verify this fact. On the other hand, if this is not the case, then no quantum state could convince us otherwise. The optimization problem

associated with the k-LOCAL HAMILTONIAN is to compute the ground state energy of a Hamiltonian up to an additive polynomial error, which is QMA-hard. We shall now introduce the verifier circuit used in order to verify the energy of the quantum proof state.

Verifier Circuit

The verifier circuit is a quantum circuit implementing an N qubit unitary operator U, acting on the proof which is an m-qubit quantum state $|\xi\rangle$, as well as $N-m$ auxiliary qubits initialised in the state $|0\rangle$. At the end of the computation, a measurement in the computational basis of the first qubit is performed, with measurement outcome denoted by m. This will determine whether the computation accepts or rejects, and we have that the probability of obtaining outcome m is given by:

$$\mathrm{P}[m] = \langle \xi, 0|U^\dagger \Pi_1^{(m)} U|\xi, 0\rangle = |\langle \xi, 0|U^\dagger|m\rangle|^2, \tag{1.67}$$

where $\Pi_1^{(m)}$ denotes the projector of the first qubit onto m, with identity applied onto all others.

Circuit-to-Hamiltonian Construction

The circuit-to-Hamiltonian construction encodes this quantum circuit in a Hamiltonian, thus providing us with a tangible link between ground state energy and computation. From the Solovay-Kitaev theorem, the unitary U may be decomposed into a polynomial sequence of single and two qubit gates U_i picked from a universal gate set $\mathcal{G}$: $U = U_L \dots U_1$, where L =poly(n). Thus, the gates can be applied sequentially, one after the other, with gate U_j being applied after j time steps, which thus results in the input state $|\xi, 0\rangle$ having evolved to $U_j \dots U_1|\xi, 0\rangle$. In order to capture this notion of time, a second register is added to our system, which is a qudit of dimension L. We can thus now express the history state of the computation as:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{j=1}^{L} U_j \dots U_1|\xi, 0\rangle \otimes |j\rangle. \tag{1.68}$$

The next step is to construct a Hamiltonian operator H such that the history state lies within its kernel. It will be made up of three Hamiltonians: an input, a propagation and an output Hamiltonian. The role of the input Hamiltonian H_{in} is to verify that the $N-m$ ancillary qubits have been correctly initialised in the $|0\rangle$ state, which lie within the kernel of the operator:

$$H_{in} = \sum_{s=m+1}^{N} \Pi_s^{(1)} \otimes |0\rangle\langle 0|. \tag{1.69}$$

Next, the propagation Hamiltonian is defined as the sum of the individual propagation Hamiltonian terms $H_{prop} = \sum_{j=1}^{L} H_j$, where H_j contains the evolution from time step $j-1$ to j. In this case, the

state $|\psi\rangle$ evolves to a new state $U_j|\psi\rangle$ via unitary evolution:

$$|\psi\rangle \otimes |j-1\rangle + U_j|\psi\rangle \otimes |j\rangle, \tag{1.70}$$

which can easily be verified to lie within the kernel of:

$$H_j = \frac{1}{2}(-U_j \otimes |j\rangle\langle j-1| - U_j^\dagger \otimes |j-1\rangle\langle j| + \mathbb{1} \otimes |j\rangle\langle j| + \mathbb{1} \otimes |j-1\rangle\langle j-1|). \tag{1.71}$$

Finally, at time step L, a computational basis measurement of the first qubit is performed, which in the case of an accepting computation yields the output 1. In this case, the resulting output state resides in the nullspace of the output Hamiltonian given by:

$$H_{out} = \Pi_1^{(0)} \otimes |L\rangle\langle L|. \tag{1.72}$$

Thus, a Hamiltonian operator $H = H_{in} + H_{prop} + H_{out}$ encoding the computation has been constructed, and the next task is to determine its eigenvalues.

Spectral Analysis

More specifically, the task at hand is to compute the spectrum of the Hamiltonian and, in particular, to derive an analytic expression for its smallest non-zero eigenvalue. The input and output Hamiltonian operators are projectors, thus each having eigenvalues 0 and 1. In contrast, the propagation Hamiltonian is an a priori complex mathematical object, whose spectrum does not have any known analytic expression. For this reason, the operators will be transformed and expressed in a new basis, which as we shall see, will considerably simplify the task.

First, we note that the history state $|\eta\rangle$ may be expressed as $|\eta\rangle = W|\xi, 0\rangle \otimes |\psi\rangle$, where the change of basis operator W is defined as $W = \sum_{j=1}^{L} U_j \dots U_1 \otimes |j\rangle\langle j|$, and where $|\psi\rangle = \frac{1}{\sqrt{L+1}} \sum_{i=1}^{L} |i\rangle$ is a uniform superposition over all time steps. Thus, we can now alternatively consider the state $|\xi, 0\rangle \otimes |\psi\rangle$ as the correct computational state of the transformed Hamiltonian $W^\dagger H W$, which shall be henceforth refer to as $\tilde{H}$. Crucially, as W is a unitary operator, the spectrum of the Hamiltonian will be conserved under this transformation.

The Hamiltonian input term is invariant under this change of basis, $W^\dagger H_{in} W = H_{in}$. The individual propagation terms are transformed to:

$$W^\dagger H_j W = \mathbb{1}_N \otimes \frac{1}{2}(|j-1\rangle\langle j-1| - |j\rangle\langle j-1| - |j\rangle\langle j-1| + |j\rangle\langle j|) = \mathbb{1}_N \otimes E_j, \tag{1.73}$$

which results in the Hamiltonian propagation term being given by the operator:

$$W^\dagger H_{prop} W = \mathbb{1}_N \otimes \sum_j W^\dagger H_j W = \mathbb{1}_N \otimes \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 & \dots & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & \\ 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & \\ & & & & \end{pmatrix}. \tag{1.74}$$

The clock register is now given by a tridiagonal matrix, demonstrating a surprising amount of structure and symmetry, which shall later be exploited for the spectral analysis. Finally, the basis change is applied to the output Hamiltonian H_{out}, leading to:

$$\tilde{H}_{out} = W^\dagger H_{out} W = U^\dagger \Pi_1^{(0)} U \otimes |L\rangle\langle L|. \tag{1.75}$$

Thus, we can now finally discuss Kitaev's proof of QMA-completeness. The proofs proceeds in two parts: first, the k-LOCAL HAMILTONIAN problem is shown to be in QMA, that is, it can be verified by a quantum computer, and then it is shown to be QMA-hard.

In QMA

First, we must show that the k-LOCAL HAMILTONIAN problem is in the class QMA. In other words, given access to a quantum computer and a quantum certificate $|\xi\rangle$, can we determine whether a given Hamiltonian has energy less than a or greater than b?

Although the Hamiltonian H may be non-local, the individual terms H_j are local by assumption, and we can thus construct a quantum circuit which estimates their energy. Each term is positive with spectral decomposition given by: $H_j = \sum_s^{\dim(H_j)} \lambda_s |\psi_s\rangle\langle\psi_s|$. These can be efficiently obtained as each individual term H_j acts on a constant number of at most k qubits. The certificate state is then decomposed in this eigenbasis $|\xi\rangle = \sum y_s |\psi_s\rangle$, and thus we have that $\langle\xi|H_j|\xi\rangle = \sum_s \lambda_s |y_s|^2$.

Next, we define the verifier circuit W_j of constant size as:

$$W_j|\psi_s, 0\rangle = |\psi_s\rangle \otimes (\sqrt{\lambda_s}|0\rangle + \sqrt{1-\lambda_s}|1\rangle). \tag{1.76}$$

If the second qubit is now measured in the computational basis, then the probability of obtaining

outcome 1 is given by:

$$\begin{aligned}
\mathrm{P}_j[1] &= \langle \xi, 0 | W_j^\dagger | 1 \rangle \langle 1 |_2 W_j | \xi, 0 \rangle, \\
&= \sum_{s,t} \sqrt{1-\lambda_s} y_s^* \sqrt{1-\lambda_t} y_t \langle \psi_s | \psi_t \rangle, \\
&= \sum_s (1-\lambda_s) |y_s|^2, \\
&= 1 - \langle \xi | H_j | \xi \rangle.
\end{aligned}$$

Now, the final goal is to estimate the energy $\langle \xi | H | \xi \rangle$, where we let r denote the total number of terms in the Hamiltonian H. An integer j is chosen uniformly at random from $\{1, \ldots, r\}$, and the circuit W_j is then applied to the input state $|\xi, 0\rangle$. This can alternatively be expressed by adding an index register to the input state $\frac{1}{\sqrt{r}} \sum |j\rangle_{index} \otimes |\eta\rangle \otimes |0\rangle$ to which the operator $\sum_{j=1}^r |j\rangle\langle j|_{index} \otimes W_j$ is then applied. We thus finally have that the probability of obtaining outcome 1 is given by:

$$\mathrm{P}[1] = \sum_j \frac{1}{r} \mathrm{P}_j[1] = \sum_j \frac{1}{r} (1 - \langle \xi | H_j | \xi \rangle) = 1 - \frac{1}{r} \langle \xi | H | \xi \rangle. \tag{1.77}$$

If there exists a quantum state $|\xi\rangle$ which has energy less than a, then the probability that the computation is accepting is given by $\mathrm{P}[1] \geq 1 - \frac{1}{r}a$. On the other hand, if the energy of every possible quantum state is greater than b, then the probability of accepting is given by $\mathrm{P}[1] \leq 1 - \frac{1}{r}b$. As these energy thresholds are separated by an inverse polynomial in system size n, then the acceptance and rejection criteria allow us to determine the k-LOCAL HAMILTONIAN problem.

Next, we must show that the k-LOCAL HAMILTONIAN problem is QMA-hard. In order to do so, the central idea hinges upon the Hamiltonian having a small eigenvalue if and only if there exists a verifier circuit outputting a 1 with high probability.

QMA-Hard: Yes-Instances

First, we show that if upon input x the circuit outputs a yes, then this in turn means that the corresponding Hamiltonian will have ground state energy less then a. More precisely, if $x \in \mathcal{L}_{yes}$, then there exists an m-qubit quantum proof state $|\xi\rangle$ which will cause the circuit to output 1 with high probability: $\mathrm{P}[1] \geq 1 - \varepsilon$. Equivalently, the probability that the circuit will output a 0 is small and is given by: $\mathrm{P}[0] = \langle \xi, 0 | U^\dagger \Pi_1^{(0)} U | \xi, 0 \rangle \leq \varepsilon$.

Now, the history state $|\eta\rangle = W|\xi, 0\rangle \otimes |\psi\rangle$ corresponds precisely to the correct sequence of quantum state which causes the computation to accept. This, by definition, is the lowest energy state of the Hamiltonian associated to the quantum circuit, and we shall thus consider the energy $\langle \eta | H | \eta \rangle$.

Let the quantum input state be given by $|\tilde{\eta}\rangle = |\xi, 0\rangle \otimes |\psi\rangle$, and we thus have that $\langle \eta | H | \eta \rangle = \langle \tilde{\eta} | \tilde{H} | \tilde{\eta} \rangle$. It is easy to see that $\langle \tilde{\eta} | \tilde{H}_{in} | \tilde{\eta} \rangle = \langle \tilde{\eta} | \tilde{H}_{prop} | \tilde{\eta} \rangle = 0$. With respect to the output term of the

Hamiltonian, we have that:

$$\langle\tilde{\eta}|\tilde{H}_{out}|\tilde{\eta}\rangle = \langle\tilde{\eta}|(U^{\dagger}\Pi_1^{(0)}U \otimes |L\rangle\langle L|)|\tilde{\eta}\rangle, \tag{1.78}$$

$$= \mathrm{P}[0]\frac{1}{L+1}, \tag{1.79}$$

$$\leq \frac{\varepsilon}{L+1}. \tag{1.80}$$

Thus, we can define the lower energy bound as $a = \frac{\varepsilon}{L+1}$.

Next, we introduce the Projection Lemma which shall later be used in order to provide a bound on the eigenvalues in the case of no-instances.

The Projection Lemma

The Projection Lemma provides a lower bound for the minimum non-zero eigenvalue of the sum of two operators A_1 and A_2, with non overlapping kernels $\mathcal{L}_1 = \mathrm{Ker}(A_1)$, and $\mathcal{L}_2 = \mathrm{Ker}(A_2)$.

Lemma 1. *Let A_1, A_2 be two operators such that A_1 and A_2 are positive, with no common non null vector, $Ker(A_1) \cap Ker(A_2) = \{0\}$, and each having a lower bound on smallest non zero eigenvalue $\lambda_i(A_1) \geq \nu$ and $\lambda_i(A_2) \geq \nu \quad \forall i$. Then:*

$$\lambda(A_1) + \lambda(A_2) \geq \nu \cdot 2\sin^2\frac{\theta}{2}, \tag{1.81}$$

where $\theta = \theta(\mathcal{L}_1, \mathcal{L}_2)$ is the angle between the two nullspaces considered and where $\lambda(A)$ denotes the smallest non-zero eigenvalue of operator A.

Proof. By assumption, we have that the smallest non zero eigenvalue of operators A_1 and A_2 is greater than a constant ν, which we write $A_k \geq \nu\mathbb{1}$, and which in turn can be expressed as $A_k \geq \nu(\mathbb{1} - \Pi_{\mathcal{L}_k})$, for $k \in \{1, 2\}$, and where $\Pi_{\mathcal{L}_k}$ is the projector onto the subspace $\mathcal{L}_k$.

Next, we introduce the projector $\Pi = \Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2}$, a positive operator which is the sum of two non-commuting projectors. Let the state $|\xi\rangle$ be an eigenvector of eigenvalue λ for the operator Π, i.e. we have that $\Pi|\xi\rangle = \lambda|\xi\rangle$. This eigenvector has components in each of the kernel subspaces given by: $\Pi_{\mathcal{L}_k}|\xi\rangle = u_k|\eta_k\rangle$, where $|\eta_k\rangle \in \Pi_{\mathcal{L}_k}$ and $u_k \in \mathbb{R}_+, k \in \{1, 2\}$. By using the fact that $\Pi = \Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2}$ and that projectors are idempotent, it can be shown that: $u_1^2 + u_2^2 = \lambda$.

We now consider the eigenvalues of the operator $\Pi^2 = (\Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2})^2$. In order to do so, we start with the eigenvalue equation $\Pi|\xi\rangle = \lambda|\xi\rangle$, where $\lambda > 0$. This leads to $\Pi^2|\xi\rangle = \lambda^2|\xi\rangle$, which in turn can be expressed as: $\langle\xi|(\Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2})^2|\xi\rangle = \lambda^2$. By considering the components in each subspace we get that: $(\langle\eta_1|u_1 + \langle\eta_2|u_2)(u_1|\eta_1\rangle + u_2|\eta_2\rangle) = \lambda^2$, which if we multiply out leads to $u_1^2 + u_2^2 + 2u_1u_2\mathbb{R}\mathrm{e}\langle\eta_1|\eta_2\rangle = \lambda^2$.

Let $x = |\mathbb{R}\mathrm{e}\langle\eta_1|\eta_2\rangle|$. By using the fact that $u_1^2 + u_2^2 + 2u_1u_2\mathbb{R}\mathrm{e}\langle\eta_1|\eta_2\rangle = \lambda^2$ and $u_1^2 + u_2^2 = \lambda$, it can be shown that the quantity $(1+x)\lambda - \lambda^2$ is non negative and that thus $1 + x \geq \lambda$. Now, the angle between two vectors is given by $\theta = \min\left|\arccos\frac{\langle u|w\rangle}{\|u\|\|w\|}\right|$, which for normalised states reduces to $\theta = \min|\arccos\langle u|w\rangle|$, or alternatively $\cos\theta \geq \mathbb{R}\mathrm{e}\langle\eta_1|\eta_2\rangle$.

Thus, the expression $1 + x \geq \lambda$ leads to the following upper bound on tλ: $1 + \cos\theta \geq \lambda$, where λ corresponds to any non zero eigenvalues of the operator $\Pi = \Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2}$, which, in the previously introduced notation can be expressed as: $(1 + \cos\theta)\mathbb{1} \geq \Pi = \Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2}$.

As $A_k \geq \nu(\mathbb{1} - \Pi_{\mathcal{L}_k})$, we have that: $A_1 + A_2 \geq \nu(2\mathbb{1} - (\Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2}))$. Thus, we finally obtain:

$$A_1 + A_2 \geq \nu(2\mathbb{1} - (\Pi_{\mathcal{L}_1} + \Pi_{\mathcal{L}_2})) = \nu(1 - \cos\theta)\mathbb{1} = \nu \cdot 2\sin^2\frac{\theta}{2}\mathbb{1}, \tag{1.82}$$

which concludes the proof of the Projection Lemma. □

QMA **Hardness:** No**-Instances**

We now consider the case where the input x is a no-instance. This should correspond to the verifier circuit outputting a 0 with high probability, thus resulting in a rejecting computations. More precisely, here the computation will reject for all m-qubit quantum proof states with probability $P[0] = \langle\xi, 0|U^\dagger\Pi_1^{(0)}U|\xi, 0\rangle \geq 1 - \varepsilon$. Equivalently, the probability of the wrong output occurring is given by $P[1] \leq \varepsilon$.

We now define the operator $A_1 = \tilde{H}_{in} + \tilde{H}_{out}$. Its kernel $\mathcal{L}_1$ contains the following: states which at time step 0 have all $N - m$ ancillary qubits correctly initialised to $|0\rangle$ alongside any arbitrary m qubit proof state, any arbitrary N-qubit state at time steps 1 to $L - 1$, and finally the state $U^\dagger|1\rangle$ at time step L:

$$\mathcal{L}_1 = (\mathcal{B}^m \otimes |0\rangle^{N-m} \otimes |0\rangle) \oplus ((\mathcal{B}^m \otimes (\mathcal{B}^{N-m} \otimes \mathbb{C}(|1\rangle, \ldots, |L-1\rangle))) \oplus (U^\dagger|1\rangle \otimes \mathcal{B}^{N-1} \otimes |L\rangle).$$

Henceforth, we shall write this as: $\mathcal{L}_1 = \mathcal{K}_1 \oplus \mathcal{K}_2 \oplus \mathcal{K}_3$, with $\mathcal{K}_1 = \mathcal{B}^m \otimes |0\rangle^{N-m} \otimes |0\rangle$, $\mathcal{K}_2 = (\mathcal{B}^m \otimes (\mathcal{B}^{N-m} \otimes \mathbb{C}(|1\rangle, \ldots, |L-1\rangle)$ and $\mathcal{K}_3 = U^\dagger|1\rangle \otimes \mathcal{B}^{N-1} \otimes |L\rangle$

Next, we define the operator $A_2 = \tilde{H}_{prop} = \mathbb{1} \otimes E$, whose kernel $\mathcal{L}_2$ contains any arbitrary state on the N qubits, with the clock register in an equal superposition over all time steps, i.e. $\mathcal{L}_2 = \mathcal{B}^N \otimes |\psi\rangle$. It is easy to see that the intersection of these kernels does not contain any non-trivial eigenvector.

The operator A_1 is the sum of two non-commuting projectors, and it is thus a positive operator whose smallest non zero-eigenvalue $\lambda(A_1)|_{\mathcal{L}_1^\perp}$ is at least 1: $\lambda(A_1)|_{\mathcal{L}_1^\perp} \geq 1$. The operator A_2 consists of, as we have seen, a particular tridiagonal matrix, whose spectrum is given by $\lambda_k = 1 - \cos(q_k)$,

where $q_k = \frac{\pi k}{L+1}$, for $k = 0, \ldots, L$ with and with corresponding eigenvectors given by:

$$|\psi_k\rangle = \alpha_k \sum_{j=0}^{\mathcal{L}} \cos(q_k(j + \frac{1}{2}))|j\rangle. \tag{1.83}$$

Here, we focus on the eigenvalues, and by performing a Taylor expansion of the cosine function, we find that the smallest non-zero eigenvalue of A_2, $\lambda(A_2|_{\mathcal{L}_2^\perp})$, is lower bounded by an inverse polynomial:

$$\lambda(A_2|_{\mathcal{L}_2^\perp}) \geq \lambda_1 = 1 - \cos(q_1) = 1 - \cos\frac{\pi}{L+1} \geq \frac{c'}{L^2}, \tag{1.84}$$

where c' is a constant and L =poly(n).

Thus, all the conditions required by the projection lemma are fulfilled, and our last task is to determine the angle between the kernels of A_1 and A_2. By definition, the angle θ between two subspaces $\mathcal{L}_1$ and $\mathcal{L}_2$ is defined as $\cos^2\theta = \max|\langle\eta_1|\eta_2\rangle|^2$, where $|\eta_i\rangle \in \mathcal{L}_i$ for $i = 1, 2$. This can be rewritten as $\cos^2\theta = \max|\langle\eta_2|\Pi_{\mathcal{L}_1}|\eta_2\rangle|$.

First, as the state $|\eta_2\rangle$ lies within the kernel of A_2, it can be expressed as $|\xi, 0\rangle \otimes |\psi\rangle$, where $|\xi, 0\rangle$ is an arbitrary N qubit state. Next, the projector onto the kernel of A_1 is decomposed and written as: $\Pi_{\mathcal{L}_1} = \Pi_{\mathcal{K}_1} + \Pi_{\mathcal{K}_2} + \Pi_{\mathcal{K}_3}$. We thus now consider:

$$\langle\eta_2|\Pi_{\mathcal{L}_1}|\eta_2\rangle = \langle\xi, 0, \psi|(\Pi_{\mathcal{K}_1} + \Pi_{\mathcal{K}_3})|\xi, 0, \psi\rangle + \langle\xi, 0, \psi|\Pi_{\mathcal{K}_2}|\xi, 0, \psi\rangle \tag{1.85}$$

By applying the Projection Lemma to the first term of the sum, we obtain that:

$$\langle\eta_2|\Pi_{\mathcal{L}_1}|\eta_2\rangle \leq \frac{1 + \cos\varphi}{\mathcal{L}+1} + \frac{\mathcal{L}-1}{\mathcal{L}+1}, \tag{1.86}$$

where φ is the angle between the subspaces $\mathcal{K}_1$ and $\mathcal{K}_3$.

By definition, the angle between two spaces corresponds to the square of the maximum overlap between two of their respective states. But, we recall that the subspace $\mathcal{K}_1$ contains correctly initialised states at time step 0, whereas $\mathcal{K}_3$ contains states which undergo the unitary transform with output 1. We previously established that on input of a no-instance, the probability of the computation erroneously accepting is given by $\mathrm{P}[1] = |\langle\xi, 0|U^\dagger|1\rangle|^2$. This probability is maximal when the overlap between the input state $|\xi, 0\rangle \in \mathcal{K}_1$ and the output state $U^\dagger|1\rangle \in \mathcal{K}_3$ is maximal. This is precisely that which defines the angle between the kernel subspaces, and is thus at most ε, and we have that:

$$\langle\eta_2|\Pi_{\mathcal{L}_1}|\eta_2\rangle \leq \frac{1 + \sqrt{\varepsilon}}{\mathcal{L}+1} + \frac{\mathcal{L}-1}{\mathcal{L}+1} = 1 - \frac{1 - \sqrt{\varepsilon}}{\mathcal{L}+1}. \tag{1.87}$$

Next, as $\sin^2\theta = 1 - \cos^2\theta$, we have that $\sin^2\theta \geq \frac{1-\sqrt{\varepsilon}}{\mathcal{L}+1}$. This allows us to apply the Projection

Lemma to the operators A_1 and A_2:

$$A_1 + A_2 \geq 2\nu \sin^2 \frac{\theta}{2} \geq 2\frac{c'}{L^2}\frac{1-\sqrt{\varepsilon}}{\mathcal{L}+1} = cL^{-3}(1-\sqrt{\varepsilon}), \tag{1.88}$$

where c is a constant. Thus, as $H = A_1 + A_2$, this has allowed us to determine that in the case of no-instances, the smallest non-zero eigenvalue of the Hamiltonian operator will be greater than $b = cL^{-3}(1-\sqrt{\varepsilon})$.

Conclusion

We have thus established, that for yes-instances, the ground state energy is less than $a = \frac{\varepsilon}{L+1}$, whereas for no-instances it is greater than $b = \frac{c(1-\sqrt{\varepsilon})}{L^3}$, where $L = O(n)$ and $\varepsilon = \exp(-\Omega(n^\alpha))$. We can define the promise gap as $\delta = b - a$, and we thus finally have that:

$$\delta = \frac{c(1-\sqrt{\varepsilon})}{L^3} - \frac{\varepsilon}{L+1} \geq \frac{1}{\text{poly}(n)}, \tag{1.89}$$

with the promise gap thus scaling as an inverse polynomial in system size. This concludes the proof.

1.4.4 Postselection

"What would you do if you won the lottery?" Every week, people ask themselves this question as they buy lottery tickets, firm in their knowledge that their chance of winning is infinitesimal, more of a dream than a tangible reality. What if the question could be transformed to a new and perhaps more enticing, however infeasible "Given that I have won the lottery, what shall I do?" Here, we discard all the disappointing outcomes of loss, and focus on what can be done given that success has occurred.

This seemingly dishonest trick is known as postselection, and can be defined as the ability to exclusively consider certain events, even though these might occur with exponentially small probability. However esoteric this may seem, these conditional probabilities are precisely what the well-known Baye's Rule of probability theory allow us to calculate:

$$\mathrm{P}[A|B] = \frac{\mathrm{P}[A \cap B]}{\mathrm{P}[B]}, \tag{1.90}$$

where A and B are two events.

Postselection as a Resource: postBQP

How would the ability to postselect on outcomes impact on the power of a quantum computer? In order to study postselection as a resource, a postselection register is added to the quantum cir-

cuit. Here, conditioned upon the measurement outcome of the postselection register, the output of the computation will or not be considered. This defines the class postBQP [111], of postselected Bounded error Quantum Polytime computation. A language is said to be in postBQP if there exists a uniform family of polynomial size quantum circuits such that when C_n is applied to $|0\ldots0\rangle|x\rangle$ and the probability that measuring the first qubit in the computational basis yields a 1 is non zero, i.e. $\mathrm{P}[1_1] \neq 0$, then:

$$x \in \mathcal{L} \quad \mathrm{P}[1_2|1_1] \geq 1 - \varepsilon, \tag{1.91}$$

$$x \notin \mathcal{L} \quad \mathrm{P}[1_2|1_1] \leq \varepsilon, \tag{1.92}$$

where 1_i denotes qubit i being measured in the computational basis and yielding a 1, and where $\varepsilon \geq \frac{1}{\mathrm{poly}(n)}$.

Key Results and Relations to other Classes

In a similar way, we can consider how adding postselection to a classical device will affect its power. This corresponds to the class postBPP, and is thus the classical analogue of the quantum class postBQP. It is equivalent to the class $\mathsf{BPP}_{\mathsf{path}}$ [112], where each computational path may be of different length.

First, we note that both $\mathsf{BPP}_{\mathsf{path}}$ and postBQP contain NP, thus postselection clearly increases computational power in both classical and quantum frameworks. Yet, we have that $\mathsf{BPP}_{\mathsf{path}} \subseteq$ postBQP, that is, postselection is more powerful taken in conjunction with quantum mechanics than with classical computing. But, exactly how powerful is it? Aaronson showed that giving the ability to postselect on outcomes occurring with exponentially small probability would grant a quantum computer enormous power. Indeed, the class postBQP is as powerful as the class PP:

Theorem 2. postBQP = PP

We recall that in the definition of the class PP, we considered a Non Deterministic Turing Machine (NDTM) with 2^n possible computational paths, with s being the number of computational paths leading to a 1. If half or more of these paths yield a 1, i.e. $s \geq 2^{n-1}$, then the computation is said to accept, whereas if $s < 2^{n-1}$ it is said to reject. Thus, in the worst case scenario, the error probability might be exponentially small.

In the next section, we review the proof of theorem 2. First, it is shown that postBQP $\subseteq$ PP, and then that PP $\subseteq$ postBQP.

The Proof of postBQP = PP

First, the inclusion postBQP $\subseteq$ PP is shown by proving that if the PP-complete problem MAJSAT can be decided, then membership in postBQP may be determined. Given a standard quantum circuit, let $|\psi\rangle = \sum_{z_1 \ldots z_n} \alpha_{z_1 \ldots z_n} |z_1 \ldots z_n\rangle$, where $\alpha_{z_1 \ldots z_n} \in \mathbb{C}$, be the state before the final measurement is performed. Next, the first qubit is measured in the computational basis and we postselect on the outcome 1 occurring, which thus yields the state $|\psi\rangle = \sum_{1 \ldots z_n} \alpha_{1 \ldots z_n} |1 \ldots z_n\rangle$. Next, the second qubit is measured, and let $k \in \{0, 1\}$ be the measurement outcome obtained, which thus results in the state $|\psi\rangle = \sum_{1k \ldots z_n} \alpha_{1k \ldots z_n} |1k \ldots z_n\rangle$, occurring with probability $p_k = \sum_{i,j} \alpha_i^{[1k \ldots z_n]} \alpha_j^{[1k \ldots z_n]}$. In order to determine whether this is an accepting or rejecting instance, we must be able to calculate the probability p_k, and determine which of p_0 or p_1 is greater. The claim is that this question lies in the complexity class PP, and that hence being able to solve MAJSAT will also allow us to decide this question.

First, each complex coefficient may be expressed as an infinite sum of rational numbers a_i, each thus classically efficiently computable, giving $\alpha_z = \sum_{i=1}^{N} a_i^{[z]}$. The probability of obtaining outcome k can be split into positive and negative contributions S_k^+ and S_k^-, thus giving $\mathrm{P}[k] = S_k^+ + S_k^-$. The positive contributions are given by $S_k^+ = \sum_{\substack{z_2 \ldots z_n \\ a_i a_j \geq 0}} a_i^{[1k \ldots z_n]} a_j^{[1k \ldots z_n]}$ and the negative ones by $S_k^- = \sum_{\substack{z_2 \ldots z_n \\ a_i a_j < 0}} a_i^{[1k \ldots z_n]} a_j^{[1k \ldots z_n]}$. We thus seek to ascertain whether the $\mathrm{P}[0] > \mathrm{P}[1]$, that is whether the inequality $S_0^+ + S_0^- > S_1^+ + S_1^-$ holds. This may be rearranged as $S_0^+ - S_1^- > S_1^+ - S_0^-$, and we can now define the left hand side of the equation as the number of accepting paths of a NDTM, and the right hand side as the number of rejecting paths. This belongs to PP, and thus we have that postBQP $\subseteq$ PP.

The second part of the proof is to show the inclusion PP $\subseteq$ postBQP. This means that the ability to postselect on a quantum circuits allows us to decide whether the majority of paths of a NDTM are accepting or not. More specially, given an NDTM with 2^n computational paths, each leading to a 1 or a 0, we are asked to determine whether $s < 2^{n-1}$ or $s \geq 2^{n-1}$, where s is once again the number of accepting paths.

The first step is to prepare a quantum state $|\psi\rangle$ which encodes the number of accepting paths s in its complex amplitudes:

$$|\psi\rangle = \frac{(2^n - s)|0\rangle + s|1\rangle}{\sqrt{(2^n - s)^2 + s^2}}. \tag{1.93}$$

In order to do so, we start with two n-qubit registers, each initialised in the $|0\rangle^{\otimes n}$ state. Next, Hadamard gates are applied to all qubits, resulting in an equal superposition over all computational basis states.

Now, each branch of the n-step computation of the NDTM can be associated with a computational basis state $x = x_1 \ldots x_n$. The output of the NDTM is thus associated to an efficiently

computable boolean function $f(x) : \{0,1\}^n \to \{0,1\}$, where we now have: $s = |\{x|f(x) = 1\}|$.

