# Computational power of one-dimensional symmetry-protected topological phases

by

David Thomas Stephen

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Physics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2017

# Abstract

We consider ground states of quantum spin chains with symmetry-protected topological (SPT) order as resources for measurement-based quantum computation (MBQC). Using tensor network methods, we show that SPT phases protected by a finite abelian on-site symmetry group exhibit uniform computational power. That is, any state from a given phase leads to the same Lie group of executable gates when used as a resource for MBQC. This Lie group is determined by the same algebraic information that labels the SPT phase itself, and we give a necessary condition on the phase that guarantees a full set of single-qubit gates. To obtain our results, we construct several new techniques in MBQC and refine the structure of quantum states with abelian SPT order. Our results are analogous to similar results relating topological order and topological quantum computation, and we comments on their implications on the general connection between quantum phases of matter and quantum computation.

# Lay Summary

The organization of matter into distinct phases is a fundamental property of physics with numerous practical applications. Water in its liquid, gas, and solid phases is essential for life, while magnetic materials in their ordered phase provide the basis for memory in computers. An exciting area of current research suggests that certain phases of matter may also help in building the coveted quantum computer. A quantum computer uses quantum resources like entangled particles to solve certain problems faster than any conventional computer. Recently, it has been suggested that the usefulness of these quantum resources for computation depends only on their phase, akin to deducing properties of chemical elements from their location in the periodic table. This thesis shows that this is true for a class of exotic phases of matter called the symmetry-protected topological phases, pointing to the possibility of a deep relation between quantum computation and phases of matter.

# Preface

The contents of this thesis have lead to two publications: *Computational power of symmetry-protected topological phases* published in Physical Review Letters, 2017 [1] and *Symmetry-protected topological phases with uniform computational power in one dimension* published in Physical Review A, 2017 [2], involving the following co-authors: Robert Raussendorf, Dong-Sheng Wang, Abhishodh Prakash, and Tzu-Chieh Wei. The former publication was written by myself, while the latter was written by R. Raussendorf. Parts of the the former publication have been reproduced verbatim in this thesis in Chapter 3, Section 5.3, and Appendix A.

All sections of this thesis are written by myself, with the exception of Section 3.3, which was written by R. Raussendorf. Chapter 3 involves the most collaboration between the above authors and myself. The construction of the three computational steps leading to a Lie group of gates is due mainly to R. Raussendorf. The interpretation of these techniques, their relation to symmetry-protected topological order, and certain other details were discovered by myself, aided by discussions with all above authors. The research found in Chapters 4 and 5 was done primarily by myself, aided by discussion with R. Raussendorf and D. -S. Wang.

# Table of Contents

# List of Figures

# Acknowledgements

I will be eternally grateful to my supervisor, Robert Raussendorf, for helping me to mature as a physicist, conquer my self-doubts, and find my passion. I attribute the success of my degree to his constant support, guidance, tutelage, and the countless opportunities to connect to other members of my field that he presented to me.

I would also like to thank my fellow students and the staff at UBC for their support both on and off campus, particularly the members of the UBC quantum information group and my roommate, rival, and long-time friend Jordan Wilson.

# Chapter 1

# Introduction

This thesis lies at the intersection between the fields of condensed matter physics and quantum information science. We study the relationship between two phenomena of highly-entangled many-body quantum systems: quantum phases of matter and quantum computation. Due to the interdisciplinary nature of this thesis, our motivation can come from two different perspectives.

Let us start from the condensed matter side. A phase of matter is a collection of states of a system that share some property distinct from states in a different phase. In many-body physics, the essential properties of a state are often determined by the phase of matter in which it resides. Recent years have witnessed tremendous progress in the discovery and classification of exotic quantum phases [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13], and it is thus pertinent to ask—what can a phase of matter be used for? A traditional example is the ubiquitous superconductor, while newly discovered phases such as topological insulators [14] and quantum spin liquids [15] have promising future applications. Quantum phases are useful in quantum information processing as well: certain topological phases allow for error-resilient topological quantum computation via the braiding and fusion of their anyonic excitations [16, 17].

Why is it beneficial for an application to take advantage of a phase of matter? For one, they require less accuracy in their preparation, which needs only prepare any state from a given phase, rather than a particular target state. Furthermore, applications which utilize the topological properties of phases, such as topological quantum computation, are robust against any local sources of noise which cannot detect the non-local topological features. Unfortunately, despite the rich zoo of quantum phases, existing applications tend to use only the simplest examples of quantum phases, such as the simple $\mathbb{Z}_2$ topological order of the toric code [16]. This leads one to seek applications that delve deeper into the algebraic framework underpinning the classification of phases, possibly leading to useful or interesting new phenomena. This is the first goal of this thesis.

On the other side we have quantum computation, which is a method

of computation that exploits quantum resources to achieve computational speedups over classical algorithms [18]. A preeminent example of this is Shor's algorithm [19], which solves the factoring problem exponentially faster than any known classical algorithm. Despite the apparent supremacy of quantum computers over their classical counterparts, the source of quantum computational power remains unknown. It is not clear which phenomena of quantum mechanics are responsible for the observed speedup, whether it be superposition [20], entanglement [21], or more contemporary ideas like contextuality [22, 23]. Solving this problem would lead to a deeper understand of the relationship between quantum mechanics and information theory, and better guidelines to design new quantum algorithms.

In a particular model of quantum computation called measurement-based quantum computation (MBQC) [24, 25], the quantum resource is a highly-entangled state of a many-body quantum system—a *resource state*. Computation is implemented through the use of single-body projective measurements alone, such that the power of an MBQC scheme is completely determined by the properties of the resource state. Because of this, MBQC provides a setting in which the above problem can be phrased in terms of properties of many-body quantum states, and therefore in the realm of condensed matter physics. The most relevant question in the context of quantum phases is whether the computational power of MBQC is particular to individual states, or a property of a phase of matter. This is a long-standing open problem in the field [26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40]. Identifying *computational phases of matter*, where a physical phase corresponds with a region of uniform computational power, is the second goal of this thesis.

In this thesis, we successfully address the two goals given above. We consider the *symmetry-protected topological* (SPT) phases of matter of spin chains [5, 6, 7], and show that every state in a given phase has equivalent power as a resource state for MBQC. Furthermore, our results make full use of the algebraic structures that classify SPT phases and reveal that the same structures also determine MBQC power. Overall, this thesis contributes to the effort to unite the fields of quantum phases of matter and quantum computation, and investigate how research in one may aid or influence the other.

In the following chapter, we give the necessary background from both fields. We first introduce SPT phases and MBQC, and see how they can both be compactly described using the language of matrix product states. We will see that SPT phases are characterized by certain patterns of entanglement, and that it is exactly this entanglement that we use for computation. We

then review the history of the search for computational phases of matter, leading into our own results. In Chapter 3, we introduce three new computational elements that allow us to construct a general scheme of MBQC that takes advantage of the part of a quantum state that is uniform throughout a phase. With this, we show that MBQC power is uniform in SPT phases, subject to a condition called *maximal non-commutativity*. In Chapter 4, we remove this condition, proving the necessary theorems about the structure of quantum states with SPT order and adding new computational techniques. Then, in Chapter 5, we determine the uniform computational power of these phases in terms of a Lie group of executable operations, proving that the maximally non-commutative phases always allow for a full set of single-qubit operations. Finally, in Chapter 6, we discuss possible extensions of our results, as well as their impact on the general relation between quantum phases of matter and quantum computation.

# Chapter 2

# Background

## 2.1 Gapped quantum systems and the area law

In this thesis, we will consider quantum spins chains. These are systems that consist of spin degrees of freedom arranged in a one dimensional (1D) line. Here, by a spin degree of freedom, we simply mean a finite dimensional Hilbert space; a $d$-dimensional spin is associated to a Hilbert space $\mathbb{C}^d$, such that total Hilbert space of a chain of length $N$ is $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$. More specifically, we consider the ground states of gapped local Hamiltonians acting on these chains, which are defined by local interactions and a finite gap between the ground state energy and the next excited state that persists as the system size is increased. Such *gapped quantum systems*, besides providing a setting for interesting and exotic physical phenomena, are also good models of certain strongly-correlated systems. These the include half-filled Hubbard model that describes magnetic properties of crystals [41], and many systems used for quantum simulations [42] such as optical lattices [43, 44] or certain superconducting circuits [45].

In general, the Hilbert space dimension of our spin chain is exponential in its length, a fact that prohibits naive numerical and analytical studies of such systems even for modest system sizes of $N \approx 50$. Luckily, one avoids this problem by considering gapped quantum states, which have very little entanglement as quantified by the *area law* [46]. The area law, which has been rigorously proven for gapped quantum systems in 1D [47], says that the entanglement between two regions scales with the size of the boundary between them, rather than their volume as would be expected from a generic state [48]. Because of this, gapped quantum systems occupy only a tiny fraction of the total available Hilbert space, the so-called "physical corner". This makes such systems amicable to more efficient descriptions that also explore only the physical corner, serving as a basis for powerful numerical techniques and new mathematical tools. One such example is the tensor networks formalism, which is the central tool used for the analysis in this thesis.

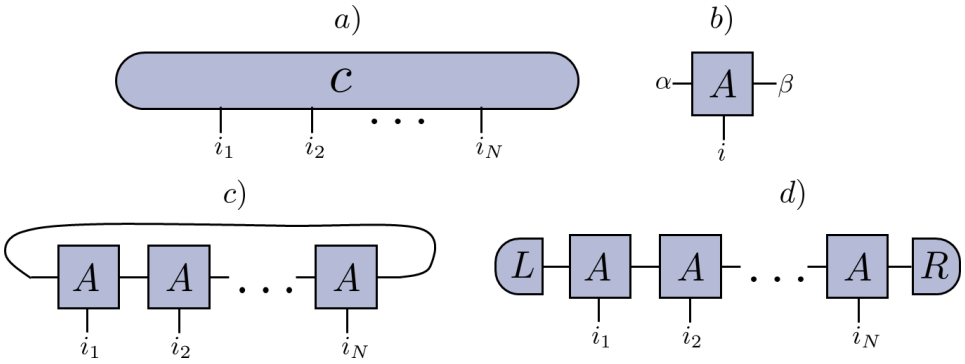


Figure 2.1: Tensor network representations of the objects encountered in this section. a) An $N$ index tensor like $c_{i_1,\ldots,i_N}$ is represented by a box with $N$ legs. b) The matrix elements $A^i_{\alpha\beta}$ of the MPS matrices can be represented by an 3-leg tensor. $i$ corresponds to the physical index, while the other two are virtual indices. c) Joining legs of two tensors corresponds to summing over that index, so this network represents Eq. 2.2. d) Tensor network representation of Eq. 2.3

## 2.2 Matrix product states

In this section, we introduce *matrix product states* (MPS) [49], which are the simplest example of the more general tensor network states. As proven in Refs. [47, 50, 51], the ground states of gapped 1D systems can be efficiently represented by MPS. Conversely, every MPS is the ground state of a gapped spin chain satisfying an area law, so they are an essential tool for exploring the physical corner of Hilbert space.

A general wavefunction of a spin chain consisting of $N$ spins of dimension $d$ can be written as:

$$|\psi\rangle = \sum_{i_1,\ldots,i_N=0}^{d-1} c_{i_1,\ldots,i_N} |i_1 \ldots i_N\rangle \tag{2.1}$$

Here we would like to interpret $c_{i_1,\ldots,i_N}$ as an $N$-index tensor with $d^N$ coefficients that specifies the wavefunction of our $N$ spins, see Fig. 2.1a). To represent this state as an MPS, we decompose this tensor into a number of smaller tensors[1]. For a translationally invariant system with periodic

[1] While this decomposition can be always be accomplished via successive schmidt decomposition [21], we consider states that are given to us already in MPS form.

boundary conditions (ie. a ring), we write

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \mathrm{Tr}\left(A^{i_N} A^{i_{N-1}} \ldots A^{i_1}\right) |i_1 \ldots i_N\rangle \tag{2.2}$$

See Fig. 2.1c). Here the MPS matrices $A^i$ are $\chi \times \chi$ matrices where $\chi$ is called the *virtual dimension* or *bond dimension* of the MPS. These matrices act in the *virtual space* of the tensor network. The origin of the name MPS is now apparent: The overlap of $|\psi\rangle$ with any configuration of the local spins $|s_1 s_2 \ldots s_N\rangle$ is efficiently determined by tracing the product of matrices $A[s_1]A[s_2]\ldots A[s_N]$, where $A[s] = \left(\sum_i \langle s|i\rangle A^i\right)$. This fact, combined with the fact that we now have only $d\chi^2$ coeffcients ($Nd\chi^2$ in the absence of translation invariance) rather than $d^N$, underpins the success of MPS in 1D numerical techniques such as the density matrix renormalization group [52, 53].

If we choose to have open boundary conditions, our state takes the general form of

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \langle R|A^{i_N} A^{i_{N-1}} \ldots A^{i_1}|L\rangle |i_1 \ldots i_N\rangle. \tag{2.3}$$

Here, the boundary conditions are specified by the vectors $|L\rangle$ and $|R\rangle$ living in the virtual space, see Fig. 2.1d). The open boundary form is what we will consider for the remainder of this thesis.

**Example: The AKLT state**

The prototypical example of a MPS is the Affleck-Kennedy-Lieb-Tasaki (AKLT) state [54]. This is the ground state of the following spin-1 Hamiltonian written in terms of the spin-1 operators $\vec{S}_j$ acting on site $j$:

$$H = \sum_j \frac{1}{2}\vec{S}_j \cdot \vec{S}_{j+1} + \frac{1}{6}\left(\vec{S}_j \cdot \vec{S}_{j+1}\right)^2 + \frac{1}{3}. \tag{2.4}$$

The AKLT state can be written as a MPS with $\chi = 2$. The MPS matrices are the Pauli matrices, $A^i = \sigma^i$, with respect to the *wire basis* $\mathcal{B} = \{|x\rangle, |y\rangle, |z\rangle\}$ where $|i\rangle$ is the 0 eigenstate of the $i$-th component of $\vec{S}$. This example will be referred to several times throughout this thesis due to its relevance to both quantum phases and quantum computation.

### 2.2.1 Injectivity

In this thesis, we will only consider MPS that satisfy a property called *injectivity*. This condition is equivalent to many important physical properties, and it also is an essential tool in proofs due to its connection to quantum channels.

One motivation for this assumption, besides its technical use, is related to certain experimental considerations. To every MPS, we can associate a gapped, local *parent Hamiltonian* for which the MPS is a (possibly degenerate) ground state [49]. Injectivity is equivalent to the condition that the MPS with periodic boundaries is the unique ground state of its parent Hamiltonian [49]. If we aim to prepare our states by cooling a physical system subject to the parent Hamiltonian, then this uniqueness is essential.

To define injectivity, we need to introduce the following quantum channel:

$$\mathcal{E}(X) = \sum_i A^i(X) A^{i\dagger}. \tag{2.5}$$

Such a channel is naturally associated to every MPS, and it encodes many of the important physical properties. It will also appear as part of our computational scheme in the next chapter. We can always assume that the largest eigenvalue of this map is 1 by proper normalization of the MPS matrices. Since this channel is completely positive, it always has a positive fixed point $\rho_{\text{fix}}$ [49]. One possible definition of injectivity is in terms of the other eigenvalues of $\mathcal{E}$:

**Definition 1.** *[49] A MPS is injective if the channel $\mathcal{E}$ has only one eigenvalue of modulus 1.*

This definition shows that, for injective MPS, $\rho_{\text{fix}}$ is the unique fixed point of $\mathcal{E}$. While we have chosen this as our definition of injectivity, there are a number of equivalent conditions on both $\mathcal{E}$ and the MPS matrices $A^i$:

**Theorem 1.** *[55] Given a MPS described by the matrices $A^i$, the following conditions are equivalent:*

1. *The MPS is injective.*
2. *The map defined by $\Gamma_L(X) = \sum_{i_1 \dots i_L} \operatorname{Tr}\left(X A^{i_L} \dots A^{i_1}\right) |i_1 \dots i_L\rangle$ is injective for some finite $L$.*
3. *The set of products matrices $\{A^{i_1} A^{i_2} \dots A^{i_L}\}$ spans the whole space of $\chi \times \chi$ matrices for the same $L$ as in condition (2).*

4. *There exists some $q \leq L$ such that, for every density operator $\rho$, $\mathcal{E}^q(\rho)$ has full rank.*

All of these conditions will be relevant to our cause. For example, we may use them to deduce useful physical properties that are consequences of injectivity, in addition to uniqueness of ground state. Perhaps the most immediate is that an injective MPS has a finite correlation length. A simple calculation shows that the correlation length of a MPS is given by $\xi = -1/\ln|\lambda_1|$ where $\lambda_1$ is the second largest eigenvalue of $\mathcal{E}$ [56]. This is finite if and only if $\mathcal{E}$ is injective.

A consequence of condition (2) is that injectivity is necessary for computational readout. The map $\Gamma_L$ can be interpreted as a map from the boundary conditions of an open boundary chain of length $L$ to the resulting quantum state (set $X = |L\rangle\langle R|$ to regain the form of Eq.2.3). If this map is injective then different boundary conditions give rise to different states. This will be important to us later on when we encode information in the virtual state $|L\rangle$. If different states $|L\rangle$ gave the same physical state, then we could not reliably deduce the information it encodes.

