4-6-2023

A Menagerie of Symmetry Testing Quantum Algorithms

Margarite Lynn LaBorde
Louisiana State University and Agricultural and Mechanical College

A MENAGERIE OF SYMMETRY TESTING QUANTUM ALGORITHMS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Physics and Astronomy

by
Margarite Lynn LaBorde
B.S., Louisiana State University, 2018
B.S., Louisiana State University, 2018
M.S., Louisiana State University, 2022
May 2023

To my parents, Rebecca and Raymond LaBorde. My greatest privilege has been being your child.

Acknowledgments

I would like to take this opportunity to thank everyone who supported me throughout my experiences as a graduate student. I would like to thank Dr. Jonathan Dowling for his mentorship and for welcoming me into quantum physics. He was a great mentor and friend and will be greatly missed. I would especially like to thank Dr. Mark Wilde for his mentorship and guidance. He stepped in to offer support during a tumultuous time—during a pandemic and the loss of an advisor—and I am extremely grateful to have been his student. I would also like to thank Dr. Stephen Shipman, Dr. Ivan Agullo, Dr. Mette Gaarde, and Dr. Feng Chen for taking the time to be a part of my graduate committee.

Additionally, I would like to acknowledge my husband, Zachary Bradshaw. Many restaurant napkins and whiteboards have seen our discussions, and there isn't an idea in math or physics that I find fascinating that isn't immediately shared with him. He is not only my best friend but my favorite mathematician.

Special thanks go to my fellow students of the Quantum Science and Technologies group. In particular, I would like to thank Soorya Rethinasamy, Aliza Siddiqui, and Roy Pace for their friendship and conversation. Discussing physics and research with them made being at LSU all the more fulfilling.

All of these people were instrumental in making my graduate studies enjoyable and fruitful. It is through their support that I was able to explore so many opportunities and choose to pursue my doctoral research in physics.

Funding for this work was provided by the Department of Defense SMART Scholarship. Funding for travel to conferences and research visits was provided by

Table of Contents

Abstract

In Chapter 1, we establish the mathematical background used throughout this thesis. We review concepts from group and representation theory. We further establish fundamental concepts from quantum information. This will allow us to then define the different notions of symmetry necessary in the following chapters.

In Chapter 2, we investigate Hamiltonian symmetries. We propose quantum algorithms capable of testing whether a Hamiltonian exhibits symmetry with respect to a group. Furthermore, we show that this algorithm is that this algorithm is DQC1-Complete. Finally, we execute one of our symmetry-testing algorithms on existing quantum computers for simple examples.

In Chapter 3, we discuss tests of symmetry for quantum states. For the case of testing Bose symmetry of a state, there is a simple and efficient quantum algorithm, while the tests for other kinds of symmetry rely on the aid of a quantum prover. We prove that the acceptance probability of each algorithm is equal to the maximum symmetric fidelity of the state being tested Finally, we establish various generalizations of the resource theory of asymmetry, with the upshot being that the acceptance probabilities of the algorithms are resource monotones.

In Chapter 4, we begin by showing that the analytical form of the acceptance probability of such a test is given by the cycle index polynomial of the symmetric group S_k. We derive a family of quantum separability tests, each of which is generated by a finite group; for all such algorithms, we show that the acceptance probability is determined by the cycle index polynomial of the group. Finally, we produce and analyze explicit circuit constructions for these tests, showing that the tests corresponding to the symmetric and cyclic groups can be executed with $O(k^2)$ and $O(k \log(k))$ controlled-SWAP gates, respectively, where k is the number of copies of the state

being tested.

In Chapter 5, we include additional results not previously published; in particular, we give a test for symmetry of a quantum state using density matrix exponentiation, a further result of Hamiltonian symmetry measurements when using Abelian groups, and an alternate Hamiltonian symmetry test construction for a block-encoded Hamiltonian.

Chapter 1. Mathematical Background and Introduction to Quantum Symmetry

1.1. Introduction

Before we begin discussing in any detail the finer aspects of symmetry-testing algorithms on quantum computers, we must necessarily establish for ourselves the language and tools we will employ to do so. The work described in this thesis rests primarily on three pillars—a basic understanding of group theory with an accompanying idea of group representations, a strong familiarity with quantum information, and concepts of symmetry with regards to both of the former.

We begin in Section 1.2 by introducing only so much math as an uninitiated reader may need to follow along with the more abstract notions in this text. This includes an elementary review of groups, group representations, and a smattering of examples of common groups. Someone well-versed with group theory may very easily skip this section and expect no repercussions in their understanding of the work. It is presented in a spirit of compassion to those with an interest in quantum symmetry without the benefit of some *a priori* knowledge of abstract algebra.

Section 1.3 continues with introducing concepts of quantum information that will be integral to the comprehension of this thesis. This section considers common terms and concepts such as density matrices, quantum channels, and common norms. Additionally, we give some derivations for important lemmas that will open the gateway to future proofs.

In Section 1.4, we come to the primary function of this chapter, which is to introduce notions of symmetry. We concern ourselves with the symmetries of states, Hamiltonians, and channels. The definitions herein are remarkably similar, but the nuances are great. In this section, we endeavor to delineate them here in appropriate detail as a reference for the rest of the thesis.

1.2. Mathematical Background

1.2.1. A Gentle Overview of Group Theory

For each section, we will provide a text which guides the knowledge and information reviewed therein. Our inaugural effort is Nicholson's *Introduction to Abstract Algebra* [Nic12], which is a standard undergraduate text on the matter. Here, the focus remains on finite, discrete groups as that is the primary concern of this body of work. (As an aside, continuous, compact groups are also within the capabilities of our future effort, as per the result of [GL21].) This section endeavors to introduce elementary aspects of group theory while introducing and defining groups of interest for this work as we proceed.

Let us start by defining a group. A set G equipped with a binary operation, $*$, is called a group if

1. $\forall g_1,\ g_2 \in G$, we have $g_1 * g_2 \in G$.
2. The operation $*$ is associative, i.e., $\forall g_1,\ g_2,\ g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.
3. There exists a unity element ϵ such that $\forall g \in G$, $g * \epsilon = \epsilon * g = g$.
4. $\forall g \in G$, there exists an inverse $g^{-1} \in G$ such that $g * g^{-1} = \epsilon$.

For finite groups, $|G|$ denotes the order of the group, which is the number of unique elements of the group. Additionally, note that we often suppress the binary operation "$*$" in favor of using juxtaposition.

This list of axioms encapsulates a powerful but simple mathematical object, best studied via examples. An illustrative but simple example is the integers modulo n, where n is some integer. This group is denoted $\mathbb{Z}_n$ and comes equipped with addition as its binary operator. We already know that addition is associative and has an identity, $\epsilon = 0$. For inverses, consider

$$z + z^{-1} = 0 \bmod n \cong n\,. \tag{1.1}$$

This equation shows that any integer z in $\mathbb{Z}_n$ has an inverse $n - z$ also in $\mathbb{Z}_n$. Elementary investigations will also demonstrate that this group is closed under this modulo addition. We can convince ourselves that many other sets form groups under addition in just such a way, be they the reals, complex numbers, etc., but $\mathbb{Z}_n$ is a nice, finite plaything to illustrate these traits. It will also reappear quite often as we progress throughout this work.

Those familiar with quantum mechanics (or mathematics) likely won't be surprised to learn that not all groups are Abelian (or commutative, if you prefer the term), but we caution the reader anyway. For an intuitive picture of this, consider the dihedral group D_n which has order $2n$. Picture a regular polygon of n sides; D_n is defined to be the set of all transformations that leave the shape invariant. For instance, an equilateral triangle is invariant under flips and rotations of $1/3$ the way around the shape. Obviously, combinations of these actions will also leave the shape invariant. Yet, if we identify each vertex of a triangle, it becomes immediately clear that a flip followed by a rotation is *not* the same as a rotation followed by a flip. Figure 1.1 visualizes this discrepancy.

Any definition of the groups should encapsulate these observed rules. First, identify the rotations with the symbol r and flips with f. Then define the group as

$$D_3 \coloneqq \langle f, r | f^2 = r^3 = \epsilon \text{ and } rf = fr^2 \rangle \,. \tag{1.2}$$

A quick sanity check indicates that two flips or three rotations give us back the original triangle exactly as expected. Figure 1.1 demonstrates the last rule regarding the commutation of flips and rotations. Often, non-Abelian groups like the dihedral group will have relationships like this explicitly specified.

Now, given some group G, we might also be interested in any subgroup contained within

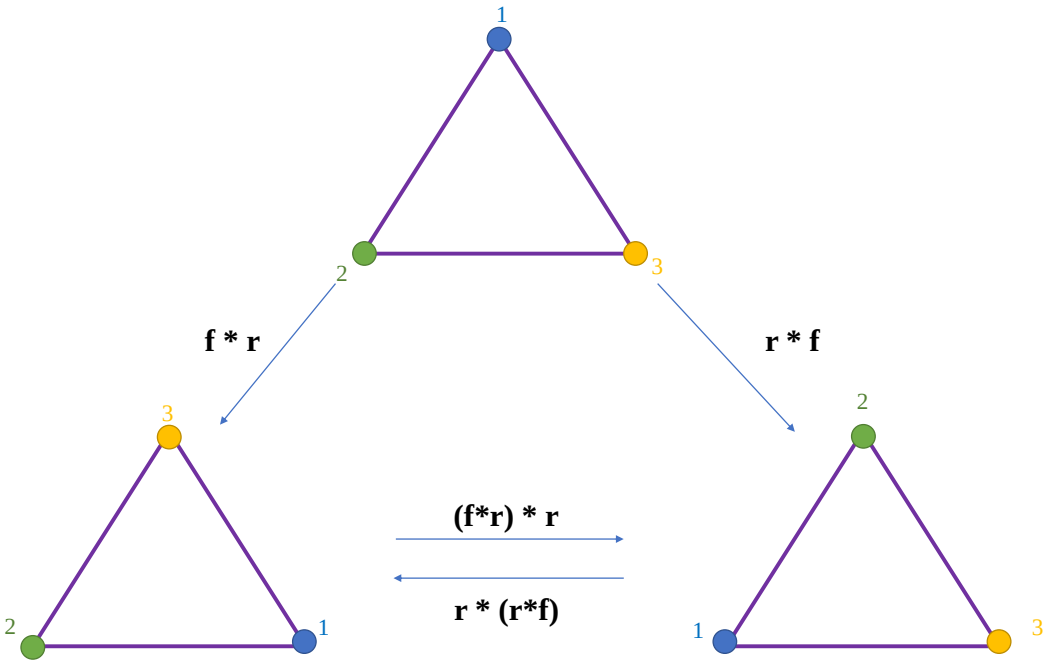


Figure 1.1. A cartoon demonstrating that the dihedral group D_3 is non-Abelian. Colored circles identify the three vertices, and it becomes visually obvious that the rotation and flip operations do not commute.

it. We call a subset H a *subgroup* of G if it is also a group under the same operation as G. Every group has at least two subgroups—the identity and the entirety of G. Since these cases are ubiquitous, they are typically referred to as *trivial* subgroups. Any other valid subgroup is a *proper* subgroup.

Subgroups feature prominently in the set of permutations on k letters, denoted S_k. Elements of this group take the form $(1\ 2\ \cdots\ k)$ (this as an example; not all permutations involve all k elements) where they are read from left to right within the parentheses but right-to-left without. For example, consider S_4 and its elements. The element $(1\ 2)$ says to permute the first object with the second. Now, consider the product $(1\ 2)(2\ 3) = (1\ 2\ 3)$.

So why is this group interesting? Well, Cayley's theorem states that all finite groups are

isomorphic to a subgroup of a permutation group[Jor70]. That is a hefty assertion! However, the totality of Cayley's theorem is even stronger than that. It further states that any group is a subset of a symmetric group even for infinite groups, and it can be given a more general definition as well in terms of cosets. For our needs, the restricted case of finite groups and the standard symmetric group of S_k will suit just fine.

Consider the example of the alternating group of degree k, or A_k. This is the set of all even permutations of S_k. We can employ the subgroup test [Nic12, Section 2.3] to ensure that A_k is indeed a subgroup. First, it contains the identity permutation ( ). Second, the product of two even permutations g_1 and g_2 is also even; therefore, $g_1 * g_2 \in A_k$. Third, if some permutation g is even, its inverse is also even. This last fact can be verified by writing g as a product of transpositions. Then g^{-1} is just those same transpositions in the opposite order; therefore, if there are an even number of transpositions in g, there is also an even number in g^{-1} and $g^{-1} \in A_k$. These three facts tell us A_k is a subgroup of S_k. Furthermore, for $k \geq 2$, we know A_k is a proper subgroup because $\forall k \geq 2$, the symmetric group S_k has at least one odd transposition.

Throughout, we have been defining groups using intuitive concepts or words. A diligent student may be discontent with this approach, as it lacks mathematical elegance and succinctness. This is where generators make their appearance. The generating set of a group G is a subset of elements by which every other group element can be produced as a combination of these elements, called generators, and their inverses.

In (1.2), we actually made use of the generating set to define D_3, but let's consider a simpler example as well. Define the cyclic group of order k to be the groups generated by cyclic shifts of k elements. For example, consider the group $C_4 = \{( ),\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2)\}$. The elements of this group read as shifting four things by nothing, one spot, two spots, and three

spots respectively. However, an equivalent interpretation is to simply apply the element (1 2 3 4) once, twice, thrice, or four times for the identity. Therefore, (1 2 3 4) generates C_4. Mathematically, this is denoted by

$$C_4 = \langle (1\ 2\ 3\ 4) \rangle \,, \tag{1.3}$$

and in general we have

$$C_k = \langle (1\ 2\ \ldots\ k) \rangle \,. \tag{1.4}$$

Generating sets are not necessarily unique in the sense that one group may be generated equivalently by different generating sets. This can be understood through some rudimentary representation theory, which we defer until the next section.

There is another important property of groups we should define, which is the notion of a normal subgroup. This we may not use, but it is good to know in general. To do so, we must first describe what it means for a group to be self-conjugate. Suppose that H is a subgroup of G. Then if $g \in G$, we can define another subgroup called the *conjugate* of H in G by

$$gHg^{-1} = \{ghg^{-1} | h \in H\} \,. \tag{1.5}$$

Of course, since the identity element is always in G, every group is a conjugate of itself. A group H is only called self-conjugate or *normal* if it is its only conjugate in G. If a group has no proper, normal subgroups, it is called *simple*.

Alas, we come to the final aspect of basic group theory with which we will concern ourselves in this section. As with many fields in mathematics, group theory must be able to address a fundamental question: when is one group different from another? To this purpose, we will discuss the group homomorphism and isomorphism.

A group homomorphism is a map $\phi : G \to H$ from one group G to another H such that the group action is preserved. That is, $\forall g_1, g_2 \in G$,

$$\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2) \,. \tag{1.6}$$

For ϕ to be a group homomorphism it must preserve the identity, inverses, and powers. All these criteria result from the above statement. If ϕ is additionally one-to-one and onto (thus a bijection) then ϕ is called an isomorphism. If two groups G and H are isomorphic, denoted $G \cong H$, then they are the same up to notation.

To exemplify this, let's look at two previous examples—C_k and Z_n. We will show that $C_k \cong Z_n$ when $k = n$. First, recall that C_k is generated by $(1\ 2\ ...\ k)$. Then each element of C_k is just this element multiplied by itself some m times. Define the homomorphism ϕ such that $\phi((1\ 2\ ...\ k)) = 1$. Then by (1.6),

$$\phi((1\ 2\ ...\ k)^m) = \phi((1\ 2\ ...\ k)) + ... + \phi((1\ 2\ ...\ k)) = m \,. \tag{1.7}$$

Thus we have identified each element of C_k with an element of Z_k. Note that the order of both groups is k, so we can restrict m such that $m \in \{0, 1, ..., k-1\} = Z_k$. Clearly, this map is one-to-one and onto by construction. Thus ϕ is a group isomorphism and $C_k \cong Z_k$.

With this, we close our review of group theory in order to progress necessarily to representations of groups. Know that group theory as a topic in mathematics is rich and well worth future study beyond the elementary concepts reviewed here. We merely hope that readers completely unfamiliar with its jargon will now be equipped to follow along with relevant discussions pertinent to the results presented in future sections.

1.2.2. Just Enough Representation Theory to be Dangerous

Groups are all well and good, but we need to know how to apply them to physical quantities to say anything meaningful. After all, it may not be immediately obvious how a quantum state may exhibit dihedral symmetry if we have only defined D_n geometrically. Representation theory saves the day here. Exactly as might be expected, representation theory lets us *represent* a group on a mathematical space that we care about. For this work, we need only consider finite-dimensional group representations. We offer as further reference the books *Representation Theory of Finite Groups* by Benjamin Steinberg [Ste09, Chapters 2-4] and *Representing finite groups: a semisimple introduction* by Ambar Sengupta [Sen11] for those interested in learning representation theory beyond the context given here.

We note, as a preface, that representations are usually defined in reference to a vector space (typically V or W in this context) over a field (F). In quantum computing and indeed quantum physics at large, we almost always consider F to be the complex numbers and V our Hilbert space. This is application dependent, however, and we will suppress such assumptions for now.

That being said, let's begin. A *representation* ϕ of a group G on a vector space V is defined to be a group homomorphism that preserves the action of the group. That is to say, ϕ associates to every group element a linear map $\phi : G \to \mathrm{GL}(V)$ such that

$$\phi(g)\phi(h) = \phi(gh) \quad \text{and}$$

$$\phi(\epsilon) = \mathbb{I},$$

$\forall g, h \in G$ and ϵ the identity element. (As an aside, we have chosen to use $\mathrm{GL}(V)$ instead of $\mathrm{End}_F(V)$ but the general idea remains the same. The map ϕ sends elements of the group G to the set of automorphisms on the vector space V. In the context of quantum mechanics, matrix

representations will be of utmost importance, and this notation fits nicely with that need.) Indeed, these conditions play well with the definition of group homomorphism introduced in the previous section.

We say that a representation is faithful if ϕ is a group isomorphism. This can be succinctly enforced by the rule that $\phi(g) \neq \mathbb{I}$ unless $g = \epsilon$. If the identity uniquely maps to the identity and the action of the group is obeyed, it can be quickly determined that $\phi(G)$ is isomorphic to G.

What if this is not the case? Suppose we have a map $\phi_t : G \to 1$ where every element of G is mapped to the number 1. Is this even a representation? Well, yes, it obeys both of the above rules in our definition of a representation, although it certainly isn't a faithful one. This is called the trivial representation, and it is literally a textbook example of not being faithful.

There are two other example representations which it will behoove us to cover. These are the standard representation and matrix representations. Consider first the latter. Suppose that $V = F^n$; then if $\phi : G \to \mathrm{GL}_n(F)$, ϕ is called a matrix representation.

Now suppose we have a matrix representation of the group S_n such that $\phi : S_n \to GL_n(\mathbb{C})$. Intuitively, such a representation can be obtained by letting the permutations in S_n permute the basis vectors in $\mathbb{C}^n$. Thus the standard representation of a permutation group is defined to be

$$\phi(\pi) \coloneqq [e_{\pi(1)} \ldots e_{\pi(n)}], \tag{1.8}$$

where e_i is the i-th basis vector and $\pi \in S_n$ is some permutation. Note that since every permutation group is a subgroup of S_n for some n, this defines the standard representation for all of them

simultaneously. As an example, consider the standard representation of $(1\ 3)$ acting on $V = \mathbb{C}^3$:

$$\phi((1\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{1.9}$$

where it is clear the first and third basis vectors have been swapped.

Again, we ask ourselves that ever-pertinent question: how do we know when two representations are equivalent to each other? Well, two representations $\phi : G \to \mathrm{GL}(V_1)$ and $\psi : G \to \mathrm{GL}(V_2)$ are considered equivalent if there exists an isomorphism or equivalence $T : V_1 \to V_2$ such that T is a linear map satisfying

$$\psi(g) \circ T = T \circ \phi(g)\,, \tag{1.10}$$

for all $g \in G$.

Now that we have a way to identify equivalent representations, we can observe a particularly useful fact; all finite dimensional representations are equivalent to matrix representations. To see this, [Sen11] notes that whenever a basis in V is chosen, if $\dim(V) = n < \infty$, then $\phi(g)$ is encoded in the following matrix:

$$\begin{pmatrix} \phi(g)_{11} & \phi(g)_{12} & \dots & \phi(g)_{1n} \\ \phi(g)_{21} & \phi(g)_{22} & \dots & \phi(g)_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \phi(g)_{n1} & \phi(g)_{n2} & \dots & \phi(g)_{nn} \end{pmatrix}. \tag{1.11}$$

This matrix essentially encodes an equivalence between a representation ϕ and a matrix group once a basis is specified. Thus we are guaranteed to have a matrix representation for any finite group. If F is the complex numbers and V is a Hilbert space, as is the case in quantum physics,

then we can further guarantee that a unitary representation of G exists, which we typically denote $\{U(g)\}_{g\in G}$.

As an aside, guaranteed unitary representations do not necessarily mean these representations will be useful for quantum computing purposes. Often, we augment these with the requirement that they are *projective* representations, which means they project into the set space of unitary operators modded out by the identity. In other words, projective unitary representations enforce the equivalence

$$U \cong \lambda U\,, \tag{1.12}$$

where $\lambda \in \mathbb{C}$. This reflects the irrelevance of global phases in quantum mechanics; we do not consider $e^{i\phi}|\psi\rangle$ to be different from $|\psi\rangle$, and so this should be reflected in our operators.

We move now to concepts that, while not immediately apparent in later chapters, underpin the intuition behind choosing certain representations over others. It may well be surmised that, in the course of examining group symmetries on quantum computers, we will take a group G and a unitary matrix representation of it to act on our space. However, there are many choices of representation that each have their own benefit. When examples of representations are proffered in future chapters, these considerations inevitably played a role in why and how these examples were formed: Is it faithful? What are the invariant subspaces? Is it irreducible—if not, what are the irreducible representations?

We have already discussed faithfulness, so let us begin with invariant subspaces. The vector space V on which the elements $\phi(g)$ act is called the representation space of ϕ. (Sometimes it is simply called the representation V, but this terminology can quickly become confusing.) If

there exists a subspace $W \subseteq V$ such that, $\forall g \in G$,

$$\phi(g)W = W\,,$$

then W is called an invariant subspace of V. If the only invariant subspaces of V are itself and 0, then the representation ϕ of G on V is said to be *irreducible* as long as $V \neq 0$. As a side note, every one-dimensional representation is an irreducible representation.

Invariant subspaces give rise to another representation—the subrepresentation. A subrepresentation $\phi|_W : G \to \mathrm{GL}(W)$ formed by the restriction of the representation ϕ to W is defined as

$$(\phi|_W)(w) \coloneqq \phi(w)\,, \tag{1.13}$$

for all elements $w \in W$. In the same manner that V is sometimes called the representation, W is occasionally referenced as the subrepresentation itself. Unfortunately, this confusing terminology cannot be abolished once established in mathematical texts, so it pays to be aware of it.

It turns out that every non-trivial representation of a finite group is either irreducible or decomposable, where decomposable means it can be written as a direct sum of two or more proper, nontrivial subrepresentations. Note that if ϕ_1 and ϕ_2 are representations of G on V_1 and V_2 respectively, then the direct sum $\phi_1 \oplus \phi_2$ is a representation of G on $V_1 \oplus V_2$, and similarly for tensor products.

Here are the fun statements for which all of this machinery has been building: every finite-dimensional representation on a Hilbert space V is the direct sum of irreducible representations. Furthermore, for unitary representations on Hilbert spaces relevant to quantum physics, all irreducible representations of G are one dimensional if and only if G is Abelian. Identifying the relevant decomposition proves greatly useful for investigations into symmetry in the Hilbert

space in question. Furthermore, the intuition used to generate examples in future chapters heavily relies on these facts.

Throughout this section, we have hopped from concept to concept haphazardly to cover the bare essentials required to comprehend the remainder of the text. To be fair, this review was prefaced to be dangerous in nature and should not be considered the ultimate authority on representation theory. Far from it, we have merely hoped to convey succinctly concepts that are not necessarily part of a standard physics curriculum but will recur within this text nonetheless.

