Randomness for quantum information processing

Rawad Mezher

THESE DE DOCTORAT DE
SORBONNE UNIVERSITÉ FACULTÉ DES SCIENCES

Spécialité

Informatique

École doctorale Informatique, Télécommunications et Electronique (Paris)

Présentée par

Rawad Mezher

Pour obtenir le grade de

DOCTEUR de SORBONNE UNIVERSITÉ

Sujet de la thèse :

Randomness for Quantum Information Processing

soutenue le 15 Novembre 2019

devant le jury composé de :

M. Damian Markham	Directeur de thése
M. Joseph Dgheim	Directeur de thése
M. Joe Ghalbouni	Encadrent de thése
M. Ashley Montanaro	Rapporteur
M. Peter Turner	Rapporteur
Mme. Elham Kashefi	Examinatrice
Mme. Nancy Rahbany	Examinatrice

Abstract

This thesis is focused on the generation and understanding of particular kinds of quantum randomness. Randomness is useful for many tasks in physics and information processing, from randomized benchmarking [1], to black hole physics [2], as well demonstrating a so-called quantum speedup [3], and many other applications. On the one hand we explore how to generate a particular form of random evolution known as a t-design. On the other we show how this can also give instances for quantum speedup - where classical computers cannot simulate the randomness efficiently. We also show that this is still possible in noisy realistic settings.

More specifically, this thesis is centered around three main topics. The first of these being the generation of ε-approximate unitary t-designs. In this direction, we first show that non-adaptive, fixed measurements on a graph state composed of $\Omega(n(nt + log(\frac{1}{\varepsilon})))$ qubits, and with a regular structure (that of a brickwork state [4]) effectively give rise to a random unitary ensemble which is a ε-approximate t-design. This work is presented in Chapter 3. Before this work, it was known that non-adaptive fixed XY measurements on a graph state give rise to unitary t-designs [5], however the graph states

used there were of complicated structure and were therefore not natural candidates for measurement based quantum computing (MBQC), and the circuits to make them were complicated. The novelty in our work is showing that t-designs can be generated by fixed, non-adaptive measurements on graph states whose underlying graphs are regular 2D lattices. These graph states are universal resources for MBQC. Therefore, our result allows the natural integration of unitary t-designs, which provide a notion of quantum pseudorandomness which is very useful in quantum algorithms, into quantum algorithms running in MBQC. Moreover, in the circuit picture this construction for t-designs may be viewed as a constant depth quantum circuit, albeit with a polynomial number of ancillas.

We then provide new constructions of ε-approximate unitary t-designs both in the circuit model and in MBQC which are based on a relaxation of technical requirements in previous constructions [6]. These constructions are found in Chapters 4 and 5.

The second topic of this thesis deals with sampling from the output probabilities of quantum devices which demonstrate a quantum speedup, in the sense that no classical polynomial time algorithm can sample from these probabilities given some complexity theoretic conjectures - which are widely held to be true - hold. In this direction, we present new examples of such sampling problems defined by non-adaptive fixed angle measurements on 2D graph states with a regular structure. Our sampling problems possess desirable properties for experimental implementation such as nearest neighbor interactions, fixed non-adaptive measurements. These sampling problems are presented in Chapters 4 and 6.

The third topic of this thesis concerns observing quantum speedup in a realistic, noisy setting. We present a new example of a sampling problem defined by measurements on a $poly(n)$ sized 2D graph state with n-input qubits. Again, we show that this sampling problem cannot be performed efficiently on a classical computer unless complexity-theoretic conjectures which are widely believed to be true, turn out to be false. Crucially, this sampling problem is robust against general noise models, by virtue of quantum error correction, and also posseses desirable properties for experimental implementation such as low overhead, nearest neighbor interactions, regular structure, and fixed angle, non-adaptive Pauli measurements. Furthermore, when viewed in the circuit model, this result can be understood as constant depth circuits giving rise to a fault tolerant quantum speedup. This robustness result is found in Chapter 6.

Dedication

To my Mother.

Publications

- R. Mezher et al. **Efficient quantum pseudorandomness with simple graph states. Physical Review A 97.2 (2018): 022333.** This paper forms the basis of Chapter 3 in this thesis.

- R. Mezher et al. **Efficient approximate unitary t-designs from partially invertible universal sets and their application to quantum speedup. arxiv: 1905.01504v3 (Submitted to Communications In Mathematical Physics).** This paper forms the basis of Chapter 4 in this thesis.

- R. Mezher et al. **On unitary t-designs from relaxed seeds arXiv: 1911.03704 (Submitted to Entropy)**. This paper forms the basis of Chapter 5 in this thesis.

- R. Mezher et al. **Fault-tolerant quantum speedup with constant depth circuits (Manuscript in preparation).** This paper forms the basis of Chapter 6 in this thesis.

Acknowledgements

I would like to begin by thanking my Thesis advisor Damian Markham. I think it is safe to say that I would have progressed very little if it were not for his support and guidance. Throughout these three years, and thanks to Damian, I have learned to think like a scientist, to be patient, to write in a scientific way, to think before saying anything which I am not sure of. But there is more, in addition to the scientific guidance, Damian would never miss an oportunity to boost my morale when I needed it, or to help me in any way he can. Thank you for being an amazing advisor, on every level.
Thanks also to my advisor Joseph Dgheim who also proof-read the entire thesis and gave me valuable feedback, and my co-advisor Joe Ghalbouni for the support and encouragement, and for reading meticulously through this manuscript and providing valuable feedback.

I would also like to thank the other permanents of LIP6 Eleni Diamanti, Elham Kashefi, and Frederic Grosshans, for useful discussions and lessons. In particular, I always enjoyed listening to Frederic's opinions on how to be a good scientist, as well as on the politics of the region!
These three years would have been much less enjoyable if it were not for the

friends I met along the way. I would like to thank each and every one of the postdocs, PhD's, and interns at the group in LIP6, who have become too numerous now to state on an individual basis! Thanks guys for making my stay at Paris super cool!

I have had the pleasure to work with two very bright Masters students from the Lebanese University (my home university) who have become dear friends. To Elie Merhej and Marie-Jose Saleh Afif, I wish you the best of luck in your scientific careers.

To my old friends Doumet Helou, Hala Rammouz, Sandy Makhlouf, Jamil Rahme, George Nicolas, Helen Ibrahim, Sevag Abadian, Hagop Abadian, and Oscar Daoura thanks for making my time outside of work enjoyable both in Lebanon and in Paris.

Thanks also to Pr. Youssef Zaatar, and Pr. Ziad Herro for their hospitality in the LPA lab at the Lebanese University : Faculty of Sciences 2.
Thanks to the members of the Jury, for taking the time to read through this thesis, and for agreeing to be part of my Jury.

Thanks to my close family members, Roland Asmar and his family, and Jeannette Frenn and her family who have always stood by my side when I needed it.

Finally, the greatest of thanks goes to my sister Yara, my girlfriend Sally, and to my Mother, to whom I dedicate this thesis. Thank you for all the sacrifices you made, and are still making, to help me reach my goals. I hope someday I will be able to repay the favour.

Contents

List of Figures

Chapter 1

General Introduction

The great promise offered by quantum technologies is getting ever closer to a reality. Indeed, quantum technologies promise revolutionary developments in various fields, from breaking RSA encryption in polynomial time [10], to simulating quantum mechanics as originally suggested by Feynman [11], as well as advances in sensing [12], metrology [13], combinatorial optimization [14], and many other areas.

Critical to many of these developments is the building of the so-called quantum computer, which is a device which uses the laws of quantum mechanics to process information, analogous to how a classical computer processes information by using the laws of classical physics. Of course one should mention that the processing of information is a physical process [15] which involves the evolution of a physical state. The evolution in quantum mechanics being more general than that of classical physics opens up the possibility that quantum computers could be more powerful than their classical counterparts [16].

The pioneering works of Shor [10] and Grover [17] were the first to provide compelling evidence for the above mentioned claim by giving examples of *quantum algorithms* [1] to solve particular computational tasks which demonstrate a quantum advantage − in the sense that quantum algorithms can solve the computational task faster − over the best known classical algorithms to solve these tasks. These seminal results have sparked a surge of research in the field of quantum algorithms leading to the discovery of a plethora of quantum algorithms which outperform their classical counterparts for particular computational tasks. Active research is also being conducted to understand the *resources* unique to quantum theory which are at the heart of quantum-over-classical-advantage in computing and communication tasks (see for example [18, 19, 20]). It is worth mentioning that quantum computers, even though they seem to provide an advantage over classical computers for particular computational tasks, are not expected to solve *every* computational task more efficiently than a classical computer, nor are they expected to solve problems which are generally thought to be truly intractable such as, say, NP-complete problems [21].

In classical computing, *randomness* and *pseudo-randomness* play key roles in developping new and faster classical algorithms [16]. Therefore, it makes sense to pursue the quantum analogues of classical randomness, or simply *quantum randomness* with the same goals in mind. Indeed, quantum randomness has found many applications across quantum informa-

[1] Which are algorithms that can be performed on an *ideal universal* quantum computer. Where it is meant by ideal that the quantum computer is isolated from the effects of noise, which irrevocably damage the precious quantum information. By universal it is meant that the quantum computer can perform *any* quantum operation, more about this is to be said in the coming chapters.

tion and physics in general, ranging from randomized benchmarking [1], secure private channels [22], to understanding how quantum systems thermalize [23], as well as modeling black holes [2], and recently as providing natural candidates for devices demonstrating a *quantum speedup* [24, 25, 26, 27]. Unfortunately, genuine (Haar) quantum randomness is computationally inefficient, as it requires exponential quantum resources [28]. This fact naturally leads us to search for efficient alternatives to genuine quantum randomness. These alternatives have been shown to exist, and are known as *pseudo-random* quantum unitary ensembles, or more formally as unitary t-designs [29]. [2] One of the goals of this thesis will be to explore the problem of generating unitary t-designs. We will present novel advancements in this area by providing new constructions of *random quantum circuits* giving rise to unitary t-designs which remove rigid requirements in previous constructions [6]. We will also show that unitary t-designs can be generated by non-adaptive fixed angle measurements on 2D cluster states, which arguably is of important practical relevance [30].

Although, to date, there are examples of quantum algorithms which outperform classical algorithms, on the practical level, these algorithms in general require quantum computers with a suitable level of fault-tolerance and scalability [3], the likes of which appear to be out of the reach of current technological developments [31]. An interesting question is thus, what can be done with so-called *sub-universal* quantum devices which are not universal in the sense that they can perform any quantum operation, are realizable in principle by our current technologies, but nevertheless capture

[2] The reason behind this nomenclature will be made clear in forthcoming chapters.

the power of quantum computing. Examples of such devices are those of [3, 32, 24, 25, 26, 27]. Sampling from the output probability of these devices has been shown to be classically impossible efficiently, provided widely believed complexity theoretic conjectures hold [3, 32]. Thus, these devices demonstrate what is known as an exponential *quantum speedup*. This speedup is based on strongly believed complexity theoretic conjectures, and thus there is compelling evidence to believe it. The same cannot be said of some quantum algorithms, for which no such complexity theoretic evidence exists. In this thesis, we will add to the established literature new examples of sub-universal devices demonstrating a quantum speedup, and obtained by practically relevant means; namely fixed non-adaptive measurements on 2D cluster states.

A main road block in the way of building a fully-fledged universal quantum computer is noise. Indeed, there is evidence that whatever quantum advantage a particular quantum device gives, disappears when this device is noisy [33, 34, 35]. To counter this problem, in this thesis, we provide an example of a 2D graph state architecture with practically desired properties such as nearest neighbor interactions, which when measured at fixed angles non-adaptively gives rise to output probabilities whose sampling shows a quantum speedup. Crucially, this quantum speedup is *robust* to noise, because the qubits of this graph state are based on a particular quantum error correcting code.

This thesis is divided into seven chapters. Chapter 2 gives some background into the various ideas and technicalities used in this thesis. Our

contributions begin in Chapter 3 where we show that non-adaptive, fixed angle measurements on efficiently preparable graph states with a regular structure can give rise to so-called unitary t-designs [30, 29, 36]. In Chapter 4, we provide new efficient constructions of unitary t-designs both in the circuit model [37] and in the measurement based model [30] which go beyond standard constructions of these t-designs [6]. We also find examples of new sampling problems, based on these constructions, which demonstrate a quantum speedup, up to standard complexity theoretic conjectures [33]. In Chapter 5, we present a new efficient construction for unitary t-designs which also goes beyond the standard constructions [6], and proves a conjecture raised in [6]. In Chapter 6, we present an example of a sampling problem which is robust to general noise models, and which can be viewed as a constant depth-circuit acting on a polynomial number of ancillas. This sampling problem also posseses desirable properties such as nearest-neighbor gates, non-adaptivity, and single instance hardness [38], among others. Chapter 7 is a general conclusion which also discusses some open questions to be treated.

For ease of reading and accessibility, each Chapter is written to be largely self contained, which means some notions will be repeated, and where necessary we will refer back to earlier parts of the thesis or external material.

Chapter 2

Background

In this chapter, we introduce some basic concepts which will be made use of in the later chapters of this thesis where we will present our research results. The concepts introduced here will be a brief mix of each of the mathematical formalism of Quantum Mechanics (QM), Complexity Theory (CT), measurement based Quantum Computing (MBQC), the theory of exact and approximate unitary t-designs, as well notions of classical simulability and quantum speedup.

2.1 Quantum Mechanics

In this section we present a brief introduction to QM. More detailed introductions can be found in references like [37, 39] (see also [40]).

QM is based on mathematical axioms. The first being that a quantum system is completely defined by specifying its *state vector*, called a $wavefunction$. The wavefunction is a complex vector with unit norm de-

fined on the Hilbert space $\mathcal{H} = \mathbb{C}^d$, which is just the usual d-dimensional complex space $\mathbb{C}^d$ endowed with an inner product. We will use *Dirac notation* and denote a wave function of a physical system as

$$|\psi\rangle \in \mathcal{H}. \tag{2.1}$$

$|\psi\rangle$ can be thought of as a column vector with d complex entries, and it is commonly referred to as a *pure state* in the quantum information literature [37]. The corresponding *conjugate* row vector is then denoted as $\langle\psi|$. We also write the inner product of two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ as

$$\langle\psi_1|\psi_2\rangle. \tag{2.2}$$

Systems can also be in states which are probabilistic mixtures of pure states, and are called *mixed* states, we describe mixed states using their density matrix ρ as

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

where $p_i \in [0, 1]$ and $\sum_i p_i = 1$, and where $|\psi_i\rangle$ are pure states.

The second axiom deals with *physical properties* such as energy, momentum,... To every physical property $\mathcal{A}$, we associate a *linear*, *Hermitian* operator A which acts on states $|\psi\rangle \in \mathcal{H}$, and whose *eigenvalues* are the possible values taken by physical property $\mathcal{A}$.

The third axiom is known as *Born*'s *rule*, and relates the mathematical formalism of QM to experiment. Born's rule states that, given a system in the state $|\psi\rangle$, the probability of *measuring* this system in a state $|\phi\rangle$ is

given by

$$p = |\langle\phi|\psi\rangle|^2. \tag{2.4}$$

It is said that the wave function $|\psi\rangle$ of the system *collapses* to the state $|\phi\rangle$ after measurement. This axiom also gives us a way of finding the probabilities of observing the different values of physical properties $\mathcal{A}$. Indeed, using the *spectral theorem* [41] and the second axiom, one finds that the Hermitian operators A, associated to physical properties $\mathcal{A}$ can be written as

$$A = \sum_i \lambda_i |i\rangle\langle i|, \tag{2.5}$$

where λ_i are the eigenvalues of A, and $|i\rangle$ are the *eigenstates* corresponding to the eigenvalues λ_i. For a system in a state $|\psi\rangle$, the probability of observing eigenvalue λ_i is given by

$$p = |\langle i|\psi\rangle|^2. \tag{2.6}$$

The fourth axiom deals with the *evolution* of the state of a physical system [1], and says that this evolution is *unitary* for *closed* quantum systems. More precisely, the state of a quantum system at time t, $|\psi(t)\rangle$, is derived from the *initial* (at time t_0) state $|\psi(t_0)\rangle$ by

$$|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle, \tag{2.7}$$

where $U(t, t_0)$ is a *unitary matrix*. In QM, this unitary evolution is governed by, and determined from a linear partial differential equation called the

[1] Note that the projection may also be thought of as a form of, non-unitary, evolution.

Schrödinger Equation [42]. It is worth noting that QM has been derived by extending probability theory to vectors of complex amplitude [43], as well as from arguably more reasonable axioms [44].

The axioms of QM give rise to a rich mathematical structure which can be exploited to gain *computational advantages* on the practical level. These advantages are in the sense that quantum protocols, or quantum algorithms can perform some computational tasks faster than any of their known classical counterparts, a feature we will call *quantum advantage* [2]. Before elaborating on this idea, let us define the basic unit of quantum information processing, the *quantum bit*, or *qubit*. The qubit is a 2-level quantum system, for example the up and down spin states of an electron, or the horizontal and vertical polarizations of a photon [37]. The Hilbert space of a qubit is $\mathcal{H} = \mathbb{C}^2$, the qubit at any point in time can be in either the two states $|0\rangle$ and $|1\rangle$ which are, for example, the two spin states of an electron, or in a superposition of these two states (by the fourth axiom) given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.8}$$

[2] In this thesis we will mainly use two terms to refer to computational advantages offered by QM. The first of these terms is *quantum advantage* which we take to mean *any* advantage offered by quantum devices over there classical counterparts for particular tasks, whether it be a polynomial advantage (in the sense that the quantum device requires polynomially less resources than its classical counterpart to perform a particular given task) as in [20] for example, or an exponential one (in the sense that the quantum device requires exponentially less resources to perform a particular given task) as in [3]. Whereas the second term, *quantum speedup*, we reserve for tasks demonstrating an exponential advantage, and where this exponential advantage is backed up by widely believed complexity theoretic conjectures, as in [3].

with α and β two complex numbers related by

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.9}$$

Equation (2.8) is called the *principle of superposition*, and is the first striking departure from the laws of classical information theory (where binary digits are always either 0 or 1, and never in superposition). When the number of qubits is n – which would correspond to a quantum system defined on a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 ... \otimes \mathcal{H}_n$, where $\mathcal{H}_i = \mathbb{C}^2$ – the state of such an n-qubit quantum system can be in a superposition of 2^n states of the form

$$|i_1 ... i_n\rangle := |i_1\rangle \otimes |i_2\rangle \otimes ... \otimes |i_n\rangle, \tag{2.10}$$

where $i_j \in \{0, 1\}$. One would be tempted to say at this point that a quantum computer made up of n qubits can perform 2^n computations *simultaneously*, this is, however, an *erroneous* assumption. Particularly because to extract useful information out of a quantum computation, one would need to perform a measurement which collapses the wavefunction of the system to a *single* state, by the third axiom. Nevertheless, the *superposition principle* can be used to extract some quantum advantage, along with other techniques in quantum computing which ensure a *destructive* interference of all but the *good* state corresponding to the desired computation [21], as is done for example in [10].

Another striking feature of QM is *entanglement* [45]. As an example of this feature for the bipartite case, the mathematical structure of the Hilbert space of a bipartite system $\mathcal{H}_1 \otimes \mathcal{H}_2$ allows the existence of pure

states which *cannot* be written as a single product of the form $|\psi_1\rangle \otimes |\psi_2\rangle$, where $|\psi_1\rangle \in \mathcal{H}_1$, and $|\psi_2\rangle \in \mathcal{H}_2$. These bipartite qubit states which cannot be written as a single product of one-party states are called *entangled states*. A more general formulation of (bipartite) entanglement which encompasses mixed states as well as pure states is as follows. A (pure or mixed) state whose density matrix cannot be written as a convex combination of product state density matrices, which are density matrices having the form $\rho = \rho_1 \otimes \rho_2$ where $\rho_i = |\psi_i\rangle\langle\psi_i|$ with $|\psi_i\rangle \in \mathcal{H}_i$ and $i \in \{1, 2\}$, is said to be entangled with respect to partitions 1 and 2 [45]. One can also generalize the concept of entanglement to a multipartite setting using similar arguments as those seen above [45]. Entanglement, and the intimately related concept of *non-locality* [46] are more and more being understood as a main resource behind the quantum advantage found for example in communication protocols [47], as well as the universality of measurement based quantum computing [48]. Morever, the phenomenon of *contextuality* [49] (of which non-locality is understood as being a special case of [50]) arises naturally when trying to understand how commuting quantum observables act on quantum states, at the level of their eigenvalues [49]. Contextuality, which has been generalized to a broad extent [51, 52], is now being understood to lie at the heart of quantum computational advantage [19, 20, 51, 53].

Perhaps, what is even more bizarre is that there is evidence that quantum theory may turn out to be an *island* in theory space [54, 55, 56]. Indeed, changing the axioms of QM only slightly results in *perverse* physical consequences, such as signalling [54]. Also, considering slightly more general correlations than those allowed by QM leads to the violation of, arguably,

fundamental principles [55, 56].

The above mentioned facts make the study of QM, quantum information, and quantum computing fascinating topics [3], and it is in the wise words of Eugene Wigner [57] that I choose to end this paragraph : **The miracle of the appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve. We should be grateful for it and hope that it will remain valid in future research and that it will extend, for better or for worse, to our pleasure, even though perhaps also to our bafflement, to wide branches of learning.**

2.1.1 Basic Tools

In this subsection we define some of the basic tools, relevant to this thesis, used in quantum computation. More detailed expositions can be found in references like [37].

A qubit in a pure state can be thought of as a point on the surface of a sphere of radius one, called the Bloch sphere. Or equivalently as a Bloch vector which starts at the origin of the Bloch sphere and terminates on a point of the sphere [37]. Mixed states in this picture correspond to points inside the Bloch sphere. In this way, single qubit unitaries (or gates) can be thought of as norm-preserving rotations on the Bloch sphere, around particular axes. As an example, the Pauli matrices

[3] At least to the author of this thesis.

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

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

and

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

can be thought of as rotations by an angle π around the X, Y, and Z axes of the Bloch sphere respectively. In this thesis, we will often use rotations around the Z axis at specified angles $\theta \in [0, 2\pi]$. We will denote these rotations as $Z(\theta)$, and their corresponding unitaries have the form

$$Z(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}.$$

We will similarly denote rotations by θ around the X and Y axes as $X(\theta)$ and $Y(\theta)$. Another single qubit gate which we will make frequent use of is the Hadamard gate H, which is given by

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

H acts on the basis states $\{|0\rangle, |1\rangle\}$ as

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

and

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

We will denote

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

and

$$|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Single qubit gates do not suffice for universal quantum computation, and must be complemented with at least one *entangling* 2-qubit gate to achieve this universality [58]. Whenever we refer to universality in this thesis, we mean *approximate universality* where products of unitaries from a (usually finite) set of fixed unitaries can approximate *any* unitary up to arbitrary precision (see [58] for example for a more formal definition). A particularly useful 2-qubit entangling gate which we will frequently use is the controlled Z gate, which is denoted as CZ and whose unitary matrix is given by

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Indeed, the CZ gate, together with the Hadamard gate are used in generating graph states for MBQC [30], as we will see in Section 2.3. We end this subsection by describing a type of measurement which we will use frequently in our MBQC protocols, namely a (single-qubit) measurement at an angle θ in the XY plane. In the Bloch sphere picture, this means projecting the Bloch vector of a qubit onto an axis having an angle θ with respect to the X axis. More details on this are found in Section 2.3.

2.2 Complexity Theory

In this section, we present a very brief overview of Complexity Theory (CT). More detailed introductions can be found in references like [37], for example. The purpose of this section is to familiarize the reader with *complexity classes* such as **P**, **NP**, $\sharp$**P**, **BQP**,... as well as notions of *hardness* which will be made use of in forthcoming chapters.

The goal of CT is to study the *spatial* and *temporal* resources needed to solve *computational problems*, and give lower bounds on these resources required by an algorithm which solves these problems *optimally*. Before going any further, it is convenient to define a *computational problem*. In a computational problem we are given an *input*, and we want to return an *output* which must satisfy some property, given the input. Computational problems can either be *decision problems*, *search problems*, *counting problems*, or *optimization problems* [4]. A decision problem is a *yes-no* answer to a given question. For example, given a number n, is it even? Other problems are

[4]Note however that every type of these problems can be viewed as a search problem.

a little bit trickier to define, and require the introduction of some mathematical machinery first. Computational problems can be rather cleanly defined in terms of *strings*, *languages* and *alphabets*. An *alphabet* is a non-empty finite set Σ. For our purposes, let $\Sigma = \{0, 1\}$. An element $x \in \Sigma$ is called a *symbol*. A *string* s is a finite sequence of symbols from Σ. The set of all possible strings will be denoted as S. A *language* L over Σ is a subset of S. In this sense, any *decision* problem can be formulated as follows : Decide whether a given input string $s \in S$ belongs to the language $L_f = \{s \in S \mid f(s) = 1\}$, where $f : S \to \{0, 1\}$ is a *boolean* function defining the decision problem. An algorithm solves a decision problem by *accepting* any input string $s \in L_f$, or *rejecting* any input string $s^{'} \notin L_f$. In a *search* problem, given an input $s_1 \in S$, we want to compute an output $s_2 \in S$ which is a solution (if one exists) to the search problem, such that s_1 and s_2 are related by some *search relation* $R \subseteq S \times S$, where s_2 is an accepted solution to the search problem iff $(s_1, s_2) \in R$. A *counting* problem counts the number of solutions of a search problem. More precisely, if R is a search relation, then the corresponding counting problem is defined by $C_R(x) = |\{y \mid (x, y) \in R\}|$.

With the relevant (to this thesis) types of computational problems being defined, we will now define some well-known complexity classes, we will often make use of these classes in later parts of this thesis. Let the *complexity class* **P** be the class of decision problems *solvable* in polynomial time by a

classical algorithm.[5] **NP** is the class of decision problems whose *accept* instances can be *verified* in polynomial time by a classical algorithm. One of the deepest questions in Mathematics (and worth a million bucks! [59]) is whether **P**=**NP**. Although it is strongly believed that $\mathbf{P} \neq \mathbf{NP}$ [60] , yet it appears that the proof of this claim is beyond the scope of what is considered a *natural proof* [61] (see also [62]). The proofs of hardness of classical simulability presented in this thesis rely on the fact that $\mathbf{P} \neq \mathbf{NP}$ [6]. Among the problems in **NP**, are the so-called **NP**-*complete* problems which are in a sense the *hardest* problems to solve in **NP**, since solving these problems in time $poly(n)$, allows to solve *any* problem in **NP** in time $poly(n)$ [37]. **NP**-*hard* problems are decision problems, not necessarily in **NP** (in contrast to **NP**-complete problems), but to which *every* problem in **NP** can be reduced to by a polynomial time classical algorithm, given *oracle access* to the function f defining the **NP**-hard problem [64]. Clearly, the set of **NP**-hard problems contains all the **NP**-complete problems. The notions of *hard* and *complete* extend also to other complexity classes, in the same manner as they are defined for **NP**. The class $\sharp\mathbf{P}$ is the class of *counting* problems associated with decision problems in **NP** [65]. That is, $\sharp\mathbf{P}$ is the set of all functions which count the number of accepting paths of any given **NP**-problem [64]. **BQP** is the class of decision problems solvable by a polynomial time *quantum* algorithm (which is an algorithm which runs on a quantum computer [37]), with bounded probability of error [37].

[5] We mean by classical algorithm, an algorithm which *runs* on a classical deterministic Turing machine [37].

[6] Actually, we will rely on a slightly weaker conjecture, that the so-called *polynomial heirarchy* does not collapse [63], as seen in later chapters

Postselection, which is defined as the ability to discard all computations in which a given event does not occur, is a powerful theoretical tool in complexity theory. Although postselection is not *practical*, in the sense that one cannot, in general, assume in a computation that one has the ability to postselect, nevertheless it can be used as a tool to get insight about the power of a computation. An interesting result in this direction which is relevant to this thesis is that quantum circuits which are universal under post-selection give rise to probability distributions whose relative error approximation is $\sharp\mathbf{P}$-hard [66].

We will illustrate how the proof of [66] proceeds. The proof begins by noting that if one can approximate up to relative error the output probabilities (which are the probabilities obtained by measuring the output qubits of a quantum device) $\{p\}$ of a quantum device (which is universal under postselection), one can use these probabilities to get a relative error approximation of the postselected output probabilities $\{p_{post}\}$. Next, consider the power of postselected universal quantum computation, Scott Aaronson showed that **PostBQP**=**PP** [67], where **PP** is the class of decision problems solvable by a *probabilistic Turing machine* [68] in polynomial time with a probability of error of less than 1/2 for all instances. Using this result, together with the fact that $\mathbf{P}^{\sharp\mathbf{P}} = \mathbf{P}^{\mathbf{PP}}$ [66], with $\mathbf{A}^{\mathbf{C}}$ meaning the complexity class **A**, with *oracle* access to **C**, it can be shown that, given access to a relative error approximation of the probabilities $\{p\}$, and a polynomial time classical algorithm, it is enough to solve a $\sharp\mathbf{P}$-complete problem. Therefore, the probabilities $\{p\}$ are $\sharp\mathbf{P}$-hard (by definition of *hard* in this section) to compute up to relative error, thereby completing the proof (more details in

[66]).

2.3 Measurement Based Quantum Computation (MBQC)

MBQC is a model of *universal* quantum computation which proceeds in general by performing *adaptive* single qubit measurements on a highly entangled multi-partite quantum state [30]. This model allows for *universal quantum computation* [30], as is the case for the conventional *circuit model* of quantum computing [37], which we will not discuss here. MBQC is a natural landscape for the generation of *random unitary* ensembles [5], which are one of the main objects of interest in this thesis.

Definition 1. *A random unitary ensemble in* $U(N)$ *is a couple* $\{p_i, U_i \in \mathcal{U}\}_{i=1,\dots|\mathcal{U}|}$ *(or simply* $\{p_i, U_i\}$ *for ease of notation), where each unitary* $U_i \in \mathcal{U}$ *is drawn with probability* $p_i \geq 0$*, and* $\sum_i p_i = 1$*, with* $\mathcal{U} \subset U(N)$*.*

This section shows how one can generate such ensembles in the language of MBQC. We begin by introducing graph states (see e.g. [69]), a main component of MBQC.

Graph states are a family of multipartite quantum states, with simple descriptions in terms of graphs [69]. They are very useful resources for quantum information, with applications in measurement based quantum computing [30], fault tolerance [70], cryptographic multiparty protocols [71], quantum networks [72] and recently for generating t-designs [5, 36] and

instances of quantum speedup [25, 26]. They represent the cutting edge in terms of size of entangled states that can be generated and controlled in experiments, with implementations demonstrated in optics [73, 74, 75], [76, 77] including on chip [78], in ion traps [79, 80], super conducting qubits [81] and NV centres [82]. Remarkably, in continuous variable quantum optics graph states of up to 10^4 parties have been created [77]. Furthermore there are several techniques that have been developed to verify the quality of graph states in various settings of trust [25, 51, 38, 83, 84] which can often be translated into verification of their applications. More formally, one can define graph states as follows.

Definition 2. *A graph state $|G\rangle$ is a pure entangled multipartite state of n qubits in one-to-one correspondance with a graph $G = \{E, V\}$ of n vertices. Every vertex $i \in V$ represents a qubit, and each edge $(i, j) \in E$ can be understood as a preparation entanglement.*

$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j}|+\rangle^{\otimes n}, \tag{2.11}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $CZ_{i,j}$ is the controlled Z gate applied to qubits i and j (see e.g. [37]).

For the purposes of computation, a subset of qubits $I \subset V$ is defined as the computational input with initial input state $|\psi_{in}\rangle_I$, and the associated *open* graph state has the form

$$|G(\psi)\rangle = \prod_{(i,j)\in E} CZ_{i,j}|\psi_{in}\rangle_I \otimes |+\rangle_{V/I}. \tag{2.12}$$

A cluster state [85] is a particular type of graph state whose corresponding graph is a regular two dimensional square lattice. In MBQC, computation is carried out by performing measurements on all but a subset $O \subset V$ of qubits. In general one has $|O| \geq |I|$, though here we are concered only with the case $|I| = |O|$ in this thesis. By performing the measurements adaptively on a universal resource state (such as the cluster state) - via some corrective strategy such as the gflow [86] - one can implement any desired unitary $U \in U(2^{|O|})$ on the input state, which is teleported to the (unmeasured) output position by the end of the computation. At the end of the computation, we are left with the following state

$$|OUT\rangle = |M\rangle_{V/O} \otimes U|\psi_{in}\rangle_O, \tag{2.13}$$

where $|M\rangle_{V/O}$ represents the measurement outcomes, performed adaptively. Cluster states are universal resources for measurement based quantum computation (MBQC) [30, 85], even when all the measurement angles are chosen from the XY plane [87].

On the other hand, performing the measurements non-adaptively (that is, simultaneously and without a corrective strategy) generates a random unitary ensemble $\{p_i, U_i\}$, seen from noting that we can (for an appropriate choice of measurement bases) write $|G(\psi)\rangle$ as,

$$|G(\psi)\rangle = \sum_i \sqrt{p_i}|M_i\rangle_{V/O} \otimes U_i|\psi_{in}\rangle_O. \tag{2.14}$$

$|M_i\rangle_{V/O}$ denotes a possible string of measurement results which implements

unitary U_i on the input state. This measurement result occurs with probability p_i. In our case [88], the probability distribution is uniform, $p_i = \frac{1}{2^{|V/O|}}$. Figure 2.1 shows an example of a non-adaptive MBQC scheme on a 2-row, 2-column cluster state at XY plane measurements α, β, $|V| = 4$, and $|O|$=2. This non-adaptive scheme generates the random unitary ensemble,

$$\{\frac{1}{4}, CZ(HZ(\alpha + m_1\pi) \otimes HZ(\beta + m_2\pi))\}, \tag{2.15}$$

where H is the Hadamard gate, $Z(\alpha)$ is a rotation by angle α around the Z axis, CZ is the controlled-Z gate and $m_i \in \{0, 1\}$ represents the measurement outcome of qubit i, following the convention that $m_1 = 0$ is taken to mean measurement outcome corresponding to a projection onto $|+_\alpha\rangle = \frac{|0\rangle + e^{i\alpha}|1\rangle}{\sqrt{2}}$ (respectively $|+_\beta\rangle = \frac{|0\rangle + e^{i\beta}|1\rangle}{\sqrt{2}}$ for $m_2 = 0$) and $m_1 = 1$ a projection onto $|-_\alpha\rangle = \frac{|0\rangle - e^{i\alpha}|1\rangle}{\sqrt{2}}$ (respectively $|-_\beta\rangle = \frac{|0\rangle - e^{i\beta}|1\rangle}{\sqrt{2}}$ for $m_2 = 1$).