### 2.2.2 Canonical form and symmetries

Given a state $|\psi\rangle$, there is freedom in the choice of MPS representation. Given a set of MPS matrices $A^i$, one way to obtain a new set of matrices $B^i$ which represent the same state is by a *gauge transformation*, $B^i = XA^iX^{-1}$ $\forall i$ for some invertible matrix $X$. It is clear the matrices $B^i$ generate the same MPS as $A^i$ since the transformation matrices $X$ annihilate pairwise in the virtual space.

Using a gauge transformation it is possible to put any MPS into a *canonical form* which has particularly nice properties:

**Theorem 2.** *[49] Given any translationally invariant and injective MPS, it is always possible to use gauge transformations such that*

- *The unique fixed point $\rho_{\text{fix}}$ of the channel $\mathcal{E}$ is the identity matrix $\mathbb{I}$.*
- *The adjoint channel $\mathcal{E}^\dagger(X) = \sum_i A^{i\dagger}(X)A^i$ has a unique fixed point $\Lambda$ which can be taken to be a density matrix.*

In the non-injective case, an MPS decomposes as a superposition of injective MPS, each of which satisfy the theorem. The canonical form of an MPS is unique up to a unitary gauge transformation, a fact which is essential to classifying symmetries in MPS. Indeed, we have the following fundamental

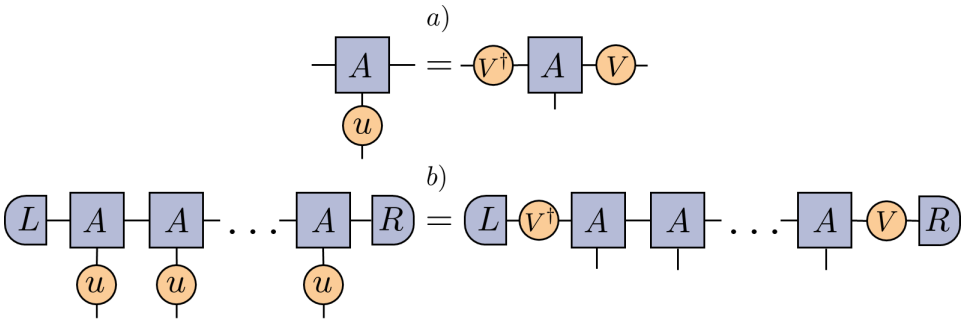


Figure 2.2: a) Illustration of Theorem 3. b) The on-site symmetry is equivalent to a virtual symmetry.

result regarding on-site symmetries, which are symmetries which act locally at every site in the same way:

**Theorem 3.** *[57] For an injective MPS, a unitary $u$ is an onsite symmetry, $u^{\otimes N}|\psi\rangle = |\psi\rangle$, if and only if there exists a unitary $V$ and a phase $e^{i\theta}$ such that $\sum_j u_{ij} A^j = e^{i\theta} V^\dagger A^i V$*

From now on, we will absorb the phase $e^{i\theta}$ into the unitary $u$ such that we can ignore it without loss of generality. See Fig. 2.2a) for a tensor network diagram illustrating this result. This result shows that it is possible to deduce the presence of an on-site symmetry of the whole state using only the symmetry properties of a single tensor $A^i$. Furthermore, it shows that acting with the symmetry on the physical index is equivalent to a unitary gauge transformation on the virtual indices. Because of this, acting on all spins of an open chain with the symmetry $u$ is equivalent to acting on the boundary states with $V$, see Fig. 2.2b). These facts are essential to our understanding of quantum phases and quantum computation in 1D.

## 2.3 Quantum phases of matter

In this section, we consider quantum phases of matter. These are families of quantum states at zero temperature that cannot be connected without passing through a phase transition, marked by the divergence of some physical observable. The simplest of phase transitions can be explained by *spontaneous symmetry breaking* [58]. This process is defined by the situation in which the ground state has less symmetry than the Hamiltonian, and can be completely understood by examining the original symmetry group and

the broken symmetry subgroup. Because of this, the theory of symmetry breaking phases of matter can be completely described using elementary group theory.

However spontaneous symmetry breaking is inherently associated with ground state degeneracy [59], and hence it is excluded by our assumption of injectivity. Hence, in this section we consider the *topological* phases of matter, which do not involve symmetry breaking. We begin with a definition that reveals the nature of such phases, and then give an example of how they may be classified using MPS technology, leading to mathematical structure beyond elementary group theory.

### 2.3.1 Definition of gapped phases of matter

In this section, we define *gapped phases of matter*, which are equivalence classes of ground states of gapped quantum systems related by finite depth quantum circuits [60]. A quantum circuit is defined by $k$ layers of local unitaries that act on a state, see Fig. 2.3. Finite depth means that $k$ does not grow with the size of the state (here, the length of the spin chain). Precisely, we define quantum phases as follows:

**Definition 2.** *[60] Two injective states $|\psi_0\rangle$ and $|\psi_1\rangle$ are in the same gapped quantum phase if there exists a finite depth circuit $U_c$ such that $U_c|\psi_0\rangle \propto |\psi_1\rangle$.*

Under this definition, the trivial phase contains all short-range entangled states—those that can be transformed into local product states—and non-trivial phases are referred to the topological phases of matter. While this definition may seem unfamiliar, it turns out to be essentially equivalent to the definition that two states are in different phases if and only if they cannot be smoothly connected without passing through a phase transition [60].

This definition can be refined in the presence of symmetry. If a state $|\psi\rangle$ has a symmetry $G$, such that $U(g)|\psi\rangle = |\psi\rangle \ \forall g \in G$ for some representation $U$ of $G$, then we can add the additional constraint that the finite depth circuit $U_c$ must also respect this symmetry, $[U_c, U(g)] = 0 \ \forall g \in G$. Even the trivial phase can split into many non-trivial phases in the presence of symmetry. These short-range entangled phases are called the *symmetry-protected topological* (SPT) phases of matter [5, 6, 7]. We note that it is possible to extend the definition of SPT phases such that the representation $U$ of the symmetry group $G$ can vary throughout the phase [6]. In order to not exclude this definition, we will also allow $U$ to vary throughout our SPT phases.

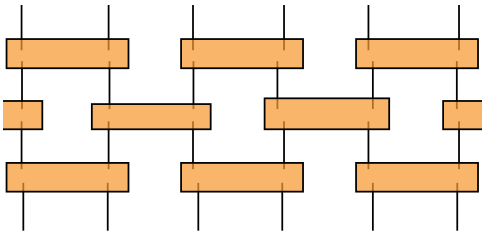

Figure 2.3: A finite depth quantum circuit contains several layers of local gates (3 layers pictured), where the number of layers does not grow with system size.

These definitions reveal the nature of quantum phases: they are defined by the entanglement structure of states. Topological order is characterized by patterns of long-ranged entanglement that cannot be removed by the local operations of a finite depth circuit, whereas SPT order is characterized by short-ranged, symmetric entanglement which cannot be removed by symmetric local operations. This is the key insight of this section, as it is precisely this symmetric entanglement that allows us to achieve quantum computation with SPT phases.

### 2.3.2 Symmetry-protected topological phases in 1D

In this section we apply the MPS formalism to explain how SPT phases can be classified in 1D. We consider MPS $|\psi\rangle$ with an onsite symmetry represented by a group $G$, meaning that there exists a unitary representation $u$ of $G$, which acts on a single spin in the chain, such that $u(g)^N|\psi\rangle = |\psi\rangle$ $\forall g \in G$. Typical examples of an onsite symmetry are spin-flip symmetry ($G = \mathbb{Z}_2$) and spin-rotation symmetry ($G = SU(N)$). While it is possible to also consider spatial symmetries like inversion and non-unitary time-reversal symmetry, here we restrict to unitary on-site symmetries.

The basic argument is this: On an open chain, we have degrees of freedom localised near the edge, spanned by the boundary vectors $|L\rangle$ and $|R\rangle$. As shown in Fig. 2.2b), which now holds for all $g \in G$, the symmetry $u(g)$ acts as $V(g)$ on these edge modes. The non-trivialness of the SPT phase comes from the fact that these operators can be non-trivial representations of the symmetry. What is the structure of the operators $V(g)$ acting in the virtual space? By using the fact that $u(g)u(h) = u(gh)$, we find that

$$V(g)^\dagger V(h)^\dagger A^i V(h) V(g) = V(gh)^\dagger A^i V(gh). \tag{2.6}$$

If we apply this relation to $L$ sites in a row, where $L$ is the constant appearing in Theorem 1, we find that the above relation holds with $A^i$ replaced by $A^{i_1} \dots A^{i_L}$. By injectivity, the sets of such products span the space of whole matrices. Hence $V(g)V(h)V(gh)^\dagger$ commutes with every matrix, and hence it must be a scalar matrix. Then we can write

$$V(g)V(h) = \omega(g,h)V(gh), \tag{2.7}$$

showing that $V(g)$ is a *projective representation* of $G$, with $\omega(g,h)$ the *factor system*. In the language of group cohomology $\omega(g,h)$ is called a *cocycle*. The details of this language are not necessary to understand our results, so we do not include them here. A detailed discussion of group cohomology and its application to SPT phases can be found in Refs. [5, 7].

Notice that $V(g)$ appears with its complex conjugate in Fig. 2.2a). This means that we are free to rephase the representation, writing $V'(g) = \beta(g)V(g)$ for any phases $\beta(g)$. If we rephase the representation in this way, the factor system is changed to $\omega'(g,h) = \frac{\beta(gh)}{\beta(g)\beta(h)}\omega(g,h)$. The factor $\frac{\beta(gh)}{\beta(g)\beta(h)}$ is called a *coboundary*. We say that two cocycles are equivalent if they differ only by a coboundary, as above, and denote equivalence classes by the *cohomology class* $[\omega]$. The different cohomology classes form a finite group $H^2[G, U(1)]$ called the second cohomology group of $G$.

In Refs. [5, 6], it was proven that two states of a spin chain are in the same SPT phase if and only if the projective representations of the symmetry acting on the virtual level of the MPS correspond to the same cohomology class. In a hand-waving argument, this makes sense because it is impossible to smoothly interpolate between two such discrete labels, hence they label different phases. This means that, given a group $G$, the different possible phases are labelled by elements of $H^2[G, U(1)]$, with the identity element labelling the trivial phase. We see that, in the same way group theory describes the possible symmetry breaking phases, group cohomology is the language used to classify SPT phases.

**Example: SPT order of AKLT state**

We can use the above classification to show that the AKLT state has non-trivial SPT order. The symmetry group we consider consists of $\pi$ rotations about the $x$, $y$, and $z$ axes; $G = \{e, R_x(\pi), R_y(\pi), R_z(\pi)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Our basis $\mathcal{B} = \{|x\rangle, |y\rangle, |z\rangle\}$ consists of rotation eigenstates, such that $R_i(\pi)$ leaves $|i\rangle$ invariant while giving the other two basis states a $-1$ phase factor, $i = x, y, z$. It is straightforward to check that this symmetry action can be achieved in the virtual space by setting $V(R_i(\pi)) = \sigma^i$. The Pauli matrices

form a non-trivial projective representation of $\mathbb{Z}_2 \times \mathbb{Z}_2$, as evidenced by the fact that they do not commute. Hence, the AKLT state has non-trivial order protected by $\mathbb{Z}_2 \times \mathbb{Z}_2$. The corresponding SPT phase is known as the Haldane phase, which is another key example for the next chapter.

## 2.4 Measurement-based quantum computation

As stated in the introduction, *measurement-based quantum computation* (MBQC) is model of quantum computation in which the quantum resource is an entangled state of a many-body quantum system [24, 25]. Initialization, processing, and readout of information are all executed by interpreting the outcomes of single-site projective measurements performed on the resource state. Which algorithm is executed is controlled by the order in which the sites are measured and the basis of measurement at each site. The computational power of an MBQC scheme, defined by the set of logical gates that can be executed, is related to the entanglement structure of the resource state.

Identifying the common properties of universal resource states, those which leads to universal computation, is an ongoing problem in the field. With too little entanglement, measurement can be efficiently simulated with a classical computer [61, 62, 63]. However, it turns out that most quantum states, in a quantifiable sense, are too entangled to be useful [64, 65]. Somehow, there exists a "sweet spot" of entanglement which balances richness and structure. This thesis aims to argue that this particular kind of entanglement is exactly that which is present in resource states with SPT order. To this effort, we use this section to show how MBQC can be understood in the MPS picture.

### 2.4.1 Computation in virtual space

The MPS representation of a spin chain leads to a unique picture of MBQC that occurs in the virtual space of the tensor network [66, 67]. Consider a resource state with open boundaries in the form of Eq. 2.3. If we measure the first spin in the chain with measurement outcome $|s\rangle$, then the resulting state of the rest of the chain is:

$$|\psi'\rangle = \sum_{i_2,\ldots,i_N} \langle R|A^{i_N} A^{i_{N-1}} \ldots A^{i_2}|L'\rangle|i_2 \ldots i_N\rangle. \tag{2.8}$$

where $|L'\rangle = \frac{1}{p_s} A[s]|L\rangle$ and $p_s$ is the probability of measuring outcome $|s\rangle$. We see that the length of the chain has been reduced by 1, and the left

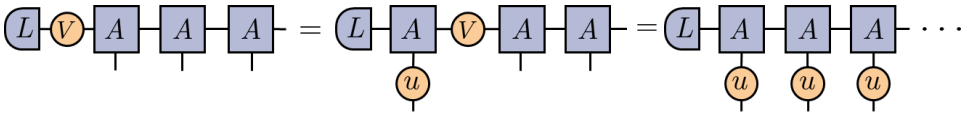


Figure 2.4: Byproduct propagation by symmetry

boundary condition has evolved in some way that depends on the measurement outcome $|s\rangle$. We are interested in resource states for which this operator is unitary for a proper choice of measurement basis, perhaps only on a subspace of the virtual space. In this case, projective measurement of the physical system is equivalent to unitary evolution of the virtual system. This is the strength of the virtual space picture of MBQC.

An essential aspect of MBQC is *byproduct propagation*. While we can ideally choose any basis for our measurement, we cannot control the outcome of measurement. For a given outcome, we decompose the resulting operator into the desired gate and an outcome-dependent *byproduct operator* acting in the virtual space. In general, this byproduct operator must be *propagated* through the computation by altering the bases of future measurements. In this way, we can eliminate part of the outcome-dependence of the computation.

The virtual space picture provides a particularly nice picture of byproduct propagation in terms of MPS symmetries [35]. Indeed, suppose that our byproduct operator is an element $V(g)$ of the virtual representation of $G$. Then, by Fig. 2.2, if we act with $u(g)$ on the next physical site, we can propagate the byproduct operator past this site, see Fig. 2.4. This operation is achieved by modifying our intended measurement basis $\{|i\rangle\}$ to $\{u(g)|i\rangle\}$. We can modify all future measurement bases in this same way to propagate the byproduct to the very end of computation, where it affects the basis used for computational readout. It will turn out that, for resource states with certain types of SPT order, the byproduct operators are always in the virtual symmetry representation, so they can always be propagated in this way.

**Example: Computation with AKLT state**

The AKLT state provides a simple example of MBQC in virtual space [68]. To achieve a rotation by $\theta$ about the $z$-axis, we measure in the basis

$$\mathcal{B}(z,\theta) = \{|\theta_x\rangle, |\theta_y\rangle, |z\rangle\} \equiv \left\{\cos\frac{\theta}{2}|x\rangle - \sin\frac{\theta}{2}|y\rangle, \sin\frac{\theta}{2}|x\rangle + \cos\frac{\theta}{2}|y\rangle, |z\rangle\right\}. \tag{2.9}$$

The resulting operator in virtual space for each possible measurement outcome is:

$$\begin{aligned} |\theta_x\rangle &: \ \sigma^x e^{-i\theta\sigma^z/2} \\ |\theta_y\rangle &: \ \sigma^y e^{-i\theta\sigma^z/2} \\ |z\rangle &: \ \sigma^z \end{aligned} \tag{2.10}$$

As we saw in the previous section, the virtual representation of the AKLT state's $\mathbb{Z}_2 \times \mathbb{Z}_2$ symmetry consists of the Pauli matrices. Hence, we can treat any Pauli matrix acting in the virtual space as a byproduct operator. After propagation, we see that the first two results give the desired rotation, while the third enacts the identity gate. We see that computation with the AKLT state is probabilistic; the executed gate depends on the measurement outcome even after byproduct propagation. However, if the gate fails, one can simply attempt the rotation again, so that the only effect of this outcome dependence is an indeterminate length of chain needed to execute a computation.

One can similarly achieve arbitrary rotations about the $x$ (and $y$) axes, thereby giving a full set of single-qubit $SU(2)$ gates. Since the AKLT state encodes only one qubit of information, we will say that it is a universal resource state, in a slight abuse of terminology. Is it possible that every state within the Haldane phase has the same universality AKLT state? This question is answered affirmatively in the next section.

## 2.5 Computational phases of matter

In an effort to understand the structure of resource states for MBQC, one may ask the following question: If we begin with a universal resource state and perturb it in some way, does it remain universal? This question began by looking at perturbations caused by non-zero temperature [39, 27, 69] and lattice site deletion [26, 67]. In each case, it was shown that the resource remained useful up to a certain threshold temperature or loss rate, which in

some cases also corresponded to a physical phase transition. This was the first evidence that phases of computational power may overlap with physical phases.