Thus, if a black box applies this function $f(x)$ to the second qubit register, then we obtain: $\frac{1}{2^{n/2}} \sum |i_1 \dots i_n\rangle|f(i_1 \dots i_n)\rangle$. Hadamard gates are then applied to every qubit in the first register, which results in the state $\frac{1}{2^n} \sum_i \sum_j |j_1 \dots j_n\rangle|f(i_1 \dots i_n)\rangle$. Finally, each qubit in the first register is measured in the computational basis, the measurement is postselected on the outcome being $|0\rangle^{\otimes n}$ and we thus have that:

$$\frac{1}{2^n}|0\rangle^{\otimes n} \sum_{i_1,\dots,i_n} |f(i_1 \dots i_n)\rangle = \frac{1}{2^n}|0\rangle^{\otimes n}\big((2^n - s)|0\rangle + s|1\rangle\big), \tag{1.94}$$

thus yielding the sought after state $|\psi\rangle$ on the second register.

A new single qubit state $\alpha|0\rangle + \beta|1\rangle$ is prepared, and a controlled-Hadamard gate is applied to $|\psi\rangle$, which results in the two qubit state:

$$\alpha|0\rangle|\psi\rangle + \beta|1\rangle H|\psi\rangle = \alpha(2^n - s)|0\rangle|0\rangle + \alpha s|0\rangle|1\rangle + \beta 2^n|1\rangle|0\rangle + \beta(2^n - 2s)|1\rangle|1\rangle. \tag{1.95}$$

The second qubit is then measured in the computational basis, with outcome 1 postselected upon, which thus leaves the first qubit in the (renormalised) state:

$$\frac{\alpha s|0\rangle + \beta\frac{1}{\sqrt{2}}(2^n - 2s)|1\rangle}{\sqrt{\alpha^2 s^2 + (\beta^2/2)(2^n - 2s)^2}}. \tag{1.96}$$

By dividing both the numerator and the denominator by αs, we obtain:

$$|\psi(\beta/\alpha)\rangle = \frac{|0\rangle + \frac{\beta}{\alpha}\frac{1}{\sqrt{2}}(2^n - 2s)/s|1\rangle}{\sqrt{1 + \beta^2/\alpha^2(1/2)(2^n - 2s)^2/s^2}}. \tag{1.97}$$

The goal is to determine whether $s < 2^{n-1}$ or $s \geq 2^{n-1}$. First, we consider the case when less than half of the paths are accepting i.e $s < 2^{n-1}$, with $s \geq 1$, and obtain the following inequality:

$$\frac{1}{2^n} \leq \frac{1}{\sqrt{2}}\frac{(2^n - 2s)}{s} < 2^n. \tag{1.98}$$

Until now, there were no constraints on the allowed values of the complex coefficients α and β. Now, it is required that $\beta/\alpha = 2^i$, where $i \in [-n, n-1]$:

$$|\psi(2^i)\rangle = \frac{|0\rangle + 2^i\frac{1}{\sqrt{2}}(2^n - 2s)/s|1\rangle}{\sqrt{1 + 2^{2i}(1/2)(2^n - 2s)^2/s^2}}, \tag{1.99}$$

which can be expressed as:

$$\frac{|0\rangle + 2^i\theta|1\rangle}{\sqrt{1 + 2^{2i}\theta^2}}, \tag{1.100}$$

with $\theta = \frac{1}{\sqrt{2}}(2^n - 2s)/s$ and $\frac{1}{2^n} \leq \theta < 2^n$. As both coefficients are positive, this is a state which lies in the first quadrant .

In the special case when $\theta = 2^{-i}$, which satisfies the above inequality, we obtain the $|+\rangle$ state. For arbitrary values of $\theta = 2^i \pm \varepsilon$, the state $|\psi(2^i)\rangle$ will lie on either side of the $|+\rangle$ state. For $i = -n$ the state lies close to the $|0\rangle$ state, and as i increases towards $n - 1$, spans the first quadrant, finally coming closer to the $|1\rangle$ state. Thus, at some point, there is a value of i where $|\psi(2^i)\rangle$ will lie below the $|+\rangle$ state, and $|\psi(2^{i+1})\rangle$ above. One of these, the closest to the $|+\rangle$ state will have maximum overlap, or, at worst, they will both have maximum overlap if $\langle\psi(2^i)|+\rangle = \langle\psi(2^{i+1})|+\rangle$.

The worst case scenario occurs when $|\varphi_1\rangle = \frac{|0\rangle+\sqrt{2}|1\rangle}{\sqrt{3}}$ and $|\varphi_2\rangle = \frac{\sqrt{2}|0\rangle+|1\rangle}{\sqrt{3}}$. Here we have $\langle\psi(2^i)|+\rangle = \langle\psi(2^{i+1})|+\rangle$. Thus we can write $|\langle+|\psi(2^i)\rangle| \geq |\langle+|\varphi_k\rangle| = \frac{1+\sqrt{2}}{\sqrt{6}} > 0.985$, for $k \in \{1, 2\}$.

The second case to consider is when half or more of the paths are accepting: $s \geq 2^{n-1}$. In this case, $2^n - 2s \leq 0$ and we have that $|\psi(2^i)\rangle$ lies in the fourth quadrant. The overlap with the $|+\rangle$ state is then maximal for the state $|0\rangle$, thus providing us with an upper bounded: $|\langle+|\psi(2^i)\rangle| \leq |\langle+|0\rangle| = \frac{1}{\sqrt{2}} < 0.985$.

There are $2n + 1$ choices for i, and for each choice we repeat this procedure n times, and thus the algorithm is repeated a total of $n(2n + 1)$ times. Effectively, we are measuring the final state in the X basis, and sampling from the output probability distribution. In the next section, we consider simulatability, whereby we seek to compare the computational power of a given model to that of a classical device.

1.4.5 Simulatability

We have until now explored how both quantum and classical resources can be exploited in order to perform a computation. We first, in the context of decision and search problems, introduced various classical complexity classes, which allowed us to compare the power of different models of computations using various resources. Crucially, we saw that a quantum computer could solve certain problems faster than a classical device, which motivated our study of different models of this time quantum computation. Yet, however profound these theoretical results might be, building a scalable universal quantum computer remains beyond current experimental capabilities. At the same time, advances in experimental physics allow for non-universal quantum computational to be constructed, and thus the question arises as to the nature of the computation these systems may perform and their corresponding power.

We can model this situation by imagining being given a mysterious black box, which takes an n-bit string x as input and outputs an m-bit string y_x. Given that nothing is know regarding the nature of computation performed in the box, can the computational power of this device be gauged? The first obvious answer would be to break the box apart and study its various components in order

to understand the nature of the computation at hand.

Yet, there exists an alternative which would not require for the physical components of the box to be themselves studied, which instead exclusively focusses on the output of the computation. This is the approach adopted in classical simultability [113–115], where the question is whether a classical device can produce the identical output y_x on a given input x. In the following, we first formally consider and define the question of whether a sampling problem is or not classically efficiently simulatable. This provides us with a measure to judge the power of intermediate models of computation, such as those achieved by the family of IQP circuits. Finally, we discuss a mixed state model of computation, the one clean qubit model, whereby a maximally resource state is utilised in order to perform a non-classical task.

Strong and Weak Sampling

Formally, the input to the computation is an n-bit string x, and the output is an m-bit string y_x, which may take one of $N = 2^m$ possible values $y \in \{y_1, \ldots, y_N\}$. This is thus a random variable where each possible outcome y_i occurs with probability $\mathrm{P}[Y_x = y_i] = p_i$, for $i \in \{1, \ldots, N\}$ and where $\sum_{i=1}^{N} p_i = 1$ and $0 \leq p_i \leq 1$, $i = 1, \ldots, N$. In order to test the power of the device in question, we are in addition given access to a classical computer, which is modelled as a probabilistic Turing Machine whose output is an m-bit random variable $\tilde{Y}_x$.

First, we define weak sampling, where the classical device must output an m-bit string $y = y_1 \ldots y_m$ with probability $\mathrm{P}[\tilde{Y}_x = y]$ equal to $\mathrm{P}[Y_x = y]$. For instance, we can imagine a player being given a balanced coin and asked to simulate the output of a die. Here, given a uniform random bit, the player is asked to output samples according to a specified probability distributions.

More generally, the output of a quantum computer is not the final quantum state, but an output string resulting from its measurement. Thus, we have a probability distribution over the set of orthonormal computational basis states. From this perspective, the computation is simply outputting a sample from this a priori unknown probability distribution. Thus, if our classical computer could output a sample according to the same probability distribution, then the quantum process would be said to be classically simulatable. We note that if quantum computation could be classically efficiently simulatable then we would have that BQP = BPP.

We can extend our definition of weak sampling to allow for a multiplicative error $c \geq 1$:

$$\frac{1}{c}\mathrm{P}[Y_x = y_1 \ldots y_m] \leq \mathrm{P}[\tilde{Y}_x = y_1 \ldots y_m] \leq c\mathrm{P}[Y_x = y_1 \ldots y_m]. \tag{1.101}$$

It is important to note that another type of error can be defined, which is called an additive error. These reflect physical errors occurring throughout the computation stemming from the physical

implementation of the process. As such, these errors are of particular relevance in order to model the processes in a laboratory.

Previously, when defining complexity classes where errors could occur on output, we saw that if the error was at most polynomial, then we could repeat the process, and by majority vote get the correct answer, i.e. make it close to one. This thus gives us an estimate of the output probabilities up to a polynomial precision. Effectively, this models the situation that would occur given access to a quantum computational device. Thus, we can ask in turn whether a classical computer could provide us with an estimate of this probability to polynomial precision? That is, if the following can be achieved,

$$|\mathrm{P}[\tilde{Y}_x = y_1 \dots y_m] - \mathrm{P}[Y_x = y_1 \dots y_m]| \leq \frac{1}{\mathrm{poly}(n)}, \tag{1.102}$$

then the quantum device is said to be weakly efficiently simulatable to additive error.

Finally, we define the more powerful notion of strong simulatability, where we not only ask for the complete probability distribution to be explicitly computed but also for all its marginals. Thus, if a system can be strongly simulated then it can be weakly simulated, but not vice versa. This is a much stronger requirement than could be achieved by a quantum computer, and thus we shall henceforth exclusively consider weak sampling.

We next consider non-universal models of computation, and use the above defined notion of simulatability in order to gauge whether these may be deemed non-classical.

Intermediate Models of Computation

We have until now exclusively considered universal models of computation, whereby an arbitrary unitary operator was to be implemented. Here, we ask whether interesting—or more precisely non-classical—models of computation which are at the same time non-universal can be built. This could be done by limiting the resources we have access to, by for example placing restrictions on the allowed gate set.

First, this approach allows the study of more realistic models of computation, that is, models which may be implemented in a laboratory and which showcase a quantum speed-up. Secondly, this in turn allows us to fine grain our understanding of what are the non-classical elements required for a computational speed-up, and thus allows us to probe the boundary between quantum and classical computation.

For example, the Gottesman Knill theorem established that quantum circuits with input $|0\rangle^n$ acted upon by a polynomial amount of Clifford gates are classically efficiently simulatable. Yet, if we allow magic states then universality is regained. Alternatively, one can search for non-universal models which are nonetheless non-classical [116–119], yielding new models such as IQP circuit families or the one clean qubit model of computation, which shall be introduced in the following

sections.

IQP Circuits

The family of IQP—Instantaneous Quantum Polytime—circuits [52–54] corresponds to a quantum computation whereby the quantum circuit is constructed from a set of commuting gates. Here, as all the gates commute, the order in which these are applied does not matter. It is thus an unstructured form of computation, where all the gates could be applied in a single round. Moreover, such a gate set is not universal, and thus radically limits the class of computations which might be performed.

Formally, the family of IQP circuits will be required to satisfy the uniformity condition, and they are defined as follows:

Definition 2. *An IQP circuit with classical input bit string x of size $|x| = n$, acting on $N \geq n$ qubits consists of a quantum register prepared in the input state $|x\rangle|0\rangle^{\otimes N-n}$. Next, a unitary operator U is applied to the register, where U is diagonal with respect to the eigenbasis of Pauli-X operators. Finally, every single qubit is measured in the computational basis, yielding an N-bit string Y.*

Here, we note that the output is an n-bit string resulting from a measurement of every single qubit, and thus corresponds to sampling problems. In the next section, we consider the computational power of such circuit families.

Sampling from commuting circuits

On first impression, one might think that IQP circuits would fail to exhibit any form of non-classical behaviour due to the commuting structure of the gate set. And indeed, it is true that if only a single or even logarithmic (in input size) number of qubits were measured, then this process would be classical. But, if a polynomial number of qubits are measured, striking new behaviour emerges. Indeed, it was shown [53] that it if were possible to weakly sample from IQP circuits up to multiplicative error $1 \leq c < \sqrt{2}$, then this would entail a collapse of the polynomial hierarchy. Thus, as the levels of the polynomial hierarchy are hypothesised to be distinct, this leads to the conclusion that IQP circuits are essentially non-classical.

It is interesting to note that the proof of this relied on the use of postselection. Indeed, it is first shown that postIQP = postBQP = PP, where postIQP corresponds to IQP circuit families taken in conjunction with postselection. This, in itself, is not a surprising result, as postselection is an extremely powerful tool. Now, if IQP circuits could be weakly simulated up to multiplicative error $c \geq 1$, that we would have that IQP $\subseteq$ BPP. This in turn implies that postIQP $\subseteq$ postBPP, which is itself contained within the third level of the polynomial hierarchy BPP $\subseteq \mathsf{PH}_3$. Thus, when these two results are combined yields PP $\subseteq \mathsf{PH}_3$, and thus the polynomial hierarchy collapses to the third

level. Given the extreme implausibility of this result, we are forced to conclude the following: our assumption that IQP circuits were weakly simulatable was wrong, and that despite their seemingly simple structure they thus exhibit non-classical behaviour.

We will now finally consider another model of non-universal computation, whereby both pure and mixed states are utilised.

One Clean Qubit Model

Until now, we have exclusively considered noiseless models of computation which rely on the experimental ability to prepare a polynomial number of qubits in a pure state. In contrast, the one clean qubit model considers the class of computations that might be performed given access to a noisy resource state [52]. More specifically, we are given access to a single pure qubit in the state $|0\rangle$ and n qubits in the maximally mixed state $\frac{1}{2^n}\mathbb{1}_n$.

First, a Hadamard gate is applied to the clean qubit:

$$\frac{1}{2}\sum_{i,j}|i\rangle\langle j|\otimes\frac{\mathbb{1}_n}{2^n}. \tag{1.103}$$

Next, an arbitrary controlled-unitary operator U is applied to the n qubits, with the first qubit as the control:

$$\sum_{i,j}\frac{1}{2}|i\rangle\langle j|\otimes\frac{1}{2^n}U^iU^{j\dagger}. \tag{1.104}$$

Finally, the first qubit is measured in the X basis.

The probability of obtaining outcome $m = 0$ is then given by the following expression:

$$\mathrm{P}[0] = \mathrm{Tr}\Big((|+\rangle\langle+|\otimes\mathbb{1}_n)\sum_{i,j}\frac{1}{2}|i\rangle\langle j|\otimes\frac{1}{2^n}U^iU^{j\dagger}\Big), \tag{1.105}$$

which may be simplified to $\mathrm{P}[0] = \frac{1}{4}\frac{1}{2^n}\sum_{i,i}\mathrm{Tr}(U^iU^{\dagger i})$. Next, by expanding the sum we obtain: $\mathrm{P}[0] = \frac{1}{4}\frac{1}{2^n}\big(2\mathrm{Tr}\mathbb{1}_n + \mathrm{Tr}U + \mathrm{Tr}U^\dagger\big)$. Thus, finally we have that:

$$\mathrm{P}[0] = \frac{1}{2}\Big(1 + \frac{1}{2^n}\mathbb{Re}\ \mathrm{Tr}(U)\Big) \tag{1.106}$$

Thus, the outcome probability encodes information about the trace of the unitary operator.

This provides us with the insight that even given to a single pure state, we can exploit a maximally mixed state as a resource in order to learn properties of the operator which was applied. Thus, we have seen that computation in a mixed state framework can be both meaningful and powerful.

Chapter 2

Noisy Measurement-Based Quantum Computation

Quantum computing is a new and powerful paradigm of computation. Although a plethora of results have been obtained on both the theoretical and experimental fronts, a scalable quantum computer is yet to be built. Both the models of unitary quantum circuits and MBQC provide us with a blueprint on how to achieve computation using quantum systems. Yet, both of these are fundamentally noiseless models of computation, which require that pure states be experimentally prepared which are subsequently acted upon by unitary gates, before finally being measured. In contrast, quantum systems are sensitive noise. From preparation to measurement, noise affects quantum states and operations, thus corrupting the computation and rendering the output useless.

Computation in the presence of noise

Fault tolerance can be achieved by building error correction codes. Here, errors are first detected by performing measurements and then corrected by applying relevant operations, thus recovering the framework of pure states undergoing unitary evolution. But, motivated by the one clean qubit model of computation, we ask whether a mixed state model could be used in order perform a non-trivial computation. This would enable us to understand the connection between physical errors acting on quantum states and logical errors acting on the computation. Furthermore, such a model could be used in order to simulate noisy systems and computations.

Thus, the first question to be addressed is what is meant by the general term of noise. A priori, noise refers to any process whereby information is corrupted, thus resulting in an uncertainty regarding the state of the system. A priori, the breadth of operations and models which could cause this transition from a pure state formalism to a mixed one is daunting. Yet, it has been shown that a wide class of physical behaviour can be captured by modelling noise as a single qubit local Pauli

operator acting probabilistically on the system.

Noise in one-dimensional MBQC

This would thus result in Pauli operators being probabilistically applied to the state, which would cause errors on the computation. This is reminiscent of the random by-product operators previously encountered within the context of MBQC, where the outcome of a measurement revealed whether a random Pauli by-product operator had been applied or not. As all the operators involved were Clifford operators, the effect of the unwanted Pauli gates could be tracked throughout the computation. This could either then lead to an unimportant global phase, or alternatively require for adaptive measurements to be implemented in order to compensate for the randomness.

One-dimensional MBQC refers to MBQC performed on a cluster state of dimension one, i.e. qubits placed on a line. It has been shown that a computation performed on a one-dimensional resource state is classically efficiently simulatable [28, 120–122], and thus two or three dimensional resource states are typically considered. Nonetheless, the study of one-dimensional MBQC has allowed for interesting results, such as for different families of resource states to be studied, and in addition, it has notably been shown that one-dimensional MBQC can be represented with Matrix Product States (MPS) [25, 77–79].

From physical to logical noise

With this in mind, we ask whether by extending MBQC to a mixed state model of computation we might be able to analyse the effect of local noise acting on the computation to be performed. This would require for noise processes to be modelled as local channels, and our aim would be to map noise acting on physical states to logical noise acting on the computation, thus allowing us to determine the experimentally implemented noisy computation. Moreover, understanding how these interact with the adaptive measurements would then allow us to understand whether there exists certain classes of noise models which can be tolerated.

Finally, it has been customary to assume that errors occurring throughout the computation consist of Pauli operators probabilistically applied to the state. However, it has recently been proposed that exclusively focusing on Pauli noise could lead underestimating error rates[123], and that thus more general noise models should be considered.

Structure

In this chapter, we shall seek to investigate the question of modelling noise in one-dimensional MBQC. In order to do so, we shall first introduce in section 2.1 various common channels, such as Pauli channels, the unital channel and the dephasing channel, which shall subsequently be used to

model the noise acting throughout the computation. Next, in section 2.2 we return to the one-bit teleportation protocol, and consider the case where the resource state has been corrupted by a local noise process. This motivates section 2.3, whereby we introduce a mixed model of computation for MBQC on a one-dimensional cluster state, and study the effect local noise channels on the computational output. In chapter 1, the MPS formalism was shown to naturally lends itself to the study of MBQC in one dimensions. Thus, in section 2.4, we first develop a generalisation to mixed states, known as Matrix Product Operators (MPO), which we then apply to the study of mixed one-dimensional MBQC in section 2.5. Finally, in section 3.4, we discuss both our results and directions for future work.

2.1 Models of Noise

A simple yet powerful model of a noise process is given by a local single qubit noise channel. Here, given an initial state ρ, an error will occur with probability p, thus potentially modifying the quantum state. This is modelled by a CPTP map acting on the input state ρ and mapping it to a new, possibly unknown, state $\rho' = \varepsilon(\rho)$, as depicted in Fig. 2.1. This channel may be expressed as a Kraus decomposition $\rho' = \sum_m p_m K_m \rho K_m^\dagger$, with Kraus operators K_m satisfying the relation $\sum_m K_m^\dagger K_m = \mathbb{I}$.

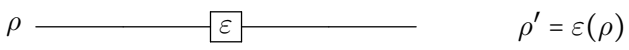


Figure 2.1: *Single qubit quantum channel.* The initial state ρ is mapped to a new state $\rho' = \varepsilon(\rho)$ by the application of a quantum channel.

However useful such models might be, we note that these are ultimately local, and that thus the errors occurring on different qubits are uncorrelated. In the following, we shall discuss various examples of common noise channels, starting with Pauli channels in section 2.1.1, before considering the unital channel in section 2.1.2 and finally the dephasing channel in section 2.1.3.

2.1.1 Pauli Channels

A Single Pauli Error

We first consider the special case where a single Pauli operator is applied to the state with probability p. The bit flip channel maps computational basis states $|i\rangle$ to $|i \oplus 1\rangle$ with probability p and leaves them invariant with probability $1 - p$. This corresponds to a Pauli operator X being applied with probability p, which can be represented as a quantum channel with Kraus operators $K_s = \sqrt{p_s} X^s$,

$s = 0, 1$, and thus the input state ρ evolves according to:

$$\rho \to (1-p)\rho + pX\rho X. \tag{2.1}$$

Another example of a Pauli channel is the phase flip channel, which has the effect of probabilistically adding a phase factor of (-1) to the $|1\rangle$ state. This corresponds to a Pauli operator Z being applied with probability p, which can be expressed as a channel with Kraus operators $K_s = \sqrt{p_s}Z^s$, $s = 0, 1$. In this case, the input state ρ will evolve according to:

$$\rho \to (1-p)\rho + pZ\rho Z. \tag{2.2}$$

Finally, we consider the effect of applying a Pauli Y operator with probability p. The Pauli Y may be expressed in terms of Pauli operators X and Z as $Y = iXZ$, and thus a Y error can be interpreted as a Z error followed by an X error. This corresponds to a combination of both the phase and bit flip channels being applied, and thus results in the bit-phase channel. Here, the Kraus operators are given by $K_s = \sqrt{p_s}Y^s$, $s = 0, 1$, and thus the input state evolves according to:

$$\rho \to (1-p)\rho + pY\rho Y. \tag{2.3}$$

Next, we consider quantum channels whereby multiple Pauli errors might occur.

Depolarising Channel

The depolarising channel maps the initial quantum state to the maximally mixed state with probability p:

$$\rho \to (1-p)\rho + \frac{p}{2}\mathbb{1}. \tag{2.4}$$

It can easily be seen that the identity operator may be expressed as:

$$\frac{1}{2}\mathbb{1} = \frac{1}{4}(\rho + X\rho X + Z\rho Z + Y\rho Y), \tag{2.5}$$

and thus we can substitute equation 2.5 into 2.4, which by rearranging gives:

$$\rho \to (1 - \frac{3p}{4})\rho + \frac{p}{4}(X\rho X + Z\rho Z + Y\rho Y). \tag{2.6}$$

Thus, the depolarising channel corresponds to a quantum channel where every single Pauli operator occurs with probability $\frac{p}{4}$. For example, if all the information pertaining to the state is lost, then it is effectively mapped to the maximally mixed state with probability $p = 1$. Thus, by rearranging equation 2.6, it can be seen that this corresponds to the application of the quantum channel given

by:

$$\rho \to \frac{1}{4}\sum_{ab}\sigma_{ab}\rho\sigma_{ab}, \tag{2.7}$$

which is called the the completely depolarising channel. Next, we consider the more general case where a unitary operator is probabilistically applied to the initial state.

2.1.2 Unital Channel

A unital channel is one under which the maximally mixed state is invariant. For example, this occurs when a single qubit unitary operator U is applied to the state with probability p. In this case, the Kraus operators are proportional to unitary operators, and the quantum state evolves according to:

$$\rho \to (1-p)\rho + pU\rho U^{\dagger}. \tag{2.8}$$

Next, the unitary operator U can be decomposed in the Pauli basis as $U = \sum_{i,j} u_{ij}\sigma_{ij}$, and by substituting this expression into equation 2.8, we get that the input state evolves according to:

$$\rho \to (1-p)\rho + p\sum_{i,j}\sum_{k,l} u_{ij}u^{*}_{kl}\sigma_{ij}\rho\sigma_{kl}. \tag{2.9}$$

Thus, the effect of an arbitrary unitary operator acting probabilistically on a quantum state can be determined by studying the effect of the individual Pauli operators. This approach will later be generalised in our study of noise in one-dimensional MBQC, in order to analyse the effect of general noise models in terms of Pauli errors. Next, the last channel we introduce is the dephasing channel, whereby the initial quantum state is rendered diagonal with respect to a given basis.

2.1.3 Dephasing Channel

The dephasing channel has the effect of diagonalising the input state with respect to a specified basis. For example, if a Pauli Z operator is applied with probability $\frac{1}{2}$, then the state will become diagonal in the computational basis. Thus, we speak of dephasing channels with respect to a specified eigenbasis, where the associated operator is being applied with probability p. The effect of such a channel is to destroy the coherence of the state in the associated eigenbasis. More generally, the quantum state will undergo the mapping:

$$\rho \to \rho + pO\rho O^{\dagger}, \tag{2.10}$$

where the state will now be diagonal with respect to the eigenbasis of the observable O.

This concludes our discussion of frequent single qubit noise channels which may be encountered and the effect of which we ultimately seek to determine. In order to study this question, we will first

consider the case of noisy teleportation, whereby the resource state has been affected by noise.

2.2 Motivation: Teleportation with Mixed States

The entanglement present between two or more qubits is a resource which can be exploited for quantum computation and communication tasks. For instance, a two-qubit resource state is prepared in a laboratory, before one qubit is given to Alice and the other to Bob. Alice then comes across an arbitrary single qubit mixed state $\rho = \sum_{u,v} \alpha_{uv} |u\rangle\langle v|$ which she wishes to teleport to Bob by performing a Bell measurement on her pair of qubits, as illustrated in Fig. 2.2. She knows that if the shared resource is a maximally entangled pure Bell state then this is possible up to some additional Pauli operators which will depend on her measurement outcome. Sending these two bits of information to Bob will allow him to undo the Pauli operators, and he will thus be in possession of the original unknown state ρ.

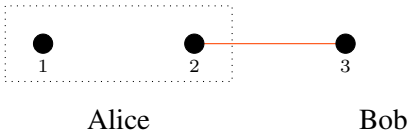


Figure 2.2: *Teleportation.* Alice is in possession of the two leftmost qubits (labelled 1 and 2), on which she shall perform a Bell measurement (illustrated with the dotted box), whilst Bob has the qubit on the right (labelled 3). The qubits 2 and 3 are the entangled resource state, which is diagonal in the Bell basis.

Crucially, this protocol relies on our ability to prepare the pure maximally entangled two-qubit Bell state:

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.11}$$

In the following, we ask what would be the effect of instead having access to a noisy mixed resource state. This is modelled by the application of a single qubit local Pauli channel to the originally entangled state $|B_{00}\rangle$.

More specifically, we here consider the special case where one half of the entangled Bell state goes through a local Pauli channel. This approach is connected to the Choi-Jamiolkowski isomorphism, previously discussed in chapter 1, where a quantum channel can be fully specified by looking at its effect on half of a maximally entangled state. This in turn determines the Choi matrix, which completely characterises the applied quantum channel and maps the effect of the CPTP map on each operator basis state.

First, in section 2.2.1, we consider the effect of applying an arbitrary Pauli channel to half

of the original resource state. Next, in section 2.2.2, we consider the special case of a resource state diagonal in the Bell basis, and determine, through proposition 1 its effect on the teleportation protocol. Finally, we applied this result to a couple of examples of noise models by considering the bit flip and phase flip channels.

2.2.1 Mixed resource states

In the following, we consider the case where a local Pauli channel is applied to the second qubit of the pure resource state $|B_{00}\rangle$, which will thus evolve to a new mixed state given by:

$$\Lambda = \sum_{i,j} \frac{1}{2} |i\rangle\langle j| \otimes \varepsilon(|i\rangle\langle j|, \tag{2.12}$$

and ask whether such a state may still be used as a resource. The applied quantum channel corresponds to Pauli operators $X^k Z^l$ applied with probability p_{kl} to the second qubit of the entangled pair $|B_{00}\rangle$, although we note that the first qubit could equivalently have been chosen. The effect of applying a Pauli operator σ_{ij} to the Bell state will be to evolve it to another orthogonal Bell state $|B_{ij}\rangle = \frac{1}{\sqrt{2}}(\mathbb{I} \otimes X^i Z^j)(|00\rangle + |11\rangle)$.

Once again, the quantum channel ε implements a CPTP map, with Kraus operators $K_{kl} = \sqrt{p_{kl}} X^k Z^l$, and thus the resource state can be expressed as:

$$\Lambda = \sum_{k,l} \sum_{i,j} \frac{1}{2} p_{kl} (\mathbb{1} \otimes X^k Z^l) |ii\rangle\langle jj| (\mathbb{1} \otimes Z^l X^k), \tag{2.13}$$

which we shall henceforth refer to as a diagonal resource state. Indeed, the set of four Bell states form an orthonormal basis, and we can thus express any arbitrary two-qubit state as $\rho = \sum \rho_{ijkl} |B_{ij}\rangle\langle B_{kl}|$, where $\rho_{ijkl} \in \mathbb{C}$. In particular, the state is said to be diagonal in the Bell basis if it can be expressed as $\rho = \sum_{ij} \rho_{ij} |B_{ij}\rangle\langle B_{ij}|$, where $\rho_{ij} \in \mathbb{C}$.

2.2.2 Diagonal Bell States as Resource

We will thus now consider the special case of teleportation when the resource state is diagonal in the Bell basis. In this case, we might think that having access to a noisy resource state would destroy the teleportation protocol. Yet, if ρ is the unknown state we seek to teleport, we can show that in the case of resource state diagonal in the Bell basis, it is $\varepsilon(\rho)$ which will be teleported across, where ε refers to the original noise channel. Thus, this is equivalent to a noise channel acting directly on the original input state. More formally:

Proposition 1. *Given a resource state diagonal in the Bell basis, the application of the teleportation protocol will result in the state $X^s Z^t \varepsilon(\rho) Z^t X^s$ being teleported.*

Proof. If we express the state on the first two qubits in the Bell basis, then the state of the joint system $\rho \otimes \Lambda$ is given by:

$$\rho \otimes \Lambda = \frac{1}{4} \sum_{u,v} \sum_{i,j} \alpha_{uv} (-1)^{uk_1 + vk_2} |B_{u\oplus i, k_1}\rangle\langle B_{v\oplus j, k_2}| \otimes \varepsilon(|i\rangle\langle j|). \tag{2.14}$$

Next, the first two qubits are measured in the Bell basis $(P_{st} \otimes \mathbb{1})(\rho \otimes \Lambda)(P_{st} \otimes \mathbb{1})$, where $P_{st} = |P_{st}\rangle\langle P_{st}|$. The orthogonality of Bell states will require that we have $s = u \oplus i = v \oplus j$ and $t = k_1 = k_2$, which translates to:

$$(P_{st} \otimes \mathbb{1})(\rho \otimes \Lambda)(P_{st} \otimes \mathbb{1}) = \frac{1}{4} \sum_{u,v,k,l} \alpha_{uv} (-1)^{(u+v)t} P_{st} \otimes K_{kl} X^s |u\rangle\langle v| X^s K_{kl}^\dagger, \tag{2.15}$$

$$= \frac{1}{4} \sum_{u,v,k,l} \alpha_{uv} P_{st} \otimes K_{kl} X^s Z^t |u\rangle\langle v| Z^t X^s K_{kl}^\dagger, \tag{2.16}$$

$$= \frac{1}{4} \sum_{k,l} P_{st} \otimes X^s Z^t K_{kl} \rho K_{kl}^\dagger Z^t X^s, \tag{2.17}$$

$$= \frac{1}{4} P_{st} \otimes X^s Z^t \varepsilon(\rho) Z^t X^s. \tag{2.18}$$

We can see that the state $\varepsilon(\rho)$ has been teleported instead of the original state ρ, and thus the quantum channel can be thought of as acting directly on the input state itself. □

Next, we consider a couple of examples of such noise channels affecting the resource state, and apply proposition 1 in order to determine what state has been teleported. This will allow us to observe the trade-off taking place between the amount of noise affecting the resource state and the entanglement left to be exploited.