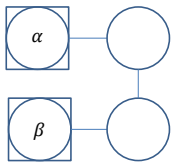

Figure 2.1: MB scheme on a 2-row, 2-column cluster state. The input qubits (squared circles) when measured non-adaptively at XY angles α and β apply to the unmeasured output qubits (empty circles) a random unitary of the ensemble of Equation (2.15) chosen with a uniform probability of $\frac{1}{4}$. The horizontal and vertical lines are preparation entanglements.

2.4 Unitary t-designs

2.4.1 t-wise Independence

As mentioned in the introduction to this thesis, randomness is an extremely useful resource in generating new, faster algorithms both classically [89], and quantumly [37]. However, the generation of *genuine* random resources is usually computationally inefficient [89, 28]. In [89], an efficient construction for sampling from so called *t-wise independent* random variables was presented. Perhaps an intuitive way to think of a *quantum t-design* is that it is the *quantum analogue* of t-wise independence [90, 16]. A collection of n random variables $\mathcal{X} = \{X_1, ..., X_n\}$, where $X_i \in \{0, 1\}$ (for our purposes) is said to be t-wise independent, if for any subset $\{X_1, ..., X_j\}$ with $j \leq t < n$, where $X_j \in \mathcal{X}$, it holds that

$$P(X_1 = x_1, .., X_j = x_j) = P(X_1 = x_1)...P(X_j = x_j), \tag{2.16}$$

where $P(X_i = x_i)$ is the probability that random variable X_i takes the value $x_i \in \{0, 1\}$ [89]. There are also notions of *approximate* t-wise independence [91]. t-wise independent random variables are resources which *save* randomness, in the sense that the number of independently random bits is less in $t < n$-wise independent random variables than that in $\mathcal{L} = \{Y_1, ..., Y_n\}$, where $Y_i \in \{0, 1\}$, and where each of the Y_i's is an idependent random variable [16]. It is in the same sense that quantum t-designs save *quantum randomness*. The notion of *quantum randomness* which has been studied extensively for its usefullness, and which will be studied in this thesis,

is sampling from the Haar measure on the unitary group $U(N)$ [92]. The Haar measure can be thought of as the most natural group theoretical definition of random, and chosing unitaries from the Haar measure has wide applications [1, 22, 23, 93, 24, 25, 26, 27, 94]. However, the construction of Haar distributed unitaries requires exponential resources to be realized [28], and is thus computationally inefficient. On the other hand, quantum t-designs (like t-wise independent sets, their classical analogues) can be generated efficiently, and act exactly as the Haar measure up to tth order in the statistical moments, which is often sufficient for the application in mind [1, 22, 23, 93, 24, 25, 26, 27, 94]. Quantum t-designs are of two types, *projective* or *state* t-designs [95, 96, 97], and their generalization, *unitary* t-designs [29, 98, 6, 99, 24, 5, 36, 100, 101, 102, 103, 94] which will be the focus of this thesis. In the next sections we will define *exact* [29, 5, 99, 102] and ε-*approximate* [29, 98, 6, 99, 24, 5, 36, 100, 101, 102, 103, 94] *unitary* t-designs. In this thesis we concentrate on studying ε-approximate t-designs.

2.4.2 Exact Unitary t-designs

Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ be the n-qubit Hilbert space. A random unitary ensemble $\{p_i, U_i \in \mathcal{U}\}$ (see Definition 1), where $U_i \in U(2^n)$ is called an *exact* unitary t-design if the following relation holds [29, 102, 103]

$$\sum_i p_i P_{(t,t)}(U_i) = \int_{U(2^n)} P_{(t,t)}(U) \mu_H(dU), \tag{2.17}$$

where μ_H denotes the Haar measure on the n-qubit unitary group $U(2^n)$, and $P_{(t,t)}(U)$ is *any* polynomial of degree exactly t in the matrix elements

of U, and of degree exactly t in the complex conjugates of these matrix elements [7]. Equation (2.17) allows us to easily see the following property

Proposition 1. *[103] Any exact unitary t-design is also an exact unitary t-1 design.*

To see why Proposition 1 is true, consider the particular choice of

$$P_{(t,t)}(U) = Tr(\frac{U.U^{\dagger}}{2^n}).P_{(t-1,t-1)}(U) = P_{(t-1,t-1)}(U), \tag{2.18}$$

where $P_{(t-1,t-1)}(U)$ is *any* polynomial of degree at most $t-1$ in the matrix elements of U, and degree at most $t-1$ in the complex conjugate of these matrix elements. Then, replace Equation (2.18) in Equation (2.17). Proposition 1 then follows straightforwardly. Note that Proposition 1 holds also for ε-approximate unitary t-designs which will be defined explicitly in the next section.

Not much is known about the structure of ensembles giving rise to exact unitary t-designs. In [102], a group theoretic criterion based on the *characters* of group representations was derived which allowed one in principle to crunch through the character tables of finite groups in search for t-designs. [29] and [103] derived lower bounds on the cardinality $|\mathcal{U}|$ of ensembles $\mathcal{U}$ which can give rise to weighted and unweighted exact unitary t-designs. The uniform distribution over the Clifford group has been shown

[7] In our case, the random ensembles are generated by measurements on *unweighted* graph states [69], meaning that our unitary t-designs are *unweighted* [29, 103] in the sense that $p_i = \frac{1}{|\mathcal{U}|}$.

to be an exact unitary 3-design on $U(2^n)$ [29, 99], but not a 4-design [104]. In [5], a 32 element exact unitary 3-design on $U(2)$ was found. Also, several constructions of exact unitary $t = 2, 3, 5$-designs on $U(2)$ were reported in [103] (as well as various exact unitary $t = 2, 3$-designs on $U(d)$ for various values of d [103]). Only very recently was an exact unitary 4-design on $U(4)$ found [105], albeit numerically. There is also an apparent difficulty in using group theoretic constructions directly when searching for exact unitary $t > 3$-designs on $U(d)$ when $d \geq 3$ [105].

As conveyed in the previous paragraph, the study of exact t-designs is an extremely formidable task. Moreover, for most applications, one only requires a notion of *approximate* unitary t-designs [29, 1, 22, 93, 24, 25, 26, 27, 23, 94]. Furthermore, approximate unitary t-designs can usually be implemented using sets of lower cardinality than their exact counterparts [16].[8] The previously mentioned points motivate the study of ε-approximate unitary t-designs [29, 98, 6, 99, 24, 5, 36, 100, 101, 102, 103, 94], which are the main focus of this thesis, and which will be defined explicitly in the next subsection.

2.4.3 ε-approximate Unitary t-designs

We now formalize the definition of ε-approximate unitary t-designs (or just ε-approximate t-designs for simplicity) which are the main objects of study in this thesis.

[8] Although in this thesis we do not focus on generating t-designs with an *optimal* number of elements, indeed as will be seen in some parts of this thesis, the number of elements in our designs is of higher order than the optimal lower bound.

Definition 3. *[6, 101] Let $\mathcal{H}$ be the n-qubit Hilbert space $(\mathbb{C}^2)^{\otimes n}$. A random unitary ensemble $\{p_i, U_i\}$ (Definition 1) with $U_i \in U(2^n)$ is said to be an ε-approximate t-design if the following holds*

$$(1-\varepsilon)\int_{U(2^n)} U^{\otimes t}\rho U^{\dagger\otimes t}\mu_H(dU) \leq \sum_i p_i U_i^{\otimes t}\rho U_i^{\dagger\otimes t} \leq (1+\varepsilon)\int_{U(2^n)} U^{\otimes t}\rho U^{\dagger\otimes t}\mu_H(dU), \quad (2.19)$$

for all $\rho \in B(\mathcal{H}^{\otimes t})$, where μ_H denotes the Haar measure on $U(2^n)$. For positive semi-definite matrices A and B, $B \leq A$ means $A - B$ is positive semi-definite, ε is a positive real, and t is a positive integer.

Definition 3 is sometimes referred to as the *strong definition* of a ε-approximate t-design [6, 24]. Note that when $\varepsilon = 0$, one recovers a definition of an exact unitary t-design which is equivalent to the definition of Equation (2.17) [106]. Similarly, one can define an approximate t-design in terms of various (inequivalent) norms, depending on the application in mind [6, 24]. All results shown in this thesis concerning approximate t-designs are with respect to the strong definition of a ε-approximate t-design.

To prove our results, we will study the properties of an operator referred to as the *moment superoperator* $M_t[\mu]$ defined as follows [100, 98, 6].

Definition 4. *For a random unitary ensemble $\{p_i, U_i \in \mathcal{U}\}$,*

$$M_t[\mu] = \sum_i p_i U_i^{\otimes t,t}, \quad (2.20)$$

where μ is the probability measure [9] *over the set $\mathcal{U}$ which results in choosing $U_i \in \mathcal{U}$ with probability p_i, and $U^{\otimes t,t} = U^{\otimes t} \otimes U^{*\otimes t}$, and U^* is the complex conjugate of U.*

A useful concept we will frequently make use of is that of an (η, t)-tensor product expander [107, 108] (TPE) defined as follows.

Definition 5. *[107, 108] A random unitary ensemble $\{p_i, U_i\}$ is said to be an (η, t)-TPE if the following holds,*

$$||M_t[\mu] - M_t[\mu_H]||_\infty \leq \eta < 1, \tag{2.21}$$

where $M_t[\mu_H] = \int_{U(2^n)} U^{\otimes t,t} \mu_H(dU)$.

In particular, we will adopt the usual path [6, 98, 101, 36, 5, 94] of showing that our random unitary ensembles are (η, t)-TPE's, then use the following proposition to obtain statements about t-designs.

Proposition 2. *[6, 98, 101] If $\{p_i, U_i \in \mathcal{U}\}$ is an (η, t)-TPE, then the **k-fold concatenation** of $\{p_i, U_i\}$: $\{\prod_{j=1,...k} p_{\pi(j)}, \prod_{j=1,...k} U_{\pi(j)}\}$* [10] *is an ε-approximate t-design when*

$$k \geq \frac{1}{log_2(\frac{1}{\eta})}(4nt + log_2(\frac{1}{\varepsilon})). \tag{2.22}$$

Here π is a function acting on $\{1, ..., k\}$, resulting in a set $\{\pi(1), ...\pi(k)\}$

[9] As shown in [98] one can shift between a probability distribution over a discrete ensemble $\{p_i, U_i\}$ and a continuous distribution by defining the measure $\mu = \sum_i p_i \delta_{U_i}$.

[10] Note that the random ensemble $\{\prod_{j=1,...k} p_{\pi(j)}, \prod_{j=1,...k} U_{\pi(j)}\}$ has a moment super operator $M_t[\mu_k] = (M_t[\mu])^k$ [100].

where $\pi(j) \in \{1, ..., |\mathcal{U}|\}$, the $\pi(j)'s$ can be identical. There are $|\mathcal{U}|^k$ such functions π and the k-fold concatenation includes all of them.

Proof. [6, 101] The k-fold concatenation of $\{p_i, U_i\}$ satisfies $||\delta_{\mu_k} - \delta_{\mu_H}||_\diamond \leq 2^{2nt}\eta^k$, where $||.||_\diamond$ is the diamond norm [6], and δ_μ is defined as $\delta_\mu(X) = \int_{U\sim\mu} U^{\otimes t} X U^{\dagger\otimes t} d\mu(U)$. Furthermore, if $||\delta_{\mu_k} - \delta_{\mu_H}||_\diamond \leq \frac{\varepsilon}{2^{2nt}}$, then $\{\prod_{j=1,...k} p_{\pi(j)}, \prod_{j=1,...k} U_{\pi(j)}\}$ is an ε approximate t-design in the strong sense ($cf.$ Definition 3) [6]. The value of k in Proposition 2 is thus obtained by setting: $\frac{\varepsilon}{2^{2nt}} \geq 2^{2nt}\eta^k$. □

We will often make use of the following fact proven in [98].

Proposition 3. *[98] If μ is a probability measure with support on a universal gate set $\mathcal{U} \subset U(2^n)$ [11], then the following inequality holds for any positive integer t.*

$$||M_t[\mu] - M_t[\mu_H]||_\infty < 1. \tag{2.23}$$

In recent work, ε-approximate t-designs have been shown to anti-concentrate [26, 27]. Fundamentally, anti-concentration is a statement about probability distributions. For circuits that anti-concentrate, the probability of occurrence of *most* outcomes is reasonably large [109]. The property of anti-concentration, plays a key role in proofs of hardness approximate classical sampling [25, 26, 27, 109], and we will use it in our proof of hardness of classical sampling seen in later chapters. We now present a theorem on the anti-concentration of $t \geq 2$ -designs, shown in [26] (a similar result was derived independently in [27]).

[11] In other words, for all $U \in \mathcal{U}$, $\mu(U) \neq 0$.

Proposition 4. *[26] Let* $\{p_i,U_i\}$ *be an* ε*-approximate 2-design on* $U(2^n)$*. Let* $|0\rangle^{\otimes n}:=|0\rangle$ *be an n-qubit input state to which we apply a unitary* U_i *from the 2-design. Then, for any* $x \in \{0,1\}^n$ *there exists a universal constant* $0 \leq \alpha \leq 1$ *such that:*

$$Pr_{U_i\sim\mu}(|\langle x|U_i|0\rangle|^2 > \frac{\alpha(1-\varepsilon)}{2^n}) \geq \frac{(1-\alpha)^2(1-\varepsilon)}{2(1+\varepsilon)}. \tag{2.24}$$

μ *being the probability measure over the t-design that results in choosing* U_i *with probability* p_i*.*

2.5 Notions of Simulability and Structure of a Standard Hardness of Approximate Classical Sampling Proof

Let $\{C_n\}$ be a family of quantum circuits with n input qubits. Suppose also that this family satisfies some uniformity condition (e.g. [3, 110]) to ensure no computationally unreasonable preparations are required with varying inputs of the family. Let P_n denote the probability distribution associated with measuring the outputs of C_n in the computational (Z) basis. We say that the circuit family $\{C_n\}$ is *classically simulable in the strong sense* if any output probability in P_n, and any marginal probability of P_n can be approximated up to m digits of precision by a classical $poly(n,m)$ time algorithm [3].

Because the output probabilities of universal-under-post-selection quantum circuits are ♯P-hard to exactly compute in worst-case [111] (and even

♯P-hard to approximate up to relative error 1/4 in worst-case [66, 112]), this makes the task of strong classical simulability formidable even for quantum computers. In order to find tasks where one clearly sees a quantum speedup, one needs to introduce the notion of classical simulability in the weak sense.

Classical simulability in the weak sense means that the classical algorithm can sample, i.e output x (one of the possible outputs of circuit C_n) with probability $p_x \in P_n$, in $poly(n)$ time. For practical purposes (due to experimental imperfections), one usually requires a notion of approximate classical simulability in the weak sense (henceforth referred to as **approximate classical sampling**), of which many exist [111, 3]. In our work we adopt the following definition of approximate classical sampling (taken from [3]).

Definition 6. *We say that a family of circuits $\{C_n\}$ on n-qubits where each C_n has a set of possible outputs x with an associated output probability p_x is* approximately classically simulable in the weak sense *(i.e admits an approximate classical sampling), up to an l_1-norm distance σ (or equivalently up to total variation distance $\sigma/2$), if there exists a $poly(n)$ time classical algorithm A sampling x with probability p_{A_x} for which the following holds*

$$\forall C_n \in \{C_n\}, \sum_x |p_x - p_{A_x}| \leq \sigma. \tag{2.25}$$

The expression of quantum speedup is precisely that no classical $poly(n)$ time algorithm A exists which can approximately sample (in the sense of Equation (2.25)) given that some complexity theoretic conjectures hold. The argument for quantum speedup comes from two directions. Firstly

consider the power of a classical algorithm which is able to approximately sample from the distribution p_x as defined above. The trick is to boost this up from sampling p_x, to approximating p_x (that is a simulation in the strong sense). This is the role of Stockmeyer's counting theorem, and it does this at the third level of the polynomial hierarchy (PH) [113]. In particular it says that there is an algorithm at the third level (concretely in $FBPP^{NP}$) which takes the classical algorithm for sampling p_x and outputs an approximation of p_x, up to **additive error**. The remaining steps on the classical side are to make this approximation stronger, and work for **relative errors**, which is what one wants in order to establish complexity theoretic statements on the hardness of approximating p_x, which are needed in the proof [114, 25, 26]. To do this step we rely on the fact that the output distributions of our families of circuits are not too peaked, this is exactly the anti-concentration property discussed in the previous subsection [115]; where this cannot be proven, this is where one of the standard conjectures of the proofs appears ((Conjecture III) in Section 4.2.2). The final statement is that for a fraction f of the family of circuits considered, the output distrubution p_x can be approximated up to a relative error.

The other direction comes from the known hardness of sampling quantum distributions. The first statement in this direction says that appoximating p_x (exactly, or up to relative error) is $\sharp$P hard in the worst case (that is, for one or more of the circuits in the family), as mentioned earlier. This is standard following universality of the circuit families [114, 33, 38, 26, 25, 27, 66, 116, 115]. The difficulty here is to match this to the statement about the fractions of the circuits considered, in order to match the relative error approximation

we would have classically from above. To this end we are forced to add an assumption about the hardness of the average case (over the circuit family). This is the content of another of the standard conjectures in such proofs (see Conjecture II) in Section 4.2.2.). There are various justifications for this conjecture, depending on which families of problems it is related to [26, 25, 114, 66, 33, 27]. Bringing these together we have that the existence of a classical algorithm approximately sampling p_x (in the sense of Equation (2.25)) implies that solving a $\sharp$P hard problem can be achieved at the third level of the PH. This implies the collapse of the PH to its 3rd level by a theorem of Toda [117]. Thus, if one believes this cannot be possible (the final standard conjecture, and conjecture I) in Section 4.2.2.) one is forced to give up the possibility of such a classical sampling algorithm.

Chapter 3

Efficient Quantum Pseudrandomness With Simple Graph States

3.1 Introduction

As described in Section 2.3, MBQC [30] allows for universal quantum computing by measuring individual qubits prepared in entangled multipartite states, known as graph states [69]. Unless corrected for, the randomness of the measurements leads to the generation of ensembles of random unitaries (see Definition 1 in Section 2.3), where each random unitary is identified with a string of possible measurement results.

In this chapter, we show that repeating a measurement based (MB) scheme, which we define as an assignment of fixed measurement angles on a

graph state of fixed size, an efficient (in the input size) number of times, on a simple graph state, with measurements at fixed angles and no feed-forward corrections, produces a random unitary ensemble that is an ε-approximate t-design on n input qubits (or an n-qubit t-design, as we will sometimes refer to here) [29, 6] (see Section 2.4 for full definitions). Unlike previous constructions for t-designs in MBQC [5], the graph state is regular and is also a universal resource for measurement based quantum computing, closely related to the brickwork state [4]. Following [5] our approach is to harness the quantum randomness arising from applying an MB scheme to produce approximate designs. If one does not apply the adaptive feedforward corrections required for universal deterministic computation (see Section 2.3 for details), the inherent randomness of the measurements effectively samples from ensembles of random unitaries (see Section 2.3).

In [5] it was shown that starting with a graph state with polynomial (in n) number of qubits, and applying fixed angle, translationally invariant, measurements (with no need for feedforward corrections), effectively samples from an approximate t-design. Furthermore this process is efficient in the number of qubits, preperation and measurements, following from the efficiency of the construction of Brandao et al. [6]. Indeed, the construction of the graph state essentially mimics the random circuit construction of Brandao et al. [6]. However, in doing so, the graph itself is rather complicated, and moreover is not a simple regular lattice.

A natural question is then, can simple, regular lattices (such as those useful for universal measurement based computation [85], [4]) be applied to generate t-designs? As well as being more convenient from a practical point

of view (in terms of generating the graph state), this connects the question of optimal generation of ensembles to standard measurement based quantum computation. Furthermore it requires a new proof that it is an approximate t-design (though the techniques we use also follow along the lines of [6] it does not follow directly from their results).

In this chapter we show that it is possible. In particular we show that fixed, translationally invariant, measurements on a regular graph state with poly-log (in n, t, and $\frac{1}{\varepsilon}$) number of qubits, with no feed-forward, results in an ensemble of random unitaries which forms a ε-approximate t-design ensemble. The graph state we use is very similar to the brickwork state known to be a universal resource for MBQC [4]. The proofs presented here rely principally on the G-local random circuit construction (GLRC) of Brandao et al. [6], and the detectability lemma (DL) of Aharonov et al [118].

3.2 Preliminaries

3.2.1 Many Body Physics and t-designs

A well established technique for estimating the scaling rate (number of iterations needed to reach a desired accuracy ε) of an ε- approximate t-design can be reduced to a problem of finding the spectral gap (the difference of energy between the ground and first excited state) of some many-body Hamiltonian [6, 100, 98]. Here we give an overview of these techniques, in particular as used in [6]. This technique requires some conditions on the ensemble of unitaries, which we will reduce in Chapters 4 and 5. The results presented in this section are based on the work of [6].

An extensive body of research ([119, 120, 121, 122] and many others) has been devoted to the case of 1D spin chains, with local Hamiltonians (we assume a finite interaction range) with translational symmetry (see Figure3.1). We will focus exclusively on this case, and more precisely on a type of 1D Hamiltonian (the one we use in our proof) consisting of local terms acting on nearest neighbor spins i and i+1 with translational symmetry, which are frustration free (the entire Hamiltonian can be minimized by minimizing each of its local terms individually) as well as verifying the Nachtergaele criterion ([119], condition C.3). This family of Hamiltonians was used by Brandao et al. [6] to study their local random circuit (LRC) construction, and later the so-called G-local random circuits (GLRC). We will briefly define these families of circuits and review these proofs.

The local random circuits (LRC) in [6] generate random circuits on n-qubits as follows. For each run of the LRC, a unitary $U \in$ U(4) is chosen from the Haar measure on U(4), then an index i is chosen uniformly at random from the set {1,. . . ., n-1} , finally U is applied to qubits i and i+1. The LRC defines a couple $\{\mu_{LRC},\mathcal{U}\}$ where μ_{LRC} is the probability measure induced by one LRC run, and $\mathcal{U}$ is the set of all the possible unitaries which can be generated by one LRC run. We arrive at the following moment super operator associated to one run of the LRC

$$M_t[\mu_{LRC}] = \frac{1}{n-1}\sum_{i=1}^{n-1}\int_{U(4)} U_{i,i+1}^{\otimes t,t}\mu_H(dU) = \frac{1}{n-1}\sum_{i=1}^{n-1} P_{i,i+1}, \qquad (3.1)$$

where $U_{i,i+1}$=$1^{\otimes i-1}\otimes U\otimes 1^{\otimes n-i-1}$, $U \in$ U(4), $P_{i,i+1} := \int_{U(4)} U_{i,i+1}^{\otimes t,t}\mu_H(dU)$,

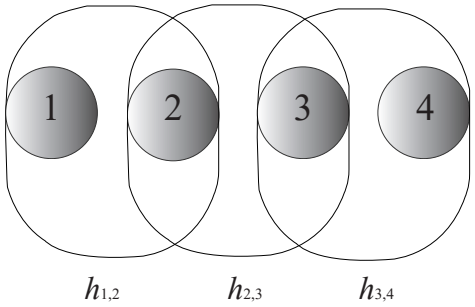

Figure 3.1: Example of a 4 spins 1D system. The local Hamiltonians $h_{i,i+1}$ have a range of 2 (i.e. act on nearest neighbor spins). For example $h_{1,2}$ acts on spins 1 and 2. Translational invariance means that any $h_{i,i+1}$ has the same form on all 2 qubit systems (i, i+1). In this case the total Hamiltonian of the system of 4 spins can be written as a sum of local Hamiltonians, i.e. H=$h_{1,2}$+$h_{2,3}$+$h_{3,4}$.

and μ_H is the Haar measure on U(4), 1 denotes the 2×2 identity matrix.

Since each of the $P_{i,i+1}$'s is Hermitian, then $M_t[\mu_{LRC}]$ is itself Hermitian. Now consider the Hamiltonian

$$H = \sum_i h_{i,i+1}, \tag{3.2}$$

where $h_{i,i+1}$=$I - P_{i,i+1}$, I is the $4^{nt} \times 4^{nt}$ identity matrix. Then

$$M_t[\mu_{LRC}] = I - \frac{H}{n-1}. \tag{3.3}$$

The ground space of H has an eigenvalue of 0 and the gap between its ground

and first excited spaces gives the second highest eigenvalue of $M_t[\mu_{LRC}]$. This H is a 1D spin chain Hamiltonian with nearest neighbor local terms which are translationally invariant. It is also frustration free by construction because the Hamiltonian can be minimized simply by minimizing all of its local terms (taking their ground state of energy 0) individually. Brandao et al. also proved that this Hamiltonian verifies the Nachtergaele criterion, then also bounded the Nachtergaele Bound using techniques from [123]. In this way they show that the spectral gap ΔH of H admits the following (polynomial in t) bound for $n \geq \lfloor 2.5 log_2(4t) \rfloor$:

$$\Delta H \geq (1700. \lfloor log_2(4t) \rfloor^2 . t^5 . t^{\frac{3.1}{log(2)}})^{-1}, \tag{3.4}$$

where $\lfloor x \rfloor$ denotes the floor function acting on variable x.

We now move to G-local random circuits, which are the finite set counter parts of LRC [6]. One run of the GLRC follows exactly as the LRC case, but instead of choosing a unitary U from the Haar measure of U(4), we choose with uniform probability from a finite set G of SU(4) which is universal and contains inverses. One can show from the beautiful result of Bourgain and Gamburd [122] that the Hamiltonian $H_{GLRC}=\sum_i h'_{i,i+1}=\sum_i (I-P'_{i,i+1})$ with $P'_{i,i+1} = \frac{1}{|G|} \sum_{U \in G} (1^{\otimes i-1} \otimes U \otimes 1^{\otimes n-i-1})^{\otimes t,t}$ admits the following bound for its spectral gap:

$$\Delta H_{GLRC} \geq \alpha . \Delta H, \tag{3.5}$$

with α a constant and ΔH the spectral gap of the LRC Hamiltonian.

Note that because the set G contains unitaries and their inverses and samples them uniformly, then $\mu_G(U)=\mu_G\ (U^\dagger)$, for all U, $U^\dagger \in$ G. This

means that $P'_{i,i+1}$ (hence H_{GLRC}) is a Hermitian operator, and the above definition of a GLRC Hamiltonian makes sense. We will see in Chapters 4 and 5 how the restrictions on the unitary ensembles and the Hermiticity of the moment superoperators discussed in this section can be circumvented, but in this chapter, we will construct examples which satisfy these properties. We can rewrite Equation (3.5) as follows:

$$\Delta H_{GLRC} \geq (C.\lfloor log_2(4t) \rfloor^2.t^5.t^{\frac{3.1}{log(2)}})^{-1} = P_{GLRC}, \tag{3.6}$$

C being a constant depending on the gate set G.

These spectral gaps directly give the second highest eigenvalue of the corresponding moment super operators (LHS in Equation (2.21), see [100]) confirming the TPE conditions, which through Proposition 2 then allow statements about their efficiency as t-designs [6].

In the coming parts of this chapter, we will construct a random unitary ensemble satisfying the conditions of a GLRC construction [6], and we will use this ensemble in a non-adaptive MBQC formed by concatenating a fixed MB scheme a polynomial (in n and t) number of times, and which we will show gives rise to an approximate t-design. The circuit analogue of this MBQC construction, which is discussed in detail in Section 4.3 in Corollary 2, is new and–unlike the constructions in [6]– does not require any classical randomness in the choice of nearest neighbor pair (see Chapter 4 for details). We will also, in Chapters 4 and 5, show how to use our developped circuit construction (and its MBQC analogue) on unitary ensembles not verifying the conditions of the GLRC construction.

3.3 Main Results

In order to state the main results, we define some simple graph states for two input qubits. We will hence forth refer to a graph state with an MB scheme applied to it as a gadget. These will act as the building blocks for our construction. Consider the 5-column 2-row brickwork states with a fixed angle MB scheme in Figure 3.2 and Figure 3.3 which we call S_{I_1} and S_{I_2} (Note, the numbers inside the circles denote the measurement angles. See Figure 2.1 for conventions of graph states and measurement in figures).

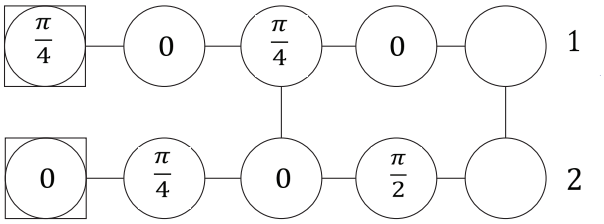

Figure 3.2: The 2-row, 5-column brickwork state gadget giving rise to S_{I_1}

S_{I_1} and S_{I_2} give rise respectively to 2 random MB ensembles (see Definition 1) $\{\frac{1}{2^8}, U_{1_i}\}$ and $\{\frac{1}{2^8}, U_{2_i}\}$. The number of unitaries generated by the MB scheme on the 2-row, 5-column brickwork state is 2^8.

It can be easily checked [5] that each unitary of the ensembles S_{I_1} and S_{I_2} contains (up to a global phase) an inverse in the ensemble. That is,

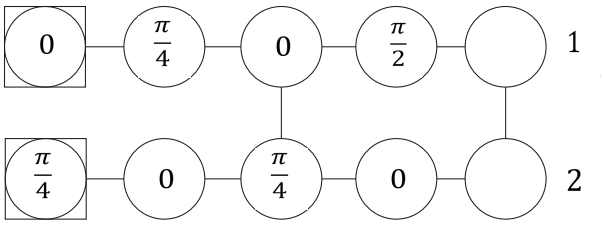

Figure 3.3: The 2-row, 5-column brickwork state gadget giving rise to S_{I_2}

denoting $\mathcal{U}_{S_{I_1}}$ as the set of unitaries generated by S_{I_1} (and similarly for S_{I_2}), for all $U_{1_i} \in \mathcal{U}_{S_{I_1}}$ there exists $U_{1_j} \in \mathcal{U}_{S_{I_1}}$ such that $U_{1_i} = U_{1_j}^{\dagger}$. Simlarly for S_{I_2}.

Consider now a 13-column brickwork gadget: B= $S_{I_1} \circ S_{I_2} \circ S_{I_1}$, where we mean by W $\circ$ V a concatenation which identifies the output of graph W as an input of graph V. We are now in a position to state our main results:

Theorem 1. *The gadget B gives rise to an ensemble of unitaries which is*
(i) universal on SU(4)
(ii) contains elements and their inverses, and
(iii) is sampled with uniform probability.

This theorem means that the set of unitaries generated by B (call it $\mathcal{U}_B$) satisfies the conditions necessary to form a GLRC. Though this is not exactly how our construction works, it will be important in proving our construction works in the proof of Theorem 2.

Now consider the gadget on n-qubits given in Figure3.4 which we call G_n. The horizontal line with a circle in the middle means a direct link between output and input performed only on the 1st and last rows. The square with the letter B is our 13-column brickwork gadget B, and the empty 3 sided square means that there is no vertical entanglement.

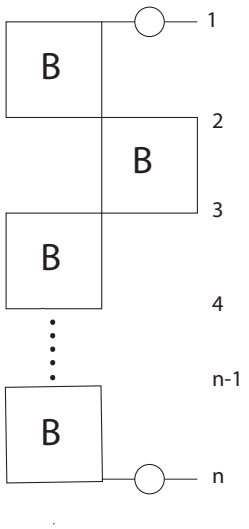

Figure 3.4: The graph gadget G_n pictured here for even n (the odd n case follows straightforwardly)

The first and last rows of G_n are made up of 13 qubits, and all rows in between are made up of 25 qubits. This gives rise in total to a graph composed of 26+25(n−2) = 25n−24 qubits. We now state our second main result.

Theorem 2. *The k(n,t,ε)-fold concatenation of G_n,*
$E_n = G_n \circ G_n \circ \ldots$, results in an ensemble of unitaries which forms an ε-approximate t-design on n-qubits ($n \geq \lfloor 2.5 log_2(4t) \rfloor$), with:
k(n,t,ε) $\geq \dfrac{3}{log_2(1 + \dfrac{P_{GLRC}}{2})}(4nt + log_2(\dfrac{1}{\varepsilon}))$.

3.4 Proofs

3.4.1 Proof of Theorem 1

Before going on to universality, let us briefly explain why the set of unitaries generated by B, $\mathcal{U}_B$ contains inverses ((ii) in Theorem 1). Any element $U \in \mathcal{U}_B$ may be written as: $U{=}U_1.U_2.U_1^{'}$, where U_1 , $U_1^{'} \in \mathcal{U}_{S_{I_1}}$ and $U_2 \in \mathcal{U}_{S_{I_2}}$. Since $\mathcal{U}_{S_{I_1}}$ and $\mathcal{U}_{S_{I_2}}$ contain unitaries and their inverses, we can always find $U^{\dagger}{=}U_1^{'\dagger}.U_2^{\dagger}.U_1^{\dagger} \in \mathcal{U}_B$. Furthermore, each unitary $U_{\{m\}} \in \mathcal{U}_B$ associated to a specific binary string $\{m\}$ is sampled with a uniform probability of $\dfrac{1}{|\mathcal{U}_B|}$, proving (iii) in Theorem 1.

The remainder of this subsection is devoted to proving universality ((i) in Theorem 1), and we will use the approach outlined in [124, 125] for doing so. Following [124, 125], one can show that the group generated by the

set of unitaries $\{A,A^\dagger,C,C^\dagger,E,E^\dagger,F,F^\dagger\}$ is dense (universal) on U(4) if the following conditions are satisfied:

C_1 : $H_1{:=}\frac{log(A)}{i}$, $H_2{:=}\frac{log(C)}{i}$, $H_3{:=}\frac{log(E)}{i}$ and $H_4{:=}\frac{log(F)}{i}$ and their commutators contain a set of 16 linearly independent Hamiltonians which span the Lie algebra [126] of U(4).

C_2 : H_1, H_2, H_3 and H_4 have eigenvalues that are irrationally related to π.