The idea of looking at zero-temperature quantum phases as resources began with the effort to find resource states which are ground states of natural Hamiltonians, which naturally led to the question of whether changes in the parameters of these Hamiltonians could affect resource quality [70, 28, 29]. To track the history of our approach and the connection to SPT phases, it is best to start with Miyake, who showed that the aforementioned computational power of the AKLT state persists throughout an $SO(3)$ invariant subset of the Haldane phase [30]. This approach required more control than only projective measurements, but this was remedied the next year by Bartlett *et. al.* [31]. The new scheme, dubbed "computational renormalization", used measurements to drive the resource state back towards the AKLT point, allowing computation to proceed. This scheme was unfortunately heavily specialized to the specific phase under consideration, and could not be easily generalised.

Later, a general result from Else *et. al* put the resource quality of Haldane phase on clearer footing using the language of MPS [35, 36]. They showed that, for every phase with in the Haldane phase, the MPS matrices take the form:

$$A^i = B^i \otimes \sigma^i \tag{2.11}$$

for some square matrices $B^i$. Since the AKLT state satisfies $A^i = \sigma^i$, we see that every state in the Haldane phase can be viewed as an AKLT state with some additional entanglement on top. The microscopic details of this entanglement are encoded in the $B^i$ matrices, which vary freely throughout the phase, subject only to constraints of injectivity. We call the subspace of virtual space in which the Pauli part acts the *logical subspace*, while the matrices $B^i$ act in the *junk subspace*. The $\mathbb{Z}_2 \times \mathbb{Z}_2$ symmetry acts non-trivially only in the logical subspace, $V(R_i(\pi)) = \mathbb{I} \otimes \sigma^i$.

This result immediately explains the ability for states in the Haldane phase to execute the identity gate, ie. to transport quantum state along a spin chain via measurement [36]. Indeed, measuring in the wire basis results in Pauli evolution of the logical subspace which can be propagated via symmetry. If we encode our logical qubit $|\phi\rangle$ in this subspace, $|L\rangle = |J\rangle \otimes |\phi\rangle$ for some state $|J\rangle$, then measurement in the wire basis enacts the identity gate, as claimed. Since all microscopic details appear in the junk subspace, this works even without knowledge of which state in the phase is being

used [2].

The importance of this result came from its generality: it applies to any phase satisfying a condition they called *maximal non-commutativity*, which we define later. Thus any state coming from a maximally non-commutative SPT phase can act as a quantum wire. Unfortunately, this uniform computational power appeared to be restricted to the identity gate only. To achieve a non-trivial gate, the basis of measurement must be changed. But measurement outside of the wire basis will in general result in entanglement between the junk and logical subspaces [36]. Consider the case the measurement outcome $\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$ is obtained, giving

$$|J\rangle \otimes |\phi\rangle \to \frac{1}{\sqrt{2}} \left( B^x |J\rangle \otimes \sigma^x |\phi\rangle + B^y |J\rangle \otimes \sigma^y |\phi\rangle \right). \tag{2.12}$$

Unless $B^x = B^y$, the resulting state is entangled between the two subspaces. Since there is no reason for this to hold in general, a random state from the phase cannot be used as a resource for non-trivial gates, at least not without some additional steps to the computation.

This was partially solved by Miller and Miyake, who translated the computational renormalization scheme of Bartlett *et. al.* into the MPS language [37]. They showed that, for the non-trivial SPT phase protected by $S_4$, which is contained in the Haldane phase, the computational renormalization scheme has the effect of driving $B^y$ and $B^x$ to the same operator, such that the above measurement will not entangle the subspaces. This allowed them to prove that the entire $S_4$ phase could be used for $SU(2)$ rotations of the logical qubit. Once again, this scheme relied on some specific properties of the particular phase, and could not obviously be extended to the other maximally non-commutative phases.

These works leave open several questions. Can other SPT phases support non-trivial gates throughout the phase? Can the maximal non-commutativity assumption be removed? Is there a way to determine which phases lead to universal sets of gates? In the following chapters, we answer all three questions affirmatively in the order given. We construct a novel scheme that allows non-trivial gates throughout the entire Haldane phase, as well as every other maximally non-commutative phase. We then remove the maximal non-commutativity property and examine what modifications to our scheme are required to still allow computation. We then determine which gates can be executed in each SPT phase.

[2] In reality, the steps required to initialize information into the logical subspace and later read it out cannot be performed without some knowledge of the microscopic details, as observed in Ref. [71]

# Chapter 3

# Computation with maximally non-commutative SPT phases

In this section, we introduce three simple modifications to the usual MBQC scheme that allow the computational power of the AKLT state to extend throughout the entire Haldane phase. These modifications are described in Fig. 3. We then extend this scheme to all maximally non-commutative phases.

## 3.1 Computation in the Haldane phase

We begin this section by introducing the *mixed state interpretation* of MBQC that will be used throughout this letter. Here we argue its validity, with a formal proof given in the Appendix. We define a computation by a sequence of $n$ measurement bases, which are fixed modulo byproduct propagation. That is, we do not allows a "trial-until-success" strategy as is required in the computational renormalization scheme mentioned in the previous chapter.

In general, an input state $|\psi\rangle$ will be taken to a final state $|\psi_{\vec{s}}\rangle$ which depends on the measurement outcomes $\vec{s} = (s_1, \ldots, s_n)$. Then we measure some observable $O$ on $|\psi_{\vec{s}}\rangle$, whose eigenvalues $o_i$ appear with probability $p(o_i|\vec{s})$. To garner measurement statistics of $O$, we must repeat the computation many times, whereupon the full statistics are given by $p(o_i) = \sum_{\vec{s}} p(o_i|\vec{s})p_{\vec{s}}$ where $p_{\vec{s}}$ is the probability of outcomes $\vec{s}$. These statistics are encoded in the mixed state $\hat{\sigma} = \sum_{\vec{s}} p_{\vec{s}} |\psi_{\vec{s}}\rangle\langle\psi_{\vec{s}}|$, for instance $\langle O\rangle = \sum_{\vec{s}} p_{\vec{s}} \langle\psi_{\vec{s}}|O|\psi_{\vec{s}}\rangle \equiv \mathrm{Tr}\,(O\hat{\sigma})$. Hence in this probabilistic scenario the computational output must be interpreted to be $\hat{\sigma}$.

To determine the mixed state $\hat{\sigma}$, we simply sum over all possible outcomes of each measurement. It is crucial that this sum-over-outcomes is implemented *after* byproduct propagation, making it very different from simply tracing over each spin in the chain. The byproducts accumulated at

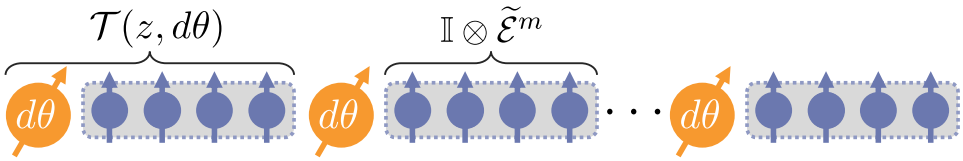


Figure 3.1: Illustration of the measurements needed to execute a rotation about the $z$-axis in the Haldane phase example. Our scheme consists of three modifications to the usual MBQC procedure: (1) In analysis of the scheme, measurement outcomes are summed over, such that the computational output is interpreted as a mixed state, (2) finite rotations are split into smaller pieces $d\theta$ that each differ only slightly from the identity, and (3) consecutive gates are separated by many applications of the identity gate.

the end of the computation affect the basis of computational readout, during which we do not sum over outcomes. By analysing the computation in this way, we can design a sequence of measurement bases such that $\hat{\sigma}$ approximates the desired output. If the computation defined by this sequence of measurements is repeated many times, it will deterministically produce the desired measurement statistics of any observable $O$, even though each run of the algorithm may produce a different output state that is meaningless on its own.

Let us return to the AKLT state as an example. By measuring in the basis $\mathcal{B}(z, \theta)$ and summing over measurement outcomes, we find that an initial state $|L\rangle\langle L|$ becomes:

$$\hat{\sigma} = \frac{2}{3} e^{-i\theta\sigma_z/2} |L\rangle\langle L| e^{i\theta\sigma_z/2} + \frac{1}{3} |L\rangle\langle L|. \tag{3.1}$$

Since the original gate is probabilistic, this is a mixed state and does not represent unitary evolution. However, for small angles $d\theta$, it is unitary up to first order:

$$\hat{\sigma} = e^{-i\frac{2}{3}d\theta\sigma_z/2} |L\rangle\langle L| e^{i\frac{2}{3}d\theta\sigma_z/2} + \mathcal{O}(d\theta^2). \tag{3.2}$$

So for small rotation angles $d\theta$, the mixed output state is our initial state rotated by a reduced angle $\frac{2}{3}d\theta$ about the $z$-axis. Restriction to gates that are close to the identity is an unavoidable consequence of the mixed state interpretation, and finite rotations must be split into many infinitesimal pieces. The number of measurements needed to execute a unitary gate with rotation angle $\theta$ and admissible error $\epsilon$ is $\mathcal{O}(\theta^2/\epsilon)$, as we discuss in detail at the end of this section.

Now consider the effect of a measurement in the infinitesimally tilted basis $\mathcal{B}(z, d\theta)$ on an arbitrary state in the Haldane phase. Without loss of generality, we assume that our initial state is factorized across the subspaces as $\mathbb{I} \otimes |\phi\rangle\langle\phi|$. If we get the outcome $|\theta_x\rangle$ and propagate $\sigma^x$ on the logical subspace, our state becomes:

$$\begin{aligned} &\mathbb{I} \otimes |\phi\rangle\langle\phi| \to B^x B^{x\dagger} \otimes |\phi\rangle\langle\phi| \\ &+ i\frac{d\theta}{2}\left(B^x B^{y\dagger} \otimes |\phi\rangle\langle\phi|\sigma^z - B^y B^{x\dagger} \otimes \sigma^z |\phi\rangle\langle\phi|\right), \end{aligned} \tag{3.3}$$

up to first order in $d\theta$. As before, we see that the two subsystems are no longer factorized, and the logical state $|\phi\rangle\langle\phi|$ has become entangled with the microscopic details of the junk state.

To remedy this, we will flow the junk subspace towards a fixed point using a technique called the *oblivious wire*. The oblivious wire is implemented simply measuring a large number $m$ of spins in the wire basis, pictured in Fig. 3 as a dotted box. In the mixed state interpretation, a measurement in the wire basis followed by logical byproduct propagation effects the operation $\sum_i B^i(\cdot)B^{i\dagger} \otimes \mathbb{I} \equiv \widetilde{\mathcal{E}} \otimes \mathbb{I}$. Since our resource state is injective $\widetilde{\mathcal{E}}$ will have a unique fixed point $\mathbb{I}$, since otherwise $\mathcal{E}$ would have more than one fixed point. Hence the oblivious wire results in the linear channel $\widetilde{\mathcal{E}}^m \otimes \mathbb{I}$ that projects the junk subspace onto the fixed point $\mathbb{I}$. The projection occurs exponentially fast over the correlation length $\xi$ of the state.

Applying this to Eq. 3.3, which must be summed with its counterparts for the other measurement outcomes $|\theta_y\rangle$ and $|z\rangle$, we find that for large enough $m$,

$$\hat{\sigma} = \mathbb{I} \otimes \left(\nu|\phi\rangle\langle\phi| + i\frac{d\theta}{2}(\nu^{xy} + \nu^{yx})\left[|\phi\rangle\langle\phi|, \sigma^z\right]\right), \tag{3.4}$$

where we have defined $\lim_{m\to\infty} \widetilde{\mathcal{E}}^m(B^i B^{j\dagger}) = \nu^{ij}\mathbb{I}$ and $\nu = \nu^{xx} + \nu^{yy} + \nu^{zz}$. Up to first order in $d\theta$, this corresponds to a unitary rotation acting on the logical subspace:

$$\mathcal{T}(z, d\theta) = \exp\left\{-id\theta\left(\frac{\nu^{xy} + \nu^{yx}}{2\nu}\right)\sigma^z\right\}. \tag{3.5}$$

Hence, making a measurement in the rotated basis $\mathcal{B}(z, d\theta)$, followed by a series of measurements in the wire basis, produces the desired rotation of the virtual state $|\phi\rangle$ up to a scaling factor $\frac{\nu^{xy}+\nu^{yx}}{\nu}$. As long as this factor is non-zero, it can be measured on the chain prior to computation by attempting a finite rotation (split into small pieces), and measuring the reduction in

rotation angle. The parameters $\nu^{ij}$ contain all relevant microscopic details of our resource state. Since they can be measured during a calibration step, any state in the phase can be used as a resource without prior knowledge of its identity.

We can repeat the above procedure for rotations about the $x$-axis to generate all of $SU(2)$. Hence every state in the Haldane phase, with the exception of a null subset in which some of the constants $\nu^{ij}$ are 0, has the same computational power as the AKLT state (which satisfies $\nu^{ij} = \frac{1}{3}\ \forall i, j$).

## 3.2 Generalization to maximally non-commutative phases

The above techniques do not depend on any properties that are particular to the Haldane phase, so they can be generalised to a large class of other SPT phases. The Haldane phase is an example of a maximally non-commutative SPT phase, first defined in Ref. [36]. Such phases satisfy all conditions needed to apply our methods, namely the existence of a logical subspace and the ability to propagate byproduct operators within it. Indeed, suppose that $G$ is finite abelian and $[\omega]$ is maximally non-commutative, meaning $\{g \in G | \omega(g, g') = \omega(g', g)\ \forall g' \in G\} = \{e\}$. By diagonalizing the representation $u$, we obtain the wire basis $\mathcal{B} = \{|0\rangle, \ldots, |d-1\rangle\}$ such that $u(g)|i\rangle = \chi^i(g)|i\rangle\ \forall g \in G$ where $\chi^i(g)$ are linear characters of $G$. Maximal non-commutativity then implies the MPS tensor $A^i$ can be written in the wire basis as [36]:

$$A^i = B^i \otimes C^i, \tag{3.6}$$

where $C^i$ are $D \times D$ unitary and trace-orthogonal matrices and $D = \sqrt{|G|}$ is the dimension of our logical subspace [3]. $C^i$ can be determined uniquely from $G$, $[\omega]$, and $\chi^i$ as described in Chapter 4. Furthermore, the operators $\mathbb{I} \otimes C^i$ are always in virtual representation of the symmetry group, so they can be propagated as byproducts in the usual way. In general, if some group $G$ has a finite abelian subgroup $H$ such that $[\omega|_H]$ is maximally non-commutative, we can make the exact same argument with $H$ taking the place of $G$ everywhere. This means the following results also apply to certain non-abelian groups and Lie groups. A full proof of these results is given in greater generality in the next chapter.

[3] $D$ is always defined since any finite abelian group which supports a maximally non-commutative factor system must have the form $G \cong G' \times G'$ for some subgroup $G'$ [72].

Now we add the same three ingredients used to perform computation in the Haldane phase: the mixed state interpretation, restriction to infinitesimal gates, and the oblivious wire. Measurement in the slightly tilted basis $\mathcal{B}(i,j;d\theta,\varphi) = \{|0\rangle,\ldots,|i\rangle + d\theta e^{i\varphi}|j\rangle,\ |j\rangle - d\theta e^{-i\varphi}|i\rangle,\ldots,|d-1\rangle\}$, followed by the oblivious wire to drive the junk subspace to a fixed-point state, induces an infinitesimal rotation in the logical subspace:

$$\mathcal{T}(i,j;d\theta,\varphi) = \exp\left\{d\theta\frac{|\nu^{ij}|}{\nu}\left(e^{i(\varphi+\delta^{ij})}C^{i\dagger}C^{j} - e^{-i(\varphi+\delta^{ij})}C^{j\dagger}C^{i}\right)\right\}, \tag{3.7}$$

where $\nu^{ij} = |\nu^{ij}|e^{i\delta^{ij}}$ is as defined earlier and $\nu = \sum_{i=0}^{d-1}\nu^{ii}$. As before, the microscopic details of the state enter only as these measurable constants. Computation can only proceed if these constants are non-zero, which is satisfied for all but a null set of states. With knowledge of these constants, $\mathcal{B}(i,j;d\theta,\varphi)$ can be chosen such that the primitive gates are generated by elements of the set of anti-hermitian operators:

$$\mathcal{O} = \left\{\alpha C^{i\dagger}C^{j} - \alpha^{*}C^{j\dagger}C^{i}\right\} \tag{3.8}$$

with $i,j = 0\ldots d-1$, $i \neq j$, $|\alpha| \ll 1$. Furthermore, we have $e^{d\theta A}e^{d\theta B}e^{-d\theta A}e^{-d\theta B} \approx e^{(d\theta)^2[A,B]}$, so that our infinitesimal generators form a real Lie algebra $\mathcal{A}[\mathcal{O}]$ which in turn generates a Lie group $\mathcal{L}[\mathcal{O}]$ of executable gates.

To complete the scheme, we would require a method to read out and initialize the virtual state which also works throughout the phase. In Ref. [2], it is shown that, by measuring in finitely tilted bases, rather than the infinitesimally tilted bases used for gates, one can approximate a projective measurement of any observable in $\mathcal{O}$ on the logical subspace. This suffices for both initialization and readout.