1.3. Quantum Information and Computation Background

This work is written, first and foremost, as a thesis of work in the field of physics. As such, we take for granted a certain modicum of knowledge in any potential readers. A review must always start somewhere, and while defining the notion of a quantum mechanical state or ideas of entanglement and superposition would prove for a grand and thorough background, such explanations would necessarily extend well beyond our scope of interest. Therefore, in this section we review only so much as a typical physics student might require to acquaint themselves with topics in quantum information and computation. Nonetheless, we shall find no lack of topics to discuss.

In Section 1.3.1, we undertake the Herculean task of reviewing all relevant terms in quantum computing. We begin at a relatively elementary level by defining basic building blocks such as qubits, density matrices, and quantum channels. Additionally, we go over how to read a quantum circuit intuitively and give reference to how they can be viewed as tensor networks. From this point, we advance to relevant norms and lemmas used throughout the literature on quantum information and computing.

In Section 1.3.2, we take a moment to review a smattering of complexity theory, only so much as to contextualize later results. This will include a cursory explanation of how complexity classes contextualize computational capability, as well as introduce some relevant complexity classes. In particular, we define as background P versus NP, QIP(n), and DQC1. If all of those acronyms prove impenetrable now, fear not, for they will be contextualized in what follows.

1.3.1. Necessarily Thorough Review of Relevant Terms

1.3.1.1. Qubits, Quantum States, and Quantum Gates

To begin, we will review the primary building blocks of quantum computing. For a thorough education in quantum computing for someone totally unfamiliar with the field, the textbook by Nelson and Chuang [NC11] is a fantastic and standard reference. However, we can quickly recount some highlights here for any readers less acquainted with the material. (Quickly being a subjective term, we suggest a more experienced reader may well skip this subsection entirely.)

The natural starting point for quantum computation is the qubit or "quantum bit". Qubits are the most basic method for encoding quantum states into a form suitable for computation, analogous to the usual bit from classical computing. Consider a pure state, $|\psi\rangle$, a vector that lives in some two-dimensional Hilbert space $\mathcal{H}_A$. (We will often write $|\psi\rangle_A$ to indicate explicitly which Hilbert space our state is contained in.) Then a qubit represents this state as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \tag{1.14}$$

where $|\alpha|^2 + |\beta|^2 = 1$, and $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are referred to as the computational basis vectors. Unless otherwise indicated, we will always use the computational basis to express our quantum states.

The actual physical meaning behind the computational basis vectors is heavily dependent

on computational architecture. For instance, in an optical scenario, $|0\rangle$ could correspond to "no photons" and $|1\rangle$ to "one photon" in a clear analogy to how classical bits are often representative of a presence or lack of voltage. However, quantum computers vary greatly in their current implementations, so architecture is not considered here. Instead, it is helpful to view a qubit as a vector on the Bloch sphere, as in Figure 1.2. For this visualization, we take $\alpha = \cos\theta/2$ and $\beta = e^{i\phi}\sin\theta/2$.

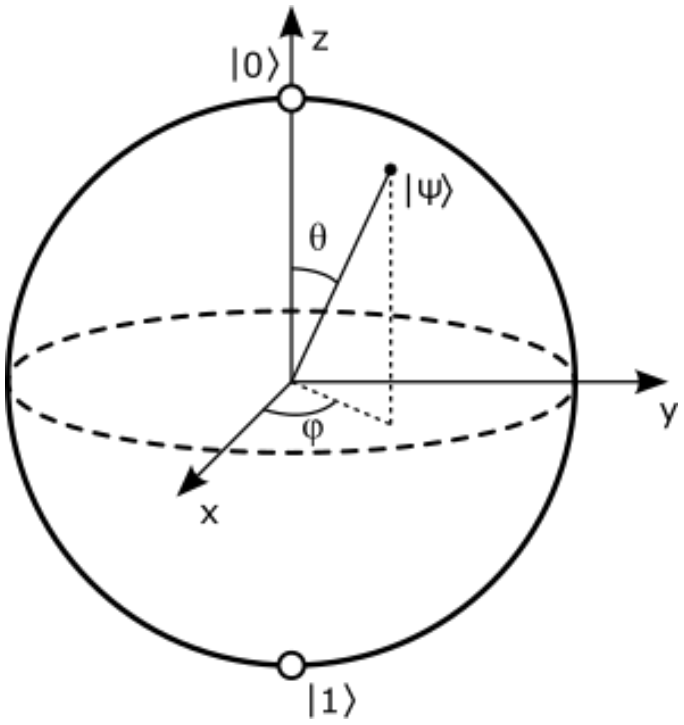


Figure 1.2. Illustration of a qubit as a vector on the Bloch Sphere. Image credit: Smite-Meister - Own work, CC BY-SA 3.0, url link

Now, given some qubit, how do we act on it to perform computations? This is achieved using unitary operators. Unitary operators can be described intuitively as "preserving probability" and are pictured as rotations on the Bloch sphere. In mathematics, this idea of preserving probability is more properly referred to as unitaries preserving the inner product. Nevertheless, we can see that acting on a single qubit by a two-by-two square unitary will result in another

properly normalized quantum state. Such unitary operators are often referred to as quantum logic gates or simply quantum gates.

Let us now take the time to define some common quantum gates. First, the Hadamard gate, normally denoted simply as H, is given by

$$H \coloneqq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.15}$$

Note each single qubit gate can be characterized by how it acts on the basis states. The Hadamard gate acts by sending $|0\rangle$ to the state $|+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ to the state $|-\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Next, the NOT gate is given by

$$X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.16}$$

As one might expect, the NOT gate sends each basis state to the other just as the classical NOT does. Why, then, do we denote it with the letter X? That is because this is exactly the Pauli-X matrix—or σ_1— that we know and love from quantum mechanics. In fact, all of the Pauli matrices are realized exactly as quantum gates for computation and adopt the moniker of "Pauli gates" to suggest this.

The next set of gates that any review of quantum computing should acknowledge are the rotation gates, of which there are three:

$$R_x(\theta) \coloneqq \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix}, \tag{1.17}$$

$$R_y(\theta) \coloneqq \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix}, \tag{1.18}$$

$$R_z(\theta) \coloneqq \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \tag{1.19}$$

Of course, there are many other gates of interest in quantum computing, infinitely so. However, as we have only finitely many pages to discuss such things, there are two more gates that should be defined for the uninitiated. These two gates are the CNOT and SWAP gates which differ from our previous examples in that they are two qubit gates.

Now, we have yet to discuss what it means to have a system of more than one qubit, but the construction is simple enough. Suppose one qubit lives in the Hilbert space $\mathcal{H}_A$ and another in the Hilbert space $\mathcal{H}_B$. Then the total state of both qubits must be contained in the tensor product Hilbert space $\mathcal{H}_{AB} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B$. However, it is not necessarily the case that the total state of the system, call it $|\psi\rangle_{AB}$, can be decomposed into a tensor product of states on each individual Hilbert space in such a manner. That is, it is not necessarily true that $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\sigma\rangle_B$ for $|\phi\rangle_A$, $|\sigma\rangle_B$ pure states. Such product states are necessarily separable and thus cannot describe entangled states on the two systems. Naturally, quantum gates are simply unitaries that act on this larger system and any further addition of qubits is accounted for in much the same way.

Now we are well-equipped to discuss the CNOT and SWAP gates. The CNOT or controlled-NOT gate acts on two qubits. One qubit is the "control", and the other is the "target". When the state of the control qubit is $|0\rangle$, nothing happens. When the state of the control qubit is $|1\rangle$, however, a NOT gate is performed on the target qubit. When combined with superpositions of states, this gate is immensely powerful. Denoting this action as a matrix is a bit tricky, because it depends on the orientation of the qubits, but supposing the control is the first qubit and the

target the second, convention gives the following matrix:

$$\text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.20}$$

Note that this is not the only controlled gate, although it is likely the most common. Any unitary gate can, in principle, have a control appended onto it.

The final gate I will be defining explicitly is the SWAP gate. This gate does exactly what it says on the label—it takes two qubits and swaps them. It is given by

$$\text{SWAP} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.21}$$

As mentioned before, this is far from an exhaustive list. There are infinitely many gates that could be called for in any given algorithm. Actually constructing these gates for use on real hardware is an issue often referred to as quantum compiling (see, e.g., [MPRP21, KLP+19, SKCC20]) which is a rich research topic all of its own. For the scope of this work, it should merely be noted that such a thing is possible.

Realizing these quantum gates on a quantum computer can be done in a number of ways, but the general approach is typically the same. Each system will have some set of "native gates" that can be performed on the physical qubits. In order to act with some arbitrary unitary gate, it must be decomposed into these elementary gates as shown in [BBC+95]. There are two main

takeaways pertinent to this discussion: all single unitary gates can be approximated by a minimal native gate set satisfying some conditions as per the results of the Solovay-Kitaev algorithm [DN06, BGT21] and all multi-qubit unitary gates and controlled-unitary gates can be continuously decomposed into only single qubit unitaries and CNOT gates [BBC+95].

At such a point, we have reviewed nearly all primary building blocks of quantum computing save one: mixed states and density matrices. Everything stated so far about qubits has been in terms of pure states—but mixed states should not be neglected. A mixed state ρ is a probabilistic mixture of pure states of the form

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \,, \tag{1.22}$$

where $|\psi_i\rangle\langle\psi_i|$ is the density matrix associated the pure state $|\psi_i\rangle$. (This can be thought of as the outer product between $|\psi\rangle$ and its dual.) In order to ensure that it describes a quantum state, ρ must be positive semi-definite $\rho \geq 0$ and have trace equal to one, $\mathrm{Tr}[\rho] = 1$. Obviously, a pure state can also be denoted this way. Thus this is the more general formalism to discuss quantum states.

So the more general quantum state is a mixed state, but we have formulated everything in terms of pure states. Why? Well, there is a result in quantum information that all mixed states can be viewed as a pure state on a higher dimensional Hilbert space that has had some part of it traced out [Wil17, Chapter 5]. This is called the purification of the mixed state. The pure state $|\psi_\rho\rangle_{AB}$ is a purification of ρ_A if

$$\rho_A = \mathrm{Tr}_B[|\psi_\rho\rangle\langle\psi_\rho|_{AB}] \,. \tag{1.23}$$

With this fact, we can confidently construct algorithms with pure states in mind and know that there will still be a way to implement them on mixed states as well.

1.3.1.2. Quantum Channels

Quantum channels are another prevalent term in quantum information. We separate this term out as, while it is certainly a prolific and important concept, it is often neglected in introductory approaches to quantum computing. Texts that focus on quantum information such as [Wil17] will have no lack of channels and thus serve as a good resource for those unfamiliar with the formalism.

Quantum channels are completely positive, trace-preserving maps that take one quantum state to another. A wise man once said, "Everything is a quantum channel." This might be overstating things a tad, but nonetheless, the insight remains somewhat true. A unitary gate is a quantum channel. The identity is a quantum channel. Teleportation is a quantum channel. The process of the environment stealing coherence from our experiments is a quantum channel. So on and so forth we continue.

Quantum channels display their usefulness best, in this author's humble opinion, in two circumstances. The first is when describing actions on density matrices. The second is for non-unitary state evolutions. The latter may grab attention more strongly than the former but its physicality is demonstrated rather simply. Suppose Alice is communicating some quantum state of d qubits to Bob when a nefarious eavesdropper intercedes. This bad actor takes all of Alice's states and replaces them with the maximally-mixed state $\pi \coloneqq \mathbb{I}/d$. This 'trace-and-replace' system may not be unitary, but it is a quantum channel. A less dramatic example is the loss of information in the form of noise introduced by the environment.

Consider for now a unitary channel $\mathcal{N}$ acting on the mixed state ρ via the unitary U. Then

we can define its action as

$$\mathcal{N} = U\rho U^\dagger = \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger \,. \tag{1.24}$$

This is a good picture to have in mind when wondering how unitary gates affect mixed states. In general, a quantum channel (often denoted $\mathcal{N}$) acts as a map

$$\mathcal{N}_{A\to B}(\cdot) : D_{\mathcal{H}_A} \to D_{\mathcal{H}_B} \tag{1.25}$$

where $D_{\mathcal{H}}$ is the space of density matrices on some Hilbert space. This concludes our toolkit of the essentials. Now, we move on to visualizations.

1.3.1.3. Reading a Quantum Circuit Diagram for Beginners

Now that we have acquainted ourselves with the relevant building blocks, we may well wish to begin constructing algorithms. To facilitate this, we turn to pictorial depictions of circuits implementable on a quantum computer. Quantum circuit diagrams are an invaluable tool that allow us to visualize sometimes immensely complex mathematics. They can be understood through the lens of tensor networks—for which Biamonte and Bergholm's "Tensor Networks in a Nutshell" [BB17] is a fantastic roadmap. We will leave all of the intricacies of tensor networks in their wise hands and cover only the very basics of quantum circuit diagram literacy.

First, we quickly run down the basic rules. Each circuit diagram is composed of wires or lines that are directly correlated to a specific Hilbert space, sometimes labelled but often not. Time progresses from left to right along these lines. Gates are usually indicated by labelled boxes that intersect these lines. Gates can be understood to act only on the Hilbert spaces that they intersect. Inputs to the circuit are kept to the left-most side and outputs to the right. A single-line wire is understood to be quantum in nature whilst double lines indicate classical communication. A dotted line, however, is usually meant to indicate that there is a space-like separation (or

at least, some sort of temporal separation).

Out of breath yet? Don't worry, because the rest of this explanation is accompanied by pictures upon which the above rules can be practiced until understood. Figure 1.3 gives a list of commonly used logic gates and their relevant symbols. In the interest of space and relative brevity, we suggest referencing the list of common gates on pages xxvii and xxviii of the tenth anniversary edition of Nielsen and Chuang [NC11] for a slightly more extensive list.

Some of the symbols in Figure 1.3 might be slightly confusing—namely, the controlled gates. We know that controlled gates have specified control and target qubits, and we need to be able to differentiate between them. A control is usually indicated by a closed circle with a vertical wire connecting it to the unitary on the target qubit. A gate can have more than one control. Additionally, gates can also be conditioned on the $|0\rangle$ state rather than the $|1\rangle$ state, and this is indicated by an open circle instead.

Let's look now at a simple example circuit. Figure 1.4 shows the Bell state circuit, so named because depending on the input, it can generate any of the four maximally-entangled Bell states. Reading the circuit from left to right, we see the input state go from $|00\rangle \rightarrow H \otimes \mathbb{I}|00\rangle \rightarrow \text{CNOT}(H \otimes \mathbb{I}|00\rangle)$. Working through this we get that the output state is given by

$$\text{CNOT}(H \otimes \mathbb{I}|00\rangle) = \text{CNOT}(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) \tag{1.26}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle\,. \tag{1.27}$$

This may seem too simple an example, but even more complicated circuits are read the same way. Just progress from left-to-right implementing each gate in its turn.

Next, let's consider a more abstract example. Figure 1.5 depicts a much more abstract circuit for us to work through. First, define U_ϕ to be the multi-qubit unitary such that $U_\phi|00\rangle =$

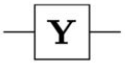
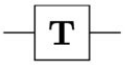
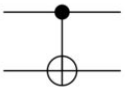
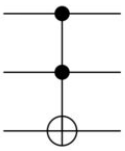
Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Figure 1.3. Commonly used quantum logic gates, their circuit diagram representations, and their typical matrix representation.

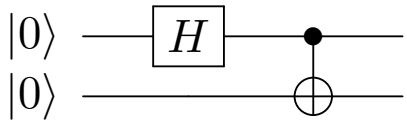


Figure 1.4. The Bell state circuit. Two qubits in the state $|00\rangle$ are acted on first by a Hadamard gate and then by a CNOT gate. The output will be the maximally-entangled state on two qubits.

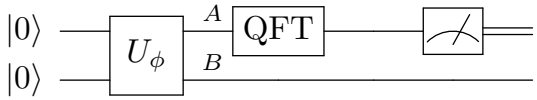


Figure 1.5. A more abstract circuit. A multiqubit gate acts on $|00\rangle$ to create the state $|\phi\rangle_{AB}$. Then a quantum Fourier transform (QFT) is performed only on the first qubit, which is then measured.

$|\phi\rangle_{AB}$ for $|\phi\rangle_{AB}$ some pure state. Then act on only on the A system with a quantum Fourier transform (QFT), and measure that system. The output of any measurement is classical, so this is denoted with doubled wires. The output of this circuit is not important, per se, but it allows us to discuss various common occurrences in circuit diagrams. For instance, the second qubit of the system is thrown out and never measured. Essentially, our measurement only considers the reduced system $\rho_A = \mathrm{Tr}_B[(\mathrm{QFT} \otimes \mathbb{I})|\phi\rangle\langle\phi|_{AB}]$. This demonstrates how mixed states are often created and denoted in circuit diagrams. Additionally, we introduce the QFT as a black-box operator that, in principle, puts a state into a superposition of some new set of basis states. (For a single qubit, the QFT is actually equal to a Hadamard, but we just wanted to have it in the circuit for discussion purposes.) For a good definition and example of the use of the QFT in quantum algorithms, see Shor's algorithm [Sho94] or review Nielsen and Chuang [NC11].

A note of caution: although typically each wire identifies a single qubit, these diagrams

aren't always so friendly. Pay attention to context clues to determine if each wire indicates a qubit or a Hilbert space. In this work, we will identify our lines with Hilbert spaces more so than qubits, but this should not lead to much confusion for a careful reader.

1.3.1.4. Advanced Terms: Norms and Important Facts

This section will consist heavily of commonly used norms and some choice lemmas that will be employed in this work. As these terms are more technical, we will simply be tersely listing them off for best reference. See [Wil17] as the source of many of these definitions unless otherwise specified.

First, we define some common norms. As a preliminary, we take the absolute value of an operator M in $\mathcal{L}(\mathcal{H}, \mathcal{H}')$ to be $|M| \coloneqq \sqrt{M^\dagger M}$.

Definition 1.3.1 ***The Trace Norm****—The trace norm, or Schatten-1 norm, $\|M\|_1$ of an operator M is defined to be*

$$\|M\|_1 \coloneqq \mathrm{Tr}[\sqrt{M^\dagger M}] = \mathrm{Tr}[|M|]\,. \tag{1.28}$$

Definition 1.3.2 ***The Hilbert–Schmidt Norm****—The Hilbert–Schmidt norm, or Schatten 2-norm, of an operator M is defined to be*

$$\|M\|_2 \coloneqq \sqrt{\mathrm{Tr}[|M|^2]}\,. \tag{1.29}$$

Definition 1.3.3 ***The Schatten p-Norm****—The Schatten p-norm for $p \geq 1$ of an operator M is defined to be*

$$\|M\|_p \coloneqq \mathrm{Tr}[|M|^p]^{1/p}\,. \tag{1.30}$$

Note that the Schatten p-Norm encompasses the first two definitions as well. Still, both are typically identified by name in quantum computing as both are common in the field.

It will be beneficial to now introduce some relevant mathematical tools. The following three (four) lemmas will be used to prove relevant results in later chapters. (It is pure coincidence that these statements are all lemmas; they come from independent works and do not build to any theorems here. As is often the case, lemmas simply tend to present amazing and useful facts.)

First, we will tackle Schur's Lemma. Indeed, there is some ambiguity here. Despite both often being referenced simply as "Schur's Lemma" there is both a concept of Schur's *first* lemma and Schur's *second* lemma. Both will be combined here into a single definition. To add to the confusion, sometimes Schur's lemma is defined in textbooks as a theorem! Will the notation abuse never cease? Below, we give both Schur's Lemma as is used often used in quantum computing [BRS07] as well as Schur's lemma as presented in representation theory [Sen11].

Now, we give the first and second lemmas as presented in [BRS07].

Theorem 1.3.1 (Schur's Lemma) *Schur's first and second lemmas are as follows:*

1. *If $T(g)$ is an irreducible representation of the group G on the Hilbert Space $\mathcal{H}$, then any operator A satisfying $T(g)AT^{\dagger}(g) = A$, $\forall g \in G$, is a multiple of the identity on $\mathcal{H}$.*
2. *If $T_1(g)$ and $T_2(g)$ are inequivalent representations of G, then $T_1(g)AT_2^{\dagger}(g) = A$, $\forall g \in G$, implies $A = 0$.*

In *Representing Finite Groups: a Semisimple Introduction*, Sengupta calls Schur's lemma "the Incredible Hulk of representation theory"—certainly, a ringing endorsement. In honor of this, we will restate Schur's lemma and further give the proof of it as given in [Sen11]. After all, Schur's lemma [Sch05] was originally a result of representation theory itself, so proving it in this context is perhaps the best use of the tools given in Section 1.2.2.

Theorem 1.3.2 (Schur's Lemma (Again)) *A morphism between irreducible representations is either an isomorphism or 0. That is, if ϕ_1 and ϕ_2 are irreducible representations of a group G on vector spaces V_1 and V_2, over an arbitrary field F, and is $T : V_1 \to V_2$ is a linear map where*

$\forall g \in G$,

$$T\phi_1(g) = \phi_2(g)T\,, \tag{1.31}$$

then T is either invertible or 0.

If ϕ is an irreducible representation of a group G on a finite-dimensional vector space V over an algebraically closed field F and $S : V \to V$ is a linear map where $\forall g \in G$,

$$S\phi(g) = \phi(g)S\,, \tag{1.32}$$

then $S = c\mathbb{I}$ for some scalar $c \in F$.

Proof. Suppose ϕ_1, ϕ_2, and T are as given above. From (1.31), we can determine that the kernel of T, $\ker(T)$, is invariant under the action of the group G. Since ϕ_1 is irreducible, and thus the only invariant subspaces are 0 and V, it follows that $\ker(T)$ is either 0 or V itself. Then if $T \neq 0$, it must be injective. Similarly, the image of T, $\mathrm{Im}(T) \subset V_2$ is also invariant under the action of the group, and thus if $T \neq 0$, it must be surjective. Therefore, either $T = 0$ or T is an isomorphism.

For the second part, suppose F is algebraically closed. (This is the case for the complex numbers $\mathbb{C}$.) Further suppose that V and S are as stated, and S is an intertwining operator from the irreducible representation ϕ on V to itself. Note that $S - c\mathbb{I} \in \mathrm{GL}_n(F)$ is not invertible, as

$$\det(S - \lambda\mathbb{I}) = 0$$

has a solution for $\lambda = c \in F$. Observe that (1.32) holds even if when replacing S with $S - c\mathbb{I}$. Thus, by (1.31), $S - c\mathbb{I} = 0$. ■

By inspection, this second statement of Schur's lemma encapsulated the first. This may well be expected, as the use case in quantum computing is much more limited. Suffice to say, this lemma-come-theorem strikes heavy significance in any application where representations of groups occur.

Our heavy hitter out of the way, we give two more lemmas simply because they will be used, and it is always helpful to have such things explained in house. The gentle measurement and gentle operator lemmas found in [Dav69, Win99, ON07] are recreated below.

Lemma 1.3.3 (Gentle Measurement Lemma) *Given a density operator ρ and a measurement operator Λ with $0 \leq \Lambda \leq \mathbb{I}$, suppose that Λ has a high probability of detecting the state ρ such that*

$$\mathrm{Tr}[\Lambda\rho] \geq 1 - \epsilon\,, \tag{1.33}$$

where $\epsilon \in [0, 1]$. (The probability is considered high if ϵ is close to zero.) Then the post-measurement state

$$\rho' \equiv \frac{\sqrt{\Lambda}\rho\sqrt{\Lambda}}{\mathrm{Tr}[\Lambda\rho]}\,, \tag{1.34}$$

is $2\sqrt{\epsilon}$-close to the original state ρ in trace distance. That is,

$$\|\rho - \rho'\|_1 \leq 2\sqrt{\epsilon}\,. \tag{1.35}$$

Thus, the measurement does not disturb the state ρ much if ϵ is small.

Lemma 1.3.4 (Gentle Operator Lemma) *Given a density operator ρ and a measurement operator Λ with $0 \leq \Lambda \leq \mathbb{I}$, suppose that Λ has a high probability of detecting the state ρ such that*

$$\mathrm{Tr}[\Lambda\rho] \geq 1 - \epsilon\,, \tag{1.36}$$

where $\epsilon \in [0, 1]$. (The probability is considered high if ϵ is close to zero.) Then $\sqrt{\Lambda}\rho\sqrt{\Lambda}$ is $2\sqrt{\epsilon}$-close to the original state in trace distance. That is,

$$\left\|\rho - \sqrt{\Lambda}\rho\sqrt{\Lambda}\right\|_1 \leq 2\sqrt{\epsilon}\,. \tag{1.37}$$

Proofs of both of these lemmas can be found in Chapter 1 of [Wil17] alongside other related quantities.