2.2.3 Noisy teleportation: examples

First, we consider the worst case scenario of a completely noisy resource state, and find that, as expected, no information will be transmitted.

Example 1. *The application of the completely depolarising channels, with corresponding Kraus operators $K_{ij} = \frac{1}{4}\sigma_{ij}$, for $i, j = 0, 1$ results in the resource state being transformed to the maximally mixed state. From proposition 1, the completely depolarising channel is applied to the transmitted state ρ. Thus, it will now be transformed to the maximally mixed state. This gives us absolutely no information as to what the unknown state ρ was, and our interpretation is that nothing has been teleported.*

Next, we consider the case when a dephasing channel with respect to the computational basis is applied, and find that in this case information has been teleported.

Example 2. *When the dephasing channel with respect to the computational basis is applied, the resource state gets mapped to an equal mixture of the two Bell states* $|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ *and* $|B_{01}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$*. We thus have that the resource state can be expressed as* $|\Lambda\rangle = 0.5|B_{00}\rangle + 0.5|B_{01}\rangle$*, which is a separable state. As a channel, this corresponds to Kraus operators* $K_m = \frac{1}{\sqrt{2}}Z^m$*. From Proposition 1, we have that the teleported output state is now be given by* $0.5\sum_s X^s Z^t Z^m \rho Z^m Z^t X^s$*. Thus, enough entanglement has been left in the resource state in order to perform a non-trivial task.*

Thus, the effect of a having access to a noisy resource state can be observed in the output of the computation, which crucially will depend on the noise channel that occurred. This thus motivates our study of one-dimensional MBQC within the context of a noisy resource state, and in the next section, we introduce a framework which will allow us to map the effect of local noise channels acting on the state onto the computation.

2.3 Noise in MBQC via One Bit Teleportation protocol

In chapter 1, the MBQC model of quantum computation was introduced, whereby the computation is implemented by performing single qubit adaptive measurements on an entangled resource state. The resource state considered was the cluster state, which consists of qubits organised in a lattice geometry initialised in the $|+\rangle$ state and where nearest neighbours are entangled via a control-Z operation. A measurement results in the application of a unitary operator to the input state, up to some random by-product operators. In order to model the experimental computation, we now wish to develop a generalisation of this model to mixed states.

Our approach to this problem, in section 2.3.1, will be to first break down pure state MBQC into a sequence of fundamental "building block" of the computation. These blocks can then be concatenated in order to form a greater and more powerful structure. In section 2.3.2, we will discuss a couple of simple examples in order to gain an intuition as to the noise propagation within the building block. This will thus allow us, in section 2.3.3 to generalise one-dimensional MBQC to mixed states by applying local noise channels to the building block. Doing so will allow us to study the effect of the local noise channel on the output state, in a similar approach to that adopted in the previous section. We will argue that by concatenating such noisy blocks, we can model the effect of noise in the computation, by realising how noise affecting the physical state gets mapped to noise on the computation. Finally, in section 2.3.4, we will consider various examples illustrating how the derived formalism can be applied to the study of logical errors.

2.3.1 The Noiseless Model

The Building Block

The fundamental building block of one-dimensional MBQC is given by a two qubit state, where the first qubit is in an arbitrary mixed state ρ and where the second qubit is a pure qubit initialised in the $|+\rangle$ state, which are then entangled via a controlled-Z gate. Finally, a measurement of either the observable Z or $R_z(\phi)XR_z(-\phi)$ is performed, yielding measurement outcome k.

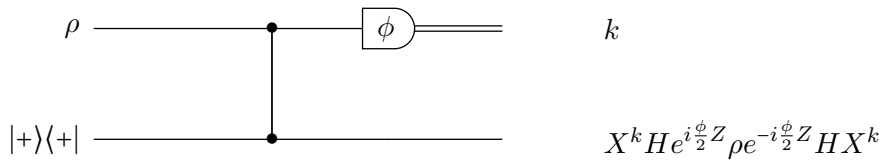


Figure 2.3: *The MBQC building block for a measurement in the equatorial basis.* The two qubits are entangled via a controlled-Z gate, and the first qubit is measured in the equatorial plane of the Bloch sphere with measurement outcome k.

This is illustrated in Fig. 2.3, where ϕ refers to the observable $R_z(\phi)XR_z(-\phi)$, and where the application of the circuit results in the state ρ being teleported onto the second qubit, with the added application of the unitary operator $He^{i\frac{\phi}{2}Z}$, which is dependent on the measurement basis, as well as a potential random Pauli by-product operator.

Block Notation

Henceforth, for ease of notation, we shall say that the observable i is measured where i corresponds to either Z or ϕ. Thus, the more general expression for the building block is depicted in Fig. 2.4, where we have introduced the superoperator $\varepsilon_{i,k}$ in order to describe the output, which depends on both the measurement bases i and the measurement outcome k.

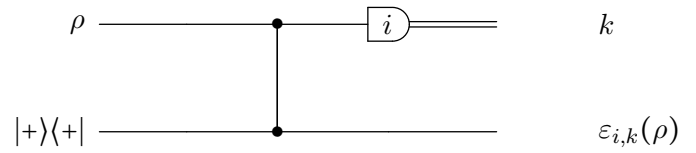


Figure 2.4: *General MBQC building block.* The two qubits are entangled, and the first qubit is measured in basis i which corresponds to either to a measurement in the computational basis or onto the equatorial plane of the Bloch sphere.

In the case of a computational basis measurements, this corresponds to:

$$\varepsilon_{z,k}(\rho) = \frac{1}{2} Z^k \rho Z^k, \tag{2.19}$$

whereas in the case of an equatorial basis measurement we have that:

$$\varepsilon_{\phi,k}(\rho) = \frac{1}{2} X^k H e^{i\frac{\phi}{2}Z} \rho e^{-i\frac{\phi}{2}Z} H X^k. \tag{2.20}$$

Effective Computation

Thus, we can think of each block as implementing a unitary operator on the input state ρ, described by the superoperator $\varepsilon_{i,m}$, as shown in Fig. 2.5. This output state $\varepsilon_{i,m}(\rho)$ can then be used as the input to a new building block.

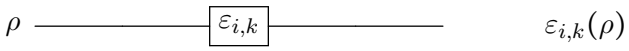


Figure 2.5: *Effective channel implemented by the building block.* The building block effectively implements a quantum channel $\varepsilon_{i,k}$ on the input state ρ where i refers the measurement bases and k the measurement outcome.

Concatenating Blocks

Thus, in the case where the computation requires for L such blocks to be implemented, the final output state is given by:

$$\rho' = \varepsilon_{i_L,k_L} \circ \varepsilon_{i_2,k_2} \circ \ldots \varepsilon_{i_1,k_1}(\rho), \tag{2.21}$$

where $\circ$ denotes the composition of superoperators defined as $\alpha \circ \varepsilon(\rho) = \alpha(\varepsilon(\rho))$, and where $i_j \in \{z, \phi\}$, $k_j \in \{0, 1\}$for $j = 1, \ldots, L$. We note that the measurement bases are still dependent on previous measurement outcomes, although we have for clarity chosen not to explicitly state this dependence.

We have thus now decomposed one-dimensional MBQC as a sequence of building blocks acting on an input state ρ. We shall now focus our attention on the building block itself, and investigate how noise acting on the physical states is mapped to noise acting on the computation. In order to do this, we shall first consider a couple of simple examples in order to develop an intuition as to how noise channels propagate in this model.

2.3.2 Examples: Pauli Noise

In the following we shall consider two examples of local noise acting on the building block, in order to motivate what we shall call either a noisy cluster state or a noisy measurement.

Noisy Cluster State

If a quantum channel acts on the second qubit initialised in the $|+\rangle$ state, then we can interpret this as noise acting on the resource state. If a bit flip channel is applied, then this corresponds to a Pauli X operator being applied probabilistically. As the $|+\rangle$ state is a $+1$ X eigenstate, the qubit will be left invariant under the action of this channel. In contrast, in the case of the phase flip channel, a Z error is applied with probability p, as shown in Fig. 2.6, and its effect will be to transform the $|+\rangle$ state to the mixed state $(1-p)|+\rangle\langle+| + p|-\rangle\langle-|$.

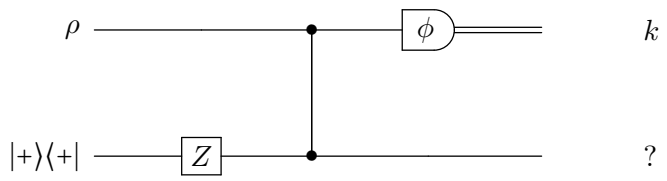


Figure 2.6: *A phase flip channel acts on the resource state.* A Pauli Z operator acts on the ancillary qubit initialised in the $|+\rangle$ state.

On the other hand, as the Z error commutes with the CZ gate, we can view it as being probabilistically applied to the output, which would then result in the state $\sum_s p_s Z^s \varepsilon_{\phi,k}(\rho) Z^s$ being transmitted, where $p_0 = 1-p$ and $p_1 = p$, as illustrated in Fig. 2.7.

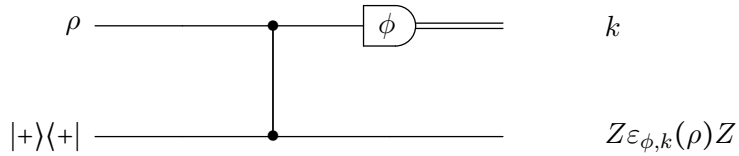


Figure 2.7: *A phase flip channel acts directly on the output.* Effectively, a Pauli operator Z is applied to the output state.

.

Thus, we see that the noise originally acting upon the resource can be mapped to noise acting on the output of the computation. Next, we consider the case of a noisy measurement.

Noisy Measurements

The case when the noise channel is applied to the first qubit just before the measurement is performed is interpreted as a noisy measurement. If for instance the phase flip channel is applied, then an error Z occurs with probability p, as shown in Fig. 2.8.

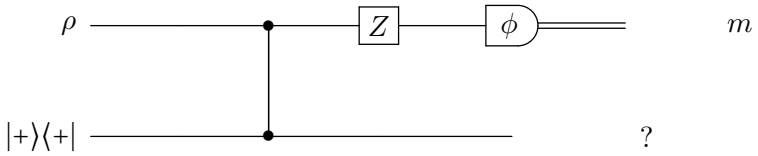


Figure 2.8: *A phase flip channel acts just before the measurement.* A Pauli error Z acts on the first qubit just before the measurement onto the equatorial basis.

This can equivalently be interpreted as a noisy channel acting directly on the input state, as shown in Fig. 2.9. Thus, using the building block picture of MBQC, we can see how Pauli errors occurring in the circuit get mapped to Pauli errors on the output state. This motivates us to adopt a more formal and general approach to the study of local errors in the building block picture.

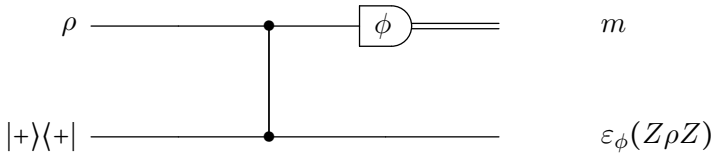


Figure 2.9: *Phase flip channel on input.* A Pauli Z error is applied to the first qubit, the input, just before the channel is applied.

Such an approach would then allow for more general models of single qubit noise acting on the circuit to be analysed. Indeed, it has recently been argued that the ability to model and correct for Pauli noise could prove to be limiting, and that unitary operators acting probabilistically on the state could have a severe effect on the computation. Thus, in the next section we introduce a framework which will allow us to study general single qubit noise models acting on physical states and their effect on the computation.

2.3.3 General Local Noise

We now introduce a framework which will allow for the study of arbitrary noise acting on single qubits, by providing us with a systematic method of mapping errors acting on the circuit to errors

acting on the computation. In order to do so, we will once again consider the fundamental building block which we previously introduced, and consider how errors acting at various locations are transmitted. Henceforth, we shall exclusively consider measurements onto the equatorial plane of the Bloch sphere, as measurements in the computational basis simply have the effect of destroying the entangled between the measured qubit and its neighbours. Thus, we shall now write ε_k for $\varepsilon_{\phi,k}$.

Choi Map

The input state ρ can be decomposed in the computational basis as $\rho = \sum \alpha_{i_0 j_0} |i_0\rangle\langle j_0|$. The Choi matrix C_ε of a CPTP map ε stores the transformed basis states $\varepsilon(|i_0\rangle\langle j_0|)$ of a quantum channel ε, in a similar way to matrices which store transformed basis vectors. By linearity, the Choi matrix thus provides us with a way of computing the output state of a quantum channel. Thus, we henceforth limit our study to that of inputs of the type $|i_0\rangle\langle j_0|$. This, in turn, will allow us to compute the output states of the computation on arbitrary inputs.

Noise Model

The noise model considered will be that of local single qubit noise, represented by a CPTP map having a Kraus representation $\alpha(\rho) = \sum_m K_m \rho K_m^\dagger$. Each of these Kraus operators is a matrix of dimension two, which can thus be decomposed in the Pauli basis:

$$K_m = \sum_{g,h} a_{gh} \sigma_{gh}, \tag{2.22}$$

where we have that $\sigma_{gh} = i^{gh} X^g Z^h$ and $a_{gh} \in \mathbb{C}$.

The noise channel α may act at one of four possible locations, as show in Fig. 2.10. We will now consider each one of the four possible locations wherein the noise channel α might act, and study its effect on the output of the computation. First, we introduce two lemmas which treat the

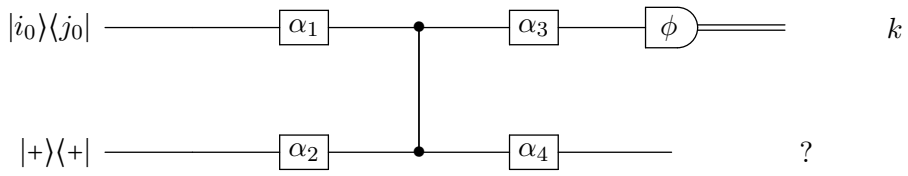


Figure 2.10: *General noise on the building block.* An input $|i_0\rangle\langle j_0|$ is entangled with $|+\rangle\langle +|$ before the first qubit is measured in the equatorial plane of the Bloch sphere. The noise channels α_i may occur at four possible locations, thus disrupting the computation.

two trivial cases of having a noise channel acting directly on the input or output state.

Noise Acting on the Input

In the case when the noise channel α_1 acts directly on the input state, then this new state is simply the input to the building block, resulting in the channel $\varepsilon_k \circ \alpha_1(|i_0\rangle\langle j_0|)$ being implemented, as illustrated in Fig. 2.11

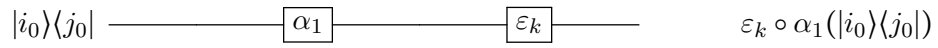


Figure 2.11: *Effective resulting channel: noise on input.* The input $|i_0\rangle\langle j_0|$ undergoes two successive channels, with the noise channel α_1 applied first followed by ε_k.

Lemma 2. *Let α_1 be the single qubit noise channel acting at location* 1*, as shown in Fig. 2.12. Then, the output is given by the channel*

$$\varepsilon_k \circ \alpha_1. \tag{2.23}$$

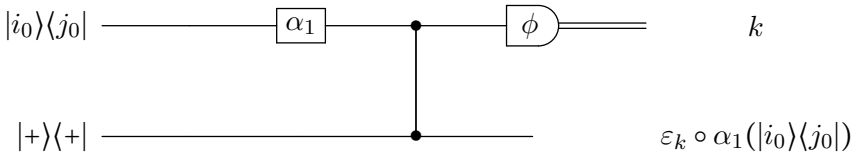


Figure 2.12: *Noise acting on the input state.*The noise channel α_1 acts directly on the input $|i_0\rangle\langle j_0|$, which is thus directly transmitted, resulting in the output $\varepsilon_k \circ \alpha_1(|i_0\rangle\langle j_0|)$.

Proof. This is equivalent to the noise channel α_1 acting on the input state itself, and thus the teleportation protocol is directly applied to $\alpha_1(|i_0\rangle\langle j_0|)$, thus resulting in the state $\varepsilon_k \circ \alpha_1(|i_0\rangle\langle j_0|)$ being transmitted. □

Noise Acting on the Output

In contrast, when the noise channel acts on the output state, then it is the entire teleported output which is acted upon by the channel, and thus the effective channel is given by $\alpha_4 \circ \varepsilon$, as shown in Fig. 2.14

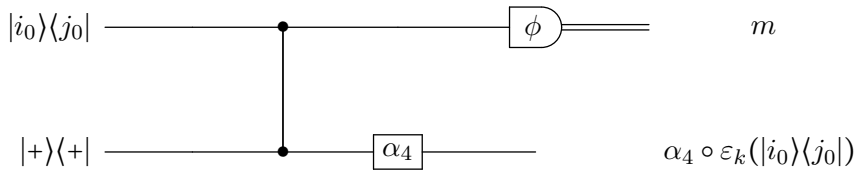


Figure 2.13: *Noise acting on the output.* A local noise channel α_4 acts on the input. This results in the output being $\alpha_4 \circ \varepsilon_k(|i_0\rangle\langle j_0|)$.

Lemma 3. *Let α_4 be the single qubit noise channel acting at location 4, as shown in Fig. 2.13. Then, the output is given by the channel*

$$\alpha_4 \circ \varepsilon_k. \tag{2.24}$$

Proof. Trivial. □

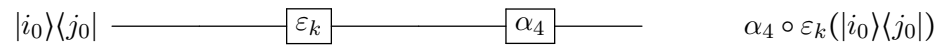


Figure 2.14: *Effective resulting channel: noise on output.* The input $|i_0\rangle\langle j_0|$ undergoes two successive channels: ε_k followed by α_4.

Next, we consider the generalisation of the previously introduced noisy cluster state and noisy measurement examples, where we now study the effect of an arbitrary CPTP map acting on the physical state.

Noisy Cluster State

First, if the noise channel is applied onto the resource, i.e. the second qubit, just before the two qubits are entangled, then this corresponds to a noisy cluster state. MBQC relies on the preparation of a pure cluster state which serves as a reservoir of correlations to be used by the subsequent computation. As we previously saw, noisy resource states are not entirely useless, and thus we shall study computation in the presence of a noisy resource. In order to do so, the noisy cluster state is modelled by the application of a local noise channel acting to the ancillary qubit in the $|+\rangle$ state, as shown in Fig. 2.15.

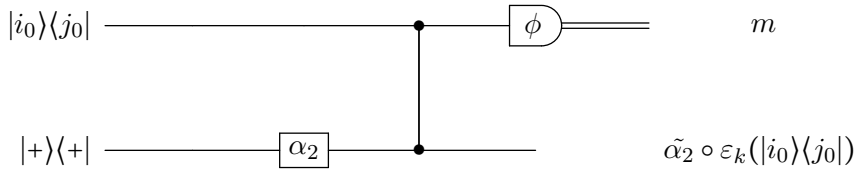


Figure 2.15: *Noise acting on the resource state.* The noise channel α_2 acts directly on the resource, thus resulting in the output $\tilde{\alpha_2} \circ \varepsilon_k(|i_0\rangle\langle j_0|)$.

Lemma 4. *Let α_2 be the single qubit noise channel acting at location 2, as shown in Fig.2.15 and which is expressed in Kraus form $\alpha_2(\rho) = \sum_m K_m \rho K_m^\dagger$. If the Kraus operators are decomposed in the Pauli basis $K_m = \sum_{gh} a_{gh}^{(m)} \sigma_{gh}$, then the output is given by:*

$$\tilde{\alpha_2} \circ \varepsilon_k, \tag{2.25}$$

where the modified channel $\tilde{\alpha}_2(\rho) = \sum_m \tilde{K}_m \rho \tilde{K}_m^\dagger$ has Kraus operators given by:

$$\tilde{K}_m = \sum_u \tilde{a}_{u0}^{(m)} Z^{(m)u}, \tag{2.26}$$

with $\tilde{a}_{u0} = \sum_v (-i)^{uv} a_{uv}^{(m)}$, as shown in Fig. 2.16.

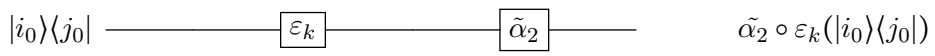


Figure 2.16: *Effective resulting channel: noisy resource.* A noisy resource state effectively corresponds to the channel ε followed by $\tilde{\alpha_2}$ being applied to the input.

Proof. The quantum channel $\alpha_1(\rho) = \sum_m K_m \rho K_m^\dagger$ is applied to the cluster state. Each Kraus operator K_m can be decomposed in the Pauli basis as $K_m = a_{00}^{(m)} \mathbb{I} + a_{01}^{(m)} X + a_{10}^{(m)} Z - i a_{11}^{(m)} ZX$, where $a_{ij} \in \mathbb{C}$ for $i, j = 0, 1$. Here, we know that this channel is applied to the cluster and can thus exploit this information by considering the action of a Kraus operator K_m on an X eigenstate $|+\rangle$. It can easily be seen that this is equivalent to applying the operator $\tilde{K}_m = (a_{00}^{(m)} + a_{01}^{(m)})\mathbb{I} + (a_{10}^{(m)} - i a_{11}^{(m)})Z$ to the $|+\rangle$ state. By defining $\tilde{a}_{00}^{(m)} = a_{00}^{(m)} + a_{01}^{(m)}$ and $\tilde{a}_{10}^{(m)} = a_{10}^{(m)} - i a_{11}^{(m)}$, this new modified Kraus operator can be expressed as: $\tilde{K}_m = \tilde{a}_{00}^{(m)} \mathbb{I} + \tilde{a}_{10}^{(m)} Z$.

Thus, the original quantum channel $\alpha_2(\rho) = \sum_m K_m \rho K_m^\dagger$ has been mapped to a new channel $\tilde{\alpha}_2(\rho) = \sum_m \tilde{K}_m \rho \tilde{K}_m^\dagger$, where $\tilde{K}_m = \sum_u \tilde{a}_{u0}^{(m)} Z^u$ and where $\tilde{a}_{u0} = \sum_v (-i)^{uv} a_{uv}$.

Thus, if we consider the circuit shown in Fig. 2.15, the input is given by $|i_0\rangle\langle i_0| \otimes |+\rangle\langle +|$. First, the second undergoes the noise channel α_2 and which, given the previous argument, can now be expressed as:

$$\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle +|)\big) = \big(|i_0\rangle\langle j_0| \otimes \tilde{\alpha}_2(|+\rangle\langle +|)\big). \tag{2.27}$$

Next, the two qubits are entangled via the control-Z gate:

$$\mathrm{CZ}\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle +|)\big)CZ = |i_0\rangle\langle j_0| \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)} \tilde{a}_{v0}^{(m)*} Z^u H |i_0\rangle\langle j_0| H Z^v, \tag{2.28}$$

Finally, the first qubit is measured in the equatorial basis $|s_k\rangle = e^{-i\frac{\phi}{2}Z}Z^k|+\rangle$ and the measurement outcome k obtained. Thus, the system is now given by $P_{sk}\text{CZ}\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle+|)CZ\big)P_{sk}$, which can be expressed as:

$$\langle+|Z^k e^{i\frac{\phi}{2}Z}|i_0\rangle\langle j_0|e^{-i\frac{\phi}{2}Z}Z^k|+\rangle P_{s_k} \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)}\tilde{a}_{v0}^{(m)*} Z^u H|i_0\rangle\langle j_0|HZ^v, \tag{2.29}$$

where $P_{sk} = |s_k(\phi)\rangle\langle s_k(\phi)|$.

This can be seen to be equal to the following expression for $P_{sk}\text{CZ}\big(|i_0\rangle\langle j_0|\otimes\alpha_2(|+\rangle\langle+|)CZ\big)P_{sk}$:

$$\frac{1}{2}e^{i\frac{\phi}{2}(-1)^{i_0}}e^{-i\frac{\phi}{2}(-1)^{j_0}}(-1)^{(i_0+j_0)k}P_{sk} \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)}\tilde{a}_{v0}^{(m)*} Z^u H|i_0\rangle\langle j_0|HZ^v. \tag{2.30}$$

By rearranging the coefficients onto the state of the second qubit, the original channel ε_k can be recognised to have been applied to the original input $|i_0\rangle\langle j_0|$:

$$P_{sk}\text{CZ}\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle+|)CZ\big)P_{sk} = \frac{1}{2}P_{s_k} \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)} Z^u \varepsilon_k(|i_0\rangle\langle j_0|)(\tilde{a}_{v0}^{(m)}Z^v)^\dagger, \tag{2.31}$$

which can be written as:

$$P_{sk}\text{CZ}\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle+|)CZ\big)P_{sk} = \frac{1}{2}P_{s_k} \otimes \sum_m \tilde{K}_m \varepsilon_k(|i_0\rangle\langle j_0|)\tilde{K}_m^\dagger. \tag{2.32}$$

Thus, the output on the second qubit is given by $\tilde{\alpha}_2 \circ \varepsilon_k(|i_0\rangle\langle j_0|)$. □

The results from lemma 4 are summarised in table 2.4, which illustrates how each Pauli basis element is mapped to a Pauli element in order to form the final noise channel acting on the output.

Coefficient	a_{00}	a_{01}	a_{10}	a_{11}
Initial operator	$\mathbb{I}$	X	Z	$-iZX$
Final operator	$\mathbb{I}$	$\mathbb{I}$	Z	$-iZ$

Table 2.1: *Mapping of Pauli basis elements for a noisy cluster.* The initial channel α_2 is given by Kraus operators which can be decomposed in the Pauli bases σ_{gh} with coefficient a_{gh}. The final channel $\tilde{\alpha}_2$ is given in terms of Pauli operators $\mathbb{I}$ and Z, with coefficients determined by the mapping.

Thus, lemma 4 provides a more general treatment of the case of a noisy resource. Next, we consider the general case of a noisy measurement.

Noisy Measurement

Finally, we consider the case of a noisy measurement, which is modelled by applying a noise channel to the first qubit just before the measurement is performed, as illustrated in Fig. 2.17. Here, we can exploit the fact that the measurement basis is known. Indeed, a unitary operator U followed by a projective measurement in the basis $|v_k\rangle$ can alternatively be viewed as a measurement onto the state $U^\dagger|v_k\rangle$. Here, the measurements are onto $e^{-i\frac{\phi}{2}Z}Z^k|+\rangle$, and we thus choose to decompose the Kraus operators in the rotated Pauli basis $U\sigma_{gh}U^\dagger$, with $U = e^{-i\frac{\phi}{2}Z}$. Hence, each Kraus operator can now be expressed as $K_m = \sum a_{gh}U\sigma_{gh}U^\dagger$, where $a_{gh} = \mathrm{Tr}(K_m U\sigma_{gh}U^\dagger)$, and where we now define $\sigma_{gh} = (-i)^{gh}Z^gX^h$.

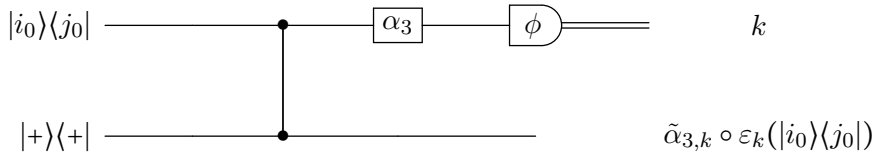


Figure 2.17: *Noisy Measurement.* The noise channel α_3 acts on the first qubit just before the measurement in the equatorial plane. This results in the output given by $\tilde{\alpha}_{3,k} \circ \varepsilon(|i_0\rangle\langle j_0|)$, where the noise now also depends on the measurement outcome k.

Lemma 5. *Let α_3 be the single qubit noise channel acting at location 3, as shown in Fig.2.17 and which is expressed in Kraus form $\alpha_3(\rho) = \sum_m K_m\rho K_m^\dagger$. If the Kraus operators are decomposed in the Pauli basis $K_m = \sum_{gh} a_{gh}^{(m)} e^{-i\frac{\phi}{2}Z}\sigma_{gh}e^{i\frac{\phi}{2}Z}$, then the output is given by:*

$$\varepsilon_k \circ \tilde{\alpha}_{3,k} \tag{2.33}$$

where the channel $\tilde{\alpha_3}^k$ has Kraus operators defined as:

$$\tilde{K}_m = \sum_u \tilde{a}_{uk}^{(m)} Z^u, \tag{2.34}$$

with coefficients $\tilde{a}_{uk}^{(m)} = \sum_v (i)^{uv}(-1)^{kv}a_{uv}^{(m)}$ and k denoting the measurement outcome, as illustrated in Fig. 2.18.

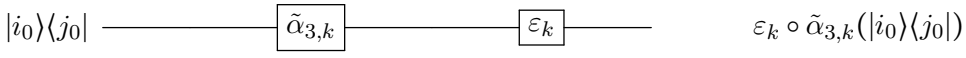


Figure 2.18: *Effective resulting channel: noisy measurement.* A noisy measurement is performed on the first qubit.

Proof. The quantum channel $\alpha_3(\rho) = \sum_m K_m \rho K_m^\dagger$ is applied to the first qubit just before a measurement is performed. Each Kraus operator is decomposed in the rotated Pauli basis, where the rotation is around the Z axis by an angle ϕ, that is $e^{-i\frac{\phi}{2}Z}\sigma_{gh}e^{i\frac{\phi}{2}Z}$. Thus, we can express each Kraus operator as $K_m = \sum_m a_{gh} i^{gh} e^{-i\frac{\phi}{2}Z} X^g Z^h e^{i\frac{\phi}{2}Z}$ and thus $K_m^\dagger = \sum_m a_{gh}^{(m)*}(-i)^{gh} e^{-i\frac{\phi}{2}Z} Z^h X^g e^{i\frac{\phi}{2}Z}$.

We now study the effect of the operator $K_m^\dagger$ on an equatorial basis state $|s(\phi)_k\rangle = e^{-i\frac{\phi}{2}Z}Z^k|+\rangle$:

$$K_m^\dagger e^{-i\frac{\phi}{2}Z}Z^k|+\rangle = \sum_{gh} a_{gh}^{(m)*}(-i)^{gh} e^{-i\frac{\phi}{2}Z} Z^h X^g e^{i\frac{\phi}{2}Z} e^{-i\frac{\phi}{2}Z}Z^k|+\rangle, \tag{2.35}$$

$$= \sum_{gh} a_{gh}^{(m)*}(-i)^{gh}(-1)^{gk} e^{-i\frac{\phi}{2}Z} Z^h Z^k|+\rangle, \tag{2.36}$$

$$= \sum_{u} \tilde{a}_{uk}^{(m)*} Z^u e^{-i\frac{\phi}{2}Z}Z^k|+\rangle, \tag{2.37}$$

where $\tilde{a}_{uk}^{(m)*} = \sum_v (-i)^{uv}(-1)^{kv} a_{vu}^{(m)*}$. This allows us to define the new modified Kraus operator $\tilde{K}_m^\dagger = \sum_u \tilde{a}_{uk}^{(m)*} Z^u$, and associated quantum channel $\tilde{\alpha}_{3,k}$, where the index k has been appended in order to emphasis the dependency on the measurement outcome k.