## 3.3 Error and cost analysis

The gates described above are only approximations of the desired gate. Here we address the question of what the computational cost is to implement a unitary gate with rotation angle $\theta$ while allowing for an error $\epsilon$. The basic argument is that if a rotation about an angle $\theta$ is subdivided into $N$ rotations about an angle $\theta/N$, then the error per individual small rotation is of order $(\theta/N)^2$, and the cumulative error over $N$ such rotations is thus $\epsilon_N = \mathcal{O}(1/N)$. Hence, to get by with a total error of $\epsilon$, we require a subdivision of the rotation into $N \sim 1/\epsilon$ steps.

In more detail, there are two sources of error in the present construction for unitary gates. First, an elementary unitary operation with small rotation angle $d\theta$ incurs an error at second order in $d\theta$, as discussed above. Second, every individual rotation $\mathcal{T}(d\theta)$ requires the junk system to be brought into the fixed point state $\rho_{\text{fix}}$. This could be achieved by measuring an infinite number of spins in the wire basis. In any reasonable implementation, we measure only a finite number of spins, producing an error in the state of the junk system compared to the true fixed point state. Fortunately, this error is exponentially small in the number $n$ of measured spins,

$$\|\rho_{\text{junk}} - \rho_{\text{fix}}\| \sim \exp(-n/\widetilde{\xi}),$$

where $\widetilde{\xi}$ is a correlation length $\widetilde{\xi} = -\ln(\lambda_1)$ associated to the junk subsystem, with $\lambda_1$ the second-largest eigenvalue of the channel $\widetilde{\mathcal{E}}$. This correlation length is less than or equal to the true correlation length $\xi$ of our resource state.

The cumulative error due to imperfect preparation of the fixed point state of the junk system is $\epsilon_{\text{fix}} = \mathcal{O}\left(N{\lambda_1}^n\right)$. Therefore, the choice

$$n = 2\widetilde{\xi}\log N \tag{3.9}$$

leads to an error $\epsilon_{\text{fix}} = \mathcal{O}(1/N)$, which is the same scaling as for $\epsilon_N$.

Splitting the total error $\epsilon$ evenly between $\epsilon_{\text{fix}}$ and $\epsilon_N$, $\epsilon_{\text{fix}} = \epsilon_N = \epsilon/2$, we find that we can achieve a total error of $\epsilon$ for the choice

$$N \sim \frac{1}{\epsilon}.$$

With Eq. (3.9), the total cost of implementing a unitary gate within an error $\epsilon$, in terms of total number $C = N(n+1)$ of local measurements, is thus

$$C = \mathcal{O}\left(\frac{\widetilde{\xi}}{\epsilon}\log\left(\frac{1}{\epsilon}\right)\right). \tag{3.10}$$

## 3.4 Main theorem

With the above discussion, we are ready to state our first main result as the following theorem:

**Theorem 4.** *Consider a state in a symmetry-protected topological phase without symmetry breaking described by a group $G$, an on-site representation $u$, and a cohomology class $[\omega]$. If there exists a finite abelian subgroup $H \subset G$*

*such that* $[\omega|_H]$ *is maximally non-commutative, then for any state in the phase, except a null subset, a Lie group of gates determined only by* $G$*,* $u$*, and* $[\omega]$ *can be efficiently implemented in MBQC with arbitrary high gate fidelity.*

Before the computation, we must determine the constants $\nu^{ij}$ in a calibration step. The null subset refers to those states for which $\nu^{ij} = 0$ for some $i, j$.

Theorem 4 showcases the main strength of our methods. Given only the algebraic quantities $G$, $u$, and $[\omega]$ which describe the SPT phase of our resource state, we are able to define a complete MBQC scheme, including the set of gates and the measurements needed to execute them. The computational power of each state in the phase is uniformly defined as the Lie group $\mathcal{L}[\mathcal{O}]$, which is completely determined by the same algebraic quantities. This signifies the existence of a deep connection between SPT order and MBQC via the language of group cohomology. In a later chapter, we prove that this Lie group always contains a full set of single-qudit relations, regardless of the representation $u$. This shows that ground states with SPT order are generically useful as MBQC resources.

Now we must ask: which symmetry groups protect phases that satisfy Theorem 4? To answer this in general is a difficult problem of group cohomology, but we can identify some particularly relevant examples. When $G$ is a classical Lie group (except $Spin(4n)$), there is a subgroup of the form $\mathbb{Z}_N \times \mathbb{Z}_N \subset G$ such that $H^2(G, U(1)) \cong H^2(\mathbb{Z}_N \times \mathbb{Z}_N, U(1))$ [73, 74]. Since $\mathbb{Z}_N \times \mathbb{Z}_N$ protects a maximally non-commutative phase [72, 36], $G$ must protect a phase which satisfies our theorem. The same can be said for any subgroup $G'$ such that $\mathbb{Z}_N \times \mathbb{Z}_N \subset G' \subset G$. This has already been observed in Ref. [38] for the groups $D_4, A_4, S_4 \subset SO(3)$, which each contain $\mathbb{Z}_2 \times \mathbb{Z}_2$. Another example is the class of groups for which the subgroup $H$ specified in Theorem 4 appears as a (semi)direct factor, that is $G = H' \rtimes H$ for some subgroup $H'$ which could represent eg. time reversal symmetry [75].

# Chapter 4

# Computation in general abelian SPT phases

The results of the previous chapter were dependent on the condition of maximal non-commutativity of the SPT phase, which guarantees that a decomposition of the form $A^i = B^i \otimes C^i$ holds throughout the phase. Certainly this form makes it clear that there is a protected subspace in which information can be encoded, but is it required?

In Ref. [71] the idea of SPT-entanglement is introduced, although previous works investigated similar ideas [73, 76]. For all abelian SPT phases, the SPT-entanglement is a formal order parameter that detects the symmetric entanglement that is present throughout SPT phases. In this setting, there is no essential difference when assuming maximal non-commutativity; it simple corresponds to the case where the SPT-entanglement is maximised. In light of this, one is led to question whether this condition of maximal non-commutativity is necessary to perform MBQC using SPT-entanglement. In this chapter, we show that this is not, and that our computational scheme can be extended to general abelian SPT phases, which we define as phases that can be protected by a finite abelian group. Note the wording "can be protected", which emphasizes that the finite abelian group may be a subgroup of the full symmetry group.

## 4.1 A phase with no logical subspace

Before proving general results on the structure of abelian SPT phases, we present the simplest example of a non-trivial SPT phase that does not have the structure $A^i = B^i \otimes C^i$. The symmetry group is $\mathbb{Z}_4 \times \mathbb{Z}_2$. Since $H^2[\mathbb{Z}_4 \times \mathbb{Z}_2, U(1)] = \mathbb{Z}_2$, we have only one non-trivial phase. When only the $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup is enforced this phase becomes trivial, so we cannot use Theorem 4. Using the Clebsch-Gordon methods of Ref. [38], we can constrain the form of the MPS matrices for states in this phase. The different matrices can be labelled by the 8 different 1D irreps $\chi^i(g)$ of $\mathbb{Z}_4 \times \mathbb{Z}_2$, $i = 0, \ldots, 7$. The matrix

$A^i$ is associated to a basis state $|i\rangle$ which transforms like $u(g)|i\rangle = \chi^i(g)|i\rangle$. The resulting matrices have the following forms:

$$A^0 = \begin{pmatrix} B^0_{11} \otimes \mathbb{I} & 0 \\ 0 & B^0_{22} \otimes \mathbb{I} \end{pmatrix}$$
$$A^1 = \begin{pmatrix} B^1_{11} \otimes \sigma^z & 0 \\ 0 & B^1_{22} \otimes \sigma^z \end{pmatrix}$$
$$A^2 = \begin{pmatrix} B^2_{11} \otimes \sigma^y & 0 \\ 0 & B^2_{22} \otimes \sigma^y \end{pmatrix}$$
$$A^3 = \begin{pmatrix} B^3_{11} \otimes \sigma^x & 0 \\ 0 & B^3_{22} \otimes \sigma^x \end{pmatrix}$$
$$A^4 = \begin{pmatrix} 0 & B^4_{12} \otimes \sigma^z \\ B^4_{21} \otimes \sigma^x & 0 \end{pmatrix}$$
$$A^5 = \begin{pmatrix} 0 & B^5_{12} \otimes \mathbb{I} \\ B^5_{21} \otimes \sigma^y & 0 \end{pmatrix}$$
$$A^6 = \begin{pmatrix} 0 & B^6_{12} \otimes \sigma^x \\ B^6_{21} \otimes \sigma^z & 0 \end{pmatrix}$$
$$A^7 = \begin{pmatrix} 0 & B^7_{12} \otimes \sigma^y \\ B^7_{21} \otimes \mathbb{I} & 0 \end{pmatrix}$$

The symmetry representation $u(g)$ is built up of these 1D irreps. Not every choice is allowed, since it must lead to an injective MPS. For example, if $u(g)$ consists only of irreps $\chi^i(g)$ for $i = 0, \dots 3$, then there is a tensor product structure, but also the virtual space will be block diagonal and hence non-injective, which contradicts the method used to construct these matrices. No injective state in this phase admits a structure of the form $A^i = B^i \otimes C^i$. This phase the simplest example of the general structure we derive in the following section.

## 4.2 Structure of abelian SPT phases

Let $G$ be our symmetry group, and $[\omega]$ a non-trivial cohomology class labelling our phase. Since we are dealing with an abelian group, the physical representation of the symmetry must be diagonal, so that

$$u(g) = \bigoplus_{i=0}^{d-1} \chi^i(g) \ \forall g \in G$$

where each $\chi^i$ is a linear character of $G$ (a 1D representation). We will call the basis in which $u(g)$ is diagonal the wire basis $\mathcal{B}$ as before. The corresponding representation in the virtual space has the general form:

$$V(g) = \bigoplus_\alpha \mathbb{I}_{n_\alpha} \otimes V_\alpha(g)$$

where $V_\alpha(g)$ are all of the irreducible projective representations with factor system $\omega$ ($\omega$-irreps), and $n_\alpha$ is the number of times irrep $\alpha$ appears. We now require an essential fact about projective representations of abelian groups: all $V_\alpha(g)$ corresponding to the same cohomology class are projectively equivalent [77]. That is, we can write

$$V_\alpha(g) = \lambda_\alpha(g) U_\alpha \widetilde{V}(g) U_\alpha^\dagger,$$

for some preferred irrep $\widetilde{V}(g)$ which will be identified later. Let $D$ denote the common dimension of these irreps. We will ignore the unitaries $U_\alpha$, which can be eliminated by proper choice of the basis in virtual space. Note that the case where $[\omega]$ is maximally noncommutative is equivalent to there being only one $\omega$-irrep, ie. only one block in the virtual space [72].

### 4.2.1 Clebsch-Gordon decomposition

To find the form of ground states in abelian SPT phases, we present a proof that can be viewed as either a generalisation of the proof in Ref. [36] or a restriction of that found in Ref. [38] to abelian SPT phases.

In this setting, the symmetry relation of Fig. 2.2a) reads:

$$\left( \bigoplus_\alpha \mathbb{I}_{n_\alpha} \otimes \chi^i(g) V_\alpha(g) \right) A^i = A^i \left( \bigoplus_\alpha \mathbb{I}_{n_\alpha} \otimes V_\alpha(g) \right) \tag{4.1}$$

Now $\chi^i(g)V_\alpha(g)$ is still an $\omega$ representation of $G$, so it is equivalent to an $\omega$-irrep which we denote $V_{\pi_i(g)}(g)$:

$$\chi^i(g) V_\alpha(g) = C^i_{\pi_i(\alpha)} V_{\pi_i(\alpha)} C^{i\dagger}_{\pi_i(\alpha)} \tag{4.2}$$

where $C^i_{\pi_i(\alpha)}$ are the Clebsch-Gordon matrices associated with the fusion of irreps $i \otimes \alpha$. This fusion induces induces a permutation $\pi_i(\alpha)$ of irreps according to the Clebsch-Gordon series:

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi^i(g) \mathrm{Tr}\, V_\alpha(g) \mathrm{Tr}\, V_{\pi_i(\alpha)}(g)^*. \tag{4.3}$$

With this, we can rewrite Eq. 4.1 as

$$\left(\bigoplus_\alpha \mathbb{I}_{n_{\pi_i^{-1}(\alpha)}} \otimes V_\alpha(g)\right)\left[\left(\bigoplus_\alpha \mathbb{I}_{n_{\pi_i^{-1}(\alpha)}} \otimes C_\alpha^{i\dagger}\right)\mathcal{P}_i A^i\right] = \tag{4.4}$$

$$\left[\left(\bigoplus_\alpha \mathbb{I}_{n_{\pi_i^{-1}(\alpha)}} \otimes C_\alpha^{i\dagger}\right)\mathcal{P}_i A^i\right]\left(\bigoplus_\alpha \mathbb{I}_{n_\alpha} \otimes V_\alpha(g)\right). \tag{4.5}$$

Here, we have introduced the matrix $\mathcal{P}_i$ which permutes blocks of the virtual space in accordance with the action of $\pi_i$ on the irreps. Now, by Schur's Lemma, we have:

$$\left(\bigoplus_\alpha \mathbb{I}_{n_{\pi_i^{-1}(\alpha)}} \otimes C_\alpha^{i\dagger}\right)\mathcal{P}_i A^i = \bigoplus_\alpha B_\alpha^i \otimes \mathbb{I}_D, \tag{4.6}$$

where $B_\alpha^i$ is some $n_{\pi_i^{-1}(\alpha)} \times n_\alpha$ matrix. Finally, we have:

$$A^i = P_i^\dagger \left(\bigoplus_\alpha B_\alpha^i \otimes C_\alpha^i\right). \tag{4.7}$$

When $\omega$ is maximally non-commutative, there is only one $\omega$-irrep, hence only one block in virtual space, and the above form reduces to the more familiar $A^i = B^i \otimes C^i$. In the general case, we see that the MPS matrices act in the virtual space as a junk and logical operator in each block followed by a permutation of blocks. The logical operators are the Clebsch-Gordon coefficients. This structure agrees with our $\mathbb{Z}_4 \times \mathbb{Z}_2$ example.

### 4.2.2 Main structure theorem

We now prove that the Clebsch-Gordon matrices which will be our logical operators are in the projective symmetry irrep $\widetilde{V}(g)$, such that we will be able to use the standard method of byproduct propagation. First, we define the linear character $\chi_\alpha^i = \chi^i \lambda_\alpha \lambda_{\pi_i(\alpha)}^{-1}$ and rewrite Eq. 4.2 as:

$$\chi_\alpha^i(g) V(g) = C_\alpha^i \widetilde{V}(g) C_\alpha^{i\dagger} \tag{4.8}$$

**Theorem 5.** *The CG-matrices $C_\alpha^i$ are in the projective symmetry representation $\widetilde{V}(g)$. That is, we have $C_\alpha^i = \widetilde{V}(g_\alpha^i)$ where $g_\alpha^i$ is uniquely determined by the relation:*

$$\chi_\alpha^i(g) = \omega(g_\alpha^i, g)\omega(g, g_\alpha^i)^{-1}$$

To set up the proof, we first define the normal subgroup $K \subset G$ by $K = \{s \in G : \omega(s,g)\omega(g,s)^{-1} = 1 \; \forall g \in G\}$. $K$ is equivalent to the subgroup of group elements that are represented projectively as a scalar matrices in $\widetilde{V}(g)$ ([72], Lemma 6.38'(b)). Since we have a phase degree of freedom in defining $\widetilde{V}(g)$, we can write $K = \{s \in G : \widetilde{V}(s) = \mathbb{I}\}$. Since $K$ is a normal subgroup, we can form the quotient group $\bar{G} = G/K$. Now we need the following lemma:

**Lemma 1.** *(a) $\chi^i_\alpha$ is a linear character of $\bar{G}$. (b) $\widetilde{V}(g)$ is a faithful, irreducible, projective representation of $\bar{G}$.*

*Proof.* Consider a partition of G into cosets of $K$, $G = \cup_{a\in\bar{G}} K g_a$, where $g_a g_b = s(a,b) g_{ab}$ for $s(a,b) \in K$.
(a) If we define $\bar{\chi}(a) = \chi^i_\alpha(g_a) \; \forall a \in \bar{G}$, we have

$$\bar{\chi}(a)\bar{\chi}(b) = \chi^i_\alpha(s(a,b))\bar{\chi}(ab)$$

Now it is clear by Eq. 4.8 that $\chi^i_\alpha(s) = 1 \; \forall s \in K$ since $\widetilde{V}(s(a,b))$ is a scalar matrix. So $\bar{\chi}$ is indeed a linear character of $\bar{G}$
(b) Similarly, define the projective representation of $\bar{G}$ as $\bar{V}(a) = \widetilde{V}(g_a)$ $\forall a \in \bar{G}$. Since $\widetilde{V}(s) = \mathbb{I} \; \forall s \in K$, we can again see that $\bar{V}(a)$ is an $\bar{\omega}$-representation of $\bar{G}$ where $\bar{\omega}(a,b) = \omega(g_a, g_b)$. It is irreducible since $V(g)$ is and the only elements we have removed are scalar matrices, which do not influence reducibility. Finally, it is faithful, since if $\bar{V}(a) = \widetilde{V}(g_a) = 1$, then $g_a \in K$ so $a = 1$. □

Essentially, modding out the subgroup $K$ gives us the minimal group in which $\widetilde{V}(g)$ is a faithful representation. This is important because we can now repeat the argument used by Else *et. al.* [36].