We first consider C_1. We found 4 distinct unitaries $A{=}U_{\{m\}}$, $C{=}U_{\{m'\}}$, $E{=}U_{\{m''\}}$, and $F{=}U_{\{m'''\}}$, where $U_{\{m\}}$, $U_{\{m'\}}$, $U_{\{m''\}}$ and $U_{\{m'''\}} \in \mathcal{U}_B$ are associated to the binary strings $\{m\}$=\{0,1,1,0,1,1,1,0,0,1,1,0,0,0,0,0,0,1,1,0,1,1,1,0\},
$\{m^{'}\}$=\{0,0,0,1,1,1,1,0,1,0,1,0,1,1,1,1,0,1,1,1,0,1,0,0\},
$\{m^{''}\}$=\{0,0,0,1,1,1,1,0,1,0,1,0,1,1,1,1,0,1,1,1,0,1,0,0\}, and
$\{m^{'''}\}$=\{0,1,1,1,0,1,1,0,0,0,0,1,0,0,0,1,0,0,1,0,0,0,1,0\}.
We adopt the convention that the first 12 binary numbers appearing in a given binary string represent the measurement results on qubits of the first row of B from left to right (input towards output), and the last 12 binaries represent the measurements performed on the qubits of the second row of B from left to right.

We then construct 16 Hamiltonians H_1 ,..., H_{16} as follows

$$H_1 = \frac{log(A)}{i},$$
$$H_2 = \frac{log(C)}{i},$$

$$H_3 = \frac{log(E)}{i},$$
$$H_4 = \frac{log(F)}{i},$$
$$H_5 = i.[H_1, H_2],$$
$$H_6 = i.[H_1, H_3],$$
$$H_7 = i.[H_1, H_4],$$
$$H_8 = i.[H_2, H_3],$$
$$H_9 = i.[H_2, H_4],$$
$$H_{10} = i.[H_2, H_5],$$
$$H_{11} = i.[H_2, H_6],$$
$$H_{12} = i.[H_3, H_4],$$
$$H_{13} = i.[H_3, H_5],$$
$$H_{14} = i.[H_3, H_6],$$
$$H_{15} = i.[H_4, H_5],$$
$$H_{16} = i.[H_4, H_6].$$

After that, we expand each of the 16 Hamiltonians in the basis: P=$\{P_{ij}\}$ i,j=0,..,3, where P is a basis of the Lie algebra of U(4). In other words, we write each: H_k=$a_k^{ij}.(P_{ij})$ (Einstein summation convention adopted over i and j), where the a_k^{ij} ' s are real numbers. Since P is a basis of the Lie algebra of U(4) (over the field of real numbers), proving linear independence of the 16 Hamiltonians $\{H_k\}$ k=1,..16 in the basis P means that the set $\{H_k\}$ is itself a basis of the Lie algebra of U(4). The linear independence of the 16 generators $\{H_k\}$ is equivalent to the non-vanishing of the determinant of a 16 by 16 matrix M, where each of the 16 columns of M are made up of the

16 coefficients$\{a_k^{ij}\}$ for a given k. We found that the 16 Hamiltonians of our above constructed scheme give rise to a matrix M with non-vanishing determinant [1], thus this scheme forms a basis of the Lie algebra of U(4) and C_1 is verified for a subset of $\mathcal{U}_B$ (and hence for $\mathcal{U}_B$ itself).

Proving C_2 requires the use of a result in algebraic number theory called Lehmer's theorem [127]. Its context is described in the following lemma:

Lemma 1. *[127] If $n > 2$ and k and n are coprime integers, then $2cos(\frac{2k\pi}{n})$ is an algebraic integer.*

An algebraic number is a complex number which is a solution of a polynomial equation with integer coefficients. The minimal polynomial of an algebraic number z is the polynomial of lowest degree with integer coefficients for which z is a solution. An algebraic integer is an algebraic number whose minimal polynomial is monic (that is, the coefficient in front of the highest degree variable is 1) [127].

Lehmer's theorem states that angles $\alpha = \frac{2k\pi}{n}$ which are rationally related to π must have $2cos(\alpha)$ an algebraic integer. So, if we can find instances of angles α in which $2cos(\alpha)$ is not an algebraic integer, then α has to be irrationally related to π as a consequence of Lehmer's theorem. Each of the eigenvalues λ of A, C, E or F is a complex number with unit norm (because they are unitary matrices). Thus, λ=$e^{i\theta}$. We calculated the expression $2cos(\theta)$ and constructed its minimal polynomial. We found that for each of the eigenvalues λ of A , C, E and F, $2cos(\theta)$ does not verify a monic minimal polynomial (not an algebraic integer) and thus all the θ's

[1] this was done numerically however well within numerical precision

are irrationally related to π by Lehmer's theorem. Further, because A, C, E and F are diagonal in the same basis as their Hamiltonians H_1, H_2, H_3 and H_4 [125], the θ's we calculated are the eigenvalues of these Hamiltonians. Hence, the eigenvalues of the Hamiltonians are irrationally related to π which proves C_2.

Proving C_1 and C_2 means that the subset $\{A,A^\dagger,C,C^\dagger,E,E^\dagger,F,F^\dagger\}$ of $\mathcal{U}_B$ is universal on U(4), and thus so is $\mathcal{U}_B$. But (i) further requires that the set be on SU(4). Fortunately, the moment super operator of a set sampled from U(4) can always be thought of as a sampling from SU(4). This can be seen by noting that for all $U \in$ U(4) we have $det(U) \neq 0$, hence $U^{\otimes t,t}=|det(U)|^{\frac{t}{2}}.U'^{\otimes t,t}=U'^{\otimes t,t}$, where $U' \in$ SU(4).

3.4.2 Proof of Theorem 2

Our approach for proving Theorem 2 can be summarized by two steps. In the first step, we prove that the ensemble generated by the gadget G_n is an (η,t)-TPE with $\eta = poly(t) < 1$ (see Definition 5). We do so by using Aharonov et al.'s detectability lemma [118]. The second step uses Proposition 2 (see Section 2.4) to establish the bound on $k(n,t,\varepsilon)$.

Consider a GLRC n-qubit Hamiltonian

$$\begin{aligned} H_{GLRC} &= \sum_i h'_{i,i+1} \\ &= \sum_i (1 - P'_{i,i+1}), \end{aligned} \tag{3.7}$$

with G $= \mathcal{U}_B$, and

$P'_{i,i+1}=\frac{1}{|\mathcal{U}_B|}\sum_{U\in\mathcal{U}_B}(1^{\otimes i-1}\otimes U\otimes 1^{\otimes n-i-1})^{\otimes t,t}$. Define $P_{odd}=P'_{1,2}.P'_{3,4}\ldots$ and $P_{even}=P'_{2,3}.P'_{4,5}\ldots.P_{odd}$ and P_{even} can be considered as projectors onto the "odd" and "even" ground spaces of H_{GLRC}. Let P_0 be the projector onto the entire ground space of H_{GLRC}. Further, because H_{GLRC} is constructed from universal sets on U(4), then its ground space projector is nothing but the t'th Haar moment super operator [100], In other words $P_0=\int_{U(2^n)}U^{\otimes t,t}\mu_H(dU)$; $U\in \mathrm{U}(2^n)$ and μ_H being the Haar measure on $\mathrm{U}(2^n)$.

The statement of the detectability lemma is the following :

Lemma 2. [6]

$$|| P_{even}.P_{odd}-P_0 ||_\infty \leq (1+\frac{\Delta H_{GLRC}}{2})^{-\frac{1}{3}}. \tag{3.8}$$

To relate this to the ensemble generated by the gadget G_n we prove the following lemma:

Lemma 3.

$$M_t[\mu_{G_n}]=P_{even}.P_{odd}. \tag{3.9}$$

Proof of Lemma 3 : We first note that because all unitaries are drawn independently, we can think of the moment super operator as being composed of 2 layers (an odd layer (left part of the gadget of Figure3.4) and an even layer (right part of the gadget of Figure3.4), this is similar to reasoning found in [101]). Then:

$$M_t[\mu_{G_n}]=(\frac{1}{|\mathcal{U}_B|})^{\delta_{even}}\sum_{U_{23}\in\mathcal{U}_B,U_{45}\in\mathcal{U}_B,\ldots}(U_{23}\otimes U_{45}\otimes\ldots)^{\otimes t,t}.$$

$(\frac{1}{|\mathcal{U}_B|})^{\delta_{odd}} \sum_{U_{12}\in\mathcal{U}_B, U_{34}\in\mathcal{U}_B,\ldots}(U_{12}\otimes U_{34}\otimes\ldots)^{\otimes t,t}$,

where δ_{odd}={ $\frac{n}{2}$ if n *mod* 2=0 or $\frac{n-1}{2}$ if n *mod* 2 =1 }
and δ_{even}={ $\frac{n}{2}-1$ if n *mod* 2=0 or $\frac{n-1}{2}$ if n *mod* 2=1 }.

Note that since the U_{ii+1} ' s are independently drawn from $\mathcal{U}_B$, one can rewrite this as:

$M_t[\mu_{G_n}]$= $(\frac{1}{|\mathcal{U}_B|}\sum_{U_{23}\in\mathcal{U}_B}(1\otimes U_{23}\otimes 1^{\otimes n-3})^{\otimes t,t}$.
$\frac{1}{|\mathcal{U}_B|}(\sum_{U_{45}\in\mathcal{U}_B}(1^{\otimes 3}\otimes U_{45}\otimes 1^{\otimes n-5})^{\otimes t,t}...)$.
$(\frac{1}{|\mathcal{U}_B|}(\sum_{U_{12}\in\mathcal{U}_B}(U_{12}\otimes 1^{\otimes n-2})^{\otimes t,t}$.
$\frac{1}{|\mathcal{U}_B|}\sum_{U_{34}\in\mathcal{U}_B}(1^{\otimes 2}\otimes U_{34}\otimes 1^{\otimes n-4})^{\otimes t,t}...)$
$=(P'_{2,3}.P'_{4,5}...).(P'_{1,2}.P'_{3,4}...)$
$=P_{even}.\ P_{odd}.$ □

Then, as a direct consequence of the detectability lemma we obtain:

$$g(t,\mu_{G_n}) =|| M_t[\mu_{G_n}] - P_0 ||_\infty \leq (1+\frac{\Delta H_{GLRC}}{2})^{-\frac{1}{3}}. \tag{3.10}$$

All that remains now is to bound the RHS of Equation (3.10). Using Equation (3.6) one directly obtains:

$$(1+\frac{\Delta H_{GLRC}}{2})^{-\frac{1}{3}} \leq (1+\frac{P_{GLRC}}{2})^{-\frac{1}{3}}. \tag{3.11}$$

Equation (3.10) along with Equation (3.11) directly leads to the following

corollary:

Corollary 1. *The ensemble* $\{\frac{1}{|\mathcal{U}_\mathcal{G}|}, \mathcal{U}_\mathcal{G}\}$ *generated by the gadget* G_n *is an* (η,t)*-TPE with :*
$\eta = (1 + \frac{P_{GLRC}}{2})^{-\frac{1}{3}} = poly(t) < 1.$

Plugging Corollary 1 into Proposition 2 with:
$\{ p_i, U_i \} = \{\frac{1}{|\mathcal{U}_\mathcal{G}|}, \mathcal{U}_\mathcal{G}\}$, $d = 2^n$ and $\eta = (1 + \frac{P_{GLRC}}{2})^{-\frac{1}{3}}$ allows one to obtain Theorem 2.

3.5 Conclusion

In this chapter, have found a simple n-qubit graph gadget which implements an ε-approximate t-design under repeated concatenations with fixed measurement and no feedforward. The number of concatenations $k(n, t, \varepsilon) = \Omega(nt + log(\frac{1}{\varepsilon}))$ required is linear in both the input qubit number n, and order t of the design. The n dependence of the number of concatenations is optimal, whereas one can suspect the t dependance can be improved, even to get a number of concatenations independant of t [6]. Because the number of qubits in the graph gadget scales linearly with n, we thus only require $\Omega(n^2 t + nlog(\frac{1}{\varepsilon}))$ qubits in total to implement the gadget $E_n = G_n \circ G_n \circ ....$ Furthermore, the choice of the 2-qubit gadget B is not at all unique. In fact, G_n could be made even more practical provided simpler (less number of qubits, less needed entanglements,...) 2-qubit gadgets possessing the properties of B can be found. Indeed, we do not claim our construction of B to be optimal, mainly because 3 CZ's (as opposed to 6 CZ's in our gadget

B) are sufficient to realize any unitary in SU(4). Furthermore, in the next chapter we will show different examples of gadgets which work, but require different proof techniques.

Our construction is very similar to the brickwork state, which is a universal resource for MBQC [4] - it is basically the brickwork state but with regular holes. In MBQC these holes would simply teleport the inputs through, so that the proofs of universality of [4] easily extend to our graph - that is, concatenations of the graph used in G_n is also a universal resource for MBQC. In addition to being pleasing from a practical point of view, this opens the door to applications of techniques for delegation of ensemble generation, as done for computation [4, 128], and indeed the possibility to hide whether one is sampling unitaries or performing some deterministic computation.

Chapter 4

Efficient Approximate Unitary t-designs From Partially Invertible Universal Sets and Their Application to Quantum Speedup

4.1 Introduction

In this chapter, we construct new families of quantum circuits on n-qubits giving rise to ε-approximate unitary t-designs efficiently in $O(n^3t^{12})$ depth. These quantum circuits are based on a relaxation of technical requirements in previous constructions, including that of Chapter 3. In particular, the

construction of circuits which give efficient approximate t-designs by Brandao, Harrow and Horodecki [6] (and our construction in Chapter 3, and other constructions following their technique [5, 36]) required choosing gates from ensembles which contained inverses for all elements, and that the entries of the unitaries are algebraic. In this chapter, we reduce these requirements to sets that contain elements without inverses in the set, and non-algebraic entries, which we dub *partially invertible universal* sets.

We then adapt this circuit construction to the framework of measurement based quantum computation (MBQC) and give new explicit examples of n-qubit graph states with fixed assignments of measurements (graph gadgets) giving rise to unitary t-designs based on partially invertible universal sets, in a natural way. Our work opens up the set of graph states where we can demonstrate t-designs to more graphs, of which we give an example in Figure 4.4.

We further show that these graph gadgets demonstrate a quantum speedup, up to standard complexity theoretic conjectures. The proofs of quantum speedup presented here can also be directly applied to show that our brickwork construction in Chapter 3 also demonstrates a quantum speedup.

We provide numerical and analytical evidence that almost any assignment of fixed measurement angles on an n-qubit cluster state give efficient t-designs and demonstrate a quantum speedup. Therefore, our techniques developped here show the potential of cluster states, which are widely used resources in many applications, to form t-designs and demonstrate a quantum speedup.

4.2 Overview of Chapter

The prevalent technique for generating a t-design is through random circuits, where gates are randomly chosen from some ensemble of small, typically two qubit gates, and put together in a specific way to form a circuit [98, 6, 24, 5, 36, 100]. Though essentially any universal set of two qubit gates can be used to generate this ensemble, the precise conditions on this ensemble are somewhat strict (due to technical reasons in the proofs, see for example Chapter 3) - they require that each gate has an inverse in the ensemble and that their entries are algebraic. The former condition is also imposed on universal ensembles when proving the Solovay Kiteav theorem for efficient approximate universality [129]. Though usually this is not an issue, it can be, particularly when these sets of unitaries are generated in a restricted manner - for example arising from measurements on graph states [5, 36, 26, 25] (see Section 2.3 of Chapter 2 for a definition of graph states, and the pictoral conventions used in their use for our schemes.).

Our work connects these different questions and approaches, first by proving a general relaxation of the conditions on a set of ensembles used to generate a t-design, leading to new constructions for circuits, which we then translate to the graph state, measurement based approach. We then give explicit examples where the relaxation to partially invertible sets is useful in graph state constructions. Following along the lines of [26, 25] we then show that these examples give rise to natural instances of provably hard sampling problems demonstrating quantum speedup.

We now give a bit more background into the three areas of our main

results.

4.2.1 t-designs in Partially Invertible Universal Sets

Exact t-designs, where the condition on the tth order moments are satisfied exactly, are only known for a few cases [29, 99, 5, 103] (as seen in Chapter 2). We are thus often interested in approximate versions, where conditions hold up to some error ε - we call these ε-approximate t-designs [98, 6, 24, 5, 36, 100, 101]. We say a circuit construction is efficient if the size of the circuit, k does not scale exponentially in n, t or $1/\varepsilon$. Previous work showed that random n-qubit quantum circuits formed of k applications of 2-qubit gates form efficient ε-approximate t-designs with $k = poly(n, t, log(\frac{1}{\varepsilon}))$ [98, 6], where these 2-qubit gates are chosen from the Haar measure on $U(4)$ [6, 98], or uniformly randomly from a universal [1] set $\mathcal{U}_{\mathcal{B}} \subset U(4)$ which contains unitaries and their inverses [2], and is made up of unitaries with algebraic entries [6] (as seen in Chapters 2 and 3).

The first question we ask here is whether the restriction that $\mathcal{U}_{\mathcal{B}}$ contains unitaries and their inverses can be avoided. Such a possibility opens up different possible constructions, which are notably important considering measurement based approaches, where one does not easily have full control over the whole ensemble. The answer to this question, as we will show, turns out to be positive, provided (I): we can find sets $\mathcal{U}_{\mathcal{B}}$ containing a subset $\mathcal{U}_{\mathcal{M}} \subset \mathcal{U}_{\mathcal{B}}$ formed of unitaries with algebraic entries [6], such that $\mathcal{U}_{\mathcal{M}}$ contains unitaries and their inverses, and (II) both $\mathcal{U}_{\mathcal{M}}$ and its complement

[1] A set $\mathcal{U} \subset U(N)$ is said to be universal in $U(N)$, when the group generated by $\mathcal{U}$ is dense in $U(N)$.

[2] We mean by this that for every $U \in \mathcal{U}_{\mathcal{B}}$, there exists $U_1 \in \mathcal{U}_{\mathcal{B}}$, such that $U_1 = U^{\dagger}$.

in $\mathcal{U}_{\mathcal{B}}$ - denoted by $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ - which need not nescessarily contain unitaries and their inverses nor have algebraic entries are universal in $U(4)$. For simplicity, we refer to sets $\mathcal{U}_{\mathcal{B}}$ verifying (I) and (II) as *partially invertible universal sets*. Thus, a partially invertible universal set can be defined as follows.

Definition 7. *A partially invertible universal set $\mathcal{U}_{\mathcal{B}} \subset U(4)$ is a (universal in $U(4)$) set which can be partitioned into two sets, $\mathcal{U}_{\mathcal{M}} \subset \mathcal{U}_{\mathcal{B}}$ which contains unitaries and their inverses and is composed of unitaries with algebraic entries, and its complement $\mathcal{U}_{\mathcal{B}/\mathcal{M}} \subset \mathcal{U}_{\mathcal{B}}$ which need not nessesarily contain unitaries and their inverses nor be composed of unitaries with algebraic entries. Both $\mathcal{U}_{\mathcal{M}}$ and $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ are universal in $U(4)$.*

Based on this we derive a construction of n-qubit quantum circuits formed of blocks of 2-qubit unitaries chosen uniformly from *any* partially invertible universal set in $U(4)$, and show that these circuits are efficient ε-approximate t-designs in depth $O(n^3 t^{12})$. In our proofs, we use technical tools such as the Detectibility lemma [118], and techniques from [98, 6].

We then adapt this circuit construction to MBQC [30, 85], where partially invertible universal sets arise quite naturally, since it is not possible to choose freely all the unitaries in this ensemble. As discussed in Chapter 2, in MBQC, measuring the non-output qubits of an n-qubit graph state at particular angles in the XY, XZ, or YZ planes of the Bloch sphere, and performing a corrective strategy, for example given by the g-flow [86], is sufficient to implement any unitary $U \in U(2^n)$ on the n unmeasured output qubits. On the other hand, and as seen in Chapter 2 and 3, performing

non-adaptive [3] measurements on graph states effectively implements on the (unmeasured) output qubits unitaries sampled uniformly from an ensemble of random unitaries [5, 36].

Here, we find examples of small graph states along with measurement angles which generate ensembles of random unitaries which are partially invertible universal sets. This means that the proof techniques of [6], and of the previous chapter do not work. Nevertheless, with our new proof technique developed in this chapter, we see that by concatenating this seed construction in a specific way we generate ensembles from non-adaptive fixed measurements on regular graph states with $O(n^4t^{12})$ qubits which form an ε-approximate t-design on $U(2^n)$.

Translated into the circuit model, these MBQC circuits have constant depth, albeit with a $O(n^4t^{12})$ number of ancilla qubits. This observation could be very beneficial from the point of view of experimental implementation.

4.2.2 Connection to Quantum Speedup

There is currently a tremendous effort being made to build a quantum computer, and develop quantum technologies more generally. An important benchmark for this ambitious project will be proving a computational advantage over what can be done with classical computers. Two results in this direction have sparked a surge in research. Boson sampling [130, 62] and IQP [3] are subuniversal families of computation which can be shown to be impos-

[3] Non-adaptive means, as seen in Chapter 2, with no corrective strategy, non-adaptive measurements can be performed simultaneously.

sible to replicate efficiently classically assuming some standard, and strongly believed, complexity theoretic conjectures hold. This is often referred to as quantum speedup. Since then, there have been many developments of these and related models [25, 26, 38, 27, 3, 33, 114, 66, 130, 62, 131, 116] to state a few. A review can be found in [115]. In all of these cases two features are significant. Firstly, they do not require the full capabilities of a universal quantum computer and so are expected to be much simpler to implement, and second they are all what is known as sampling problems. That is, the statements of difficulty are that a classical computer cannot efficiently sample from the same distribution as what can be achieved in these quantum architectures efficiently.

More concretely, the statements run somewhat as follows (see also Section 2.5). Each of these computational models is essentially a family of circuits followed by measurements, the results of which follow a particular probability distribution. If it is possible for a classical computer to efficiently sample from this distribution, then, certain strongly believed complexity conjectures would be proved invalid. For proofs which hold for approximate sampling, the standard conjectures are of the form [25, 26, 38, 33, 114, 27, 3]
I) the polynomial hierarchy does not collapse to the third level [132].
II) the average case of the associated problem (usually $\sharp$P) is also hard ($\sharp$P).
III) the quantum circuit families considered output distributions which are not too peaked - technically known as anti-concentration [116, 26, 33, 114, 27].

One of the goals of the field now is to reduce the number of required assumed conjectures, or justify them, and understand their relationship to

other properties of a given architecture such as universality. There are many architectures demonstrating quantum speedup, suited to different implementations with different versions of the conjectures which link them in different ways to different problems. The average case complexity can be linked to conjectures of average case hardness of solving certain Ising problems [66], or of Jones polynomials [27] for example. For several architectures anticoncentration can be proven explicitly [26, 27]. The work of [26, 24, 27] shows an interesting link between t-designs and anticoncentration.

In this work, and as an application to our t-design graph gadgets, we use techniques from [26, 25] and introduce new families of MBQC architectures showing a quantum speedup. We show that *every* MBQC 2-design constructed from partially invertible universal sets is hard to sample from classically, and we give a new explicit example that can be prepared efficiently using n-qubit cluster states with $O(n^3)$ columns - thereby presenting a quantum speedup. Because our architectures are t-designs by construction, Conjecture (III) is proven [26, 27], thus we only require 2 complexity theoretic conjectures in our proofs (namely, Conjectures I) and II)). Also, because our gadgets have quite a regular structure, they can be translated into a constant depth quantum circuits as seen above. This makes these architectures desirable for near-term experimental implementation.

4.2.3 Families of Universal Ensembles

In the final part of this work we explore how common universal ensembles are in the measurement based framework, and how they can be used for t-designs. We present two results in this direction, one analytical and the

other numerical.

Analytically, we show that *almost any* [4] assignment of fixed XY angle measurements on a $n = 2^\gamma$-row, 2-column cluster state (where γ is an integer) gives a random unitary set $\mathcal{U}_\mathcal{B}$ which is universal in $U(2^n)$. We use a Lie algebraic approach outlined by [58], and observations in [124, 125] to prove this result. In particular, when $\gamma = 1$ we get that almost any assignment of fixed XY angle measurements generates universal sets $\mathcal{U}_\mathcal{B} \subset U(4)$, which in general can be invertible, partially invertible or non invertible.

We then provide numerical evidence that for almost any fixed assignment of XY measurements, the subdominant eigenvalue of the operator $M_t[\mu] = \frac{1}{|\mathcal{U}_\mathcal{B}|} \sum_{i=1,\ldots|\mathcal{U}_\mathcal{B}|} U_i^{\otimes t} \otimes U_i^{*\otimes t}$ scales efficiently with t. [5] If the numerical result is true, then together with the analytical result on universality, one can show from our techniques developed for the partially invertible case, that cluster state gadgets with almost any fixed XY angle assignment give an efficient n-qubit t-design under concatenation. Further, the results imply that these gadgets are also hard to sample from classically under concatenation, and thus these gadgets may also be used as architectures presenting a quantum speedup.

In the previous chapter, a particular set of fixed non-adaptive measurements on a brickwork state gave rise to an ensemble which is an approximate t-design, and which demonstrates a quantum speedup. This chapter goes significantly beyond this result in two ways. First, by showing that graph states other than the brickwork state, such as the graph state in Figure 4.4

[4] Meaning that the set of angles which don't work form a set having zero Lebesgue measure [133].

[5] $U_i \in \mathcal{U}_\mathcal{B}$. $M_t[\mu]$ is usually called the moment superoperator.

and the cluster state, can also give rise to t-designs and demonstrate quantum speedup under fixed non-adaptive measurements. Second, it shows that the choice of fixed measurements can be varied widely, with almost any choice working (see the next section for more details).

4.3 Main Results

Let $\mathcal{U}_{\mathcal{B}} \subset U(4)$ be *any* partially invertible universal set in $U(4)$ (see Definition 7). Let $\mathcal{U}_{\mathcal{M}} \subset \mathcal{U}_{\mathcal{B}}$, with $\mathcal{U}_{\mathcal{M}}$ containing unitaries and their inverses and with unitaries composed of algebraic entries, and its complement $\mathcal{U}_{\mathcal{B}/\mathcal{M}} \subset \mathcal{U}_{\mathcal{B}}$ such that $\mathcal{U}_{\mathcal{M}}$ and $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ are both universal in $U(4)$. Define

$$B = \{\frac{1}{|\mathcal{U}_{\mathcal{B}}|}, U_i \in \mathcal{U}_{\mathcal{B}}\}. \tag{4.1}$$

Denote the k-fold concatenation of B by

$$B^k = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|}, \prod_{j=1,...k} U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}^k}\}, \tag{4.2}$$

where $U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}}$, and π is a function defined as in Proposition 2. Define [6]

$$block(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}}, (1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes U_{4,5}^{j_2} \otimes ... \otimes U_{n-2,n-1}^{j_{\frac{n}{2}-1}} \otimes 1_{2\times 2}).$$
$$(U_{1,2}^{j_{\frac{n}{2}}} \otimes U_{3,4}^{j_{\frac{n}{2}+1}} \otimes ... \otimes U_{n-1,n}^{j_{n-1}}) \in \mathcal{U}_{block(\mathcal{B}^k)}\}, \tag{4.3}$$

[6] This definition of $block(B^k)$ is for even n , the odd n case follows straightforwardly.

where $U_{i,i+1}^{j} \in \mathcal{U}_{\mathcal{B}^k}$, $i \in \{1, ..., n-1\}$ and $j \in \{1, ..., |\mathcal{U}_{\mathcal{B}^k}|\}$. Let $block^L(B^k)$ be the L-fold concatenation of $block(B^k)$, defined as

$$block^L(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{(n-1)L}}, \prod_{j=1,...,L} U_{\pi(j)} \in \mathcal{U}_{block^L(\mathcal{B}^k)}\}, \tag{4.4}$$

where here also π is defined as in Proposition 2, and $U_{\pi(j)} \in \mathcal{U}_{block(\mathcal{B}^k)}$.

Finally, let $a = \frac{|\mathcal{U}_{\mathcal{M}}|}{|\mathcal{U}_{\mathcal{B}}|}$. Our first main result is the following theorem which holds for the above defined partially invertible universal set $\mathcal{U}_{\mathcal{B}}$:

Theorem 3. *For any $0 < \varepsilon_d < 1$, and for some $0 < C < 1$, if :*

$$k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(10t + n^2t - nt + n + log_2(\frac{1}{\varepsilon^{'}})), \tag{4.5}$$

and

$$L \geq \frac{1}{log_2(\frac{1}{\varepsilon^{'}+P(t)})}(4nt + log_2(\frac{1}{\varepsilon_d})), \tag{4.6}$$

where

$$P(t) = (1 + \frac{(425\lfloor log_2(4t)\rfloor^2 t^5 t^{3.1/log(2)})^{-1}}{2})^{-1/3}, \tag{4.7}$$

$\varepsilon^{'} < 1 - P(t)$, and $n \geq \lfloor 2.5 log_2(4t)\rfloor$, then $block^L(B^k)$, formed from partially invertible universal set $\mathcal{U}_{\mathcal{B}}$, is a ε_d- approximate t-design on $U(2^n)$, for any t, where ε_d is a positive real.

Here $\lfloor . \rfloor$ denotes the floor function. An Immediate corollary to the above theorem is the following less technical statement.

Corollary 2. *Let B be the random unitary ensemble formed by chosing uniformly at random from a partially invertible universal set. Random quantum*

circuits on n-input qubits of depth $D = 2.k.L = O(n^3t^{12})$ [7] *and described as follows (for n even, odd n case follows straightforwardly.)*

1. *For steps 1 to k (layer* $j = 1$*), apply unitaries of the form* $U_{1,2} \otimes U_{3,4} ... \otimes U_{n-1,n}$*, where the* $U_{i,i+1}$*'s are random unitaries sampled independently from the random unitary ensemble B, and acting non-trivially on input qubits i and i+1.*

2. *For steps* $k+1$ *to* $2k$ *(layer* $j = 2$*), apply unitaries of the form* $U_{2,3} \otimes U_{4,5} ... \otimes U_{n-2,n-1}$*, where the* $U_{i,i+1}$*'s are random unitaries sampled independently from the random unitary ensemble B, and acting non-trivially on input qubits i and i+1.*

3. *Repeat 1. for every odd numbered layer j formed of k steps, and repeat 2. for every even numbered layer j formed of k steps, for* $j = 3, ..., 2L$*.*

are ε_d*-approximate t-designs, for any t and for* $n \geq \lfloor 2.5 log_2(4t) \rfloor$*.*

As shown in Chapter 3, one can generate random ensembles in MBQC by connecting 2-qubit graph gadgets in a regular way. Given a graph gadget G_B, which gives an ensemble over a partially invertible universal set, we will see that Figures 4.1, 4.2 and 4.3 show how to compose copies of G_B to get the n-qubit cluster state gadget $LG_{block(B^k)}$ giving rise to the ensemble $block^L(B^k)$. In this way, we go beyond the results of the previous chapter (which uses the same $block(.)$ construction) in the sense that the underlying gadgets G_B may be chosen so as not to follow the conditions of the GLRC

[7] Note that, as in [6], $\frac{1}{log_2(\frac{1}{P(t)+\varepsilon'})} \sim O(t^{9.47} log^2(t)) < O(t^{10})$, as $t \to \infty$ and thus $k.L \sim O(t^{10}).O(n^3t^2) = O(n^3t^{12})$.

construction [6]. Indeed, we give explicit examples of such gadgets G_B below (see Figure 4.4). We also give numerical and analytical evidence that G_B can also be a cluster state gadget, with almost any fixed assignment of measurement angles (not nessesarily giving rise to a partially invertible universal set even) giving approximate t-designs and demonstrating a quantum speedup. Obtaining the k-fold concatenation B^k of the random unitary ensemble B translates in MBQC to constructing a graph state gadget kG_B which is formed of sticking together k copies of G_B. More precisely, if G_B is a cluster state gadget formed of m columns and 2-rows, then kG_B is a cluster state gadget formed of $k(m-1)+1$ columns and 2-rows, where the measurement angles are repeated after each block of m columns, see Figure 4.1. Then, connecting these kG_B gadgets in a brickwork like fashion gives rise to the $block(B^k)$. We call this the graph state gadget $G_{block(B^k)}$ and it is represented in Figure 4.2. Finally, taking L copies of these, concatenated after each other as in Figure 4.3 gives rise to a t-design, as is captured in the following corollary - which is a direct consequence of Theorem 3, and the graph state translation to MBQC.

Corollary 3. *If G_B is a 2-qubit graph state gadget giving rise to a random unitary ensemble B over a partially invertible universal set $\mathcal{U}_{\mathcal{B}}$, then, for any $0 < \varepsilon_d < 1$, and for some $0 < C < 1$, the graph state gadget $LG_{block(B^k)}$ applies to its unmeasured n output qubits a unitary sampled from a ε_d-approximate t-design on $U(2^n)$ when,*

$$k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(8t + (nt + 2t + n^2t - 2nt + n) + log_2(\frac{1}{\varepsilon'})),$$

$$L \geq \frac{1}{log_2(\frac{1}{\varepsilon'+P(t)})}(4nt + log_2(\frac{1}{\varepsilon_d})),$$

$\varepsilon^{'} < 1 - P(t)$, *and* $n \geq \lfloor 2.5log_2(4t) \rfloor$, *for any* t. [8]

The graph state gadget G_B in Figure 4.4 generates a random unitary ensemble where elements of a partially invertible universal set are selected uniformly at random. This is proven in Section 4.6.

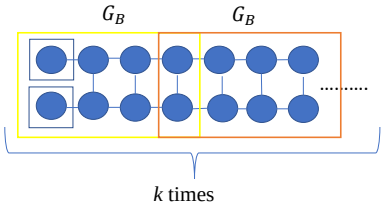

Figure 4.1: Graph state gadget kG_B giving rise to the random ensemble B^k.

[8] A particular choice of $\varepsilon^{'}$ can be $\varepsilon^{'} = a(1 - P(t))$, where $0 < a < 1$ is a constant independent of t.

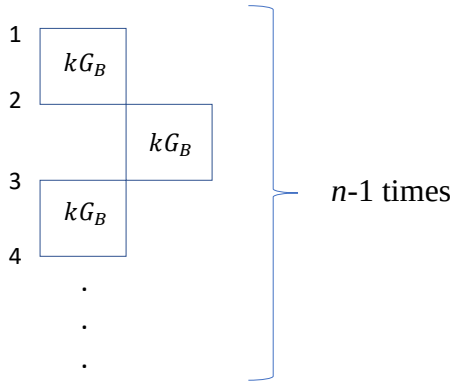

Figure 4.2: Graph state gadget $G_{block(B^k)}$ giving rise to the random ensemble $block(B^k)$. The squares are 2-qubit gadgets kG_B.The empty 3 sided square means that there is no vertical entanglement.