Thus, the input to the circuit depicted in Fig. 2.17 is $|i_0\rangle\langle j_0| \otimes |+\rangle\langle +|$. The two qubits ae entangled by a control-Z gate, and then the quantum channel α_3 is applied to the first qubit, which can be transformed to $\tilde{\alpha}_3$:

$$\sum_m \langle +|Z^k e^{i\frac{\phi}{2}Z}\tilde{K}_m|i_0\rangle\langle j_0|\tilde{K}_m^\dagger e^{-i\frac{\phi}{2}Z}Z^k|+\rangle P_{s_k} \otimes H|i_0\rangle\langle j_0|H, \tag{2.38}$$

or equivalently:

$$\sum_m a_{uk}^{(m)} a_{vk}^{(m)*} \langle +|Z^k e^{i\frac{\phi}{2}Z} Z^u|i_0\rangle\langle j_0|Z^v e^{-i\frac{\phi}{2}Z}Z^k|+\rangle P_{s_k} \otimes H|i_0\rangle\langle j_0|H. \tag{2.39}$$

By expanding out this expression, we obtain:

$$\frac{1}{2}\sum_{m,u,v} \tilde{a}_{uk}^{(m)} \tilde{a}_{vk}^{(m)} e^{i(-1)^{i_0}\frac{\phi}{2}}(-1)^{i_0(k+u)} e^{-i(-1)^{j_0}\frac{\phi}{2}}(-1)^{i_0(k+v)} P_{sk} \otimes H|i_0\rangle\langle j_0|H. \tag{2.40}$$

This can alternatively be expressed as:

$$\frac{1}{2}P_k \otimes \sum_{m,u,v} \tilde{a}_{uk}^{(m)} \tilde{a}_{vk}^{(m)*} H Z^k e^{i\frac{\phi}{2}Z} Z^u|i_0\rangle\langle j_0|Z^v e^{-i\frac{\phi}{2}Z}Z^k H, \tag{2.41}$$

where we recognise the initial channel acting on the output:

$$\frac{1}{2}P_k \otimes \sum_m H Z^k e^{i\frac{\phi}{2}Z}\tilde{K}_m|i_0\rangle\langle j_0|\tilde{K}_m^\dagger e^{-i\frac{\phi}{2}Z}Z^k H. \tag{2.42}$$

Thus, this results in the channel $\varepsilon_k \circ \tilde{\alpha}_{3,k}$ being applied to the input state, where we note the depen-

dency on measurement outcome for both channels. □

This mapping is summarised in table 2.2, where each Pauli basis element is mapped to a Pauli element, with certain coefficients now depending on measurement outcome k.

Coefficient	a_{00}	a_{01}	a_{10}	a_{11}
Initial	$\mathbb{I}$	$e^{-i\frac{\phi}{2}Z}Ze^{i\frac{\phi}{2}Z}$	$e^{-i\frac{\phi}{2}Z}Xe^{i\frac{\phi}{2}Z}$	$ie^{-i\frac{\phi}{2}Z}XZe^{i\frac{\phi}{2}Z}$
Final	$\mathbb{I}$	Z	$(-1)^k\mathbb{I}$	$i(-1)^kZ$

Table 2.2: *Mapping of Pauli basis elements for a noisy measurement.* The initial channel α_3 is given by Kraus operators which can be decomposed in the rotated Pauli bases $e^{-i\frac{\phi}{2}Z}\sigma_{gh}e^{i\frac{\phi}{2}Z}$ with coefficient a_{gh}. The final channel $\tilde{\alpha}_3$ is given in terms of Pauli operators $\mathbb{I}$ and Z, with coefficients determined by the mapping.

A theorem for local single qubit noise

Thus, the effect of noise acting at one of the four possible locations of the building block, as depicted in Fig. 2.10, has been studied and their effect on the output determined . By combing the four previous lemmas, we obtain the following theorem, mapping noise acting on the physical state to logical noise on the computation.

Theorem 3. *Let α_i, for $i = 1,2,3,4$ be noise channels acting at all four possible locations of the building block, as depicted in Fig. 2.10. Each channel is a single qubit CPTP map which may be expressed as a Kraus decomposition. Then, upon input $|i_0\rangle\langle j_0|$, the output is given by the channel:*

$$\alpha_4 \circ \tilde{\alpha}_2 \circ \varepsilon_k \circ \tilde{\alpha}_{3,k} \circ \alpha_1, \tag{2.43}$$

where the new channels $\tilde{\alpha}_2$ and $\tilde{\alpha}_{3,k}$ are defined as follows and where we have defined $\varepsilon_k(\rho) = \frac{1}{2}X^kHe^{i\frac{\phi}{2}Z}\rho e^{-i\frac{\phi}{2}Z}HX^k$.

If the original channel α_3 can be expressed as a Kraus decomposition $\alpha_3(\rho) = \sum_m K_m\rho K_m^\dagger$, and each Kraus operator decomposed in the rotated Pauli basis $K_m = \sum_{gh} a_{gh}^{(m)}e^{-i\frac{\phi}{2}Z}\sigma_{gh}e^{i\frac{\phi}{2}Z}$, then the channel $\tilde{\alpha_3}^k$ will have Kraus operators given by:

$$\tilde{K}_m = \sum_u \tilde{a}_{uk}^{(m)}Z^u, \tag{2.44}$$

with coefficients $\tilde{a}_{uk}^{(m)} = \sum_v (i)^{uv}(-1)^{kv}a_{uv}^{(m)}$ and k denoting the measurement outcome. If the original channel α_2 is expressed as a Kraus decomposition $\alpha_2(\rho) = \sum_m K_m\rho K_m^\dagger$, then the channel

$\tilde{\alpha}_2(\rho)$ *will have Kraus operators given by:*

$$\tilde{K}_m = \sum_u \tilde{b}_{u0}^{(m)} Z^{(m)u}, \tag{2.45}$$

and with coefficients $\tilde{b}_{u0} = \sum_v (-i)^{uv} b_{uv}^{(m)}$.

Proof. In order to determine the output of Fig. 2.10, we will first consider the simpler case depicted in Fig. 2.19. The input to the circuit is given by $|i_0\rangle\langle j_0| \otimes |+\rangle\langle +|$. Next, the noise channel α_2 affects

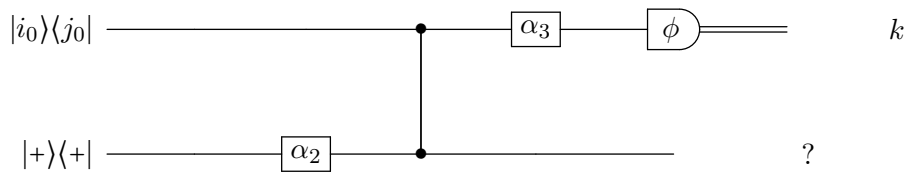


Figure 2.19: *Noisy cluster state and measurement.* The cluster state is affected by the noise channel α_2 whilst the measurement will be affected by the noise channel α_3.

the cluster state, which can be transformed to $\tilde{\alpha}_2$ as discussed in lemma **??**, before a control-Z gate acts on the two qubits:

$$\mathrm{CZ}\big(|i_0\rangle\langle j_0| \otimes \alpha_2(|+\rangle\langle +|)\big)CZ = |i_0\rangle\langle j_0| \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)} \tilde{a}_{v0}^{(m)*} Z^u H |i_0\rangle\langle j_0| H Z^v. \tag{2.46}$$

Next, the noise channel $\tilde{\alpha}_3$ is decomposed in the rotated Pauli basis, as discussed in lemma 5 and applied to the first qubit:

$$\sum_{n,g,h} a_{gk}^{(n)} a_{hk}^{(n)*} \langle +|Z^k e^{i\frac{\phi}{2}Z} Z^g |i_0\rangle\langle j_0| Z^h e^{-i\frac{\phi}{2}Z} Z^k |+\rangle P_{s_k} \otimes \sum_{m,u,v} \tilde{a}_{u0}^{(m)} \tilde{a}_{v0}^{(m)*} Z^u H |i_0\rangle\langle j_0| H Z^v. \tag{2.47}$$

From here, we see that the coefficients can be directly moved onto the state of the second qubit, as in the proof of lemma 5:

$$P_{s_k} \otimes \sum_{m,u,v,n} \tilde{a}_{u0}^{(m)} \tilde{a}_{v0}^{(m)*} Z^u e^{i\frac{\phi}{2}Z} \tilde{K}_n |i_0\rangle\langle j_0| \tilde{K}_n^\dagger e^{-i\frac{\phi}{2}Z} Z^k H Z^v. \tag{2.48}$$

Thus, the channel $\tilde{\alpha}_2 \circ \varepsilon_k \circ \varepsilon_{3,k}$ was applied to the input. □

Thus, we are now able to study the effect of physical noise acting on the qubits, and determine its effect on the output of the computation. Next, we shall apply the derived framework to a couple of examples.

2.3.4 Examples

First, we shall discuss the effect of Pauli noise on the computation, by considering both the cases of a noisy resource and a noisy measurement.

Pauli Noise

When we have access to a noisy cluster state, lemma 4 allows us to map the effect of the noise onto the computational output state. Indeed, we know that the output will have undergone a noise channel, resulting in the state $\tilde{\alpha} \circ \varepsilon(\rho)$. In the following, we shall consider the bit flip and phase flip channels, and realise how quickly and systematically we are now able to obtain an expression for the resultant state, in contrast with our previous analysis. Thus, we next revisit the previous examples of the bit flip and phase flip channels acting on either the cluster state or the measurement, before considering a more general noise model. First, we consider a noisy cluster state, which may easily be studied using lemma 4 and table 2.4.

Example 3. *When the bit flip channel is applied, the Kraus operators* $K_s = \sqrt{p_s} X^s$, $s = 0, 1$ *are mapped to* $\tilde{K}_s = \sqrt{p_s}\mathbb{I}$, *thus resulting in the identity channel: the output state* $\varepsilon_k(\rho)$ *has been unaffected by the noise channel.*

Example 4. *When the phase flip channel is applied, the Kraus operators* $K_s = \sqrt{p_s} Z^s$, $s = 0, 1$ *remain unchanged under the mapping* $\tilde{K}_s = \sqrt{p_s} Z^s$, *and thus the phase flip channel has been applied to the output* $\sum_s p_s Z^s \varepsilon(\rho) Z^s$.

Next, we consider the case of a noisy measurement in the X basis, which may easily be studied using lemma 5 and table 2.2, which reduces to table 2.3 for the case $\phi = 0$. Once again, we consider the effect of the bit and phase flip channels on the output.

Coefficient	a_{00}	a_{01}	a_{10}	a_{11}
Initial	$\mathbb{I}$	Z	X	iXZ
Final	$\mathbb{I}$	Z	$(-1)^k\mathbb{I}$	$i(-1)^k Z$

Table 2.3: *Mapping of Pauli basis elements for a noisy X measurement.* Here, we consider the special case of lemma 5, where the measurement is in the X basis and thus $\phi = 0$. The initial channel α_3 is given by Kraus operators which can be decomposed in the Pauli bases σ_{gh} with coefficient a_{gh}. The final channel $\tilde{\alpha}_3$ is given in terms of Pauli operators $\mathbb{I}$ and Z, with coefficients determined by the mapping.

Example 5. *When the bit-flip channel is applied, the Kraus operators $K_s = \sqrt{p_s}X^s$, $s = 0, 1$ are mapped to $\tilde{K}_s = \sqrt{p_s}(-1)^{ks}\mathbb{I}$, thus resulting in the identity channel: the output state $\varepsilon_k(\rho)$ has been unaffected by the noise.*

Example 6. *When the phase-flip channel is applied, the Kraus operators $K_s = \sqrt{p_s}Z^s$ are mapped to $\tilde{K}_s = \sqrt{p_s}Z^s$, thus resulting in the phase-flip channel acting on the output $\sum_s p_s Z^s \varepsilon_k(\rho) Z^s$.*

Unitary Noise

Next, having considered Pauli noise, we look at the more general case of unitary noise, whereby a unitary operator is applied to a physical qubit with probability p, thus disrupting and potentially destroying the computation. In the following, we shall study the effect of a Hadamard gate $H = \frac{1}{\sqrt{2}}(X + Z)$ on both the cluster and the measurement.

Coefficient	0	$\sqrt{\frac{p}{2}}$	$\sqrt{\frac{p}{2}}$	0
Initial operator	$\mathbb{I}$	X	Z	$-iZX$
Final operator	$\mathbb{I}$	$\mathbb{I}$	Z	$-iZ$

Table 2.4: *A Hadamard acting on the cluster.* The initial channel α_2 is given by Kraus operators which can be decomposed in the Pauli bases σ_{gh} with coefficient a_{gh}. The final channel $\tilde{\alpha}_3$ is given in terms of Pauli operators $\mathbb{I}$ and Z, with coefficients determined by the mapping.

Example 7. *When a Hadamard gate is applied with probability p_1, the Kraus operators of the corresponding channel are $K_s = \sqrt{p_s}H^s$, $s = 0, 1$. From table 2.4 which are mapped to $\tilde{K}_0 = K_0$ and $\tilde{K}_1 = \sqrt{2p_1}|0\rangle\langle 0|$ thereby destroying the computation.*

Coefficient	0	$\frac{\sqrt{p}}{\sqrt{2}}$	$\frac{\sqrt{p}}{\sqrt{2}}$	0
Initial	$\mathbb{I}$	Z	X	iZX
Final	$\mathbb{I}$	Z	$(-1)^k\mathbb{I}$	$i(-1)^k Z$

Table 2.5: *A Hadamard before the measurement.* The initial channel α_3 is given by Kraus operators which can be decomposed in the rotated Pauli bases σ_{gh} with coefficient a_{gh}. The final channel $\tilde{\alpha}_3$ is given in terms of Pauli operators $\mathbb{I}$ and Z, with coefficients determined by the mapping.

Example 8. *Here, with probability p a Hadamard gate is applied to the second qubit before the control-Z and a measurement in the X basis is performed. This corresponds to Kraus operators*

$K_1 = \sqrt{1-p}\mathbb{I}$ and $K_2 = \sqrt{p}H$. From table 2.2, the new modified Kraus operators can be immediately computed, and we find that: $\tilde{K}_1 = K_1$ and $\tilde{K}_2 = \sqrt{2p}|k\rangle\langle k|$

Thus, we have been able to use the framework derived in order to map physical errors acting on qubits to logical errors acting throughout the computation. This could first be used in order to simulate noisy quantum channels. Next, this formalism could be applied to the study of more complex forms of computation could be considered, with noise channels act throughout. This would result in errors being layered throughout the computation, and we could then ask how measurement patterns, logical operators and noise channels relate to one another.

In order to study this question further, we now consider whether noisy MBQC may be expressed within a generalised mixed MPS framework. Indeed, MPS were previously introduced as a natural framework for the study of MBQC, whereby the effect of measurements on the physical state could easily be observed as logical operators acting on the correlation space. This provides us with a strong motivation to investigate how a mixed state generalisation of MPS could be used in order to study noisy MBQC, and understand the mapping between the noise channels acting on the state and the information being processed.

2.4 Matrix Product Operators

In chapter 1, we introduced the formalism of MPS which provided an efficient representation of one-dimensional states with bounded bipartite entanglement. Furthermore, it was shown that this framework lent itself particularly well to the study of MBQC on a one-dimensional cluster state. Indeed, as a measurement is performed on a physical qubit, the associated logical operator evolves within the correlation space, thereby processing the computation.

Thus, given the insights gained by representing MBQC in the MPS formalism, we now consider the question of representing noisy MBQC in the mixed state analogue of MPS, which is known as Matrix Product Operators (MPO) [124–126]. In order to approach this question, we first, in section 2.4.1, present an intuitive argument as to what an MPO representation might resemble by considering the MPS representation of a cluster state. Next, in section 2.4 we formalise this argument by considering an arbitrary one-dimensional mixed state, which is purified before the proof technique used by Vidal are applied. Thus, we will obtain an MPO representation, which we will finally, in section 2.4.3 use in order to represent some examples of mixed states.

2.4.1 Motivation

MPS of a Cluster State

The one-dimensional cluster state $|\psi\rangle$ can be expressed as an MPS:

$$|\psi\rangle = \sum_i \langle i_n|A[i_{n-1}]\dots A[i_1]|+\rangle|i_1\dots i_n\rangle, \tag{2.49}$$

where the logical operators $A[k] = H|k\rangle\langle k|$ act on the input $|+\rangle$ state in the correlation space. When a physical qubit is measured, its associated logical operator is updated and mapped to a new logical operator which is now proportional to a unitary operator. Thus, as measurements are successively performed on the physical qubits, the associated logical operators are processed and the evolution of the computation can be seen to take place in the auxiliary space.

Rank One Density Matrix of a Cluster State

Given the expression in equation 2.49, the rank one density matrix of a pure cluster state can be expressed as:

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \langle i_n|A[i_{n-1}]\dots A[i_1]|+\rangle\langle+|A[j_1]\dots A[j_{n-1}]|j_n\rangle|i_1\dots i_n\rangle\langle j_1\dots j_n|. \tag{2.50}$$

Previously, in analogy with unitary operators acting on pure quantum states, we chose to think of the logical operators $A[i]$ as acting on the logical $|+\rangle$ state. In contrast, mixed state evolution is considered is typically modelled by a CPTP map, and represented by a superoperator acting on a density matrix. Thus, we propose to now interpret the Matrix Product Operator (MPO) representation as that of a map acting upon the input density matrix $|+\rangle\langle+|$. We thus write:

$$|\psi\rangle\langle\psi| = \sum_i \sum_j \sigma^{[i_n,j_n]} \circ \varepsilon^{[i_n,j_n]} \dots \varepsilon^{[i_1,j_1]}(|+\rangle\langle+|)|i_1\dots i_n\rangle\langle j_1\dots j_n|, \tag{2.51}$$

where we have introduced the logical superoperator $\varepsilon^{[i_k,j_k]}$ acting on qubit k, which is defined as:

$$\varepsilon^{[i_k,j_k]}(\rho) = A[i_k]\rho A[j_k], \tag{2.52}$$

and where the boundary conditions are given by:

$$\sigma^{[i_n,j_n]}(\rho) = \langle i_n|\rho|j_n\rangle. \tag{2.53}$$

This expression is reminiscent of the Kraus representation of a CPTP map, and building on this observation, we can imagine adding an index s in order to introduce a summation over indices

similar to the Kraus decomposition. This would thus yield an expression of the form $\varepsilon^{[i_k,j_k]}(\rho) = \sum_s A[i_k,s]\rho A[j_k,s]$,. Next, this argument is both formalised and extended to more general one-dimensional quantum states, before we then discuss the effect of measurements within the MPO framework.

2.4.2 Matrix Product Operators

We now formally consider the MPO representation of a one-dimensional mixed quantum state, which corresponds to qubits on a one-dimensional lattice. Whereas the complex coefficients were previously determined by logical operators $A[i_k]$ acting upon an input state in the correlation space, we now find that it is a density matrix ρ which is acted upon by logical superoperators $\varepsilon^{[i_k,j_k]}$. This provides us with an MPO representation for a mixed n-qubit quantum state, as given by lemma 6, which formalises the intuition provided in the previous section.

This is achieved by adding an auxiliary system to the original one, which allows for the mixed state to be purified. Then, the proof techniques introduced by Vidal, as discussed in chapter 1, are applied before finally, the auxiliary system is traced over. Thus, the mixed state on the original n qubits is obtained, with complex coefficients now expressed as the composition of logical superoperator on a single qubit state.

Lemma 6. *An n-qubit mixed state ρ can be expressed as an MPO:*

$$\rho = \sum_{i,j} \sigma^{[i_n,j_n]} \circ \varepsilon^{[i_{n-1},j_{n-1}]} \circ \ldots \circ \varepsilon^{[i_2,j_2]}(\rho[i_1,j_1])|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n|, \tag{2.54}$$

where $\varepsilon^{[i_k,j_k]}(\rho) = \sum_s A[i_k,s]\rho A^\dagger[j_k,s]$ denote the logical superoperator associated with qubit k and where the boundary conditions are given by $\sigma^{[i_n,j_n]}(\rho) = \sum_s v^\dagger[i,s]\rho v[j,s]$. $A[i_k,s]$ correspond to matrices of dimension ξ and the $v[j_k,s]$ to vectors, both of which depend on the state of the physical qubit k and an index s.

Proof. We consider a mixed state on n qubits on a space $\mathcal{H}_A$, which is expressed in its diagonal eigenbasis:

$$\rho^{[A]} = \sum_k p_k |v_k^{[A]}\rangle\langle v_k^{[A]}|. \tag{2.55}$$

The Schmidt decomposition tells us that there exists an auxiliary system $\mathcal{H}_R$, of identical dimension 2^n, which we may add to the original system. The resulting joint state $|\psi\rangle$ on the total Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_R$ is thus now a pure state:

$$|\psi\rangle = \sum_k \sqrt{p_k}|v_k^{[A]}\rangle \otimes |v_k^{[R]}\rangle, \tag{2.56}$$

where we have that $\mathrm{Tr}_R|\psi\rangle\langle\psi| = \rho[A]$. We note that nothing is a priori known about the entangle-

ment induced by the purification between the original and reference systems. These can be depicted as shown in Fig. 2.20, where the original qubits are labelled from $1 \dots n$, and the qubits from the reference system from $1' \dots n'$. The idea is now to consider the joint system of a real and auxiliary

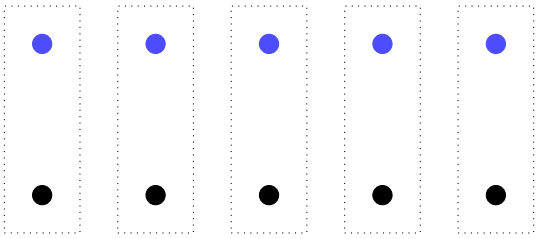


Figure 2.20: *Purification of the mixed state.* The original system is labelled from $1 \dots n$, whereas the added reference system from $1' \dots n'$. Whereas the original system was in a mixed state, the system on the $2n$ qubits now corresponds to a pure state.

qubit, and apply the same proof as Vidal to such an object. Thus, we first partition the qubits between the utmost left real and auxiliary qubits, and the other $2(n-1)$ qubits. A Schmidt decomposition is then performed across this partition, resulting in the state:

$$|\psi\rangle = \sum_{\alpha_1} \lambda_{\alpha_1}^{[1,1']} |\Phi_{\alpha_1}^{[1,1']}\rangle \otimes |\Phi_{\alpha_1}^{[2,2'\dots,n,n']}\rangle, \tag{2.57}$$

where the sums contains a number $\chi_{[1,1']}$ of terms, a quantity proportional to the amount of bipartite entanglement present between the first qubits of the initial and reference systems and the rest of the qubits. The first Schmidt vector is expanded in the computational basis, where the index i is used for the real qubit and s for the virtual qubit:

$$|\Phi_{\alpha_1}^{[1,1']}\rangle = \sum_{i_1,s_1} \Gamma_{\alpha_1}^{[1,1']i_1 s_1} |i_1 s_1\rangle, \tag{2.58}$$

thus yielding the state:

$$|\psi\rangle = \sum_{\alpha_1,i_1} \lambda_{\alpha_1}^{[1,1']} \Gamma_{\alpha_1}^{[1,1']i_1 s_1} |i_1 s_1\rangle \otimes |\Phi_{\alpha_1}^{[2\dots n']}\rangle. \tag{2.59}$$

Now, the second Schmidt vector is expressed as:

$$|\Phi_{\alpha_1}^{[2\dots n']}\rangle = \sum_{i_2 s_2} |i_2 s_2\rangle \otimes |\tau_{\alpha_1 i_2 s_2}^{[3\dots n']}\rangle, \tag{2.60}$$

and thus the state $|\psi\rangle$ may be written:

$$|\psi\rangle = \sum_{\alpha_1,i_1,i_2} \lambda^{[1,1']}_{\alpha_1} \Gamma^{[1,1']i_1 s_1}_{\alpha_1} |i_1 s_1\rangle \otimes |i_2 s_2\rangle \otimes |\tau^{[3\ldots n']}_{\alpha_1 i_2 s_2}\rangle. \tag{2.61}$$

The arbitrary state on the qubits $[3,\ldots,n']$ is expressed in the Schmidt bases for the partition $[3,\ldots,n']$:

$$|\tau^{[3\ldots n']}_{\alpha_1 i_2 s_2}\rangle = \sum_{\alpha_2} \Gamma^{[2,2']i_2 s_2}_{\alpha_1 \alpha_2} \lambda^{[2,2']}_{\alpha_2} |\Phi^{[3\ldots n']}_{\alpha_2}\rangle, \tag{2.62}$$

which thus give:

$$|\psi\rangle = \sum_{\alpha_1,i_1,i_2,\alpha_2} \lambda^{[1,1']}_{\alpha_1} \Gamma^{[1,1']i_1}_{\alpha_1} \Gamma^{[2,2']i_2 s_2}_{\alpha_1 \alpha_2} \lambda^{[2,2']}_{\alpha_2} |i_1 s_1\rangle \otimes |i_2 s_2\rangle \otimes |\Phi^{[3\ldots n']}_{\alpha_2}\rangle. \tag{2.63}$$

This process is repeated, until finally we obtain:

$$|\psi\rangle = \sum_{\alpha_1,i_1\ldots\alpha_n} \lambda^{[1,1']}_{\alpha_1} \Gamma^{[1,1']i_1 s_1}_{\alpha_1} \Gamma^{[2,2']i_2 s_2}_{\alpha_1 \alpha_2} \lambda^{[2,2']}_{\alpha_2} \ldots \Gamma^{[n,n']i_n s_n}_{\alpha_n} |i_1 s_1 \ldots i_n s_n\rangle. \tag{2.64}$$

The Schmidt coefficients are then absorbed into the tensors:

$$|\psi\rangle = \sum_{\alpha_1,i_1\ldots\alpha_n} \tilde{\Gamma}^{[1,1']i_1 s_1}_{\alpha_1} \tilde{\Gamma}^{[2,2']i_2 s_2}_{\alpha_1 \alpha_2} \ldots \tilde{\Gamma}^{[n,n']i_n s_n}_{\alpha_n} |i_1 s_1 \ldots i_n s_n\rangle. \tag{2.65}$$

The alpha indices can be thought of as implementing the multiplication between these different tensors, and thus, by associating vectors v with tensors with one index and matrices A for those with two, we obtain:

$$|\psi\rangle = \sum_{i_1 s_1 \ldots i_n s_n} v[i_1, s_1] A[i_2, s_2] \ldots v[i_n, s_n] |i_1 s_1 \ldots i_n s_n\rangle, \tag{2.66}$$

where we have also assumed translation independence. By relabelling, we finally get:

$$|\psi\rangle = \sum_{i_1 s_1 \ldots i_n s_n} v[i_n, s_n] A[i_{n-1}, s_{n-1}] \ldots v[i_1, s_1] |i_1 s_1 \ldots i_n s_n\rangle. \tag{2.67}$$

These tensors now are not only dependent on the state of the real qubits, but also on the state of the auxiliary qubits. Whereas previously the dimensions of the matrices were upper bounded by the maximum Schmidt rank over the $(n-1)$ partitions, their dimension is now dependent on the amount of entanglement induced by the reference system.

Next, we can trace over the reference system and obtain an expression for the state of the system, and by defining the matrix $\rho[i_1, j_1] = \sum_{s_1} v^\dagger[i_1, s_1] v[j_1, s_1]$, where $v[i_1, s_1]$ denotes a line vector

and $\vec{v}^{\dagger}[j_1, s_1]$ a column vector, we thus obtain:

$$\rho^{[A]} = \sum_s \sum_i v[i_n, s_n] \dots A[i_2, s_2] \rho[i_1, j_1] A^{\dagger}[j_2, s_2] \dots v^{\dagger}[j_n, s_n] |i_1 \dots i_n\rangle\langle j_1 \dots j_n|. \quad (2.68)$$

The superoperator $\varepsilon^{[i_k, j_k]}$ is defined as:

$$\varepsilon^{[i_k, j_k]}(\rho) = \sum_s A[i_k, s] \rho A^{\dagger}[j_k, s], \quad (2.69)$$

and

$$\sigma^{[i,j]}(A) = \sum_s v^{\dagger}[i, s] A v[j, s]. \quad (2.70)$$

Thus, the mixed state is finally given by:

$$\rho^A = \sum \sigma^{[i_n, j_n]} \circ \varepsilon^{[i_{n-1}, j_{n-1}]} \circ \dots \varepsilon^{[i_{n-1}, j_{n-1}]}(\rho[i_1, j_1]) |i_1 \dots i_n\rangle\langle j_1 \dots j_n|. \quad (2.71)$$

This initial state is thus acted upon by sequence of $n-2$ superoperators denoted by ε, and where $\circ$ denotes the composition of superoperators. Finally, the operator σ^{i_n, j_n} acts on the evolved logical state, and is analogous to a measurement. The key difference with MPS is the additional index s which arise in the logical operators $A[k, s]$. □

Thus, having obtained an expression for the MPO representation for a one-dimensional quantum state, we consider the effect of single qubit measurements on their associated logical superoperators.

Measurement in the MPO Representation

In MPS, when a physical qubit is measured, its associated logical operator evolves to one proportional to a unitary operator. Similarly, proposition 2 shows us that te effect of a projective measurement on the physical qubits is to map the associated logical superoperator to a new logical superoperator.

Proposition 2. *When the k^{th} physical qubit is measured in an orthonormal basis $|v_m\rangle$, the logical superoperator $\varepsilon^{[i_k, j_k]}$ evolves to the logical superoperator $\varepsilon^{[v_m, v_m]}$:*

$$\varepsilon^{[v_m, v_m]}(\rho) = \sum_s A[v_m, s] \rho A^{\dagger}[v_m, s], \quad (2.72)$$

where $A[v_m, s] = \sum_i \langle v_m | i \rangle A[i, s]$.

The proof simply relies on applying the measurement and studying its effect on the relevant operators. In the next section, we will consider various examples of mixed quantum states which can be represented in the MPO formalism introduced in lemma 6.

2.4.3 MPO Representation: Examples

The cluster state on n qubits, as previously seen, has an MPS representation given by equation 2.49. Here, as discussed in section 2.4.1, we find that a cluster state may also be expressed as an MPO.

Example 9. *The MPO representation of a cluster state is given by:*

$$\rho = \sum_{i,j} \sigma^{[i_n,j_n]} \varepsilon^{[i_{n-1},j_{n-1}]} \circ \ldots \circ \varepsilon^{[i_2,j_2]}(|+\rangle\langle+|)|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n|, \tag{2.73}$$

where $\varepsilon^{[i,j]}(\rho) = A[i]\rho A[j]$, $A[k] = H|k\rangle\langle k|$ *and* $\sigma^{[i,j]}(\rho) = \langle i|\rho|j\rangle$.

Next, we consider the case of the maximally mixed state on n qubits, $\frac{1}{2^n}\mathbb{I}_n$. This can be easily obtained by first constructing the all zero state, and then applying the channel $K_s = \frac{1}{\sqrt{2}}X^s$ to every qubit.