1.3.1.5. Parting Words

Thus we conclude our review of terms in quantum information theory, including both elementary concepts and more advanced ones. Readers fully unfamiliar with the topics introduced here are encouraged not to rely on this work alone, but instead to investigate any of the references given. With such context out of the way, the way forward holds more interesting and niche information that would be of greater interest to more advanced audiences. The next subsection, for instance, introduces quantum complexity theory, which should rouse anyone bored from the material reviewed so far.

1.3.2. Complexity Theory but Only So Far as We are Concerned

The aim of this section is to acquaint any unwary reader with the smattering of complexity theory terms that will inevitably make themselves known in this work. For an enjoyable sojourn on quantum computing that relates the topic to complexity theory, we proffer Scott Aaronson's "Quantum Computing Since Democritus" [Aar13]. Do not think, however, that upon completing this section alone a reader would be fit to debate hot topics in complexity theory with Aaronson himself. We cover only the classes of P, NP, QIP(n), and DQC1, and even then we do so in a rather cursory manner.

Generally, complexity classes concern themselves with one primary question: "As the problem grows larger in scale, how many more resources does the solution require?" These can be either time or space resources, but generally speaking most limit themselves to time. Space rarely proves to be the limiting factor. As such, many complexity classes define themselves pri-

marily with time taken to solve some problem. The class P is a prime example of this: it is the class of problems that are solvable in polynomial time on a classical computer.

We believe—indeed, the field in general believes—that any quantum computer worth its salt will be able to solve problems in the class P efficiently. Why? Because problems in P are already efficiently solvable on classical computers, and few people interest themselves in making a worse machine than we already have. The interesting question comes about when we discuss P versus NP.

Here is the rub with complexity classes–their distinctions are rather fuzzy. Indeed, disguising if P is equal to NP is one of the Millennium Prize Problems [CJW06], so it must be a difficult feat. For our purposes, we will assume P $\neq$ NP in the grand tradition of many complexity theorists before us. But what is NP? Again, before defining these terms, we will meander to a few preliminary concepts first.

Every computational class has a set of problems that define a class. That is, every problem in the class can be mapped to these problems in polynomial steps. These are referred to as being complete, e.g., NP-Complete. Often, decision problems hold this seat. A decision problem is an algorithm that returns 'yes' if some verifiable question is true and 'no' otherwise. NP is short for "nondeterministic polynomial time", and it is the class of decision problems that a probabilistic classical computer could solve in polynomial time. As that is rather esoteric and we would rather not delve too deeply into the implications of probabilistic Turing machines, we will adopt a more colloquial definition of NP. NP is often thought of as the class of decision problems whose solutions are "easy to check, hard to find." It is a widespread belief that NP problems are difficult for classical computers to solve efficiently.

We have introduced this concept of completeness in our definition so that we may make

some rather tenuous statements about relative hardness of algorithms. (Complexity theory is always rather tenuous as it is very hard to prove that one class of problems is definitively more difficult than another.) The current attitude of the quantum computing community is that quantum computers should also be able to solve some problems in NP efficiently. NP-Complete or NP-Hard problems are not generally included in this number. As evidence for this claim, most present Shor's algorithm [Sho94] which allows quantum computers to factor large numbers in polynomial time on a quantum computer. Factoring is classically an NP problem—that is, there is no currently known classical algorithm to efficiently factor large numbers—but not NP-Complete. Thus, this result indicates that there exists some sweet spot of computational problems that are only efficient on quantum computers.

Now that we have established that there exists a class of easy problems (P), a class of difficult problems (NP-Complete), and a class of interesting problems (NP), we can restrict ourselves to definitions of quantum complexity classes. There are two which we will need for further reading: DQC1 and QIP(n).

1.3.2.1. DQC1

DQC1 stands for "deterministic quantum computation with one clean qubit", or "one clean qubit" colloquially. The one clean qubit problem models systems with one pure state qubit and the rest of the system consisting of maximally-mixed qubits at the input. As one clean qubit is complete for DQC1, is can be considered emblematic of the class. In what follows, we review the definition of this class [KL98, SJ08]. An important note on the class, however, is that its problems are deemed classically intractable, thus making it a complexity class of interest in quantum computing.

Suppose we have n qubits. The basic model involves preparing one qubit in a pure state $|0\rangle\langle 0|$ and all other qubits in the maximally mixed state $\pi := \mathbb{I}/d$ where $d := 2^n$. Further suppose we have a quantum circuit generating a unitary U and perform this on all of the qubits. Then the first qubit is measured in the computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. The algorithm accepts if the outcome $|1\rangle\langle 1|$ occurs. The problem of estimating the acceptance probability $\mathrm{Tr}\left[(|1\rangle\langle 1| \otimes I)U(|0\rangle\langle 0| \otimes I/d)U^\dagger\right]$ to within additive error is a DQC1-complete problem by definition.

An insight of [SJ08, Section 1] is that the problem of estimating $\mathrm{Re}[\mathrm{Tr}[U]]/d$ to within additive error, where U is the unitary realized by a quantum circuit acting on n qubits and consisting of polynomially many gates, is a DQC1-complete problem. This means that the problem can be solved within the computational model mentioned above, and it is also just as hard as every other problem that can be solved in the model. Thus, this problem of normalized trace estimation characterizes the class DQC1. Another key observation of [SJ08, Section 1] is that the complexity class DQC1 does not change if there are a constant or even logarithmic number of pure qubits, where here we mean logarithmic in n.

1.3.2.2. QIP(n)

In classical computational complexity theory, there is a concept of something called a "Merlin-Arthur Proof". This class proffers a decision problem wherein an all-powerful prover with infinite computational resources interacts with a practically-limited verifier. This prover is analogized as the wizard Merlin and the verifier as the human king Arthur, who must take the information Merlin provides him and make a final decision.

If this all sounds like fantasy, let us recontextualize. In this formalism, the verifier must

accurately decide whether or not some input satisfies a decision problem. The prover acts as an oracle who wishes to maximize the acceptance probability of the algorithm. The prover is not limited by time or space but is limited by the laws of nature. Colloquially, if a solution exists, then the prover will find it. If not, the prover will attempt to fool the verifier by choosing an input as close to the acceptance condition as possible. When all parties involved are quantum mechanical (meaning, for our purposes, that the verifier has a resource-limited quantum computer and the all-powerful wizard has an unlimited quantum computer) then this situation describes a quantum interactive proof (QIP) [Wat09, VW16].

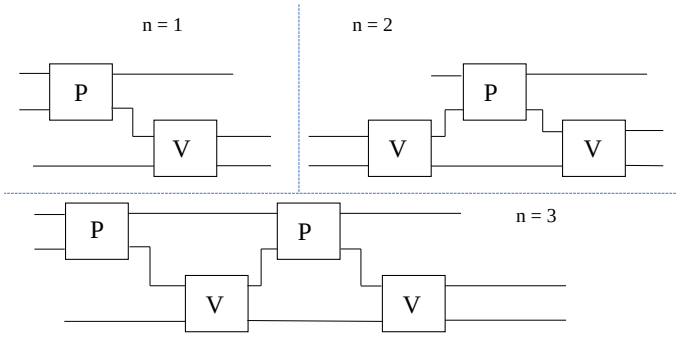


Figure 1.6. A cartoon demonstrating the different numbers of messages exchanged between a prover system P and a verifier system V. This figure shows the basic form of QIP(n) algorithms for n=1, n=2, and n=3.

These quantum interactive proofs are characterized by a parameter n, which refers to the number of messages exchanged between the verifier and the prover, QIP(n). A system in which no messages are exchanged, QIP(0), is considered to be efficient on a quantum computer (equivalent to BQP, the so-called quantum analogy of P). If the prover acts as an oracle sending only one message, that is QIP(1), so on and so forth. A result of Kitaev and Watrous [KW00] showed that the upper limit is three messages; any exchange beyond that reduces to QIP(3). This exchange of messages is shown pictorially in Figure 1.6.

1.4. Defining Notions of Symmetry

We may now finally progress from background to original contributions rather than review. The primary focus of this thesis is evaluating symmetry of various quantities of interest in quantum mechanics. However, the concept of symmetry can be ambiguous and abstract. Defining what symmetries we plan to encounter is thus a necessary preliminary, and we have amassed within this work quite a menagerie. In Section 1.4.1, we give a series of four definitions of symmetries of quantum states originally presented in [LRW21], the contents of which will be utilized in Chapters 3 and 4. In Section 1.4.2, we review the definitions of covariance of a quantum channel and Hamiltonian symmetries, which will be paramount in Chapters 2 and 3. While the latter section is well-studied in the literature, the former should be considered minutely as part of the research contributions collected herein.

For further reading on symmetry in quantum information, we point to various resources which have influenced our own work and education. The work of Iman Marvian, particularly his PhD thesis [Mar12], gives a fantastic picture of the topic. Additionally, Aram Harrow's "Church of the Symmetric Subspace" [Har13] provides a great starting place and overview of the topic. Both of these works we cite in later chapters where their influence has made its mark, but we provide the citations here in a continuous effort to give additional reference texts throughout the introduction.

1.4.1. Various Symmetries for Quantum States

We introduce the notions of G-symmetric extendibility and G-Bose symmetric extendibility of a state, as generalizations of the notions of G-symmetry [MS13, Section 2] and extendibility [Wer89, DPS02, DPS04]. Later on in Chapter 3, we devise quantum algorithms to

test for these symmetries.

Let ρ_S be a quantum state of system S with corresponding Hilbert space $\mathcal{H}_S$. Let G be a finite group, and let $U_{RS}(g)$ be a unitary representation [MS13, Section 2] of the group element $g \in G$, where R indicates another Hilbert space, so that $U_{RS}(g)$ acts on the tensor-product Hilbert space $\mathcal{H}_R \otimes \mathcal{H}_S$. Let Π^G_{RS} denote the following projection operator:

$$\Pi^G_{RS} \coloneqq \frac{1}{|G|} \sum_{g \in G} U_{RS}(g). \tag{1.38}$$

Observe that

$$\Pi^G_{RS} = U_{RS}(g)\Pi^G_{RS} = \Pi^G_{RS} U_{RS}(g), \tag{1.39}$$

for all $g \in G$.

We now define G-symmetric-extendible and G-Bose-symmetric-extendible states.

Definition 1.4.1 (G-symmetric-extendible) *A state ρ_S is G-symmetric-extendible if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{1.40}$$

2. *the state ω_{RS} is G-invariant, in the sense that*

$$\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \qquad \forall g \in G. \tag{1.41}$$

Definition 1.4.2 (G-Bose-symmetric-extendible) *A state ρ_S is G-Bose-symmetric-extendible (G-BSE) if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_R, \tag{1.42}$$

2. *the state ω_{RS} satisfies*

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}. \tag{1.43}$$

Note that the condition in (3.4) is equivalent to $\omega_{RS} = \Pi^{G}_{RS}\omega_{RS}$ or $\omega_{RS} = U_{RS}(g)\omega_{RS}$ for all $g \in G$. Observe also that ρ_S is G-symmetric-extendible if it is G-Bose-symmetric-extendible, but the opposite implication does not necessarily hold.

We have made no assumptions about the unitary representation used thus far. It is important to mention the case of projective unitary representations, due to their physical relevance in the case of symmetries of density operators. See, e.g., Eqs. (1.2) and (1.3) of [Mar12] for a definition of a projective unitary representation. Restricting to projective unitary representations helps in avoiding trivial representations, and when considering symmetries of density operators, they necessarily arise. Furthermore, when considering implementations of groups in later chapters, we limit ourselves to faithful representations of the group. In principle, neither faithfulness nor a projective representation are required unless stated otherwise. (The choice of representation will matter when considering the symmetry of a state, for instance; however, in the manner of existing literature, we describe all symmetries with respect to the group and omit the reliance on the representation in notation.)

Although the concepts of G-symmetric extendibility and G-Bose-symmetric extendibility, in Definitions 1.4.1 and 1.4.2 respectively, are generally different, we can relate them by purifying a G-symmetric-extendible state to a larger Hilbert space. The ability to do so plays a critical role in the algorithms proposed in Chapter 3.

Theorem 1.4.1 *A state ρ_S is G-symmetric-extendible if and only if there exists a purification $\psi^{\rho}_{RS\hat{R}\hat{S}}$ of ρ_S satisfying the following:*

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = \left(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)\right) |\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} \quad \forall g \in G, \tag{1.44}$$

where the overbar denotes the complex conjugate. The condition in (1.44) *is equivalent to*

$$|\psi^\rho\rangle_{RS\hat{R}\hat{S}} = \Pi^G_{RS\hat{R}\hat{S}}|\psi^\rho\rangle_{RS\hat{R}\hat{S}}, \tag{1.45}$$

where

$$\Pi^G_{RS\hat{R}\hat{S}} := \frac{1}{|G|}\sum_{g\in G} U_{RS}(g)\otimes \overline{U}_{\hat{R}\hat{S}}(g). \tag{1.46}$$

Proof. We give the proof for completeness, and we note here that it is very close to the proof of [CKMR07, Lemma II.5] (see also [KW20, Lemma 3.6]).

We begin with the forward implication. Suppose that ρ_S is G-symmetric extendible. By definition, this means that there exists a state ω_{RS} satisfying (3.1) and (3.2). Suppose that ω_{RS} has the following spectral decomposition:

$$\omega_{RS} = \sum_k \lambda_k \Pi^k_{RS}, \tag{1.47}$$

where λ_k is an eigenvalue and Π^k_{RS} is a spectral projection. We can write Π^k_{RS} as

$$\Pi^k_{RS} = \sum_\ell |\phi^k_\ell\rangle\langle\phi^k_\ell|_{RS}, \tag{1.48}$$

where $\{|\phi^k_\ell\rangle_{RS}\}_\ell$ is an orthonormal basis. Now define

$$|\Gamma^k\rangle_{RS\hat{R}\hat{S}} := \sum_\ell |\phi^k_\ell\rangle_{RS}\otimes \overline{|\phi^k_\ell\rangle}_{\hat{R}\hat{S}}, \tag{1.49}$$

$$|\psi^\rho\rangle_{RS\hat{R}\hat{S}} := \sum_k \sqrt{\lambda_k}|\Gamma^k\rangle_{RS\hat{R}\hat{S}}, \tag{1.50}$$

where $\overline{|\phi^k_\ell\rangle}_{\hat{R}\hat{S}}$ is the complex conjugate of $|\phi^k_\ell\rangle_{RS}$ with respect to the standard basis. Observe that $|\psi^\rho\rangle\langle\psi^\rho|_{RS\hat{R}\hat{S}}$ is a purification of ω_{RS}. Now let us establish (1.44). Given that ω_{RS} satisfies (3.2), it follows that

$$U_{RS}(g)^\dagger \omega_{RS} U_{RS}(g)|\phi^k_\ell\rangle_{RS} = \omega_{RS}|\phi^k_\ell\rangle_{RS} = \lambda_k|\phi^k_\ell\rangle_{RS}, \tag{1.51}$$

for all k, ℓ, and g. Left multiplying by $U_{RS}(g)$ implies that

$$\omega_{RS} U_{RS}(g) |\phi_\ell^k\rangle_{RS} = \lambda_k U_{RS}(g) |\phi_\ell^k\rangle_{RS}, \tag{1.52}$$

so that $U_{RS}(g)|\phi_\ell^k\rangle_{RS}$ is an eigenvector of ω_{RS} with eigenvalue λ_k. We conclude that the k-th eigenspace corresponding to eigenvalue λ_k is invariant under the action of $U_{RS}(g)$ because $|\phi_\ell^k\rangle_{RS}$ and $U_{RS}(g)|\phi_\ell^k\rangle_{RS}$ are eigenvectors of ω_{RS} with eigenvalue λ_k. This implies that the restriction of $U_{RS}(g)$ to the kth eigenspace is equivalent to a unitary $U_{RS}^k(g)$. Then it follows that

$$\begin{aligned} &(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))|\Gamma^k\rangle_{RS\hat{R}\hat{S}} \\ &= (U_{RS}^k(g) \otimes \overline{U}_{\hat{R}\hat{S}}^k(g))|\Gamma^k\rangle_{RS\hat{R}\hat{S}} \qquad (1.53) \\ &= |\Gamma^k\rangle_{RS\hat{R}\hat{S}}, \qquad (1.54) \end{aligned}$$

for all $g \in G$. The first equality follows from the fact stated just above. The second equality follows from the invariance of the maximally entangled vector $|\Gamma^k\rangle_{RS\hat{R}\hat{S}}$ under unitaries of the form $V \otimes \overline{V}$. Thus, it follows by linearity that

$$|\psi^\rho\rangle_{RS\hat{R}\hat{S}} = (U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))|\psi^\rho\rangle_{RS\hat{R}\hat{S}}, \tag{1.55}$$

for all $g \in G$, which is the statement of (1.44).

Let us now consider the opposite implication; suppose that $\psi^\rho_{RS\hat{R}\hat{S}}$ is a purification of ρ_S and $\psi^\rho_{RS\hat{R}\hat{S}}$ satisfies (1.44). Set

$$\omega_{RS} = \mathrm{Tr}_{\hat{R}\hat{S}}[\psi^\rho_{RS\hat{R}\hat{S}}]. \tag{1.56}$$

Then ω_{RS} is an extension of ρ_S. Furthermore, employing the shorthand $U_{RS} \equiv U_{RS}(g)$ and $\overline{U}_{\hat{R}\hat{S}} \equiv \overline{U}_{\hat{R}\hat{S}}(g)$, we find that $\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger$ for all $g \in G$ because

$$\omega_{RS} = \mathrm{Tr}_{\hat{R}\hat{S}}[\psi^\rho_{RS\hat{R}\hat{S}}]$$

$$= \operatorname{Tr}_{\hat{R}\hat{S}}[(U_{RS} \otimes \overline{U}_{\hat{R}\hat{S}})\psi^{\rho}_{RS\hat{R}\hat{S}}(U_{RS} \otimes \overline{U}_{\hat{R}\hat{S}})^{\dagger}] \tag{1.57}$$

$$= U_{RS}(g) \operatorname{Tr}_{\hat{R}\hat{S}}[\overline{U}_{\hat{R}\hat{S}}(g)\psi^{\rho}_{RS\hat{R}\hat{S}}\overline{U}_{\hat{R}\hat{S}}(g)^{\dagger}]U_{RS}(g)^{\dagger} \tag{1.58}$$

$$= U_{RS}(g) \operatorname{Tr}_{\hat{R}\hat{S}}[\overline{U}_{\hat{R}\hat{S}}(g)^{\dagger}\overline{U}_{\hat{R}\hat{S}}(g)\psi^{\rho}_{RS\hat{R}\hat{S}}]U_{RS}(g)^{\dagger} \tag{1.59}$$

$$= U_{RS}(g) \operatorname{Tr}_{\hat{R}\hat{S}}[\psi^{\rho}_{RS\hat{R}\hat{S}}]U_{RS}(g)^{\dagger} \tag{1.60}$$

$$= U_{RS}(g)\omega_{RS}U_{RS}(g)^{\dagger}. \tag{1.61}$$

Thus, it follows that ρ_S is G-symmetric extendible.

We now justify the equivalence of (1.44) and (1.45). Using the result in (1.55), observe that

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = \frac{1}{|G|}\sum_{g\in G}(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}}, \tag{1.62}$$

which simplifies to (1.45) by substituting in (1.46). Now starting with (1.46), let us apply the property in (1.39), and we have that

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = (U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))\Pi^{G}_{RS\hat{R}\hat{S}}|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}}, \tag{1.63}$$

for all $g \in G$. This reduces to (1.44) by applying (1.45). ■

Now, both of these definitions of symmetry contain a condition of extendibility, but that criterion may not always be necessary for particular applications. In those cases, simply let the extension be trivial to regain a related, simpler notion of symmetry. We present those cases here as examples.

Example 1.4.1 (G-symmetric) *Let G be a group with projective unitary representation $\{U_S(g)\}_{g\in G}$, and let ρ_S be a quantum state of system S. A state ρ_S is symmetric with respect to G [MS13, MS14] if*

$$\rho_S = U_S(g)\rho_S U_S(g)^{\dagger} \quad \forall g \in G. \tag{1.64}$$

Thus, the established notion of symmetry of a state ρ_S with respect to a group G is a special case of G-symmetric extendibility in which the system R is trivial.

Example 1.4.2 (G-Bose-symmetric) *A state ρ_S is Bose-symmetric with respect to G if*

$$\rho_S = U_S(g)\rho_S \quad \forall g \in G, \tag{1.65}$$

which is equivalent to the condition

$$\rho_S = \Pi_S^G \rho_S \Pi_S^G, \tag{1.66}$$

where the projector Π_S^G is defined as

$$\Pi_S^G \coloneqq \frac{1}{|G|} \sum_{g \in G} U_S(g). \tag{1.67}$$

Thus, the established notion of Bose symmetry of a state ρ_S with respect to a group G is a special case of G-Bose symmetric extendibility in which the system R is trivial.

Thus we have defined the notions of G-symmetric extendibility, G-Bose-symmetric extendibility, and the related notions of G-symmetry and G-Bose symmetry. These concepts will be revisited in Chapter 3 and are described in great detail in [LRW21].

1.4.2. Hamiltonian Symmetry and Covariance of a Quantum Channel

Finally, we arrive at Hamiltonian symmetry and covariance of quantum channels. The former will be integral to the discussions in Chapter 2 and the latter both in Chapters 2 and 3. We will begin by reviewing very briefly the notion of Hamiltonian symmetry and then spend much more time recalling the definition of covariance symmetry.

In quantum mechanics, a Hamiltonian H is symmetric with respect to an operator O if it commutes with H:

$$[O, H] = 0\,.$$

We say that H commutes with a unitary representation of a group G, $\{U(g)\}_{g\in G}$, if

$$[H, U(g)] = 0 \qquad \forall g \in G\,. \tag{1.68}$$

Given this basic concept of Hamiltonian symmetry, let us move on to the covariance symmetry of quantum channels. Let G be a group with projective unitary representations $\{U(g)_A\}_{g\in G}$ and $\{V(g)_B\}_{g\in G}$ on the A and B subsystems respectively. Then the channel $\mathcal{N}_{A\to B}$ is covariant if the following G-covariance symmetry condition holds

$$\mathcal{N}_{A\to B} \circ \mathcal{U}_A(g) = \mathcal{V}_B(g) \circ \mathcal{N}_{A\to B} \qquad \forall g \in G, \tag{1.69}$$

where the unitary channels $\mathcal{U}_A(g)$ and $\mathcal{V}_B(g)$ are respectively defined from $U_A(g)$ and $V_B(g)$ as

$$\mathcal{U}_A(g)(\omega_A) \coloneqq U_A(g)\omega_A U_A(g)^\dagger, \tag{1.70}$$

$$\mathcal{V}_B(g)(\tau_B) \coloneqq V_B(g)\tau_B V_B(g)^\dagger. \tag{1.71}$$

Furthermore, a channel is covariant in the sense above if and only if its Choi state is invariant in the following sense [CDP09, Eq. (59)]:

$$\Phi^{\mathcal{N}}_{RB} = (\overline{\mathcal{U}}_R(g) \otimes \mathcal{V}_B(g))(\Phi^{\mathcal{N}}_{RB}) \quad \forall g \in G, \tag{1.72}$$

where

$$\overline{\mathcal{U}}_R(g)(\omega_R) \coloneqq \overline{U}_R(g)\omega_R U_R(g)^T. \tag{1.73}$$

Note that the Choi state of the channel $\mathcal{N}_{A\to B}$, denoted $\Phi^{\mathcal{N}}_{RB}$, is defined to be

$$\Phi^{\mathcal{N}}_{RB} \coloneqq \mathcal{N}_{A\to B}(\Phi_{RA}), \tag{1.74}$$

$$\Phi_{RA} \coloneqq \frac{1}{|A|}\sum_{i,j} |i\rangle\langle j|_R \otimes |i\rangle\langle j|_A. \tag{1.75}$$

We can note a different condition by specifying a projector over the space of states symmetric with respect to group G [Har13]. Denote the projector of this group as

$$\Pi^G = \frac{1}{|G|} \sum_{g \in G} \overline{U}_R(g) \otimes U_B(g). \tag{1.76}$$

Then the Choi state is symmetric with respect to G if

$$\Phi^{\mathcal{N}}_{RB} = \Pi^G \Phi^{\mathcal{N}}_{RB}. \tag{1.77}$$

The above definition is a stronger condition of symmetry; thus, if the Choi state obeys (1.77) then (1.72) follows.