*Proof. of Theorem*
Define the homomorphism $\phi_\omega$ from $\bar{G}$ to its character group $\bar{G}^*$ by $\phi_\omega(a)(b) = \bar{\omega}(a,b)\bar{\omega}(b,a)^{-1}$. By construction of $\bar{G}$, $ker\phi_\omega = \{e\}$, so this is in fact an isomorphism. That means we can find an element $a^i_\alpha \in \bar{G}$ such that:

$$\bar{\chi}(a) = \bar{\omega}(a^i_\alpha, b)\bar{\omega}(b, a^i_\alpha)^{-1} \; \forall a \in \bar{G}.$$

Since $\chi^i_\alpha = 1$ on $K$, this extends to $G$ itself. Defining $g^i_\alpha = g_{a^i_\alpha}$, we have

$$\chi^i_\alpha(g) = \omega(g^i_\alpha, g)\omega(g, g^i_\alpha)^{-1} \; \forall g \in G$$

Then it is easy to verify that setting $C^i_\alpha = \widetilde{V}(g^i_\alpha)$ satisfies Eq. 4.8, which proves the theorem.

□

For our $\mathbb{Z}_4 \times \mathbb{Z}_2$ example, $K = \mathbb{Z}_2 \times \{e\} \cong \mathbb{Z}_2$, so $\bar{G} = \mathbb{Z}_2 \times \mathbb{Z}_2$. By the theorem, $C^i_\alpha$ form an faithful irreducible projective representation of $\bar{G}$, and hence they are Pauli matrices, as was observed.

### 4.2.3 Refining structure

We now require three propositions which refine the structure proven by Theorem 5. The first proposition elucidates the structure of the permutations $\mathcal{P}_i$:

**Proposition 1.** *$\mathcal{P}_i = \mathcal{P}_j$ if and only if $\chi^i(s) = \chi^j(s)\ \forall s \in K$.*

*Proof.* The different irreps $V_\alpha(g)$ are labelled by characters $\psi_\alpha$ of $K$ according to the relation $V_\alpha(s) = \psi_\alpha(s)\mathbb{I}$, $\forall s \in K$ (see Lemma 6.44 of Ref. [72]). Then the permutation $\mathcal{P}_i$ is defined such that $\chi^i(s)\psi_\alpha(s) = \psi_{\mathcal{P}_i(\alpha)}(s)\ \forall s \in K$. Clearly, this depends only on the values that $\chi^i$ takes on $K$, proving the proposition. □

Since the group $K^*$ of characters of $K$ is isomorphic to $K$ itself, the permutations $\mathcal{P}_i$ are elements of the regular representation of $K$. Hence they commute, and we see that $n_\omega = |K|$ gives the number of different irreps of type $\omega$, the number of distinct permutations $\mathcal{P}_i$, and also the number of blocks in virtual space.

For the $\mathbb{Z}_4 \times \mathbb{Z}_2$ example, $K = \mathbb{Z}_2$, so there are two blocks in virtual space, and the only non-trivial permutation $\mathcal{P}_i$ swaps these two blocks.

Now our second proposition regards the byproduct operators $C^i_\alpha$:

**Proposition 2.** *The matrices $C^i_\alpha$ can be decomposed as $C^i_\alpha = D^i_\alpha C^i$, where $D^i_\alpha$ depends only on $\mathcal{P}_i$ and not $i$ itself. Furthermore, $C^i$ and $D^i_\alpha$ are both elements of the projective symmetry representation $V(g)$.*

*Proof.* Fix an arbitrary $j$ and pick any $i$ such that $\mathcal{P}_i = \mathcal{P}_j$. The result is proven if we show that $C^i_\alpha$ can be written as $C^j_\alpha C^i$ for some operator $C^i$, $\forall \alpha$, whereupon $D^i_\alpha = C^j_\alpha$. Let $C^i = V(g_i)$ for $g_i$ such that $\omega(g_i, g)\omega(g, g_i)^{-1} = \chi^i(g)\chi^j(g)^{-1}\ \forall g \in G$. Such a $g_i$ must exist since $\chi^i(s)\chi^j(s)^{-1} = 1\ \forall s \in K$ by Prop. 1, which implies that $\chi^i\chi^{j^{-1}} \in \mathrm{Im}\ \phi_\omega$. Then it is clear to check that $\chi^i(g)V_\alpha(g) = C^j_\alpha C^i V_{\mathcal{P}_i(\alpha)}(g) C^{i\dagger} C^{j\dagger}_\alpha$. □

This proposition will ensure that the same logical gates are executed in each block of the virtual space. This theorem is again evident in our $\mathbb{Z}_4 \times \mathbb{Z}_2$ example.

The dimension $D$ of the byproduct operators is equal to $d_\omega$, the dimension of $\widetilde{V}(g)$. By Theorem 6.39(b) of Ref. [72], this is equal to $\sqrt{G:K} = \sqrt{|G|/|K|}$.

We will require one final proposition which shows how the operators $D^i_\alpha$ change under a change of the basis of the virtual space.

**Proposition 3.** *Under the change of virtual basis given by* $A^i \to U_j A^i U_j^\dagger$ *with* $U_j = \bigoplus_\alpha \mathbb{I} \otimes D^j_{\mathcal{P}_j^\dagger(\alpha)}$*, the operators* $D^i_\alpha$ *become* $D^i_{\mathcal{P}_j^\dagger(\alpha)}$

*Proof.* By direct computation, we see that $D^i_\alpha$ becomes $D^j_{\mathcal{P}_j^\dagger(\alpha)} D^i_\alpha D^{j\dagger}_{\mathcal{P}^i \circ \mathcal{P}_j^\dagger(\alpha)}$ up to irrelevant phases in each block which are absorbed into $B^i_\alpha$. Using the Clebsch-Gordon relations self-consistently, it is easy to show that this operator is equivalent to $D^i_{\mathcal{P}_j^\dagger(\alpha)}$ as claimed. □

This result will remove any ambiguities present in byproduct propagation.

## 4.3 Computation in abelian SPT phases

Now we use the structure derived in the previous section to show how computation can be performed throughout abelian SPT phases. The key observation is the following: if our virtual state is supported on a single block $\alpha$ of the virtual space, then the matrices in Eq. 4.7 act in essentially the same way as Eq. 3.6. The difference is that the byproduct operators depend on which block our state is in. However, Prop. 2 will guarantee that the the same logical gate is performed no matter which block our state is in. Because of these two facts, computation will work in nearly the same way as in the maximally non-commutative case.

### 4.3.1 Encoding and byproduct propagation

The first issue to deal with is how to encode information such that we can take care of byproduct propagation. Our mechanism of byproduct propagation is as usual symmetry transformations of future measurement bases. Again, we have:

$$\sum_j u(g)_{ij} A^j = V(g) A^i V(g)^\dagger,$$

where $V(g) = \bigoplus_\alpha \lambda_\alpha(g)\mathbb{I}_{n_\alpha} \otimes \widetilde{V}(g)$. We see that the same byproduct will be undone in each block $\alpha$, up to irrelevant phases. In general, measurement in the wire basis will result in a different byproduct operator $C_\alpha^i$ in each block, so this symmetry transformation is not sufficient for propagation. If, however, we restrict to quantum states supported in only one known block, we can always propagate the byproduct completely. Since we will be employing the mixed-state interpretation, we consider only states which are a probabilistic mixture over single-blocked states:

$$\rho = \bigoplus_\alpha p_\alpha \rho_\alpha. \tag{4.9}$$

The interpretation of this state is that we have performed some initialization procedure which puts our virtual state into a single block. In the mixed state interpretation, we sum over the possible outcomes of this initialization, leading to the above state. However in a given run of the computation we always know which block supports our state, so we can perform byproduct propagation. The details of this initialization procedure are given in Sec 4.4. For now, we assume that it has been done.

We can again define a logical subspace in which we store information. A logical state $\sigma = |\phi\rangle\langle\phi|$ will be encoded as:

$$\rho = \bigoplus_\alpha (p_\alpha \widetilde{\rho}_\alpha \otimes \sigma) = \left(\bigoplus_\alpha p_\alpha \widetilde{\rho}_\alpha\right) \otimes \sigma \equiv \widetilde{\rho} \otimes \sigma. \tag{4.10}$$

$\sigma$ is acted on by the CG matrices $C_\alpha^i$, which are defined by the symmetry and phase. $\widetilde{\rho}$ lives in the junk system, which now also includes the information about which block the state is in.

### 4.3.2 Oblivious wire

Consider any state of the form given in Eq. 4.10. In this section we will show how to send this state to the fixed point $\mathbb{I} \otimes \sigma$. The protocol is identical to the oblivious wire used in the maximally non-commutative case: repeated measurements in the wire basis with byproduct propagation.

After a single measurement in the wire basis with byproduct propagation, we have:

$$\rho \to \left(\sum_\alpha B^i_{\mathcal{P}_i^\dagger \alpha} \widetilde{\rho}_{\mathcal{P}_i^\dagger(\alpha)} B^{i\dagger}_{\mathcal{P}_i^\dagger \alpha}\right) \otimes \sigma = \widetilde{\mathcal{E}}(\widetilde{\rho}) \otimes \sigma.$$

After $m$ measurements, the junk state $\widetilde{\rho}$ is acted on by the channel $\widetilde{\mathcal{E}}^m$. It is easy to see that $\widetilde{\mathcal{E}}$ is unital since $\mathcal{E}$ is. Furthermore, $\mathbb{I}$ is the only fixed point of $\widetilde{\mathcal{E}}$, since any other fixed point would define a fixed point of $\mathcal{E}$, violating injectivity. So the oblivious wire projects the junk space onto the maximally mixed state, just as in the maximally non-commutative case.

### 4.3.3 Infinitesimal gates and measurements

With the oblivious wire, we can get infinitesimal gates in the same way as before, with one key difference. In the maximally non-commutative case, we would perform an infinitesimal gate by measuring in the basis

$$\mathcal{B}(i,j;d\alpha,\beta) = \{|0\rangle,\ldots,|i\rangle + d\alpha e^{i\beta}|j\rangle, |j\rangle - d\alpha e^{-i\beta}|i\rangle,\ldots,|d-1\rangle\},$$

followed by the oblivious wire. The procedure is the same in the present case, except now we must restrict the possible pairs $i,j$ to perturb in the basis. If we perturb basis states $i,j$ where $\mathcal{P}_i \neq \mathcal{P}_j$, then we will introduce coherence between blocks of the virtual space and lose the block diagonal structure. This is not permissible since it removes our ability to propagate byproduct operators.

Let our initial state be $\rho = \mathbb{I}\otimes\sigma$. Suppose we measure in the basis $\mathcal{B}(i,j;d\alpha,\beta)$ such that $\mathcal{P}_i = \mathcal{P}_j$. If we propagate the byproducts $C^i_\alpha$ and sum over outcomes, a simple calculation gives the resulting state as:

$$\begin{aligned}\rho \to \bigoplus_\alpha \Bigg( &\left\{\sum_i B^i_{\mathcal{P}_i^\dagger\alpha} B^{i\dagger}_{\mathcal{P}_i^\dagger\alpha}\right\}\otimes\sigma \\ &+d\alpha\left\{e^{i\beta}B^i_{\mathcal{P}_i^\dagger\alpha}B^{j\dagger}_{\mathcal{P}_i^\dagger\alpha}\otimes\left[\sigma,C^{j\dagger}C^i\right] + e^{-i\beta}B^j_{\mathcal{P}_i^\dagger\alpha}B^{i\dagger}_{\mathcal{P}_i^\dagger\alpha}\otimes\left[C^iC^{j\dagger},\sigma\right]\right\}\Bigg).\end{aligned} \tag{4.11}$$

Therein, we have used Prop. 2 since $\mathcal{P}_i = \mathcal{P}_j$. Finally, we follow this with the oblivious wire, giving:

$$\rho \to \mathbb{I}\otimes\left(\nu\sigma + d\alpha\left[\sigma, \nu^{ij}e^{i\beta}C^jC^{i\dagger} - \nu^{ji}e^{-i\beta}C^iC^{j\dagger}\right]\right)$$

where we have defined $\lim_{m\to\infty}\widetilde{\mathcal{E}}^m(\bigoplus_\alpha B^i_\alpha B^{j\dagger}_\alpha) = \nu^{ij}\mathbb{I}$ and $\nu = \sum_i \nu^{ii}$. We see that, as in the maximally non-commutative case, we get an infinitesimal rotation of the logical subspace. If $\sigma = |\phi\rangle\langle\phi|$, we have:

$$\mathcal{T}(i,j;d\alpha,\beta)|\phi\rangle = \exp\left\{d\alpha\frac{|\nu^{ij}|}{\nu}\left(e^{i(\beta+\delta^{ij})}C^{i\dagger}C^{j} - e^{-i(\beta+\delta^{ij})}C^{j\dagger}C^{i}\right)\right\}|\phi\rangle$$

Once again, we get a Lie algebra $\mathcal{A}[\mathcal{O}]$ of infinitesimal rotations and a corresponding Lie group of operators $\mathcal{L}[\mathcal{O}]$. We can similarly generalize the scheme for projective measurement of the virtual system given in Ref. [2].

## 4.4 Initialization

In order for the gates to work as described above, we needed to initialize our state into a known block of the virtual space. This was to ensure that we could always propagate the byproduct operators. We will now see that this can always be done, although it is somewhat tricky and requires additional knowledge of the microscopic details of the state (beyond $\nu^{ij}$).

First, we run "completely" oblivious wire, which is the usual oblivious wire only with no byproduct propagation. Measuring $m$ spins results in the channel $\mathcal{E}^m$ where $\mathcal{E}(X) = \sum_i A^i(X)A^{i\dagger}$. By injectivity and the canonical form, this channel projects the virtual space onto the state $\mathbb{I} = \bigoplus_\alpha \mathbb{I}_\alpha$. We can interpret this state as a statistical ensemble over the states $\mathbb{I}_\alpha$, each of which are supported only one block $\alpha$. So we interpret the completely oblivious wire as a projection onto a single unknown block of the virtual space. At the very beginning of computation (ie. the first repetition of an algorithm), we assign this block the label "1". For the rest of the initialization process, we track the accumulated permutation $\mathcal{P}_\Sigma = \prod_i \mathcal{P}_i^\dagger$, such that our virtual state at any time is supported in the block $\mathcal{P}_\Sigma(1)$.

From Eq. 4.7, we see that the byproduct operators depend on both the measurement outcome and the block that supported the virtual state before measurement: block $\alpha$ and outcome $i$ result in $C_\alpha^i$. The above procedure gives us a way to identify which block we are in, but only with respect to an arbitrary reference point "1" which does not necessarily correspond to the block with $\alpha = 1$ in Eq. 4.7. How do we match up these block labels with the labels of the byproduct operators? The answer is, we don't have to. Suppose the block we called "1" actually corresponds to block $\beta$ in Eq. 4.7. Then, by Prop. 3, we change the basis of our virtual space by the unitary $U_j$ with $\mathcal{P}_j^\dagger(\beta) = 1$ (such a unitary always exists), such that the block we called "1" does indeed transform like the block corresponding to $\alpha = 1$ in Eq. 4.7. Furthermore, since the permutations $\mathcal{P}_i$ all commute, we have $\mathcal{P}_j^\dagger \circ \mathcal{P}_\Sigma(\beta) = \mathcal{P}_\Sigma \circ \mathcal{P}_j^\dagger(\beta) = \mathcal{P}_\Sigma(1)$, hence all byproducts are as dictated

by Eq. 4.7. So we can match up the labels of byproduct operators with our arbitrary labelling of blocks by a passive choice of virtual basis.

It would seem as though we are done: for each run of the computation, we choose a different virtual basis such that we can propagate byproduct operators as described above. Unfortunately, this is inconsistent with the mixed state interpretation. Here, different runs of the computation are interpreted as different paths, which we eventually sum over. We cannot perform this sum in the desired way if each path uses a different virtual basis. Because of this, we require a procedure to determine which block we are in with respect to "1" that will be performed at the start of every subsequent repetition of the computation.

To do this, we first need an extra calibration step to characterize the different blocks. This step involves simply measuring in the wire basis, collecting every $m$-th outcome for some $m \gg \xi$, and binning these outcomes according to $\mathcal{P}_\Sigma$ before the measurement (so there are $|K|$ bins). What we get out of this procedure is the set of constants $\{\nu_\alpha^{ii}\}$ as defined in the appendix, where $\alpha$ is defined with respect to 1 as above. To see how this works, suppose our virtual space is in the state $\mathbb{I}_\alpha$. Then, by the Born rule described in the appendix, the probability of obtaining outcome $i$ after measuring in the wire basis is $\nu_\alpha^{ii}$. If we were able to repeat this measurement many times, the outcome statistics would be as dictated by the constants $\nu_\alpha^{ii}$.