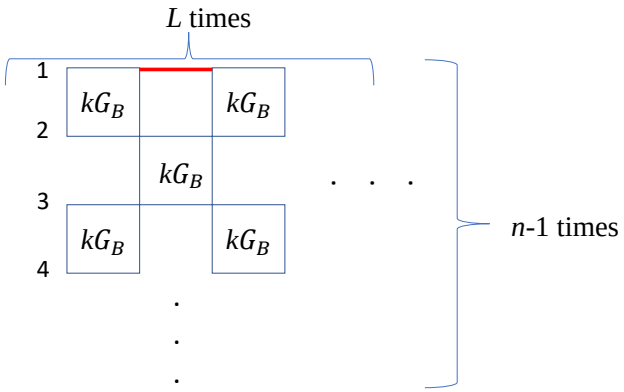

Figure 4.3: Graph state gadget $G_E := LG_{block(B^k)}$, giving rise to the ensemble $E = block^L(B^k)$. The horizontal red line is a preparation entanglement (see also Figure 3.4 in Chapter 3 where this horizontal red line is denoted as a horizontal line with a circle in the middle).

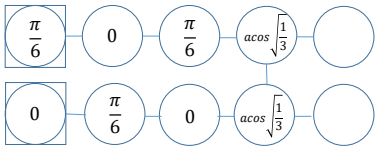

Figure 4.4: Graph state gadget G_B giving rise to a partially invertible universal set.

Our next main result concerns sampling problems and quantum speedup using graph state gadgets $LG_{block(B^k)}$, Figure 4.3. For ease of notation, we denote $E = block^L(B^k)$, $\mathcal{U}_{block^L(\mathcal{B}^k)} = \mathcal{U}_E$ and $G_E := LG_{block(B^k)}$. Note that the total number of qubits of G_E is $O(n.L.k)$, out of which n qubits are identified input, and another n qubits as output. The expressions of L and k are given in Theorem 3. We will fix ε_d to a specific value (which we will calculate in later sections) and $t = 2$, which gives $O(n.L.k) = O(n^4)$.

Consider the sampling problem consisting of measuring the output qubits of G_E in the computational basis, with the input state of G_E being $|0\rangle^{\otimes n} := |0\rangle$ and let x be a bit string representing the outcomes of measurement of the output qubits of G_E, and y a bit string representing the outcomes of measurements performed on the non-output qubits. All measurements are non-adaptive, with angles defined by the graph state gadgets, and can be

performed simultaneously. Let

$$|\psi\rangle := \prod_{i,j} CZ_{i,j}(|+\rangle^{\otimes O(n^4)-n} \otimes |0\rangle^{\otimes n}) := \prod_{i,j} CZ_{i,j}(|+\rangle^{\otimes O(n^4)-n} \otimes |0\rangle),$$

denote the graph state corresponding to the graph state gadget G_E before any measurements are performed. This sampling gives rise to a probability distribution over $x \in \{0,1\}^n$ and $y \in \{0,1\}^{|V|-n}$, with $|V| = O(n^4)$ is the number of vertices in the graph state, defined by :

$$D(x,y) = \{p(x,y) = |\langle x,y|\psi\rangle|^2 = \frac{1}{2^{O(n^4)-n}} |\langle x| U_y |0\rangle|^2\}, \tag{4.8}$$

where $U_y \in \mathcal{U}_E$, $|\mathcal{U}_E| = 2^{O(n^4)-n}$, and $|x,y\rangle = |y\rangle \otimes |x\rangle$. The relation

$$|\langle x,y|\psi\rangle|^2 = \frac{1}{2^{O(n^4)-n}} |\langle x| U_y |0\rangle|^2,$$

is obtained by noting that

$$|\psi\rangle = \frac{1}{\sqrt{2^{O(n^4)-n}}} \sum_y |y\rangle \otimes U_y |0\rangle ,$$

(see Equation(2.14)), where $|y\rangle$ is a string of measurement results of non-output qubits sampling the random unitary $U_y \in \mathcal{U}_E$ which is applied to the n-qubit input state $|0\rangle$ now teleported to the output position.

In order to relate this to hardness, we first note that by construction our graph gadgets G_E give rise to universal sets under post-selection $\mathcal{U}_E$ in $U(2^n)$ [9]. This fact means that outputs x are $\sharp$P-hard to approximate

[9]To see this, note for large enough k in B^k we can generate any unitary in $U(4)$ under

up to relative error 1/4 + O(1) in worst-case [66, 114]. In the language of our MBQC gadgets, this translates to the fact that for some $U_y \in \mathcal{U}_E$ there exists outputs x such that approximating $|\langle x|U_y|0\rangle|^2$ up to a relative error of 1/4 + O(1) is ♯P-hard. This property is often referred to as worst-case ♯P hardness [25, 114] (or, for brevity, worst-case hardness), and is usually taken as a stepping stone for claiming average-case hardness conjectures of the likes of Conjecture 2 stated below. Hence, to obtain a working hardness proof (see Sections 4.2.2 and 4.3), we assume the 2 following complexity theoretic conjectures hold:

1. *Conjecture 1*: The widely believed conjecture that the polynomial hierarchy (PH) does not collapse to its 3rd level. [132]

2. *Conjecture 2*: Approximating the output probabilities $\frac{1}{2^{O(n^4)-n}}|\langle x|U_y|0\rangle|^2$ up to relative error $\frac{1}{4}+O(1)$ for a constant fraction of unitaries $U_y \in \mathcal{U}_E$ is ♯P-hard.

Conjecture 2 seems plausible because one can relate the sampling problem $D(x, y)$ to an IQP* sampling problem [110], and thus associate to it an appropriate Ising partition function [66, 112]. These Ising partition functions are known to be ♯P-hard to approximate in worst case up to relative error $\frac{1}{4} + O(1)$ for circuits which are universal under post selection [66, 112, 114, 25]. In this way, *Conjecture 2* can be viewed as an average-case complexity conjecture on the approximation of Ising partition functions which is present in the usual hardness proofs [38, 25, 26, 114].

post-selection, because of universality of $\mathcal{U}_{\mathcal{B}}$. In particular, we can generate to arbitrary accuracy the universal gate sets in [134, 135] for example, and SWAP's which are needed for universal quantum computation on $U(2^n)$.

We are now ready to precisely state our second main result in the form of the following theorem:

Theorem 4. *Assuming Conjectures 1 and 2 hold, a classical computer cannot sample from the distribution $D(x, y)$ (Equation (4.8)), formed from the concatenation of sampling partially invertible universal sets described above, up to l_1-norm error $\frac{1}{22}$ in time poly(n).*

Our last analytical contribution concerns the universality of sets associated with random unitary ensembles generated by non-adaptive fixed XY angle measurements on cluster states. As seen in [5, 36, 87] and for example in Figure 4.4, non adaptive fixed XY angle measurements on cluster states suffice for generating random unitary ensembles $\{p_i, U_i \in \mathcal{U}\}$, with $\mathcal{U}$ universal in $U(2^n)$. Here we show that this universality is *generic*, meaning that almost any assignment of non-adaptive fixed XY angle measurements on cluster states gives random unitary ensembles with support on universal gate sets $\mathcal{U} \in U(2^n)$, when $n = 2^\gamma$, where γ is a positive integer.

Our starting point is the random unitary ensemble,

$$CGEN = \{\frac{1}{2^n}, CZ_{1,2}...CZ_{n-1,n}(HZ(\alpha_1 + m_1\pi) \otimes .... \otimes HZ(\alpha_n + m_n\pi))\}, \tag{4.9}$$

with $m_i \in \{0, 1\}$. We show that this is an $(\eta < 1, t)$-tensor product expander (TPE) [108, 100, 36, 107], meaning that (see Equation (2.21))

$$||M_t[\mu_{CGEN}] - M_t[\mu_H]||_\infty \leq \eta < 1. \tag{4.10}$$

$CGEN$ in Equation (4.9) can be generated by an n-row, 2-column cluster state with n output qubits-the last column is the (unmeasured output), and with n XY plane measurement angles α_i, see Figure 4.5. We denote the set $\mathcal{U}_{\mathcal{CGEN}} = \{CZ_{1,2}...CZ_{n-1,n}(HZ(\alpha_1+m_1\pi)\otimes....\otimes HZ(\alpha_n+m_n\pi))\}$. As seen in [98, 100], showing that Equation (4.10) holds amounts to showing that the set $\mathcal{U}_{\mathcal{CGEN}}$ is a universal set in $U(2^n)$ [124, 125, 58]. Our result about the universality of $\mathcal{U}_{\mathcal{CGEN}}$ can be summarized in the following theorem.

Theorem 5. *$\mathcal{U}_{\mathcal{CGEN}}$ is a universal set in $U(2^n)$ for almost all choices of $\alpha_1, ..., \alpha_n$, for $n = 2^\gamma$, where γ is a positive integer.*

Two immediate corrolaries follow from Theorem 5 and the results of [100, 98].

Corollary 4. *$CGEN$ is an $(\eta < 1, t)$-TPE for almost all choices of $\alpha_1, ..., \alpha_n$.*

Corollary 5. *$CGEN^k$ is an ε-approximate t-design for almost all choices of $\alpha_1, ..., \alpha_n$, and sufficiently large k.*

$CGEN^k$ can be easily seen to generated by an n row, $k+1$ column cluster state, with measurement angles α_i, as illustrated in Figure 4.6.

A particularly interesting observation is the case when $\gamma = 1$. The result of Theorem 5 in this case says that almost any 2-qubit cluster state gadgets G_B generate random unitary ensembles B, with universal sets $\mathcal{U}_\mathcal{B} \subset U(4)$ [10], where $\mathcal{U}_\mathcal{B}$ can be invertible, partially invertible, or non-invertible [11]. What remains in order to obtain *efficient* t-designs is to show that the moment

[10] This is not surprising, since it was shown in [124, 125] that almost any 2-qubit gate is universal for quantum computing.

[11] We mean by non-invertible that for all $U \in \mathcal{U}_\mathcal{B}$, $U^\dagger \notin \mathcal{U}_\mathcal{B}$; We mean by invertible that for all $U \in \mathcal{U}_\mathcal{B}$, $U^\dagger \in \mathcal{U}_\mathcal{B}$

superoperator $M_t[\mu_B]$ of B has a subdominant (second largest) eigenvalue λ, and

- *Conjecture A: $|\lambda|$ does not scale badly (inefficiently) with t.*

If *Conjecture A* is true, then we can apply the techniques we used in Theorem 3 to show that we can construct n-qubit cluster state gadgets $LG_{block(B^k)}$ which sample from t-designs for efficient L and k from almost all 2-qubit cluster state gadgets G_B. Then, as a consequence of Theorem 4, these n-qubit cluster state gadgets can be used in quantum speedup proposals.

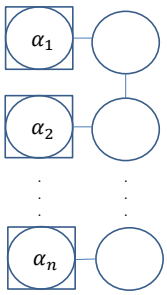

Figure 4.5: Cluster state gadget generating $CGEN$. Corollary 4 states that almost any choice of measurement angles $\alpha_1, ..\alpha_n$ give rise to a TPE.

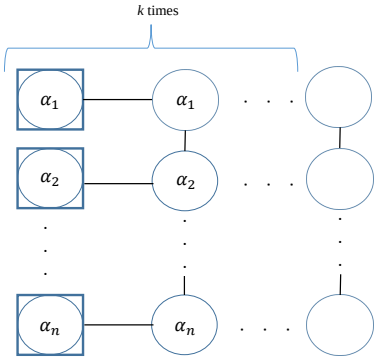

Figure 4.6: Graph gadget giving rise to $CGEN^k$. Corollary 5 states that almost any choice of measurement angles $\alpha_1, ..\alpha_n$ give rise to a $t-design$. Numerics suggest this is also an efficient construction.

Concerning *Conjecture A*, we performed numerical calculations on linear cluster states composed of 3 qubits, and on 2-row, 2-column cluster states like those of Figure 2.1. The random unitary ensembles of the 3 qubit linear cluster state have the form $\{\frac{1}{4}, HZ^m Z(\alpha) HZ^{m'} Z(\alpha) \in U(2)\}$ where $m, m' \in \{0, 1\}$. These random ensembles are generated by measuring two of the qubits of the linear cluster state at an angle α in the XY plane. The random unitary ensembles corresponding to the 2-row, 2- column cluster states have the form of Equation (2.15), and are generated by XY plane measurements performed as in Figure 2.1. The numerics are based on calculating the subdominant eigenvalue $|\lambda|$ of the moment superoperator (see Definition 4) corresponding to each of the above random unitary ensembles, for various values of t, and for various choices of the XY plane measurement angles. For the 3 qubit linear cluster states the values of t tested

were $t = 2, 3, 4, 5$, and for the 2-row, 2-column cluster states we tested for $t = 2, 3$. Beyond these values the numerical investigation becomes unfeasible as our numerical algorithms scale exponentially with n and t. [12]. For all the choices of fixed angle, non-adaptive XY measurements tested, we found that the subdominant eigenvalue $|\lambda|$ was independent of t for $t = 2, 3$ for both the 3 qubit linear cluster states and the 2-column, 2-row cluster states, which is in line with calculations in [136]. On the other hand, for the 3 qubit linear cluster states some angles tested showed a $|\lambda|$ *independent* of t for $t = 2, 3, 4, 5$, which is in line with the result of [122], other angles showed that $|\lambda|$ changes values from $t = 3$ to $t = 4$, but remains the same for $t = 4$ and $t = 5$. These numerical calculations seem to support *Conjecture A*, at least for small values of t. (see Section 4.5 for further discussion.)

As a final remark, note that in our numerics we assume $\eta \sim |\lambda|$ (see Definition 5) for moment superoperators of random ensembles defined on universal sets $\mathcal{U}$. We mean by this that the rate at which t-designess is attained is determined asymptotically by $|\lambda|$. This is indeed true, and common practice, when this moment superoperator is Hermitian and, more importantly, diagonalizable [100]. This corresponds to the case when $\mathcal{U}$ contains unitaries and their inverses. However, this approximation also works for general moment superoperators $M_t[\mu]$, namely because the set of diagonalizable square N by N matrices is *dense* in the set of N by N square matrices [137]. This means that any non-diagonalizable $M_t[\mu]$ is arbitrarily close in norm to a diagonal matrix, and in particular their eigenvalues are arbitrarily

[12]Note that in the $t = 1$ case, we obtained exact 1-designs ($|\lambda| = 0$) for both linear cluster states and 2-row, 2-column cluster states. This is in line with numerical calculations performed in [5].

close.

4.4 Proof of Theorems

4.4.1 Proof of Theorem 3

We begin by proving the following lemma regarding the ensemble B which samples from the partially invertible set $\mathcal{U}_{\mathcal{B}}$ (see Equation (4.1)).

Lemma 4. *B is an (η, t)-TPE with $\eta = 1 + (C-1)a < 1$ where $0 < C < 1$, and $a = \frac{|\mathcal{U}_{\mathcal{M}}|}{|\mathcal{U}_{\mathcal{B}}|}$.*

Proof.

$$M_t[\mu_B] = \sum_{i=\{1,\ldots,|\mathcal{U}_{\mathcal{B}}|\}} \frac{1}{|\mathcal{U}_{\mathcal{B}}|} U_i^{\otimes t,t} = aM_t[\mu_M] + (1-a)M_t[\mu_{B/M}],$$

where

$$M_t[\mu_M] = \sum_{i=\{1,\ldots,|\mathcal{U}_{\mathcal{M}}|\}} \frac{1}{|\mathcal{U}_{\mathcal{M}}|} U_i^{\otimes t,t}, U_i \in \mathcal{U}_{\mathcal{M}},$$

and

$$M_t[\mu_{B/M}] = \sum_{i=\{1,\ldots,|\mathcal{U}_{\mathcal{B}/\mathcal{M}}|\}} \frac{1}{|\mathcal{U}_{\mathcal{B}/\mathcal{M}}|} U_i^{\otimes t,t}, U_i \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}.$$

Since, by our definition of a partially invertible universal set, $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ is universal in $U(4)$, meaning by Proposition 3, that [98]

$$||M_t[\mu_{B/M}] - M_t[\tilde{\mu}_H]||_\infty \leq 1, \tag{4.11}$$

where $\tilde{\mu}_H$ is the Haar measure on $U(4)$ (as opposed to μ_H in Equation (2.19) which refers to the Haar measure over $U(2^n)$), and $M_t[\tilde{\mu}_H] = \int_{U(4)} U^{\otimes t,t} \tilde{\mu}_H(dU)$. Furthermore, $M_t[\mu_M]$ is the moment superoperator associated to a random ensemble sampling uniformly from a universal set in $U(4)$ having unitaries with algebraic entries [13], and which contains inverses, $M = \{\frac{1}{|\mathcal{U}_\mathcal{M}|}, U_i \in \mathcal{U}_\mathcal{M}\}$. Then, from the result of [122], there is a constant $0 < C < 1$ independent of t such that the following relation holds

$$||M_t[\mu_M] - M_t[\tilde{\mu}_H]||_\infty \leq C. \tag{4.12}$$

Now,

$$||M_t[\mu_B] - M_t[\tilde{\mu}_H]||_\infty = ||aM_t[\mu_M] - aM_t[\tilde{\mu}_H] + (1-a)M_t[\mu_{B/M}] - (1-a)M_t[\tilde{\mu}_H]||_\infty,$$

thus

$$\begin{aligned} ||M_t[\mu_B] - M_t[\tilde{\mu}_H]||_\infty &\leq a||M_t[\mu_M] - M_t[\tilde{\mu}_H]||_\infty \\ &\quad + (1-a)||M_t[\mu_{B/M}] - M_t[\tilde{\mu}_H]||_\infty = \eta. \end{aligned} \tag{4.13}$$

Replacing Equations (4.12) and (4.11) in Equation (4.13) allows to obtain the desired value of η.

□

[13] In [122], one requires sampling from SU(4). Fortunately, the moment super operator of a set sampled from U(4) can always be thought of as a sampling from SU(4). This can be seen by noting that for all $U \in$ U(4) we have $det(U) \neq 0$, hence $U^{\otimes t,t} = |det(U)|^{\frac{t}{2}} . U'^{\otimes t,t} = U'^{\otimes t,t}$, where $U' \in$ SU(4).

Using Proposition 2 and Lemma 4 we have the direct corollary concerning the k-fold concatenation of B, denoted by B^k (see Equation (4.2)).

Corollary 6. *B^k is a ε-approximate t-design in $U(4)$ for* $k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(8t + log_2(\frac{1}{\varepsilon}))$.

The next step is to consider the random unitary ensemble $block(B^k)$ (Equation (4.3)) whose associated moment superoperator is $M_t[\mu_{block(B^k)}]$. We will prove the following lemma.

Lemma 5. *$M_t[\mu_{block(B^k)}] = P'_{even}P'_{odd}$, where*

$$P'_{even} = P'_{2,3}.P'_{4,5}...,$$

$$P'_{odd} = P'_{1,2}.P'_{3,4}...,$$

and

$$P'_{i,i+1} = \frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j=\{1,...,|\mathcal{U}_{\mathcal{B}^k}|\}} (1_{2\times 2}^{\otimes i-1} \otimes U_{i,i+1}^{j} \otimes 1_{2\times 2}^{\otimes n-i-1})^{\otimes t,t},$$

where $U_{i,i+1}^{j} \in \mathcal{U}_{\mathcal{B}^k}$.

Proof.

$$block(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}}, (1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes U_{4,5}^{j_2} \otimes ... \otimes U_{n-2,n-1}^{j_{\frac{n}{2}-1}} \otimes 1_{2\times 2}).$$
$$(U_{1,2}^{j_{\frac{n}{2}}} \otimes U_{3,4}^{j_{\frac{n}{2}+1}} \otimes ... \otimes U_{n-1,n}^{j_{n-1}})\},$$

where $U_{i,i+1}^{j} \in \mathcal{U}_{\mathcal{B}^k}$.

$$M_t[\mu_{block(B^k)}] = \sum_{j_1,j_2,..,j_{n-1}=1,...|\mathcal{U}_{\mathcal{B}^k}|} \frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}} \big((1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes U_{4,5}^{j_2} \otimes$$
$$... \otimes U_{n-2,n-1}^{j_{\frac{n}{2}-1}} \otimes 1_{2\times 2}).(U_{1,2}^{j_{\frac{n}{2}}} \otimes U_{3,4}^{j_{\frac{n}{2}+1}} \otimes ... \otimes U_{n-1,n}^{j_{n-1}})\big)^{\otimes t,t}. \quad (4.14)$$

$M_t[\mu_{block(B^k)}]$ can be rewritten as :

$$M_t[\mu_{block(B^k)}] = \left(\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j_1=1,...|\mathcal{U}_{\mathcal{B}^k}|} (1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes 1_{2\times 2}^{\otimes n-3})^{\otimes t,t}\right)$$
$$\times \left(\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j_2=1,...|\mathcal{U}_{\mathcal{B}^k}|} (1_{2\times 2}^{\otimes 3} \otimes U_{4,5}^{j_2} \otimes 1_{2\times 2}^{\otimes n-5})^{\otimes t,t}\right) ...\times$$
$$\left(\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j_{\frac{n}{2}}=1,...|\mathcal{U}_{\mathcal{B}^k}|} (U_{1,2}^{j_{\frac{n}{2}}} \otimes 1_{2\times 2}^{\otimes n-2})^{\otimes t,t} ...\right) = [P_{2,3}^{'}.P_{4,5}^{'}...].[P_{1,2}^{'}.P_{3,4}^{'}...]$$
$$= P_{even}^{'} P_{odd}^{'}. \quad (4.15)$$

□

Next, we would like to bound $||P_{even}^{'} P_{odd}^{'} - P_{even}^{H}.P_{odd}^{H}||_\infty$, where

$$P_{even}^{H} = P_{2,3}^{H}.P_{4,5}^{H}...,$$

$$P_{odd}^{H} = P_{1,2}^{H}.P_{3,4}^{H}...,$$

and

$$P^H_{i,i+1} = \int_{U(4)} (1^{\otimes i-1}_{2\times 2} \otimes U \otimes 1^{\otimes n-i-1}_{2\times 2})^{\otimes t,t} \tilde{\mu}_H(dU).$$

We start by bounding each $P^{'}_{i,i+1}$ individually. Recall the 2 following well known and easily provable facts. *Fact 1*: for complex N by N matrices A we have

$$\frac{1}{\sqrt{N}}||A||_\infty \leq ||A||_2 \leq \sqrt{N}||A||_\infty. \tag{4.16}$$

Fact 2 : For Complex matrices A and B,

$$||A \otimes B||_2 = ||A||_2.||B||_2. \tag{4.17}$$

Now,

$$||P^{'}_{i,i+1} - P^H_{i,i+1}||_\infty \leq 2^{nt}.||P^{'}_{i,i+1} - P^H_{i,i+1}||_2 \leq$$
$$2^{nt}||\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j=\{1,\ldots,|\mathcal{U}_{\mathcal{B}^k}|\}} (U^j_{i,i+1})^{\otimes t,t} - \int_{U(4)} U^{\otimes t,t} \tilde{\mu}_H(dU)||_2.$$

The rightmost term is obtained using *Fact 2* (Equation (4.17)) and noting that $||1||_2 = 1$. Using *Fact 1* (Equation (4.16)) again, we get:

$$||P^{'}_{i,i+1} - P^H_{i,i+1}||_\infty$$
$$\leq 2^{nt+t}||\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j=\{1,\ldots,|\mathcal{U}_{\mathcal{B}^k}|\}} (U^j_{i,i+1})^{\otimes t,t} - \int_{U(4)} U^{\otimes t,t} \tilde{\mu}_H(dU)||_\infty.$$

Note that,

$$M_t[\mu_B^k] = \frac{1}{|\mathcal{U}_{\mathcal{B}^k}|} \sum_{j=\{1,\ldots,|\mathcal{U}_{\mathcal{B}^k}|\}} (U_{i,i+1}^j)^{\otimes t,t},$$

and

$$M_t[\tilde{\mu}_H] = \int_{U(4)} U^{\otimes t,t} \tilde{\mu}_H(dU).$$

Now, because B^k is a ε-approximate t-design on $U(4)$ (see Corollary 6), we have from [6] that:

$$||M_t[\mu_B^k] - M_t[\tilde{\mu}_H]||_\infty \leq 2^{t+1}\varepsilon.$$

Substituting this inequality in $||P_{i,i+1}^{'} - P_{i,i+1}^H||_\infty$ gives,

$$||P_{i,i+1}^{'} - P_{i,i+1}^H||_\infty \leq 2^{nt+2t+1}\varepsilon. \tag{4.18}$$

Choosing $\varepsilon = \frac{\varepsilon_1}{2^{nt+2t+1}}$ we get that,

$$||P_{i,i+1}^{'} - P_{i,i+1}^H||_\infty \leq \varepsilon_1, \tag{4.19}$$

when

$$k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(10t + nt + 1 + log_2(\frac{1}{\varepsilon_1})). \tag{4.20}$$

Equation (4.20) is found by plugging the value of ε in Corollary 6. Now we are ready to bound

$$||P_{even}^{'} P_{odd}^{'} - P_{even}^H . P_{odd}^H||_\infty.$$

We claim

Lemma 6. $||P'_{even}P'_{odd} - P^H_{even}.P^H_{odd}||_\infty \leq 2^{n^2t-2nt+n-1}\varepsilon_1$.

Proof. From Equation (4.19), we can write for all i , $P'_{i,i+1} = P^H_{i,i+1} + \gamma_i$, where $||\gamma_i||_\infty \leq \varepsilon_1$.

$$||P'_{even}P'_{odd} - P^H_{even}.P^H_{odd}||_\infty = ||(P^H_{1,2} + \gamma_1)(P^H_{3,4} + \gamma_3)... - P^H_{1,2}P^H_{3,4}...||_\infty.$$

Thus,

$$||(P^H_{1,2} + \gamma_1)(P^H_{3,4} + \gamma_3)... - P^H_{1,2}P^H_{3,4}...||_\infty =$$
$$||P^H_{1,2}P^H_{3,4}.. + P^H_{1,2}\gamma_3.. + \gamma_1P^H_{3,4}.. + \gamma_1\gamma_3... - P^H_{1,2}P^H_{3,4}...||_\infty.$$

Thus,

$$||(P^H_{1,2}+\gamma_1)(P^H_{3,4}+\gamma_3)...-P^H_{1,2}P^H_{3,4}...||_\infty \leq ||P^H_{1,2}\gamma_3..||_\infty+||\gamma_1P^H_{3,4}..||_\infty+||\gamma_1\gamma_3..||_\infty+...$$

$||P^H_{1,2}\gamma_3..||_\infty + ||\gamma_1P^H_{3,4}..||_\infty + ||\gamma_1\gamma_3..||_\infty + ...$ is a sum of $2^{n-1} - 1$ terms, each containing at most a product of $n-2$ $P^H_{i,i+1}$'s. Noting that, $||P^H_{i,i+1}||_\infty \leq 2^{nt}||P^H_{i,i+1}||_2$ using *Fact 1* (Equation (4.16)), and - using *Fact 2* (Equation (4.17))- that $||P^H_{i,i+1}||_2 = ||M_t[\tilde{\mu}_H]||_2 = 1$, then every term of the sum is individually less than $(2^{nt})^{n-2}\varepsilon_1$ [14], which means the whole sum (i.e $||P'_{even}P'_{odd} - P^H_{even}.P^H_{odd}||_\infty$) is less than $(2^{n-1}-1)(2^{nt})^{n-2}\varepsilon_1$, or equivalently

[14] Noting that $\varepsilon_1 < 1$, so $\varepsilon_1^m < \varepsilon_1$ for all $m > 1$

less than $2^{n^2t-2nt+n-1}\varepsilon_1$. □

Again, choosing $\varepsilon_1 = \frac{\varepsilon^{'}}{2^{n^2t-2nt+n-1}}$, we get

$$||P^{'}_{even}P^{'}_{odd} - P^{H}_{even}.P^{H}_{odd}||_\infty \leq \varepsilon^{'}, \tag{4.21}$$

when

$$k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(10t + n^2t - nt + n + log_2(\frac{1}{\varepsilon^{'}})). \tag{4.22}$$

Finally, we prove the following lemma.

Lemma 7. *For $n \geq \lfloor 2.5log_2(4t) \rfloor$, $block(B^k)$ is an (η, t)-TPE on $U(2^n)$ with $\eta = P(t) + \varepsilon^{'}$, where $P(t)$ is a polynomial in t given by Equation (4.7)*

Proof. We need to bound $||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty$, where $M_t[\mu_H] = \int_{U(2^n)} U^{\otimes t,t}\mu_H[dU]$, and μ_H is the Haar measure on $U(2^n)$. from Lemma 5,

$$||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty = ||P^{'}_{even}P^{'}_{odd} - M_t[\mu_H]||_\infty.$$

By a triangle inequality,

$$||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty \leq ||P^{H}_{even}P^{H}_{odd} - M_t[\mu_H]||_\infty + ||P^{'}_{even}P^{'}_{odd} - P^{H}_{even}.P^{H}_{odd}||_\infty.$$

Plugging in Equation (4.21) we get :

$$||M_t[\mu_{block(B^k)} - M_t[\mu_H]||_\infty \leq ||P^{H}_{even}P^{H}_{odd} - M_t[\mu_H]||_\infty + \varepsilon^{'}.$$

Finally, from the Detectibility lemma [118] (see also Lemma 2 in Chapter

3) and the result of [6] we get that when

$$n \geq \lfloor 2.5 log_2(4t) \rfloor,$$

$$||P^H_{even} P^H_{odd} - M_t[\mu_H]||_\infty \leq (1 + \frac{(425 \lfloor log_2(4t) \rfloor^2 t^5 t^{3.1/log(2)})^{-1}}{2})^{-1/3} := P(t),$$

and hence,

$$||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty \leq P(t) + \varepsilon^{'}.$$

□

Using Lemma 7 and Proposition 2 one obtains directly the value of L in Theorem 3 with k given by Equation (4.22), and $n \geq \lfloor 2.5 log_2(4t) \rfloor$. This Completes our proof of Theorem 3.

4.4.2 Proof of Theorem 4

We will follow the standard technique of applying Stockmeyer's theorem [113] along with some average-case hardness conjecture [38, 25, 26, 114] to prove hardness of approximate classical sampling up to a constant l_1-norm error. These techniques are the same as those used in [25, 26] (see also Chapter 2 Section 2.5 for an overview of these techniques). However, we will provide below a detailed proof of Theorem 4 in order to show how technical ingredients, such as anti-concentration for example, fit into our MBQC picture. Also, in our case the anti-concentration property is explicitly proven due to the 2-design property that our architectures possess [26], and we used a fixed assignment of measurement angles. In some sense, our result can be viewed as combining the two desirable properties of anti-conconcentration

(which was conjectured in [25], and which used fixed angle assignments) and fixed angle measurements (which was absent in [26] where they used variable angles, but had a provable anti-concentration). In our proof we will rely only on the 2 conjectures mentioned in Section 4.3.

Let $D(x,y)$ be the distibution given by probabilities $p(x,y) = |\langle x,y|\psi\rangle|^2$ as defined in Equation (4.8). Suppose there exists a classical $poly(n) = poly(O(n^4))$- time algorithm C which can sample from a probability distribution that approximates $D(x,y)$ up to an additive error μ in l_1-norm. In other words (following Equation (2.25)) :

$$\sum_{x,y} |p(x,y) - p_C(x,y)| \leq \mu, \tag{4.23}$$

where $p_C(x,y)$ is the output probability of the classical algorithm C. Then by Stockmeyer's theorem [113] there exists an $FBPP^{NP}$ algorithm that computes an estimate $p_C^{\sim}(x,y)$ of $p(x,y)$ such that:

$$|p_C^{\sim}(x,y) - p(x,y)| \leq \frac{p(x,y)}{poly(O(n^4))} + |p_C(x,y) - p(x,y)|(1 + \frac{1}{poly(O(n^4))}). \tag{4.24}$$

Using Markov's inequality:

$$Pr_{x,y}(|p_C(x,y) - p(x,y)| \geq \frac{E(|p_C(x,y) - p(x,y)|)}{\delta}) \leq \delta, \tag{4.25}$$

where $0 < \delta \leq 1$ and $|x,y\rangle$ picked uniformly at random. Noting that Equation (4.23) implies $E(|p_C(x,y) - p(x,y)|) \leq \frac{\mu}{2^{O(n^4)}}$

we get:

$$Pr_{x,y}(|p_C(x,y) - p(x,y)| \geq \frac{\mu}{\delta 2^{O(n^4)}}) \leq \delta. \tag{4.26}$$

Equation (4.26) means that the following relation holds with probability $1-\delta$:

$$|p_{\widetilde{C}}(x,y) - p(x,y)| \leq \frac{p(x,y)}{poly(O(n^4))} + \frac{\mu}{\delta 2^{O(n^4)}}. \tag{4.27}$$

We now use the following anti-concentration property for 2-designs (see Equation (2.24)):

$$Pr_{U_y \sim \mu}(|\langle x| U_y |0\rangle|^2 > \frac{\alpha(1-\varepsilon_d)}{2^n}) \geq \frac{(1-\alpha)^2(1-\varepsilon_d)}{2(1+\varepsilon_d)}, \tag{4.28}$$

where $0 < \alpha \leq 1$. Note that measurement of the $O(n^4) - n$ non-output qubits simply induces a uniform $\frac{1}{2^{O(n^4)-n}}$ distribution, and one can recast Equation (4.28) to reflect anti-concentration on the entire $O(n^4)$ measured qubits:

$$Pr_{U_y \sim \mu}(p(x,y) > \frac{\alpha(1-\varepsilon_d)}{2^{O(n^4)}}) \geq \frac{(1-\alpha)^2(1-\varepsilon_d)}{2(1+\varepsilon_d)}. \tag{4.29}$$

Equation (4.29) implies:

$$\frac{\mu}{\delta 2^{O(n^4)}} \leq \frac{\mu}{\delta\alpha(1-\varepsilon_d)} p(x,y). \tag{4.30}$$

Equation (4.30) holds with probability $\frac{(1-\alpha)^2(1-\varepsilon_d)}{2(1+\varepsilon_d)}$. Plugging Equation (4.30) into Equation (4.27) we obtain:

$$|p_{\widetilde{C}}(x,y) - p(x,y)| \leq (O(1) + \frac{\mu}{\delta\alpha(1-\varepsilon_d)}) p(x,y). \tag{4.31}$$

Equation (4.31) is an approximation of $p(x,y)$ by $p_C^{\sim}(x,y)$ with relative error $O(1)+\frac{\mu}{\delta\alpha(1-\varepsilon_d)}$.We claim, by a similar reasoning as can be found in [114, 25], that Equation (4.31) holds with probability $(1-\delta)\frac{(1-\alpha)^2(1-\varepsilon_d)}{2(1+\varepsilon_d)}$, or in other words Equation (4.31) is true for a $(1-\delta)\frac{(1-\alpha)^2(1-\varepsilon_d)}{2(1+\varepsilon_d)}$ fraction of unitaries $U_y \in \mathcal{U}_E$. Choosing $\mu = \frac{1}{22}$, $\delta = \alpha = \varepsilon_d$ $\sim$0.1132, we get that $p_C^{\sim}(x,y)$ approximates $p(x,y)$ to a relative error of $\frac{1}{4}+O(1)$ for an ~ 0.28 fraction of unitaries $U_y \in \mathcal{U}_E$. Assuming *Conjecture 2* to be true, we now have an $FBPP^{NP}$ algorithm which solves a $\sharp$ P-hard problem. But, this would imply by Toda's theorem [117] that the PH collapses to its 3rd level. Because we conjecture (*Conjecture 1*) the PH collapse to be impossible, we thus obtain a contradiction. As a conclusion, $D(x,y)$ cannot be sampled from up to a constant l_1-norm error by a classical polynomial time algorithm. This concludes our proof of Theorem 4.