If a channel describing Hamiltonian dynamics exhibits G-covariance symmetry, then the underlying Hamiltonian is symmetric with respect to G. This will become paramount to the results in Chapter 2, but can be verified easily.

1.5. Conclusion

With this, we have defined all of the relevant background knowledge necessary to comprehend the work beyond a basic background in physics. We have equipped ourselves with some meager knowledge of group theory and representation theory, and we have a handy guide for the formalities of quantum computing. Furthermore, we have established the utmost important concept of symmetry, upon which all the work in this thesis is based. Hopefully, this chapter will serve as a lighthouse to guide anyone unfamiliar with these concepts through the results we wish to communicate in later chapters.

Chapter 2. Hamiltonian Symmetry

2.1. Introduction

Symmetry is a key facet of nature that plays a fundamental role in physics [Gro96, FR96], and for many physics students this is first stressed via Noether's theorem [Noe18], which states that symmetries in Hamiltonians correspond with conserved quantities in the related physical systems. In much the same manner, we too begin with a discussion of symmetry tests for a Hamilitonian. Hamiltonian symmetries have a number of immediate and profound effects. For instance, the symmetries of a Hamiltonian indicate the presence of superselection rules [AS67, WWW52]. In quantum computing and information, symmetry can indicate the presence of resources or lack thereof [Mar12], and it can be useful for improving the performance of variational quantum algorithms [SSY20, GZB+20, BGA+21, LXYB22]. Identification of symmetries can simplify calculations by eliminating degrees of freedom associated with conserved quantities—this is at the heart of Noether's theorem. This makes symmetries, and especially Hamiltonian symmetries, extraordinarily useful in the context of physics.

In comparison, quantum computing is a significantly younger field of study. First introduced as a quantum-mechanical model of a Turing machine [Ben80], the intrigue of quantum computers lies in their potential to outperform their classical counterparts. The most obvious asset of quantum computers is the inherent physics behind the calculation, utilizing non-classical features such as superposition and entanglement. Classical simulations of quantum systems quickly become intractable as the size of the Hilbert space grows, needing exponentially many bits to explore the state space which multiple qubits naturally occupy. Intuitively, the

Sections 2.2-2.6 of this chapter were previously published in *Physical Review Letters* in "Quantum Algorithms for Testing Hamiltonian Symmetry" by Margarite L. LaBorde and Mark M. Wilde, Phys. Rev. Lett. 129, 160503.

quantum mechanical nature of these computers allows for simulations of quantum systems in a forthright way (see [CMN+18] and references therein).

A pertinent example of this, Hamiltonian simulation [Llo96], garners high interest in the field [BR12, Som16, CMP18, CBC21]. Much work has been done to understand how to simulate these dynamics on quantum hardware such that they can be efficiently realized; however, to the best of our knowledge, before our work in [LW22], there were no algorithms that test Hamiltonian symmetries on a quantum computer, even though simulating Hamiltonians in this manner and identifying the symmetries of said Hamiltonian are both deemed to be of utmost importance.

In this chapter, we give quantum algorithms to test whether a Hamiltonian evolution is symmetric with respect to the action of a discrete, finite group. This property is often referred to as the covariance [CDP09] of the evolution. If the evolution is symmetric, then the Hamiltonian itself is also symmetric, and so our algorithms thus test for Hamiltonian symmetry. Furthermore, we show that for a Hamiltonian with an efficiently realizable unitary evolution and a group with an efficiently realizable unitary representation, we can perform our first test efficiently on a quantum computer [CBC21]. "Efficiently" here means that our algorithm is in the complexity class DQC-1. We give a second quantum algorithm for testing Hamiltonian symmetry which can be implemented by means of a variational approach [CAB+20, BCLK+21]. The acceptance probabilities of both algorithms can be elegantly expressed in terms of familiar expressions of Hamiltonian symmetry. We further consider physically relevant examples demonstrating the capabilities of our algorithms.

The consequences of such results extend throughout many areas of physics. Any study of a physical Hamiltonian can benefit from finding its symmetries, and our algorithms allow for an efficient check for these symmetries. With this knowledge, dynamics can be simplified by ex-

cluding symmetry-breaking transitions, calculations can be reduced into fewer dimensions, and intuition can be gained about the system of interest. Our first algorithm also scales well, meaning that systems too large and cumbersome to be studied by hand or classical computation can instead be investigated in a practical time scale. Our quantum tests offer meaningful insight into physical dynamics.

In Section 2.2, we begin by describing covariance symmetry of a unitary quantum channel—of which Hamiltonian dynamics are a special case. This section revisits the notion of symmetry given in Section 1.4.2 in a more abstract, conversational frame. This description will directly motivate the algorithms proffered. Next, in Section 2.3 we briefly review how Hamiltonian dynamics can be simulated on a quantum computer through the Trotter–Suzuki approximation [Suz76]. We describe the assumptions of Trotterization and the resultant evolution approximation. Section 2.4 presents our main result of this chapter. We give a quantum algorithm to test the covariance symmetry of Hamiltonian dynamics, and we show that this algorithm is DCQ1-complete. Section 2.5 gives the derivation of the acceptance probability for our algorithm. The result shows demonstrable reliance on the quantum mechanical notion of Hamiltonian symmetry. Following this, in Section 2.6, we further give another, related algorithm achievable with the aid of a quantum variational approach. This related test assumes a maximization over all input states, and thus is less efficient, yet realizes an interesting bound on Hamiltonian symmetry via the commutator norm and the twirl. Finally, in Section 2.7 we demonstrate examples of symmetry tests on currently available quantum computers. We consider the transverse-field Ising model, the Heisenberg XY model [LSM61], and the weakly J-coupled NMR Hamiltonian [vdV96], whose evolution we test for various symmetry cases.

2.2. Covariance of a Quantum Channel

Before describing the symmetries of a Hamiltonian, we first recall the notion of covariance symmetry of a quantum channel [Hol02]. Quantum channels transform one quantum state to another and are described by completely positive, trace-preserving maps. They serve as a convenient mathematical description of the dynamics induced by a Hamiltonian. The symmetries of a Hamiltonian naturally correspond to a covariance symmetry in the channel given by its evolution, and we exploit this in our algorithms.

As the mathematical description has been given in greater detail previously, let us instead take a high-level, intuitive review of the matter. (We recall the established concept of covariance symmetry in more detail in Chapter 1 in Section 1.4.2.) Suppose there is a channel sending Alice's quantum system to Bob's. For simplicity, we consider their systems to have the same dimension, though this is not required in general. Further suppose that we wish to determine if this channel is symmetric with respect to some finite, discrete group G, which has a projective unitary representation (as usual, denoted $\{U(g)\}_{g\in G}$). Then the channel is covariant if Alice acting with her representation $U(g)$ before sending the system through the channel is completely equivalent to Bob acting on his system with his representation of g after the state has been sent through the channel. In this sense, the channel commutes with the action of the group.

One method for testing this property given some channel involves using its Choi state, formally defined in (1.74). The Choi state is generated by sending one half of a maximally-entangled state through the channel, which we now assume to be unitary. Given the same group and its unitary representation, we define a projector

$$\Pi^G := \frac{1}{|G|} \sum_{g\in G} \overline{U}_R(g) \otimes U_B(g), \tag{2.1}$$

onto the space of states of a composite system RB that are symmetric with respect to the group G, where the overline denotes complex conjugation. (Here we use R to refer to a reference system and B to refer to Bob's system after the channel, a notion we use throughout.) The Choi state of the channel is equal to its projection onto the symmetric space if and only if the Choi state is symmetric with respect to G, given unitary representations of the system. If the Choi state of a channel exhibits this symmetry, then the channel itself is covariant [CDP09], and the converse is true as well.

This last notion of symmetry allows us to directly prescribe an algorithm to test for Hamiltonian symmetries. If we can emulate the dynamics of a Hamiltonian efficiently, we can test for the symmetry of its Choi state. The symmetry of the Choi state then directly implies symmetry of the Hamiltonian being tested.

2.3. Quantum Simulations of Hamiltonians

A necessary preliminary to testing Hamiltonian dynamics in any respect is first making sure they can be imported to computational framework to begin with. Quantum simulation techniques directly answer this need by providing a method for implementing Hamiltonian dynamics on quantum computers. Usually, this approach involves approximating them as sequences of quantum logic gates [Llo96, CMN+18]. Much work has been conducted in this field, including work on implementations on near-term hardware [CBC21, CCH+20], simulation by qubitization [LC19], simulation of operator spread [GAH+22], and more. Here, we review a rather popular example implementation, though be advised that this is not the only method available for this purpose.

One common approach [Llo96] employs the Trotter–Suzuki approximation [Tro59,

Suz76]. This method allows for decomposition into local Hamiltonian evolutions with some specified error. In this approximation, we suppose that the Hamiltonian H is of the form $H = \sum_{i=1}^{m} H_i$, where each H_i is a k-local Hamiltonian, which means H_i affects at most k systems simultaneously. Then we can describe its evolution by

$$e^{-iHt} = \left(\prod_{j=1}^{m} e^{-iH_j t/r} \right)^r + O\left(\frac{m^2 t^2}{r^2} \right), \tag{2.2}$$

where the correction term is negligible for $mt/r \ll 1$ and vanishes when the terms in the decomposition commute. (Here and throughout, we take $\hbar = 1$.) By other methods, the error can be reduced to higher orders in t [BACS07].

2.4. An Efficient Quantum Algorithm to Test Hamiltonian Symmetries

Given the notion of covariance recalled above and a way to simulate the applicable Hamiltonian, we now propose a quantum algorithm to test a Hamiltonian for covariance symmetry. We begin by supposing that we have a Hamiltonian composed of a finite sum of k-local Hamiltonians, as described previously, with dynamics realized by higher-order methods such that the simulation error is $O(t^4)$. Then we claim a test for symmetries of this Hamiltonian with respect to a group G with a projective unitary representation $\{U(g)\}_{g \in G}$ can be performed efficiently on a quantum computer.

The circuit presented in Figure 2.1 implements just such a test, and we sketch its action here. Let the input state to the circuit be the maximally-entangled state Φ_{RA}. Then act on the A subsystem with the unitary Hamiltonian dynamics. As indicated in Figure 2.1, the depth of the circuit to realize this algorithm can be cut in half by taking advantage of the transpose trick $(X \otimes I)|\Phi\rangle = (I \otimes X^T)|\Phi\rangle$ and the decomposition $e^{-iHt} = W_1 W_2^\dagger$, which is clearly possible for Hamiltonian simulations of the form in (2.2) or from [BACS07]. (The transpose trick, for those

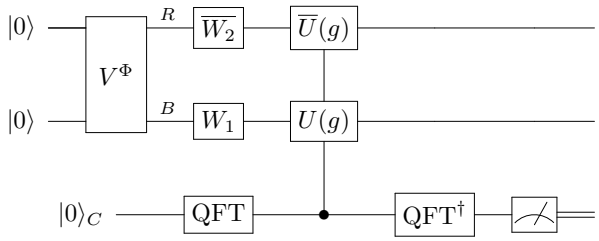


Figure 2.1. Quantum circuit to test for the covariance of a unitary Hamiltonian evolution. The unitary V^{Φ} generates the state $|\Phi\rangle_{RA}$, the maximally-entangled state on RA. The evolution of the system is given by $e^{-iHt} = W_1 W_2^{\dagger}$ and the $U(g)$ gates are controlled on a superposition over all of the elements $g \in G$, as in (2.4).

unfamiliar, can be understood best pictographically. A common shorthand for quantum circuits is to represent a maximally-entangled state as a 'cap' or a Bell measurement as a 'cup'. When there is a cup or cap present in the circuit diagram, a tensor can be moved around to the other leg of the cup/cap if the transpose of the tensor is used instead. See [BB17] for further illustration.)

The state of the system after such tricks have been applied is given by

$$\Phi_{RB}^{t} := (\mathbb{I}_R \otimes e^{-iHt})\Phi_{RA}(\mathbb{I}_R \otimes e^{iHt}), \tag{2.3}$$

which is exactly the Choi state of the channel generated by e^{-iHt}. We then use the quantum Fourier transform (QFT) to generate a control register in the following superposed state:

$$|+\rangle_C := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle. \tag{2.4}$$

Implementing the controlled $\overline{U}(g)$ and $U(g)$ gates using the above control register yields the state

$$\frac{1}{|G|} \sum_{g,g' \in G} (\overline{U}_R(g) \otimes U_B(g))(\Phi_{RB}^{t} \otimes |g\rangle\langle g'|_C)(\overline{U}_R^{\dagger}(g') \otimes U_B^{\dagger}(g')). \tag{2.5}$$

Finally, we perform the measurement $\mathcal{M} = \{|+\rangle\langle+|_C, \mathbb{I} - |+\rangle\langle+|_C\}$ on the control register and accept if and only if the outcome $|+\rangle\langle+|_C$ is observed. With this condition, the acceptance probability is

given by

$$P_{\text{acc}} = \text{Tr}[\Pi^G \Phi^t_{RB}], \tag{2.6}$$

where we have used the projector defined in (2.1) (see Appendix A.1 for a quick derivation of (2.6), which we do not present here in an effort to preserve coherentness). As a limiting case of the gentle measurement lemma (see Section 1.3.1, and references [Dav69, Win99, ON07]), we have that

$$\text{Tr}[\Pi^G \Phi^t_{RB}] = 1 \quad \Leftrightarrow \quad \Phi^t_{RB} = \Pi^G \Phi^t_{RB} \Pi^G, \tag{2.7}$$

where the second statement is equivalent to the condition on the Choi state given in (1.77) in Section 1.4.2. Therefore, by implementing this algorithm, we can determine whether a Hamiltonian exhibits a symmetry under a group G with some projective unitary representation $\{U(g)\}_{g\in G}$.

Now, indulge us in a minor aside to demonstrate approximate equivalence in (2.7); specifically, to show that the acceptance probability is near to one if and only if the Choi state is approximately Bose symmetric. This will endow our test with a sense of continuity and robustness, and thus merits taking the time to ascertain.

First, consider the situation where the Choi state is approximately Bose symmetric, and set ϵ such that

$$\epsilon := \left\| \Phi^t_{RB} - \Pi^G \Phi^t_{RB} \Pi^G \right\|_1 . \tag{2.8}$$

Here we employ the trace distance as a standard metric between states or subnormalized states. From this point, we use the reverse triangle inequality to conclude that

$$\left\| \Phi^t_{RB} - \Pi^G \Phi^t_{RB} \Pi^G \right\|_1 \geq \left\| \Phi^t_{RB} \right\|_1 - \left\| \Pi^G \Phi^t_{RB} \Pi^G \right\|_1 , \tag{2.9}$$

where the first term on the right-hand side is equal to one for every quantum state, and the left-hand side is equal to ϵ by definition. Meanwhile, recall that our acceptance probability is given

by

$$P_{\text{acc}} = \text{Tr}[\Pi^G \Phi^t_{RB}] = \text{Tr}[\Pi^G \Phi^t_{RB} \Pi^G] = \left\| \Pi^G \Phi^t_{RB} \Pi^G \right\|_1 , \tag{2.10}$$

where the second equality follows from cyclicity of trace and the last equality follows because $\Pi^G \Phi^t_{RB} \Pi^G$ is positive semi-definite. This is the final term on the right-hand side of (2.9). Thus, by substituting in these terms and conducting some simple algebra, we conclude that

$$P_{\text{acc}} \geq 1 - \epsilon . \tag{2.11}$$

Consequently, whenever the state is approximately symmetric (in the sense that $\epsilon \approx 0$ in (2.8)), the acceptance probability is near to one. Thus, our acceptance probability demonstrates a continuity property.

Next, we will show that the reverse direction is also true. This relationship can be demonstrated via the gentle operator lemma (see, again, Sec 1.3.1 or references [Dav69, Win99, ON07]). Let Φ be a density operator and Λ a measurement operator satisfying $0 \leq \Lambda \leq I$. If $\text{Tr}[\Lambda \Phi] \geq 1 - \epsilon$ for $\epsilon \in [0, 1]$, then by Lemma 1.3.4, the following inequality holds

$$\left\| \Phi - \sqrt{\Lambda} \Phi \sqrt{\Lambda} \right\|_1 \leq 2\sqrt{\epsilon} . \tag{2.12}$$

In our case, set $\Lambda = \Pi^G$. (Note that $\Pi^G = \sqrt{\Pi^G}$ for a projector.) Then suppose our acceptance probability is close to one, as in

$$P_{\text{acc}} = \text{Tr}[\Pi^G \Phi^t_{RB}] \geq 1 - \epsilon , \tag{2.13}$$

for some $\epsilon \in [0, 1]$. Then Lemma 1.3.4 implies that the state is approximately symmetric:

$$\left\| \Phi^t_{RB} - \Pi^G \Phi^t_{RB} \Pi^G \right\|_1 \leq 2\sqrt{\epsilon} . \tag{2.14}$$

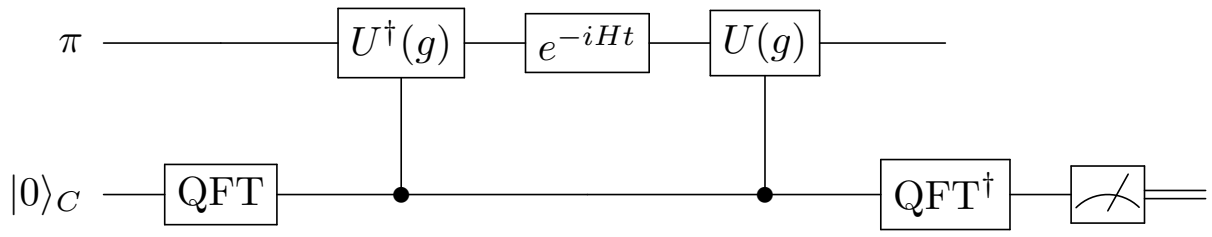


Figure 2.2. Quantum circuit to test for the covariance of a unitary Hamiltonian evolution. Here, π denotes the maximally-mixed state $\mathbb{I}/d$.

Returning to the algorithm with renewed confidence, upon investigation, it can be further simplified. By invoking the transpose trick (see, e.g., [BB17]), we can identify the unitary on the reference system, $\overline{U}_R(g)$, with an equivalent action on A given by $U_A^\dagger(g)$. Since the action of the circuit would then take place solely on the subsystem A, the reference system R is traced out. This is equivalent to preparing the maximally-mixed state (denoted by π) on A, such that this variation of our algorithm bears some resemblance to a one-clean-qubit algorithm [KL98], or a DQC1 algorithm, as discussed in Section 1.3.2. The only exception is that it requires $\log_2 |G|$ clean qubits for the control register. Figure 2.2 shows this simplification. The acceptance probability corresponding to this described situation is

$$P_{\text{acc}} = \frac{1}{d|G|} \sum_{g \in G} \text{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}], \tag{2.15}$$

where d is the dimension of the system being tested. Appendix A.1 gives a proof that the expression in (2.15) is equal to the acceptance probability of the circuit in Figure 2.1 using only elementary methods.

The proposed circuit in Figure 2.2 is limited in complexity only by the implementation of the Hamiltonian and unitary representation. Thus, our first quantum algorithm is efficiently realizable. Furthermore, we have shown that entanglement resources usually necessary for character-

izing the Choi operator of a quantum channel are not necessary here. We also note that the statistics accumulated for the maximally-mixed state can be equivalently found in a sampling manner using computational basis state inputs.

2.4.1. DQC1-Completeness of Acceptance Probability

Having established the algorithm, it is now necessary to provide evidence that our algorithm cannot generally be simulated efficiently by classical computers—else, that would certainly be the preferred calculation method by most. For this purpose, we turn to established notions of computational complexity we so fortuitously described in Section 1.3.2. In this section, we prove that estimating the acceptance probability in (2.15) to within additive error is a DQC1-complete problem. This means that (2.15) can be estimated within a restricted model of quantum computing (via our algorithm and by an observation of [SJ08, Section 1]), and thus can be estimated efficiently on a quantum computer. Furthermore, this demonstrates that estimating (2.15) is just as computationally hard as any problem in this complexity class. Strong evidence exists that classical computers cannot solve DQC1-complete problems efficiently [MFF14, FKM+18], thus ruling out any possibility of estimating the acceptance probability in (2.15) by a classical sampling approach. It is the end goal of this section, then, to convince any wary reader that this approach belongs firmly to the class of problems best handled by a quantum machine.

Before establishing our primary claim, we must first prove that estimating $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$, where U is the unitary generated by a quantum circuit, is a DQC1-complete problem. This will be a useful tool in asserting our claim. To do this, we will make use of the established fact that estimating $\mathrm{Re}[\mathrm{Tr}[U]]/d$ is a DQC1-complete problem. First, consider the usual construction with U substituted by U^2. (The usual construction, as it were, is that which is succintly given in

Section 1.3.2, but more thoroughly presented [SJ08, Section 1].) Similarly, we prepare a control qubit in the $|+\rangle$ state and all other qubits in the maximally-mixed state, act with controlled-U^2 (easily realized as two applications of controlled-U), and then measure in the Hadamard basis. Assigning the values $+1$ and -1 to the measurement outcomes, the expected value of the measurement outcomes is equal to $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$. This implies that the problem is in DQC1.

To show hardness, suppose that we have a way of estimating $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$ for every U, where U is the unitary generated by a quantum circuit. We can then show that it possible to use such an algorithm to estimate $\mathrm{Re}[\mathrm{Tr}[U]]/d$. The key idea behind the reduction is the following unitary

$$V := \begin{bmatrix} 0 & I \\ U & 0 \end{bmatrix} = |0\rangle\langle 1| \otimes I + |1\rangle\langle 0| \otimes U, \tag{2.16}$$

which can be realized in terms of a quantum circuit as a σ_X acting on a control qubit, followed by a controlled-U, i.e.,

$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)\,(\sigma_X \otimes I)\,. \tag{2.17}$$

We then observe that

$$\mathrm{Tr}\left[V^2\right] = \mathrm{Tr}\left[\begin{bmatrix} 0 & I \\ U & 0 \end{bmatrix}\begin{bmatrix} 0 & I \\ U & 0 \end{bmatrix}\right] \tag{2.18}$$

$$= \mathrm{Tr}\left[\begin{bmatrix} U & 0 \\ 0 & U \end{bmatrix}\right] \tag{2.19}$$

$$= 2\,\mathrm{Tr}[U]. \tag{2.20}$$

Thus, by using the method to estimate $\mathrm{Re}[\mathrm{Tr}[V^2]]/d$, we estimate $\mathrm{Re}[\mathrm{Tr}[U]]/d$ up to a constant factor of 2. This completes the proof that estimating $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$ is a DQC1-complete prob-

lem.

Now let us turn to the main goal of this section: proving that estimating the acceptance probability in (2.15) to within additive error is a DQC1-complete problem. Let H be a local Hamiltonian, and let $\{U(g)\}_{g\in G}$ be a unitary representation of a group G, such that each $U(g)$ can be realized by a quantum circuit. Furthermore, suppose that the size $|G|$ of the group G is no larger than linear in the number of qubits on which each circuit for $U(g)$ acts (so that $\log|G|$ is logarithmic in the number of qubits). Thus, the size of the computational problem depends solely on the classical description of the Hamiltonian H and the circuit descriptions of each unitary $U(g)$. Then we assert that the task of estimating the value

$$\frac{1}{d\,|G|}\sum_{g\in G}\mathrm{Tr}[U^{\dagger}(g)e^{iHt}U(g)e^{-iHt}] \tag{2.21}$$

is a DQC1-complete problem. To show this is in DQC1, we use the quantum algorithm presented above and in [LW22], as well as the observation from [SJ08, Section 1], that the class DQC1 does not change if there are a logarithmic number of pure qubits, which is the case under our description of the problem stated above.