Example 10. *The MPO representation of the maximally mixed state on n qubits is given by*

$$\frac{1}{2^n}\mathbb{I}_n = \sum_{i,j} \sigma^{[i_n,j_n]} \circ \varepsilon^{[i_{n-1},j_{n-1}]} \circ \cdots \circ \varepsilon^{[i_1,j_1]}(|0\rangle\langle 0|)|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n| \tag{2.74}$$

where $\varepsilon^{[i,j]}(\rho) = \frac{1}{2}\sum_s A[i]X^s\rho X^s A[j]$, $\sigma^{[i_n,j_n]}(\rho) = \frac{1}{2}\sum_t \langle i_n|X^t\rho X^t|j_n\rangle$, *and* $A[k] = |0\rangle\langle k|$.

Finally, we consider the input state used in the one clean qubit model of computation, which is the state $|0\rangle\langle 0| \otimes \frac{1}{2^n}\mathbb{I}$.

Example 11. *The state* $|0\rangle\langle 0| \otimes \frac{\mathbb{I}}{2^n}$*, which was the input state of the one clean qubit Model can be expressed as:*

$$|0\rangle\langle 0| \otimes \frac{\mathbb{I}}{2^n} = \sum_{\boldsymbol{i},\boldsymbol{j}} \sigma^{[i_n,j_n]} \circ \varepsilon^{[}i_{n-1}, j_{n-1}] \circ \cdots \circ \epsilon^{[i_0,j_0]}|0\rangle\langle 0| \\ |i_i \ldots i_n\rangle\langle j_1 \ldots j_n| \tag{2.75}$$

where the superoperators are defined as $\epsilon^{[i_0,j_0]}(\rho) = A[i_0]\rho A[j_0]^\dagger$, $\sigma^{[i_n,j_n]}(\rho) = \frac{1}{2}\sum_{s_n}\langle i_n|X^t\rho X^t|j_n\rangle$, $\varepsilon^{[i_k,j_k]}(\rho) = \frac{1}{2}\sum_{s_k} A[i_k]X^s\rho X^s A[j_k]^\dagger$, , *and* $A[k] = |0\rangle\langle k|$. *We note that the assumption of translational invariance no longer holds.*

Thus, these examples illustrate how the MPO expression introduced in lemma 6 may be applied. Next, we shall study the effect of noise channels occurring in the context of one-dimensional MBQC performed on a cluster state.

2.5 Noise in MBQC in the MPO Framework

In the following, we consider noise in one-dimensional MBQC expressed in the MPO framework, and ask whether the physical errors occurring on the state may be mapped to logical errors within the computation. In order to do so, we successively consider the effect of a Pauli operator, a unitary operator and finally a channel on a physical qubit and determine its effect on the associated logical operator. Then, we shall consider a couple of examples using the derived framework.

2.5.1 Error Propagation: Framework

Our goal is to develop a mixed state framework which will show us how CPTP maps acting on the physical qubits get mapped on to the logical state. In order to approach this question, we shall first study the simple case of Pauli operators acting on the physical state, and see how these are mapped onto logical operators. This will provide us with the tools to understand how the application of a single qubit unitary operator modifies the logical operators, before finally considering the more general case of a CPTP map.

Pauli Operator

Pauli noise is a simple and physically relevant model of noise, and we will thus start by considering the case when a Pauli operator is applied to the cluster state. Proposition 3 allows us to map the effect of a single Pauli operator applied to the physical qubit to a transformation of the associate logical operator.

Proposition 3. *If a Pauli operator σ_{ab} is applied to the j^{th} qubit, the logical operator $A[i_j]$ is mapped to the logical operator $\sigma_{0a}A[i_j]\sigma_{ab}$, as illustrated in table 2.6.*

Proof. The MPS representation of a cluster state is given by $|\psi\rangle = \sum\langle i_n|A[i_{n-1}]\dots A[i_2]A[i_1]|+\rangle|i_1\dots i_n\rangle$. If a Pauli X is applied to the j^{th} qubit, then the state evolves to:

$$X_j|\psi\rangle = \sum(-1)^{i_n i_{n-1}}\dots(-1)^{i_{j+1}i_j}(-1)^{i_j i_{j-1}}\dots(-1)^{i_1 i_2}|i_1\dots i_{j-1}\rangle|i_j\oplus 1\rangle|i_{j+1}\dots i_n\rangle. \quad (2.76)$$

By relabelling:

$$X_j|\psi\rangle = \sum(-1)^{i_n i_{n-1}}\dots(-1)^{i_{j+1}(i_j\oplus 1)}(-1)^{(i_j\oplus 1)i_{j-1}}\dots(-1)^{i_1 i_2}|i_1\dots i_{j-1}\rangle|i_j\rangle|i_{j+1}\dots i_n\rangle, \quad (2.77)$$

$$= \sum\langle i_n|A[i_{n-1}]\dots H|i_{j+1}\rangle\langle i_{j+1}|H|i_j\oplus 1\rangle\langle i_j\oplus 1\rangle H|i_{j-1}\rangle\langle i_{j-1}|\dots A[i_1]|+\rangle|i_1\dots i_n\rangle, \quad (2.78)$$

$$= \sum\langle i_n|A[i_{n-1}]\dots A[i_{j+1}]ZA[i_j]XA[i_{j-1}]\dots A[i_1]|+\rangle|i_1\dots i_n\rangle, \quad (2.79)$$

and we can now define $\tilde{A}[k] = ZA[k]X = \sigma_{01}A[i_j]\sigma_{10}$.

If a Pauli Z is applied to the j^{th} qubit, then the state evolves to:

$$Z_j|\psi\rangle = \sum(-1)^{i_n i_{n-1}} \dots (-1)^{i_{j+1} i_j} (-1)^{i_j i_{j-1}} \dots (-1)^{i_1 i_2} (-1)^{i_j} |i_1 \dots i_n\rangle. \tag{2.80}$$

The effect on the logical operators can be expressed in two ways. Either:

$$Z_j|\psi\rangle = \sum\langle i_n| \dots A[i_{j+1}]H|i_j\rangle\langle i_j|ZA[i_{j-1}] \dots |+\rangle|i_1 \dots i_n\rangle, \tag{2.81}$$

$$= \sum\langle i_n| \dots A[i_{j+1}]A[i_j]ZA[i_{j-1}] \dots |+\rangle|i_1 \dots i_n\rangle, \tag{2.82}$$

where we can now define $\tilde{A}[k] = A[k]Z$, or alternatively:

$$Z_j|\psi\rangle = \sum\langle i_n|A[i_{n-1}] \dots A[i_{j+1}]XH|i_j\rangle\langle i_j|A[i_{j-1}] \dots A[i_1]|+\rangle|i_1 \dots i_n\rangle, \tag{2.83}$$

$$= \sum\langle i_n|A[i_{n-1}] \dots A[i_{j+1}]XA[i_j]A[i_{j-1}] \dots A[i_1]|+\rangle|i_1 \dots i_n\rangle, \tag{2.84}$$

where we can now define $\tilde{A}[k] = XA[k]$. Thus, when the Pauli $Z = \sigma_{01}$ operator is applied, the logical operators can be represented by two equivalent evolutions: $A[i_j]Z = A[i_j]\sigma_{01} = XA[i_j] = \sigma_{10}A[i_j]$.

Finally, if a Pauli operator $Y = iXZ$ is applied to the j^{th} qubit, then the state evolves to:

$$Y_j|\psi\rangle = \sum(-1)^{i_n i_{n-1}} \dots (-1)^{i_2 i_1} i (-1)^{i_j} |i_1 \dots i_{j-1}\rangle|i_j \oplus 1\rangle|i_{j+1} \dots i_n\rangle. \tag{2.85}$$

Once again, its effect on the logical operators can be expressed in two ways:

$$Y_j|\psi\rangle = \sum(-1)^{i_n i_{n-1}} \dots (-1)^{i_{j+1} i_j} (-1)^{i_j i_{j-1}} \dots (-1)^{i_1 i_2} (-1)^{i_j} |i_1 \dots i_{j-1}\rangle|i_j \oplus 1\rangle|i_{j+1} \dots i_n\rangle, \tag{2.86}$$

$$= \sum\langle i_n|A[i_{n-1}] \dots H|i_j\rangle\langle i_j|Z \dots A[i_1]|+\rangle|i_1, \dots i_{j-1}\rangle|i_j \oplus 1\rangle|i_{j+1} \dots i_n\rangle, \tag{2.87}$$

which if we relabel:

$$Y_j|\psi\rangle = \sum\langle i_n| \dots H|i_j \oplus 1\rangle\langle i_j \oplus 1|Z \dots |+\rangle|i_1, \dots i_{j-1}\rangle|i_j\rangle|i_{j+1} \dots i_n\rangle, \tag{2.88}$$

$$= \sum\langle i_n| \dots ZA[i_j]XZ \dots |+\rangle|i_1 \dots i_n\rangle, \tag{2.89}$$

where we can now define $\tilde{A}[i_j] = ZA[i_j]XZ = ZA[i_j]Y$. Alternatively,

$$Y_j|\psi\rangle = \sum \langle i_n| \dots HZ|i_j \oplus 1\rangle\langle i_j \oplus 1| \dots |+\rangle|i_1, \dots i_{j-1}\rangle|i_j\rangle|i_{j+1} \dots i_n\rangle, \tag{2.90}$$

$$= \sum \langle i_n| \dots HZX|i_j\rangle\langle i_j|X \dots |+\rangle|i_1 \dots i_n\rangle, \tag{2.91}$$

$$= \sum \langle i_n| \dots XZA[i_j]X \dots |+\rangle|i_1 \dots i_n\rangle, \tag{2.92}$$

where we can now define $\tilde{A}[i_j] = iXZA[i_j]X = YA[i_j]X$. Thus, when the Pauli operator $Y = \sigma_{11}$ acts on the state, the logical operators evolve to: $ZA[i_j]XZ = ZA[i_j]Y = \sigma_{01}A[i_j]\sigma_{11} = YA[i_j]X = \sigma_{11}A[i_j]\sigma_{10}$. □

Unitary Operator

Thus, now that we can map the effect of a single Pauli operator onto the correlation space, we next consider the effect of a single qubit unitary operator U on the j^{th} qubit. More precisely, by decomposing the unitary in the Pauli bases, we are able to express the transformation of the associated logical operator.

Proposition 4. *When a unitary operator $U = \sum_{g,h} u_{gh}\sigma_{gh}$ acts on qubit j, the logical operator evolves to:*

$$\tilde{A}[i_j] = \xi(A[i_j]) = \sum_{g,h} u_{gh}\sigma_{0g}A[i_j]\sigma_{gh}. \tag{2.93}$$

This defines a channel ξ which maps logical operators to logical operators.

Proof. The unitary operator U may be decomposed in the Pauli bases: $U = \sum_{g,h} u_{gh}\sigma_{gh}$. Then, by proposition 3, the effect of Pauli operators on logical operators can be determined, and by linearity the final result obtained. □

This result is summarised in table 2.6, which maps the effect of each Pauli operator on the physical state onto the associated logical operator.

Pauli operator	X	Z	iXZ
Logical operator	$ZA[k]X$	$A[k]Z$	$iZA[k]XZ$

Table 2.6: *Mapping from Pauli errors to logical errors.* A Pauli operator is applied to the k^{th} physical qubit, which will cause its associated logical operator to evolve to a new logical operator.

CPTP Map

Finally, we consider the effect of applying a CPTP map to the cluster state, which will thus no longer be a pure state. The CPTP map will be expressed as a Kraus decomposition, and in turn, each Kraus operator may be decomposed in the Pauli bases, thus allowing for the new logical operator to be determined.

Proposition 5. *If the l^{th} qubit undergoes a CPTP map, represented by the quantum channel $\eta(\rho) = \sum_m K_m \rho K_m^\dagger$, where each Kraus operator can be decomposed in the Pauli basis as $K_m = \sum_{a,b}^{(m)} k_{ab}\sigma_{ab}$, then the logical operator is mapped to $\tilde{\varepsilon}^{[i,j]}(\rho) = \sum_m \xi_m(A[i])\rho\xi_m(A[i])$, where:*

$$\xi_m(A[i]) = \sum_{a,b} k_{ab}^{(m)} \sigma_{0a}^{(m)} A[i] \sigma_{ab}^{(m)}. \tag{2.94}$$

Proof. The Kraus operators K_m are decomposed in the Pauli bases: $K_m = \sum_{a,b} k_{ab}^{(m)} \sigma_{ab}^{(m)}$. Thus, when the CPTP map acts on the l^{th} qubit, we have:

$$\eta_j(\rho) = \sum_m \sum_{i,j} \sum_{a,b,g,h} \sigma^{[i_n,j_n]} \circ \ldots \circ \varepsilon^{[i_2,j_2]}(|+\rangle\langle+|)|i_1\rangle\langle j_1| \ldots k_{ab}^{(m)} k_{gh}^{(m)*} \sigma_{ab}^{(m)}(|i_l\rangle\langle j_l|)\sigma_{gh}^{(m)\dagger} \ldots |i_n\rangle\langle j_n|. \tag{2.95}$$

By linearity, and applying proposition 3, this can be expressed as:

$$\eta_j(\rho) = \sum_{i,j} \sigma^{[i_n,j_n]} \circ \varepsilon^{[i_{n-1}j_{n-1}]} \circ \ldots \circ \tilde{\varepsilon}^{[i_l,j_l]} \circ \ldots \circ \varepsilon^{[i_2j_2]}(|+\rangle\langle+|)|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n|, \tag{2.96}$$

where we have defined $\tilde{\varepsilon}^{[i,j]}(\rho) = \sum_m \xi_m(A[i])\rho\xi_m^\dagger(A[j])$, and where $\xi_m(\rho) = \sum_{a,b} k_{ab}^m \sigma_{0a}^{(m)} \rho \sigma_{ab}^{(m)}$. □

Thus, we are now able to map the effect of local noise channels acting on the cluster state onto the correlation space. Next, in section 2.5.2 we consider various examples whereby the derived framework is applied.

2.5.2 Noise in One-dimensional MBQC

We assume that an n-qubit pure cluster state is initially prepared, which is expressed as an MPO:

$$\rho = \sum_{i,j} \sigma^{[i_n,j_n]} \varepsilon^{[i_{n-1},j_{n-1}]} \circ \ldots \circ \varepsilon^{[i_2,j_2]}(|+\rangle\langle+|)|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n|, \tag{2.97}$$

where the logical superoperator is given by $\varepsilon^{[i,j]}(\rho) = A[i]\rho A[j]$, and where the boundary conditions are given by $\sigma^{[i,j]}(\rho) = \langle i|\rho|j\rangle$. First, we consider the case where a unitary operator, the Hadamard gate, is applied to one of the qubits, and determine its effect on the computation.

Unitary Operator

First, we consider that a single qubit unitary operator is applied to one of the qubits. By applying proposition 4 we are able to determine its effect on the associated logical operator.

Example 12. *For a Hadamard gate* $H = \frac{1}{\sqrt{2}}(X + Z)$*gate, we have that* $u_{00} = 0, u_{01} = \frac{1}{\sqrt{2}}, u_{00} = \frac{1}{\sqrt{2}}$, $u_{11} = 0$*. Thus, if it is applied to the* j^{th} *qubit, then* $A[i_j]$ *evolves to:*

$$\tilde{A}[i_j] = \frac{1}{\sqrt{2}} A[i_j]Z + \frac{1}{\sqrt{2}} ZA[i_j]X. \tag{2.98}$$

Pauli Noise Channels

Next, we assume that the l^{th} qubit is affected by a local noise channel, which is modelled by a quantum channel implementing a CPTP map $\eta(\rho) = \sum_m K_m \rho K_m^\dagger$. By applying proposition 5, its effect on the logical superoperators within the auxiliary space is determined. First, we consider the effect of the phase flip channel, and then the bit flip channel.

Example 13. *When the phase flip channel with Kraus operators* $K_s = \frac{1}{\sqrt{2}} Z^s$*,* $s = 0, 1$ *is applied, the associated logical operator evolves to:*

$$\xi_s(A[i]) = \frac{1}{\sqrt{2}} A[i]Z^s, \tag{2.99}$$

and thus the logical superoperator to:

$$\tilde{\varepsilon}^{[i,j]}(\sigma) = \frac{1}{2} \sum_s A[i]Z^s \sigma Z^s A[j]. \tag{2.100}$$

Example 14. *When the bit flip channel with Kraus operators* $K_s = \frac{1}{\sqrt{2}} X^s$*,* $s = 0, 1$ *is applied, the associated logical operator evolves to:*

$$\xi_s(A[i]) = \frac{1}{\sqrt{2}} Z^s A[i]X^s, \tag{2.101}$$

and thus the logical superoperator evolves to:

$$\tilde{\varepsilon}^{[i,j]}(\sigma) = \frac{1}{2} \sum_s Z^s A[i]X^s \sigma X^s A[j]Z^s. \tag{2.102}$$

Thus, these examples illustrate the effect of local noise channel on the logical computation. Next, we consider the interaction of the errors due to the randomness of the measurement outcomes with the errors due to noise. Here, the measurements will be in the X basis, and we recall that if a qubit is measured in the X basis, then its logical operator $A[i]$ is mapped to $\frac{1}{\sqrt{2}} HZ^m$, with m denoting the measurement outcome.

Example 15. *If a bit-flip channel is applied to the k^{th} qubit, then its associated logical superoperator evolves to $\tilde{\varepsilon}^{[i_k,j_k]}(\rho) = \frac{1}{2}\sum_s Z^s A[i_k]X^s \rho X^s A[j_k]Z^s$. If the qubit is now measured in the X basis, the associated logical superoperator to evolve to $\tilde{\varepsilon}^{[i_l,j_l]}(\rho) = \frac{1}{4}\sum_s Z^s H Z^m X^s \rho X^s Z^m H Z^s = \frac{1}{2} H Z^m \rho Z^m H$, and thus the output has not been affected by the channel.*

Example 16. *The channel given by Kraus operators $K_0 = \sqrt{p_0}\mathbb{I}$, $K_1 = \sqrt{p_1}X$ and $K_2 = \sqrt{p_2}Y$ is applied to the k^{th} physical qubit. Thus, the associated superoperator evolves to: $\tilde{\varepsilon}^{[i_k,j_k]} = \sqrt{p_0}A[i_k]\rho A^\dagger[j_k] + \sqrt{p_1}ZA[i_k]X\rho X A^\dagger[j_k]Z + \sqrt{p_2}ZA[i_k]Y\rho Y A^\dagger[j_k]Z$. Next, the qubit is measured in the X basis, resulting in: $\tilde{\varepsilon}^{[x_m,x_m]} = \frac{1}{2}(\sqrt{p_0}+\sqrt{p_1})HZ^m\rho Z^m H + \frac{1}{2}\sqrt{p_2}HZ^m Z\rho Z Z^m H$. This is equivalent to a Z gate applied with probability p_2 to the qubit before the measurement.*

Finally, we consider the more general model of unitary noise by studying the effect of a Hadamard gate probabilistically applied to the physical qubit followed by an X measurement, as we previously discussed in example 8.

Example 17. *The channel with Kraus operators $K_1 = \sqrt{1-p}\mathbb{I}$ and $K_2 = \sqrt{p}H$ is applied to the physical qubit. Thus, the associated logical superoperator evolves to $\tilde{\varepsilon}^{[i_k,j_k]} = \tilde{A}[i_k]\rho\tilde{A}^\dagger[j_k]$, where:*

$$\tilde{A}[i] = \frac{1}{\sqrt{2}}A[i]Z + \frac{1}{\sqrt{2}}ZA[i]X. \tag{2.103}$$

Next, the qubit is measured in the X basis, and thus the logical operator is transformed to $\tilde{\varepsilon}^{[x_m,x_m]}(\rho) = \tilde{A}[x_m]\rho\tilde{A}^\dagger[x_m]$, with:

$$\tilde{A}[x_m] = \frac{1}{\sqrt{2}}HZ^m Z + \frac{1}{\sqrt{2}}ZHZ^m X, \tag{2.104}$$

which reduces to $\tilde{A}[x_m] = \sqrt{2}H|k\rangle\langle k|$.

2.6 Conclusion

Noise processes remain a great challenge in the race to build a scalable quantum computer. Noise is typically modelled as Pauli errors, which has proven to be a powerful tool. Nonetheless, it has in recent years been argued that more general forms of noise should be considered, and their effect on the computation determined. Furthermore, this might lead to more general noise models being developed, which could be useful in the analysis of error correction.

Results

Here, we have introduced two frameworks which allow for the effect of physical noise on the computation to be studied. More precisely, we considered the effect of single qubit local noise channels in the context of one-dimensional MBQC. This was achieved both in the circuit model, and in the derived MPO representation.

First, we considered teleportation in the presence of a noisy resource state, and found that the effect of the noise channel on the output could be determined. This then motivated us to consider the impact of noise in one-dimensional MBQC, as indeed, preparing pure states and performing clean measurements is experimentally challenging. Here, the introduced framework allowed us to understand the impact of having access to a mixed resource state on the computation, and the effect of performing noisy measurements. Moreover, this could be used in order to simulate noisy computation.

Future directions

First, more complex computations and noise models might be considered, by for instance studying the effect of logical errors on the computation when the building blocks are concatenated. Indeed, the computation requires for precisely these blocks to be concatenated, sequentially implementing a logical operator on the teleported state. Now, in the presence of noise, errors will be layered throughout the computation. It would be useful to study how the measurement patterns, the logical operators and the noise channels relate to one another, and what is their effect on the computation output. Furthermore, a natural extension would be to study the generalisation of this framework to two-dimensions, by for instance considering grid-like structures [79].

The next step would be to use these frameworks in order to represent noisy computations as well as to perform simulations of noise computations. When MBQC is represented in the MPS formalism, the goal is to implement an operator A via successive measurements in the correlation space. Due to the random nature of measurement outcomes, random Pauli by-product operators will occur throughout. By exploiting the properties of Clifford operators, we find that we are instead implementing the operator UA where U is a unitary operator depending on measurement outcomes and which may be subsequently corrected for. A similar analysis could be performed in the case of mixed states acted upon by logical superoperators. Another interesting question would be to study the numerical simulation of errors on the state and their impact on the computation. Overall, MPO offer us a flexible framework in which we can study how noise on cluster state computations affects the computation. Here, our simple examples illustrate its capabilities. Its full power might be in modelling the error channels that arise in experiments, and may prove to be useful for experimental groups in their modelling.

We have studied the effect of local noise channels on physical states and their impact on the computation performed. The former provides a better understanding of the role of errors in the computation, and the latter could allow for the simulation of noisy quantum computation.

Chapter 3

Measurement Based Classical Computation

MBQC, which was introduced in chapter 1, provides an alternative model of computation to that of the circuit model. Here, the computation is implemented by performing single qubit measurements on an entangled resource state. Thus, the computation exploits the correlations present within the quantum state, which is thereby destroyed as the computation proceeds. The probabilistic nature of measurement outcomes will cause random by-product operators to be applied. In order to correct for these, measurements will now be allowed to depend on prior measurement outcomes. Thus, it is thanks to this adaptivity of measurements that an algorithm can be implemented.

Adaptivity

Adaptivity thus plays a central role within the MBQC computation scheme. It has previously been studied within the context of the Gottesman-Chuang construction for computation [73], whereby it was shown that non-adaptive models of computation can exhibit non-classicality [127]. In the following, we propose to further investigate the role of adaptivity in computation by introducing a classical analogue of MBQC, which we name Measurement Based Classical Computing (MBCC). More precisely, we consider a non-adaptive model of computation for which the resource is no longer a quantum state but a sample polled from a classical probability distribution.

Thus, whereas previously the resource state was required to be an entangled quantum state whose correlations were to be exploited, we now instead consider classical bit strings. More specifically, we consider a classical bit string sampled from a probability distribution. Here, we argue that the resulting non-adaptive model of computation can nonetheless result in a non-classical computation.

The Complexity of Sampling

This paradigm raises the question as to the complexity of the underlying probability distribution. In order to further study this, we introduce the idea of quantum preparations. This highlights the role of the process giving rise to the considered probability distribution, thus allowing us to distinguish quantum from classical preparations. More precisely, we introduce the family of IQP^* circuits, closely related to that of IQP circuits. Once again, we find that these can not be classically efficiently simulated unless the polynomial hierarchy collapses to the third level. This was previously stated under Hypothesis 1, and constitutes a foundational assumptions of computational complexity.

Structure

In section 3.1, we introduce the classical analogue of MBQC, which we call Measurement Based Classical Computing (MBCC), whereby classical post-processing is performed on a sample taken from a probability distribution. Next, in section 3.2, we introduce the class of IQP^* circuit families. Then, in section 3.3, we can finally study the complexity of MBCC. Finally, in section 3.4, we review our results and future directions for research.

3.1 Classical MBQC

In chapter 1, we first introduced the unitary circuit model as the quantum analogue of the classical circuit model. We then discussed MBQC, an alternative computational scheme, which although equivalent in terms of power, provided insight into the role of quantum resources. Indeed, within the MBQC framework, the computation is split between tasks that are quantum and classical tasks. More specifically, the resource state and the measurements are quantum processes, whereas the post-processing is classical.

This approach allows us to study what exactly are the quantum ingredients which render a computation non-classical, and thus understand which are the truly non-classical operations required by a quantum device in order to supersede a classical computer. In the following, we consider what would be the classical analogues of a resource state and a measurement within the context of computation.

3.1.1 From Quantum to Classical Resource States

In MBQC, the cluster state serves as a reservoir of quantum correlations to be exploited by the computation. As both the computation and measurements proceed, the cluster state is progressively destroyed, and is thus a single use resource.

Sampling from a Probability Distribution

The resource is thus a quantum state, which, when measured, yields a classical bit string with a given probability. Thus, the classical analogue of a cluster state will be defined to be a sample bit string from a multi-bit probability distribution.

More formally, the resource is now a classical m-bit string $w = x_1 \dots x_m$, where $x_i \in \{0, 1\}$. The string w thus takes one of 2^m possible values, each occurring with a given probability. That is, we are now sampling multi-bit strings from a probability distribution of exponential size.

Efficiently quantum preparable

The probability distribution itself may originate from a complicated process, and, until now, we have placed no assumptions on the nature of this process itself. Here, we say that an m-bit distribution is efficiently quantum preparable if it can be exactly prepared by performing single qubit measurements on the output state of a quantum circuit of polynomial description. Having thus argued for what we shall henceforth consider to be classical analogue of a quantum resource state, we now introduce the classical analogue of MBQC.

3.1.2 Measurement Based Classical Computing

As we have seen, MBQC can be split into three main components, two of which are quantum — resource state and adaptive measurements — and one of which, the post processing, is classical. MBCC will now be defined as the classical analogue of MBQC, whereby all three of the computational components will be classical.

The first element to consider is the resource state, which shall now consist of a sample polled from a probability distribution over m-bit strings. The second element will be the classical analogue of adaptive measurements. Instead of these, we shall now exclusively consider classical post-processing on the output bit-strings. More specifically, only the classical NOT and the XOR gates will be allowed. This thus defines a new restricted model of computation, whereby classical post processing is performed on a sample from a probability distribution. In the following section, we introduce IQP^* circuit families, and study the complexity of probability distributions such circuits can generate.

3.2 IQP^* Circuit Families

In IQP circuit families, we saw that a gate set diagonal in the X basis is applied to an input state w, before all the qubits are measured in the computational basis, thus yielding an output bit-string m. We shall now, by considering a different uniformity condition, define a related family of quantum

circuits, IQP*. Next, by using postselection, it will be shown that IQP* can not be classically efficiently simulatable under Hypothesis 1. Finally, in order to study the complexity of quantum states generated by IQP* circuits, we introduce IQP* zero input state families.

3.2.1 IQP*

In the following, we first introduce the family of IQP* circuit families, before discussing how these circuits expressed in terms of generalised X rotations may be mapped to circuits in terms of generalised Z rotations.

Definition

In the original definition of the class IQP [53] and depicted in Fig. 3.1, the circuit families $\{C_n\}_{n\geq 1}$ were parametrised with the size of the input n. In the following, the uniformity condition is modified in order to depend on the input state itself $w = x_1 \dots x_n$, which will thus result in a circuit family $\{C_w\}$.

This choice is made in order to highlight the origin of the complexity present in the actual circuit, by pushing the dependency on the input into the actual circuit itself. Indeed, given an input initialised in the all zero state $|0\rangle^{\otimes n}$, any correct input can be obtained by simply applying Pauli X flips to the relevant qubits. Here, this will be treated as classical pre-processing.

Definition 3. *An IQP* circuit family is a family of IQP circuits, with input x and input size $n = |x|$, followed by computational basis measurements on every qubit, such that the number of qubits q is polynomial in n, and where the unitary operator U_n (which has an explicit n-dependence) is a poly(n) product of gates of the form*

$$D(\theta_z, z) = e^{i\theta_z X[z]}, \tag{3.1}$$

where each angle $\theta_z \in (0, 2\pi]$ has a description polynomial-size in n, z is a q-bit string, and we introduce the notation $X[z] = \bigotimes_j X^{z_j}$, where z_j is the jth bit of z. E.g. $D(\theta_{101}, 101) = \exp[i\theta_{101}(X \otimes \mathbb{1} \otimes X)]$.

The circuits are thus described by a polynomial list of q-bit strings z and corresponding angles θ_z, where the all zero bit string z corresponds to a global phase. These correspond to generalised X rotations, and thus IQP* circuit families can not achieve universal quantum computation.

Computation in IQP* Circuit Families

Thus, here the input state $|w\rangle$ and ancillary qubits in the $|0\rangle$ state are acted upon by a circuit implementing the operator D_n, which is an operator diagonal in the X basis. Next, each qubit is measured

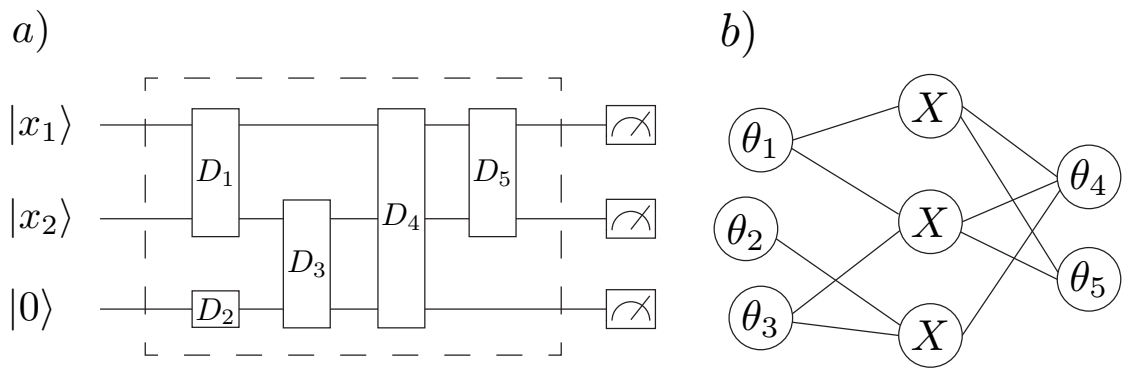


Figure 3.1: IQP *and MBQC*a) Standard form of an IQP circuit, where each gate is diagonal in the Pauli-X basis and (x_1, x_2) is the two bit input string. All measurements are in the computational (Pauli-Z) basis. The boxed gates give the unitary D. b) A MBQC implementation of the circuit in a), where each circle represents a qubit prepared in the state $|+\rangle$ and edges between circles represent the application of a controlled-Z gate. The contents of the circles represent the basis in which the corresponding qubit is measured, where X represents the Pauli-X basis, and θ_j represents the basis $U_X(-\theta_j)ZU_X(\theta_j)$, where $U_X(\theta_j)$ is a rotation by θ_j about the Pauli-X axis. The angles θ_j are in one-to-one correspondence with the θ_z in the representation of D_j in Eq. (3.1). All of these measurements can be implemented simultaneously (non-adaptively) in MBQC.

and we choose to express the output bit string as modulo two sum of the input w and a new bit string y, that is the output s given by $|w \oplus y\rangle$. Here, we see that this is equivalent to the unitary operator D_n acting on the all null state $|0\rangle^{\otimes n}$ with computation output $|y\rangle$. That is, IQP* circuits have the following interesting property, which shall be of subsequent use:

$$\langle w \oplus y|D_n|w\rangle = \langle y|D_n|0\rangle, \tag{3.2}$$

for all w, y, where $|0\rangle = |0\rangle^{\otimes q}$, and where $\oplus$ is bit-wise sum modulo 2.