The problem is that the first measurement (a) puts us in a different block and (b) makes our virtual state different from the maximally mixed state. (a) is solved by binning the outcomes according to the block the virtual space was in before measurement, ie. the accumulated permutation $\mathcal{P}_\Sigma$. (b) is solved by running completely oblivious wire between each measurement. To see why, consider the evolution under the completely oblivious wire of an initial state $\rho_\alpha$ which is supported only in block $\alpha$. Since we are binning measurement outcomes according to the accumulated permutation $\mathcal{P}_\Sigma$, we must only sum over those strings of outcomes which lead to the same $\mathcal{P}_\Sigma$. The resulting channel $\mathcal{E}_{\mathcal{P}_\Sigma}$ thus gives a state supported only in block $\mathcal{P}_\Sigma(\alpha)$. Since $\mathcal{E}^m = \sum_{\mathcal{P}_\Sigma} \mathcal{E}_{\mathcal{P}_\Sigma}$, and since $\mathcal{E}^m$ has the fixed point $\mathbb{I} = \bigoplus_\alpha \mathbb{I}_\alpha$, $\mathcal{E}_{\mathcal{P}_\Sigma}$ must project the initial state $\rho_\alpha$ onto the state $\mathbb{I}_{\mathcal{P}_\Sigma(\alpha)}$. This prepares us for another calibrating measurement.

We now have a procedure to determine the constants $\nu_\alpha^{ii}$ for all blocks $\alpha$ (with respect to block 1). For the next run of the computation, the initialization is carried out in the same way, only now we use the measurements statistics to determine which block we are in. Note that, if $\nu_\alpha^{ii} = \nu_\beta^{ii}$ for some $\alpha$, $\beta$, then we cannot distinguish if we are in block $\alpha$ or block $\beta$ with the

above procedure. This means we do not know which byproducts to propagate, and the computation may fail. This condition holds for the case where the junk part is trivial.

## 4.5 Main theorem

With the above results, we can state our next main theorem, which is strictly stronger than Theorem 4:

**Theorem 6.** *Consider a state in a symmetry-protected topological phase without symmetry breaking described by a group $G$, an on-site representation $u$, and a cohomology class $[\omega]$. If there exists a finite abelian subgroup $H \subset G$ such that $[\omega|_H]$ is not the trivial class, then for any state in the phase, except a null subset, a Lie group of gates determined only by $G$, $u$, and $[\omega]$ can be efficiently implemented in MBQC with arbitrary high gate fidelity.*

Before computation, we must perform a calibration step to obtain the constants $\nu^{ij}$ and $\nu_\alpha^{ii}$. The null subset of states which cannot be used refers to those with either $\nu^{ij} = 0$ or $\nu_\alpha^{ii} = \nu_\beta^{ii}$ for some $\alpha, \beta$.

Every phase which satisfies Theorem 4 also satisfies this one, but this does not make the maximally non-commutative case irrelevant. For one, the maximally non-commutative case corresponds to when the logical subspace has maximum dimension, so it is desirable for this reason. More importantly, we will see in the next chapter that only in the maximally non-commutative case can we guarantee that $\mathcal{L}[\mathcal{O}]$ contains a full set of single-qudit gates.

# Chapter 5

# Determining computational power

In the previous two chapters, we saw that SPT phases protected by an abelian (sub)group have uniform computational power, as summarized in Theorems 4 and 6. The final step is to determine the Lie group $\mathcal{L}[\mathcal{O}]$ that quantifies this uniform power by using the algebraic structure inherited from the SPT phase classification. For the maximally non-commutative case, we are able to prove that this Lie group is always universal, in that it always allows arbitrary operations on a qudit of some dimension. For the general case, this is not true, and as a counterexample we construct of a phase which allows only $z$-axis rotations of a qubit, which is not universal.

## 5.1 Maximally non-commutative case

Recall that we begin with a symmetry group $G$ and then restrict to a finite abelian subgroup $H$, whereupon our logical dimension is $D = \sqrt{|H|}$. Consider first the case where the representation $u|_H$ contains all non-trivial characters of the subgroup $H$. This means that $\mathcal{O}$ contains $D^2 - 1$ trace-orthogonal, antihermitian operators, so $\mathcal{L}[\mathcal{O}] \cong SU(D)$. If the Hilbert space dimension of our physical sites is smaller than $D^2 - 1$, or certain characters $\chi^i$ do not appear in $u|_H$, $\mathcal{L}[\mathcal{O}]$ may be some Lie subgroup of $SU(D)$. However, with the condition of maximal non-commutativity, this subgroup is always universal on a qudit system, as stated in the following theorem:

**Theorem 7.** *Consider an SPT phase defined by an on-site symmetry group $G$ and cohomology class $[\omega]$. Suppose there exists a finite abelian subgroup $H \subset G$ such that $[\omega|_H]$ is maximally non-commutative, and let $p^n$ be a prime power dividing $\sqrt{|H|}$. Then $\mathcal{L}[\mathcal{O}] \supset SU(p^n)$. That is, every state in the phase, except for a null subset, is a resource for universal computation on a $p^n$ level system.*

This result, proven after the next section, determines the *minimal* computational power of the phase, which is *independent* of $u$ and hence uniform

amongst the phase. This shows that 1D ground states with SPT order are generically useful as MBQC resources.

Beyond this minimal case, $\mathcal{L}[\mathcal{O}]$ can often be expanded to gain additional computational power. For example when $H = (\mathbb{Z}_2)^4$, our theorem guarantees that $SU(2) \subset \mathcal{L}[\mathcal{O}]$, but this can be expanded to either $SU(4)$ or $SU(2) \times SU(2)$ depending on the on-site symmetry representation $u$. So, while changing $u$ is generally considered to not change the SPT phase of a system [6], it remains an important label for total computational power in our scheme. If, however, we allow ourselves to redefine the locality of measurements by blocking neighbouring sites, $\mathcal{L}[\mathcal{O}]$ will always equal $SU(D)$ after sufficient blocking.

## 5.2 Non-universality in abelian phases

In the general abelian case, without the assumption of maximal noncommutativity, determining $\mathcal{L}[\mathcal{O}]$ becomes more difficult. This is because we can only perturb or measurement basis between certain basis states. Furthermore, we cannot always restrict to a subgroup of convenient form, as in the proof contained in the next section. As in the previous section, for each phase it is possible to choose the representation $u$ such that $\mathcal{L}[\mathcal{O}] = SU(D)$ where $D = \sqrt{|G|/|K|}$. However, we can no longer prove that all choices of $u$ lead to a full set of single-qudit gates. In fact, this is not true in general, as illustrated by the following example.

Consider the following state in the non-trivial phase of $\mathbb{Z}_4 \times \mathbb{Z}_2$. The physical system is a qutrit with MPS matrices given by:

$$\begin{aligned} A^0 &= \begin{pmatrix} B^0_{11} \otimes \mathbb{I} & 0 \\ 0 & B^0_{22} \otimes \mathbb{I} \end{pmatrix} \\ A^1 &= \begin{pmatrix} B^1_{11} \otimes \sigma^z & 0 \\ 0 & B^1_{22} \otimes \sigma^z \end{pmatrix} \\ A^6 &= \begin{pmatrix} 0 & B^6_{12} \otimes \sigma^x \\ B^6_{21} \otimes \sigma^z & 0 \end{pmatrix} \end{aligned} \tag{5.1}$$

One can confirm numerically that this state is injective for most choices of matrices $B^i_{\alpha\beta}$. Our scheme only gives a single type of gate, which is rotation about the $Z$ axis. This does not lead to a universal set of single-qubit gates.

## 5.3 Proof of Theorem 7

By Lemma 36 of Ref. [72] and its proof within, if $[\omega|_H]$ is maximally non-commutative then $H$ must have the form $H_1 \times \cdots \times H_r$ where $H_i \cong \mathbb{Z}_{p_i^{n_i}} \times \mathbb{Z}_{p_i^{n_i}}$ and $p_i^{n_i}$ is a prime power. Furthermore, $[\omega|_{H_i}]$ is also maximally non-commutative for all subgroups $H_i$. By restricting to any such subgroup $\tilde{H} = \mathbb{Z}_D \times \mathbb{Z}_D$ for $D = p^n$, the operators $C^i$ can be taken to be Heisenberg-Weyl operators of the form $Z^i X^j$ where $XZ = \Omega ZX$ and $\Omega = e^{\frac{2\pi i}{D}}$. In this way, we are able to prove that $\mathcal{L}[\mathcal{O}]$ is $SU(D)$ for all physical representations $u$; see below.

### 5.3.1 Graphical Description of Computational Power

The primitive gates in our scheme that can be executed in a single step are generated by elements from the following set $\mathcal{O}$ of antihermitian opertors:

$$\mathcal{O} = \left\{ \alpha C^{i\dagger} C^j - \alpha^* C^{j\dagger} C^i \right\} \quad \forall i \neq j,\ \forall |\alpha| \ll 1$$

Throughout the following, $\alpha$ always represents an arbitrary complex number of small magnitude, unless stated otherwise. By concatenating these primitive gates, we can execute any unitary gate generated by elements of the algebra $\mathcal{A}[\mathcal{O}]$ defined as the smallest Lie algebra containing $\mathcal{O}$. This algebra, called the dynamical Lie algebra in the context of quantum control, determines the computational power of the resource state; the set of gates $\mathcal{L}[\mathcal{O}] = e^{\mathcal{A}[\mathcal{O}]}$. We call our resource state universal if $\mathcal{L}[\mathcal{O}] = SU(N)$, such that $\mathcal{A}[\mathcal{O}] = su(N)$, the Lie algebra of traceless antihermitian matrices with commutator bracket. $su(N)$ can be spanned by the operators $\alpha X^i Z^j - \alpha^* Z^{j\dagger} X^{i\dagger}$ for $i, j = 0, \ldots, N-1$, and $\alpha \in \mathbb{C}$. Denote these operators by $O_{i,j}(\alpha)$. Clearly, by the definition of $\mathcal{O}$, we have $\mathcal{A}[\mathcal{O}] \subset su(N)$ always.

The task is then, given $\mathcal{O}$, to determine $\mathcal{A}[\mathcal{O}]$. This is facilitated by a graphical interpretation. The elements of $\mathcal{A}[\mathcal{O}]$ can be indexed by a pair of mod $D$ integers $(i, j)$, which refer to the set of operators $\{O_{i,j}(\alpha)\}$ for all $\alpha \in \mathbb{C}$. We can construct a $D \times D$ grid, whose vertices correspond to pairs $(i, j)$. We place a marker on a vertex if the corresponding operators are in $\mathcal{A}[\mathcal{O}]$(See Fig. 5.1). It is then clear that we have $\mathcal{A}[\mathcal{O}] = su(N)$ if and only if we can mark all vertices on the graph. Note that half of the points on the graph are redundant, since $(i, j)$ and $(D - i, D - j)$ refer to the same operators. So whenever $(i, j)$ is marked, we can mark $(D-i, D-j)$ for free.

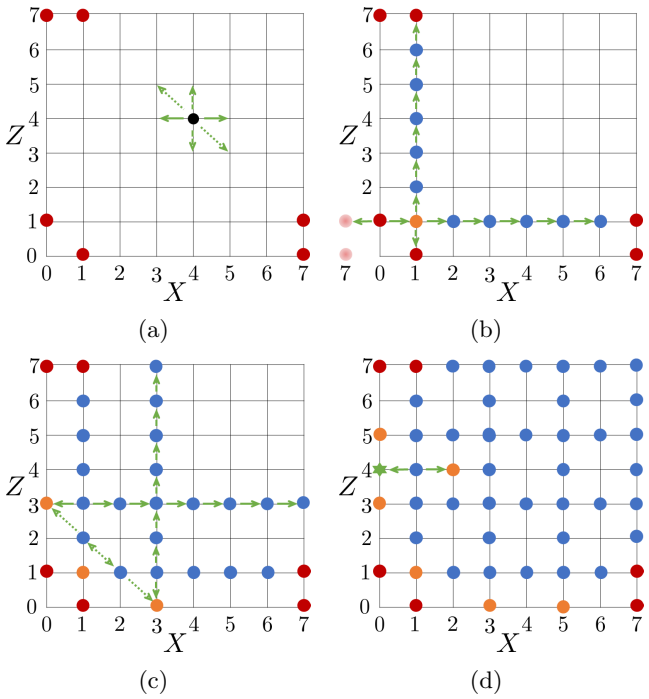


Figure 5.1: Illustration of graphical description of $\mathcal{A}[\mathcal{O}]$ and proof of Lemma 3 for $D = 8$ and $r = 1$. (a) Initial points guaranteed by Lemma 2 (red marks). Arrows indicate basic moves: X move is solid, Z dashed, Y dotted. Starting from a marked point, if any arrow points to another marked point, its opposite can be marked as well. (b) First basic move is done from position (0,1), abusing periodic boundary conditions indicated by faded marks, creating orange mark. Starting from the orange mark, row/column 1 are filled using X/Z moves. (c) A Y move is used to obtain new starting points in row/column 3 (orange marks), which are then filled using X/Z moves. (d) After every other row/column is filled, the point (2,4) is filled using the special rule with the green star indicating the hermitian point (0,4). The remaining points can now be filled with basic moves.

Different physical representations $u$ determine the operators in $\mathcal{O}$, which in turn determines the initial conditions of our grid. We briefly pause for a Lemma that restricts the possible initial conditions and is a consequence of injectivity:

**Lemma 2.** *If $D = p^n$ is a prime power, then there exists an integer $r$ which is not divisible by $p$ such that:*

$$\{O_{1,0}(\alpha), O_{0,r}(\alpha), O_{D-1,r}(\alpha)\} \subset \mathcal{O} \tag{5.2}$$

The proof will be presented shortly. This lemma allows us to define the basic moves that can be used to fill up the graph starting from this initial point. Consider the following commutator of two elements in $\mathcal{A}[\mathcal{O}]$:

$$[O_{i,j}(\alpha), O_{1,0}(1)] = O_{i+1,j}(\alpha(\Omega^{-j} - 1)) - O_{i-1,j}(\alpha(\Omega^{j} - 1)) \tag{5.3}$$

So, starting from the point $(i, j)$, we get out a linear combination of operators represented by points $(i - 1, j)$ and $(i + 1, j)$. If either of these points are already filled, we can simply subtract out that part we already have, allowing us to fill the other point since $\alpha$ is a free parameter. We can do the same thing with the operator $O_{0,r}(1)$ and also $O_{D-1,r}(1)$. So our three basic moves are, starting from a marked point $(i, j)$:

X) Inspect points $(i + 1, j)$ and $(i - 1, j)$. If one is marked already and $j \neq 0$, mark the other.

Z) Inspect points $(i, j + r)$ and $(i, j - r)$. If one is marked already and $i \neq 0$, mark the other.

Y) Inspect points $(i-1, j+r)$ and $(i+1, j-r)$. If one is marked already and $ir + j \neq 0$, mark the other.

See Fig. 5.1(a) for an illustration. Recall that, since we are working with integers mod $D$, our graph has periodic boundaries. Basic moves are forbidden for certain values of $(i, j)$ because these correspond to taking the commutator of commuting operators, which will give 0. The points where a Y move are forbidden form a line with slope $-r$ starting from the origin,

There is one final rule that applies only when $D$ is even: If at any time a point corresponding to a hermitian operator [i.e. $(\frac{D}{2}, 0), (0, \frac{D}{2}), (\frac{D}{2}, \frac{D}{2})$] can be inspected by a basic X, Y, or Z move, it can be considered marked. This rule can be explained by an example. Consider the commutator:

$$\left[O_{1,\frac{D}{2}}(\alpha), O_{1,0}(\beta)\right] = O_{0,\frac{D}{2}}(2\alpha\beta^*) - O_{2,\frac{D}{2}}(2\alpha\beta) \tag{5.4}$$

Since $Z^{\frac{D}{2}}$ is hermitian, we can choose $\alpha = \beta$ and annihilate the first term automatically, leaving the second term with the free coefficient $\alpha$. This allows us to mark $O_{2,\frac{D}{2}}(\alpha)$, which in turn allows us to mark $O_{0,\frac{D}{2}}(\alpha)$. This process generalises whenever one of the operators is hermitian, giving the basis for the final rule. With these rules in hand, we have our final lemma:

**Lemma 3.** *With the initial conditions of Lemma 2, each point on the graph can be marked using basic moves. That is, the set of operators in Eq. 5.2 generates $su(p^n)$.*

*Proof.* We prove first for the case $r = 1$, and comment on general $r$ at the end. Based on Lemma 2, our initially marked points include $(1,0),(0,1),(D-1,1)$ where $D = p^n$. We also get $(D-1,0),(0,D-1),(1,D-1)$ by the aforementioned redundancy of the points (See Fig. 5.1(a)) We start with an X move from $(0,1)$. Since $(D-1,1)$ is filled, we can fill $(1,1)$. Using a sequence of X/Z moves, we get $(i,1)/(1,i)$ for all $i$ (See Fig. 5.1(b)). Now we perform a Y move from $(2,1)/(1,2)$ to get $(3,0)/(0,3)$. Again using a sequence of X/Z moves, we get $(i,3)/(3,i)$ for all $i$ (See Fig. 5.1(c)). Continuing in this fashion, we can fill every other row and every other column. We must now separate the proof into two cases:

Case 1: $p$ odd ($p \neq 2$). In this case, the periodic boundary conditions mean that filling every other row/column will in fact fill every row/column. So the above procedure is enough to fill the grid.