To show hardness, let U be a unitary realized by an arbitrary quantum circuit. We will now use the fact that estimating $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$ is a DQC1-complete problem by showing that an algorithm for estimating the value in (2.21) can estimate the value $\mathrm{Re}[\mathrm{Tr}[U^2]]/d$. To this end, we let the group G be $\mathbb{Z}_2$ with representation $\{I, V\}$, where

$$V = |0\rangle\langle 1|\otimes U + |1\rangle\langle 0|\otimes U^{\dagger}. \tag{2.22}$$

(A quick calculation indicates that $V^2 = I$, so that indeed $\{I, V\}$ is a representation of $\mathbb{Z}_2$.) A circuit for realizing V can be efficiently generated from the circuit for realizing U. Indeed, we can

construct a 0-controlled-U from U:

$$|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes I, \tag{2.23}$$

and a 1-controlled-$U^\dagger$ from U, by reversing the order of the gates used to construct U, essentially running it backwards, with each circuit gate controlled on 1, leading to

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U^\dagger. \tag{2.24}$$

The overall circuit consists of $X \otimes I$, and then the above controlled gates, so that

$$\begin{aligned}
&\left(|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes I\right) \left(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U^\dagger\right) (X \otimes I) \\
&= \left(|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U^\dagger\right) (X \otimes I) && (2.25) \\
&= |0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^\dagger && (2.26) \\
&= V. && (2.27)
\end{aligned}$$

We take the Hamiltonian to be one that realizes $H_2 \otimes I$ via Hamiltonian evolution, where H_2 is a 2×2 Hadamard gate. Indeed, such a Hamiltonian is local and acts non-trivially on only one qubit. Then we have that $|G| = 2$, its unitary representation is $\{I, V\}$, and $e^{-iHt} = H_2 \otimes I$. Plugging into (2.21), we find that

$$\begin{aligned}
\frac{1}{d\,|G|} \sum_{g\in G} \mathrm{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] = \frac{1}{2d} \mathrm{Tr}\left[I\,(H_2 \otimes I)\,I\,(H_2 \otimes I)\right] \\
+ \frac{1}{2d} \mathrm{Tr}\left[V\,(H_2 \otimes I)\,V\,(H_2 \otimes I)\right]. \quad (2.28)
\end{aligned}$$

Consider that

$$\mathrm{Tr}\left[I\,(H_2 \otimes I)\,I\,(H_2 \otimes I)\right] = \mathrm{Tr}[I], \tag{2.29}$$

and

$$\mathrm{Tr}\left[V\,(H_2 \otimes I)\,V\,(H_2 \otimes I)\right]$$

$$= \mathrm{Tr}\left[\left(|0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^\dagger\right)(H_2 \otimes I)\left(|0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^\dagger\right)(H_2 \otimes I)\right] \tag{2.30}$$

$$= \mathrm{Tr}\left[\left(|0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^\dagger\right)\left(|+\rangle\langle -| \otimes U + |-\rangle\langle +| \otimes U^\dagger\right)\right] \tag{2.31}$$

$$= \mathrm{Tr}\left[|0\rangle\langle 1|+\rangle\langle -| \otimes U^2 + |1\rangle\langle 0|+\rangle\langle -| \otimes I + |0\rangle\langle 1|-\rangle\langle +| \otimes I + |1\rangle\langle 0|-\rangle\langle +| \otimes \left(U^\dagger\right)^2\right] \tag{2.32}$$

$$= \langle 1|+\rangle\langle -|0\rangle\,\mathrm{Tr}\left[U^2\right] + \langle 0|+\rangle\langle -|1\rangle\,\mathrm{Tr}\left[I\right] + \langle 1|-\rangle\langle +|0\rangle\,\mathrm{Tr}\left[I\right] + \langle 0|-\rangle\langle +|1\rangle\,\mathrm{Tr}\left[\left(U^\dagger\right)^2\right] \tag{2.33}$$

$$= \frac{1}{2}\left(\mathrm{Tr}\left[U^2\right] - \mathrm{Tr}\left[I\right] - \mathrm{Tr}\left[I\right] + \mathrm{Tr}\left[\left(U^\dagger\right)^2\right]\right). \tag{2.34}$$

Putting together (2.28), (2.29), and (2.30)–(2.34), and noting the dimensions of the identities in (2.29) and (2.34), this implies for the above choices that

$$\frac{1}{d\,|G|}\sum_{g\in G}\mathrm{Tr}[U^\dagger(g)e^{iHt}U(g)e^{-iHt}] = \frac{1}{4} + \frac{\mathrm{Re}\left[\mathrm{Tr}\left[U^2\right]\right]}{4d} \tag{2.35}$$

Thus, the acceptance probability of this algorithm is an estimate of the desired quantity, up to a constant factor of $1/4$, establishing DQC1-hardness of our problem. Though this may seem unintuitive, since this reappropriation of the Hamiltonian symmetry testing algorithm takes only a few short steps, it suffices to verify our claims of computational complexity.

2.5. A Derivation of Symmetry in the Acceptance Probability

We have given statements about complexity and circuit construction, but the connection to symmetry may yet still seem aloof. Thus, we will continue no further without addressing the elephant in the room; from the acceptance probability given in (2.15), we will derive a relationship with the familiar expression of Hamiltonian symmetry in quantum mechanics, further establishing this as an authentic test of symmetry.

Begin by expanding the Hamiltonian evolution e^{iHt}, under the assumption that $\tau := \|H\|_\infty t < 1$, where $\|X\|_\infty := \sup_{|\psi\rangle\neq 0}\frac{\||X|\psi\rangle\|_2}{\||\psi\rangle\|_2}$:

$$e^{iHt} = \mathbb{I} + iHt - \frac{H^2t^2}{2} - \frac{iH^3t^3}{6} + O(\tau^4). \tag{2.36}$$

(This expansion is simply a truncated Taylor series.) Substituting this relation into the trace argument of (2.15), we find that

$$\operatorname{Tr}[U^\dagger e^{iHt} U e^{-iHt}] = d + t^2(\operatorname{Tr}[HU^\dagger HU] - \operatorname{Tr}[H^2]) + \frac{it^3}{2}(\operatorname{Tr}[U^\dagger H^2 U H] - \operatorname{Tr}[U^\dagger H U H^2]) + O(\tau^4), \quad (2.37)$$

where the equality is obtained using the linearity and cyclicity properties of the trace. After summing over all group elements, as in (2.15), and using the group property (that $g \in G$ implies $g^{-1} \in G$), we find that $\frac{1}{|G|}\sum_{g\in G}(\operatorname{Tr}[U^\dagger(g)H^2U(g)H] - \operatorname{Tr}[U^\dagger(g)HU(g)H^2]) = 0$. Thus, the third-order term of (2.15) vanishes. We can simplify the second-order term of (2.15) by using

$$\frac{1}{2}\operatorname{Tr}\left[|[U,H]|^2\right] = -\operatorname{Tr}[HU^\dagger HU] + \operatorname{Tr}[H^2], \quad (2.38)$$

where $|X|^2 \coloneqq X^\dagger X$ implies that

$$|[U,H]|^2 = H^2 - HU^\dagger HU - U^\dagger HUH + U^\dagger H^2 U. \quad (2.39)$$

Putting these equations together, we can rewrite the acceptance probability of our first quantum algorithm elegantly as

$$P_{\text{acc}} = 1 - \frac{t^2}{2d|G|}\sum_{g\in G}\left\|[U(g),H]\right\|_2^2 + O(\tau^4), \quad (2.40)$$

where $\|A\|_2 \coloneqq \sqrt{\operatorname{Tr}[|A|^2]}$ is the Hilbert–Schmidt norm defined in Section 1.3.1. Thus, to the first non-vanishing order of time t, the acceptance probability is equal to one if and only if

$$[U(g),H] = 0, \quad \forall g \in G. \quad (2.41)$$

This is exactly the familiar expression for symmetry in quantum mechanics. Furthermore, the expression in (2.40) clarifies that the normalized commutator norm $\frac{1}{d|G|}\sum_{g\in G}\left\|[U(g),H]\right\|_2^2$ can be

estimated efficiently by employing our algorithm. From (2.40), we can see that the normalized commutator norm is small—equivalently, the Hamiltonian H is approximately symmetric—if and only if the acceptance probability is close to one. Finally, as we show at length in Appendix A.2, the acceptance probability has an exact expansion as follows, such that all odd powers in t vanish and the even powers are scaled by normalized nested commutator norms, quantifying higher orders of symmetry:

$$P_{\text{acc}} = \sum_{n=0}^{\infty} \frac{(-1)^n t^{2n}}{(2n!)} \left(\frac{1}{d\,|G|} \sum_{g \in G} \left\| \left[(H)^n, U(g) \right] \right\|_2^2 \right) \tag{2.42}$$

where the nested commutator is defined as

$$[(X)^n, Y] \coloneqq \underbrace{[X, \cdots [X, [X}_{n \text{ times}}, Y]] \cdots], \qquad [(X)^0, Y] \coloneqq Y. \tag{2.43}$$

Note that the expansion in (2.42) is valid for all $t \in \mathbb{R}$. We also provide an alternative formula for P_{acc} in Appendix A.2 using the group twirl. However, that formula lacks the elegant simplicity shown here, so we defer to (2.42) in an act of blatant favoritism.

2.6. Variational Quantum Algorithm for Symmetry Testing

Rather than feeding in the maximally-mixed state to the input of the circuit in Figure 2.2, we can instead feed in an arbitrary input state $|\psi\rangle$. The acceptance probability when doing so is equal to

$$\left\| \mathcal{T}_G(e^{-iHt}) |\psi\rangle \right\|_2^2 = 1 - t^2 \left\langle \mathcal{T}_G(H^2) - (\mathcal{T}_G(H))^2 \right\rangle_\psi + O(\tau^3), \tag{2.44}$$

where $\mathcal{T}_G(X) \coloneqq \frac{1}{|G|} \sum_{g \in G} U(g) X U^\dagger(g)$ is the group twirl. (Appendix A.3 gives the full derivation for this expression.) Note that the bracketed term is non-negative as a consequence of the Kadison–Schwarz inequality [Bha07, Theorem 2.3.2]. If we had the ability to prepare arbitrary quantum states as modeled in [VW16], we could optimize this acceptance probability over all

states, resulting in the following value:

$$\left\|\mathcal{T}_G(e^{-iHt})\right\|_\infty^2 \geq 1 - \frac{2}{|G|}\sum_{g\in G}\left\|\left[U(g), e^{-iHt}\right]\right\|_\infty \tag{2.45}$$

$$\geq 1 - \frac{2t}{|G|}\sum_{g\in G}\left\|[U(g), H]\right\|_\infty - 4\tau^2. \tag{2.46}$$

These inequalities are proven in Appendix A.3, and the second holds under the assumption that $\tau < 1$. This demonstrates that the acceptance probability $\left\|\mathcal{T}_G(e^{-iHt})\right\|_\infty^2$ can be bounded from below in terms of a familiar expression of Hamiltonian symmetry. Thus, if the commutator norm $\frac{1}{|G|}\sum_{g\in G}\left\|[U(g), H]\right\|_\infty$ is small, as is the case when the Hamiltonian is approximately symmetric, then the acceptance probability of this algorithm is close to one. In Appendix A.3, we also prove that the acceptance probability satisfies

$$\left\|\mathcal{T}_G(e^{-iHt})\right\|_\infty^2 \geq \left(1 - \sum_{n=1}^{\infty}\frac{t^n}{n!}\frac{1}{|G|}\sum_{g\in G}\left\|\left[(H)^n, U(g)\right]\right\|_\infty\right)^2. \tag{2.47}$$

(Safe to say that Appendix A.3 contains all of the proofs for this section, as they are rather drawn-out mathematically but not particularly enlightening beyond their conclusions.)

Unfortunately, it is physically impossible to optimize over all input states. Instead, we can employ a variational ansatz to do so, in order to arrive at a lower-bound estimate of the acceptance probability on the left-hand side of (2.45). These methods have been vigorously pursued in recent years in the quantum computing literature [CAB+20, BCLK+21], and they can be combined with our approach here. In short, the acceptance probability in (2.44) is a reward function that can be estimated by means of the circuit in Figure 2.2 and a parameterized circuit that prepares the state $|\psi\rangle$. Then one can employ gradient ascent on a classical computer to modify the parameters used to prepare the state $|\psi\rangle$. After many iterations, these algorithms typically converge to a value, which in our case provides a lower bound estimate of the acceptance probability

on the left-hand side of (2.45). In practice, it might be difficult in experiments to optimize over all pure states, and one could instead consider a variational product state ansatz, as in [GLX+21].

2.7. Examples

To exhibit our first algorithm, we consider three different examples. Namely, we consider the transverse Ising model with a cyclic boundary condition, the weakly J-coupled NMR Hamiltonian, and the Heisenberg XY model. In each case, we have employed IBM Quantum's noisy simulator to demonstrate the behavior of a quantum computer. In the near future, we suspect all of these algorithms will be testable on physical systems available to the public.

First, we consider the dynamics given by the transverse Ising model with a cyclic boundary condition. This Hamiltonian is given as $H_{\mathrm{TIM}} \coloneqq \sigma_N^Z \otimes \sigma_1^Z + \sum_{i=1}^{N-1} \sigma_i^Z \otimes \sigma_{i+1}^Z + \sum_{i=1}^{N} \sigma_i^X$. It is permutationally invariant, so that $[H_{\mathrm{TIM}}, W^\pi] = 0$ for all $\pi \in S_N$, where W^π is a unitary representation of the permutation $\pi \in S_N$, with S_N denoting the symmetric group on N letters. It also obeys the symmetry $[H_{\mathrm{TIM}}, \sigma_1^X \otimes \cdots \otimes \sigma_N^X] = 0$. Thus, we can use our algorithm to test these symmetries, and we do so in Figure 2.3 for $N = 3$ and $N = 4$. (Rather than test all permutations, we indicate here that we test for invariance under a cyclic shift, a subgroup of S_N.) We find that each respective symmetry test passes with reasonable probability, with deviation from one due to noise added to the simulation.

Next, we consider the example dynamics given by a weakly J-coupled NMR Hamiltonian [vdV96]. This Hamiltonian can be expressed as

$$H_{\mathrm{NMR}} \coloneqq \frac{\omega_1}{2}\sigma_1^Z + \frac{\omega_2}{2}\sigma_2^Z + \frac{\pi J}{2}\sigma_1^Z \otimes \sigma_2^Z, \tag{2.48}$$

in units of $\hbar = 1$, where ω_i is the frequency associated to spin $i \in \{1, 2\}$ and J is the coupling constant. This can be written as a diagonal matrix in the eigenbasis basis of the Pauli-Z matrix;

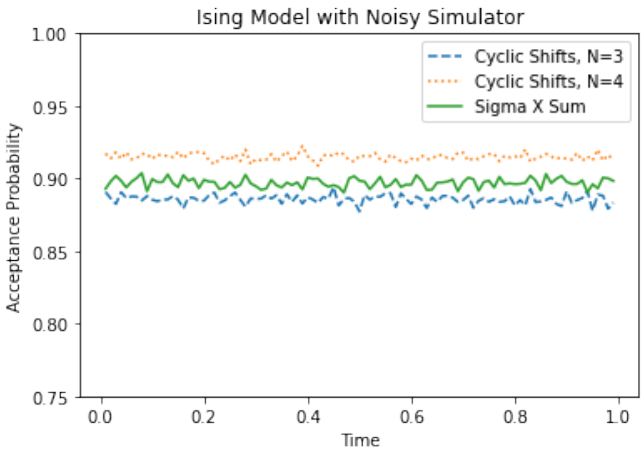


Figure 2.3. Results of symmetry tests for the transverse Ising model for $N = 3$ and $N = 4$, using IBM Quantum's noisy simulator. The symmetries in question are given by acting simultaneously on all systems by either the cyclic group of order N or a conjugation by $(\sigma^X)^{\otimes N}$.

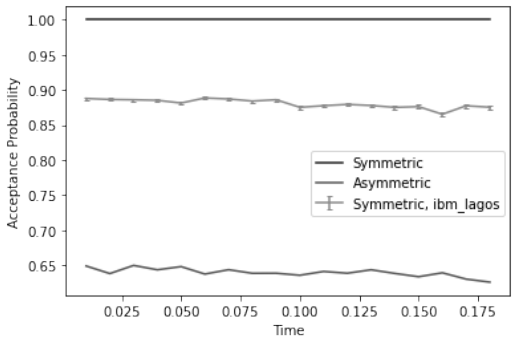


Figure 2.4. Acceptance probability of our Hamiltonian symmetry testing algorithm over time, for the NMR Hamiltonian example and a group for which the Hamiltonian is either symmetric or asymmetric. The acceptance probability decays as time gets larger for the asymmetric case, even ideally. Example calculations using *ibm_lagos* show a large degree of initial symmetry before noise begins to dominate.

therefore, the time-evolution dynamics are also given by a diagonal matrix, as shown below. Due to this simplicity, this example can be easily simulated on noisy quantum computers for appropriately short times using a two-qubit system.

It is clear that H_{NMR} is symmetric with respect to the group generated by taking the Pauli-Z gates on either qubit—this corresponds to a representation of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. It is not, however, symmetric under the group generated by the CNOT and SWAP gates acting on the two-

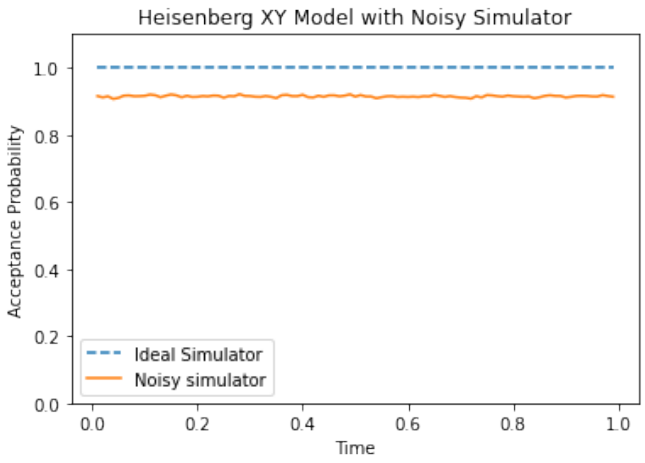


Figure 2.5. Results of testing the Heisenberg XY model on four qubits using IBM Quantum's noisy simulator. The symmetries in question are given by acting simultaneously on all systems by the stated σ_i matrix.

qubit system—corresponding to D_3, the triangular dihedral group. Thus, using these two groups as described in our algorithms, we can visualize examples of both symmetry and asymmetry, as shown in Figure 2.4. To generate this Hamiltonian, we define the terms $\omega_{\text{AVG}} = \frac{1}{2}(\omega_1 + \omega_2)$ and $\Delta\omega = \omega_2 - \omega_1$ as is common. Then the Hamiltonian can be written as:

$$H_{\text{NMR}} = \begin{pmatrix} -\omega_{\text{AVG}} + \frac{\pi J}{2} & 0 & 0 & 0 \\ 0 & \frac{\Delta\omega - \pi J}{2} & 0 & 0 \\ 0 & 0 & -\frac{\Delta\omega + \pi J}{2} & 0 \\ 0 & 0 & 0 & \omega_{\text{AVG}} + \frac{\pi J}{2} \end{pmatrix}. \tag{2.49}$$

As a final example, we consider the Heisenberg XY model [LSM61]. The Hamiltonian under consideration is given by

$$H_{\text{XY}} := J\left(\sum_{i=1}^{N-1} \sigma_i^X \otimes \sigma_{i+1}^X + \sigma_i^Y \otimes \sigma_{i+1}^Y\right), \tag{2.50}$$

where $J > 0$ is the antiferromagnetic exchange interaction between spins. This Hamiltonian showcases symmetry with respect to conjugation by each Pauli matrix acting on all qubits simul-

taneously. That is,

$$[H_{\mathrm{XY}}, \sigma_1^X \otimes \cdots \otimes \sigma_N^X] = 0, \tag{2.51}$$

$$[H_{\mathrm{XY}}, \sigma_1^Y \otimes \cdots \otimes \sigma_N^Y] = 0, \tag{2.52}$$

$$[H_{\mathrm{XY}}, \sigma_1^Z \otimes \cdots \otimes \sigma_N^Z] = 0. \tag{2.53}$$

The symmetry group to consider in this case is thus $\{\pm 1, \pm i\} \times \{I^{\otimes N}, (\sigma^X)^{\otimes N}, (\sigma^Y)^{\otimes N}, (\sigma^Z)^{\otimes N}\}$. As the global phase factors are irrelevant in this case, we can test this symmetry by having two control qubits prepared in a uniform superposition, one of which activates $(\sigma^X)^{\otimes N}$ and the other activating $(\sigma^Z)^{\otimes N}$. We tested this symmetry by implementing our algorithm on the IBM Quantum noisy simulator, with $N = 4$, and find that the symmetry test passes with reasonable probability, as indicated in Figure 2.5. The fact that the acceptance probability is not exactly equal to one has to do with the noise involved in the simulation.

We note here that all computer codes used to generate the examples in the main text and the supplementary material are available online.

2.8. Conclusion

In this work, we have specified algorithms to test a Hamiltonian for symmetry with respect to a group. We have demonstrated this construction from a ground-up perspective beginning with channel covariance and ending with an efficient algorithm that relies solely on a maximally-mixed state as input. We show that this test is DQC1-complete and therefore considered classically hard and is furthermore efficiently realizable on quantum computers given similarly efficient Hamiltonian simulations. Even better, the acceptance probability directly relies upon the familiar expression of symmetry from quantum mechanics. We then give a second test

https://github.com/mlabo15/Hamiltonian-Symmetry

employing a variational approach to estimate the commutator norm between the Hamiltonian evolution and group action. We have been successful in showing that these algorithms are useful tools that should be of interest throughout many realms of physics.

Chapter 3. Symmetry Testing of Quantum States

3.1. Introduction

In many applications, the symmetries of states themselves are the most interesting investigation. For instance, permutation symmetry in the extension of a bipartite quantum state indicates a lack of entanglement in that state [Wer89, DPS02, DPS04]. This permutation symmetry limits entanglement, which relates to fundamental principles of quantum information such as the no-cloning theorem [Par70, Die82, WZ82] and monogamy [Ter04]. Additionally, consider a system of two parties when there is a lack of a shared reference frame between them. This implies that a quantum state prepared relative to another party's reference frame respects a certain symmetry and is less useful than one that breaks the same symmetry [BRS07]. In all of these cases, a state respecting a symmetry is less resourceful than one that breaks it.

Resource theory in quantum information is its own beast to consider. In recent years, quantum resource theories have been proposed for each of the above scenarios. Asymmetry in general has been established via resources theories [MS13, MS14], and the concept of unextendibility—a quantum state that disobeys permutation symmetry when artificially extended to larger Hilbert spaces—has been proposed as a potential resource as well [KDWW19]. The above example of shared reference frames, or frameness, was discussed in [GS08]. All of these aim to quantify the resourcefulness of quantum states. (For a more thorough review, see [CG19].) As such, it is useful to be able to test whether a quantum state possesses symmetry and quantify how much symmetry it possesses.

In this chapter, we show how a quantum computer can test for symmetries of quantum states and channels generated by quantum circuits. In fact, our quantum-computational tests ac-

tually quantify how symmetric a state or channel is. Given that asymmetry is a useful resource in a wide variety of contexts, as alluded to above, while being potentially difficult for a classical computer to verify, our tests are helpful in determining how useful a state will be for certain quantum information processing tasks. These tests are in the spirit of the larger research program of using quantum computers to understand fundamental quantum-mechanical properties of high-dimensional quantum states, such as symmetry and entanglement, that are out of reach for classical computers.

We will make use of a general form of symmetry of quantum states, originally introduced in [LRW21], that captures both the extendibility of bipartite states [Wer89, DPS02, DPS04], as well as symmetries of a single quantum system with respect to a group of unitary transformations [MS13, MS14]. Luckily, we have already introduced such notions of symmetry in Chapter 1! We will draw heavily on the notions of G-symmetric extendibility and related definitions given in Section 1.4.1, which were originally published contiguous with the results of this chapter—however, those notions will serve us well not only here but also in the next chapter (and to some degree, the previous chapter as well) so we have sneakily chosen to introduce them right from the beginning.

In Section 3.2, we discuss the most important contribution of this chapter—namely, how a quantum computer can test for and estimate quantifiers of G-symmetric extendibility. These quantifiers are collectively called *maximum symmetric fidelities*, with more particular names given as appropriate. We prove that our quantum computational tests of symmetry have acceptance probabilities precisely equal to these fidelities, thus endowing these resource-theoretic measures with operational meanings and allowing us to estimate them to arbitrary precision. Using complexity-theoretic language, we demonstrate that these quantum-computational tests of sym-

metry can be conducted in the form of a QIP(2) system [Wat09, VW16]. (See Chapter 1 for a review of relevant quantum complexity theory, and Section 1.3.2 for QIP in particular.) Our results thus generalize previous results in the context of unextendibility and entanglement of bipartite quantum states [HMW13, HMW14]; additionally, we go on in the next section to clarify the relation between our results and previous ones in the literature. Simpler forms of the test can be conducted without any prover are thus efficiently computable on a quantum computer.