4.4.3 Proof of Theorem 5

We start with $\gamma = 1$, then

$$\{p_i, U_i\} = \{\frac{1}{4}, CZ(HZ(\alpha_1 + m_1\pi) \otimes HZ(\alpha_2 + m_2\pi))\},$$

where $m_1, m_2 \in \{0,1\}$, and

$$\mathcal{U}_{\mathcal{CGEN}} = \{CZ(HZ(\alpha_1 + m_1\pi) \otimes HZ(\alpha_2 + m_2\pi))\}.$$

We suppose $\alpha_1 \in [0, 2\pi]$ and $\alpha_2 \in [0, 2\pi]$ are fixed angles irrationally related to π. Note that *almost any* angle is irrationally related to π, meaning that

the set of angles rationally related to π in the interval $[0, 2\pi]$ have Lebesgue measure zero [133] [15]. Denote by $Lie(U(4))$ the Lie algebra of $U(4)$ and $Lie(U(2) \times U(2))$ that of $U(2) \times U(2)$ [127] [16]. We want to prove, following [124, 125], that one can find at least two unitaries U_1 and U_2 in the random ensemble that have eigenvalues having arguments irrationally related to π and whose Lie algebra spans $Lie(U(4))$, and not any subalgebra. In that way we can construct any element of $U(4)$ from products of U_1 and U_2 [124, 125]. For our purposes, consider

$$U_1 = CZ_{1,2}(HZ(\alpha_1) \otimes HZ(\alpha_2)),$$

and

$$U_2 = CZ_{1,2}(HZ(\alpha_1 + \pi) \otimes HZ(\alpha_2 + \pi)).$$

The requirement of eigenvalues having arguments irrationally related to π is fulfilled by our choice of angles. We still need to prove we can find unitaries whose Lie algebras are in $Lie(U(4))$ and not any subalgebra.We begin by proving the following lemma.

Lemma 8. *$\frac{log(HZ(\alpha_1) \otimes HZ(\alpha_2))}{i}$ and $\frac{log(HZ(\alpha_1+\pi) \otimes HZ(\alpha_2+\pi))}{i}$ are generic elements of $Lie(U(2) \times U(2))$ for α_1, α_2 irrationally related to π.*

Proof. It suffices to prove that $HZ(\alpha)$ (or equivalently $HZ(\alpha)HZ(\alpha)$)is a

[15] Note also that the Lebesgue measure of the set of all points of the form $\{\alpha_1, ..., \alpha_n\}$, where each of the α_i's are rationally related to π is also zero. That is because the Lebesgue measure of a cartesian product of sets is equal to the product of Lebesgue measures of individual sets, and each of the individual sets (i.e a set of angles which is rationally related to π) has Lebesgue measure zero [133].

[16] We mean by this that $Lie(U(2) \times U(2))$ is the Lie algebra of unitary matrices $S \otimes T$, where $S, T \in U(2)$

generic element of $U(2)$ (and not any subgroup), for α generically chosen. Direct calculation gives

$$HZ(\alpha)HZ(\alpha) = e^{i\alpha} \begin{bmatrix} \frac{1+e^{-i\alpha}}{2} & \frac{1-e^{i\alpha}}{2} \\ \frac{e^{-i\alpha}-1}{2} & \frac{1+e^{i\alpha}}{2} \end{bmatrix},$$

where

$$R = \begin{bmatrix} \frac{1+e^{-i\alpha}}{2} & \frac{1-e^{i\alpha}}{2} \\ \frac{e^{-i\alpha}-1}{2} & \frac{1+e^{i\alpha}}{2} \end{bmatrix} \in SU(2).$$

A well known fact about $SU(2)$ is that a generic element can be represented as $e^{i\delta\vec{n}\vec{\sigma}}$ [37], where $\vec{n} = a\vec{x} + b\vec{y} + c\vec{z}$. a, b and c are real numbers such that $|a|^2 + |b|^2 + |c|^2 = 1$.

$\sigma = X\vec{x} + Y\vec{y} + Z\vec{z}$, X, Y and Z are the Pauli matrices. Again, a direct calculation for R gives $\delta = cos^2(\frac{\alpha}{2})$, $a = c = -\frac{sin\alpha}{2\sqrt{1-cos^4(\frac{\alpha}{2})}}$, and $b = -\frac{1-cos\alpha}{2\sqrt{1-cos^4(\frac{\alpha}{2})}}$. None of δ, a, b or c are zero for generically chosen α, this means that R is a generic element of $SU(2)$. Since

$$det(HZ(\alpha)HZ(\alpha)) = det(e^{i\alpha} \begin{bmatrix} \frac{1+e^{-i\alpha}}{2} & \frac{1-e^{i\alpha}}{2} \\ \frac{e^{-i\alpha}-1}{2} & \frac{1+e^{i\alpha}}{2} \end{bmatrix}) = e^{2i\alpha} \neq 1,$$

for generically chosen α, it means $HZ(\alpha)HZ(\alpha)$ (and hence $HZ(\alpha)$) is a generic element of $U(2)$ for generic α. □

Now, since $CZ \notin Lie(U(2) \otimes U(2))$ because CZ is not decomposable into a product of 1-qubit gates. Thus, $\frac{log(U_1)}{i}$ and $\frac{log(U_2)}{i} \in f$, where $Lie(U(2) \otimes U(2)) \subset f$. By Lemma 6.1 in [58] we have that there is no intermediate Lie algebra between $Lie(U(d) \otimes U(d))$ and $Lie(U(d^2)$, hence $f = Lie(U(4))$, and

thus $\frac{log(U_1)}{i}$ and $\frac{log(U_2)}{i}$ are generic elements of $Lie(U(4))$. This concludes the proof of the $\gamma = 1$ case [17]. Note that the proof we found is for angles irrationally related to π, however it extends to instances of angles rationally related to π. This is due to the fact that these angles give U_1 and U_2 whose eigenvalues have arguments irrationally related to π or eigenvalues equal to 1 [18], thereby fulfilling the requirements in [124, 125]. The proof for any $n = 2^\gamma$ can be extended by induction from the $\gamma = 1$ case, using the same methods, while noting that an element of $\mathcal{U}_{\mathcal{CGEN}}$ in this case can be written as $U = CZ_{\frac{n}{2},\frac{n}{2}+1}(A \otimes B)$ where

$$A \otimes 1_{2\times 2}^{\otimes \frac{n}{2}} = CZ_{1,2}...CZ_{\frac{n}{2}-2,\frac{n}{2}-1}(HZ(\alpha_1 + m_1\pi) \otimes ... \otimes HZ(\alpha_{\frac{n}{2}} + m_{\frac{n}{2}}\pi)),$$

and

$$1_{2\times 2}^{\otimes \frac{n}{2}} \otimes B = CZ_{\frac{n}{2}+1,\frac{n}{2}+2}...CZ_{n-1,n}(HZ(\alpha_{\frac{n}{2}+1}+m_{\frac{n}{2}+1}\pi)\otimes...\otimes HZ(\alpha_n+m_n\pi)),$$

where $A, B \in U(d) = U(2^{\frac{n}{2}})$, and $CZ_{\frac{n}{2},\frac{n}{2}+1} \in U(2^n) = U(d^2)$.

4.5 Comment on *Conjecture A*

At some point in the **Main Results** section, we mentioned that if *Conjecture A* (see Section 4.3) is true, then we can use techniques from Theorem 3 to prove that n-qubit cluster state gadgets $LG_{block(B^k)}$ effectively give rise to ef-

[17] A similar proof of this is found in [138], while noting that Lemma 5 along with results of [124, 125] implies $< HZ(\alpha_1) \otimes HZ(\alpha_2)), HZ(\alpha_1 + \pi) \otimes HZ(\alpha_2 + \pi) >= U(2) \otimes U(2)$ for generically chosen α_1 and α_2, with $< S >$ denoting the group generated by set S.

[18] more precisely some integer powers of U_1 and U_2 give these eigenvalues.

ficient t-designs for almost all choices of 2-qubit cluster state gadgets G_B. In what follows, we illustrate how this can be done for the particular version of *Conjecture A* suggested by our numerics - which are performed on 1-qubit and 2-qubit cluster state gadgets. Namely that the subdominant eigenvalue $|\lambda|$ of $M_t[\mu_B]$ is upper bounded by a constant independent of t for almost all 2-qubit cluster state gadgets G_B. This version of Conjecture A is inspired from our numerics, as well as from the result of [122] which showed that $|\lambda|$ is upper bounded by a constant independent of t when the universal set is invertible and composed of algebraic entries, and also from the results of [107] which showed a $|\lambda|$ upper bounded by a constant independent of t (up to large values of t scaling with the dimension of the unitaries) for finite gate sets chosen from the Haar measure. In other words, if the above version of *Conjecture A* is true, then as a direct corollary

Lemma 9. *B is an (η, ∞)-TPE with $\eta \sim |\lambda| \leq C < 1$, and C is indpendent of t.*

Now, replacing Lemma 4 in the proof of Theorem 3 by Lemma 9, then performing the exact same steps as in the proof of Theorem 3 allows us to obtain the required result. Then, the corresponding statement for gadgets $LG_{block(B^k)}$ follows straightforwardly from the translation to MBQC developped in previous sections.

As a final remark, if *Conjecture A* is true, we would not require $\mathcal{U}_{\mathcal{B}}$ to be composed of unitaries with algebraic entries in our proofs anymore. The only reason we require unitaries with algebraic entries is to use techniques in [6, 122] in order to arrive at Lemma 4.

4.6 Proof of Example Sampling From a Partially Invertible Set

For simplicity, let $\alpha = \frac{\pi}{6}$ and $\beta = acos(\sqrt{\frac{1}{3}})$. The graph gadget G_B in the example of Figure 4.4 gives rise to a random unitary ensemble $\mathcal{U}_{\mathcal{B}}$ with random unitaries of the form

$$U_m = (HZ(\beta+m_8\pi)\otimes HZ(\beta+m_7\pi))CZ(HZ(m_6\pi)HZ(\alpha+m_5\pi)HZ(m_4\pi)\otimes HZ(\alpha+m_3\pi)HZ(m_2\pi)HZ(\alpha+m_1\pi)),$$

where $m_i \in \{0,1\}$ for $i = 1,...,8$. Let

$$U_m = B_m.A_m,$$

where

$$B_m = HZ(\beta+m_8\pi)\otimes HZ(\beta+m_7\pi)$$

$$A_m = CZ(HZ(m_6\pi)HZ(\alpha+m_5\pi)HZ(m_4\pi)\otimes HZ(\alpha+m_3\pi)HZ(m_2\pi)HZ(\alpha+m_1\pi)).$$

Brute force calculation shows that $\mathcal{U}_{\mathcal{B}}$ is partially invertible (up to a global phase). What remains to be shown is that $\mathcal{U}_{\mathcal{B}}$ is universal. This amounts to showing that products of unitaries $U_m, U_m^{'} \in \mathcal{U}_{\mathcal{B}}$ can generate any unitary in $U(4)$, in line with the results of [124, 125]. Thus, as for Theorem 5, we will show that

(I) the Hermitian matrices $\frac{log(U_m)}{i}$ are elements of $Lie(U(4))$, and
(II) that eigenvalues of integer multiples U_m^k of U_m have eigenvalues with arguments irrationally related to π.

For (II), notice that $det(U_m) = e^{i(-4\beta + r\pi)}$, where r is a rational number. Then, at least one of the eigenvalues $e^{i\theta}$ of U_m has θ irrationally related to π, since β is iraationally related to π. This means that for some integer k, $V = U_m^k$ has eigenvalues 1 or eigenvalues with arguments irrationally related to π. Then, for all real numbers λ, there exists an integer m such that $V^m = V^{\lambda + O(1)}$, fulfilling one of the two requirements in [124, 125]. (I) follows straightforwardly from techniques in Theorem 5. $\frac{log(B_m)}{i}$ is a general element of $Lie(U(2) \otimes U(2))$ by Lemma 8, since β is an angle irrationally related to π. Furthermore, A_m is an entangling gate not expressible as a single product of 1-qubit gates, which means that $\frac{log(B_m A_m)}{i}$ is a general element of $Lie(U(4))$ by Lemma 6.1 in [58]. Note that a multitude of other sets of angles α and β we tested also gave partially invertible universal sets. The choice of elements uniformly at random from this set is due to the uniform probability of the different measurement results to occur.

4.7 Conclusion

In this chapter, we have relaxed the strict conditions on the sets of unitaries used for generating t-designs. This relaxation has natural relevance when considering t-designs derived from measurements on graph states - i.e. in the MBQC regime. We further showed that such constructions can also be used for providing new and interesting candidates for architectures demonstrating

quantum speedup.

Using these techniques we have provided explicit constructions of regular graph states, such that measuring on fixed angles generates efficient t-designs, and classically hard to sample distributions demonstrating quanutm speedup. Thus, we go beyond the results of the previous chapter in two ways (as seen earlier). First by showing that graph states other than the brickwork state, such as the cluster state, can be used to generate t-designs and demonstrate a quantum speedup. Second, by showing that various fixed angle assignments (we conjecture that almost every such assignment) give rise to t-designs and demonstrate a quantum speedup. These techniques and graph state architectures open up more opportunities for developing and demonstrating new and simple speedup architectures. In addition, the well developed verification techniques for graph states [26, 51, 38, 83, 84] provide a natural path for verification. Moreover, graph states are broad resource across quanutm information in netwoks including computing [30], fault tolerance [70], cryptographic multiparty protocols [71]. Indeed, the same graph state gadgets used here are universal for quantum computation [30] and can be used to distill optimal resources for quantum metrology [139]. In this context, our results lend themselves to the integration of these ideas into future quantum networks.

An open question is whether the $O(n^3t^{12})$ bound on efficiency of t-designness shown here can be enhanced to the (optimal in n) bounds in [6, 5, 36]. Another open question would be an analytical demonstration of efficiency of t-designness for cluster state gadgets with almost any assignment of non-adaptive fixed XY angle measurements.

Chapter 5

On Unitary t-designs From Relaxed Seeds

5.1 Introduction

In this chapter, we show that random quantum circuits with support over a particular family of finite sets of unitaries which are approximately universal in $U(4)$ (which we call *relaxed seeds*), converge towards t-designs efficiently in $poly(n, t)$ depth, where n is the number of inputs of the random quantum circuit, and t is the order of the design. We show this convergence for particular families of seeds which are *relaxed* in the sense that they do not satisfy the standard constraints [6]. These constraints are that every unitary matrix in the seed need not have an inverse in the seed, nor be composed entirely of algebraic entries in general.

Our families of seeds are derived from the partially invertible universal sets seen in the previous chapter, therefore these seeds are constructed in a

particular way and cannot be viewed as Haar sampled unitaries.

This result is novel in the sense that it removes completely the need for inverses in the seed ((i)) and the need for unitaries in the seed to be composed of algebraic entries ((ii)), thereby complementing the results of the previous chapter which managed to partially remove the requirements (i) and (ii).

We believe this result is not optimal, and can be improved. Particularly because the number of gates in the *relaxed* seeds introduced here grows with n and t. We conjecture that constant sized seeds such as those in [6, 94], and previous chapters, are sufficient.

5.2 Summary of the Results

In [6], it was shown that $n-$qubit random quantum circuits composed of layers of nearest neighbor unitaries $U \in U(4)$ drawn uniformly at random from a seed $\mathcal{U}_{\mathcal{B}} \subset U(4)$ [1], sample from an ε-approximate unitary t-design [29] efficiently in $poly(n, t, log(\frac{1}{\varepsilon}))$ depth. However, their proof required the following technical requirements to be verified.

- *Requirement* (i)*: Every* $U \in \mathcal{U}_{\mathcal{B}}$ *has an inverse* $U^{\dagger} \in \mathcal{U}_{\mathcal{B}}$*.*
- *Requirement* (ii)*: The unitaries* $U \in \mathcal{U}_{\mathcal{B}}$ *are composed entirely of algebraic entries.*

Ref. [6] also conjectured that the algebraic entry requirement is a technical issue (due mostly to using a result of [122]), and therefore could be dropped.

[1] As mentioned in the abstract, a finite set of unitaries which is approximately universal in $U(4)$ will be referred to as a seed.

In the previous chapter (see also [94]), we showed that these requirements can be reduced to seeds $\mathcal{U}_{\mathcal{B}}$ composed partially of a seed $\mathcal{U}_{\mathcal{M}}$ made up of unitaries with algebraic entries, and inverses in $\mathcal{U}_{\mathcal{M}}$; and its complement in $\mathcal{U}_{\mathcal{B}}$ denoted as $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ which need not nessesarily contain unitaries and their inverses nor be composed of algebraic entries.

In this chapter, we remove completely the requirements (i) and (ii) by giving examples of seeds in which every unitary in these seeds does not in general have an inverse in these seeds, nor are the unitaries in these seeds composed of algebraic entries in general, and yet we show efficient convergence to t-designs in a particular random circuit model we will define explicitly below. Thereby proving, and ultimately extending the scope of, the conjecture proposed in [6]. We will refer to these seeds as *relaxed seeds* throughout this chapter. However, it is to be noted that we **do not** mean that these seeds are *arbitrary* in the sense that the unitaries making up these seeds are chosen from the Haar measure on $U(4)$. Indeed, because our proofs are based on the partially invertible universal sets of Chapter 4, this endows the unitaries composing our relaxed seeds with some structure which makes them different from Haar distributed unitaries or indeed other ensembles not having this structure. The notation we will use in this chapter is the same as that in the previous chapter, but we will restate it here for the sake of using it in our proofs.

The seed $\mathcal{U}_{\mathcal{B}} \in U(4)$ is a *partially invertible universal* set composed of a seed $\mathcal{U}_{\mathcal{M}}$ which contains unitaries and their inverses, and is composed of unitaries with algebraic entries, and its complement, the seed $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ which is not in general composed of unitaries and inverses, nor unitaries with

algebraic entries. Define the random unitary ensemble [2]

$$B = \{\frac{1}{|\mathcal{U}_{\mathcal{B}}|}, U_i \in \mathcal{U}_{\mathcal{B}}\}. \tag{5.1}$$

Denote the k-fold concatenation of B by

$$B^k = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|}, \prod_{j=1,...k} U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}^k}\}, \tag{5.2}$$

where $U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}}$, $\mathcal{U}_{\mathcal{B}^k} = \{\prod_{j=1,...k} U_{\pi(j)} | U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}}\}$. π is a function acting on $\{1, ..., k\}$, resulting in a set $\{\pi(1), ...\pi(k)\}$ where $\pi(j) \in \{1, ..., |\mathcal{U}_{\mathcal{B}}|\}$, the $\pi(j)'s$ can be identical. There are $|\mathcal{U}_{\mathcal{B}^k}| = |\mathcal{U}_{\mathcal{B}}|^k$ such functions π and the k-fold concatenation includes all of them. Define [3]

$$block(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}}, (1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes U_{4,5}^{j_2} \otimes ... \otimes U_{n-2,n-1}^{j_{\frac{n}{2}-1}} \otimes 1_{2\times 2}).$$
$$(U_{1,2}^{j_{\frac{n}{2}}} \otimes U_{3,4}^{j_{\frac{n}{2}+1}} \otimes ... \otimes U_{n-1,n}^{j_{n-1}}) \in \mathcal{U}_{block(\mathcal{B}^k)}\}, \tag{5.3}$$

where $U_{i,i+1}^j \in \mathcal{U}_{\mathcal{B}^k}$, $i \in \{1, ..., n-1\}$ and $j \in \{1, ..., |\mathcal{U}_{\mathcal{B}^k}|\}$. Let $block^L(B^k)$ be the L-fold concatenation of $block(B^k)$, defined as

$$block^L(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{(n-1)L}}, \big(\prod_{j=1,...,L} U_{\pi(j)}\big) \in \mathcal{U}_{block^L(\mathcal{B}^k)}\}, \tag{5.4}$$

where here also π is as defined previously, and $U_{\pi(j)} \in \mathcal{U}_{block(\mathcal{B}^k)}$.

[2] A random unitary ensemble is a set of unitaries with a probability distribution over these unitaries. It was defined explicitly in the previous chapter.

[3] This definition of $block(B^k)$ is for even n , the odd n case follows straightforwardly.

Finally, let

$$a = \frac{|\mathcal{U}_{\mathcal{M}}|}{|\mathcal{U}_{\mathcal{B}}|}. \tag{5.5}$$

One of the main results of the previous chapter was Theorem (3), saying that one can obtain approximate unitary t-designs efficiently from partially invertible universal sets in $poly(n, t, log(\frac{1}{\varepsilon'}), log(\frac{1}{\varepsilon_d})) = O(n^3 t^{12} + log(\frac{1}{\varepsilon'})log(\frac{1}{\varepsilon_d}))$ depth. Define

$$\mathcal{U}^k = \mathcal{U}_{\mathcal{B}^k} - \mathcal{U}_{\mathcal{M}^k}, \tag{5.6}$$

to be the seed consisting of unitaries of the form

$$U = U_1 ....U_k,$$

where for all $j \in \{1, ..., k\}$, $U_j \in \mathcal{U}_{\mathcal{B}}$, and such that $\exists\ l \in \{1, .., k\}$ such that $U_l \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$. k is as defined in Equation (4.5) in Theorem (3). $\mathcal{U}^k$ in Equation (5.6) is the *relaxed* seed we will consider in this chapter. We will first show that, in general, $\mathcal{U}^k$ truly is *relaxed* by proving the following theorem which is the first main result of this chapter.

Theorem 6. *For a given value of k, there is a choice of the seed $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ such that $\mathcal{U}^k$ does not satisfy requirement (ii), and completely violates requirement (i) .*

It is meant by *completely violates* requirement (i) that, for some choices of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, every unitary in $\mathcal{U}^k$ does not have an inverse in $\mathcal{U}^k$.

Then, as promised, we will show that a particular random quantum circuit with seed $\mathcal{U}^k$ converges to an ε-approximate t-design efficiently in $O(nt + log(\frac{1}{\varepsilon}))$ depth. But first, define the random unitary ensemble

$$B_1 = \{\frac{1}{|\mathcal{U}^k|}, \mathcal{U}^k\}. \tag{5.7}$$

It is straightforward to see that

$$|\mathcal{U}^k| = (1 - a^k)|\mathcal{U}_{\mathcal{B}^k}|, \tag{5.8}$$

since

$$|\mathcal{U}_{\mathcal{M}^k}| = a^k|\mathcal{U}_{\mathcal{B}^k}|, \tag{5.9}$$

and by looking at Equation (5.6). $\mathcal{U}_{\mathcal{M}^k}$ being the set formed of unitaries of the form

$$W = W_1....W_k, \tag{5.10}$$

where $W_i \in \mathcal{U}_{\mathcal{M}}$, $\forall\, i \in \{1, ..., k\}$, k as defined in Equation (4.5). The random quantum circuits considered will be random unitaries in $block^L(B_1)$ defined for the random unitary ensemble B_1 (Equation (5.7)) in the exact same way as $block^L(B^k)$ in Equation (5.4) is defined for the random unitary ensemble B^k in Equation (5.2). We will show that $block^L(B_1)$ is a ε-approximate t-design, first by showing that $block(B_1)$, which is defined for B_1 of Equation (5.7) in the exact same way as $block(B^k)$ of Equation (5.3) is defined for the random unitary ensemble B^k in Equation (5.2)), is an $(\eta < 1, t) - TPE$ (see previous chapters and [107, 108] for a precise definition of an $(\eta, t) - TPE$),

then using Proposition 2 [4].

We now state the three theorems which establish that *relaxed* seeds can give rise to efficient approximate t designs, and which are the second, third, and fourth main results of this chapter.

Theorem 7. *$block(B_1)$ is an $(\eta, t) - TPE$ with*

$$\eta = \frac{P(t) + \varepsilon^{'}}{(1-a^k)^{n-1}} + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}}. \tag{5.11}$$

Theorem (7) holds, as Theorem (3) , when $n \geq \lfloor 2.5 log_2(4t) \rfloor$, $P(t)$, $\varepsilon^{'}$, k, are exactly as defined in Theorem (3). a is as defined in Equation (5.5).

Theorem 8. *$\forall\ t$, $\exists\ n_0 \geq \lfloor 2.5 log_2(4t) \rfloor$ such that $\forall\ n \geq n_0$*

$$\frac{P(t) + \varepsilon^{'}}{(1-a^k)^{n-1}} + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} \leq 1. \tag{5.12}$$

Theorem 9. *$\forall\ t$, $\exists\ n_0 \geq \lfloor 2.5 log_2(4t) \rfloor$ such that $\forall\ n \geq n_0$, $block^L(B_1)$ is an ε-approximate t-design in $U(2^n)$ in the strong sense, with L given by Equation (2.22) [5], and η given by Equation (5.11).*

Note that Theorem (9) means, as Theorem (3), that one can obtain efficient approximate t-designs efficiently from relaxed seeds $\mathcal{U}^k$.

The intuition behind why Theorems (7), (8), and (9) are true is quite straightforward. In the previous chapter, $block(B^k)$ was shown to be an $(\eta \leq 1, t)$-TPE [107, 108]. An overwhelmingly large fraction of random unitaries (tending to one in the $n, t \to \infty$ limit, see Equation (5.8)) in $block(B^k)$

[4] Again, we emphasize the k in Proposition 2 is taken to mean L here.

[5] we take the k in Equation (2.22) to be L

are also contained in $block(B_1)$. Therefore, one should expect $block(B_1)$ to be an $(\eta \leq 1, t)$-TPE. Section 5.3 will be devoted to technical proofs of Theorems (6)−(9).

As a final remark in this section, note that Equations (5.8) and (4.5) tell us that the number of unitaries in the *relaxed* seed $\mathcal{U}^k$ (Equation (5.6)) grows with n and t. This technical issue is due to us using the results on *partially invertible universal* sets in our proofs. This is in contrast with the seeds used in [6] and in Chapter 4 where these seeds were finite and were composed of a *constant* number of elements. We believe the results presented here are not optimal, and that finite *constant* sized sets not verifying requirement (ii), and completely violating requirement (i) are sufficient to give approximate unitary t-designs in a random quantum circuit model efficiently in $poly(n, t)$ depth.

5.3 Proofs

5.3.1 Proof of Theorem 6

Proving requirement (ii) is not verified by $\mathcal{U}^k$ is straightforward. By our definition of the *relaxed* seed $\mathcal{U}^k$ (Equation (5.6)) , any unitary $U \in \mathcal{U}^k$ can be written as a product of k unitaries in $\mathcal{U}_{\mathcal{B}}$ (with k defined in Equation (4.5)) $U = U_1...U_k$ with at least one $U_j \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$, and since in general $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ contains unitaries with non-algebraic entries, then the unitaries $U \in \mathcal{U}^k$ are in general composed of non-algebraic entries. To see this more clearly, let k

be odd, and consider for example

$$U = U_1....U_{\frac{k-1}{2}}.U_{\frac{k-1}{2}+1}...U_{k-1}.U_k \in \mathcal{U}^k,$$

where $U_{\frac{k-1}{2}+i} = U^{\dagger}_{\frac{k-1}{2}-i+1}$ for $i \in \{1, ..., \frac{k-1}{2}\}$, and $U_k \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$ is a unitary with non-algebraic entries. Then

$$U = U_k \in \mathcal{U}^k,$$

and is thus composed of non-algebraic entries.

We will now prove that (i) is completely violated in general by $\mathcal{U}^k$, this proof will be done by contradiction. Suppose, by contradiction, that $\forall$ choices of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ and for a fixed choice of $\mathcal{U}_{\mathcal{M}}$, $\exists\ U, U^{'} \in \mathcal{U}^k$ such that

$$U^{'} = U^{\dagger}. \tag{5.13}$$

Without loss of generality, we can write

$$U = \prod_{i=1,..,k} V_i^{m_i} W_i^{n_i}, \tag{5.14}$$

$$U^{'} = \prod_{j=k+1,..,2k} V_j^{m_j} W_j^{n_j}, \tag{5.15}$$

where $V_i, V_j \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$, and $W_i, W_j \in \mathcal{U}_{\mathcal{M}}$ for $i \in \{1, .., k\}$, and where $m_i, m_j, n_i, n_j \in \{0, 1\}$ with $n_i \neq m_i$ and $n_j \neq m_j$, $\forall\ i \in \{1, ...k\}$, $\forall$ $j \in \{k+1, .., 2k\}$, and such that $\exists\ i_1 \in \{1, .., k\}$ and $j_1 \in \{k+1, .., 2k\}$

such that $m_{i_1} = m_{j_1} = 1$. Equations (5.14), (5.15), and (5.13) imply

$$V_{j_1} = \prod_{j=j_1-1,\ldots,k+1} W_j^{\dagger n_j} V_j^{\dagger m_j} . \prod_{i=k,\ldots,1} W_i^{\dagger n_i} V_i^{\dagger m_i} . \prod_{j=2k,\ldots,j_1+1} W_j^{\dagger n_j} V_j^{\dagger m_j} . \tag{5.16}$$

Now, we will prove that Equation (5.16) does not hold for some choices of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, thereby establishing a contradiction. We will consider all the possible cases as follows.

- **Case 1:** $V_j \neq V_{j_1}\ \forall\ j \neq j_1$ in Equation (5.16).

  W.l.o.g, let $\mathcal{U}_{\mathcal{M}} = \{W_1, ..., W_n\}$ and $\mathcal{U}_{\mathcal{B}/\mathcal{M}} = \{V_1, ..., V_m\}$, with $m, n \in \mathbb{N}$, and let $V_{j_1} = V_m$. Fix $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$, and list all the possible relations of the form of the R.H.S of Equation (5.16), where $W_j \in \{W_1, ..., W_n\}$, $\forall j \in \{k+1, .., 2k\}$, and $V_i, V_j \in \{V_1, ..., V_{m-1}\}$, $\forall i \in \{1, ..., k\}$, $\forall j \in \{k+1, ..., j_1 - 1, j_1 + 1, ...2k\}$. Since there are *countably* many relations of the form of the R.H.S of Equation (5.16) [6], choose $V_{j_1} = V_m$ such that it is not equal to any of the listed relations of the R.H.S of Equation (5.16). Therfore, Equation (5.16) does not hold in general in **Case 1**.

- **Case 2:** $\exists\ j \neq j_1$ such that $V_j = V_{j_1}$ in Equation (5.16).

  Here it will be convenient to rewrite Equation (5.16) as

  $$V_{j_1} = \prod_{i=1,\ldots,2k-1} C_i^{\pi(i)} (V_{j_1}^{\dagger})^{1-\pi(i)}, \tag{5.17}$$

  where again we take that $V_{j_1} = V_m$, $C_i \in \{V_1^{\dagger}, ..., V_{m-1}^{\dagger}, W_1^{\dagger}, ..., W_n^{\dagger}\}$,

[6] and *uncountably* many choices of V_m.

and $\{V_1^\dagger, ..., V_{m-1}^\dagger, W_1^\dagger, ..., W_n^\dagger\}$ are fixed (as in **Case 1**.). $\pi(.)$ is a map

$$i = \{1, ..., 2k-1\} \rightarrow \pi(i) \in \{0, 1\}.$$

We consider the two following subcases

- **Case 2a:** $\pi(i) = 0$, $\forall i \in \{1, ..., 2k-1\}$.

  Equation (5.17) becomes in this case

$$V_{j_1} = (V_{j_1}^\dagger)^{2k-1}. \tag{5.18}$$

  Equation (5.18) does not hold *exactly* for general choices of $V_{j_1} = V_m$, since products of the form of the R.H.S of Equation (5.18) can only *approximate* V_{j_1} up to a given precision in general [108].

- **Case 2b:** $\exists\ i_1$ such that $\pi(i_1) = 1$.

  Equation (5.17) can be rewritten in this case as

$$C_{i_1} = \prod_{i_1-1,...,1} V_{j_1}^{1-\pi(i)}{}_{j_1} C_i^{\dagger\pi(i)}.V_{j_1}. \prod_{i=2k,...,i_1+1} V_{j_1}^{1-\pi(i)}{}_{j_1} C_i^{\dagger\pi(i)}. \tag{5.19}$$

  Since $C_{i_1} \in \{V_1^\dagger, ..., V_{m-1}^\dagger, W_1^\dagger, ..., W_n^\dagger\}$, and these unitaries are fixed, therefore Equation (5.19) cannot hold for a general choice of $V_{j_1} = V_m$.