From X to Z Diagonal circuits

Finally, in definition 3, IQP* circuits were introduced, whereby only operations implementing generalised X rotations were allowed. An alternative, equivalent definition of IQP* circuits may be given in terms of generalised Z rotations. We now explain how this can be achieved.

Given that the Hadamard gate is its own inverse, i.e. $H^2 = \mathbb{1}$, we can place two consecutive Hadamard gates on every single qubit at the beginning of the IQP* circuit, then in between of every single gate, and finally, on each qubit at the end of the circuit. Under Clifford conjugation, gates diagonal in the X basis will now get mapped to gates diagonal in the Z basis, i.e. $Z = HXH$. Thus, the input states are transformed from computational basis states to $|+\rangle$ states, and the final measurement is now of the observable X.

3.2.2 The C omplexity of IQP^*

In order to study the complexity of IQP^* circuit families, we use the same approach as that adopted in [53]. Here, postselection is introduced in order to first study the class $\mathsf{postIQP}^*$, which can then be used in order to make a statement about IQP^*.

Postselection and IQP^*

By adding postselection to our toolbox, we can consider the class of computation achieved by an IQP^* circuit family, given the ability to postselect on measurement outcomes which we call $\mathsf{postIQP}^*$. This is achieved by adding a postselection register, similarly to the classes $\mathsf{postBQP}$ or $\mathsf{postIQP}$.

Complexity of $\mathsf{postIQP}^*$

We previously saw that by adding postselection to IQP circuit families, these achieved the full power of universal quantum computing and postselection and thus of the class PP. Here, in lemma 7, we show that the ability to postselect on exponentially small outcomes boosts the power of IQP^* circuits to that of PP, precisely as was the case with IQP circuits.

Lemma 7. $\mathsf{postIQP}^* = \mathsf{postBQP} = \mathsf{PP}$.

The crucial element of the proof is to show that, given postselection, any computation in $\mathsf{postBQP}$ can be achieved in a $\mathsf{postIQP}^*$ circuit. This is achieved by considering how, given postselection, an MBQC instance can be implemented in a postselected IQP^* circuit family.

Proof. From Aaronson, it is known that $\mathsf{postBQP} = \mathsf{PP}$. Thus, in order to prove lemma 7, we need to show that $\mathsf{IQP}^* \subseteq \mathsf{postBQP}$ and $\mathsf{postBQP} \subseteq \mathsf{postIQP}^*$. The first inclusion is obvious, as IQP^* circuits form a subclass of general quantum circuits. Thus, we shall now show how an instance of $\mathsf{postBQP}$ can be implemented in a $\mathsf{postIQP}$ circuit.

We start with an instance of an MBQC circuit. Here, the input determines the generated graph state, which comprises of qubits initialised in the $|+\rangle$ state which are connected via controlled-Z gates. Next, single qubit measurements are performed in either the computational basis or onto the equatorial plane of the Bloch sphere. These measurements are adaptive, that is, dependant on previous outcomes in order to compensate for the by-product operators due to the randomness of measurement outcomes.

Now, as we consider that postselection is part of our toolbox, we can simply postselect on measurement outcomes thereby no longer generating unwanted Pauli errors. Thus, the measurements are no longer required to be adaptive. Next, we shall show that such an instance may be implemented in a $\mathsf{postIQP}^*$ circuit.

First, in the case of an MBQC instance, a graph state determined by the input is prepared. This is a state where the qubits are initialised in the $|+\rangle$ state and where adjacent qubits are connected by a controlled-Z gate. As $\mathsf{postIQP}^*$ circuits act on the all zero input, we now require the parametrisation to be shifted into the measurements to be performed. This can be done as given a sufficiently large cluster state, we can generate any graph state by performing Z measurements on it.

Thus, the first step is to express the MBQC instance in the circuit model.

More precisely, the following procedure is applied to an n-qubit state we follow the following procedure. For an input $w = x_1 \dots x_m$, if $x_i = 0$ then an X measurement is performed, whereas if $x_i = 1$ a rotation around Z by an angle π is performed. The second case effectively applies a Z gate to the qubit up to a global phase. As these commute with the controlled-Z gates, these can be incorporated into state preparation, and we thus prepare $|+\rangle$ or $|-\rangle$ states if respectively x_i is 0 or 1. For the rest of the qubits, measurements are determined by the size n.

First, we express our MBQC instance in the circuit model. Next, a measurement in the equatorial plane of the Bloch sphere corresponds to a measurement of the observable $R_z(\theta)XR_z(-\theta)$. We can thus equivalently perform a rotation around Z axis followed by X measurement, which can now be implemented in the circuit model.

Thus, the circuit is made up of gates diagonal in the Z basis acting on an input state which is an eigenstate of the Pauli X operator. Finally, a measurement of the observable X is performed on every qubit. Previously, we saw how such a circuit could be mapped to a generalised X rotation acting on the all zero state, with output determined by computational basis measurements. This corresponds to an IQP^* circuit thus implementing an MBQC instance, as illustrated in Fig.3.1. □

The class of $\mathsf{postIQP}^*$circuits is thus very powerful, and we next investigate the question of sampling from such families.

Sampling from IQP^*

In the following, we consider the question of weakly sampling from the output probability distribution of an IQP^* circuit family up to a multiplicative error. As seen in section X, this means that we ask whether a classical device could output samples from a distribution that closely approximates those generated by IQP^* circuits. Here, lemma 3 tells us that this is impossible, similarly to what we saw in the case of IQP circuits.

Lemma 8. *The output probability distributions generated by IQP^*circuit families cannot be efficiently and exactly simulated on a standard classical computing device unless the polynomial hierarchy collapses to the third level.*

In chapter 1, we introduced Hypothesis 1, a fundamental assumption in computer science, which

stated that the levels of the polynomial hierarchy are distinct. We now briefly sketch the proof of lemma 8 , which relies on combining lemma 7 with the proof techniques used in [53]. More precisely if IQP^* circuits could be weakly simulated up to multiplicative error $c \geq 1$, then we would have that IQP is contained in BPP. This in turn implies that $\mathsf{postIQP} \subseteq \mathsf{postBPP}$, which is itself contained within the third level of the polynomial hierarchy $\mathsf{BPP} \subseteq \mathsf{PH}_3$. Thus, when these two results are combined, we obtain that $\mathsf{PP} \subseteq \mathsf{PH}_3$, which implies that the polynomial hierarchy collapses to the third level. As this result is extremely unlikely, we are thus forced to conclude that IQP^* circuits can not be weakly classically simulated.

Thus, these circuits can be considered non-classical, and in the the next section we considers the families of quantum states such circuits can generate, as well as the resulting statistics from performed measurements.

3.2.3 The Complexity of IQP* Zero Input Families

We now consider the families of quantum states obtained at the end of an IQP^* circuit. In order to ensure no complexity is hard-wired into the input state, we require the circuit to act on the all zero input state, that is we now have that $|w\rangle = |0\rangle^{\otimes n}$.

More formally, we introduce IQP^* zero-input state families in order to capture the class of quantum states which can be generated by an IQP^* circuit.

Definition 4. *An IQP* zero-input state family is the set of quantum states created by an IQP* circuit family when the input is set to the all zeros string* $0 \ldots 0$.

Next, we will wonder whether such classes of quantum states can be used as a resource state, even though these originated from a restricted class of quantum circuits. We imagine that a measurement is performed on an IQP^* state, and we consider its output statistics. Here, we find that these can not be classically efficiently simulated, and are thus in a sense non-classical.

Corollary 1. *The statistics of computational basis measurements on IQP* zero input state families cannot be efficiently and exactly simulated on a standard classical computer unless Hypothesis* 1 *is false.*

Proof. First, in order to make the input string x of same size as the output, it is appended with zeroes, resulting in the string $\bar{x}$. Next, the operator D_n, which is diagonal in the X basis, is applied to the input $\bar{x}$, before every single qubit is measured in the computational basis thus yielding the classical output bit string m. We have that the probability of obtaining the output m given the input $\bar{x}$ is given by:

$$\mathrm{P}[m|x] = |\langle m|D_n|\bar{x}\rangle|^2. \tag{3.3}$$

But, we previously saw that $\langle m|D_n|\bar{x}\rangle = \langle m \oplus \bar{x}|D_n|0\rangle$, and thus $\mathrm{P}[m|x] = |\langle m \oplus \bar{x}|D_n|0\rangle|^2$. This can now be interpreted as the probability of obtaining the output string $m \oplus \bar{x}$ on the all zero input, and thus we have that: $\mathrm{P}[m|x] = \mathrm{P}[m \oplus \bar{x}|0]$.

Thus, the probability of outcome is identical to that obtained by applying the circuit to the all zero input state and doing some classical post-processing on the output, mapping m to $m + \bar{x}$. This will involve at most n bit flips, and can be efficiently performed classically. Thus, our result follows from lemma 1. □

This tells us that the classical distribution has inherited the hardness of the of exact simulation of the IQP^* quantum circuit families. We will now investigate how this may be used as a resource for MBCC, and study the nature of the resulting computation.

3.3 The Complexity of MBCC

Having thus introduced both the model of MBCC as well as the family of IQP^* circuits, we can proceed to consider the power of MBCC and the role of adaptivity in computation.

3.3.1 MBQC and IQP^*

First, we consider MBQC where the measurements are restricted to being non-adaptive and fixed, that is, not depending on previous measurement outcomes. Although this poses a severe restriction on the classes of achievable computations, we find that it is nevertheless possible to implement an IQP^* circuit instance.

Lemma 9. *Given a member of an IQP^* circuit family, there is an efficient implementation in MBQC whose measurements are fixed and non-adaptive.*

Proof. Previously, in the proof of corollary 1, we saw that for IQP^* circuits, the probability of getting outcome string m given an input x is given by $\mathrm{P}[m|x]$ =$\mathrm{P}[m\oplus\bar{x}|0]$. Thus, we can exclusively consider circuits acting on the all zero state, given some additional classical post-processing. In addition, as previously discussed, as Hadamard gates have the property that $H^2 = \mathbb{1}$, we can add these to the circuit in order to map the original X diagonal circuit to one diagonal in the Z eigenbasis. The inputs will now correspond to $+1$ eigenvalue X eigenstates and the qubits will be measured in the X basis. Since the control-Z gate has the property that $\mathrm{CZ}^2 = \mathbb{1}$, these can be inserted into the circuit. The first one will be pulled towards the input state in order to obtain the cluster state, whilst the second will be considered to be part of the circuit.

A generalised Z-rotation can be expressed:

$$D_z(\theta_z, z) = e^{i\theta_z Z[z]}, \tag{3.4}$$

where $z = z_1 \dots z_n$, and $Z[z] = Z^{z_1} \otimes \dots Z^{z_n}$. In MBQC, these can be implemented by performing simultaneous measurements, which will give rise to by product operators of the form $Z \otimes \mathbb{1}$. As these now commute with the gate set, they can be pushed to the end of the computation, and thus the measurements will no longer be required to be adaptive. Thus, we have shown that IQP^* circuit instances can be implemented in non-adaptive MBQC. □

3.3.2 Fixed Bases MBQC

Here, we once again consider MBQC with fixed bases, and now find that even though the computation still has access to an entangled resource state, it can be simulated by an MBCC.

Lemma 10. *For every instance of MBQC on an n-qubit resource, where every measurement basis is fixed, there is a corresponding instance of MBCC with an n bit resource, whose output statistics simulate it exactly.*

Proof. Let O be the observable to be measured. The output statistics will be completely determined by the elements of O which are diagonal in its eigenbasis. If a completely dephasing channel with respect to O's eigenbasis is applied, then all the non-diagonal elements disappear, and the resulting state is separable and discord-free.

Thus, when a measurement of the observable O is performed, the output statistics are left invariant by the application of the completely dephasing channel in the O eigenbasis prior to measurement. Such a measurement will define a probability distribution, a sample of which can be used in MBCC, thus simulating an MBQC instance. □

3.3.3 Non-classicality of MBCC

Finally, we consider the power of MBCC. First, we found that even if an MBQC is restricted by requiring the measurement bases to be fixed, it can nonetheless implement IQP^* circuit families. Next, we found that fixed basis MBQC could be implemented by an MBCC. Thus, by combing these two results and recalling that IQP^* circuits are hard to classically efficiently simulate we find that MBCC is an essentially non-classical model of computation.

Theorem 4. *There exist uniform families of MBCC computations with efficiently quantum preparable resources which cannot be efficiently exactly simulated via a standard classical computing device unless the polynomial hierarchy collapses to the third level.*

Proof. From lemma 10 and 9, we get that IQP^* circuit families can be implemented in MBCC with efficiently preparable quantum resource. In conjunction with lemma 8, we obtain our main result, theorem 1 stating that MBCC demonstrates non-classicality. □

3.4 Conclusion

It is known that there exists restricted quantum circuits which although may seem very simple, such as in the case of IQP circuit families, which are hard to classically efficiently simulate. Here, it is important to note that sampling problems are now considered. These have experimental implications, for they reflect the classes of quantum devices which may currently be built and suggest that these non-universal models may be more powerful than classical computers, as for instance in Boson Sampling [119].

3.4.1 Results

Here, we have studied the complexity of probability distributions arising from quantum processes, and have shown that these exhibit non-classical behaviour and can thus be used as a resource. By exploiting this property, we were able to define the computational model of MBCC as the classical analogue of MBQC, which we found is not classically efficiently simulatable.

This work probes the role of adaptivity in computation, via the connection between MBQC and IQP circuits. In addition, this research highlights the importance of the processes giving rise to probability distributions we wish to sample from. Indeed, we have seen that probability distributions arising from quantum processes can be intrinsically complex, which, in turn, will translate into hardness of sampling.

3.4.2 Future Directions

Further work in the study of sampling from probability distributions is required, with an emphasis on the more direct experimental applications. Furthermore, the tool of postselection was once again used in order to determine the complexity of a computational class.

Chapter 4

Non-Unitary Quantum Computation in the Ground Space of Local Hamiltonians

The k-LOCAL HAMILTONIAN problem connects the field of physics to that of computer science, through the study of a Hamiltonian's spectrum via the lens of computational complexity. This idea, originally due to Kitaev [45], builds upon a mapping between quantum circuits and Hamiltonian operators which is known as the circuit-to-Hamiltonian construction.

The starting point of this construction is to consider the unitary evolution of a given input state which is implemented by the application of a quantum circuit. By decomposing the unitary operator in a finite sequence of local unitary gates and by appending a clock register to the system in order to track the time, the discrete evolution of the input state throughout the successive stages of the computation is modelled. The history state $|\eta\rangle$ of the computation can then be defined as an equal superposition over all correct computational states. Finally, a Hamiltonian operator whose kernel contains precisely this history state can thus be constructed.

Crucially, it was shown that the k-LOCAL HAMILTONIAN problem is QMA-complete, thus providing the fundamental insight that computing ground state energies is a hard problem, even given access to a quantum computer. More precisely, determining whether a system has ground state energy E_0 that is less than a or greater than b is a hard problem, where $\delta = b - a$ defines an important quantity known as the promise gap.

The Promise Gap

Indeed, the k-LOCAL HAMILTONIAN's proof of QMA-hardness hinges upon the correspondence between the promise gap and the error resolution of the computational device. In chapter 1, we saw that in any probabilistic computation there exists the possibility of obtaining an erroneous output, whereby the computation will output either a 1 in the case of a no-instance or a 0 for a yes-instance.

If the error probability scales as an inverse polynomial with system size, then by repeating the computation a polynomial number of times and taking a majority vote, the correct output will be determined.

For the k-LOCAL HAMILTONIAN problem, the ability to resolve between the cases when the Hamiltonian has ground state energy less than a or greater than b in turn allows us to determine whether a quantum circuit is accepting or rejecting upon input. Crucially, this reduction will hold only if the promise gap δ satisfies a scaling constraint, as this in turn places a lower bound on the tolerated error resolution. Thus, for the problem to be in QMA, a spectral gap scaling as an inverse polynomial with system size $b - a \geq \frac{1}{\text{poly}(n)}$ is required, and we can thus think of this as approximating the ground state energy to polynomial accuracy. It is for these reasons that the promise gap plays a central role in the field of Hamiltonian complexity.

Hamiltonians and Non-Unitary Evolution

Yet, since the original formulation of the k-LOCAL HAMILTONIAN problem, alternative models of computation have been devised such as MBQC, which was discussed and introduced in chapter 1. Here, the computation is driven by performing single qubit measurements on an entangled resource state. This is a non-unitary model of computation, which is nonetheless equivalent to the circuit model in terms of computational power. Thus, the question arises as to whether the k-LOCAL HAMILTONIAN problem might be extended to such a non-unitary computational paradigm.

In the following, we introduce a novel family of Hamiltonian operators which encode non-unitary computation within their groundspace. These will correspond to evolutions implemented by measurements, which we model as a renormalised projector applied to a quantum state. Ultimatelty, the complexity of the states encoded within the Hamiltonian's kernel needs to be analysed. But first, this will require for an additional element to be considered: postselection on measurement outcomes.

Postselection as a Resource

Postselection was previously introduced as a novel computational tool, which led to the intriguing if unrealistic model of postselected computation, captured by the complexity class postBQP. It was shown that the ability to postselect on measurement outcomes increases the power of a quantum computer, boosting the class BQP to that of PP, and thus providing us with the insight that quantum mechanics taken in conjunction with postselection is a powerful tool.

At the same time, postselection can be viewed as a resource, one of the many tools one might use in order to probe the power of computation. For instance, the proof that postIQP circuits are hard to classically efficiently simulate relies on the use of postselection, and thus ultimately allows

for a strong claim about the power of IQP circuits, as opposed to postIQP, to be achieved.

Postselection and Hamiltonians

Thus, the ability to postselect on measurement outcomes will allow for the spectrum of Hamiltonian operators encoding non-unitary evolution to be probed. Furthermore, this approach provides us with a framework in order to study postselection within the context of quantum verification problems. That is, we ask how adding the ability to postselect on measurement outcomes impacts on the power of QMA. Here, the output of the verifier circuit would now be conditioned on the measurement outcomes of a postselection register. In terms of local Hamiltonian's, this would dramatically increase the computational power of the verifier and thus, a priori, it would seem difficult to include states encoding postselected circuits in the ground space of a Hamiltonian. Indeed, one would expect this to lead to an exponentially closing gap.

Tame Postselection

Yet, we wish to consider postselection as part of the computational toolbox, and investigate the resulting family of Hamiltonians and their complexity. This motivates us to introduce tame postselection as a restricted form of postselection, which subsequently allows us to generalise the class of postselection gadgets of which the Hadamard gadget is an example. Here, we propose to study the effect of postselection in circuits and their associated Hamiltonian, with the aim of finding examples of these which do not demonstrate an unreasonable increase in computational power resulting in an exponentially closing gap. We will thus wonder whether postselection may be used in a manner, which, although non trivial, does not dramatically increase our computational power.

Structure

First, in section 4.1 we will investigate the role of postselection, by first introducing the notion of tame postselection, and then discussing its connection to the application of a renormalised projector to a quantum state. Next, in section 4.2 we shall consider how general evolution can be encoded within the kernel of a Hamiltonian, an analysis which will allow us to recover Kitaev's original Hamiltonian formulation. Next, this will allow us in section 4.1.3 to introduce a new family of Hamiltonian operators encoding evolution via renormalised projectors in its nullspace. We shall see how such a construction is relevant to a Hamiltonian encoding IQP circuits, before focusing on the Hadamard gadget. Next, in order to study the spectrum of Hamiltonian operators encoding both unitary and non-unitary evolution, we shall, in section 4.3, conduct a numerical analysis of two circuits which although similar produce strikingly different results. Finally, we will close this chapter with some comments for future work and a discussion of further connections to computational

complexity.

4.1 Hamiltonians, Postselection and Renormalised Projectors

In the following, we wish to consider the case of quantum evolution implemented by performing measurements on subsystems. First, in section 4.1.1, we discuss postselection, and introduce the concept of tame postselection, motivated by the idea that the outcome probabilities don't necessarily yield information regarding the output state. Then, proposition 6 shows us that in certain cases measurements implemented on one part of the system implement an operator proportional to a unitary on the other part of the system, and we shall see that the Hadamard gadget is one such example. Next, in section 4.1.2, we discuss the general form of evolution of a quantum state, and the associated Hamiltonian operator, which will then allow us, in section 4.1.3, to consider the case of non-unitary evolution.

4.1.1 Measurements, Postselection and Renormalised Projectors

Tame Postselection

Postselection on measurement outcomes corresponds to conditioning the computation on the outcome of a measurement. Here, we consider that a unitary operator is applied to an initial input state $|\psi\rangle|00...0\rangle$, which thus evolves to $U|\psi\rangle|00...0\rangle$. Then, a measurement $\{\Pi, \mathbb{I} - \Pi\}$ is applied to the system, where Π and $\mathbb{I} - \Pi$ are projectors. We then postselect on the outcome associated with Π occurring, and consider the case where the probability of obtaining this outcome is independent of the initial state $|\psi\rangle$. Note that the probability of obtaining the outcome could be exponentially small in the size of $|\psi\rangle$. We emphasize that we only demand that the probability be independent of only $|\psi\rangle$; it could vary if we replace the state $|00...0\rangle$ with another (known) quantum state.

Definition 5. *Given a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_{sys} \otimes \mathcal{H}_{anc}$ consisting of a system with space $\mathcal{H}_{sys}$, and an ancillary system with space $\mathcal{H}_{anc}$ (both with the same dimension), in an initial quantum state $|\phi\rangle = |\psi\rangle|0\rangle$ such that $|\psi\rangle \in \mathcal{H}_{sys}$ and $|0\rangle \in \mathcal{H}_{anc}$, if a unitary U is applied to $|\phi\rangle$ followed by a projective measurement $\{\Pi_k := |k\rangle\langle k|\}_k$ with outcomes $\{k\}$ applied to the system $\mathcal{H}_{sys}$, then post-selection on a particular outcome k' is **tame post-selection** if $p(k') := \langle\psi|\langle 0|U^\dagger(\Pi_{k'} \otimes \mathbb{I}_{anc})U|\psi\rangle|0\rangle$ is the same for all $|\psi\rangle \in \mathcal{H}_{sys}$.*

An example of tame post-selection would be the Hadamard gadget, which was used in Ref. [53] to show the classical hardness of IQPSAMPLING. This is a method of implementing a Hadamard gate via measurement and postselection, as illustrated in Fig. 4.1. Here, a qubit in an arbitrary state $|\psi\rangle$ is entangled with an ancilla (initialised in the fixed $|+\rangle$ state) via a controlled-Z operator

$|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes Z$, with Z being the Pauli-Z operator. Then, the first qubit is measured in the Pauli-X basis $\{|+\rangle, |-\rangle\}$ and we post-select upon obtaining the outcome associated with state $|+\rangle$. This results in the state on the second qubit being $H|\psi\rangle$. Here, the probability of obtaining the measurement outcome is $1/2$ for both outcomes, and thus is independent of the state $|\psi\rangle$. On the other hand, if we were to alter the ancilla to have another state other than $|+\rangle$, this probability could change. This helps us emphasize that tame postselection is tame with respect to a particular input subsystem.

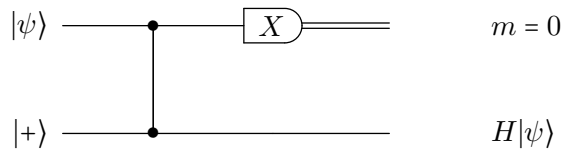


Figure 4.1: *Hadamard gadget.* The input state $|\psi\rangle$ is entangled with an ancilla in the $|+\rangle$ state via a controlled-Z operator. Then, the first qubit is measured in the X basis. By postselecting on outcome $m = 0$, a Hadamard gate is applied to the unknown input state.

Unitary Evolution via Measurement

In both MBQC and one-bit teleportation, measurements performed on one part of a system can effectively implement a unitary operator on a set of unmeasured qubits. Here, we consider an unknown arbitrary state $|\psi\rangle$ to which a projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ is applied, yielding outcome $m = 0$ with probability p and $m = 1$ with probability $(1 - p)$. If the outcome $m = 0$ is obtained, then the renormalised post measurement state is given by $\frac{1}{\sqrt{p}}\Pi|\psi\rangle$, where the probability p needs to be known in order for the state to be renormalised. Thus, if we know that the outcome $m = 0$ occurs, we can interpret this as a renormalised projector $\frac{1}{\sqrt{p}}\Pi$ having been applied to the input state. Postselection offers us the guarantee that a given measurement outcome is obtained, and thus, if the outcome probability is constant for all input states, we can view postselection as having effectively applied a renormalised projector to the input state.

This postselection results in a unitary operator being applied to the unmeasured system, a concept which is at the core of MBQC wherein unitary evolution is simulated by measurements. We generalise this kind of postselection gadget in the following result.

Proposition 6. *Let $|\psi\rangle \otimes |e_0\rangle$ be a quantum state in a Hilbert space $\mathcal{H} = \mathcal{H}_{sys} \otimes \mathcal{H}_{env}$, where $|\psi\rangle \in \mathcal{H}_{sys}$ and $|e_0\rangle \in \mathcal{H}_{env}$, and the two Hilbert spaces have the same dimension. Suppose a unitary operator U is applied to the joint system, followed by a projective measurement on the environment in the orthonormal basis $\{|e_k\rangle\} \in \mathcal{H}_{env}$, as illustrated in Fig. 4.2. Let $p_m = \langle\psi| \otimes \langle e_0|(|e_m\rangle\langle e_m| \otimes$*

$\mathbb{1}$)$|\psi\rangle \otimes |e_0\rangle$ *denote the probability of outcome* m *occurring. Then, if* p_m *is independent of the input state* $|\psi\rangle$*, the action of this process on the system is equivalent to applying* $\sqrt{p_m}V_m$ *to* $|\psi\rangle$*, where* V_m *is a unitary operator.*

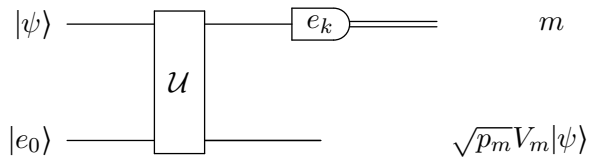


Figure 4.2: *Evolution via measurement.* A unitary operator is applied to an unknown state $|\psi\rangle$ and an uncorrelated ancilla $|e_0\rangle$, before the system is measured. This results in a sub-normalised unitary being applied to the ancilla.

Proof. The system is prepared in the state $|\psi\rangle \in \mathcal{H}_{sys}$ and is initially uncorrelated with the ancillary qubit $|e_0\rangle \in \mathcal{H}_{env}$. A unitary operator U acting on the joint state space $\mathcal{H} = \mathcal{H}_{sys} \otimes \mathcal{H}_{env}$ is applied, followed by a projective measurement onto a set of orthonormal states $\{|e_k\rangle\}$, as illustrated in Fig. 4.2. If the measurement outcome m is obtaine, then the resulting evolution is given by:

$$\rho \otimes |e_0\rangle\langle e_0| \to (\mathbb{1} \otimes |e_m\rangle\langle e_m|)U(|\psi\rangle\langle\psi| \otimes |e_0\rangle\langle e_0|)U^\dagger(\mathbb{1} \otimes |e_m\rangle\langle e_m|). \tag{4.1}$$

Once the unitary operator U and measurement $\mathbb{1} \otimes |e_m\rangle\langle e_m|$ have been applied, the environment system with Hilbert space $\mathcal{H}_{env}$ is in the state ρ'_{env}. The evolution of the environment state can be modelled by a CPTP map acting on the input state $|e_0\rangle\langle e_0|$, which is defined by:

$$\rho' = \varepsilon_m(\rho) = \mathrm{tr}_{sys}\left(\mathbb{1} \otimes |e_m\rangle\langle e_m|)U(|\psi\rangle\langle\psi| \otimes |e_0\rangle\langle e_0|)U^\dagger(\mathbb{1} \otimes |e_m\rangle\langle e_m|\right), \tag{4.2}$$

and where m denotes the measurement outcome.

The CPTP map acting on the ancillary qubit can alternatively be expressed as a Kraus decomposition, where Kraus operators K_m are defined by: $K_m = \langle e_m|U|e_0\rangle$. The measurement outcome m occurs with probability p_m given by $p_m = \mathrm{Tr}(|\psi\rangle\langle\psi|K_m^\dagger K_m)$. The sum of probabilities over measurement outcomes is required to equal one, and thus we have that $\sum_m K_m^\dagger K_m = \mathbb{1}$. Here, in addition, we demand that the outcome probabilities be independent of the input state $|\psi\rangle$:

$$p_m = \langle\psi|K_m^\dagger K_m|\psi\rangle, \quad \forall|\psi\rangle. \tag{4.3}$$

As the operator $K_m^\dagger K_m$ is hermitian, it has has a spectral decomposition given by:

$$\sum_k \lambda_k^{(m)} |v_k^{(m)}\rangle\langle v_k^{(m)}|, \tag{4.4}$$

and the constraint on outcome probabilities is thus given by:

$$p_m = \lambda^{(m)} \sum_k |\langle\psi|v_k^{(m)}\rangle|^2 = \lambda^{(m)}, \quad \forall|\psi\rangle. \tag{4.5}$$

In order for this constraint to be satisfied for all input states, we require that:

$$K_m^\dagger K_m = p_m \mathbb{1}. \tag{4.6}$$

This, in turn, means that each Kraus operator must be proportional to a unitary operator, that is $K_m = \sqrt{p_m} V_m$, where $V_m = \frac{1}{\sqrt{p_m}}\langle e_m|U|e_0\rangle$. We can interpret this as applying a renormalised projector $\frac{1}{\sqrt{p_m}}|e_m\rangle\langle e_m|$ to the environment. Thus, a unitary operator can be implemented on a subsystem by applying a renormalised projector on a larger system in the case when the outcome probabilities are input independent. □

This proposition tells us that when a unitary operator is followed by a measurement, if the outcome probabilities do not yield any information about the input state, then we can equivalently view this as unitary operator having been applied to the input state. Thus, we can now realise that the Hadamard gadget is one such example.

Example: the Hadamard Gadget

We previously introduced the Hadamard gadget, a key construction in the proof of hardness of IQP sampling. A Hadamard gate can be applied to an arbitrary single qubit state $|\psi\rangle$ by performing the circuit depicted in Fig. 4.1. The state is entangled with an ancillary qubit and subsequently measured, where we postselect on measurement outcome $m = 0$. This method of implementing a Hadamard gate via measurement and postselection is known as a Hadamard gadget. Here, the probability of obtaining outcome m is given by $\mathrm{P}[m] = \frac{1}{2}$ for $m \in \{0, 1\}$, and thus yields no information as to the unknown input state $|\psi\rangle$.

Example 18. *For a Hadamard gadget, the environment is initialised in the state $|e_0\rangle = |+\rangle$, the applied operator is the controlled-Z gate, i.e. $U = CZ$ and the measurement is in the X basis. From proposition 6, this results in the single qubit operator given by $V_m = \langle+|Z^m CZ|+\rangle = HZ^m$ being implemented. The outcome probability is input independent and equal to 0.5. When we postselect on outcome $m = 0$, a Hadamard gate is applied, i.e. $V_0 = H$.*

Having now introduced tame postselection, we can now consider the question of Hamiltonian operators encoding evolution via renormalised projectors. In order to do so, the first step is to discuss how the general evolution of a quantum state may be encoded within the groundspace of a Hamiltonian operator.