In Section 3.3, we show how the various symmetry tests specialize for testing the k-extendibility or k-Bose extendibility [Wer89, DPS02, DPS04] of both bipartite and multipartite states. These serve as tests of separability, and we will be expanding upon them in Chapter 4. We also show how to test for the covariance symmetry of a quantum channel, which includes testing the symmetries of Hamiltonian evolution as a special case, generalizing the case discussed in the previous chapter.

Finally, in Section 3.4, we review the resource theory of asymmetry [MS13, MS14]. After doing so, we define several generalized resource theories of asymmetry, including both the resource theory of asymmetry and the resource theory of k-unextendibility [KDWW19] as special cases. We also define resource theories of Bose asymmetry, which is an original contribution of our work in [LRW21]. This development shows that the acceptance probabilities of the aforementioned algorithms, i.e., maximum symmetric fidelities, are resource monotones and thus well-motivated from the resource-theoretic perspective.

In what follows, we proceed in the aforementioned order, and we finally reflect on these concepts in Section 3.5.

3.2. Tests of Symmetry & Extendibility

To begin, recall the definitions given in Section 1.4.1 for G-Bose symmetric extendibility and G-symmetric extendibility.

Definition 3.2.1 (G-symmetric-extendible) *A state ρ_S is G-symmetric-extendible if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{3.1}$$

2. *the state ω_{RS} is G-invariant, in the sense that*

$$\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \qquad \forall g \in G. \tag{3.2}$$

Definition 3.2.2 (G-Bose-symmetric-extendible) *A state ρ_S is G-Bose-symmetric-extendible (G-BSE) if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_R, \tag{3.3}$$

2. *the state ω_{RS} satisfies*

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}. \tag{3.4}$$

where Π^G_{RS} is defined as in (1.38).

Given these definitions, we will progress throughout this section by delineating algorithms to test for these abstract symmetries. We will then progressively narrow our view, moving from abstract tests of any symmetry, to separability tests, to covariance of quantum channels. We thus begin by defining tests of these above definitions, and, building upon them, we will create a managerie of algorithms forthwith.

We assert that we can use a quantum computer to test for G-symmetric extendibility of a quantum state, as well as for other previously discussed forms of symmetry given in Section 1.4.2. We assume the following in doing so:

1. there is a quantum circuit available that prepares a purification $\psi^\rho_{S'S}$ of the state ρ_S,

2. there is an efficient implementation of each of the unitary operators in the set $\{U_{RS}(g)\}_{g\in G}$,

3. and there is an efficient implementation of each of the unitary operators in the set $\{\overline{U}_{RS}(g)\}_{g\in G}$.

The first assumption can be made less restrictive by employing the variational, purification-learning procedure from [CSZW21]. That is, given a circuit that prepares the state ρ_S, the variational algorithm from [CSZW21] outputs a circuit that approximately prepares a purification of ρ_S. We should note that the convergence of the algorithm from [CSZW21] has not been established, and so the first assumption might be necessary for some applications.

The last assumption can be relaxed by the following reasoning: a standard gate set for approximating arbitrary unitaries in quantum computing consists of the controlled-NOT gate, the Hadamard gate, and the T gate [NC11]. The first two gates have only real entries while the T gate is a diagonal 2×2 unitary gate with the entries 1 and $e^{i\pi/4}$. Thus, the complex conjugate of this gate is equal to $T^\dagger$. Thus, if a circuit for $U_{RS}(g)$ is constructed from this standard gate set, then we can generate a circuit for $\overline{U}_{RS}(g)$ by replacing every T gate in the original circuit with $T^\dagger$.

We now consider various quantum computational tests of symmetry that have increasing complexity. To give insight along the way, we provide an example along with the tests below. For this purpose, we employ the triangular dihedral group D_3. This particular group was previously defined in Section 1.2.1, and for D_3, it has the lovely property of being isomorphic to the symmetric group on three elements—one of the smallest non-Abelian groups.

Of course, to actually implement this example, we will require a unitary representation that allows the group to be implemented on a quantum computer. To suit this purpose, we employ the two-qubit representation generated by setting the rotation element $r \rightarrow CNOT$ and the flip $f \rightarrow \text{CNOT} \circ \text{SWAP}$. A quick check will ensure that these generators obey the commutation

rules of the group and will generate the full group defined in Section 1.2.1. Throughout the next four sections, this group will be substituted into the presented algorithms to demonstrate their construction.

3.2.1. Testing G-Bose Symmetry

Let us begin by discussing the simplest version of the problem. Suppose that the state ρ_S is pure, so that we can write it as $\rho_S = \psi_S \equiv |\psi\rangle\langle\psi|_S$, and that the R system is trivial. We recover the traditional case of G-Bose symmetry mentioned in Example 1.4.2. Thus, our goal is to decide if

$$|\psi\rangle_S = U_S(g)|\psi\rangle, \quad \forall g \in G. \tag{3.5}$$

This condition is equivalent to

$$|\psi\rangle_S = \Pi_S^G |\psi\rangle_S, \tag{3.6}$$

where Π_S^G is as given in (1.39). This last condition is, in turn, equivalent to the statement

$$\left\|\Pi_S^G |\psi\rangle_S\right\|_2 = 1. \tag{3.7}$$

The equivalence

$$|\psi\rangle_S = \Pi_S^G |\psi\rangle_S \quad \Leftrightarrow \quad \left\|\Pi_S^G |\psi\rangle_S\right\|_2 = 1 \tag{3.8}$$

holds by expanding the norm in terms of the inner product and using the adjoint property of the projector or, alternatively, by the Pythagorean theorem. Thus, if we have a method to perform the projection onto Π_S^G, then we can decide whether (3.7) holds.

There is a simple quantum algorithm to do so. This algorithm was originally proposed in [Har05, Chapter 8] under the name of "generalized phase estimation." It proceeds as follows and can be summarized as "performing the quantum phase estimation algorithm with respect to the unitary representation $\{U_S(g)\}_{g\in G}$":

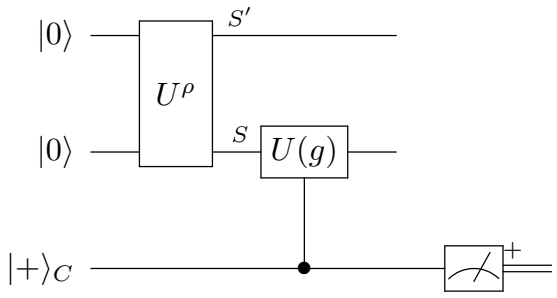


Figure 3.1. Quantum circuit to implement Algorithm 1. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 1 tests whether the state ρ_S is G-Bose symmetric, as defined in Example 1.4.2. Its acceptance probability is equal to $\mathrm{Tr}[\Pi_S^G \rho_S]$, where Π_S^G is defined in (1.39).

Algorithm 1 (G-Bose symmetry test) *The algorithm consists of the following steps:*

1. *Prepare an ancillary register C in the state $|0\rangle_C$.*

2. *Act on register C with a quantum Fourier transform or other sequence of gates capable of creating a equal superposition over group elements.*

3. *Append the state $|\psi\rangle_S$ and perform the following controlled unitary:*

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_S(g), \tag{3.9}$$

4. *Perform an inverse quantum Fourier transform on register C, measure in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accept if the zero outcome $|0\rangle\langle 0|_C$ occurs.*

Note that the register C has dimension $|G|$. Also, we can write the state $|0\rangle_C$ as $|e\rangle_C$, where e is the identity element of the group. The result of Step 2 of Algorithm 1 is to prepare the following uniform superposition state:

$$|+\rangle_C \coloneqq \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C. \tag{3.10}$$

We pause to note that although the quantum Fourier transform is specified in the above algorithm, in fact, any operation which creates the desired superposition state is equally acceptable.

Moving on, the overall state after Step 3 is as follows:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g) |\psi\rangle_S. \tag{3.11}$$

The final step of Algorithm 1 projects the register C onto the state $|+\rangle_C$. According to the aforementioned convention, Algorithm 1 accepts if the identity element outcome $|+\rangle\langle+|$ occurs. The probability that Algorithm 1 accepts is equal to

$$\begin{aligned}
&\left\| (\langle +|_C \otimes I_S) \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g) |\psi\rangle_S \right) \right\|_2^2 \\
&= \left\| \frac{1}{|G|} \sum_{g \in G} U_S(g) |\psi\rangle_S \right\|_2^2 \qquad (3.12) \\
&= \left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 . \qquad (3.13)
\end{aligned}$$

Figure 3.1 depicts this quantum algorithm. Not only does it decide whether the state $|\psi\rangle_S$ is symmetric, but it also quantifies how symmetric the state is. Since the acceptance probability is equal to $\left\| \Pi_S^G |\psi\rangle_S \right\|_2^2$, and this quantity is a measure of symmetry (see Theorem 3.4.2), we can repeat the algorithm a large number of times to estimate the acceptance probability to arbitrary precision.

The same quantum algorithm can decide whether a given mixed state ρ_S is G-Bose symmetric (see Example 1.4.2). Similar to the above, it also can estimate how G-Bose symmetric the state ρ_S is. To see this, consider that the acceptance probability for a pure state can be rewritten as follows:

$$\left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 = \mathrm{Tr}[\Pi_S^G |\psi\rangle\langle\psi|_S]. \tag{3.14}$$

Then since every mixed state can be written as a probabilistic mixture of pure states, it follows

that the acceptance probability of Algorithm 1, when acting on the mixed state ρ_S, is equal to

$$\mathrm{Tr}[\Pi_S^G \rho_S]. \tag{3.15}$$

This acceptance probability is equal to one if and only if $\rho_S = \Pi_S^G \rho_S \Pi_S^G$, and so this test is a faithful test of G-Bose symmetry. The equivalence

$$\mathrm{Tr}[\Pi_S^G \rho_S] = 1 \quad \Leftrightarrow \quad \rho_S = \Pi_S^G \rho_S \Pi_S^G \tag{3.16}$$

follows as a limiting case of Lemma 1.3.3, the gentle measurement lemma [Win99, ON07], and also the positive definiteness of the trace norm. Again, through repetition, we can estimate the acceptance probability $\mathrm{Tr}[\Pi_S^G \rho_S]$ and then employ it as a measure of G-Bose symmetry (as we will show in a later section via Theorem 3.4.2, when it becomes time to discuss such things).

Interestingly, the acceptance probability of Algorithm 1 can be expressed as the *maximum G-Bose-symmetric fidelity*, defined for a state ρ_S as

$$\max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S), \tag{3.17}$$

where

$$\text{B-Sym}_G := \left\{ \sigma_S \in \mathcal{D}(\mathcal{H}_S) : \sigma_S = \Pi_S^G \sigma_S \Pi_S^G \right\}, \tag{3.18}$$

and the fidelity of quantum states ω and τ is defined as [Uhl76]

$$F(\omega, \tau) := \left\| \sqrt{\omega}\sqrt{\tau} \right\|_1^2. \tag{3.19}$$

Thus, we arrive at the following theorem, Theorem 3.2.1, and provide a proof in Appendix B.1. As such, Algorithm 1 gives an operational meaning to the maximum G-Bose-symmetric fidelity in terms of its acceptance probability, and it can be used to estimate this fundamental measure of symmetry.

Theorem 3.2.1 *For a state ρ_S, the acceptance probability of Algorithm 1 is equal to the maximum G-Bose symmetric fidelity. That is,*

$$\mathrm{Tr}[\Pi_S^G \rho_S] = \max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S). \tag{3.20}$$

Let us construct this algorithm explicitly for the example of the dihedral group D_3. The $|+\rangle_C$ state is a uniform superposition of six elements, and we can achieve this using three qubits and unitary U_d shown in Figure 3.2:

$$U_d|000\rangle = \frac{1}{\sqrt{6}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle). \tag{3.21}$$

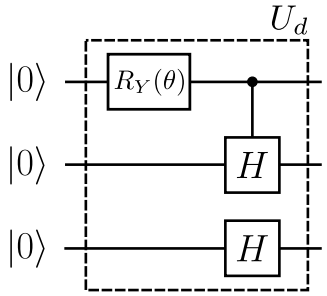


Figure 3.2. Unitary U_d, with $\theta = 2\arctan\left(\frac{1}{\sqrt{2}}\right)$, creates the equal superposition of six elements from (3.21).
.

These control register states need to be mapped to group elements to be meaningful; thus, we employ the mapping $\{|000\rangle \to e, |001\rangle \to fr^2, |010\rangle \to fr, |011\rangle \to r, |100\rangle \to f, |101\rangle \to r^2\}$. The circuit to test for D_3-symmetry is shown in Figure 3.3.

3.2.2. Testing G-Symmetry

We now discuss how to modify Algorithm 1 to one that decides whether a state ρ_S is G-symmetric (see Example 1.4.1), i.e., if

$$\rho_S = U_S(g)\rho_S U_S(g)^\dagger \quad \forall g \in G. \tag{3.22}$$

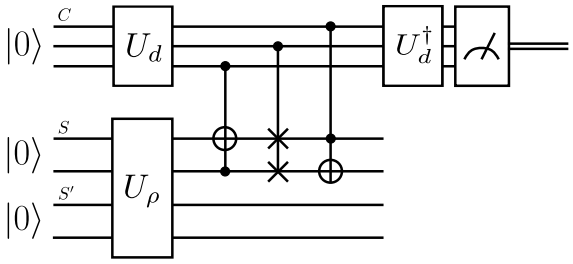


Figure 3.3. Quantum circuit implementing Algorithm 1 to test G-Bose symmetry for D_3. Compared to Figure 3.1, the systems S and S' are two qubits each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$.

There is a subtlety here in the shift from pure states to density matrices—a wider class of quantum states—but also moving from the projector condition to a conjugation condition. We will also prove that the acceptance probability of the modified algorithm is equal to the *maximum G-symmetric fidelity*, defined as

$$\max_{\sigma \in \mathrm{Sym}_G} F(\rho_S, \sigma_S), \tag{3.23}$$

where

$$\mathrm{Sym}_G := \left\{\sigma_S \in \mathcal{D}(\mathcal{H}_S) : \sigma_S = U_S(g)\sigma_S U_S(g)^\dagger \ \forall g \in G\right\}, \tag{3.24}$$

$\mathcal{D}(\mathcal{H}_S)$ denotes the set of density operators acting on the Hilbert space $\mathcal{H}_S$, and the fidelity of quantum states ω and τ is defined as [Uhl76]

$$F(\omega, \tau) := \left\|\sqrt{\omega}\sqrt{\tau}\right\|_1^2. \tag{3.25}$$

Thus, this quantum algorithm gives an operational meaning to the maximum G-symmetric fidelity in terms of its acceptance probability, and it can be used to estimate this fundamental measure of symmetry.

In the modified approach, we suppose that the quantum computer (now called the verifier) is equipped with access to a "quantum prover"—an agent who can perform arbitrarily powerful quantum computations [Wat09, VW16]. We discussed this situation exactly in Section 1.3.2

when we defined the complexity class QIP(n). We suppose that the quantum computer is allowed to exchange two quantum messages with the prover, thus placing our algorithm in QIP(2). We note here that computational problems related to entanglement of bipartite states [HMW13, HMW14] and recoverability of tripartite states [CHM+16] were previously shown to be decidable in QIP(2).

For this next algorithm, let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the verifier has access to a circuit U^ρ that prepares this purification of ρ_S. Then proceed as follows:

Algorithm 2 (G-symmetry test) *The algorithm consists of the following steps:*

1. *The verifier uses the circuit U^ρ to prepare the state $|\psi\rangle_{S'S}$.*
2. *The verifier transmits the purifying system S' to the prover.*
3. *The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to\hat{S}E'}$.*
4. *The prover sends the system $\hat{S}$ back to the verifier.*
5. *The verifier prepares a register C in the state $|0\rangle_C$.*
6. *The verifier acts on register C with a quantum Fourier transform or equivalent circuit.*
7. *The verifier performs the following controlled unitary:*

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_S(g) \otimes \overline{U}_{\hat{S}}(g). \tag{3.26}$$

8. *The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.*

Figure 3.4 depicts this quantum algorithm. The overall state after Step 3 of Algorithm 2 is

$$V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E. \tag{3.27}$$

The result of Step 6 is to prepare the uniform superposition state $|+\rangle_C$, which is defined in (3.10).

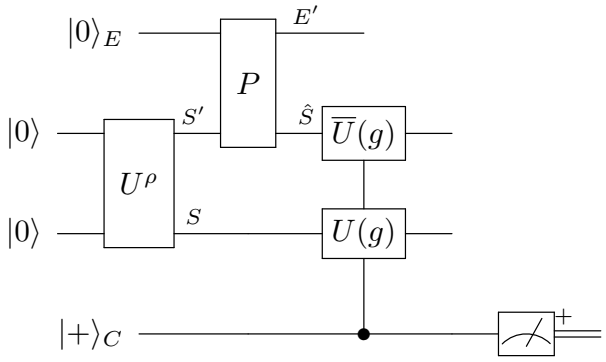


Figure 3.4. Quantum circuit to implement Algorithm 2. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 2 tests whether the state ρ_S is G-symmetric, as defined in Example 1.4.1. Its acceptance probability is equal to the maximum G-symmetric fidelity, as defined in (3.23).

After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C \left(U_S(g) \otimes \overline{U}_{\hat{S}}(g) \right) V_{S'E \to \hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E. \tag{3.28}$$

For a fixed unitary $V_{S'E \to \hat{S}E'}$, the probability of accepting, by following the same reasoning in (3.12)–(3.13), is equal to

$$\left\| \Pi^G_{S\hat{S}} V_{S'E \to \hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2, \tag{3.29}$$

where

$$\Pi^G_{S\hat{S}} := \frac{1}{|G|} \sum_{g \in G} U_S(g) \otimes \overline{U}_{\hat{S}}(g). \tag{3.30}$$

Since the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09, VW16], the prover optimizes over every unitary $V_{S'E \to \hat{S}E'}$ and the acceptance probability of Algorithm 2 is given by

$$\max_{V_{S'E \to \hat{S}E'}} \left\| \Pi^G_{S\hat{S}} V_{S'E \to \hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2. \tag{3.31}$$

The main idea behind Algorithm 2 is that if the state ρ_S possesses the symmetry in (3.22), then Theorem 1.4.1 (with trivial reference system R) guarantees the existence of a purification $\phi_{S\hat{S}}$ of ρ_S such that

$$|\phi\rangle_{S\hat{S}} = \Pi^G_{S\hat{S}}|\phi\rangle_{S\hat{S}}. \tag{3.32}$$

Since all purifications of a quantum state are related by a unitary acting on the purifying system (see, e.g., [Wil17]), the prover should be able to apply a unitary taking the purification $|\psi\rangle_{S'S}$ to the purification $|\psi\rangle_{S\hat{S}}$. After the prover sends back the system $\hat{S}$, the verifier then performs a quantum-computational test to determine if the condition in (3.32) holds.

Theorem 3.2.2 *The acceptance probability of Algorithm 2 is equal to the maximum G-symmetric fidelity in* (3.23)*, i.e.,*

$$\max_{V_{S'E\to\hat{S}E'}} \left\| \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right\|_2^2 = \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{3.33}$$

Proof. Recall the following property of the norm of an arbitrary vector $|\varphi\rangle$:

$$\||\varphi\rangle\|_2^2 = \max_{|\phi\rangle:\||\phi\rangle\|_2=1} |\langle\phi|\varphi\rangle|^2 . \tag{3.34}$$

This follows from the Cauchy–Schwarz inequality and the conditions for saturating it. The formula in (3.34) implies that

$$\max_{V_{S'E\to\hat{S}E'}} \left\| \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right\|_2^2 = \max_{V_{S'E\to\hat{S}E'}, |\phi\rangle_{S\hat{S}E'}} \left| \langle\phi|_{S\hat{S}E'} \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right|^2 . \tag{3.35}$$

For positive semi-definite operators ω_A and τ_A and corresponding rank-one operators ψ^ω_{RA} and ψ^τ_{RA} satisfying

$$\mathrm{Tr}_R[\psi^\omega_{RA}] = \omega_A, \tag{3.36}$$

$$\mathrm{Tr}_R[\psi^{\tau}_{RA}] = \tau_A, \tag{3.37}$$

Uhlmann's theorem [Uhl76] states that

$$\left\|\sqrt{\omega_A}\sqrt{\tau_A}\right\|_1^2 = \max_{V_R} \left|\langle\psi^{\omega}|_{RA}\,(V_R \otimes I_A)\,|\psi^{\tau}\rangle_{RA}\right|^2, \tag{3.38}$$

where the optimization is over every unitary V_R acting on the reference system R. Applying this theorem to (3.35) with the identifications $R \leftrightarrow \hat{S}E' \simeq S'E$ and $S \leftrightarrow A$ and noting that

$$\mathrm{Tr}_{S'E}[|\psi\rangle\langle\psi|_{S'S} \otimes |0\rangle\langle 0|_E] = \rho_S, \tag{3.39}$$

$$\mathrm{Tr}_{\hat{S}E'}[\Pi^G_{S\hat{S}}|\phi\rangle\langle\phi|_{S\hat{S}E'}\Pi^G_{S\hat{S}}] = \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma_{S\hat{S}'}\Pi^G_{S\hat{S}}], \tag{3.40}$$

where $\sigma_{S\hat{S}'}$ is a quantum state satisfying $\sigma_{S\hat{S}'} = \mathrm{Tr}_{E'}[|\phi\rangle\langle\phi|_{S\hat{S}E'}]$, we conclude that

$$\max_{V_{S'E\to\hat{S}E'},|\phi\rangle_{S\hat{S}E'}} \left|\langle\phi|_{S\hat{S}E'}\Pi^G_{S\hat{S}}V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E\right|^2 = \max_{\sigma_{S\hat{S}'}} F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma_{S\hat{S}'}\Pi^G_{S\hat{S}}]), \tag{3.41}$$

with the optimization in the last line over every quantum state $\sigma_{S\hat{S}'}$.

We finally prove that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma_{S\hat{S}'}\Pi^G_{S\hat{S}}]) = \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{3.42}$$

To prove this equality, we will first show that the left-hand side of (3.42) is greater than or equal to the right-hand side, and then we shall show it must also be less than or equal to the right-hand side. To justify the forward direction of (3.42), let $\sigma_S \in \mathrm{Sym}_G$, and pick $\sigma_{S\hat{S}}$ to be the purification $\varphi_{S\hat{S}}$ of ρ_S from Theorem 1.4.1 (with systems $R\hat{R}$ trivial) that satisfies

$$\Pi^G_{S\hat{S}}\varphi_{S\hat{S}}\Pi^G_{S\hat{S}} = \varphi_{S\hat{S}}. \tag{3.43}$$

Observe that

$$\mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\varphi_{S\hat{S}}\Pi^G_{S\hat{S}}] = \mathrm{Tr}_{\hat{S}}[\varphi_{S\hat{S}}] = \sigma_S, \tag{3.44}$$

and so, given that $\sigma_S \in \mathrm{Sym}_G$ is arbitrary, it follows that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) \geq \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S)\,. \tag{3.45}$$

To justify the reverse direction in (3.42), let $\sigma_{S\hat{S}}$ be an arbitrary state. If $\sigma_{S\hat{S}'}$ is outside of the subspace onto which $\Pi^G_{S\hat{S}}$ projects, then $\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}} = 0$ and the fidelity in (3.41) is equal to zero. Let us suppose that this is not the case, and let us define

$$\sigma'_{S\hat{S}} \coloneqq \frac{1}{p} \Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}, \tag{3.46}$$

$$p \coloneqq \mathrm{Tr}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'}]. \tag{3.47}$$

Then consider the following fidelity,

$$F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) = pF(\rho_S, \tau_S) \tag{3.48}$$

$$\leq F(\rho_S, \tau_S), \tag{3.49}$$

where

$$\tau_S \coloneqq \mathrm{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}], \tag{3.50}$$

and we used the fact that $p \leq 1$. If $\tau_S \in \mathrm{Sym}_G$, we will have completed our argument. To see that this is true, we can perform a series of manipulations using the definition of τ_S as follows

$$\tau_S = \mathrm{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}] \tag{3.51}$$

$$= \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma'_{S\hat{S}} \Pi^G_{S\hat{S}}] \tag{3.52}$$

$$= \mathrm{Tr}_{\hat{S}}[\left(U_S \otimes \overline{U}_{\hat{S}}\right) \Pi^G_{S\hat{S}} \sigma'_{S\hat{S}} \Pi^G_{S\hat{S}} \left(U_S \otimes \overline{U}_{\hat{S}}\right)^\dagger] \tag{3.53}$$

$$= U_S \,\mathrm{Tr}_{\hat{S}}[\overline{U}_{\hat{S}} \Pi^G_{S\hat{S}} \sigma'_{S\hat{S}} \Pi^G_{S\hat{S}} \overline{U}^\dagger_{\hat{S}}] U^\dagger_S \tag{3.54}$$

$$= U_S \,\mathrm{Tr}_{\hat{S}}[\overline{U}^\dagger_{\hat{S}} \overline{U}_{\hat{S}} \Pi^G_{S\hat{S}} \sigma'_{S\hat{S}} \Pi^G_{S\hat{S}}] U^\dagger_S \tag{3.55}$$

$$= U_S \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma'_{S\hat{S}} \Pi^G_{S\hat{S}}] U_S^\dagger \tag{3.56}$$

$$= U_S(g) \operatorname{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}] U_S^\dagger(g) \tag{3.57}$$

$$= U_S(g) \tau_S U_S^\dagger(g). \tag{3.58}$$

where we have used the shorthand $U_S \equiv U_S(g)$ and $\overline{U}_{\hat{S}} \equiv \overline{U}_{\hat{S}}(g)$. Since the equality $\tau_S = U_S(g)\tau_S U_S^\dagger(g)$ holds for all $g \in G$, it follows that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) \leq \max_{\tau_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{3.59}$$

■

Now let us return to our example of D_3, and use this construction to decompress from proofs for a bit. For this circuit, we use the same unitary U_d to prepare the superposition $|+\rangle_C$, and the same mapping of control states to group elements. Then the circuit to test for G-symmetry (or D_3-symmetry, as it were) is shown in Figure 3.5.