Case 2: $p = 2$. Here, filling every other row/column will miss half of the rows/columns, so we must use the final rule involving hermitian operators to continue. We use an X move at $(1,\frac{D}{2})$. Since $(0,\frac{D}{2})$ corresponds to a hermitian operator, we mark $(2,\frac{D}{2})$ for free (See Fig. 5.1(d)). It is now clear that we can mark all remaining point using basic moves.

A final check is that we did not perform any forbidden moves in the above procedure; this can be easily verified. The case $r \neq 1$ is almost identical. Our initially marked points include $(1,0),(0,r),(D-1,r)$. A key observation is that, since $r$ is coprime with $D$, all integers $0,\ldots,D-1$ can be obtained as multiples of $r$. Then we can repeat the above procedure of filling rows and columns one by one. The only difference is the order in which they are filled. □

By our two lemmas, we have $\mathcal{A}[\mathcal{O}] = su(p^n)$ in every case. Since $p^n$ was an arbitrary divisor of $|H|$, we have completed the proof of the theorem. We finish with the proof of Lemma 2.

*Proof. of Lemma 2.* It is convenient to assume that $C^0 = I$. This can always be done by enacting a transformation $C^i \to \tilde{C}^i = C^{0\dagger}C^i$. Such a

transformation does not change $\mathcal{O}$; it is just a relabelling of the elements. Define the set $\tilde{\mathcal{C}} = \left\{\tilde{C}^i, i = 0 \dots d-1\right\}$.

In order to impose further structure on $\tilde{\mathcal{C}}$, we use injectivity which states that the set of products $\{A^{i_1}A^{i_2}\dots A^{i_L}\}$ spans the space of all complex matrices for large enough $L$ (condition 3, Theorem 1). By tracing out the junk subspace corresponding to the matrices $B^i$, we see that this property holds on the logical subspace alone. That is, every $D \times D$ matrix can be expressed as a linear combination of products $C^{i_1}C^{i_2}\dots C^{i_n}$. The fact that this also holds for the matrices $\tilde{C}^i$ can be seen by using the statement of injectivity given by condition 4 of Theorem 1, which clearly holds for $\tilde{C}^i$ if it does for $C^i$.

Now, since the matrices $\tilde{C}^i$ span all matrices with their products, and their products are always Heisenberg-Weyl operators, they must generate the entire set of Heisenberg-Weyl operators, up to complex phases. This means we must have a pair of operators $\tilde{C}^a$ and $\tilde{C}^b$ such that $\tilde{C}^a\tilde{C}^b = \Omega^r\tilde{C}^b\tilde{C}^a$ where $p$ does not divide $r$. If not, define the numbers $r_{ij}$ by $\tilde{C}^i\tilde{C}^j = \Omega^{r_{ij}}\tilde{C}^j\tilde{C}^i$. Then a commutator of arbitrary elements can be written:

$$\prod_i (\tilde{C}^i)^{a_i} \prod_j (\tilde{C}^j)^{b_j} = \Omega^{\sum_{ij} a_i b_j r_{ij}} \prod_j (\tilde{C}^i)^{b_j} \prod_i (\tilde{C}^i)^{a_i} \tag{5.5}$$

If $p|r_{ij}$ for all $i, j$, then $p|\sum_{ij} a_i b_j r_{ij}$, which cannot always be true if we have a generating set. Finally, for any unitary operators that commute like $\tilde{C}^a\tilde{C}^b = \Omega^r\tilde{C}^b\tilde{C}^a$ there exists a unitary $U$ such that $UC^aU^\dagger = X$ and $UC^bU^\dagger = Z^r$ (see Ref. [78] for the case $r = 1$, which generalizes easily). In the basis defined by $U$, we have $I, X, Z^r \in \tilde{\mathcal{C}}$, which gives the claimed operators in $\mathcal{O}$. □

## 5.4 Example: $G = \mathbb{Z}_n \times \mathbb{Z}_n$

In this section, we remark on some interesting applications of our results in the context of a symmetry group $G$ is of the form $\mathbb{Z}_n \times \mathbb{Z}_n$ for some integer $n$. Note that, as discussed in Sec. 3.4, this also covers the case when $G$ is a classical Lie group as well as certain finite groups like dihedral groups. The second cohomology group is $H^2[\mathbb{Z}_n \times \mathbb{Z}_n, U(1)] = \mathbb{Z}_n$, so there are $n-1$ non-trivial phases. To label these phases, suppose the group is generated by two elements $a$ and $b$, and suppose $V(a)V(b) = \Omega^r V(b)V(a)$ where $V(g)$ is the representation of $G$ in the virtual space. Then $r$ labels the SPT phase, and the phase is maximally non-commutative if $\gcd(r, n) = 1$ [73, 74, 76].

Using the results of Ref. [77], it is possible to calculate that the dimension of irreps in the phase labelled by $r$, that is the dimension of the logical subspace, is $D_r = n/\gcd(r, n)$. By our results, we then get computation on a $D_r$-level system for all phases, consistent with the results of Refs. [79]. However, only for those satisfying $\gcd(r, n) = 1$ are we guaranteed universality (perhaps on a subspace of the whole logical subspace). Even still, the fact that all non-trivial SPT phases protected by classical Lie groups can be used for computation has great practical interest.

This result also means that we can compute on a qudit of arbitrarily large dimension with a chain of physical spins of bounded dimension. Indeed, consider the case where $n = 2^m$ and $r$ is odd. By the above arguments, this gives a universal set of gates on a system of dimension $2^m$, equivalent to that of $m$ qubits, no matter what the physical dimension is. This goes against the usual idea that 1D systems can only process a single qudit of information. However one should be careful not to take this argument too far. Suppose our physical system is a qutrit, meaning that we have only three primitive gates to work with. By the proof in the previous section, this is still enough to generate all gates in $SU(2^m)$, but the number of steps needed to generate an arbitrary gate will grow exponentially with $m$, at least when using our method. So, while we are able to process $m$ qubits with a chain of qutrits, the scaling may not be efficient, and indeed results such as that given in Ref. [49] suggest it is not.

# Chapter 6

# Conclusions and Outlook

In this thesis, we studied the relationship between measurement-based quantum computation and symmetry-protected topological order, one which sits on the border of condensed matter physics and quantum information science. More specifically, we began with the following question: Does there exist a broad family of SPT phases which support non-trivial gates throughout each phase? To answer this, we introduced three computational techniques: the mixed state interpretation, the oblivious wire, and the use of infinitesimal gates. With these pieces, we proved that all of the maximally non-commutative SPT phases have uniform computational power. By proving new results on the structure of MPS with SPT order and introducing some additional computational techniques, we were able to extend this result to all SPT phases that can be protected by a finite abelian group. We then used the algebraic structure inherited from the SPT phase classification to determine the computational power of each phase. We proved that the maximally non-commutative phases were always universal for a qudit system, but we gave a non-universal counterexample in the general case.

The immediate questions that follow are whether our results can extend to arbitrary SPT phases in 1D, and then to higher-dimensional phases. The answer to the former is likely to be negative. Firstly, most of the important results in this thesis rely crucially on the abelian condition in one way or another. Indeed, for general SPT phase we cannot even define a consistent dimension of the logical subspace since, given a phase labelled by $[\omega]$, there may be $\omega$-irreps of different dimensions. The notion of SPT entanglement is also not well-defined within non-abelian phases [71]. For higher-dimensional systems there are several examples of states with SPT order that can be used as universal resources [80, 81, 82]. In some cases, these states have certain advantages over other states without SPT order [81, 82]. On the other hand, there has been comparatively little success in extending these results throughout the corresponding SPT phases [40], and the methods developed here may aid this venture.

In general, higher-dimensional systems support more complex forms of SPT order such as weak SPT [7, 13] and phases protected by higher-form

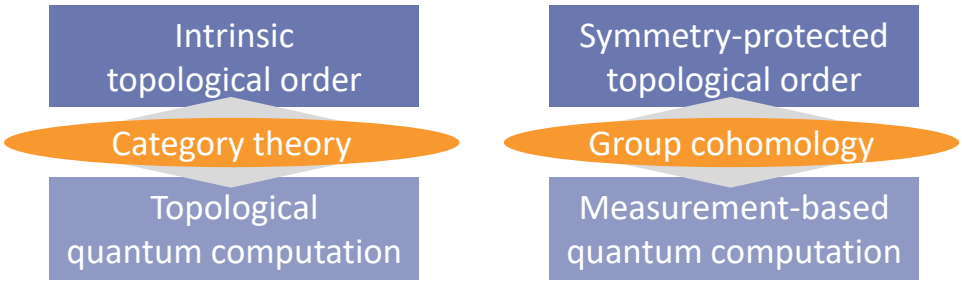


Figure 6.1: In the same way that the language of category theory allows us to classify gates that can be executed by braiding the anyonic excitations of topologically ordered systems in 2D [86, 17, 87], group cohomology determines the gates implementable in measurement-based quantum computation using 1D resource states with symmetry-protected topological order.

symmetries [83, 84, 85], and it is not yet clear which type would most naturally support computation. Another issue is how information is propagated through the virtual space of higher dimensional tensor networks. All higher-dimensional resource states known to the author have the property that individual "wires" that carry one qubit each can be cut out of the lattice, perhaps after some preparatory measurements. This property is not likely to persist throughout phases, and furthermore it inherently eliminates some aspect of the SPT order by reducing to a pseudo-1D system. The authors of Ref. [81] get around this by only cutting out wires in certain regions of the resource state, leaving other regions in tact to take advantage of the SPT order, but there may be a more natural solution.

We will end by discussing the implications of our results on the connection between quantum phases of matter and quantum computation, as summarized in Fig.6.1. A similar result to ours already exists in the context of topological quantum computation (TQC). Topological order in 2D is classified by the braiding and fusion statistics of bulk anyonic excitations, which can be compactly described by modular tensor categories [17, 88]. Because TQC relies on manipulating these excitations, it can be characterized by the same algebraic framework [86, 17, 87]. This is exactly analogous to the current result. SPT phases can be classified by their edge modes which transform non-trivially under the symmetry, as described by group cohomology. The Hilbert space associated to the logical subspace in which we encode and process information corresponds precisely to this edge mode in 1D. Because of this, group cohomology also determines the computational power of 1D SPT phases.

Thus the results in this thesis can be seen as evidence of a more general theme. A typical method to classify quantum phases is by examining the non-trivial excitations above the ground states in the phase [7, 88, 8]. If computation proceeds by manipulating these same excitations, then the computation will inherit the algebraic structure that describes the phase, and also its robustness to certain perturbations. There is already evidence of this conjecture in higher-dimensional SPT phases [81, 82, 89, 83]. It would also be interesting to see whether the mathematical frameworks that unify topological order and SPT order, such as G-crossed braided tensor categories [8], could also describe computation with systems that have both types of order.

# Bibliography


[1] David T. Stephen, Dong-Sheng Wang, Abhishodh Prakash, Tzu-Chieh Wei, and Robert Raussendorf. Computational power of symmetry-protected topological phases. *Phys. Rev. Lett.*, 119:010504, Jul 2017.

[2] Robert Raussendorf, Dong-Sheng Wang, Abhishodh Prakash, Tzu-Chieh Wei, and David T. Stephen. Symmetry-protected topological phases with uniform computational power in one dimension. *Phys. Rev. A*, 96:012302, Jul 2017.

[3] Michael A. Levin and Xiao-Gang Wen. String-net condensation: A physical mechanism for topological phases. *Phys. Rev. B*, 71:045110, Jan 2005.

[4] Lukasz Fidkowski and Alexei Kitaev. Topological phases of fermions in one dimension. *Phys. Rev. B*, 83:075103, Feb 2011.

[5] Xie Chen, Zheng-Cheng Gu, and Xiao-Gang Wen. Complete classification of one-dimensional gapped quantum phases in interacting spin systems. *Phys. Rev. B*, 84:235128, Dec 2011.

[6] Norbert Schuch, David Pérez-García, and Ignacio Cirac. Classifying quantum phases using matrix product states and projected entangled pair states. *Phys. Rev. B*, 84:165139, Oct 2011.

[7] Xie Chen, Zheng-Cheng Gu, Zheng-Xin Liu, and Xiao-Gang Wen. Symmetry protected topological orders and the group cohomology of their symmetry group. *Phys. Rev. B*, 87:155114, Apr 2013.

[8] Maissam Barkeshli, Maissam Bonderson, Meng Cheng, and Zhenghan Wang. Symmetry, defects, and gauging of topological phases. 2014.

[9] Zheng-Cheng Gu and Xiao-Gang Wen. Symmetry-protected topological orders for interacting fermions: Fermionic topological nonlinear $\sigma$ models and a special group supercohomology theory. *Phys. Rev. B*, 90:115141, Sep 2014.

[10] Anton Kapustin, Ryan Thorngren, Alex Turzillo, and Zitao Wang. Fermionic symmetry protected topological phases and cobordisms. *Journal of High Energy Physics*, 2015(12):52, 2015.

[11] Hao Song, Sheng-Jie Huang, Liang Fu, and Michael Hermele. Topological phases protected by point group symmetry. *Phys. Rev. X*, 7:011020, Feb 2017.

[12] Tian Lan, Liang Kong, and Xiao-Gang Wen. Classification of 2+1d topological orders and spt orders for bosonic and fermionic systems with on-site symmetries. 2016.

[13] Meng Cheng, Michael Zaletel, Maissam Barkeshli, Ashvin Vishwanath, and Parsa Bonderson. Translational symmetry and microscopic constraints on symmetry-enriched topological phases: A view from the surface. *Phys. Rev. X*, 6:041068, Dec 2016.

[14] Xiao-Liang Qi and Shou-Cheng Zhang. Topological insulators and superconductors. *Rev. Mod. Phys.*, 83:1057–1110, Oct 2011.

[15] Leon Balents. Spin liquids in frustrated magnets. *Nature*, 464(7286):199–208, 2010.

[16] A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2 – 30, 2003.

[17] Chetan Nayak, Steven H. Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80:1083–1159, Sep 2008.

[18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[19] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[20] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, 1985.

[21] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, Oct 2003.

[22] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the /'magic/' for quantum computation. *Nature*, 510(7505):351–355, Jun 2014. Article.

[23] Robert Raussendorf. Contextuality in measurement-based quantum computation. *Phys. Rev. A*, 88:022322, Aug 2013.

[24] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, May 2001.

[25] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, Aug 2003.

[26] Daniel E Browne, Matthew B Elliott, Steven T Flammia, Seth T Merkel, Akimasa Miyake, and Anthony J Short. Phase transition of computational power in the resource states for one-way quantum computation. *New Journal of Physics*, 10(2):023010, 2008.

[27] Sean D. Barrett, Stephen D. Bartlett, Andrew C. Doherty, David Jennings, and Terry Rudolph. Transitions in the computational power of thermal states for measurement-based quantum computation. *Phys. Rev. A*, 80:062328, Dec 2009.

[28] Andrew C. Doherty and Stephen D. Bartlett. Identifying phases of quantum many-body systems that are universal for quantum computation. *Phys. Rev. Lett.*, 103:020506, Jul 2009.

[29] Stein Olav Skrøvseth and Stephen D. Bartlett. Phase transitions and localizable entanglement in cluster-state spin chains with ising couplings and local fields. *Phys. Rev. A*, 80:022316, Aug 2009.

[30] Akimasa Miyake. Quantum computation on the edge of a symmetry-protected topological order. *Phys. Rev. Lett.*, 105:040501, Jul 2010.

[31] Stephen D. Bartlett, Gavin K. Brennen, Akimasa Miyake, and Joseph M. Renes. Quantum computational renormalization in the haldane phase. *Phys. Rev. Lett.*, 105:110502, Sep 2010.

[32] Keisuke Fujii and Tomoyuki Morimae. Topologically protected measurement-based quantum computation on the thermal state of a

nearest-neighbor two-body hamiltonian with spin-3/2 particles. *Phys. Rev. A*, 85:010304, Jan 2012.

[33] Keisuke Fujii, Yoshifumi Nakata, Masayuki Ohzeki, and Mio Murao. Measurement-based quantum computation on symmetry breaking thermal states. *Phys. Rev. Lett.*, 110:120502, Mar 2013.

[34] Andrew S Darmawan, Gavin K Brennen, and Stephen D Bartlett. Measurement-based quantum computation in a two-dimensional phase of matter. *New. J. Phys.*, 14(1):013023, 2012.

[35] Dominic V Else, Stephen D Bartlett, and Andrew C Doherty. Symmetry protection of measurement-based quantum computation in ground states. *New Journal of Physics*, 14(11):113016, 2012.

[36] Dominic V. Else, Ilai Schwarz, Stephen D. Bartlett, and Andrew C. Doherty. Symmetry-protected phases for measurement-based quantum computation. *Phys. Rev. Lett.*, 108:240505, Jun 2012.

[37] Jacob Miller and Akimasa Miyake. Resource quality of a symmetry-protected topologically ordered phase for quantum computation. *Phys. Rev. Lett.*, 114:120506, Mar 2015.

[38] Abhishodh Prakash and Tzu-Chieh Wei. Ground states of one-dimensional symmetry-protected topological phases and their utility as resource states for quantum computation. *Phys. Rev. A*, 92:022310, Aug 2015.