  In order to complete the proof of Theorem (6), we should show that a V_m exists which simultaneously violates the relations imposed in **Case 1** and **Case 2**. For a given fixed integer k, and fixed $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$ there is only a finite number of unitaries V_m satisfying Equation (5.16) in **Case 1**. Unitaries V_m satisfying Equations (5.18) and (5.19) (**Case**

2a and **2b**) also satisfy the relation

$$det(C_{i_1} - \prod_{i=i_1-1,...,1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)} V_{j_1} \prod_{i=2k,...,i_1+1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)}) = 0. \tag{5.20}$$

Using the analysis of [140], the set of unitaries V_m satisfying relations of the form Equation (5.20) has zero Haar measure on U(4). This follows from the fact that one can show that there is a one-to-one mapping between these (non-identically zero) polynomial equations in the matrix elements of V_m, and the intersection [7] of the zero sets of two real analytic functions on $\mathbb{R}^{16}$. Each such zero set has a Lebesgue measure zero, therefore their intersection (which is a subset of the two) also has Lebesgue measure zero (see [140] for more details). Therefore, the set of unitaries generated by relations of the form of Equation (5.20) has Haar measure zero [140]. The number of possible relations of the form of Equation (5.20) is countable (for fixed k and fixed $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$), thus the Haar measure of the set of unitaries V_m satisfying Equations (5.18) or (5.19) is also zero, as the countable union of measure zero sets is also measure zero. This means that we can chose V_m to be outside a measure zero set (which is the set of unitaries satisfying Equations (5.16) in **Case 1**,(5.18), and (5.19)), and we would therefore have that V_m simultaneously violates the relations imposed by **Case 1** and **Case 2**. This completes the proof of Theorem (6).

[7] Corresponding to partitioning the determinant into real and imaginary parts, each of which can be expressed as a trigonometric function of 16 real valued angles in $[0, 2\pi]$ parametrizing V_m [140].

5.3.2 Proof of Theorem 7

Define the moment superoperators [8]

$$M_t[\mu_{block(B^k)}] = \sum_{i=1,\ldots|\mathcal{U}_{\mathcal{B}^k}|^{n-1}} \frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}} U_i^{\otimes t,t}, \tag{5.21}$$

where $U_i \in \mathcal{U}_{block(B^k)}$.

$$M_t[\mu_{block(B_1)}] = \sum_{i=1,\ldots|\mathcal{U}^k|^{n-1}} \frac{1}{|\mathcal{U}^k|^{n-1}} V_i^{\otimes t,t}, \tag{5.22}$$

where $V_i \in \mathcal{U}_{block(B_1)}$.

$$M_t[\mu_{block(B_2)}] = \sum_{i=1,\ldots|\mathcal{U}_{block(B_2)}|} \frac{1}{|\mathcal{U}_{block(B_2)}|} W_i^{\otimes t,t}, \tag{5.23}$$

where $W_i \in \mathcal{U}_{block(B_2)}$. $\mathcal{U}_{block(B_2)}$ is the complement of $\mathcal{U}_{block(B_1)}$ in $\mathcal{U}_{block(B^k)}$. Straightforward calculation using Equation (5.8), leads to the following relation

$$M_t[\mu_{block(B^k)}] = (1-a^k)^{n-1} M_t[\mu_{block(B_1)}] + (1-(1-a^k)^{n-1}) M_t[\mu_{block(B_2)}]. \tag{5.24}$$

Recalling from the previous chapters that $M_t[\mu_{block(B_1)}]$ is an (η, t)-TPE if [108, 107]

$$||M_t[\mu_{block(B_1)}] - M_t[\mu_H]||_\infty \leq \eta, \tag{5.25}$$

[8] Refer to the previous chapters for a precise definition of moment superoperator.

where $M_t[\mu_H] = \int_{U(2^n)} U^{\otimes t,t} \mu_H(dU)$, μ_H being the Haar measure on $U(2^n)$, and using Equation (5.24) and a triangle inequality for norms we get

$$||M_t[\mu_{block(B_1)}] - M_t[\mu_H]||_\infty \leq \frac{1}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty. \quad (5.26)$$

Thus, $block(B_1)$ is an $(\eta, t) - TPE$ with

$$\eta = \frac{1}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty. \quad (5.27)$$

From a result in the previous chapter,

$$||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty \leq P(t) + \varepsilon^{'}, \quad (5.28)$$

where $P(t)$ and $\varepsilon^{'}$ are as defined in Theorem (3). Also, because $\mathcal{U}_{block(B_2)}$ is approximately universal on $U(2^n)$ (because its composed of unitaries which are approximately universal on $U(4)$), then by a result of [98],

$$|M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty \leq 1. \quad (5.29)$$

Replacing Equations (5.28) and (5.29) in Equation (5.27) allows to obtain the value of η in Theorem (5).

5.3.3 Proof of Theorem 8

The proof of Theorem (8) will also proceed by contradiction.

Suppose $\exists\ t_m$, such that $\forall\ n \geq \lfloor 2.5 log_2(4t) \rfloor$,

$$\frac{P(t_m) + \varepsilon^{'}}{(1-a^k)^{n-1}} + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} > 1. \tag{5.30}$$

Notice that,

$$\lim_{n\to\infty} (1-a^k)^{n-1} = 1, \tag{5.31}$$

with a and k as given in Equations (4.5) and (5.5), with t replaced by t_m. Thus, for large enough n, and by using Equation (5.31), Equation (5.30) reduces to

$$P(t_m) + \varepsilon^{'} \sim> 1. \tag{5.32}$$

Equation (5.32) leads to a contradiction, since by Theorem (3), $P(t)+\varepsilon^{'} \leq 1$, $\forall\ t$. This concludes the proof of Theorem (8).

5.3.4 Proof of Theorem 9

The proof of Theorem (9) follows directly from replacing Theorems (7) and (8) in Proposition (2).

5.4 Conclusion

In this chapter, we have shown that one can obtain efficient approximate unitary t-designs from random quantum circuits with support over families of seeds which are *relaxed* in the sense that any unitary in the seed need not

in general have its inverse in the seed, nor are the seed unitaries composed entirely of algebraic entries. This result, to the best of our knowledge, is novel, and it also proves and extends the scope of a conjecture proposed in [6].

The *relaxed* seeds presented here have a cardinality which increases with n and t (see Equation (5.8)). These seeds, we believe, are not optimal, and we conjecture that *arbitrary* seeds with a constant number of elements as in [6, 94] suffice to get efficient t-designs.

Chapter 6

Fault-Tolerant Quantum Speedup With Constant Depth Circuits

6.1 Introduction

In Chapter 4, we introduced new examples of sampling problems demonstrating a quantum speedup, the proof of which can also directly be used to show that sampling from the output distribution of our construction in Chapter 3 demonstrates a quantum speedup. However, it is not clear that the bounds found in these kind of results are meaningful in terms of the realistic noise in any implementations. Thus, noise is an obstacle in the way of achieving quantum speedup. Indeed, in [33], it was shown that a simple noise model - each output bit undergoes a bit flip with probability

ε - renders the output probabilities of IQP circuits [1] efficiently simulable classically, meaning that a classical polynomial time algorithm can approximately sample from these probability distributions, the quantum speedup is thus lost to noise. However, using classical error correction, this quantum speedup can be recovered [33]. More precisely, it was shown in [33] that encoding every qubit in the n-qubit IQP circuit [3] with $O(log(n))$ physical qubits, then measuring and performing a majority vote error correction, allows to recover quantum speedup even in the presence of noise, for the above defined simple noise model. The question of the treatment of general noise remained open [33]. There have been attempts to treat general noise in the work of [141], however, the exponentially small bounds on success mean that these do not currently offer a practical solution (see Section 6.7 for a deeper discussion of this work).

In this chapter, we are interested in general noise models, and in the question of whether we can recover quantum speedup in their presence, using relatively simple and experimentally motivated means. Our desiderata are mainly local gates (through transversality), regular structure, relatively low overhead, and fixed angle, non-adaptive Pauli measurements, amongst others [37].

We do so by building on the architectures for quantum speedup based on non-adaptive measurement based quantum computing (MBQC) [30] in [25, 26, 38, 94] and Chapters 3 and 4. Essentially we incorporate fault toler-

[1] Which are in the ideal case, when noise is neglected, hard to approximately sample from efficiently classically [114].

ant techniques using the color code [142] and efficient magic state distillation [143, 7]. The first of our desiderata is naturally fulfilled by our choice of the quantum error correction code, namely the 2D color code, which allows a transversal implementation of the entire Clifford group [142], and has a good fault-tolerance threshold [8]. The non-Clifford part needed for computational universality, and consequently quantum speedup, is supplied via magic state distillation (MSD) [143, 144, 7, 145, 146], albeit fault-tolerantly [147]. Our second desiderata is ensured by our choice of graph states [69], namely the cluster state and brickwork state [4] which are 2D lattices of qubits with nearest neighbor interactions,regular structure, and which are universal resources for MBQC [30, 85, 4]. Concerning our third desiderata, our construction achieves a quantum speedup using an overhead of at most $O(log^3(n))$ physical qubits per logical qubit (including magic state distillation overhead [7]).

Thus, our architecture requires a slightly increased overhead as compared to the $O(log(n))$ overhead in [33], but provides a quantum speedup in the presence of general noise models [8]. Our architecture consists of measuring the qubits of our 2D graph states at fixed angles non-adaptively in the Pauli X, Y, and Z bases, thereby automatically fulfilling our last desiderata, and providing additional advantages such as single instance hardness [38, 94], and translational invariance [38, 36, 94].

A striking feature in our architecture is that it can be thought of as a sort of quantum circuit of *constant* depth acting on a polynomial in n number of ancillas. Indeed, our entire sampling procedure can be executed in a constant number of rounds, as seen in the previous paragraphs, and is

also robust to general noise models by virtue of quantum error correction [37]. Furthermore, the overhead required to achieve fault-tolerant, robust quantum speedup is $\sim O(log^3(n))$ per qubit in our case (including distillation and logical encoding of qubit in a color code), which is not much worse than the $O(log(n))$ overhead per qubit in the model of [33], which only corrects for bit-flip errors. The total number of physical qubits needed for our construction is $O(n^3 log^3(n))$, as will be seen in later parts of this chapter.

In Section 6.2 we give an overview of our construction for the robust sampling architecture showing quantum speedup. In Section 6.3 we will bound the size of the error correction code required for our construction to work. We bound the size of overhead for the distillation of the magic states in Section 6.4. In Section 6.5 we will present an overview of our proof of quantum speedup. In Section 6.6 we will show that our sampling problem shows a quantum speedup. Finally, we discuss our results in Section 6.7.

6.2 Overview of the Construction

Our construction is essentially a fault-tolerant version of the measurement based construction of Chapters 3 and 4 (see also [36, 94]). In Chapter 3, and by direct analogy to the proof of hardness in Chapter 4 (see Section 4.2.2), it can be shown that performing non-adaptive measurements of local Pauli X, Y, and $X_{\frac{\pi}{4}}$ (at an angle $\pi/4$ in XY plane of the Bloch sphere) on an n-row, k-column brickwork state $|G\rangle$ [4] of polynomial length (see Figures 6.1, 3.2, 3.3, and 3.4) give statistics demonstrating quantum speedup. Our strategy for making this fault tolerant is, first, to make a fault tolerant version of

the graph state, and then second, to replace replace the $\pi/4$ measurements by instead injecting so called *magic states*, in our case the T-state, and teleporting in a rotated measurement, also in a fault tolerant way [8, 147]. Since graph states can be constructed by Clifford circuits, the encoding of the graph state can be done transversally using the color code [142], which is also used to do a fault tolerant version of the distillation of the T-state [147, 7, 8]. Furthermore, by applying measurement based versions of the fault tolerance procedures, we can achieve this using constant depth circuits.

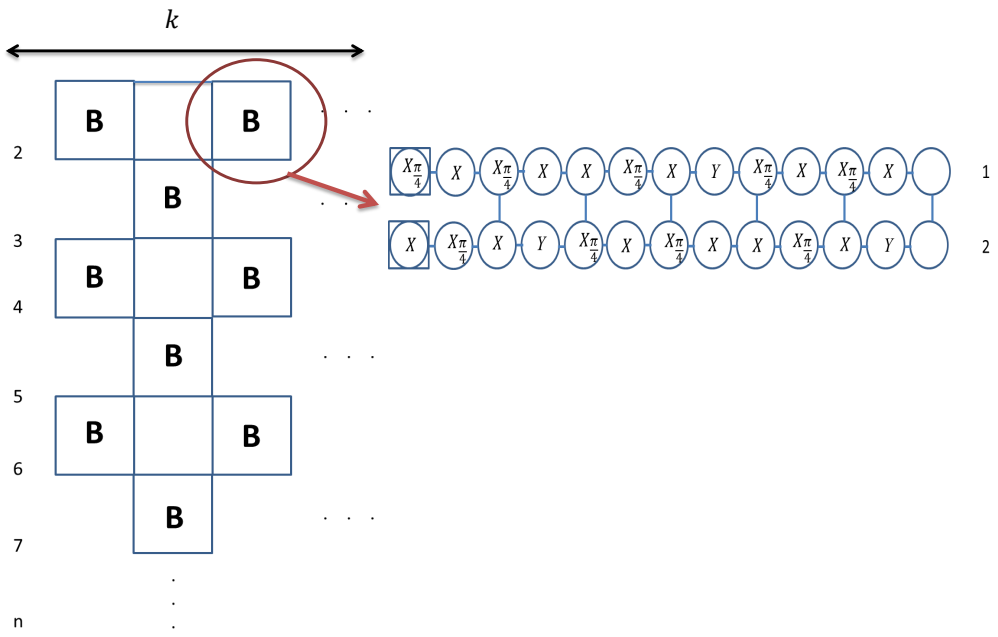

Figure 6.1: The brickwork state $|G\rangle$ with n-rows and k columns, and with an assignment of fixed angles as in Chapter 3. As per our standard convention, in the zoom in of each gadget B, the circles represent qubits. Inside is written the measurement basis to be applied, empty ones are unmeasured outputs and inputs have a square over them (see also Figures 3.4, 3.2, 3.3 and 2.1).

The graph state $|G\rangle$, which is the basis of our construction, is depicted in Figure 6.1, where the appropriate measurement angles are also indicated. It is built up by tiling of small graph states, which, together with the measurement angles, we call gadget B (see Figures 6.1, 3.4, 3.2, 3.3, and Chapter 3). These B gadgets provide the universality and structure which, when

combined in this way, give rise to quantum speedup, in an exact analogy to the examples in Chapters 3 and 4 (some of which differ only by the choice of measurement angles). Since the $\pi/4$ measurements are not Pauli, it is troublesome to do them fault tolerantly using standard stabiliser codes. A common strategy to address this is so called magic state distillation and injection [143, 7, 145, 146, 144]. In particular, given copies of the resource T state , defined as

$$|T\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\imath\pi/4}|1\rangle\right), \tag{6.1}$$

the $\pi/4$ measurements in our gadgets can be replaced by entangling the T-states and measuring them in a Pauli basis. In our case the entangling can be done by CZ and the measurement is Pauli X, so it can be viewed as an altered graph state as depicted in Figure 6.2. In this way the problem of performing a non-Pauli measurement is replaced by a Pauli measurement and the problem of generating a T-state. This, in turn, can be done by standard distillation procedures, which can be done fault tolerantly [143, 8, 147].

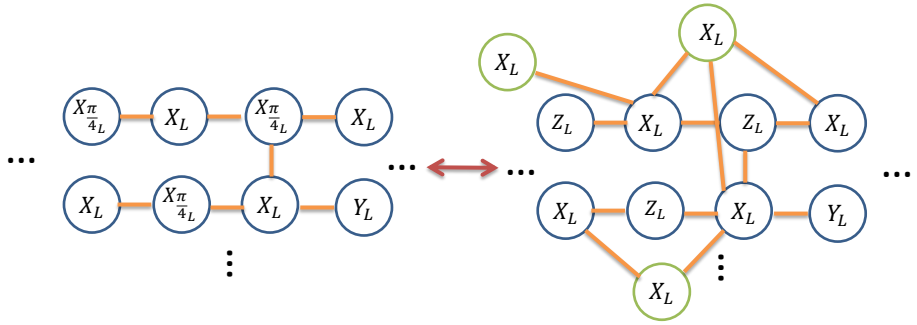

Figure 6.2: (Right) : Part of the state $|G_L\rangle$ showing various entanglements with the output T-state qubits of succesful MSD protocols (green unfilled circles). Each of the qubits of $|G_L\rangle$ (blue unfilled circles) and the output T-states is a logical qubit which is a 4.8.8 2D triangular color code composed of $O(log^2(n))$ physical qubits. The orange lines are CZ_L gates. Qubits are measured at the angles indicated by letters inside the circles. Subscript L represents logical measurements. The entanglements with the T-states in the way presented in this figure and their measurement in the X_L bases is in order to effectively implement a measurement at an angle $\pi/4$ in the XY plane of the Bloch sphere.

We begin by considering the preparation of the logical encoding of the n-row, $k = poly(n)$-column graph state, $|G_L\rangle$. To get $|G_L\rangle$, each qubit of $|G\rangle$ is replaced by a *logical* qubit which is a triangular 2D 4.8.8 color code, whose number of physical qubits is $O(log^2(n))$ [8] (thus the number of phys-

ical qubits per logical qubit of $|G_L\rangle$ is $O(log^2(n)))$, and each CZ replaced by a the logical CZ_L gate, performed by implementing CZ gates tranversally between the physical qubits of two logical qubits [142]. The preparation of $|G_L\rangle$ can be done fault-tolerantly in a constant number of rounds. Here, by round we mean either a parallel execution of measurements (i.e measurements which can be performed in a single time step), a parallel execution of one or two qubit gates, or a parallel preparation of qubits. This follows from the fact that the preparation of logical qubits of a color code in the logical $|+\rangle$ state can be performed fault-tolerantly in a constant number of rounds [8], and because the brickwork state has a regular structure, its preparation can be thought of as a constant depth quantum circuit executed on $k.n = poly(n)$ ancillas [25, 94], where at each step of the circuit (or round) one implements a parallel sequence of nearest-neighbor logical CZ gates. After each round, we perform a full sequence of syndrome measurements (error detection), followed by error correction. The procedure of error detection we will use is that of [8] which consists of using one ancilla qubit to measure each X or Z-type stabilizer of the color code, followed by applying a certain decoding algorithm to extract the error [8]. Error correction will consist of applying the appropriate multi-qubit Pauli operators which counters the detected error. This procedure of error detection and correction is also done in a constant number of rounds [8]. Throughout the rest of this chapter, we will assume, as in the code capacity noise model of [8], that the syndrome qubits are perfect, thus the error detection needs to be performed only once. Note that if we were to relax this assumption, the error detection procedure would have to be repeated a number of times of the order of the

code distance [8] (which scales as $O(log(n))$), and therefore our quantum circuits would no longer be constant depth. For the moment, we leave as an open question whether one could retain the constant depth property while assuming noisy syndrome qubits, however it is worth mentioning that there is strong evidence that the answer to this question is "yes" [148].

The Clifford part of the $|G_L\rangle$ measurements can be implemented by measuring transversally X or Y on each of the (physical) qubits of the color code [142] (this effectively implements logical logical X_L or Y_L measurements, due to the transversality properties of the color code [142].), along with error correction and detection. As mentioned, the non-Clifford part (which provides universality under post-selection; a key ingredient in hardness proofs [3]) is provided by (fault-tolerantly) injecting T-states [143].

Next, in parallel to constructing $|G_L\rangle$, we also fault-tolerantly prepare $k.n$ copies of graph states which we will call $|zMSD_L\rangle$. These $|zMSD_L\rangle$ are logical versions of graph states we call $|zMSD\rangle$, which encode a measurement based version of the concatinations of the distillation of magic states in [7]. The distillation circuits of [7] are circuits on $O(d)$ qubits, which injects $O(d^2)$ noisy T-states of fidelity $f = 1 - \epsilon$ and returns $O(d)$ noisy T-states with increased fidelity $f = 1 - \epsilon^{'}$, with $\epsilon' = O(\epsilon^d)$. The noisy T-states are injected at regular intervals in the circuit. These distillation circuits can be implemented in a measurement based way [30, 85] by creating a 2D cluster state $|1MSD\rangle$ (which through universality can implement any circuit) and injecting the T-states into it, resulting in 2D cluster states where some nodes

are the noisy injected T-states (see Figure 6.3 [2].).

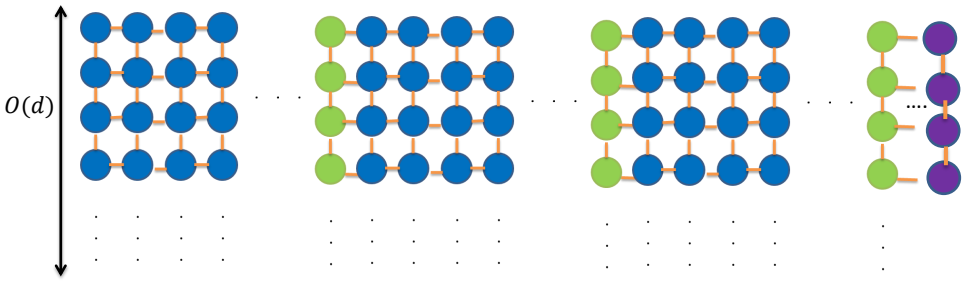

Figure 6.3: The graph state $|1MSD\rangle$ which performs, when its qubits are measured non-adaptively, the magic state distillation protocol of Theorem 4.1 in [7]. Blue and green filled circles are qubits measured in the Pauli X, Y or Z at fixed pre-assigned angles non-adaptively. The blue colored qubits perform the Clifford part of the distillation circuit in [7]. The green qubits are the noisy T-states injected at regular intervals (see main text) which, when measured at Pauli angles, provide the non-Clifford part of the distillation protocol of [7]. The orange horizontal and vertical lines are CZ gates. Purple filled qubits are the output qubits of the protocol which are T-states of fidelity $1 - O(\varepsilon^d)$ if the MSD is succesful.

In order to get the level of fidelity we require, whilst keeping resources low, we concatenate this process several (z) times. In the measurement

[2] Note that in the fault-tolerant version of our protocol in the first layer, noisy (physical) T states are encoded onto the (logical) qubits of $|1MSD_L\rangle$ at regular intervals, resulting in noisy logical T-states which are used in the MSD protocol. The encoding is as in [8, 147].

based picture this corresponds to layers of cluster states connected by long range CZ gates, which is what we denote as the graph state $|zMSD\rangle$ (see Figure 6.4). We will see that in order to achieve a good number of good enough T-states, these graph states are composed of a total of $O(log(n))$ qubits.

As before, moving to the logical version $|zMSD_L\rangle$ is the same as $|zMSD\rangle$, but with each qubit of $|zMSD\rangle$ replaced with a logical qubit which is a 4.8.8 triangular color code composed of $O(log^2(n))$ physical qubits, and the CZ gates between qubits of $|zMSD\rangle$ replaced by CZ_L gates (see Figure 6.4). The overhead of physical qubits per logical qubit needed to go from $|zMSD\rangle$ to $|zMSD_L\rangle$ is thus $O(log^2(n))$. Being of regular structure and having constant degree (each qubit is entangled to a constant number of qubits), the fault tolerant circuit to generate these states can be implemented in a constant number of rounds. Also, as with the construction of $|G_L\rangle$, error correction and detection is performed after every round, using the procedure of [8].

In MBQC local measurements drive the computation [30, 85]. In particular, a circuit is carried out by the correct choice of measurements on the associated graph state - in our case $|zMSD\rangle$. Normally these are done in an adaptive way, with the choice of measurements at any one time in the computation depending on previous results (see Section 2.3 in Chapter 2). In particular universality can be achieved by adaptive measurements on the 2D cluster states, with measurements at certain angles on the $X - Y$ equator. In our case, since we have injected the T-states, the circuit is all Clifford, so the measurements are only Pauli. Furthermore, in order to keep

time and depth resources low, we will not require corrections. A large part of our calculations in Section 6.4 is to show that this still provides enough good T-states for quantum speedup. Since the measurements are all Pauli, they can be also be done fault tolerantly, transversally, on the logical state [142].

In this way we then measure the non-output qubits of all the copies of $|zMSD_L\rangle$ non-adaptively at fixed angles either in the X_L, Y_L or Z_L bases, and we perform a classical error correction of the outcomes (because we assume faulty measurements), as in [8, 9]. Effectively, these non-adaptive measurements perform, for each of the $|zMSD_L\rangle$, z iterations of the magic state distillation (MSD) protocol of Theorem 4.1 in [7], up to random Pauli's which are due to the non-adaptivity of the measurements [30]. We keep only those copies where the MSD protocol was $successful$, that is, when the measurement results correspond to correct implementation of needed Clifford gates, and the obtaining of trivial MSD syndromes in the protocol of [7].

Finally, we entangle (using CZ_L gates) the output qubits of successful MSD protocols (i.e. the high fidelity logical T-states) onto $|G_L\rangle$ at precise positions (this can also be done in a constant number of rounds, see figure 6.2), and then measure non-adaptively all these output qubits, as well as the logical qubits of $|G_L\rangle$ at fixed X_L, Z_L or Y_L angles (which are transversaly local Pauli on the physical qubits). The position that the distilled logical T-states are attached is illustrated in Figure 6.2, filling from the side closes to the inputs. Once attached these are then measured in

X_L. When the distilled T-states are depleted by this process, we measure all the remaining qubits of $|G_L\rangle$ in the X_L basis, note however that all of these measurements are non-adaptive and therefore can be implemented simultaneously. These measurements provide the distributions which are our hard sampling problems. That is, we show that the output probabilities corresponding to measurement of qubits of $|G_L\rangle$ and the output qubits of successful MSD protocols are impossible to sample from classically efficiently, given widely-believed standard complexity theoretic conjectures are true [66, 149, 114, 3, 38]. Thus these output probabilities demonstrate a quantum speedup.

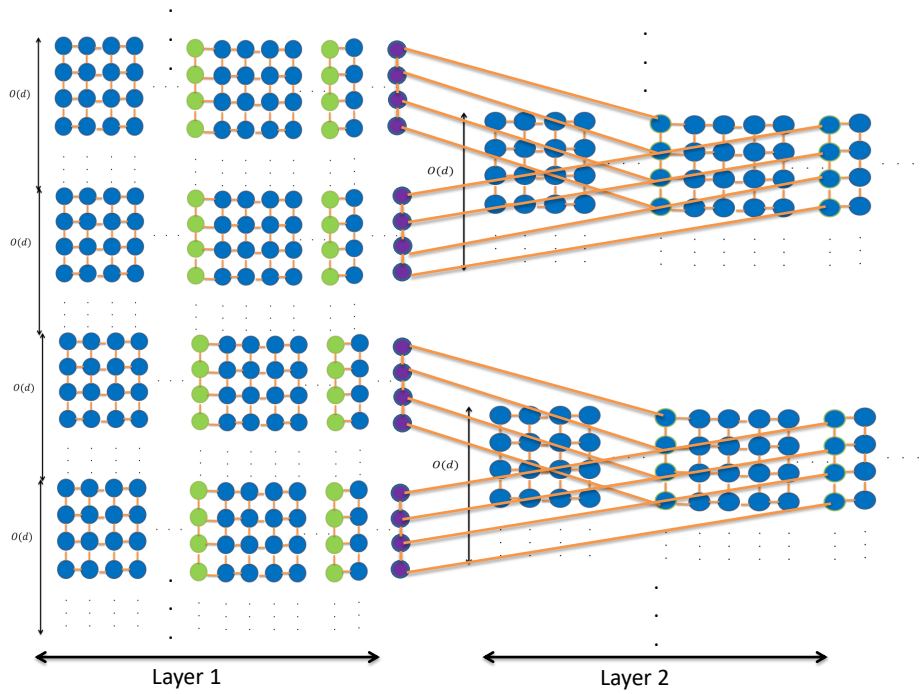

Figure 6.4: Part of the $|zMSD_L\rangle$ gadget showing $|1MSD_L\rangle$ states in the first layer, and $|1MSD_L\rangle$ states in the second layer of $|zMSD_L\rangle$. Each of the blue, green or purple filled circles is a logical qubit which is a 4.8.8 triangular 2D color code composed of $O(log^2(n))$ physical qubits (see main text). The green filled circles are encoded [8, 9] noisy input T-states of fidelity 1-ε which are injected at regular intervals onto the graph states $|1MSD_L\rangle$. The purple filled circles are the output qubits of $|1MSD_L\rangle$ which in the case where the MSD is succesful are T-states with fidelity 1-$O(\varepsilon^d)$ [7] (see main text). The vertical, horizontal, and curved orange lines are nearest-neighbor (straight orange lines) or long range (curved orange lines) CZ_L gates. The qubits of $|zMSD_L\rangle$ (blue, purple, and green filled circles) are measured non-adaptively at fixed X_L, Y_L, or Z_L angles in such a way as to, non-adaptively, implement multiple rounds of the MSD protocol of [7] (see main text).

6.3 Size Requirements of the Color Code

In this section we will find the size overheads of the color code needed for our architecture to show quantum speedup. To simplify things the overheads of the distillation part are treated separately in the next section. We will start by some notation. Let y be a bit-string representing the measurement results of all the physical qubits composing the non-output logical qubits of all the $k.n$ copies of $|zMSD_L\rangle$. Let x be a bit-string representing the measurement results of all the physical qubits composing the output logical qubits of *successful* MSD protocols (which are entangled onto $|G_L\rangle$), and of measurement results of the (physical) qubits composing the logical qubits of $|G_L\rangle$. $p^e(x, y)$ is taken to mean the probability of getting bit-string y and bit-string x. One can similarly define $p^e(x|y)$ to be the probability of getting bit-string x, conditioned on getting bit-string y. We will often be interested in *logical* bit strings representing the results of logical measurements. We define the probability $p^e(x_L, y_L)$ as

$$p^e(x_L, y_L) = \sum_{x \in S_{x_L}, y \in S_{y_L}} p^e(x, y), \tag{6.2}$$

where S_{x_L} (respectively S_{y_L}) is the set of bit strings x (respectively y) corresponding to the logical bit string x_L (respectively y_L). Also, we define $p^e(x_L|y_L)$ as

$$p^e(x_L|y_L) = \sum_{x \in S_{x_L}} p^e(x|y_L) = \sum_{x \in S_{x_L}} p^e(x|y \in S_{y_L}). \tag{6.3}$$

Let $\{p(x_L, y_L)\}$ be the output probabilities corresponding to the ideal case where the error correction and detection procedure in our sampling problem is $perfect$ (that is, the failure probability of the error detection and correction procedure is exactly zero). Similarly for $\{p(x, y)\}$ which is the distribution over physical qubit bit-strings corresponding to $\{p(x_L, y_L)\}$ (distributions over physical and logical bit-strings are related by Equations of the form of Equation (6.2)). Our strategy will be to calculate the size of the color code encoding a logical qubit such that the l_1-norm difference between these two distributions

$$\sum_{x_L, y_L} |p^e(x_L, y_L) - p(x_L, y_L)|, \tag{6.4}$$

tends asymptotically (in the $n \to \infty$ limit; n is the number of rows of $|G_L\rangle$) to zero. This will allow us in the coming sections to use $p(x_L, y_L)$ in our proof techniques, because it is simpler to do so. The hardness of the probabilities $\{p^e(x_L, y_L)\}$ of our sampling problem is then ensured (for large enough n) by the asymptotically vanishing l_1-norm of Equation (6.4).

A well known fact about Toric and color codes is that the failure probability p_{fail} (i.e the probability that the error detection and correction procedure performed fails to correct an error occuring in the code) decreases exponentially with the code size (that is, the number of physical qubits composing the code) when the error rate (i.e errors on physical qubits, the errors of preparations, gates, measurements,....) is below the threshold of fault-tolerant computing with the code [9, 8, 150]. This threshold has been calculated both analytically and numerically for the color code, and using

various general noise models [8, 9]. Given a color code of size m, the probability of success $p_{success} = 1 - p_{fail}$ is given by [150, 8, 9]

$$p_{success} \sim 1 - e^{-O(\sqrt{m})}. \tag{6.5}$$

As is commonly done, we will assume that the probabilities of failure or success of each code block (i.e each logical qubit) and over each round are independent. Because our construction consists of a constant number C of rounds, where after each round we perform an error detection and correction on each of the $O(k.n.O(log(n)) \leq poly(n)$ logical qubits of $|G_L\rangle$ and the $k.n$ copies of $|zMSD_L\rangle$, then we can write $p^e(x_L, y_L)$ as [3]

$$p^e(x_L, y_L) = (1 - e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}.p(x_L, y_L) + \sum_i p_i.p^{\tilde{e}_i}(x_L, y_L), \tag{6.6}$$

with

$$\sum_i p_i = 1 - (1 - e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))},$$

and where $\{p^{\tilde{e}_i}(x_L, y_L)\}$ represents a probability distribution corresponding to a sampling problem where a logical error e_i has occured, and which the error detection and correction procedure could not correct. This logical error could have occured in one or more rounds either in $|G_L\rangle$ or in the copies of $|zMSD_L\rangle$, and the probability of it occuring is denoted p_i. The first term in the RHS of Equation (6.6) represents the case where the error detection

[3] We have implicitly set the total number of error correction and detection procedures performed on all qubits of $|G_L\rangle$ and $|zMSD_L\rangle$ over all rounds as $CO(k.n.O(log(n) + C.k.n = C.O(k.n.O(log(n))$.

and correction procedure on all rounds was succesful, whereas the second part in the RHS represents the case where the procedure failed at least once. Replacing Equation (6.6) in the l_1-norm of Equation (6.4) we get

$$\sum_{x_L,y_L} |p^e(x_L,y_L) - p(x_L,y_L)| =$$
$$\sum_{x_L,y_L} |\big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big)p(x_L,y_L) + \sum_i p_i.p^{\tilde{e_i}}(x_L,y_L)| \leq$$
$$2\big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big), \quad (6.7)$$

where the rightmost part of Equation (6.7) is obtained by observing that

$$\sum_{x_L,y_L} |\big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big)p(x_L,y_L)$$
$$+\sum_i p_i.p^{\tilde{e_i}}(x_L,y_L)| \leq \sum_{x_L,y_L} |\big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big)p(x_L,y_L)|$$
$$+\sum_i p_i \sum_{x_L,y_L} p^{\tilde{e_i}}(x_L,y_L)$$
$$\leq \big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big) + \sum_i p_i$$
$$\leq 2\big(1-(1-e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big).$$

We now fix

$$m = r.log^2(n) = O(log^2(n)), \quad (6.8)$$

and we choose r is a positive constant chosen large enough so that the

following inequality holds

$$deg(e^{O(\sqrt{m})}) > deg(C.O(k.n.O(log(n))), \tag{6.9}$$

where $deg(.)$ represents the highest power of n contained in the expressions of $e^{O(\sqrt{m})}$ and
$C.O(k.n.O(log(n))$. We can now use (for large enough n) the approximation

$$2\big(1 - (1 - e^{-O(\sqrt{m})})^{C.O(k.n.O(log(n))}\big) \sim 2e^{-O(\sqrt{m})}.C.O(k.n.O(log(n)).$$

Plugging this approximation together with the value of m (Equation (6.8)) in Equation (6.7), we obtain

$$\sum_{x_L, y_L} |p^e(x_L, y_L) - p(x_L, y_L)| \leq O(\frac{1}{n^g}), \tag{6.10}$$

where

$$g = deg(e^{O(\sqrt{m})}) - deg(C.O(k.n.O(log(n))) > 0.$$

Equation (6.10) means that our sampling distribution $\{p^e(x_L, y_L)\}$ approaches the distribution with perfect error correction procedure $\{p(x_L, y_L)\}$ in the $n \to \infty$ limit, when the size of the color code encoding a single logical qubit scales as $O(log^2(n))$. Thus, Equation (6.10) allows us to shift back and forth between the distributions $\{p(x_L, y_L)\}$ and $\{p^e(x_L, y_L)\}$, and guarantees the hardness of one, given the hardness of the other (for large enough n). In the coming sections, we will work with the distribution $\{p(x_L, y_L)\}$ which is easier to manipulate using our techniques, and we will shift back to

$\{p^e(x_L, y_L)\}$ when needed by using Equation (6.10) and a triangle inequality.