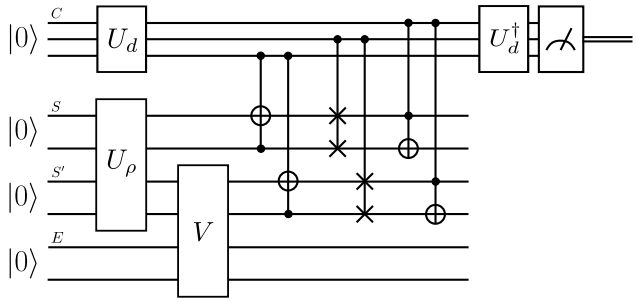


Figure 3.5. Quantum circuit implementing Algorithm 2 to test G-symmetry in the case that the group G is the triangular dihedral group. Compared to Figure 3.4, the systems S and S' are two qubits each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$. Both the SWAP and CNOT gates have no imaginary entries, and thus they are equal to their own complex conjugates.

Now, in Figure 3.5, note that we have introduced a prover in the form of a unitary V. This prover has access both to the purifying system of our state as well as the environment. As discussed before, provers in QIP(2) have unbounded computational power, and so it may feel like

we have reached a wall impeding our progress. Clearly, there is no way incorporate any physical implementation of V as required by complexity theory—so instead, we must bend the rules around this definition. For practical implementations of such algorithms, a variational quantum algorithm (VQA) can stand in as a lower-bound version of the prover. In [LRW21], the behaviors of these algorithms are shown explicitly. (These VQA results are surpressed from this text but are nonetheless impressive in demonstrating the power of machine learning to approximate all-powerful wizards as the need may be.)

Remark 1 (Testing incoherence) *We would now like to discuss a particular application of our algorithm: testing for incoherence. Testing the incoherence of a quantum state, in the sense of [BCP14, SAP17], is a special case of testing G-symmetry. To see this, pick G to be the cyclic group over d elements (C_d) with unitary representation $\{Z(z)\}_z$, where $Z(z)$ is the generalized Pauli phase-shift unitary, defined as*

$$Z(z) := \sum_{j=0}^{d-1} e^{2\pi i j z/d} |j\rangle\langle j|. \tag{3.60}$$

A state is symmetric with respect to this group if the condition in (3.22) *holds. This condition is equivalent to*

$$\rho_S = \frac{1}{|G|} \sum_{g \in G} U_S(g) \rho_S U_S(g)^\dagger. \tag{3.61}$$

For the choice mentioned above, this condition holds if and only if the state ρ_S is diagonal in the incoherent basis, i.e., if it can be written as $\rho_S = \sum_j p(j)|j\rangle\langle j|$, where $p(j)$ is a probability distribution. Thus, Algorithm 2 can be used to test the incoherence of quantum states.

3.2.3. Testing G-Bose Symmetric Extendibility

We now describe an algorithm for testing G-Bose symmetric extendibility of a quantum state ρ_S, as defined in Definition 1.4.2. The algorithm bears some similarities with Algorithms 1

and 2. Like Algorithm 2, it involves an interaction between a verifier and a prover. We prove that its acceptance probability is equal to the maximum G-BSE fidelity:

$$\max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S), \tag{3.62}$$

where BSE_G is the set of G-Bose symmetric extendible states:

$$\mathrm{BSE}_G := \left\{ \begin{array}{c} \sigma_S : \exists \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}),\ \mathrm{Tr}_R[\omega_{RS}] = \sigma_S, \\ \\ \omega_{RS} = U_{RS}(g)\omega_{RS}, \forall g \in G \end{array} \right\}. \tag{3.63}$$

Thus, the algorithm endows the maximum G-BSE fidelity with an operational meaning. Note that the condition $\omega_{RS} = U_{RS}(g)\omega_{RS}\ \forall g \in G$ is equivalent to

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}, \tag{3.64}$$

where

$$\Pi^G_{RS} := \frac{1}{|G|}\sum_{g\in G} U_{RS}(g)\,, \tag{3.65}$$

as before.

The algorithm is highly similar to Algorithm 2, but we list it here for completeness. Let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the circuit U^ρ prepares this purification of ρ_S.

Algorithm 3 (G-BSE test) *The algorithm proceeds as follows:*

1. *The verifier uses the circuit provided to prepare the state $|\psi\rangle_{S'S}$.*
2. *The verifier transmits the purifying system S' to the prover.*
3. *The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to RE'}$.*
4. *The prover sends the system R back to the verifier.*

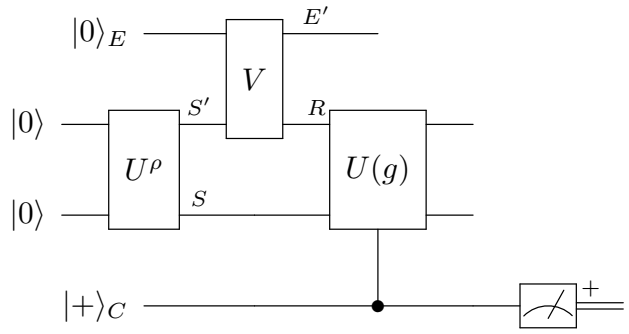


Figure 3.6. Quantum circuit to implement Algorithm 3. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 3 tests whether the state ρ_S is G-Bose symmetric extendible, as defined in Definition 1.4.2. Its acceptance probability is equal to the maximum G-BSE fidelity, as defined in (3.62).

5. *The verifier prepares a register C in the state $|0\rangle_C$.*

6. *The verifier acts on register C with a quantum Fourier transform or equivalent sequence of gates.*

7. *The verifier performs the following controlled unitary:*

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_{RS}(g), \tag{3.66}$$

8. *The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.*

Figure 3.6 depicts this quantum algorithm. The overall state after Step 3 is

$$V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E. \tag{3.67}$$

Step 6 prepares the uniform superposition state $|+\rangle_C$, which is defined in (3.10). After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C \left(U_{RS}(g)\right) V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E. \tag{3.68}$$

The last step can be understood as the verifier projecting the register C onto the state $|+\rangle_C$.

The probability of accepting, following the same reasoning as before, is equal to

$$\left\|\Pi_{RS}^{G} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_{E}\right\|_2^2, \tag{3.69}$$

where Π_{RS}^{G} is defined in (3.65). As before, the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09, VW16], and so the prover optimizes over every unitary $V_{S'E\to\hat{S}E'}$. The acceptance probability of Algorithm 3 is then given by

$$\max_{V_{S'E\to RE'}} \left\|\Pi_{RS}^{G} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_{E}\right\|_2^2. \tag{3.70}$$

For completeness, we provide our proof in Appendix B.2, but do not include it here as it is highly similar to the proof given for Theorem 3.2.2;

Theorem 3.2.3 *The maximum acceptance probability of Algorithm 3 is equal to the maximum G-BSE fidelity in* (3.62)*, i.e.,*

$$\max_{V_{S'E\to RE'}} \left\|\Pi_{RS}^{G} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_{E}\right\|_2^2 = \max_{\sigma_S\in \mathrm{BSE}_G} F(\rho_S,\sigma_S), \tag{3.71}$$

where the set BSE_G *is defined in* (3.63)*.*

3.2.4. Testing G-Symmetric Extendibility

The final algorithm that we introduce tests whether a state ρ_S is G-symmetric extendible (recall Definition 1.4.1). Similar to the algorithms in the previous sections, not only does it decide whether ρ_S is G-symmetric extendible, but it also quantifies how similar it is to a state in the set of G-symmetric extendible states. The acceptance probability is equal to the *maximum G-symmetric extendible fidelity*:

$$\max_{\sigma_S\in \mathrm{SymExt}_G} F(\rho_S,\sigma_S), \tag{3.72}$$

where

$$\mathrm{SymExt}_G := \left\{ \begin{array}{c} \sigma_S : \exists \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}), \mathrm{Tr}_R[\omega_{RS}] = \sigma_S \\ \\ \omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \ \forall g \in G \end{array} \right\}. \tag{3.73}$$

We again operate in the model of QIP(2), in which a verifier interacts with a prover via two messages.

We again list the algorithm for completeness, noting its similarity to the previous algorithms. Let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the circuit U^ρ prepares this purification of ρ_S.

Algorithm 4 *The algorithm proceeds as follows:*

1. *The verifier uses the circuit U^ρ to prepare the state $|\psi\rangle_{S'S}$, which is a purification of the state ρ_S.*
2. *The verifier transmits the purifying system S' to the prover.*
3. *The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to R\hat{R}\hat{S}E'}$.*
4. *The prover sends the systems $R\hat{R}\hat{S}$ back to the verifier.*
5. *The verifier prepares a register C in the state $|0\rangle_C$.*
6. *The verifier acts on register C with a quantum Fourier transform.*
7. *The verifier performs the following controlled unitary:*
$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g), \tag{3.74}$$
8. *The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.*

Figure 3.7 depicts this quantum algorithm. After Step 3, the overall state is

$$V_{S'E\to R\hat{R}\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E. \tag{3.75}$$

Step 5 prepares the uniform superposition state $|+\rangle_C$, which is defined in (3.10). After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C \left(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)\right) V|\psi\rangle_{S'S}|0\rangle_E, \tag{3.76}$$

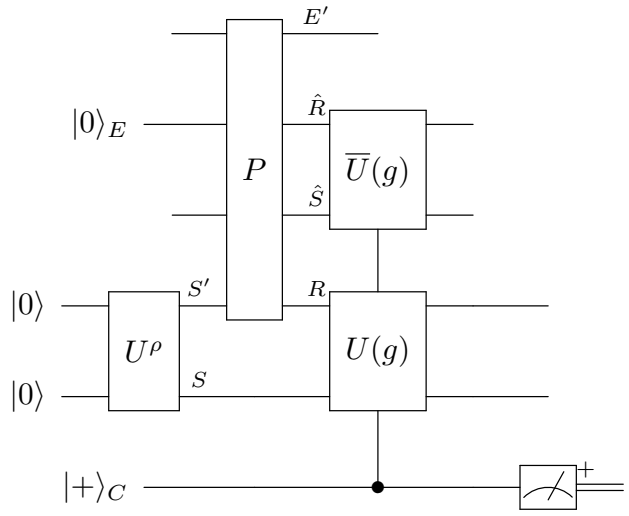


Figure 3.7. Quantum circuit to implement Algorithm 4. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 4 tests whether the state ρ_S is G-symmetric extendible, as defined in Definition 1.4.1. Its acceptance probability is equal to the maximum G-symmetric extendible fidelity, as defined in (3.72).

where $V \equiv V_{S'E\to R\hat{R}\hat{S}E'}$. The last step can be understood as the verifier projecting the register C onto the state $|+\rangle_C$.

The probability of accepting is equal to

$$\left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2, \tag{3.77}$$

where $\Pi^G_{RS\hat{R}\hat{S}}$ is defined in (1.46). As before, the prover optimizes over every unitary $V_{S'E\to R\hat{R}\hat{S}E'}$. The acceptance probability of Algorithm 4 is then given by

$$\left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2. \tag{3.78}$$

Our proof of the following theorem is similar to the proof given for Theorem 3.2.2. For completeness, we provide our proof in Appendix B.3.

Theorem 3.2.4 *The maximum acceptance probability of Algorithm 4 is equal to the maximum*

G-symmetric extendible fidelity in (3.72)*, i.e.,*

$$\max_{V_{S'E\to R\hat{R}\hat{S}E'}} \left\| \Pi^{G}_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_{E} \right\|_2^2 = \max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S), \tag{3.79}$$

where the set SymExt_G *is defined in* (3.73)*.*

Once again, we return to our familiar friend, the triangular dihedral group, to demonstrate the construction of this algorithm. As before, we use the same unitary U_d to prepare the superposition $|+\rangle_C$ and the same mapping of control states to group elements. Then the circuit to test for G-Bose symmetric extendibility is shown in Figure 3.8. Like it's predecessor, it employs a unitary V to indicate the presense of a prover (or VQA, as the case may be.)

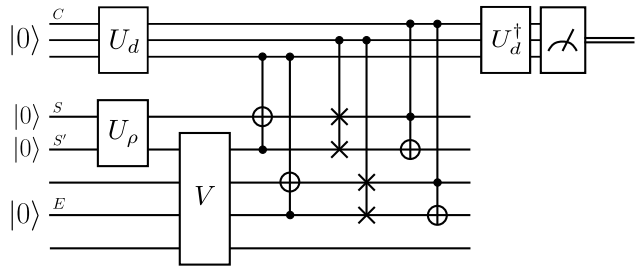


Figure 3.8. Quantum circuit implementing Algorithm 4 to test G-symmetric extendibility in the case that the group G is the triangular dihedral group. Compared to Figure 3.7, the systems S and S' are one qubit each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$. Both the SWAP and CNOT gates have no imaginary entries and thus are equal to their own complex conjugates.

Table 3.1. Summary of the various symmetry tests proposed in Section 3.2 and their acceptance probabilities. For more details, see Theorems 3.2.1, 3.2.2, 3.2.3, and 3.2.4.

Test	Algorithm	Acceptance Probability
G-Bose symmetry	1	$\max_{\sigma\in \text{B-Sym}_G} F(\rho,\sigma)$
G-symmetry	2	$\max_{\sigma\in \text{Sym}_G} F(\rho,\sigma)$
G-Bose symmetric extendibility	3	$\max_{\sigma\in \text{BSE}_G} F(\rho,\sigma)$
G-symmetric extendibility	4	$\max_{\sigma\in \text{SymExt}_G} F(\rho,\sigma)$

3.3. Tests of k-Extendibility of States and Covariance Symmetry of Channels

The theory developed in Section 3.2 is rather abstract, despite the peppering of D_3 as a demonstrable. It is natural to wonder whether these algorithms may find practical use in physics.

In the forthcoming subsections, we address this concern by applying our algorithm to test for extendibility of bipartite and multipartite quantum states and to test for covariance symmetry of a quantum channel. The former two cases are used in tests of separability, and the latter we have already employed in Chapter 2.

3.3.1. Separability Test for Pure Bipartite States

We illustrate the G-Bose symmetry test from Section 3.2.1 on a case of interest: deciding whether a pure bipartite state is entangled. This problem is known to be BQP-complete [GHMW15], and one can decide it by means of the SWAP test as considered in [HM10]. The SWAP test as a quantum computational method of quantifying entanglement has been further studied in recent work [FKS21, BGCC21].

First, let us establish that the above notions of symmetry generalize both k-extendibility of bipartite states and G-symmetry of unipartite states by introducing both as examples of our algorithm.

Example 3.3.1 (k-extendible) *Recall that a bipartite state ρ_{AB} is k-extendible [Wer89, DPS02, DPS04] if there exists an extension state $\omega_{AB_1\cdots B_k}$ such that*

$$\mathrm{Tr}_{B_2\cdots B_k}[\omega_{AB_1\cdots B_k}] = \rho_{AB} \tag{3.80}$$

and

$$\omega_{AB_1\cdots B_k} = W_{B_1\cdots B_k}(\pi)\omega_{AB_1\cdots B_k}W_{B_1\cdots B_k}(\pi)^\dagger, \tag{3.81}$$

for all $\pi \in S_k$, where each system $B_1, \ldots, B_k$ is isomorphic to the system B and $W_{B_1\cdots B_k}(\pi)$ is a unitary representation of the permutation $\pi \in S_k$, with S_k the symmetric group. Then the established notion of k-extendibility is a special case of G-symmetric extendibility, in which we set

$$S = AB_1, \tag{3.82}$$

$$R = B_2 \cdots B_k, \tag{3.83}$$

$$G = S_k, \tag{3.84}$$

$$U_{RS}(g) = I_A \otimes W_{B_1 \cdots B_k}(\pi). \tag{3.85}$$

Example 3.3.2 (k-Bose-extendible) *A bipartite state ρ_{AB} is k-Bose-extendible if there exists an extension state $\omega_{AB_1 \cdots B_k}$ such that*

$$\mathrm{Tr}_{B_2 \cdots B_k}[\omega_{AB_1 \cdots B_k}] = \rho_{AB}\,, \tag{3.86}$$

and

$$\omega_{AB_1 \cdots B_k} = \Pi^{\mathrm{Sym}}_{B_1 \cdots B_k} \omega_{AB_1 \cdots B_k} \Pi^{\mathrm{Sym}}_{B_1 \cdots B_k}, \tag{3.87}$$

where

$$\Pi^{\mathrm{Sym}}_{B_1 \cdots B_k} := \frac{1}{k!} \sum_{\pi \in S_k} W_{B_1 \cdots B_k}(\pi) \tag{3.88}$$

is the projection onto the symmetric subspace. Thus, k-Bose-extendibility is a special case of G-Bose-symmetric extendibility under the identifications in (3.82)–(3.85)*.*

Let ψ_{AB} be a pure bipartite state, and let $\psi_{AB}^{\otimes k}$ denote k copies of it. Then we can consider the permutation unitaries $W_{B_1 \cdots B_k}(\pi)$ from Example 3.3.1. This example is a special case of Bose G-symmetry with the identifications

$$S \leftrightarrow A_1 B_1 \cdots A_k B_k, \tag{3.89}$$

$$U_S(g) \leftrightarrow I_{A_1 \cdots A_k} \otimes W_{B_1 \cdots B_k}(\pi). \tag{3.90}$$

The acceptance probability of Algorithm 1 is equal to

$$\mathrm{Tr}[\Pi^{\mathrm{Sym}}_{B_1 \cdots B_k} \rho_B^{\otimes k}], \tag{3.91}$$

where the projection $\Pi^{\mathrm{Sym}}_{B_1\cdots B_k}$ onto the symmetric subspace is defined in (3.88) and $\rho_B := \mathrm{Tr}_A[\psi_{AB}]$. For $k = 2$, this reduces to the well known SWAP test with acceptance probability

$$p^{(2)}_{\mathrm{acc}} := \frac{1}{2}\left(1 + \mathrm{Tr}[\rho_B^2]\right). \tag{3.92}$$

For $k = 3$, the acceptance probability is

$$p^{(3)}_{\mathrm{acc}} := \frac{1}{6}\left(1 + 3\,\mathrm{Tr}[\rho_B^2] + 2\,\mathrm{Tr}[\rho_B^3]\right). \tag{3.93}$$

For $k = 4$, the acceptance probability is

$$p^{(4)}_{\mathrm{acc}} := \frac{1}{24}\left(1 + 6\,\mathrm{Tr}[\rho_B^2] + 3\left(\mathrm{Tr}[\rho_B^2]\right)^2 + 8\,\mathrm{Tr}[\rho_B^3] + 6\,\mathrm{Tr}[\rho_B^4]\right). \tag{3.94}$$

We conclude that

$$p^{(2)}_{\mathrm{acc}} \geq p^{(3)}_{\mathrm{acc}} \geq p^{(4)}_{\mathrm{acc}}, \tag{3.95}$$

because $\mathrm{Tr}[\rho^k] = \sum_j \lambda_j^k$, where the eigenvalues of ρ are $\{\lambda_j\}_j$, and for all $x, y \in [0, 1]$,

$$\frac{1}{2}\left(x + x^2\right) \geq \frac{1}{6}\left(x + 3x^2 + 2x^3\right) \tag{3.96}$$

$$\geq \frac{1}{24}\left(x + 6x^2 + 3x^2y + 8x^3 + 6x^4\right). \tag{3.97}$$

The inequalities in (3.95) imply that the tests become more difficult to pass, or stringent, as k increases. It may be expected that this trend of decreasing acceptance probability continues as k increases. Indeed, in [BLW22], we showed that this was the case; however, the proof requires additional machinery not yet developed, and so we will readdress this concern in Chapter 4.

We can interpret these findings in two different ways. For each k, the rejection probability $1 - p^{(k)}_{\mathrm{acc}}$ can be understood as an entanglement measure for pure bipartite states, similar to how the linear entropy $1 - \mathrm{Tr}[\rho_B^2]$ is interpreted as an entanglement measure of the reduced state ρ_B. Indeed, these quantities are non-increasing under local operations and classical communication

that take pure states to pure states, as every Rényi entropy of the reduced state is an entanglement measure for pure bipartite states [HHHH09]. Another interpretation is that, if using these tests to decide if a given pure state is product or entangled, a decision can be determined with fewer repetitions of the basic test by using tests with higher values of k.

3.3.2. Separability test for Pure Multipartite States

We can generalize the test from the previous section to one for pure multipartite entanglement. Let $\psi_{A_1\cdots A_m}$ be a multipartite pure state, and let $\psi^{\otimes k}_{A_1\cdots A_m}$ denote k copies of it. For $i \in \{1,\ldots,m\}$ and $\pi_i \in S_k$, let $W_{A_{i,1}\cdots A_{i,k}}(\pi_i)$ denote a permutation unitary, where i is an index for the i-th party, and the notation $A_{i,j}$ for $j \in \{1,\ldots,k\}$ indicates the jth system of the ith party. This example is a special case of G-Bose symmetry with the identifications:

$$S \leftrightarrow A_{1,1}\cdots A_{1,k}\cdots A_{m,1}\cdots A_{m,k}, \tag{3.98}$$

$$U_S(g) \leftrightarrow \bigotimes_{i=1}^{m} W_{A_{i,1}\cdots A_{i,k}}(\pi_i), \tag{3.99}$$

$$G \leftrightarrow \overbrace{S_k \times \cdots \times S_k}^{m \text{ times}}, \tag{3.100}$$

$$g \leftrightarrow (\pi_1,\ldots,\pi_m), \tag{3.101}$$

where $\times$ denotes the direct product of groups. The G-Bose symmetry test from Section 3.2.1 has the following acceptance probability in this case:

$$\mathrm{Tr}\left[\bigotimes_{i=1}^{m} \Pi^{\mathrm{Sym}}_{A_{i,1}\cdots A_{i,k}} \psi^{\otimes k}_{A_1\cdots A_m}\right]. \tag{3.102}$$

For $k = 2$, this test is known to be a test of multipartite pure-state entanglement [HM10], which has been considered in more recent works [FKS21, BGCC21]. As far as we aware, the test proposed above, for larger values of k, has not been considered previous to our work in [LRW21].

Presumably, as was the case for the bipartite entanglement test mentioned above, the multipartite test is such that it becomes easier to detect an entangled state as k increases.