[39] Tzu-Chieh Wei, Ying Li, and Leong Chuan Kwek. Transitions in the quantum computational power. *Phys. Rev. A*, 89:052315, May 2014.

[40] Tzu-Chieh Wei and Ching-Yu Huang. Universal measurement-based quantum computation in two-dimensional spt phases. 2017.

[41] E. Fradkin. *Field Theories of Condensed Matter Physics*. Field Theories of Condensed Matter Physics. Cambridge University Press, 2013.

[42] Iulia Buluta and Franco Nori. Quantum simulators. *Science*, 326(5949):108–111, 2009.

[43] D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, and P. Zoller. Cold bosonic atoms in optical lattices. *Phys. Rev. Lett.*, 81:3108–3111, Oct 1998.

[44] Immanuel Bloch, Jean Dalibard, and Wilhelm Zwerger. Many-body physics with ultracold gases. *Rev. Mod. Phys.*, 80:885–964, Jul 2008.

[45] Andrew A. Houck, Hakan E. Tureci, and Jens Koch. On-chip quantum simulation with superconducting circuits. *Nat Phys*, 8(4):292–299, Apr 2012.

[46] J. Eisert, M. Cramer, and M. B. Plenio. Colloquium. *Rev. Mod. Phys.*, 82:277–306, Feb 2010.

[47] M B Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007.

[48] Don N. Page. Average entropy of a subsystem. *Phys. Rev. Lett.*, 71:1291–1294, Aug 1993.

[49] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac. Matrix Product State Representations. *Quant. Inf. Comp.*, 7:401, 2007.

[50] F. Verstraete and J. I. Cirac. Matrix product states represent ground states faithfully. *Phys. Rev. B*, 73:094423, Mar 2006.

[51] Norbert Schuch, Michael M. Wolf, Frank Verstraete, and J. Ignacio Cirac. Entropy scaling and simulability by matrix product states. *Phys. Rev. Lett.*, 100:030504, Jan 2008.

[52] Steven R. White. Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett.*, 69:2863–2866, Nov 1992.

[53] U. Schollwöck. The density-matrix renormalization group. *Rev. Mod. Phys.*, 77:259–315, Apr 2005.

[54] Ian Affleck, Tom Kennedy, Elliott H. Lieb, and Hal Tasaki. Rigorous results on valence-bond ground states in antiferromagnets. *Phys. Rev. Lett.*, 59:799–802, Aug 1987.

[55] Mikel Sanz, David Pérez-García, Michael M. Wolf, and Juan I. Cirac. A quantum version of wielandt's inequality. *IEEE Trans. Inf. Theor.*, 56(9):4668–4673, September 2010.

[56] Bei Zeng, Xie Chen, Duan-Lu Zhou, and Xiao-Gang Wen. Quantum information meets quantum matter – from quantum entanglement to topological phase in many-body systems. 2016.

[57] D. Pérez-García, M. M. Wolf, M. Sanz, F. Verstraete, and J. I. Cirac. String order and symmetries in quantum spin lattices. *Phys. Rev. Lett.*, 100:167202, Apr 2008.

[58] Lev Davidovich Landau and Evgenii M Lifshitz. *Statistical Physics: V. 5: Course of Theoretical Physics*. Pergamon press, 1969.

[59] Xie Chen, Zheng-Cheng Gu, and Xiao-Gang Wen. Complete classification of one-dimensional gapped quantum phases in interacting spin systems. *Phys. Rev. B*, 84:235128, Dec 2011.

[60] Xie Chen, Zheng-Cheng Gu, and Xiao-Gang Wen. Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order. *Phys. Rev. B*, 82:155138, Oct 2010.

[61] M Van den Nest, W Dür, A Miyake, and H J Briegel. Fundamentals of universality in one-way quantum computation. *New J. Phys.*, 9(6):204, 2007.

[62] M. Van den Nest, W. Dür, G. Vidal, and H. J. Briegel. Classical simulation versus universality in measurement-based quantum computation. *Phys. Rev. A*, 75:012337, Jan 2007.

[63] Y.-Y. Shi, L.-M. Duan, and G. Vidal. Classical simulation of quantum many-body systems with a tree tensor network. *Phys. Rev. A*, 74:022320, Aug 2006.

[64] D. Gross, S. T. Flammia, and J. Eisert. Most quantum states are too entangled to be useful as computational resources. *Phys. Rev. Lett.*, 102:190501, May 2009.

[65] Michael J. Bremner, Caterina Mora, and Andreas Winter. Are random pure states useful for quantum computation? *Phys. Rev. Lett.*, 102:190502, May 2009.

[66] D. Gross and J. Eisert. Novel schemes for measurement-based quantum computation. *Phys. Rev. Lett.*, 98:220503, May 2007.

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

[68] Gavin K. Brennen and Akimasa Miyake. Measurement-based quantum computer in the gapped ground state of a two-body hamiltonian. *Phys. Rev. Lett.*, 101:010502, Jul 2008.

[69] Ying Li, Daniel E. Browne, Leong Chuan Kwek, Robert Raussendorf, and Tzu-Chieh Wei. Thermal states as universal resources for quantum computation with always-on interactions. *Phys. Rev. Lett.*, 107:060501, Aug 2011.

[70] Leong Chuan Kwek, Zhaohui Wei, and Bei Zeng. Measurement-based quantum computing with valence-bond-solids. *International Journal of Modern Physics B*, 26(02):1230002, 2012.

[71] Iman Marvian. Symmetry-protected topological entanglement.

[72] I_A G Berkovich and EM Zhmud. *Characters of finite groups*, volume 1. American Mathematical Soc., 1998.

[73] Kasper Duivenvoorden and Thomas Quella. From symmetry-protected topological order to landau order. *Phys. Rev. B*, 88:125115, Sep 2013.

[74] Kasper Duivenvoorden and Thomas Quella. Topological phases of spin chains. *Phys. Rev. B*, 87:125145, Mar 2013.

[75] Zhaoxi Xiong. Minimalist approach to the classification of symmetry protected topological phases. 2016.

[76] Dominic V. Else, Stephen D. Bartlett, and Andrew C. Doherty. Hidden symmetry-breaking picture of symmetry-protected topological order. *Phys. Rev. B*, 88:085114, Aug 2013.

[77] NB Backhouse and CJ Bradley. Projective representations of abelian groups. *Proceedings of the American Mathematical Society*, 36(1):260–266, 1972.

[78] D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun. Quantum computation based on $d$ -level cluster state. *Phys. Rev. A*, 68:062303, Dec 2003.

[79] Dong-Sheng Wang, David T. Stephen, and Robert Raussendorf. Qudit quantum computation on matrix product states with global symmetry. *Phys. Rev. A*, 95:032312, Mar 2017.

[80] Hendrik Poulsen Nautrup and Tzu-Chieh Wei. Symmetry-protected topologically ordered states for universal quantum computation. *Phys. Rev. A*, 92:052309, Nov 2015.

[81] Jacob Miller and Akimasa Miyake. Hierarchy of universal entanglement in 2d measurement-based quantum computation. *Npj Quant. Inf.*, 2:16036, 2016.

[82] Jacob Miller and Akimasa Miyake. Latent computational complexity of symmetry-protected topological order with fractional symmetry. 2016.

[83] Beni Yoshida. Topological phases with generalized global symmetries. *Phys. Rev. B*, 93:155131, Apr 2016.

[84] Sam Roberts, Beni Yoshida, Aleksander Kubica, and Stephen D. Bartlett. Symmetry protected topological order at nonzero temperature. 2013.

[85] Anton Kapustin and Ryan Thorngren. Higher symmetry and gapped phases of gauge theories. 2013.

[86] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. *Bull. Amer. Math. Soc.*, 40:31–38, 2003.

[87] Eric Rowell, Richard Stong, and Zhenghan Wang. On classification of modular tensor categories. *Communications in Mathematical Physics*, 292(2):343–389, 2009.

[88] Xiao-Gang Wen. A theory of 2+1d bosonic topological orders. *National Science Review*, 3(1):68–106, 2016.

[89] Beni Yoshida. Gapped boundaries, group cohomology and fault-tolerant logical gates. 2015.

# Appendix A

# Born rule and mixed state interprtation

Here we derive the Born rule for matrix product states in Abelian SPT phases. This will allow us to formally argue the validity of the mixed state interpretation of MBQC. Suppose our left boundary condition is in the state $\rho$ such that our ground state is the mixed state $\psi$:

$$\psi = \sum_{\substack{i_0,\ldots,i_N \\ j_0,\ldots,j_N}} \langle R|A^{i_N}\ldots A^{i_1}A^{i_0}\rho A^{j_0\dagger}A^{j_1\dagger}\ldots A^{j_N\dagger}|R\rangle |i_0\ldots i_N\rangle\langle j_0\ldots j_N| \tag{A.1}$$

This state is normalized when it is in canonical form. Now suppose we measure some observable $O$ on spin $i_0$. The probability of outcome $o_\alpha$ is then:

$$\begin{aligned} p(o_i) &= \sum_{i_1,\ldots,i_N} \langle R|A^{i_N}\ldots A^{i_1}A[o_\alpha]\rho A[o_\alpha]^\dagger A^{i_1\dagger}\ldots A^{i_N\dagger}|R\rangle \\ &= \sum_{i_1,\ldots i_N} \mathrm{Tr}\ \Big[\Big(A^{i_{k+1}\dagger}\ldots A^{i_N\dagger}|R\rangle\langle R|A^{i_N}\ldots A^{i_{k+1}}\Big) \\ &\quad \Big(A^{i_k}\ldots A^{i_1}A[o_\alpha]\rho A[o_\alpha]^\dagger A^{i_1\dagger}\ldots A^{i_k\dagger}\Big)\Big] \end{aligned} \tag{A.2}$$

Again by the canonical form, the channel $\mathcal{E}^\dagger(X) = \sum_i A^{i\dagger}(X)A^i$ is trace preserving and has a unique fixed point $\Lambda$ which is a density operator. $\Lambda$ commutes with $\mathbb{V}(g)$, so it can be decomposed as $\Lambda = \bigoplus_\alpha p_\alpha \Lambda_\alpha \otimes \Omega$ where each $\Lambda_\alpha$ is a density operator in block $\alpha$ and $\Omega = \mathbb{I}/D$ is the maximally mixed state. Then the first term in the trace evaluates to $\mathrm{Tr}\left(|R\rangle\langle R|\right)\Lambda = \Lambda$. Similarly, the second term is $\mathrm{Tr}\left(\Lambda A[o_\alpha]\rho A[o_\alpha]^\dagger\right)\mathbb{I}$ [49]. Then we have:

$$p(o_i) = \mathrm{Tr}\left(\Lambda A[o_\alpha]\rho A[o_\alpha]^\dagger\right)\mathrm{Tr}\ \Lambda = \mathrm{Tr}\left(\Lambda A[o_\alpha]\rho A[o_\alpha]^\dagger\right) \tag{A.3}$$

If the outcome $o_\alpha$ labels a state $|i\rangle$ in the wire basis, we have:

$$p(i) = \mathrm{Tr}\left[\Lambda \mathcal{P}_i^\dagger \left(\bigoplus_\alpha B_\alpha^i \otimes C_\alpha^i\right) \rho \left(\bigoplus_\alpha B_\alpha^{i\dagger} \otimes C_\alpha^{i\dagger}\right) \mathcal{P}_i\right] \tag{A.4}$$

$$= \mathrm{Tr}\left[\left(\bigoplus_\alpha p_{\mathcal{P}_i^\dagger(\alpha)} \Lambda_{\mathcal{P}_i^\dagger(\alpha)} \otimes \Omega\right) \left(\bigoplus_\alpha B_\alpha^i \otimes \mathbb{I}\right) \rho \left(\bigoplus_\alpha B_\alpha^{i\dagger} \otimes \mathbb{I}\right)\right] \tag{A.5}$$

If $\rho = \mathbb{I}_\alpha$, then we have:

$$p(i|\alpha) = \mathrm{Tr}\left(p_{\mathcal{P}_i^\dagger(\alpha)} \Lambda_{\mathcal{P}_i^\dagger(\alpha)} B_\alpha^i B_\alpha^{i\dagger}\right) \equiv \nu_\alpha^{ii} \tag{A.6}$$

Note that the constants $\nu_\alpha^{ii}$ can be summed over $\alpha$ to recover $\nu^{ii}$ as defined earlier. For any measurement basis given by an observable $O$, the sum of probabilities of all possible outcomes can be shown to be $\mathrm{Tr}(\Lambda\rho)$. This is equal to the trace of $\psi$ in the large $N$ limit, so our probabilities sum to one if our state is normalized.

## A.1 Mixed state interpretation

Now we use the above calculation to argue the validity of our mixed state interpretation and the corresponding "sum over outcomes" approach. Consider an MBQC scheme in which the logical evolution depends on measurement outcomes, even when supplemented by byproduct propagation. That is, we assume that measuring the next spin in the chain with outcome $|s\rangle$ enacts the evolution

$$|L\rangle \to \frac{1}{\sqrt{p_s}} \left(\sum_i \langle s|i\rangle A^i\right) |L\rangle = \frac{1}{\sqrt{p_s}} \Sigma_s \Gamma_s |L\rangle, \tag{A.7}$$

where $\Sigma_s$ is the unitary byproduct operator, and $\Gamma_s$ is the desired evolution, which at this point may not yet be unitary. $p_s$ is the probability of obtaining outcome $s$, which appears via the Born rule.

Now a general computation involves the measurement of $m$ spins in any basis with outcomes $\vec{s} = (s_1, \ldots, s_m)$, propagating byproduct operators after each step. The initial state $|L\rangle$ evolves to a final state $\frac{1}{\sqrt{p_{\vec{s}}}} \Sigma_{\vec{s}} |L'_{\vec{s}}\rangle$ where $|L'_{\vec{s}}\rangle = \Gamma_{s_m} \ldots \Gamma_{s_1} |L\rangle$, $\Sigma_{\vec{s}} = \prod_{i=1}^m \Sigma_{s_i}$ is the accumulated byproduct operator, and $p_{\vec{s}}$ is the probability of the outcome string $\vec{s}$. At this point, our resource state $|\psi\rangle$ has evolved to

$$|\psi_{\vec{s}}\rangle = \frac{1}{\sqrt{p_{\vec{s}}}} \sum_{i_{m+1}\ldots i_n} \langle R|A^{i_n}\ldots A^{i_{m+1}}\Sigma_{\vec{s}}|L'_{\vec{s}}\rangle|i_{m+1}\ldots i_n\rangle. \tag{A.8}$$

Computation ends with readout of some observable $O$ on the final state $|L'_{\vec{s}}\rangle$. Our only tool available to do this is a measurement of the next spin in the chain, $m+1$, whose measurement outcome must be used to infer something about $O$. Let $\{|o_i\rangle|i=0,\ldots,d-1\}$ be the relevant measurement basis for read out of $O$, which has been appropriately modified to propagate the accumulated byproduct operator $\Sigma_{\vec{s}}$ past the readout site. Letting $A[o_\alpha] = \sum_i \langle o_\alpha|i\rangle A^i$ we can use Eq. A.3 to determine the probability of obtaining the outcome $|o_\alpha\rangle$ given the previous outcomes $\vec{s}$:

$$p(o_i|\vec{s}) = \mathrm{Tr}\left(\Lambda\Sigma_{\vec{s}}A[o_\alpha]\frac{|L'_{\vec{s}}\rangle\langle L'_{\vec{s}}|}{p_{\vec{s}}}A[o_\alpha]^\dagger\Sigma_{\vec{s}}^\dagger\right). \tag{A.9}$$

Since $\Lambda$ acts trivially in the logical subspace, $\Sigma_{\vec{s}}$ can be eliminated from this equation using the unitarity and the cyclicity of the trace. We are left with:

$$p(o_i|\vec{s}) = \mathrm{Tr}\left(\Lambda A[o_\alpha]\frac{|L'_{\vec{s}}\rangle\langle L'_{\vec{s}}|}{p_{\vec{s}}}A[o_\alpha]^\dagger\right). \tag{A.10}$$

Now, the total probability of obtaining outcome $o_\alpha$ is given by $p(o_\alpha) = \sum_{\vec{s}} p(o_\alpha|\vec{s})p_{\vec{s}}$. By exploiting linearity within the above expression, we have:

$$p(o_i) = \mathrm{Tr}\left(\Lambda A[o_\alpha]\hat{\sigma}A[o_\alpha]^\dagger\right). \tag{A.11}$$

where we have introduced the mixed state $\hat{\sigma}$ given by:

$$\begin{aligned}\hat{\sigma} &= \sum_{\vec{s}} |L'_{\vec{s}}\rangle\langle L'_{\vec{s}}| \\ &= \sum_{s_m} \Gamma_{s_m}\left(\ \ldots\ \left(\sum_{s_1}\Gamma_{s_1}|L\rangle\langle L|\Gamma_{s_1}^\dagger\right)\ \ldots\ \right)\Gamma_{s_m}^\dagger.\end{aligned} \tag{A.12}$$

So we see that the readout statistics of $O$ are encoded in the mixed state $\hat{\sigma}$ which can be determined by summing over the outcomes of each measurement during computation. This sum occurs after byproduct propagation, and the accumulated byproduct operator has no effect other than changing the final readout basis.