6.4 Size Requirements for $|zMSD_L\rangle$

In this section we find the required size of the states $|zMSD_L\rangle$ used for the distillation of the T-states in order to show quanutm speedup. As explained in Section 6.2 the state $|zMSD_L\rangle$, along with the described injections of noisy T-state, effectively implements the distillation circutis of Theorem 4.1 in [7] in MBQC. In MBQC, however, feedforward measurements are required. In this work we do not do feedforward for this part, and measurements are done non-adaptively, which means that only certain measurement outcomes will be guaranteed to give a good implementation of the distillation circuit. Furthermore, the distillation circuits [7] themselves contain syndrome measurements, and good distillation is only guaranteed upon the correct syndrome measurement within the circuit (these, however occur with high probability). We say that the MSD was $succesful$ when we obtain such measurement results for a given copy of $|zMSD_L\rangle$. The goal in this section will be to calculate the number of qubits of $|zMSD_L\rangle$ which will guarantee a sufficient fidelity, and a sufficient supply of output T-states with high fidelity (succesful MSD outputs) to ensure hardness of classical simulability of our model.

We will begin by calculating the number of qubits of $|1MSD_L\rangle$. In Theorem 4.1 in [7], the MSD circuit consists of $O(d)$ qubits, where d is a positive integer, uses $O(d^2)$ noisy input T-states with fidelity 1-ε with respect to an ideal (noiseless) T-state, and outputs $O(d)$ distilled magic states with fi-

delity 1-$O(\varepsilon^d)$ with respect to an ideal T-state. Each time a noisy T-state is inserted it affects a noisy T-gate, inducing a so-called T-gate depth [7]. The depth of the entire circuit is $O(d^2.log(d))$, where $O(d)$ is the T-gate depth, and $O(d.log(d))$ is the depth of an encoding Clifford circuit of the protocol, which is composed of long-range Cliffords [7]. Therefor, the MSD circuit is an $O(d)$-qubit circuit of depth $O(d^2.log(d))$. For implementations in MBQC, one must transform the Clifford circuit composed of long range gates, to that composed of nearest neighbor and single qubit Clifford gates, since these single qubit and nearest neighbor two-qubit gates can be implemented by measuring $O(1)$ qubits in MBQC [30, 85]. An arbitrary m-qubit Clifford unitary can be implemented in depth $O(m^2)$ by a circuit composed of $\{CNOT_{i,j}; H_i; Z_i(\frac{\pi}{2})\}_{i,j\in\{1,\ldots,m\}}$ [151, 152], where H_i and $Z_i(\frac{\pi}{2})$ are the single qubit Hadamard and $\pi/2$ phase gates, which can be implemented by Pauli X_L, Y_L, and Z_L measurements on $O(1)$ qubits in a cluster state [30, 85]. $CNOT_{i,j}$ is a long range controlled not acting on qubits i and j which can be implemented on a cluster state in depth $O(i-j) \leq O(d)$ by using nearest neighbor CNOT's (each of which can be implemented using $O(1)$ qubits on a cluster state [30, 85]) [87]. $m = O(d)$ in our case, thus the number of columns of $|1MSD_L\rangle$ is

$$n_c = O(d^2 log(d)).O(d^2).O(d) = O(d^5 log(d)), \tag{6.11}$$

where the $O(d^2 log(d))$ comes from the depth of the MSD circuit with long range Cliffords, $O(d^2)$ is the depth needed to implement an arbitrary Clifford using Hadamards, phase gates, and long range CNOT's, and the $O(d)$ is an

overestimate and represents the number of nearest neighbor CNOT's needed to give a long range CNOT. The total number of qubits of $|1MSD_L\rangle$ is then

$$n_T = O(d).n_c = O(d^6.log(d)). \tag{6.12}$$

Now we will calculate the required number of qubits of $|zMSD_L\rangle$. As noted in Section 6.2, one can think of $|zMSD_L\rangle$ as composed of z *layers* of multiple $|1MSD_L\rangle$ states connected together by long range CZ_L gates (this is in order to transport the output T-states of layer j onto different positions in layer $j+1$ where they will be used as inputs, see Figure 6.4), with each of these $|1MSD_L\rangle$'s composed of $n_T = O(d^6 log(d))$ logical qubits, and upon non-adaptive measurement effectively implementing one round of MSD, up to random Paulis.

Let us suppose the first layer is composed of N $|1MSD_L\rangle$ states (with $N.O(d^2)$ noisy input T-states encoded [8, 147] onto the qubits of each of the $|1MSD_L\rangle$ states at precise positions), and this layer outputs, upon measurement and in the case the MSD on each $|1MSD\rangle$ states are successful, $N.O(d) = \frac{N}{d}.O(d^2)$ distilled T-states with fidelity $1 - O(\varepsilon^d)$ (or output error $O(\varepsilon^d) = C.\varepsilon^d$, where C is a positive constant [7]. These distilled T-states will be used as noisy T-state inputs in the next layer, which is composed of $\frac{N}{d}$ $|1MSD\rangle$'s, and which will output, when the MSD is succesful as above, $\frac{N}{d}.O(d) = \frac{N}{d^2}.O(d^2)$ distilled T-states with output error $C.(C.\varepsilon^d)^d = C^{d+1}.\varepsilon^{d^2}$. [4] Similarly, the zth layer will consist of $\frac{N}{d^{z-1}}$

[4] In the protocol of Theorem 4.1 in [7], we have that for large enough d the ratio of (noisy) input magic states to (distilled) output magic states is $\sim d$, since $\gamma \to 1$ asymptotically (see Section 6.7) [7]. This is what allowed us to say that $N.O(d) = \frac{N}{d}.O(d^2)$,

$|1MSD\rangle$'s, and will output, upon successful measurements, $\frac{N}{d^{z-1}}.O(d)$ T-states with output error (for d large enough)

$$\varepsilon_{out} \sim C^{d^{z-1}}.\varepsilon^{d^z}. \tag{6.13}$$

The total number of qubits of $|zMSD_L\rangle$ is then given by

$$n_{NMSD} = (N + \frac{N}{d} + \frac{N}{d^2} + ...).n_T = O(N). \tag{6.14}$$

We choose z to be the last layer, therefore $\frac{N}{d^{z-1}} = 1$ and thus

$$N = d^{z-1}. \tag{6.15}$$

In summary, if we have a $|zMSD_L\rangle$ which is made up of taking z rounds starting with $NO(d^2)$ T-states with noise ε, we obtain (when the MSD is succesful) $O(d)$ output T-states state with noise ε_{out} (Equation (6.13)).

In what remains of this section, we will show how to choose z and N as a function of n (the number of rows of $|G_L\rangle$), such that the final round outputs (upon a succesful MSD of $|zMSD_L\rangle$) $O(d)$ T-states with error ε_{out} sufficiently small so as to demonstrate quantum speedup of our problem. We will calculate N such that the following condition, which will be justified in

meaning that N groups of $O(d)$ distilled outputs, can be thought of as $\frac{N}{d}$ groups of $O(d^2)$ inputs (for the next layer), with $O(d^2)/O(d) = d$.

Section 6.4 and 6.5, holds for all bit strings y

$$\sum_x |p(x|y) - p^{id}(x|y)| \leq c, \tag{6.16}$$

where c is an arbitrarily small constant, $p(x|y) = p(x,y)/\sum_x p(x,y)$, $p_y := \sum_x p(x,y)$, and $\{p(x,y)\}$ is as defined in Section 6.2. $p^{id}(x|y)$ is defined similarly to $p(x|y)$, with the exception that the T-states entangled onto $|G_L\rangle$ are ideal (noiseless), as opposed to the case of $p(x|y)$ where the injected T-states are the output qubits of $|zMSD_L\rangle$. Note that this implies the same for the logical version of Equation (6.16), for all bit strings y_L

$$\sum_{x_L} |p(x_L|y_L) - p^{id}(x_L|y_L)| \leq \sum_x |p(x|y) - p^{id}(x|y)| \leq c. \tag{6.17}$$

Indeed, Equation (6.17) can be found directly by using Equation (6.3) in the LHS of Equation (6.17), then using a triangle inequality.

Now, remember that in our construction we use $k.n$ copies of $|zMSD_L\rangle$. Supposing that we obtain l copies of $|zMSD_L\rangle$ are succesful (i.e that $l.O(d) = O(l)$ output T-states with error ε_{out} were entangled with the qubits of $|G_L\rangle$), then $p(x|y)$ and $p^{id}(x|y)$ are given by

$$p(x|y) = \langle x|\rho_l|x\rangle, \tag{6.18}$$

with

$$\rho_l :=$$
$$CZ_T \otimes_{i=1,\ldots,O(l)} \left((1-\varepsilon_{out})|T_L\rangle_i\langle T_L|_i + \varepsilon_{out}.\eta_i\right) \otimes |G_L\rangle\langle G_L| CZ_T, \quad (6.19)$$

where $CZ_T = \prod_{\{i,j\}\in E_T} CZ_{L_{i,j}}$ represents the controlled Z gates needed for entangling all the output T-states with the qubits of $|G_L\rangle$, E_T is the set of all pairs of logical qubits $\{i,j\}$ where i is an output qubit of a successful MSD protocol in the state $(1-\varepsilon_{out})|T_L\rangle\langle T_L|_i + \varepsilon_{out}.\eta_i$ which is entangled with qubit j of $|G_L\rangle$. $CZ_{Li,j}$ acts as the identity on all but qubits i and j. Also

$$p^{id}(x|y) = \langle x|CZ_T\Big(\big(\otimes_{i=1,\ldots,O(l)}\,|T_L\rangle_i\langle T_L|_i\big) \otimes |G_L\rangle\langle G_L|\Big)CZ_T|x\rangle, \quad (6.20)$$

where ε_{out} and $|T_L\rangle$ are as defined in Equations (6.13) and (6.1), η_i is an arbitrary one qubit state. Note that the value of y is largely fixed by the fact it there are l $succesful$ MSD outputs. strictly speaking the places where i appear here, depend on y as do the possbile strings for the unsuceesful MSD, but we do not include them in Equation (6.20) for ease of reading.

A standard relation linking the probabilities $p(x|y)$ and $p^{id}(x|y)$ and the fidelity $F(\rho_l, \rho_l^{id})$ between ρ_l (Equation (6.19)) and

$$\rho_l^{id} = CZ_T\big(\otimes_{i=1,\ldots,O(l)}\,|T_L\rangle_i\langle T_L|_i\big) \otimes |G_L\rangle\langle G_L| CZ_T, \quad (6.21)$$

is given by [37]

$$\sum_x |p(x|y) - p^{id}(x|y)| \leq 2\sqrt{1 - F^2(\rho_l, \rho_l^{id})}. \tag{6.22}$$

From Equations (6.19) and (6.21) we have

$$F(\rho_l, \rho_l^{id}) \geq (1 - \varepsilon_{out})^{O(l)}. \tag{6.23}$$

Using Equations (6.16), (6.22), and (6.23) we can set

$$2\sqrt{1 - (1 - \varepsilon_{out})^{O(l)}} \leq c. \tag{6.24}$$

Requiring Equation (6.24) to hold for the maximum value of l, $l_{max} = k.n$ (we do this is so that Equation (6.24) holds for l_{max} which gives a maximal value of $2\sqrt{1 - F^2}$, thus it will also hold for all $l \leq l_{max}$. This will be needed in our hardness proof in Section 6.6.), which corresponds to the case where we obtain succesful MSD on all of the $k.n$ copies of $|zMSD_L\rangle$ we created, and using the approximation $(1 - \varepsilon_{out})^{O(l)} \sim 1 - O(l).\varepsilon_{out}$ we obtain

$$\varepsilon_{out} \leq O(\frac{1}{k.n}) \leq O(\frac{1}{poly(n)}). \tag{6.25}$$

Using the expression of ε_{out} in Equation (6.13), we get, for big enough n [5],

[5] From Equations (6.13) and (6.25), $C^{d^{z-1}}.\varepsilon^{d^z} \leq O(1/poly(n))$. Taking the logarithm of both sides and rearranging we get $d^z.log(C\varepsilon^d) \lesssim -O(log(poly(n)) \sim -O(deg(poly(n)).log(n)) = -O(log(n))$ for large enough n, where $deg(poly(n))$ is the value of the highest power of n in $poly(n)$. Equation (6.26) follows from observing that $C.\varepsilon^d < 1$ [7].

that

$$d^z \geq O(log(n)). \tag{6.26}$$

Replacing Equation (6.26) in Equation (6.15), we have

$$N \geq O(log(n)). \tag{6.27}$$

The success probability p_{succ}, which is the probability that $|zMSD_L\rangle$ will output magic states with error probability ε_{out} when measured non-adaptively, is given by

$$p_{succ} \geq \frac{1}{2^{n_{NMSD}}}, \tag{6.28}$$

where n_{NMSD} is given by Equation (6.14) [6]. For small enough constant (independent of n) [7] ε , we have

$$p_{succ} \geq \frac{1}{n}. \tag{6.29}$$

Now we want to calculate $p_{totfail}$, which is the probability of getting more

[6] Indeed, there is at least one string S of measurement results which corresponds to a successful distillation protocol. The total number of possible measurement strings corresponding to measurements of qubits of $|zMSD_L\rangle$ is $\leq 2^{n_{NMSD}}$. Also, given a measurement of a particular qubit of $|zMSD_L\rangle$, the probability that this measurement result is successful (that is, the measurement result corresponds to a bit of S) is $\geq 1/2$, since this bit either corresponds to the successful implementation of a Clifford, which occurs with probability 1/2 as in usual MBQC, or it is a bit of the trivial measurement syndrome which one usually post-selects on in MSD routines, this bit appears with probability close to one [7]. The lower bound in Equation (6.28) follows straightforwardly from these observations.

[7] Indeed, choosing $\varepsilon_{out} = \frac{1}{n^\beta}$, with β a positive constant chosen so that Equation (6.25) is verified, then using the expression of ε_{out} in Equation (6.13), we get $d^z = \frac{\beta.d.log(n)}{log(1/C.\varepsilon^d)}$. Replacing this in Equation (6.14) we obtain $n_{NMSD} = \gamma.\frac{\beta.d.log(n)}{log(1/C.\varepsilon^d)}$, with γ a positive constant. Equation (6.29) follows directly by choosing $\varepsilon = \frac{e^{-\gamma.\beta}}{C^{1/d}}$.

than $l_{max} - k_1.(n-1) = k.n - k_1.(n-1)$ failures out of $l_{max} = k.n$ copies of $|zMSD_L\rangle$ measured (which translates to getting less than k_1 B gadgets per row pair of $|G_L\rangle$). The calculation of $p_{totfail}$ is performed in Section 6.6.2. Choosing k such that

$$\frac{k.n}{k_1.(n-1)} \geq O(n.log(n)). \tag{6.30}$$

one obtains

$$\lim_{n\to\infty} p_{totfail} = 0. \tag{6.31}$$

Equation (6.31) is derived in the Section 6.6.2

To summarize, for $|G_L\rangle$ which is composed of $k = poly(n)$ columns (with k chosen such that Equation (6.30)) holds) and n rows, creating $k.n$ copies of $|zMSD_L\rangle$, encoding $N.O(d^2)$ noisy input T-states onto the qubits of each of these copies, and measuring the non-output qubits of each of these copies non-adaptively at fixed X_L, Y_L or Z_L [8], one is guaranteed almost surely for high enough n to get at least $k_1.(n-1) = poly(n)$ successful instances of distillation, and therefore be able to implement, by entanglement of output T-states of successful instances onto qubits of $|G_L\rangle$, followed by measurement these output states and of qubits of $|G_L\rangle$ non-adaptively and at fixed Pauli angles, a quantum circuit composed of at least k_1 B gadgets per each row

[8] Note that these Z_L measurements are harmless, since when executed the graph we obtain still has gflow [86] (see Figure 6.2), meaning that we still obtain, after non-adaptively measuring at X_L, Y_L, and Z_L, random unitary ensembles of the same form as those in Chapters 3 and 4, by arguments of [88].

pair. The significance of this last statement will be made clear in the next section.

Finally, we emphasize that it is the choice of distillation protocol of [7] which allowed Equations like (6.27) and (6.29) to hold. Indeed, choosing other MSD protocols may not lead to desired results. More about this is to be said in Section 6.7.

6.5 Approach to Our Proof of Hardness

Our proof of hardness of approximately classically sampling will be based on the standard technique of applying Stockmeyer's theorem [113], and Toda's theorem [117], along with an average-case hardness conjecture inspired from worst-case hardness of our problem [114, 33, 38, 25, 26, 94]. The proof technique will be essentially the same as that in Chapter 4 (see also Chapter 2 for an overview of this type of proof), but there are additional details such as a different proof for anti-concentration (see Section 6.6.1), and shifting between the probability distribution $\{p^e(x,y)\}$ and $\{p(x,y)\}$ which will be described below, in addition to several technicalities in the calculations which we perform in Section 6.6.

We will prove that the probability distribution $\{p^e(x_L,y_L)\}$ (see Section 6.3) cannot be sampled from efficiently classically, assuming two complexity theoretic conjectures hold. This is (to date) the minimal possible number of conjectures one can make in these types of proofs. In our proof, we will use Equation (6.10) to transform the sampling problem from sampling over $\{p^e(x_L,y_L)\}$, to sampling over $\{p(x_L,y_L)\}$, which is easier to manipulate in

our proofs. This is feasible because the difference between these two distributions vanishes in the limit of large n. This will allow us to make statements along the lines of : If sampling from $\{p(x_L, y_L)\}$ is hard to do classically up to l_1-norm error c_1 (where c_1 is a positive constant). Then for large enough $n \geq n_f$, where n_f is an appropriately large integer, sampling from $\{p^e(x_L, y_L)\}$ up to l_1-norm error $c_1 - \frac{1}{D} > 0$ where D is a positive constant is also hard to do classically, since this sampling implies the previous one by using a triangle inequality and Equation (6.10).

In our proofs also, there are many non-trivial subtleties which need to be dealt with. The first of these is that measuring the copies of $|zMSD_L\rangle$ and then using only the outputs of the succesfull ones to entangle with qubits of $|G_L\rangle$ *reveals* to the sampler which instances (with respect to the measurement of the non-output qubits in $|zMSD_L\rangle$) are hard ($\sharp$ P) to approximate. This was not a problem in previous works where single round non-adaptive measurements led to a *hiding* of these hard to approximate instances [25, 38, 26, 94].

To illustrate, let us partition the set of bit-strings $\{y\}$ into $\{y\}_{hard}$ and $\{y\}_{easy}$. $\{y\}_{hard}$ represent the instances of y bit-strings characterized by a sufficient amount of T-states with output error ε_{out}. By sufficient, we mean a number of T-states which when injected onto $|G_L\rangle$ will lead to probabilities $p(x|y)$ which are worst-case hard to approximate up to relative error $1/4 + \mathrm{O}(1)$. The probabilities $p(x|y)$ are in this case the outputs of quantum circuits, where these circuits are universal under post-selection [66, 149] (that is, the probabilities $p(x|y)$ can be used to calculate the post-selected probabilities [66]). On the contrary, $\{y\}_{easy}$ represent the instances of bit-strings

y which are characterized by a number of T-states which is not sufficient for universality under post-selection, and therfore it is expected that the $p(x|y)$ are efficiently approximately classically samplable in this case. In principle, by looking at a bit string $\{y\}$ one can directly determine whether it belongs to $\{y\}_{hard}$ or $\{y\}_{easy}$. Indeed, a succesful MSD protocol is usually characterized by a copy of $|zMSD_L\rangle$ where the logical MBQC measurement binaries [30] are all zero's, indicating a correct implementation of Cliffords of the MSD circuit and the obtaining of trivial syndromes. Thus, the sampler knows before hand which $p(x|y)$ are worst-case hard to approximate, they are simply those where $y \in \{y\}_{hard}$. If the *contribution* of these hard instances is negligible, that is, if

$$\lim_{n\to\infty} \sum_{y\in\{y\}_{hard}} p_y = 0, \tag{6.32}$$

where $p_y = \sum_x p(x,y)$, then the sampler can simply sample $p(x|y)$ where $y \in \{y\}_{hard}$ using some arbitrary efficiently classically computable probability distribution, then sample accurately from the $p(x|y)$ where $y \in \{y\}_{easy}$, and one would have sampled in this case from our distribution classically efficiently up to a given constant l_1-norm error. Equation (6.31) shows that we have avoided this scenario, since the contribution of the hard instances in our case cannot be neglected. Indeed, $p_{totfail}$ can be written as

$$p_{totfail} = 1 - \sum_{y\in\{y\}_{hard}} p_y. \tag{6.33}$$

Therefore, in our case we have, from Equations (6.31) and (6.33) that

$$\lim_{n\to\infty} \sum_{y\in\{y\}_{hard}} p_y = 1. \tag{6.34}$$

Although, it should be noted that in our case we have underestimated the number of hard instances, since one can expect hard instances with less that $k_1 = poly(n)$ B gadgets per row pair (as in our case), however these underestimated cases can only add positive values to $\sum_{y\in\{y\}_{hard}} p_y$, and therefore Equation (6.34) remains true.

Another subtlety arises when looking at $p(x|y)$. These probabilities are the outputs of quantum circuits with noisy T-gates, with noise rate given by ε_{out} (Equation (6.13)). How can one be sure that these probabilities are not efficiently samplable from classically? The condition imposed by Equations (6.16) and (6.17) ensures that the probabilities $p(x|y)$ are indeed hard to sample from classically. Since, as will be seen in the next section, we will use Equation (6.17) and to $transform$ our sampling problem from a sampling of probabilities $p(x|y)$, to a sampling of probabilities $p^{id}(x|y)$ which are definitely hard to sample from classically [36, 38, 66, 149].

The last point we would like to address in this section is more an ambiguity rather than a problem. It concerns the values of k and k_1. We will use a value of $k_1 \geq O(n)$, and that of k which verifies Equation (6.30). The reason we chose this particular value of k_1 is because we will need it to prove the anti-concentration property [26, 27] of $p^{id}(x|y)$, which is a technical ingredient needed in our proof in the next section. The anti-concentration property relevant to our case will be proven in Section 6.6.1. We will use

results from [36, 26, 27] to prove it.

6.6 Proof of Hardness of Classical Simulability

In this section we prove that our architecture gives quantum speedup. Assume that the error rates of individual qubits, preparations, two qubit gates, and measurements are below the threshold of fault-tolerant computing with the color code [8, 9]. More precisely, the error rate er must verify $er \leq min(\varepsilon_{th}, \frac{e^{-\gamma.\beta}}{C^{1/d}})$ ($min(f, g)$ being the minimum of two values f and g), where ε_{th} is the threshold for fault-tolerant computing with the color code [8], and $\frac{e^{-\gamma.\beta}}{C^{1/d}}$ is the value of the error rate on the noisy input T-states (calculated in footnote 7) so that we can get a p_{succ} of the form of Equation (6.29). Also, assume that each logical qubit of $|G_L\rangle$ and $|zMSD_L\rangle$ is a 4.8.8 2D triangular color code of size $O(log^2(n))$. Suppose a classical $poly(n)$ time algorithm C can sample from a probability distribution $\{p_c(x_L, y_L)\}$ approximating $\{p^e(x_L, y_L)\}$ to l_1-norm error $\mu - \frac{1}{D} > 0$, where μ and D are positive constants. That is,

$$\sum_{x_L, y_L} |p_c(x_L, y_L) - p^e(x_L, y_L)| \leq \mu - \frac{1}{D}. \tag{6.35}$$

Using Equation (6.10) and a triangle inequality, we have

$$\sum_{x_L, y_L} |p_c(x_L, y_L) - p(x_L, y_L)| \leq \sum_{x_L, y_L} |p_c(x_L, y_L) - p^e(x_L, y_L)| + \frac{u}{n^g},$$

where u is a positive constant. For $n \geq n_f$, where n_f is a positive integer chosen so that $n_f^g/u \geq D$. Replacing Equation (6.35) in the above Equation,

one obtains

$$\sum_{x_L,y_L} |p_c(x_L,y_L) - p(x_L,y_L)| \leq \mu. \tag{6.36}$$

We will show that the existence of such a classical algorithm is highly unlikely, based on widely believed complexity theoretic conjectures, which is the standard method in proving quantum speedup [33, 38, 27, 25, 26, 94]. The complexity theoretic conjectures we will rely on are the following.

Conjecture 1. *The polynomial Heirarchy (PH) does not collapse to its third level [132].*

We will also rely on the following average-case conjecture, the likes of which is present in the usual proofs of hardness [33, 38, 27, 25, 26, 94].

Conjecture 2. *Approximating the probabilities $p^{id}(x_L|y_L)$ for a given $y_L \in \{y_L\}_{hard}$ up to relative error 1/4 + O(1) for a constant fraction γ of the $p^{id}(x_L|y_L)$ is as hard as worst-case, and thus $\sharp$P-hard.*

Here $\{y_L\}_{hard}$ is the set of logical bit-strings y_L giving rise to a hard instance. By hard instance we mean an instance where a number of T-states $\geq O(k_1)$ with error ε_{out} are entangled onto qubits of $|G_L\rangle$ so that we get at least k_1 B gadgets applied per each row pair of $|G_L\rangle$, $i \in \{1,..,n-1\}$. [9] We will also use the following anti-concentration property [26, 27] which we can show holds when $k_1 \geq O(n)$. We will prove this property in Section 6.6.1.

[9] Again, we emphasize that we underestimate the number of hard instances, since one would expect that there are hard instances with less than k_1 B gadgets per row pair of $|G_L\rangle$.

Theorem 10. *For a given* $y_L \in \{y_L\}_{hard}$

$$pr_{x_L}\left(p^{id}(x_L|y_L) \geq \frac{\alpha}{2^{k.n+O(l)}}\right) \geq \beta. \tag{6.37}$$

α *and* $0 < \beta \leq 1$ *are positive constants,* $2^{k.n+O(l)}$ *is the number of bit-strings* x_L*.*

In the rest of this section, we will prove the following theorem which shows quantum speedup of our sampling problem.

Theorem 11. *Assume that the error rates of individual qubits, preparations, two qubit gates, and measurements verify the conditions stated at the beginning of this section. Then there exists positive constants* μ*,* D*, and* c *such that, assuming Conjecture 1 and 2 are true, there is no poly*(n) *time classical algorithm* C *which can sample from the probability distribution* $\{p^e(x_L, y_L)\}$ *up to* l_1*-norm error* $\mu - \frac{1}{D}$ *(see Equation (6.35)).*

We now go on to prove Theorem 11, by starting with the sampling problem of Equation (6.36). Since if we can prove that this sampling is hard to do classically, then it also implies that the sampling problem in Theorem 11 is also hard to do classically, by the arguments in Section 6.5 and the beginning of this section.

Equation (6.34) implies [10] that $\exists$ integer n_o, and a constant $0 < \zeta \leq 1$ such that $\forall\ n \geq n_o > n_f$

$$\sum_{y_L \in \{y_L\}_{hard}} p_{y_L} \geq \zeta. \tag{6.38}$$

[10] Note that $\sum_{y \in \{y\}_{hard}} p_y = \sum_{y_L \in \{y_L\}_{hard}} p_{y_L}$.

$p_{y_L} = \sum_{x_L} p(x_L, y_L)$. Equation (6.36) implies

$$\sum_{y_L \in \{y_L\}_{hard}} p_{y_L} \sum_{x_L} |\frac{p_c(x_L, y_L)}{p_{y_L}} - p(x_L|y_L)| \leq \mu. \tag{6.39}$$

Plugging Equation (6.38) in Equation (6.39) gives

$$\sum_{x_L} |\frac{p_c(x_L, y_L)}{p_{y_L}} - p(x_L|y_L)|_{min} \leq \frac{\mu}{\zeta}. \tag{6.40}$$

$\sum_{x_L} |\frac{p_c(x_L, y_L)}{p_{y_L}} - p(x_L|y_L)|_{min}$ meaning the minimum value of $\sum_{x_L} |\frac{p_c(x_L, y_L)}{p_{y_L}} - p(x_L|y_L)|$, where $y_L \in \{y_L\}_{hard}$. Equivalently, Equation (6.40) can be expressed as Corollary

Corollary 7. *$\exists\ y_L \in \{y_L\}_{hard}$ such that*

$$\sum_{x_L} |\frac{p_c(x_L, y_L)}{p_{y_L}} - p(x_L|y_L)| \leq \frac{\mu}{\zeta}. \tag{6.41}$$

Corollary 7 and Equation (6.17) imply, by using a triangle inequality [11],

$$\sum_{x_L} |p_c(x_L, y_L) - p^{id}(x_L, y_L)| \leq (\frac{\mu}{\zeta} + c) p_{y_L}. \tag{6.42}$$

Let $\mu' = \frac{\mu}{\zeta} + c$. Applying Stockmeyer's theorem [113] to the probabilities of Equation (6.42), and a triangle inequality [25] we get that there is an algorithm in the third level of the PH producing an approximation $\tilde{p}_c(x_L, y_L)$

[11] $p^{id}(x_L, y_L) = p_{y_L}.p^{id}(x_L|y_L)$.

of $p^{id}(x_L, y_L)$ such that

$$|\tilde{p}_c(x_L, y_L) - p^{id}(x_L, y_L)| \leq \frac{p^{id}(x_L, y_L)}{poly(n)} + |p_c(x_L, y_L) - p^{id}(x_L, y_L)|(1 + \frac{1}{poly(n)}). \quad (6.43)$$

Summing over x_L on both sides of (6.43), then using Equation (6.42), and the fact that $\tilde{p}_c(y_L) = \sum_{x_L} \tilde{p}_c(x_L, y_L)$ we get that

$$1 - \mu^{'} < \frac{\tilde{p}_c(y_L)}{p_{y_L}} < 1 + \mu^{'}. \quad (6.44)$$

Choosing $\mu^{'}$ (and thus μ and c) to be small enough, one has

$$\frac{\tilde{p}_c(y_L)}{p_{y_L}} \sim 1. \quad (6.45)$$

Dividing Equation (6.43) by p_{y_L} , then using Equation (6.45) we obtain

$$|\tilde{p}_c(x_L|y_L) - p^{id}(x_L|y_L)| \leq \frac{p^{id}(x_L|y_L)}{poly(n)} + \frac{|p_c(x_L, y_L) - p^{id}(x_L, y_L)|}{p_{y_L}}(1 + \frac{1}{poly(n)}). \quad (6.46)$$

Using Equation (6.42) and Markov's Inequality, we get that for $0 < \delta \leq 1$

$$Pr_{x_L}(\frac{|p_c(x_L, y_L) - p^{id}(x_L, y_L)|}{p_{y_L}} \leq \frac{\mu^{'}}{\delta.2^{k.n+O(l)}}) \geq 1 - \delta. \quad (6.47)$$

with Pr_{x_L} being the probability over the uniform choice of x_L. Replacing Equation (6.47) in Equation (6.46) we get the following Equation which

holds with probability at least $1-\delta$

$$|\tilde{p}_c(x_L|y_L) - p^{id}(x_L|y_L)| \leq \frac{p^{id}(x_L|y_L)}{poly(n)} + \frac{\mu^{'}}{\delta.2^{k.n+O(l)}}. \tag{6.48}$$

Again, we emphasize that in Equation (6.48) $y_L \in \{y_L\}_{hard}$, by Corollary 7.Now, using the anti-concentration property (Theorem 10) in Equation (6.48) we get the following equation which we assume holds with probability $\beta.(1-\delta)$, by similar arguments as in [26, 25, 94, 114]

$$|\tilde{p}_c(x_L|y_L) - p^{id}(x_L|y_L)| \leq (O(1) + \frac{\mu^{'}}{\delta.\alpha})p^{id}(x_L|y_L). \tag{6.49}$$

Choosing μ, c such that $\frac{\mu^{'}}{\delta.\alpha} \leq \frac{1}{4}$, Equation (6.49) means that an algorithm in the 3rd level of the PH can approximate the probabilities $\{p^{id}(x_L|y_L)\}$ for a $y_L \in \{y_L\}_{hard}$ up to relative error 1/4+O(1). This means by Conjecture 2 and Toda's theorem [117] that the PH has collapsed to its third level, which is impossible by Conjecture 1. This concludes our proof of Theorem 11.

6.6.1 Proof of Theorem 10

In this subsection we prove Theorem 10. First off, suppose that we get l succesful $|zMSD_L\rangle$ measurement instances, or equivalently $O(l) = O(d^2).l$ $|T_L\rangle$ states with output error ε_{out} (Equation (6.13)). We will suppose, so that we get $y_L \in \{y_L\}_{hard}$, that we have obtained at least k_1 (successive) B gadgets per row pair $(i, i+1)$, $i \in \{1, .., n-1\}$, with $k_1 \geq O(n)$.

We can write

$$p(x_L|y_L) = \frac{1}{2^{kn+O(l)-n}}|\langle x_L^{out}|U_j.V_i|x_L^{out}\rangle|^2, \tag{6.50}$$

where x_L^{out} is a bit-string representing the measurement results of qubits of the rightmost column of $|G_L\rangle$. U_j is a random unitary which is applied to the qubits of the rightmost column of $|G_L\rangle$ after measuring the first k_1 columns of $|G_L\rangle$, and V_i a unitary applied to these qubits after measuring the remaining $k - k_1 - 1$ columns, $j \in \{1, ..., 2^{k_1.n+O(l)}\}$, $i \in \{1, ..., 2^{(k-k_1-1).n}\}$.