4.1.2 A General Evolution

A general approach to quantum state evolution is to consider an initial quantum state $|\psi\rangle$ which evolves to a new quantum state $|\psi'\rangle$. Here, we consider discrete time evolution, and can thus say that the system is in state $|\psi\rangle$ at time step t and $|\psi'\rangle$ at time step $t+1$. We assume that the final state $|\psi'\rangle$ is related to $|\psi\rangle$ by an unknown operator L, that is $|\psi'\rangle = L|\psi\rangle$. If there are T time steps, then we can adjoin a qudit of dimension $T+1$ to the system in order to track the discrete time evolution. The evolution thus corresponds to the un-normalised history state:

$$|\eta\rangle = |\psi\rangle \otimes |t\rangle + L|\psi\rangle \otimes |t+1\rangle. \tag{4.7}$$

The next step is to construct a positive operator H_t such that this history state $|\eta\rangle$ lies within its kernel. If $|\psi\rangle$ is an N-qubit state, then the resulting dimension of the Hamiltonian operator on the state and clock space is $2^N \otimes (T+1)$. The span of the clock states $\{t, t+1\}$ forms a two dimensional Hilbert space, and the operator H_t may thus be decomposed as:

$$H_t = N\big(H_{11} \otimes |t\rangle\langle t| + H_{12} \otimes |t\rangle\langle t+1| + H_{21} \otimes |t+1\rangle\langle t| + H_{22} \otimes |t+1\rangle\langle t+1|\big), \tag{4.8}$$

where N is a normalisation constant and the operator H_ij acts on the initial state $|\psi\rangle$. The history state $|\eta\rangle$ is required to be a ground state of H_t, and thus $H_t|\eta\rangle = 0$. By substituting for the two above expressions, we obtain:

$$N(H_{11}|\psi\rangle + H_{12}L|\psi\rangle \otimes |t\rangle + H_{21}|\psi\rangle \otimes |t+1\rangle + H_{22}L|\psi\rangle \otimes |t+1\rangle) = 0. \tag{4.9}$$

In order for this to equation to be satisfied, the following system of two equations must hold:

$$\begin{cases} H_{11}|\psi\rangle + H_{12}L|\psi\rangle = 0, \\ H_{21}|\psi\rangle + H_{22}L|\psi\rangle = 0. \end{cases} \tag{4.10}$$

The operator H corresponds to a Hamiltonian, its eigenvalues correspond to energy. As these are real numbers, H_t is also demanded to be a Hermitian operator, which imposes the additional constraint

that $H_{21} = H_{12}^{\dagger}$. We thus have that:

$$\begin{cases} H_{11}|\psi\rangle + H_{12}L|\psi\rangle = 0, \\ H_{12}^{\dagger}|\psi\rangle + H_{22}L|\psi\rangle = 0. \end{cases} \tag{4.11}$$

Without loss of generality, the operator H_t is required to be a projector, and thus $H_t^2 = H_t$. This thus constitutes the constraints a Hamiltonian operator must satisfy in order to encode the evolution of a quantum state between two consecutive time steps. Next, we consider the case of unitary operations, which as expected yields Kitaev's Hamiltonian encoding unitary evolution.

Unitary Evolution

In the unitary model of quantum computation, evolution occurs via the application of a unitary operator to the system. In this case, we have that $L = U$, where U is a unitary operator such that $UU^{\dagger} = \mathbb{1}$. Thus, we can rewrite equation 4.11 as:

$$\begin{cases} H_{11}|\psi\rangle + H_{12}U|\psi\rangle = 0, \\ H_{12}^{\dagger}|\psi\rangle + H_{22}U|\psi\rangle = 0. \end{cases} \tag{4.12}$$

It is easy to see that a solution to this system of equations is given by $H_{11} = \mathbb{1}, H_{12} = -U^{\dagger}, H_{21} = -U$, and $H_{22} = \mathbb{1}$. The requirement that H_t is a projector, that is $H_t^2 = H_t$, yields the normalisation constant $N = \frac{1}{2}$. Thus, the resulting Hamiltonian operator encoding unitary evolution is given by:

$$H_t = \frac{1}{2}(\mathbb{1} \otimes |t\rangle\langle t| - U \otimes |t+1\rangle\langle t| - U^{\dagger} \otimes |t\rangle\langle t+1| + \mathbb{1} \otimes |t+1\rangle\langle t+1|), \tag{4.13}$$

which is precisely that obtained by Kitaev. Yet, evolution need no necessarily be unitary, and we next consider the case of non-unitary evolution via measurement which will thus yield a new form of Hamiltonian operator.

4.1.3 Non-Unitary Evolution via Renormalised Measurement

The unitary model of computation has given rise to an interesting class of Hamiltonian operators, which has allowed for the connections between physics and computer science to be probed. Thus, we can wonder whether it would be possible to go beyond the unitary model of evolution, by for instance considering evolution via measurements, as is the case in MBQC. This would thus correspond to a non-unitary model, which is modelled by the application of a renormalised projector to the system. This in turn requires for the outcome probabilities to be known for all input states.

More formally, we now consider the Hamiltonian encoding the evolution of a state $|\psi\rangle$ at time t

to a new state $|\psi'\rangle = L|\psi\rangle$ at time $t+1$, where the operator L is proportional to a projector, that is $L = \Pi/\sqrt{\langle\psi|\Pi|\psi\rangle}$ and where Π is a projector.

Proposition 7. *Given a projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ at time step t, for the measurement outcome on state $|\psi\rangle$ corresponding to projector Π occurring with probability $p = \langle\psi|\Pi|\psi\rangle$ independent of input state $|\psi\rangle$, then the un-normalised history state $|\eta\rangle = |\psi\rangle \otimes |t\rangle + L|\psi\rangle \otimes |t+1\rangle$ lies in the kernel of*

$$H_t = \frac{p}{p+1}\Big(\frac{1}{\sqrt{p}}\Pi \otimes \Big(\frac{1}{\sqrt{p}}|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + \sqrt{p}|t+1\rangle\langle t+1|\Big) + \Pi^{\perp} \otimes |t+1\rangle\langle t+1|, \quad (4.14)$$

for $L = \frac{\sqrt{p}}{\Pi}$.

Proof. Let the system be in a quantum state $|\psi\rangle$ at time step $|t\rangle$, which will evolve to a new state $|\psi'\rangle$ at time step $|t+1\rangle$. This evolution is implemented by a projective measurement $\{\Pi, \Pi^{\dagger}\}$, where $\Pi^{\dagger} = \mathbb{1} - \Pi$ and $\Pi^2 = \Pi$. Let $p = \langle\psi|\Pi|\psi\rangle$ be the probability that the renormalised post-measurement output state is $\frac{1}{\sqrt{p}}\Pi|\psi\rangle$. This can equivalently be viewed as a renormalised projector $\frac{1}{\sqrt{p}}\Pi$ having been applied to the input state, that is $L = \frac{1}{\sqrt{p}}\Pi$, and thus we have that the system of equations 4.11 can now be expressed:

$$\begin{cases} H_{11}|\psi\rangle + H_{12}\frac{1}{\sqrt{p}}\Pi|\psi\rangle = 0, \\ H_{21}|\psi\rangle + H_{22}\frac{1}{\sqrt{p}}\Pi|\psi\rangle = 0. \end{cases} \quad (4.15)$$

A natural solution to the above system of equations is given by: $H_{11} = \frac{1}{p}\Pi, H_{12} = -\frac{1}{\sqrt{p}}\Pi, H_{21} = -\frac{1}{\sqrt{p}}\Pi$, and $H_{22} = \Pi$. The Hamiltonian operator H_t encoding this evolution is thus given by:

$$H_t = N\Pi \otimes \Big(\frac{1}{p}|t\rangle\langle t| - \frac{1}{\sqrt{p}}|t\rangle\langle t+1| - \frac{1}{\sqrt{p}}|t+1\rangle\langle t| + |t+1\rangle\langle t+1|\Big), \quad (4.16)$$

where N is the normalisation constant which ensures that the Hamiltonian is a projector, that is that $H_t^2 = H_t$. If we consider the operator H_t^2, we have that:

$$H_t^2 = N^2(1+\frac{1}{p})\Pi \otimes \Big(\frac{1}{p}|t\rangle\langle t| - \frac{1}{\sqrt{p}}|t\rangle\langle t+1| - \frac{1}{\sqrt{p}}|t+1\rangle\langle t| + |t+1\rangle\langle t+1|\Big), \quad (4.17)$$

which can be expressed as $H^2 = cH$, where $c = N(1+\frac{1}{p})$. Thus, the normalisation constant depends on the probability outcome p:

$$N(p) = \frac{1}{1+\frac{1}{p}} = \frac{p}{p+1}. \quad (4.18)$$

By construction, the Hamiltonian operator H_t contains the history state $|\eta\rangle$ in its nullspace. But, due to the orthogonality of the projectors, the kernel will contain other states of the form:

$$\Pi^{\dagger}|\psi\rangle \otimes |t'\rangle, \quad (4.19)$$

which will be an issue for time step $t' = t+1$. In order to exclude such states form the Hamiltonian's kernel, it is necessary to add an extra term to it, penalising such states, which will be of the form:

$$\Pi^{\perp} \otimes |t+1\rangle\langle t+1|. \tag{4.20}$$

Thus, the Hamiltonian operator encoding the non-unitary evolution via renormalised measurements is given by:

$$H_t = N(p)\Big(\frac{1}{\sqrt{p}}\Pi \otimes \Big(\frac{1}{\sqrt{p}}|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + \sqrt{p}|t+1\rangle\langle t+1|\Big) + \Pi^{\perp} \otimes |t+1\rangle\langle t+1|, \tag{4.21}$$

where $N(p) = \frac{p}{p+1}$. □

Thus, having derived a Hamiltonian operator encoding evolution via renormalised measurement, we shall next investigate the class of computations whereby evolution occurs with both unitary operators and measurements.

4.2 Hamiltonians from Postselected Quantum Circuits

We now consider Hamiltonian's encoding quantum circuits whereby evolution occurs through both unitary and non-unitary processes. First, in section 4.2.1 we discuss the general structure of a circuit whereby computation proceeds through rounds of both unitary operators and renormalised measurements. Next in section 4.2.2, we discuss how IQP circuits are one such instance, and finally in section 4.2.3, we consider the Hamiltonian operator encoding a Hadamard gadget.

4.2.1 General postselected circuits

In the following, we consider the class of computations whereby the input $|\psi\rangle|00...0\rangle$ undergoes a sequence of T =poly(n) discrete time evolutions. Each individual evolution is either implemented by a unitary operator or by a renormalised projector, and thus the computation evolves in layers corresponding either to a unitary gate or a measurement. For example, after T time-steps of a circuit in which a unitary U_i is alternated with a renormalised projector L_j, the state of the system would be $|\psi_T\rangle = U_T L_{T-1} ... L_2 U_1 |\psi\rangle$, and thus the history state of the computation is given by:

$$|\eta\rangle = \frac{1}{T+1}\big(|\phi\rangle \otimes 0\rangle + \ldots + |U_T L_{T-1} \ldots U_1|\psi\rangle \otimes |T\rangle\big). \tag{4.22}$$

The Hamiltonian operator encoding the above evolution is given by the sum three terms, corresponding to an input, propagation and output Hamiltonian: $H = H_{in} + H_{prop} + H_{out}$.

Input and Output Hamiltonian

The input of the computation is the m-qubit quantum proof state $|\psi\rangle$ and a set of $N - m$ auxiliary qubits initialised in the $|0\rangle$ state. Thus, the role of the input Hamiltonian will simply be to check whether the auxiliary qubits have been correctly initialised, and is thus given by $H_{in} = \sum_{s=m+1}^{N} \Pi_s^{(1)} \otimes |0\rangle\langle 0|$. Similarly, the output Hamiltonian encodes the case when the computation is accepting, that is, when the measurement in the computational basis of the first qubit yields the output 1, and thus $H_{out} = \Pi_1^{(0)} \otimes |L\rangle\langle L|$.

The Propagation Hamiltonian

The crucial difference is thus in the propagation term H_{prop} of the Hamiltonian. Henceforth, we introduce a superscript $H_t^{(i)}$ where $i \in \{u, p\}$, where H_t^u corresponds to a Hamiltonian implementing unitary evolution, and where H_t^p corresponds to that implemented by a renormalised projector. Thus, we now have that $H_{prop} = \sum_t H_t^{(i)}$ for $i \in \{u, p\}$, depending on whether the evolution implemented corresponds to a unitary operator or a renormalised projector. The propagation Hamiltonian can thus be expressed as:

$$H_{prop} = \sum_{i=0}^{T/2} H_{2i}^{(u)} + \sum_{j=1}^{T/2} H_{2j-1}^{(p)}. \tag{4.23}$$

The above evolution corresponds to conditioning on a particular outcome occurring, that is, postselection. Here, postselection is modelled by the renormalised projector, but crucially relies on the quantum state to dictate the norm of this renormalised projector. Indeed this is one of the major modifications to the k-LOCAL HAMILTONIAN problem when we consider postselection. Here, the operator norm of the individual evolution terms $H_j^{(p)}$ in the Hamiltonian may not be bounded by a polynomial in the input size to the problem. For indeed, if the probability p of a particular event happening is exponentially small then the operator norm will be upper-bounded by an exponential.

Next, we consider the family of IQP circuits, in order to study quantum computation in which evolution occurs through both the application of unitary measurements and renormalised measurements.

4.2.2 IQP circuits

IQP circuit families were previously discussed in chapter 1, where the input to the circuit is a computational basis state which is acted upon by gates diagonal in the X basis, before a final computational basis measurement is performed. Note that to be a uniform IQP circuit, given a classical input $x \in \{0, 1\}^n$, the description of the gates must be generated by a classical computer in time at most polynomial in n. The gates thus form a commuting gate set, and are thus far more restricted quantum circuit family than the general class BQP.

We also saw that any quantum circuit can be expressed as an input of size n in the computational basis, followed by a general unitary operator U and a single-qubit computational basis measurement. The general operator U can be decomposed as a sequence of L =poly(n) single and two-qubit gates $U = U_L \dots U_1$, where each gate U_i is taken from a universal gate set $\mathcal{G}$. For instance, single-qubit Z rotations, the entangling controlled-Z and Hadamard gates form such a universal set. But, given the ability to postselect on measurement outcomes, a Hadamard gate can be implemented with a Hadamard gadget, leaving us with an IQP circuit instance and thus we have that PostIQP = PostBQP.

The question is thus now to investigate the Hamiltonians associated with such postselected circuit families, and in particular the scaling of the promise gap $b-a$. In order to do so, we first focus on a single Hadamard gadget, and study its associated Hamiltonian by using the circuit-to-Hamiltonian construction, which will implement both a unitary operator and a renormalised projectors.

4.2.3 Hamiltonian associated to a Hadamard gadget

In the following, we consider the Hamiltonian operator encoding a quantum circuit implementing a Hadamard gadget. Here, the computation proceeds in three distinct steps. First, a projector $|+\rangle\langle+|$ is applied to the ancillary qubit in the $|+\rangle$ state. Next, the two qubits are entangled with a controlled-Z gate. Finally, the first qubit is measured in the X basis where we postselect on measurement outcome $m = 0$ occurring, which effectively corresponds to the renormalised projector $\sqrt{2}|+\rangle\langle+|$ being applied to the first qubit. Proposition 6 tells us that a Hadamard gadget effectively implements the following operation:

$$\sqrt{2}\big(|+\rangle\langle+| \otimes \mathbb{1}\big)\mathrm{CZ}\big(\mathbb{1} \otimes |+\rangle\langle+|\big) = \mathrm{SWAP}\,\big(H \otimes |+\rangle\langle+|\big), \tag{4.24}$$

which thus allows us to consider the history state of the computation.

The History State

At time step t, the system is assumed to be in the state $|\xi\rangle$, to which a Hadamard gate is applied via the implementation of a Hadamard gadget, which requires an ancillary qubit in the $|+\rangle$ state. In order to track the time evolution of the system, a clock register is appended to the system. The aim is then to construct the history state of the computation, which corresponds to the state $|\eta\rangle = N \sum |\psi_i\rangle$, where N is a normalisation constant which will depend on the depth of the circuit. Initially, at time step t, the system is in the state $|\psi_t\rangle = |\xi, 0\rangle \otimes |+\rangle \otimes |t\rangle$. Next, the projector $\mathbb{1} \otimes |+\rangle\langle+|$ is applied in order to check that the postselection qubits have been correctly initialised in the $|+\rangle$ state, which results in the state $|\psi_{t+1}\rangle = (\mathbb{1} \otimes |+\rangle\langle+|)(|\xi, 0\rangle \otimes |+\rangle) \otimes |t+1\rangle$. At the next time step the two

qubits are then entangled via a controlled-Z gate $|\psi_{t+2}\rangle = \text{CZ}(\mathbb{1} \otimes |+\rangle\langle+|)(|\xi, 0\rangle \otimes |+\rangle) \otimes |t+2\rangle$. Finally a renormalised projector is applied to the first qubit, which corresponds to measurement in the X basis with outcome $|+\rangle$ occurring with probability is 0.5. This results in the state $|\psi_{t+3}\rangle = (\frac{1}{\sqrt{0.5}}|+\rangle\langle+| \otimes \mathbb{1})\text{CZ}(\mathbb{1} \otimes |+\rangle\langle+|)(|\xi, 0\rangle \otimes |+\rangle) \otimes |t+3\rangle$.

Alternatively, the history state $|\eta\rangle$ may be expressed by applying an operator W to the input state $|\xi, +\rangle \otimes |\psi\rangle$, where $|\psi\rangle$ corresponds to a clock state in equal superposition over all time steps, and where W is given by:

$$W = \mathbb{1}_2 \otimes |t\rangle\langle t| + \mathbb{1}_2 \otimes |t+1\rangle\langle t+1| + CZ \otimes |t+2\rangle\langle t+2| + \text{SWAP}(H \otimes \mathbb{1}) \otimes |t+3\rangle\langle t+3|. \quad (4.25)$$

Next, we consider the Hamiltonian which encodes precisely this history state within its groundspace.

The Propagation Hamiltonian

The Hamiltonian operator will consist of the sum of three terms, and be given by $H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$. The input Hamiltonian checks whether the postselection qubit has been correctly initialised in the $|+\rangle$ state and is given by $H_{\text{in}} = (\mathbb{1} \otimes \Pi^-) \otimes |0\rangle\langle 0|$. Next, the propagation Hamiltonian is built, which will consist of terms implementing both unitary evolution and renormalised projectors. First, the projector is applied to the first qubit, where we have $p = 1$ conditioned on a successful initialisation process:

$$H_1^p = \frac{1}{2}(\mathbb{1} \otimes |+\rangle\langle+|) \otimes \big(|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + |t+1\rangle\langle t+1|\big) + (\mathbb{1} \otimes |-\rangle\langle-|) \otimes |t+1\rangle\langle t+1|, \quad (4.26)$$

and we shall thus discard the second term in order to minimise kernel degeneracy:

$$H_1^p = \frac{1}{2}(\mathbb{1} \otimes |+\rangle\langle+|) \otimes \big(|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + |t+1\rangle\langle t+1|\big). \quad (4.27)$$

Next, the controlled-Z operator is applied, and thus the Hamiltonian term encoding unitary evolution is given by:

$$H_2^u = \frac{1}{2}(\mathbb{1} \otimes |t+1\rangle\langle t+1| - CZ \otimes |t+1\rangle\langle t+2| - CZ \otimes |t+2\rangle\langle t+1| + \mathbb{1} \otimes |t+2\rangle\langle t+2|). \quad (4.28)$$

Finally, the projective measurement is performed, where we have $p = \frac{1}{2}$ and thus the Hamiltonian encoding the evolution via renormalised projector is given by:

$$H_3^p = \frac{1}{\sqrt{2}}(|+\rangle\langle+| \otimes \mathbb{1}) \otimes \big(\sqrt{2}|t+2\rangle\langle t+2| - |t+2\rangle\langle t+3| - |t+3\rangle\langle t+2| + \frac{1}{\sqrt{2}}|t+3\rangle\langle t+3|\big) + (|-\rangle\langle-| \otimes \mathbb{1}) \otimes |t+3\rangle\langle t+3|. \quad (4.29)$$

Finally, the output Hamiltonian encodes a circuit whose output is an accepting computation and is thus given by $H_{out} = \Pi_2^{(0)} \otimes |t+3\rangle\langle t+3|$.

A Transformed Hamiltonian

Next, we seek to analyse the spectrum of the propagation Hamiltonian H_{prop}. Indeed, our capacity to resolve for the smallest non zero eigenvalue of the propagation Hamiltonian can in turn be used in order to determine whether a given quantum circuit is accepting or rejecting. As we saw in chapter 1, the Hamiltonian is an a priori complex object, whose spectrum can be hard to compute. In Kiatev's model, transforming the Hamiltonian from H_{prop} to $WH_{prop}W^\dagger$ significantly simplifies the operator and its spectrum can thus be analytically calculated. In that case W is a unitary operator, the spectrum is invariant under this transformation, and thus we have that the smallest non-zero eigenvalue of H_{prop} is conserved, i.e. $\lambda_{min}(H_{prop}) = \lambda_{min}(WH_{prop}W^\dagger)$.

Here, in contrast, the evolution occurs through both unitary operators and renormalised projections, and thus applying the transformation under W will not be enough to simplify the Hamiltonian construction and thus derive an analytic lower bound for the eigenvalues. This is primarily due to the presence of the projectors in the expression. Instead, in order to recover a similarly simple expression, we need to consider the Hamiltonian $\Pi WHW^\dagger\Pi$. Crucially, the operator ΠW is no longer a unitary operator, and thus the spectrum will not be preserved under this transformation: we no longer know how the smallest non-zero eigenvalue $\Pi WHW^\dagger\Pi$ relates to that of $WHW^\dagger$, or equivalently, H.

Here, we have that $\Pi = \mathbb{1} \otimes |+\rangle\langle+|$, and we thus transform each term of the propagation Hamiltonian as follows. The first projection which checks correct initialisation is invariant under this transformation:

$$\Pi W^\dagger H_1^p W \Pi = H_1^p. \tag{4.30}$$

Next, we can see that $W^\dagger H_2^u W = \frac{1}{2}\mathbb{1}_2 \otimes (|t+1\rangle\langle t+1| - |t+1\rangle\langle t+2| - |t+2\rangle\langle t+1| + |t+2\rangle\langle t+2|)$, and thus:

$$\Pi W^\dagger H_2^u W \Pi = \frac{1}{2}(\mathbb{1} \otimes |+\rangle\langle+|) \otimes (|t+1\rangle\langle t+1| - |t+1\rangle\langle t+2| - |t+2\rangle\langle t+1| + |t+2\rangle\langle t+2|). \tag{4.31}$$

Finally, by applying this transformation to the measurement term, the following simple expression is obained:

$$\Pi W^\dagger H_3^p W \Pi = \frac{1}{2}(\mathbb{1} \otimes |+\rangle\langle+|) \otimes (|t+2\rangle\langle t+2| - |t+2\rangle\langle t+3| - |t+3\rangle\langle t+2| + |t+3\rangle\langle t+3|).$$

Thus, by adding these terms together, we now have that:

$$(\mathbb{1} \otimes |+\rangle\langle+|) W H_{\text{prop}} W^\dagger (\mathbb{1} \otimes |+\rangle\langle+|) = \frac{1}{2}(\mathbb{1} \otimes |+\rangle\langle+|) E, \tag{4.32}$$

where E is a tridiagonal matrix whose smallest non-null eigenvalue is greater or equal than $\frac{c'}{L^2}$, that is, greater than $1/\text{poly}(n)$, where we have thus recovered polynomial scaling. But, this does not tell us anything about the spectrum of the original propagation Hamiltonian H_{prop}.

Spectral Discussion

Thus, the spectrum of a Hamiltonian operator encoding both unitary and non-unitary evolution is hard to compute. A computation which occurs in rounds or layers of both unitary gates and measurements will have an associated Hamiltonian also composed of terms encoding either unitary evolutions or renormalised projectors. Previously, even by exclusively concentrating our attention on the implementation of a Hadamard gadget in such a circuit, we did not find an expression for a lower bound on the smallest non zero energy eigenvalue for the original Hamiltonian.

We nevertheless realised that if instead we consider the spectrum of the operator $\Pi W H W^\dagger \Pi$, then an analytic expression could be recovered. But, its relationship to the spectrum of the original propagation Hamiltonian is unknown, as the kernels of $\Pi W H W^\dagger \Pi$ and H do not, a priori, have any property we might exploit, such as for instance being simultaneously diagonalisable.

Let the spectral decomposition of $W H W^\dagger$ be given by $W H W^\dagger = \sum_i \lambda_i |v_i\rangle\langle v_i|$ and of $\Pi W H W^\dagger \Pi$ be given by $\Pi W H W^\dagger \Pi = \sum_j \mu_j |w_j\rangle\langle w_j|$, where the eigenvalues are ordered in decreasing size. Thus, our problem is to determine a lower bound for the smallest non-zero eigenvalue of H, which is say, λ_m. The application of the projector Π to the operator may have caused the dimension of its kernel to increase. Thus, its smallest non-zero eigenvalue might now be μ_k. We have that $\mu_k = \langle w_k | \Pi W H W^\dagger \Pi | w_k \rangle$, and thus $\langle w_k | \tilde{H} | w_k \rangle = \sum_i \lambda_i |\langle w_k | v_i \rangle|^2$, and we wish to know whether this is less than the smallest non zero eigenvalue λ_m of the original Hamiltonian or not. If we express the eigenvectors $|w_k\rangle = \sum_s \alpha_s |v_s\rangle$ in the eigenbasis $|v_i\rangle$, then we have that: $\mu_k = \sum_i \lambda_i |\alpha_i|^2$. This approach did not yield any insight into the behaviour of the smallest non zero eigenvalue, and we thus, in the next section, consider two qualitatively different circuits, both making use of the Hadamard gadget and numerically study the scaling of the Hamiltonian's smallest non-zero eigenvalue.

4.3 Numerical Simulation

The scaling of the smallest non zero eigenvalue is, as we have seen, a critical quantity in the study of Hamiltonian complexity. In the following, we chose to consider simple models of quantum circuits implementing the Hadamard gadget, and numerically simulate the behaviour of their associated

Hamiltonian. By doing so, we are able to obtain numerical results for the smallest non-zero eigenvalue, and thus study its scaling with the system size. More precisely, we will consider two classes of post-selected circuit based on the Hadamard gadget, and numerically analyse the corresponding gaps $b - a$ between the ground state energy and the energy of the first excited state. The Hadamard gadget satisfies the notion of tame post-selection so is an ideal candidate for which we can build circuits. It should be noted that in both families of circuit the total probability of success of the post-selected event decreases exponentially in the size of the circuit. However, in terms of the gap $b - a$, this appears to decrease exponentially in the size of the post-selected circuit, whereas in the other family it seems to decrease polynomially in the size of the circuit. Thus, the intuition that the probability of success dictates the gap $b - a$ of the corresponding Hamiltonian is not immediately obvious. To emphasize this point, in both families of circuits the corresponding Hamiltonians all have terms that have operator norms that are bounded by some polynomial in the circuit size.

4.3.1 Cascaded Gadgets: the Exponential Case

The Model

We consider an arbitrary quantum state $|\psi\rangle$ and n postselection qubits initialised in the $|+\rangle$ state. Neighbouring qubits are entangled with a controlled-Z gate and are then measured one after the other in the X basis, as shown in Fig. 4.3, with outcome $m = 0$ postselected upon. Effectively, this results in the state of the first qubit being teleported onto the second and acted upon by a Hadamard gate. This is then the input to a new Hadamard gadget, which will now implement an additional Hadamard gate. Thus, the effect of this circuit is to sequentially teleport the state $|\psi\rangle$ from qubit to qubit, each time applying either a Hadamard gate or the identity to it, as $H^2 = \mathbb{I}$.

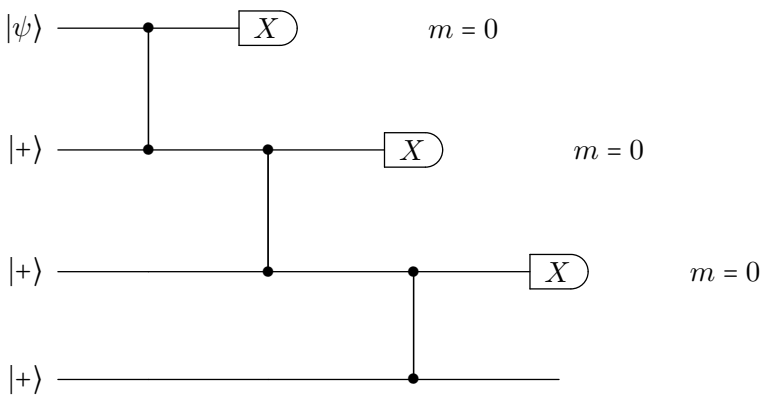


Figure 4.3: *Hadamard gadgets using multiple ancillas.* Three Hadamard gadgets are implemented using three ancillary qubits.

The computation is then broken down into successive discrete time steps, where at each round either a controlled-Z or a measurement is applied, as shown in Fig. 4.4. Thus, the input oscillates between the states $|\psi\rangle$ and $H|\psi\rangle$ at each time step.

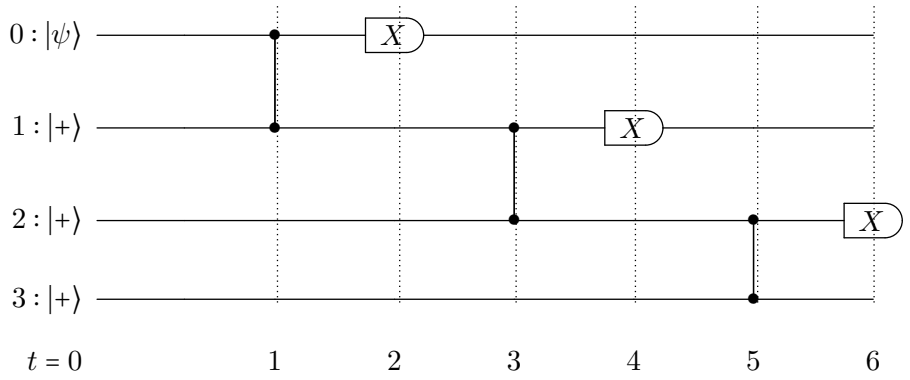


Figure 4.4: *Time steps in cascaded case, with time steps.* At each time step either a controlled-Z operator or a measurement in the X basis is applied, with measurement outcome $m = 0$ postselected upon.

The Hamiltonian

If n Hadamard gates are applied, then we need to implement n Hadamard gadgets, which requires n ancillary post-selection qubits and n measurements. The space of the qubits will be 2^{n+1}, and the clock will be a qudit of dimension $2n + 1$. The propagation Hamiltonian will be made of $2n$ terms, where odd terms correspond to Kitaev's unitary Hamiltonians and even terms to a projection Hamiltonian. Explicitly, the propagation Hamiltonian can be expressed as:

$$\begin{aligned} H_{prop} = \sum_{j=0}^{n-1} \frac{1}{2}\Big[&- CZ^{(j+1,j+2)} \otimes \big(|2j\rangle\langle 2j+1| + |2j+1\rangle\langle 2j|\big) + \mathbb{I} \otimes \big(|2j\rangle\langle 2j| + |2j+1\rangle\langle 2j+1|\big)\Big] \\ &+ \frac{1}{3}\Pi^{(j+1)} \otimes \Big[2|2j+1\rangle\langle 2j+1| - \frac{1}{\sqrt{2}}|2j+1\rangle\langle 2j+2| - \frac{1}{\sqrt{2}}|2j+2\rangle\langle 2j+1| + |2j+2\rangle\langle 2j+2|\Big] \\ &+ (\mathbb{I} - \Pi)^{(j+1)} \otimes |2j+2\rangle\langle 2j+2|, \end{aligned} \tag{4.33}$$

where $CZ^{(i,j)}$ denotes the control-Z operator acting on qubits i and j with identity on all others, and where $\Pi^{(i)}$ corresponds to the projector $|+\rangle\langle +|$ acting on qubit i, with identity on all other qubits.