Sampling from the uniform distribution over $\{U_j\}_{j\in\{1,...,2^{k_1.n+O(l)}\}}$ effectively samples from an approximate unitary 2-design [29], since as mentioned earlier, these unitaries are products n-qubit unitaries of length $k_1 \geq O(n)$ composed of two-qubit unitaries chosen from a set which is universal on $U(4)$ and contains inverses, as seen in Chapter 3 [6, 36]. For a given fixed $i \in \{1, ..., 2^{(k-k_1-1).n}\}$, the uniform distribution $\frac{1}{2^{k_1.n+O(l)}}$ over $\{V_i.U_j\}_{j\in\{1,...,2^{k_1.n+O(l)}\}}$ is also an approximate unitary 2-design , which means it satisfies the following anti-concentration property [27, 26]

$$Pr_U(|\langle x_L^{out}|U_j.V_i|x_L^{out}\rangle|^2 \geq \frac{\alpha_i}{2^n}) \geq \beta_i, \tag{6.51}$$

where α_i and $\beta_i \leq 1$ are positive constants independent of n, and Pr_U is taken to mean the probability over the choice of $U_j.V_i$ with uniform probability from $\{V_i.U_j\}_{j\in\{1,...,2^{k_1.n+O(l)}\}}$. Equation (6.51) shows that, for a given

i, a fraction of at least $\beta_i.2^{k_1.n+O(l)}$ unitaries $\{V_i.U_j\}$ satisfy

$$Pr_U(|\langle x_L^{out}|U_j.V_i|x_L^{out}\rangle|^2 \geq \frac{\alpha_i}{2^n}).$$

Summing over all the i, we get that there is at least a

$$\sum_i \beta_i 2^{k_1.n+O(l)} \geq min_i(\beta_i)2^{k.n+O(l)-n},$$

of unitaries $\{V_i.U_j\}_{j\in\{1,\ldots,2^{k_1.n+O(l)}\},i\in\{1,\ldots,2^{(k-k_1-1).n}}$ satisfying

$$Pr_U(|\langle x_L^{out}|U_j.V_i|x_L^{out}\rangle|^2 \geq \frac{min_i(\alpha_i)}{2^n}) \geq min_i(\beta_i), \tag{6.52}$$

where $min_i(\beta_i)$ and $min_i(\alpha_i)$ are the minimum values of β_i and α_i over all possible values of i, Pr_U is taken to mean the probability over the choice of $U_j.V_i$ with uniform probability from $\{V_i.U_j\}_{j\in\{1,\ldots,2^{k_1.n+O(l)}\},i\in\{1,\ldots,2^{(k-k_1-1).n}\}}$. Taking $\alpha = min_i(\alpha_i)$ and $\beta = min_i(\beta_i)$, then replacing Equation (6.52) in Equation (6.50) allows to obtain Theorem 3.

6.6.2 Calculation of $p_{totfail}$

The purpose of this subsection is to arrive at Equations (6.30) and (6.31). $p_{totfail}$ is the probability of getting at most $k_1.(n-1)$ successful instances out of $l_{max} = k.n$ instances (copies of $|zMSD_L\rangle$). Therefore, $p_{totfail}$ can be directly calculated as follows

$$p_{totfail} = \sum_{m=0,\ldots,k_1.(n-1)} p_{succ}^{k_1.(n-1)-m}.(1-p_{succ})^{l_{max}-k_1.(n-1)+m}.\binom{l_{max}}{k_1.(n-1)-m}. \tag{6.53}$$

$p_{succ} < 1 - p_{succ}$ (Equation (6.29)), therefore Equation (6.53) can be bounded as

$$p_{totfail} < \sum_{m=0,\ldots,k_1.(n-1)} (1-p_{succ})^{l_{max}} . \binom{l_{max}}{k_1.(n-1)-m}. \tag{6.54}$$

Using Equation (6.29), we get that

$$p_{totfail} < (1-\frac{1}{n})^{l_{max}} \sum_{m=0,\ldots,k_1.(n-1)} \binom{l_{max}}{k_1.(n-1)-m}. \tag{6.55}$$

A direct calculation shows that [12]

$$\sum_{m=0,\ldots,k_1.(n-1)} \binom{l_{max}}{k_1.(n-1)-m} \leq (k_1.(n-1)+1)\binom{l_{max}}{k_1.(n-1)}.$$

Plugging this into Equation (6.55), and noting that

$$\binom{l_{max}}{k_1.(n-1)} < l_{max}^{k_1.(n-1)},$$

we get that

$$p_{totfail} < (k_1.(n-1)+1).l_{max}^{k_1.(n-1)}.(1-\frac{1}{n})^{l_{max}}. \tag{6.56}$$

Recall the well known fact

$$\lim_{n\to\infty} (1-\frac{1}{n})^n = \frac{1}{e}.$$

[12] Assuming $l_{max} > 2.k_1.(n-1)$.

Plugging this into Equation (6.56) we get that the following holds for large enough n

$$p_{totfail} < (k_1.(n-1)+1).(\frac{1}{e})^{\frac{l_{max}}{n}}.l_{max}^{k_1.(n-1)}. \tag{6.57}$$

Let

$$\frac{l_{max}}{n} = p.k_1.(n-1). \tag{6.58}$$

Equation (6.57) can be rewritten as

$$p_{totfail} < (k_1.(n-1)+1).(\frac{l_{max}}{e^p})^{k_1.(n-1)}.$$

Choosing $p \geq log(l_{max}) = O(log(n))$, we get that $\frac{l_{max}}{e^p} < 1$. Plugging the value of p chosen into Equation (6.58) allows to obtain Equation (6.30). Also, plugging $\frac{l_{max}}{e^p} < 1$ into Equation (6.57), then calculating the limit as n goes to ∞ allows us to obtain Equation (6.31).

As a final remark, the $O(log(n))$ factor in Equation (6.30) is a slight overestimate due to us using various approximations to arrive to Equation (6.30), as can be seen through the claculations done in this section. Indeed, by looking at Equation (6.29), a simple heuristic argument would tell us that for each n copies measured, at least one should be succseesful. Therefore, if we desire $k_1.(n-1)$ successful instances we should measure $l_{max} \geq O(n.k_1.(n-1))$ copies. This gives, as expected, $\frac{l_{max}}{k_1.(n-1)} \geq O(n)$.

6.7 Conclusion

In summary, we have presented an example of a sampling problem which proceeds by performing non-adaptive, fixed Pauli measurements on $poly(n)$ sized 2D graph states with noisy non-Clifford inputs, and whose outputs are likely hard to approximately sample from classically, given some complexity theoretic conjectures−which are widely believed to be true−hold. This sampling problem is robust against general types of noise, and has experimentally desirable features like low overhead, nearest neighbor interactions, translational invariance, single instance hardness, and the fact that it can be executed in a constant number of rounds (i.e a constant depth circuit).

Closest to our work is that of [141]. However, there are many significant differences between our work and that of [141]. Indeed, the work of [141] treats general noise but uses for error correction the 3D RHG lattice [70], whereas we use the 2D color code [142]. Also, in [141], the anti-concentration property was conjectured, whereas in our case we prove it. Therefore, the number of complexity-theoretic conjectures we use in our proofs is less. The non-adaptive magic state distillation protocol used in [141] might lead to post-selecting an exponential number of times in order to get magic states of sufficiently high fidelity so as to enable quantum speedup to be observed. This might imply that, in practice, the sampling procedure must be repeated an exponential number of times in order to observe a hard instance. In our work, we use a special type of magic state distillation protocol, based on the work of [7], which when performed non-adaptively a *polynomial* number of times outputs enough magic states of sufficiently high fidelity so as to enable

quantum speedup to be oserved. Because these polynomial number of non-adaptive distillations are performed in parallel in our construction (as seen previously in this chapter), this gives rise in our case, with high probability, to the desirable single-instance hardness feature [38]. Finally, [141] rely on techniques of trap based verification, which we do not study here.

One might ask, why do other MSD protocols like those of [143, 144], for example, not work (using our proof techniques)? The answer to this question has to do with the number of noisy input T states n_{noisy} with fidelity $1-\varepsilon$ with respect to an ideal T-state, needed to distill a single T-state of sufficiently high fidelity $1-\varepsilon_{out}$ with respect to an ideal T-state. n_{noisy} is usually given by [143]

$$n_{noisy} = O\Big(log^{\gamma}(\frac{1}{\varepsilon_{out}})\Big). \tag{6.59}$$

Here γ is a constant which depends on the error correcting code from which the MSD protocol is derived [145]. In the protocol of [7], $\gamma \sim 1$. This is what allowed us to get a p_{succ} of the form of Equation (6.29). On the other hand, the protocols of [143, 144] have a $\gamma > 1$, which leads to a lower bound of p_{succ} which looks like $1/qp(n)$-from Equation (6.28) and by using similar arguments for calculating n_{NMSD} as in Section 6.4 - where $qp(n)$ is *quasi-polynomial* in n. Indeed, N in Section 6.4 is proportional to $\alpha.n_{noisy}$, where α is the number of output T-states with error ε_{out}. Therefore, it follows that $n_{NMSD} = O(N) = O(n_{noisy})$, and that $2^{n_{NMSD}} = 2^{O(n_{noisy})}$, which is a quasi-polynomial when $\gamma > 1$. This would mean, using our proof techniques, that we would need a quasi-polynomial in n (which is greater

than polynomial in n) number of $|zMSD_L\rangle$ copies, thereby taking us out of the scope of what is considered quantum speedup [13]. Other protocols which we could have used and could have worked are those of [146] which gives $\gamma \sim 1$, or that of [145] which gives $\gamma < 1$, albeit with a huge constant overhead of 2^{58} qubits [145].

[13] Since quantum speedup is usually defined with respect to quantum devices using polynomial quantum resources [37].

Chapter 7

General Conclusion

In this thesis, we have provided new constructions of unitary t-designs, some of which are based on relaxations of strict technical requirements in previous constructions [6, 94]. We have also shown that these unitary t-designs can be implemented by fixed, non-adaptive measurements on graph states whose underlying graph is a 2D regular lattice [36]. We have given new examples of sampling problems defined by non-adaptive, fixed angle measurements on 2D graph states with a regular lattice structure which demonstrate a quantum speedup. Finally, we have presented a sampling problem, showing a quantum speedup, which proceeds by non-adaptive fixed angle measurements on a 2D graph state, and which is robust to general noise models [37]. This sampling problem in the circuit model can be viewed as a constant depth fault-tolerant quantum circuit acting on a polynomial number of ancillas.

Several interesting open questions come to mind, in addition to the ones in the Conclusion sections of previous chapters. Concerning Chapters 4 and

5, an interesting direction to pursue would be trying to find a link between approximate t-designs, and the Solovay-Kitaev (SK) construction [129]. If such a link can be found, then the results of Chapters 4 and 5 may be used to make partial progress onto an inverse-free version of the SK Theorem, albeit without additional assumptions [153, 154]. Indeed, there are already hints at relations between the SK construction and unitary t-designs [155], and our construction is the first (to our knowledge) to remove the need for inverses in the base set generating the t-design.

Concerning Chapter 6, an interesting question would be calculating the fault-tolerance threshold for our model in the pre-threshold region, where hardness of approximate classical sampling is guaranteed by post-selecting on the non-reliable error correction to simulate a reliable one [156]. We expect this should significantly enhance the fault-tolerance threshold of our model. An interesting direction also would be adapting our ideas to work with other error correcting codes [157], which may provide better fault-tolerance thresholds, or even lower the overhead significantly [158]. One could also think of a technique to avoid multiple rounds in our construction. Perhaps by using the 3D RHG lattice [70] one can reduce our construction to a single round of non-adaptive measurements on a single (3D) $poly(n)$ sized graph state.

More broadly, an important direction to pursue would be verifying that our fault-tolerant construction demonstrates a quantum speedup. In this direction, the work of [51, 84] can be used for this purpose when the measurements (both Clifford and non-Clifford) as well as the CZ and Hadamard

gates (needed for the preparation of the graph states [69]) are assumed $perfect$ (noiseless). Indeed, in this case the verification amounts to verifying that the graph state was correctly prepared, for which [51, 84] provide a natural path to do so, by giving good lower bounds (with high confidence) on the fidelity (with respect to the ideal graph state corresponding to the sampling problem) of the prepared graph state in the case where a sufficient amount of stabilizer tests pass [51, 84]. These lower bounds on the fidelity, tending asymptotically to one [51, 84], allow one to verify that quantum speedup is being observed, as long as one trusts the local masurement devices (which, being small, can be checked by other means efficiently). This verification of quantum speedup can be done by using the standard relation between the fidelities of two quantum states (which in our case are the ideal state and the state accepted by the verification protocol) and the l_1-norm of the two output probability distributions corresponding to measuring the qubits of these two states [37].

These techniques, however, do not easily extend to the case where the measurements and gates needed for preparation are noisy; since for graph states of size n, even for an arbitrarily small (but *constant*, for example below the threshold for fault-tolerant computing.) noise strength the verification protocol might fail (not accept a good state) in the asymptotic ($n \to \infty$) limit (see for example [84] where the verification accepts with probability one asymptotically only if the noise strenght scales as $1/poly(n)$). This is a topic we are currently looking at.

One could also think about the *quantum resources* underlying the quan-

tum speedup in our case [52], along the lines of work on qudit magic states in [19], or even deriving a figure of merit for hardness of classical simulability in terms of mimimum T-gate count, as is done for example in [159].

Bibliography

[1] Jeffrey M Epstein, Andrew W Cross, Easwar Magesan, and Jay M Gambetta. Investigating the limits of randomized benchmarking protocols. *Physical Review A*, 89(6):062321, 2014.

[2] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, 2007.

[3] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2010.

[4] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009.

[5] Peter S Turner and Damian Markham. Derandomizing quantum circuits with measurement-based unitary designs. *Physical review letters*, 116(20):200501, 2016.

[6] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346(2):397–434, 2016.

[7] Jeongwan Haah, Matthew B Hastings, D Poulin, and D Wecker. Magic state distillation with low space overhead and optimal asymptotic input count. *arXiv preprint arXiv:1703.07847*, 2017.

[8] Andrew J Landahl, Jonas T Anderson, and Patrick R Rice. Fault-tolerant quantum computing with color codes. *arXiv preprint arXiv:1108.5738*, 2011.

[9] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topolgical quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.

[10] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[11] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6):467–488, 1982.

[12] Christian L Degen, F Reinhard, and P Cappellaro. Quantum sensing. *Reviews of modern physics*, 89(3):035002, 2017.

[13] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

[14] Kuk-Hyun Han and Jong-Hwan Kim. Genetic quantum algorithm and its application to combinatorial optimization problem. In *Proceedings of the 2000 Congress on Evolutionary Computation. CEC00 (Cat. No. 00TH8512)*, volume 2, pages 1354–1360. IEEE, 2000.

[15] R Landauer. Information is physical. physcomp'92. In *Workshop on Physics and Computation*, pages 2–4, 1992.

[16] Richard A Low. Pseudo-randomness and learning in quantum computation. *arXiv preprint arXiv:1006.5227*, 2010.

[17] Lov K Grover. A fast quantum mechanical algorithm for database search. *arXiv preprint quant-ph/9605043*, 1996.

[18] Harry Buhrman, Richard Cleve, and Wim Van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30(6):1829–1841, 2001.

[19] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the 'magic'for quantum computation. *Nature*, 510(7505):351, 2014.

[20] Sergey Bravyi, David Gosset, and Robert Koenig. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[21] Scott Aaronson. The limits of quantum. *Scientific American*, 298(3):62–69, 2008.

[22] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[23] Markus P Müller, Emily Adlam, Lluís Masanes, and Nathan Wiebe. Thermalization and canonical typicality in translation-invariant quantum lattice systems. *Communications in Mathematical Physics*, 340(2):499–561, 2015.

[24] Aram Harrow and Saeed Mehraban. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. *arXiv preprint arXiv:1809.06957*, 2018.

[25] Juan Bermejo-Vega, Dominik Hangleiter, Martin Schwarz, Robert Raussendorf, and Jens Eisert. Architectures for quantum simulation showing a quantum speedup. *Physical Review X*, 8(2):021010, 2018.

[26] Dominik Hangleiter, Juan Bermejo-Vega, Martin Schwarz, and Jens Eisert. Anticoncentration theorems for schemes showing a quantum speedup. *Quantum*, 2, 2018.

[27] Ryan L Mann and Michael J Bremner. On the complexity of random quantum computations and the jones polynomial. *arXiv preprint arXiv:1711.00686*, 2017.

[28] Emanuel Knill. Approximation by quantum circuits. *arXiv preprint quant-ph/9508006*, 1995.

[29] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):012304, 2009.

[30] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[31] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[32] 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.

[33] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *arXiv preprint arXiv:1610.01808*, 2016.

[34] Kaifeng Bu and Dax Enshan Koh. Efficient classical simulation of clifford circuits with nonstabilizer input states. *arXiv preprint arXiv:1902.11257*, 2019.

[35] Xun Gao and Luming Duan. Efficient classical simulation of noisy quantum computation. *arXiv preprint arXiv:1810.03176*, 2018.

[36] Rawad Mezher, Joe Ghalbouni, Joseph Dgheim, and Damian Markham. Efficient quantum pseudorandomness with simple graph states. *Physical Review A*, 97(2):022333, 2018.

[37] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[38] Xun Gao, Sheng-Tao Wang, and L-M Duan. Quantum supremacy for simulating a translation-invariant ising spin model. *Physical review letters*, 118(4):040502, 2017.

[39] Jun John Sakurai and Eugene D Commins. Modern quantum mechanics, revised edition, 1995.

[40] https://ocw.mit.edu/courses/nuclear-engineering/22-51-quantum-theory-of-radiation-interactions-fall-2012/lecture-notes.

[41] Michael Reed. B. simon methods of modern mathematical physics, iv: Analysis of operators, 1978.

[42] Erwin Schrödinger. An undulatory theory of the mechanics of atoms and molecules. *Physical review*, 28(6):1049, 1926.

[43] Scott Aaronson. *Quantum computing since Democritus*. Cambridge University Press, 2013.

[44] Lucien Hardy. Quantum theory from five reasonable axioms. *arXiv preprint quant-ph/0101012*, 2001.

[45] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[46] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[47] Nicolas Gisin and Rob Thew. Quantum communication. *Nature photonics*, 1(3):165, 2007.

[48] 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.

[49] Simon Kochen and Ernst P Specker. The problem of hidden variables in quantum mechanics. In *The logico-algebraic approach to quantum mechanics*, pages 293–328. Springer, 1975.

[50] Samson Abramsky and Adam Brandenburger. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics*, 13(11):113036, 2011.

[51] Damian Markham and Alexandra Krause. A simple protocol for certifying graph states and applications in quantum networks. *arXiv preprint arXiv:1801.05057*, 2018.

[52] Robert W Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Physical Review A*, 71(5):052108, 2005.

[53] Angela Karanjai, Joel J Wallman, and Stephen D Bartlett. Contextuality bounds the efficiency of classical simulation of quantum processes. *arXiv preprint arXiv:1802.07744*, 2018.

[54] Scott Aaronson. Is quantum mechanics an island in theoryspace? *arXiv preprint quant-ph/0401062*, 2004.

[55] Tomáš Gonda, Ravi Kunjwal, David Schmid, Elie Wolfe, and Ana Belén Sainz. Almost quantum correlations are inconsistent with specker's principle. *arXiv preprint arXiv:1712.01225*, 2017.

[56] Ana Belén Sainz, Yelena Guryanova, Antonio Acín, and Miguel Navascués. Almost-quantum correlations violate the no-restriction hypothesis. *Physical review letters*, 120(20):200402, 2018.

[57] Eugene P Wigner. The unreasonable effectiveness of mathematics in the natural sciences. In *Mathematics and Science*, pages 291–306. World Scientific, 1990.

[58] Jean-Luc Brylinski and Ranee Brylinski. Universal quantum gates. In *Mathematics of quantum computation*, pages 117–134. Chapman and Hall/CRC, 2002.

[59] https://www.claymath.org/millennium-problems.

[60] W. gasarch. the p=?np poll. sigact news, 33(2):34–47, june 2002.

[61] Alexander A Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.

[62] Scott Aaronson. Guest column: Np-complete problems and physical reality. *ACM Sigact News*, 36(1):30–52, 2005.

[63] Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *arXiv preprint quant-ph/0205133*, 2002.

[64] Ryan Lee Mann. *Quantum computation and combinatorial structures*. PhD thesis, 2019.

[65] Leslie G Valiant. The complexity of computing the permanent. *Theoretical computer science*, 8(2):189–201, 1979.

[66] Keisuke Fujii and Tomoyuki Morimae. Commuting quantum circuits and complexity of ising partition functions. *New Journal of Physics*, 19(3):033003, 2017.

[67] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482, 2005.

[68] Jean H Gallier. Harry r. lewis and christos h. papadimitriou. elements of the theory of computation. prentice-hall software series. prentice-hall, inc., englewood cliffs, nj, 1981, xiv+ 466 pp. *The Journal of Symbolic Logic*, 49(3):989–990, 1984.

[69] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, M Nest, and H-J Briegel. Entanglement in graph states and its applications. *arXiv preprint quant-ph/0602096*, 2006.

[70] Robert Raussendorf and Jim Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Physical review letters*, 98(19):190504, 2007.

[71] Damian Markham and Barry C Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78(4):042309, 2008.

[72] Clément Meignant, Damian Markham, and Frédéric Grosshans. Distributing graph states over arbitrary quantum networks. *arXiv preprint arXiv:1811.05445*, 2018.

[73] Xi-Lin Wang, Luo-Kan Chen, Wei Li, H-L Huang, Chang Liu, Chao Chen, Y-H Luo, Z-E Su, Dian Wu, Z-D Li, et al. Experimental ten-photon entanglement. *Physical review letters*, 117(21):210502, 2016.

[74] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *science*, 335(6066):303–308, 2012.

[75] BA Bell, D Markham, DA Herrera-Martí, A Marin, WJ Wadsworth, JG Rarity, and MS Tame. Experimental demonstration of graph-state quantum secret sharing. *Nature communications*, 5:5480, 2014.

[76] Y Cai, J Roslund, G Ferrini, F Arzani, X Xu, C Fabre, and N Treps. Multimode entanglement in reconfigurable graph states using optical frequency combs. *Nature communications*, 8:15645, 2017.

[77] Shota Yokoyama, Ryuji Ukai, Seiji C Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa,

Hidehiro Yonezawa, Nicolas C Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nature Photonics*, 7(12):982, 2013.

[78] Mario Arnolfo Ciampini, Adeline Orieux, Stefano Paesani, Fabio Sciarrino, Giacomo Corrielli, Andrea Crespi, Roberta Ramponi, Roberto Osellame, and Paolo Mataloni. Path-polarization hyperentangled and cluster states of photons on a chip. *Light: Science & Applications*, 5(4):e16064, 2016.

[79] Julio T Barreiro, Markus Müller, Philipp Schindler, Daniel Nigg, Thomas Monz, Michael Chwalla, Markus Hennrich, Christian F Roos, Peter Zoller, and Rainer Blatt. An open-system quantum simulator with trapped ions. *Nature*, 470(7335):486, 2011.

[80] Thomas Monz, Philipp Schindler, Julio T Barreiro, Michael Chwalla, Daniel Nigg, William A Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-qubit entanglement: Creation and coherence. *Physical Review Letters*, 106(13):130506, 2011.

[81] Chao Song, Kai Xu, Wuxin Liu, Chui-ping Yang, Shi-Biao Zheng, Hui Deng, Qiwei Xie, Keqiang Huang, Qiujiang Guo, Libo Zhang, et al. 10-qubit entanglement and parallel logic operations with a superconducting circuit. *Physical review letters*, 119(18):180511, 2017.

[82] Julia Cramer, Norbert Kalb, M Adriaan Rol, Bas Hensen, Machiel S Blok, Matthew Markham, Daniel J Twitchen, Ronald Hanson, and

Tim H Taminiau. Repeated quantum error correction on a continuously encoded qubit by real-time feedback. *Nature communications*, 7:11526, 2016.

[83] Marcus Cramer, Martin B Plenio, Steven T Flammia, Rolando Somma, David Gross, Stephen D Bartlett, Olivier Landon-Cardinal, David Poulin, and Yi-Kai Liu. Efficient quantum state tomography. *Nature communications*, 1:149, 2010.

[84] Yuki Takeuchi, Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, and Joseph F Fitzsimons. Resource-efficient verification of quantum computing using serfling's bound. *npj Quantum Information*, 5(1):27, 2019.

[85] Robert Raussendorf, Daniel E Browne, and Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical review A*, 68(2):022312, 2003.

[86] Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics*, 9(8):250, 2007.

[87] Atul Mantri, Tommaso F Demarie, and Joseph F Fitzsimons. Universality of quantum computation with cluster states and (x, y)-plane measurements. *Scientific reports*, 7:42861, 2017.

[88] Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya, and Peter S Turner. Which graph states are useful for quantum information

processing? In *Conference on Quantum Computation, Communication, and Cryptography*, pages 174–187. Springer, 2011.

[89] Noga Alon, László Babai, and Alon Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. *Journal of algorithms*, 7(4):567–583, 1986.

[90] Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 129–140. IEEE, 2007.

[91] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM journal on computing*, 22(4):838–856, 1993.

[92] Marcus D De Chiffre. *The Haar measure*. PhD thesis, Ph. D. thesis, Department of Mathematical Sciences, University of Copenhagen, 2011.

[93] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, 2007.

[94] Rawad Mezher, Joe Ghalbouni, Joseph Dgheim, and Damian Markham. Efficient approximate unitary t-designs from partially invertible universal sets and their application to quantum speedup. *arXiv preprint arXiv:1905.01504*, 2019.

[95] Joseph M Renes, Robin Blume-Kohout, Andrew J Scott, and Carlton M Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004.

[96] Howard Barnum. Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases. *arXiv preprint quant-ph/0205155*, 2002.

[97] Andreas Klappenecker and M Rotteler. Mutually unbiased bases are complex projective 2-designs. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1740–1744. IEEE, 2005.

[98] Aram W Harrow and Richard A Low. Random quantum circuits are approximate 2-designs. *Communications in Mathematical Physics*, 291(1):257–302, 2009.

[99] Huangjun Zhu. Multiqubit clifford groups are unitary 3-designs (2015). *arXiv preprint arXiv:1510.02619*.

[100] Winton G Brown and Lorenza Viola. Convergence rates for arbitrary statistical moments of random quantum circuits. *Physical review letters*, 104(25):250501, 2010.

[101] Yoshifumi Nakata, Christoph Hirche, Masato Koashi, and Andreas Winter. Efficient quantum pseudorandomness with nearly time-independent hamiltonian dynamics. *Physical Review X*, 7(2):021006, 2017.

[102] David Gross, Koenraad Audenaert, and Jens Eisert. Evenly distributed unitaries: On the structure of unitary designs. *Journal of mathematical physics*, 48(5):052104, 2007.

[103] Aidan Roy and Andrew J Scott. Unitary designs and codes. *Designs, codes and cryptography*, 53(1):13–31, 2009.

[104] Huangjun Zhu, Richard Kueng, Markus Grassl, and David Gross. The clifford group fails gracefully to be a unitary 4-design. *arXiv preprint arXiv:1609.08172*, 2016.

[105] Eiichi Bannai, Mikio Nakahara, Da Zhao, and Yan Zhu. On the explicit constructions of certain unitary t-designs. *arXiv preprint arXiv:1906.04583*, 2019.

[106] Artem Kaznatcheev. Structure of exact and approximate unitary t-designs, semantic scholar, 2010.

[107] MB Hastings. Random unitaries give quantum expanders. *Physical Review A*, 76(3):032315, 2007.

[108] Matthew B Hastings and Aram Wettroth Harrow. Classical and quantum tensor product expanders. *arXiv preprint arXiv:0804.0011*, 2008.

[109] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. Quantum supremacy and the complexity of random circuit sampling. *arXiv preprint arXiv:1803.04402*, 2018.

[110] Matty J Hoban, Joel J Wallman, Hussain Anwar, Naïri Usher, Robert Raussendorf, and Dan E Browne. Measurement-based classical computation. *Physical review letters*, 112(14):140505, 2014.

[111] M Nest. Classical simulation of quantum computation, the gottesman-knill theorem, and slightly beyond. *arXiv preprint arXiv:0811.0898*, 2008.

[112] Leslie Ann Goldberg and Heng Guo. The complexity of approximating complex-valued ising and tutte partition functions. *computational complexity*, 26(4):765–833, 2017.

[113] Larry Stockmeyer. On approximation algorithms for# p. *SIAM Journal on Computing*, 14(4):849–861, 1985.

[114] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical review letters*, 117(8):080501, 2016.

[115] Aram W Harrow and Ashley Montanaro. Quantum computational supremacy. *Nature*, 549(7671):203, 2017.

[116] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595, 2018.

[117] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[118] Dorit Aharonov, Itai Arad, Umesh Vazirani, and Zeph Landau. The detectability lemma and its applications to quantum hamiltonian complexity. *New journal of physics*, 13(11):113043, 2011.

[119] Bruno Nachtergaele. The spectral gap for some spin chains with discrete symmetry breaking. *Communications in mathematical physics*, 175(3):565–606, 1996.

[120] Matthew B Hastings and Tohru Koma. Spectral gap and exponential decay of correlations. *Communications in mathematical physics*, 265(3):781–804, 2006.

[121] Matthew B Hastings and Tohru Koma. Spectral gap and exponential decay of correlations. *Communications in mathematical physics*, 265(3):781–804, 2006.

[122] Jean Bourgain and Alex Gamburd. A spectral gap theorem in $su(d)$. *arXiv preprint arXiv:1108.6264*, 2011.

[123] Roberto Imbuzeiro Oliveira et al. On the convergence to equilibrium of kac's random walk on matrices. *The Annals of Applied Probability*, 19(3):1200–1231, 2009.

[124] Seth Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346, 1995.

[125] David Elieser Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. *Proceedings of the Royal Society of Lon-*

don. Series A: Mathematical and Physical Sciences, 449(1937):669–677, 1995.

[126] Nathan Jacobson. *Lie algebras*. Number 10. Courier Corporation, 1979.

[127] Ivan Niven. *Irrational numbers*. Number 11. Cambridge University Press, 2005.

[128] Stefanie Barz, Joseph F Fitzsimons, Elham Kashefi, and Philip Walther. Experimental verification of quantum computation. *Nature physics*, 9(11):727, 2013.

[129] Christopher M Dawson and Michael A Nielsen. The solovay-kitaev algorithm. *arXiv preprint quant-ph/0505030*, 2005.

[130] 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.

[131] AP Lund, A Laing, S Rahimi-Keshari, T Rudolph, Jeremy L O'Brien, and TC Ralph. Boson sampling from a gaussian state. *Physical review letters*, 113(10):100502, 2014.

[132] Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *arXiv preprint quant-ph/0205133*, 2002.

[133] Robert Gardner Bartle and Robert G Bartle. *The elements of integration and Lebesgue measure*, volume 27. Wiley Online Library, 1995.

[134] Yaoyun Shi. Both toffoli and controlled-not need little help to do universal quantum computation. *arXiv preprint quant-ph/0205115*, 2002.

[135] P Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing. *arXiv preprint quant-ph/9906054*, 1999.

[136] Piotr Ćwikliński, Michał Horodecki, Marek Mozrzymas, Łukasz Pankowski, and Michał Studziński. Local random quantum circuits are approximate polynomial-designs: numerical results. *Journal of Physics A: Mathematical and Theoretical*, 46(30):305301, 2013.

[137] Gilbert t Strang. *Introduction to linear algebra*, volume 3. Wellesley-Cambridge Press Wellesley, MA, 1993.

[138] Aram W Harrow. Exact universality from any entangling gate without inverses. *arXiv preprint arXiv:0806.0631*, 2008.

[139] Nicolai Friis, Davide Orsucci, Michalis Skotiniotis, Pavel Sekatski, Vedran Dunjko, Hans J Briegel, and Wolfgang Dür. Flexible resources for quantum metrology. *New Journal of Physics*, 19(6):063044, 2017.

[140] Francesco Arzani, Giulia Ferrini, Frédéric Grosshans, and Damian Markham. Random coding for sharing bosonic quantum secrets. *Physical Review A*, 100(2):022303, 2019.

[141] Theodoros Kapourniotis and Animesh Datta. Nonadaptive fault-tolerant verification of quantum supremacy with noise. *Quantum*, 3:164, 2019.

[142] Hector Bombin and Miguel Angel Martin-Delgado. Topological quantum distillation. *Physical review letters*, 97(18):180501, 2006.

[143] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, 2005.

[144] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, 2012.

[145] Matthew B Hastings and Jeongwan Haah. Distillation with sublogarithmic overhead. *Physical review letters*, 120(5):050504, 2018.

[146] Cody Jones. Multilevel distillation of magic states for quantum computing. *Physical Review A*, 87(4):042305, 2013.

[147] Emanuel Knill. Fault-tolerant postselected quantum computation: Schemes. *arXiv preprint quant-ph/0402171*, 2004.

[148] Sergey Bravyi, David Gosset, Robert Koenig, and Marco Tomamichel. Quantum advantage with noisy shallow circuits in 3d. *arXiv preprint arXiv:1904.01502*, 2019.

[149] Leslie Ann Goldberg and Heng Guo. The complexity of approximating complex-valued ising and tutte partition functions. *computational complexity*, 26(4):765–833, 2017.

[150] Fern Watson. Performance of topological codes for quantum error correction. 2015.

[151] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[152] David P DiVincenzo, Debbie W Leung, and Barbara M Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580–598, 2002.

[153] Imdad SB Sardharwalla, Toby S Cubitt, Aram W Harrow, and Noah Linden. Universal refocusing of systematic quantum noise. *arXiv preprint arXiv:1602.07963*, 2016.

[154] Adam Bouland and Maris Ozols. Trading inverses for an irrep in the solovay-kitaev theorem. *arXiv preprint arXiv:1712.09798*, 2017.

[155] Péter Pál Varjú. Random walks in compact groups. *Documenta Mathematica*, 18:1137–1175, 2013.

[156] Keisuke Fujii. Noise threshold of quantum supremacy. *arXiv preprint arXiv:1610.03632*, 2016.

[157] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. Quantum expander codes. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 810–824. IEEE, 2015.

[158] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In

2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pages 743–754. IEEE, 2018.

[159] Cupjin Huang, Michael Newman, and Mario Szegedy. Explicit lower bounds on strong simulation of quantum circuits in terms of t-gate count. *arXiv preprint arXiv:1902.04764*, 2019.