Numerical Results

Having constructed the propagation Hamiltonian of the circuit, we compute its smallest non zero eigenvalue, which is plotted in Fig. 4.5. With each round, the Hamiltonian matrix size increases

exponentially, thus limiting the number of data points we were able to obtain. An exponential function $y = A\exp(bx) + c$ can be fitted to the data yielding $A = 8.802$, $b = 0.727$ and $c = -28.767$.

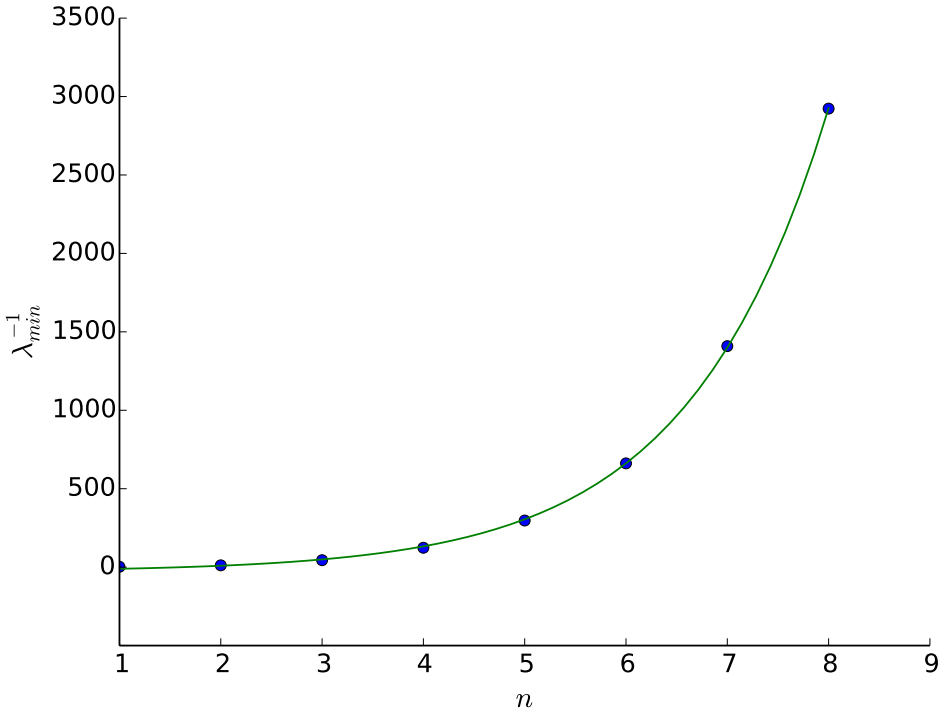


Figure 4.5: *Exponential scaling.* Here, we fit the data to an exponential function $y = Ae^{bc} + c$, yielding $A = 8.802$, $b = 0.727$ and $c = -28.767$.

Therefore, the intuition that as the probability of success decreases exponentially, the gap closes as

an inverse exponential seems to be correct.

Numerical Analysis

In order to ascertain whether the data behaves in an exponential or in a polynomial way, we can perform the following analysis. In the case of an exponential function such as $f(x) = \exp(ax)$, we have that the first derivative is given by $\frac{df(x)}{dx} = af(x)$, whereas for a polynomial function of the form $f(x) = a_n x^n + \ldots a_1 x_1 + a_0$, the first derivative is given by $\frac{df(x)}{dx} = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$. Thus, for an exponential function the quantity $\frac{\frac{df(x)}{dx}}{f(x)} = a$ is a constant, whereas for a polynomial function, we have that the ration asymptotically goes to $\frac{n}{x}$. Here, we make the following approximation: $\frac{df(x)}{dx} \approx \frac{\Delta f(x)}{\Delta x} = f(n+1) - f(n)$ where $n \in \mathbb{N}^*$ and $f(x) \approx \frac{f(n)+f(n+1)}{2}$. The resulting data is shown in figure 4.6, where the constant curve $y = 0.727$ as well as various hyperbolas corresponding to polynomial fits have been plotted

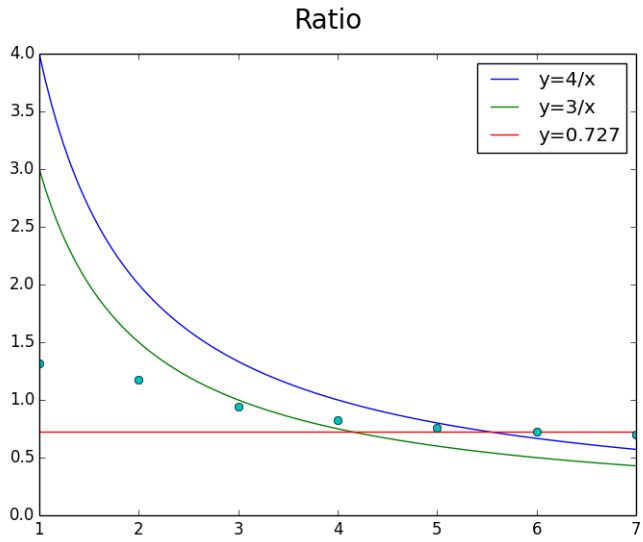


Figure 4.6: *Numerical comparison.* Numerical analysis of various candidate curves for the collected data.

Discussion

The numerical results indicate that the reciprocal of the smallest non zero eigenvalue scales as an inverse exponential. This corresponds to what would be expected from performing arbitrary post-selection on a polynomial number of qubits. In the next section, we once again consider the case where Hadamard gadgets are sequentially applied, but this time where the postselection qubit is recycled in each round.

4.3.2 Sequential Gadgets: the Polynomial Case

The Model

We consider an arbitrary quantum state $|\psi\rangle$ and a single postselection qubit initialised in the $|+\rangle$. One round of the circuit corresponds to the application of the controlled-Z gate, a measurement of the first qubit in the X basis with postselection on outcome $m = 0$, followed by another controlled-Z gate and a final measurement on the second qubit in the X basis with postselection on outcome $m = 0$. With postselection, this circuit effectively implements the identity, as the output is given by $|\psi\rangle \otimes |+\rangle$. Multiple rounds of this circuit are then repeated, and we obtain Fig. 4.7, where one box corresponds to two postselections.

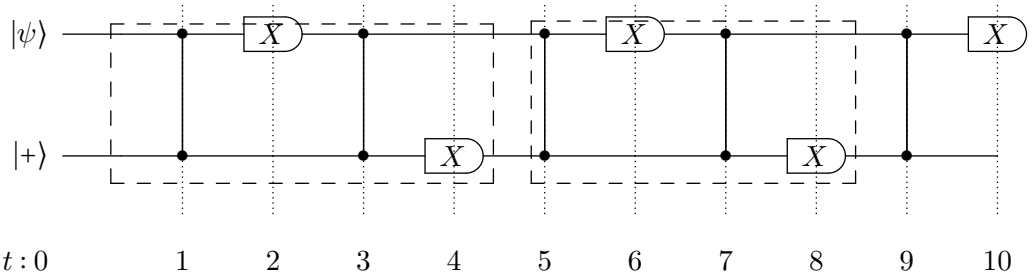


Figure 4.7: *Hadamard gates using a single ancilla.* Each box is a post-selected circuit implementing the identity on the input qubit $|\psi\rangle$ and recycling qubits since the ancillas will always be in the state $|+\rangle$.

The Hamiltonian

The propagation Hamiltonian corresponding to this circuit is now computed as a function of the number of rounds n of each gadget de, as shown in Fig. 4.7. One box corresponds to a unitary operator being applied, a renormalised projector, a unitary operator and a final renormalised projector, thus $H_{prop} = \sum_j H_j$, where:

$$\begin{aligned} H_j =& \frac{1}{2}(-CZ \otimes (|j\rangle\langle j+1| + |j+1\rangle\langle j|) + \mathbb{I} \otimes (|j\rangle\langle j| + |j+1\rangle\langle j+1|) \\ &+ \frac{1}{3}(|+\rangle\langle +| \otimes \mathbb{I}) \otimes \Big[2|j+1\rangle\langle j+1| - \frac{1}{\sqrt{2}}|j+1\rangle\langle j+2| \\ &- \frac{1}{\sqrt{2}}|j+2\rangle\langle j+1| + |j+2\rangle\langle j+2|\Big] + (|-\rangle\langle -| \otimes \mathbb{I}) \otimes |j+2\rangle\langle j+2|, \\ &+ \frac{1}{2}(-CZ \otimes (|j+2\rangle\langle j+3| + |j+3\rangle\langle j+2|) + \mathbb{I} \otimes (|j+2\rangle\langle j+2| + |j+3\rangle\langle j+3|) \\ &+ \frac{1}{3}(\mathbb{I} \otimes |+\rangle\langle +|) \otimes \Big[2|j+3\rangle\langle j+3| - \frac{1}{\sqrt{2}}|j+3\rangle\langle j+4| \\ &- \frac{1}{\sqrt{2}}|j+4\rangle\langle j+3| + |j+4\rangle\langle j+4|\Big] + (\mathbb{I} \otimes |-\rangle\langle -|) \otimes |j+4\rangle\langle j+4|. \end{aligned} \tag{4.34}$$

The dimension of the auxiliary clock depends on the number of rounds to be implemented and is given by $4n + 1$. Thus, this quantum circuit implements the same operations previously, yet as we shall see, present starkly different behaviour.

Numerical Results

A numerical simulation of this circuit allows for the smallest non-zero eigenvalue of the Hamiltonian to be computed. The reciprocal of the scaling of the smallest non zero eigenvalue with system size n is then represented in Fig. 4.8. A quadratic function $y = ax^2 + bx + c$ can be fitted to the data, yielding the coefficients: $a = 6.5$, $b = 0.04$ and $c = 1.4$. The smallest non-zero eigenvalue of the propagation Hamiltonian thus scales as an inverse polynomial.

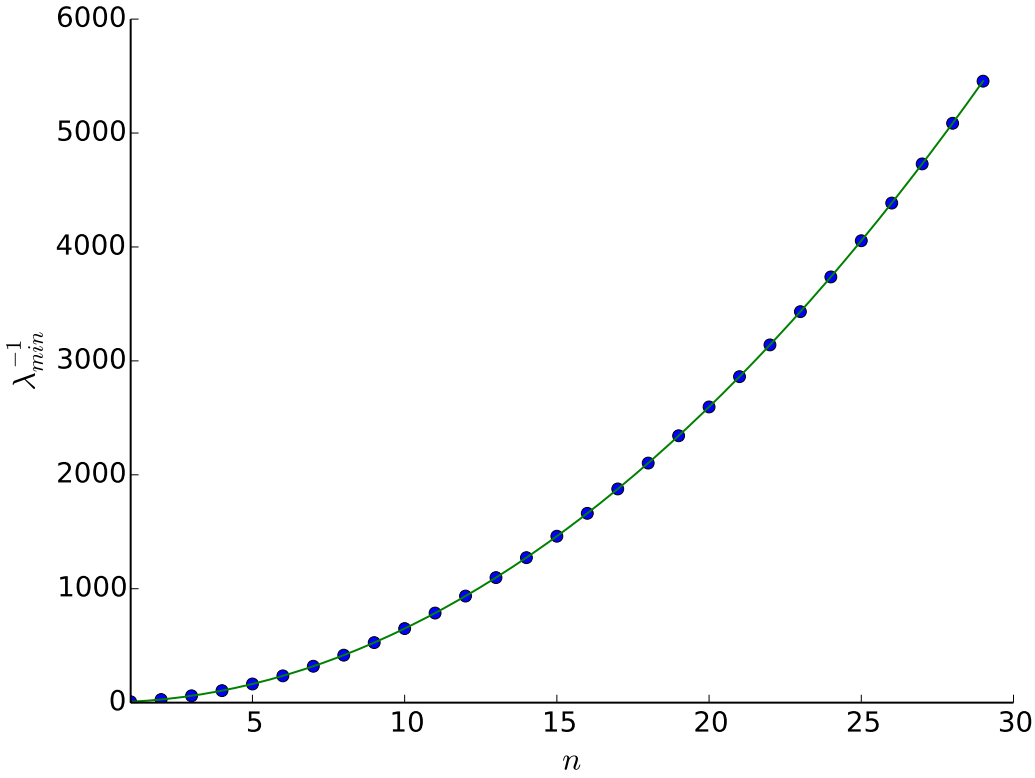


Figure 4.8: *Polynomial scaling.* Scaling of the reciprocal of the smallest eigenvalue of the Hamiltonian corresponding to the circuit family $\mathcal{F}_2$, as shown in equation 4.34. Here, the data is fitted to a quadratic function $y = ax^2 + bx + c$, and we obtain $a = 6.5$, $b = 0.04$ and $c = 1.4$.

Discussion

Our numerical results indicate that the smallest non zero eigenvalue scales as an inverse polynomial with the number of rounds n. This is in stark contrast with the previous circuit family we considered, where the reciprocal of the smallest non zero eigenvalue scaled as an exponential. Although both circuits seem nearly identical, we have established that the spectrum of their respective propagation Hamiltonians is fundamentally different. Intuitively, this could mean that the complexity of the ground space and the encoded computation are of a qualitatively different nature.

4.4 Conclusion

The growing field of Hamiltonian complexity connects the fields of physics to computer science via the Hamiltonian operator. It offers us insight into the connections between the complexity of physical ground states and the complexity of computation. In addition, postselection has proven to be both a powerful resource to exploit and a useful tool to apply. On the other hand, as we have discussed, experiments commonly repeat procedures until a successful outcome is achieved, and can thus be thought of as performing postselection on outcomes. Here, we investigated the role of

postselection and measurement in connection with the class of quantum verification problems, QMA as well as with Hamiltonian operators.

4.4.1 Results

We introduced a new class of Hamiltonians encoding non-unitary computation and postselection, and investigated the scaling of its smallest non-zero eigenvalue with system size. This was achieved by extending the circuit-to-Hamiltonian construction to evolutions via renormalised projectors, which map pure states to pure states. In order for these Hamiltonians to not depend on the input state, we introduce the idea of a restricted form of postselection, which we call tame postselection, where the probability of an event occurring is input independent.

We considered two a priori simple quantum circuits, both using postselection as renormalised projectors, and by performing a numerical simulation, analysed the scaling of their smallest non-zero eigenvalue. We found that two radically different behaviours emerged: in one case the gap scaled exponentially with the system size, whereas in the other, it scaled as a polynomial function. Thus, on one hand, we can see that encoding postselected circuits can lead an exponential scaling. Yet, the more efficient case displayed a polynomial scaling. This raises the possibility of studying more tame forms of postselection within the k-LOCAL HAMILTONIAN problem.

4.4.2 postQMA

More generally, we can consider the role of postselection in the class of quantum verification problems, QMA. Here, similarly to postBQP, we introduce a postselection register, conditioned upon which we will or not consider the output of the computation. In the same way that postselection boosts the power of postBQP, one would imagine it to increase the power of QMA. Formally, we introduce the complexity class postQMA as the following:

Definition 6. *A promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ is in* PostQMA *if for an input $x \in \{0,1\}^n$, there exists a uniform quantum circuit family $\{V_x\}$ with each V_x taking $|\psi\rangle|00...0\rangle$ as input and $|\psi\rangle$ consisting of a number of qubits w at most polynomial in n, and with post-selection and output qubits, which are all measured in the computational basis and giving outcomes as bit-strings $q_{post} \in \{0,1\}^w$ and $q_{out} \in \{0,1\}$ such that:*

$$\begin{aligned} \text{if } x \in \mathcal{L}_{yes}, \quad & \exists |\psi\rangle \; P[q_{out} = 1 | q_{post} = \mathbf{0}] \geq 2/3, \\ \text{if } x \in \mathcal{L}_{no}, \quad & \forall |\psi\rangle \; P[q_{out} = 1 | q_{post} = \mathbf{0}] \leq 1/3, \end{aligned}$$

where $P[q_{post} = \mathbf{0}] \geq 2^{-poly(n)}$ and is the same for all $|\psi\rangle$, and $poly$ is some polynomial function.

As QMA contains BQP we have that postQMA contains postBQP. thus PostBQP $\subseteq$ PostQMA.

4.4.3 Future Directions

First, further research is required in order to understand the scaling of the gap in connection with postselection. As the structure of the propagation Hamiltonian is different, it will encode ground states of different complexity to those seen in the case of unitary evolution. Next, we motivated our interest in layered quantum circuits by introducing IQP circuits. Here, the gate set is commuting, and this raises the question as to the importance of operations order within the Hamiltonian. Indeed, in the Hamiltonian construction, the role of the clock is to implement a sequential ordering for the application of quantum gates. In the case when these are all commuting, they can be implemented in a single time step, which would raise questions regarding the time structure.

The main direction for future research is to get a better characterisation of Hamiltonians resulting from post-selected quantum circuits. We numerically explored a couple of examples of post-selected circuit families that exhibited similar behaviour from the point-of-view of state transformation and the probability of success of all post-selected events exponentially decreased in the size of the circuits, however their corresponding Hamiltonians exhibited very different behaviour. It seems that one of the Hamiltonians can be solved within QMA since there was a polynomially small gap between the ground state and first excited state energies, the other family of Hamiltonians seemed to have an exponentially small gap. Therefore, this gap might not be determined by the probability of success for the post-selected events nor the effective unitary implemented by the tame post-selection. The natural question is then what determines this gap?

Finally, this work could be useful in demonstrating that the simulation of certain Hamiltonians is hard. Since post-selection is a useful tool in proving such hardness results, it seems natural to build post-selection into the Hamiltonians and then make arguments based on the k-LOCAL HAMILTONIAN problem. By bringing all of these elements together we may get a better understanding of what kinds of quantum systems are hard to classically simulate and why.

Bibliography

[1] José Ferreirós. The crisis in the foundations of mathematics. *The Princeton Companion to Mathematics*, 2008.

[2] Ernst Snapper. The three crises in mathematics: Logicism, intuitionism and formalism. *Mathematics Magazine*, pages 207–216, 1979.

[3] Rudolf Carnap. The logicist foundations of mathematics. *Bertrand Russell: History of philosophy, ethics, education, religion and politics*, 4:135, 1999.

[4] Arend Heyting. *The intuitionist foundations of mathematics*. na, 1983.

[5] Johann Von Neumann. The formalist foundations of mathematics. 1964.

[6] David Hilbert and Wilhelm Ackermann. *Grundzüge der theoretischen Logik*, volume 27. Springer-Verlag, 2013.

[7] Alonzo Church. A note on the entscheidungsproblem. *The journal of symbolic logic*, 1(01):40–41, 1936.

[8] Alan Mathison Turing. On computable numbers, with an application to the entscheidungsproblem. *J. of Math*, 58(345-363):5, 1936.

[9] Albert Einstein. Über einem die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. *Annalen der Physik*, 4, 1905.

[10] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[11] Erwin Schrödinger. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge Univ Press, 1935.

[12] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6/7):467–488, 1982.

[13] R.P. Feynman. Quantum mechanical computers. *Optics News*, **11**:11–20, (1985).

[14] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 400, pages 97–117. The Royal Society, 1985.

[15] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.

[16] David P DiVincenzo et al. The physical implementation of quantum computation. *arXiv preprint quant-ph/0002077*, 2000.

[17] J Kelly, R Barends, AG Fowler, A Megrant, E Jeffrey, TC White, D Sank, JY Mutus, B Campbell, Yu Chen, et al. State preservation by repetitive error detection in a superconducting quantum circuit. *Nature*, 519(7541):66–69, 2015.

[18] R Barends, J Kelly, A Megrant, A Veitia, D Sank, E Jeffrey, TC White, J Mutus, AG Fowler, B Campbell, et al. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature*, 508(7497):500–503, 2014.

[19] AD Córcoles, Easwar Magesan, Srikanth J Srinivasan, Andrew W Cross, M Steffen, Jay M Gambetta, and Jerry M Chow. Demonstration of a quantum error detection code using a square lattice of four superconducting qubits. *Nature communications*, 6, 2015.

[20] Andrew Steane. Multiple-particle interference and quantum error correction. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 452, pages 2551–2577. The Royal Society, 1996.

[21] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[22] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 176–188. ACM, 1997.

[23] Rolf Landauer. The physical nature of information. *Physics letters A*, 217(4):188–193, 1996.

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

[25] David Perez-Garcia, Frank Verstraete, Michael M Wolf, and J Ignacio Cirac. Matrix product state representations. *arXiv preprint quant-ph/0608197*, 2006.

[26] Frank Verstraete and J Ignacio Cirac. Matrix product states represent ground states faithfully. *Physical Review B*, 73(9):094423, 2006.

[27] Frank Verstraete and J Ignacio Cirac. Valence-bond states for quantum computation. *Physical Review A*, 70(6):060302, 2004.

[28] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Physical Review Letters*, 91(14):147902, 2003.

[29] Martin B Plenio and Shashank Virmani. An introduction to entanglement measures. *arXiv preprint quant-ph/0504163*, 2005.

[30] Fernando GSL Brandão and Michał Horodecki. An area law for entanglement from exponential decay of correlations. *Nature Physics*, 9(11):721–726, 2013.

[31] Matthew B Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007.

[32] S Bravyi, MB Hastings, and F Verstraete. Lieb-robinson bounds and the generation of correlations and topological quantum order. *Physical review letters*, 97(5):050401, 2006.

[33] Bruno Nachtergaele and Robert Sims. Much ado about something: why lieb-robinson bounds are useful. *arXiv preprint arXiv:1102.0835*, 2011.

[34] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413, 1996.

[35] Rajiah Simon. Peres-horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726, 2000.

[36] Karl Kraus, Arno Böhm, John D Dollard, and WH Wootters. States, effects, and operations fundamental notions of quantum theory. 1983.

[37] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[38] W Forrest Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[39] John S Bell et al. On the einstein-podolsky-rosen paradox. *Physics*, 1(3):195–200, 1964.

[40] N David Mermin. Hidden variables and the two theorems of john bell. *Reviews of Modern Physics*, 65(3):803, 1993.

[41] Richard Jozsa. Entanglement and quantum computation. *arXiv preprint quant-ph/9707034*, 1997.

[42] Richard Jozsa and Noah Linden. On the role of entanglement in quantum-computational speed-up. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 459, pages 2011–2032. The Royal Society, 2003.

[43] David Deutsch. Quantum computational networks. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 425, pages 73–90. The Royal Society, 1989.

[44] A Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361. IEEE, 1993.

[45] A.H. Shen A. Yu. Kitaev and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, (2002).

[46] Michael A Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57(1):147–161, 2006.

[47] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[48] HJ Briegel, DE Browne, W Dür, R Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

[49] Robert Raussendorf, Daniel E Browne, and Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical review A*, 68(2):022312, 2003.

[50] Richard Jozsa. An introduction to measurement based quantum computation. *NATO Science Series, III: Computer and systems sciences*, 199:137–158, 2006.

[51] Earl T Campbell and Joseph Fitzsimons. An introduction to one-way quantum computing in distributed architectures. *International Journal of Quantum Information*, 8(01n02):219–258, 2010.

[52] Peter W Shor and Stephen P Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Information & Computation*, 8(8):681–714, 2008.

[53] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20100301. The Royal Society, 2010.

[54] Dan Shepherd and Michael J Bremner. Temporally unstructured quantum computation. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 465, pages 1413–1439. The Royal Society, 2009.

[55] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[56] Umesh Vazirani. Quantum computation. University Lecture, 2004.

[57] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457, 1995.

[58] David P DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015, 1995.

[59] David Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 449, pages 669–677. The Royal Society, 1995.

[60] Seth Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346, 1995.

[61] P Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 486–494. IEEE, 1999.

[62] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[63] Christopher M Dawson and Michael A Nielsen. The solovay-kitaev algorithm. *arXiv preprint quant-ph/0505030*, 2005.

[64] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 454, pages 339–354. The Royal Society, 1998.

[65] Andrew M Childs and Wim Van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):1, 2010.

[66] Miklos Santha. Quantum walk based search algorithms. In *International Conference on Theory and Applications of Models of Computation*, pages 31–46. Springer, 2008.

[67] Dave Bacon and Wim VAn DAm. Recent progress in quantum algorithms. *Communications of the ACM*, 53(2):84–93, 2010.

[68] Ashley Montanaro. Quantum algorithms: an overview. *arXiv preprint arXiv:1511.04206*, 2015.

[69] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 439, pages 553–558. The Royal Society, 1992.

[70] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[71] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[72] DGBJ Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[73] Daniel Gottesman and Isaac L Chuang. Quantum teleportation is a universal computational primitive. *arXiv preprint quant-ph/9908010*, 1999.

[74] Janet Anders and Dan E Browne. Computational power of correlations. *Physical Review Letters*, 102(5):050502, 2009.

[75] Maarten Van den Nest, Akimasa Miyake, Wolfgang Dür, and Hans J Briegel. Universal resources for measurement-based quantum computation. *Physical review letters*, 97(15):150504, 2006.

[76] Matty J Hoban and Dan E Browne. Stronger quantum correlations with loophole-free postselection. *Physical review letters*, 107(12):120402, 2011.

[77] Daivd Gross, Jens Eisert, Norbert Schuch, and David Perez-Garcia. Measurement-based quantum computation beyond the one-way model. *Physical Review A*, 76(5):052315, 2007.

[78] D Gross and J Eisert. Novel schemes for measurement-based quantum computation. *Physical review letters*, 98(22):220503, 2007.

[79] D Gross and J Eisert. Quantum computational webs. *Physical Review A*, 82(4):040303, 2010.

[80] Robert Raussendorf. Contextuality in measurement-based quantum computation. *Physical Review A*, 88(2):022322, 2013.

[81] Dan Browne, Elham Kashefi, and Simon Perdrix. Computational depth complexity of measurement-based quantum computation. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 35–46. Springer, 2011.

[82] Hans J Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86(5):910, 2001.

[83] Christos H Papadimitriou. *Computational complexity*. John Wiley and Sons Ltd., 2003.

[84] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[85] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of mathematics*, pages 781–793, 2004.

[86] Raymond Greenlaw, H James Hoover, and Walter L Ruzzo. *A compendium of problems complete for P*. Department of Computer Science, University of New Hampshire, 1991.

[87] Stephen A Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158. ACM, 1971.

[88] Leonid A Levin. Universal sequential search problems. *Problemy Peredachi Informatsii*, 9(3):115–116, 1973.

[89] Lance Fortnow. Counting complexity. *Complexity theory retrospective II*, pages 81–107, 1997.

[90] Leslie G Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[91] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[92] László Babai and Shlomo Moran. Arthur-merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20. ACM, 1993.

[94] Scott Aaronson. Bqp and the polynomial hierarchy. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150. ACM, 2010.

[95] Leonard M Adleman, Jonathan DeMarrais, and Ming-Deh A Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[96] Dorit Aharonov and Tomer Naveh. Quantum np-a survey. *arXiv preprint quant-ph/0210077*, 2002.

[97] Mikhail Vyalyi. Qma= pp implies that pp contains ph. In *ECCCTR: Electronic Colloquium on Computational Complexity, technical reports*, 2003.

[98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM (JACM)*, 45(3):501–555, 1998.

[99] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of np. *Journal of the ACM (JACM)*, 45(1):70–122, 1998.

[100] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum pcp conjecture. *ACM SIGACT News*, 44(2):47–79, 2013.

[101] Matthew B Hastings. Trivial low energy states for commuting hamiltonians, and the quantum pcp conjecture. *arXiv preprint arXiv:1201.3387*, 2012.

[102] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-sat. *Contemporary Mathematics*, 536:33–48, 2011.

[103] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[104] Julia Kempe and Oded Regev. 3-local hamiltonian is qma-complete. *arXiv preprint quant-ph/0302079*, 2003.

[105] Sergey Bravyi, David P Divincenzo, Roberto I Oliveira, and Barbara M Terhal. The complexity of stoquastic local hamiltonian problems. *arXiv preprint quant-ph/0606140*, 2006.

[106] Sergey Bravyi and Mikhail Vyalyi. Commutative version of the k-local hamiltonian problem and common eigenspace problem. *arXiv preprint quant-ph/0308021*, 2003.

[107] Toby Cubitt and Ashley Montanaro. Complexity classification of local hamiltonian problems. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 120–129. IEEE, 2014.

[108] Nikolas P Breuckmann and Barbara M Terhal. Space-time circuit-to-hamiltonian construction and its applications. *Journal of Physics A: Mathematical and Theoretical*, 47(19):195304, 2014.

[109] Sergey Bravyi, Arvid J Bessen, and Barbara M Terhal. Merlin-arthur games and stoquastic complexity. *arXiv preprint quant-ph/0611021*, 2006.

[110] Sevag Gharibian, Yichen Huang, Zeph Landau, Seung Woo Shin, et al. Quantum hamiltonian complexity. *Foundations and Trends® in Theoretical Computer Science*, 10(3):159–282, 2015.

[111] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005.

[112] Yenjo Han, Lane A Hemaspaandra, and Thomas Thierauf. Threshold computation and cryptographic security. *SIAM Journal on Computing*, 26(1):59–78, 1997.

[113] Leslie 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*, pages 114–123. ACM, 2001.

[114] Richard Jozsa. Classical simulation and complexity of quantum computations. In *Computer Science–Theory and Applications*, pages 252–258. Springer, 2010.

[115] Maarten Van den Nest. Simulating quantum computers with probabilistic methods. *Quantum Information & Computation*, 11(9-10):784–812, 2011.

[116] Richard Jozsa and Akimasa Miyake. Matchgates and classical simulation of quantum circuits. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 464, pages 3089–3106. The Royal Society, 2008.

[117] Richard Jozsa and Marrten Van den Nest. Classical simulation complexity of extended clifford circuits. *Quantum Information & Computation*, 14(7&8):633–648, 2014.

[118] Martin Schwarz and Maarten Van den Nest. Simulating quantum circuits with sparse output distributions. *arXiv preprint arXiv:1310.6749*, 2013.

[119] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2011.

[120] Maarten Van den Nest, Wolfgang Dür, Guifré Vidal, and HJ Briegel. Classical simulation versus universality in measurement-based quantum computation. *Physical Review A*, 75(1):012337, 2007.

[121] Richard Jozsa. On the simulation of quantum circuits. *arXiv preprint quant-ph/0603163*, 2006.

[122] Igor L Markov and Yaoyun Shi. Simulating quantum computation by contracting tensor networks. *SIAM Journal on Computing*, 38(3):963–981, 2008.

[123] Joel Wallman, Chris Granade, Robin Harper, and Steven T Flammia. Estimating the coherence of noise. *New Journal of Physics*, 17(11):113020, 2015.

[124] Michael Zwolak and Guifré Vidal. Mixed-state dynamics in one-dimensional quantum lattice systems: a time-dependent superoperator renormalization algorithm. *Physical review letters*, 93(20):207205, 2004.

[125] Frank Verstraete, Juan J Garcia-Ripoll, and Juan Ignacio Cirac. Matrix product density operators: simulation of finite-temperature and dissipative systems. *Physical review letters*, 93(20):207204, 2004.

[126] Bogdan Pirvu, Valentin Murg, J Ignacio Cirac, and Frank Verstraete. Matrix product operator representations. *New Journal of Physics*, 12(2):025012, 2010.

[127] Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *arXiv preprint quant-ph/0205133*, 2002.