3.3.3. k-Bose Extendibility Test for Bipartite States

We now demonstrate how the test for G-Bose symmetric extendibility from Section 3.2.3 can realize a test for k-Bose extendibility of a bipartite state. Since every separable state is k-Bose extendible, this test is then indirectly a test for separability. To see this in detail, recall that a bipartite state σ_{AB} is separable if it can be written as a convex combination of pure product states [HHHH09, KW20]:

$$\sigma_{AB} = \sum_x p_X(x) \psi_A^x \otimes \phi_B^x, \tag{3.103}$$

where p_X is a probability distribution and $\{\psi_A^x\}_x$ and $\{\phi_B^x\}_x$ are sets of pure states. A k-Bose extension for this state is as follows:

$$\omega_{AB_1 \cdots B_k} = \sum_x p_X(x) \psi_A^x \otimes \phi_{B_1}^x \otimes \cdots \otimes \phi_{B_k}^x. \tag{3.104}$$

By making the identifications discussed in Example 3.3.2, it follows from Theorem 3.2.3 that the test from Section 3.2.3 is a test for k-Bose extendibility. For an input state ρ_{AB}, the acceptance probability of Algorithm 3 is equal to the maximum k-Bose extendible fidelity

$$\max_{\omega_{AB} \in k\text{-BE}} F(\rho_{AB}, \omega_{AB}), \tag{3.105}$$

where k-BE denotes the set of k-Bose extendible states, as defined in Example 3.3.2.

3.3.4. k-Extendibility Test for Bipartite States

In this section, we discuss how the test for G-symmetric extendibility from Section 3.2.4 can realize a test for k-extendibility of a bipartite state. Due to the known connections between k-extendibility and separability [CKMR07, BCY11a, BCY11b, BH13], this test is an indirect

test for separability of a bipartite state, a case we introduce here and expand upon in Chapter 4. Since every separable state is k-Bose extendible, as discussed in Section 3.3.3, and every k-Bose extendible state is k-extendible, it follows that every separable state is k-extendible.

By making the identifications discussed in Example 3.3.1, it follows from Theorem 3.2.4 that the test from Section 3.2.4 is a test for k-extendibility. For an input state ρ_{AB}, the acceptance probability of Algorithm 4 is equal to the maximum k-extendible fidelity

$$\max_{\omega_{AB} \in k\text{-E}} F(\rho_{AB}, \omega_{AB}), \tag{3.106}$$

where k-E denotes the set of k-extendible states, as defined in Example 3.3.1.

As far as we are aware, this quantum computational test for k-extendibility is original to our work in [LRW21]; however, inspired by the approach from [HMW13, HMW14]. It was argued in [HMW13, HMW14] that the acceptance probability of the test there is bounded from above by the maximum k-extendible fidelity, which is consistent with the fact that the set of k-Bose extendible states is contained in the set of k-extendible states and our observation here that the acceptance probability of the test in [HMW13, HMW14] is equal to the maximum k-Bose extendible fidelity.

3.3.5. Extendibility Tests for Multipartite States

We now would like to discuss briefly how the tests from Sections 3.2.3 and 3.2.4 apply to the multipartite case, using identifications similar to those in (3.98)–(3.101).

First, let us recall the definition of multipartite extendibility [DPS05]. Let $\sigma_{A_1 \cdots A_m}$ be a multipartite state. Such a state is $(k_1, \ldots, k_m)$-extendible if there exists a state $\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}$ such that

$$\sigma_{A_1 \cdots A_m} = \operatorname{Tr}_{A_{1,2} \cdots A_{1,k_1} \cdots A_{m,2} \cdots A_{m,k_m}} [\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}] \tag{3.107}$$

and

$$\omega_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}}$$

$$= W^{\pi}_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} \omega_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} (W^{\pi}_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}})^{\dagger}, \quad (3.108)$$

for all π, where $\pi = (\pi_1, \ldots, \pi_m) \in S_{k_1} \times \cdots \times S_{k_m}$ and

$$W^{\pi}_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} := \bigotimes_{i=1}^{m} W^{\pi_i}_{A_{i,1}\cdots A_{i,k_i}}. \quad (3.109)$$

A multipartite state is $(k_1, \ldots, k_m)$-Bose extendible if there exists a state $\omega_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}}$ such that (3.107) holds and

$$\omega_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} =$$

$$\Pi_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} \omega_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} \Pi_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}}, \quad (3.110)$$

where

$$\Pi_{A_{1,1}\cdots A_{1,k_1}\cdots A_{m,1}\cdots A_{m,k_m}} := \bigotimes_{i=1}^{m} \Pi^{\mathrm{Sym}}_{A_{i,1}\cdots A_{i,k_i}}, \quad (3.111)$$

$$\Pi^{\mathrm{Sym}}_{A_{i,1}\cdots A_{i,k_i}} := \frac{1}{k_i!} \sum_{\pi_i \in S_{k_i}} W^{\pi_i}_{A_{i,1}\cdots A_{i,k_i}}. \quad (3.112)$$

By making the identifications

$$S \leftrightarrow A_{1,1} \cdots A_{m,1}, \quad (3.113)$$

$$R \leftrightarrow A_{1,2} \cdots A_{1,k_1} \cdots A_{m,2} \cdots A_{m,k_m} \quad (3.114)$$

$$U_S(g) \leftrightarrow \bigotimes_{i=1}^{m} W_{A_{i,1}\cdots A_{i,k_i}}(\pi_i) \quad (3.115)$$

$$G \leftrightarrow S_{k_1} \times \cdots \times S_{k_m}, \quad (3.116)$$

$$g \leftrightarrow (\pi_1, \ldots, \pi_m), \quad (3.117)$$

it follows that Algorithm 3 is a test for multipartite $(k_1, \ldots, k_m)$-Bose extendibility of a state $\rho_{A_1 \cdots A_m}$, with acceptance probability equal to

$$\max_{\omega_{A_1 \cdots A_m} \in (k_1, \ldots, k_m)\text{-BE}} F(\rho_{A_1 \cdots A_m}, \omega_{A_1 \cdots A_m}), \tag{3.118}$$

and Algorithm 4 is a test for multipartite $(k_1, \ldots, k_m)$-extendibility of a state $\rho_{A_1 \cdots A_m}$, with acceptance probability equal to

$$\max_{\omega_{A_1 \cdots A_m} \in (k_1, \ldots, k_m)\text{-E}} F(\rho_{A_1 \cdots A_m}, \omega_{A_1 \cdots A_m}), \tag{3.119}$$

where $(k_1, \ldots, k_m)$-BE and $(k_1, \ldots, k_m)$-E denote the sets of $(k_1, \ldots, k_m)$-Bose extendible and $(k_1, \ldots, k_m)$-extendible states, respectively.

3.3.6. Testing Covariance Symmetry of a Quantum Channel

We can also use the test from Algorithm 2 to test for covariance symmetry of a quantum channel. We have already given a definition for covariance symmetry in Chapter 1, Section 1.4.2, and we have further already demonstrated the usefulness of channel symmetry in Chapter 2 in Section 2.2. Therefore, we will skip its redefinition here and instead focus on generalizing the approach given in Chapter 2.

We know from previous sections that a channel is covariant in the sense above if and only if its Choi state is invariant in the following sense [CDP09, Eq. (59)]:

$$\Phi^{\mathcal{N}}_{RB} = (\overline{\mathcal{U}}_R(g) \otimes \mathcal{V}_B(g))(\Phi^{\mathcal{N}}_{RB}) \quad \forall g \in G, \tag{3.120}$$

as in (1.72). (All relevant terms in this definition are given therein.) We will once again employ this definition to give a test for the covariance symmetry of a quantum channel.

Suppose now that a circuit is available that generates the channel $\mathcal{N}_{A \to B}$. Similar to the first assumption in Section 3.2, we suppose that the circuit realizes a unitary channel $\mathcal{W}_{AE' \to BE}$

that extends the original channel, in the sense that

$$\mathcal{N}_{A\to B}(\omega_A) = (\mathrm{Tr}_E \circ \mathcal{W}_{AE'\to BE})(\omega_A \otimes |0\rangle\langle 0|_{E'}). \tag{3.121}$$

Then to decide whether the channel is covariant, we send in one share of a maximally-entangled state to the unitary extension channel, such that the overall state is

$$\mathcal{W}_{AE'\to BE}(\Phi_{RA} \otimes |0\rangle\langle 0|_{E'}). \tag{3.122}$$

Now making the identifications

$$E \leftrightarrow S', \tag{3.123}$$

$$RB \leftrightarrow S, \tag{3.124}$$

$$\overline{U}_R(g) \otimes V_B(g) \leftrightarrow U_S(g), \tag{3.125}$$

we apply Algorithm 2, and as a consequence of Theorem 3.2.2, the acceptance probability is equal to

$$\max_{\sigma_{RB}\in \mathrm{Sym}_G} F(\Phi^{\mathcal{N}}_{RB}, \sigma_{RB}), \tag{3.126}$$

where

$$\mathrm{Sym}_G := \left\{ \begin{array}{c} \sigma_{RB} \in \mathcal{D}(\mathcal{H}_{RB}) : \\ \\ \sigma_{RB} = (\overline{\mathcal{U}}_R(g) \otimes \mathcal{V}_B(g))(\sigma_{RB}) \; \forall g \in G \end{array} \right\}. \tag{3.127}$$

Thus, the test accepts with probability equal to one if and only if the channel is covariant in the sense of (1.69). Indeed, this is very similar to the construction used in Chapter 2, but builds on the structure of symmetry we have been working with throughout this chapter.

3.4. Resource Theories

In this section, we prove that the various maximum symmetric fidelities proposed in Section 3.2 are proper resource-theoretic monotones, in the sense reviewed in [CG19]. By fulfilling this requirement, we can assert that these fidelities are indeed measures of symmetry as claimed.

To begin with, let us recall the basics of a resource theory (see [CG19, Definition 1]). Let $\mathcal{F}$ be a mapping that assigns a unique set of quantum channels to any arbitrary input and output systems A and B, respectively. We require that $\mathcal{F}$ include the identity channel ($\mathcal{F}(A \to A) = \mathbb{I}_A$) and that, for any three physical systems A, B, and C, any two maps $\mathcal{N}_{A\to B} \in \mathcal{F}(A \to B)$ and $\mathcal{M}_{B\to C} \in \mathcal{F}(B \to C)$ have the transitive property

$$\mathcal{M}_{B\to C} \circ \mathcal{N}_{A\to B} \in \mathcal{F}(A \to C). \tag{3.128}$$

If $\mathcal{F}$ obeys above criteria, then the mapping $\mathcal{F}$ defines the resource theory. Each instance of $\mathcal{F}$ defines a map between two mathematical spaces, and the spaces themselves define the characteristics of the resulting map. The set $\mathcal{F}(\mathbb{C} \to A)$ defines the set of free states—that is, channels from the trivial space ($\mathbb{C}$) to system A should be quantum states. The set $\mathcal{F}(A \to B)$ defines the set of free channels from system A to system B.

How can this be thought of in a more intuitive way? A resource theory defines a set of channels and rules by which they behave. Free states are, in some sense, the "allowed" states in a resource theory; they are the states that can be generated by the channels in the set $\mathcal{F}$. A state that cannot be generated this way is considered a "resource". Conversely, free channels are channels that cannot generate resources that were not already present. In this sense, the cost of creating one of the allowed states is "free", hence the name.

An intuitive picture, which may be helpful to keep in mind, is to think of the resource section of a library. Here, the valuable resource is the knowledge contained within the books. An example of a free channel would be to permute the order of books on the shelf—say we change from the Dewey decimal system to an alphabetic system. We have not gained any resources by this operation, and so it is free. In fact, we could even pile all of the texts on the floor, and, while

certainly inconvenient, the knowledge we have access to will not have changed. However, if instead we were to utilize the inter-library loan system to gain new books, clearly this is not a free operation as the amount of resources have increased. In the following section, we will discuss how asymmetry ties in with this idea of quantifying resources.

3.4.1. Resource Theory of Asymmetry

The resource theory of asymmetry is well established by now [MS13], but to the best of our knowledge, the resource theory of Bose asymmetry had not been defined prior to [LRW21]. We will begin by recalling the resource theory of asymmetry. Afterwards, we establish the resource theory of Bose asymmetry as well as two other generalizations involving unextendibility, which are in turn generalizations of the resource theory of unextendibility proposed in [KDWW19].

Let G be a group, and let $\{U_A(g)\}_{g\in G}$ and $\{V_B(g)\}_{g\in G}$ denote projective unitary representations of G. A channel $\mathcal{N}_{A\to B}$ is a free channel in the resource theory of asymmetry if the following G-covariance symmetry condition holds

$$\mathcal{N}_{A\to B}\circ\mathcal{U}_A(g)=\mathcal{V}_B(g)\circ\mathcal{N}_{A\to B}\qquad\forall g\in G, \tag{3.129}$$

where the unitary channels $\mathcal{U}_A(g)$ and $\mathcal{V}_B(g)$ are respectively defined from $U_A(g)$ and $V_B(g)$ as in (1.70). It then follows that a state σ_A is free in this resource theory if it is G-symmetric such that

$$\sigma_A=\mathcal{U}_A(g)(\sigma_A)\qquad\forall g\in G, \tag{3.130}$$

with a similar definition for the B system; furthermore, the free channels take free states to free states [MS13], in the sense that $\mathcal{N}_{A\to B}(\sigma_A)$ is a free state if $\mathcal{N}_{A\to B}$ is a free channel and σ_A is a free state.

The maximum G-symmetric fidelity is a resource monotone in the following sense:

$$\max_{\sigma_A \in \mathrm{Sym}_G} F(\rho_A, \sigma_A) \leq \max_{\sigma_B \in \mathrm{Sym}_G} F(\mathcal{N}_{A\to B}(\rho_A), \sigma_B). \tag{3.131}$$

This follows from the facts that the fidelity does not decrease under the action of a quantum channel and that free channels take free states to free states.

3.4.2. Resource Theory of Bose Asymmetry

Now we define the resource theory of Bose asymmetry and prove that the acceptance probability $\mathrm{Tr}[\Pi_A^G \rho_A]$ of Algorithm 1 is a resource monotone in this resource theory. This demonstrates that $\mathrm{Tr}[\Pi_A^G \rho_A]$ is a legitimate quantifier of Bose symmetry of a state.

Following the same notation as in Section 3.4.1, recall that a state σ_A is Bose symmetric if the following condition holds

$$\sigma_A = \Pi_A^G \sigma_A \Pi_A^G, \tag{3.132}$$

where Π_A^G is given by (1.39). Similarly, a state τ_B is Bose symmetric if it obeys the same conditions but for the projector Π_B^G specified by $\{V_B(g)\}_{g\in G}$. These are the free states in the resource theory of Bose asymmetry.

To define the resource theory, we need to specify the free channels.

Definition 3.4.1 (Bose symmetric channel) *We define a channel $\mathcal{N}_{A\to B}$ to be a Bose symmetric channel (i.e., free channel) if the following condition holds*

$$(\mathcal{N}_{A\to B})^\dagger (\Pi_B^G) \geq \Pi_A^G, \tag{3.133}$$

where $(\mathcal{N}_{A\to B})^\dagger$ is the Hilbert–Schmidt adjoint of $\mathcal{N}_{A\to B}$ [Wil17, KW20].

Proposition 3.4.1 *Bose symmetric channels include the identity channel and they obey the transitive property in* (3.128)*. Additionally, Bose symmetric states are a special case of Bose symmetric channels when the input space is trivial.*

Proof. When the input and output systems are the same, as well as the unitary representations, it follows that $\Pi_B^G = \Pi_A^G$. Since the identity channel is its own adjoint, we then conclude that (3.133) holds for the identity channel.

Suppose that $\mathcal{N}_{A\to B}$ is a quantum channel that obeys the condition in (3.133). Let $\{W_C(g)\}_{g\in G}$ be a projective unitary representation of G, and suppose that $\mathcal{M}_{B\to C}$ is a Bose symmetric channel satisfying

$$(\mathcal{M}_{B\to C})^\dagger (\Pi_C^G) \geq \Pi_B^G, \tag{3.134}$$

where $\Pi_C^G \coloneqq \frac{1}{|G|}\sum_{g\in G} W_C(g)$. Consider that

$$\begin{aligned}(\mathcal{M}_{B\to C}\circ\mathcal{N}_{A\to B})^\dagger (\Pi_C^G) &= (\mathcal{N}_{A\to B})^\dagger \left[(\mathcal{M}_{B\to C})^\dagger (\Pi_C^G)\right] \\ &\geq (\mathcal{N}_{A\to B})^\dagger \left[\Pi_B^G\right] \qquad (3.135)\\ &\geq \Pi_A^G. \qquad (3.136)\end{aligned}$$

The first equality follows by exploiting the identity $(\mathcal{M}_{B\to C}\circ\mathcal{N}_{A\to B})^\dagger = (\mathcal{N}_{A\to B})^\dagger \circ (\mathcal{M}_{B\to C})^\dagger$ for adjoints. The first inequality follows from the assumption that $\mathcal{M}_{B\to C}$ is a Bose symmetric channel and from the fact that $\mathcal{N}_{A\to B}$ is completely positive, so that $(\mathcal{N}_{A\to B})^\dagger$ is also. We thus conclude that $\mathcal{M}_{B\to C}\circ\mathcal{N}_{A\to B}$ is a Bose symmetric channel, so that the transitive property in (3.128) holds.

Finally, suppose that the input system A of a Bose symmetric channel $\mathcal{N}_{A\to B}$ is trivial. Then each group element g is trivially represented by the number one. It follows that $\Pi_A^G = 1$. Then the channel $\mathcal{N}_{A\to B}$ is really just a state ω_B [Wil17] with some spectral decomposition $\omega_B = \sum_x p(x)|x\rangle\langle x|_B$; furthermore, the associated Kraus operators are given by $\{\sqrt{p(x)}|x\rangle_B\}_x$. Then the condition

$$(\mathcal{N}_{A\to B})^\dagger (\Pi_B^G) \geq \Pi_A^G \tag{3.137}$$

reduces to

$$\sum_x p(x)\langle x|_B \Pi_B^G |x\rangle_B \geq 1, \tag{3.138}$$

which is the same as

$$\mathrm{Tr}[\Pi_B^G \omega_B] \geq 1. \tag{3.139}$$

Since ω_B is a state and Π_B^G is a projection, it follows that $\mathrm{Tr}[\Pi_B^G \omega_B] \leq 1$. Combining these inequalities, we conclude that $\mathrm{Tr}[\Pi_B^G \omega_B] = 1$. Finally, we apply (3.16) to conclude that ω_B is a Bose symmetric state. ■

Theorem 3.4.1 *Suppose that a quantum channel $\mathcal{N}_{A\to B}$ obeys the condition in* (3.133)*. Let σ_A be a Bose symmetric state. Then $\mathcal{N}_{A\to B}(\sigma_A)$ is a Bose symmetric state.*

Proof. Recall from (3.16) that a state σ_A is Bose symmetric if and only if $\mathrm{Tr}[\Pi_A^G \sigma_A] = 1$. Then consider that

$$1 \geq \mathrm{Tr}[\Pi_B^G \mathcal{N}_{A\to B}(\sigma_A)] \tag{3.140}$$

$$= \mathrm{Tr}[(\mathcal{N}_{A\to B})^\dagger (\Pi_B^G)\sigma_A] \tag{3.141}$$

$$\geq \mathrm{Tr}[\Pi_A^G \sigma_A] \tag{3.142}$$

$$= 1. \tag{3.143}$$

It follows that $\mathrm{Tr}[\Pi_B^G \mathcal{N}_{A\to B}(\sigma_A)] = 1$, and, by applying (3.16) again, that $\mathcal{N}_{A\to B}(\sigma_A)$ is Bose symmetric. ■

By essentially the same proof, it follows that the measure $\mathrm{Tr}[\Pi_A^G \rho_A]$ from (3.15) is non-decreasing under the action of a Bose symmetric channel $\mathcal{N}_{A\to B}$. Thus, the acceptance probability $\mathrm{Tr}[\Pi_A^G \rho_A]$ of a Bose symmetry test is a resource monotone in the resource theory of Bose asymmetry.

Theorem 3.4.2 *Let ρ_A be a state, and let $\mathcal{N}_{A\to B}$ be a Bose symmetric channel. Then* $\operatorname{Tr}[\Pi_A^G \rho_A]$ *is a resource monotone in the following sense:*

$$\operatorname{Tr}[\Pi_B^G \mathcal{N}_{A\to B}(\rho_A)] \geq \operatorname{Tr}[\Pi_A^G \rho_A]. \tag{3.144}$$

Proof. Consider that

$$\operatorname{Tr}[\Pi_B^G \mathcal{N}_{A\to B}(\rho_A)] = \operatorname{Tr}[(\mathcal{N}_{A\to B})^\dagger (\Pi_B^G)\rho_A] \tag{3.145}$$

$$\geq \operatorname{Tr}[\Pi_A^G \rho_A], \tag{3.146}$$

which follows from (3.133). ■

Throughout this section, we have adopted the perspective that Bose symmetric channels are defined by the condition in (3.133). It then follows as a consequence that $\operatorname{Tr}[\Pi_A^G \rho_A]$ is a resource monotone. We can adopt a different perspective and conclude consistency between them. Let us instead suppose that $\operatorname{Tr}[\Pi_A^G \rho_A]$ is non-decreasing under the action of a free channel $\mathcal{N}_{A\to B}$. That is, suppose that the following inequality holds for every state ρ_A:

$$\operatorname{Tr}[\Pi_B^G \mathcal{N}_{A\to B}(\rho_A)] \geq \operatorname{Tr}[\Pi_A^G \rho_A]. \tag{3.147}$$

Then by rewriting this inequality as

$$\operatorname{Tr}[((\mathcal{N}_{A\to B})^\dagger (\Pi_B^G) - \Pi_A^G)\rho_A] \geq 0 \quad \forall \rho_A \in \mathcal{D}(\mathcal{H}_A), \tag{3.148}$$

we conclude that $(\mathcal{N}_{A\to B})^\dagger (\Pi_B^G) - \Pi_A^G$ is a positive semi-definite operator, which is equivalent to the condition in (3.133). Thus, $\mathcal{N}_{A\to B}$ is a Bose symmetric channel if and only if $\operatorname{Tr}[\Pi_A^G \rho_A]$ is a resource monotone.

3.4.3. Resource Theory of Asymmetric Unextendibility

We now give a resource theory that generalizes that proposed in [KDWW19], just as the set of G-symmetric extendible states generalizes the set of k-extendible states (recall

Example 3.3.1). One of the main ideas is to use the notion of channel extension introduced in [KDWW19]; additionally, this resource theory allows us to conclude that the acceptance probability of Algorithm 4 (i.e., the maximum G-symmetric extendible fidelity) is a resource monotone and thus well motivated in this sense.

For the following definitions, let G be a group, and let $\{U_{RS}(g)\}_{g\in G}$ and $\{V_{R'S'}(g)\}_{g\in G}$ be projective unitary representations of G acting on $\mathcal{H}_R \otimes \mathcal{H}_S$ and $\mathcal{H}_{R'} \otimes \mathcal{H}_{S'}$ respectively.

Definition 3.4.2 (G-symmetric extendible channel) *A channel $\mathcal{N}_{S\to S'}$ is G-symmetric extendible if there exists a bipartite channel $\mathcal{M}_{RS\to R'S'}$ such that*

1. *$\mathcal{M}_{RS\to R'S'}$ is a channel extension of $\mathcal{N}_{S\to S'}$:*

$$\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} = \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R, \tag{3.149}$$

2. *$\mathcal{M}_{RS\to R'S'}$ is covariant with respect to $\{U_{RS}(g)\}_{g\in G}$ and $\{V_{R'S'}(g)\}_{g\in G}$:*

$$\mathcal{M}_{RS\to R'S'} \circ \mathcal{U}_{RS}(g) = \mathcal{V}_{R'S'}(g) \circ \mathcal{M}_{RS\to R'S'} \quad \forall g \in G, \tag{3.150}$$

where $\mathcal{U}_{RS}(g)(\cdot)$ and $\mathcal{V}_{R'S'}(g)(\cdot)$ are defined similarly to (1.70).

The condition in (3.149) implies that the extension channel $\mathcal{M}_{RS\to R'S'}$ is non-signaling from R to S' [BGNP01, ESW02, PHHH06], in the sense that

$$\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} = \mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} \circ \mathcal{R}^{\pi}_R, \tag{3.151}$$

where $\mathcal{R}^{\pi}_R(\cdot) \coloneqq \mathrm{Tr}[\cdot]\pi_R$ is a replacer channel that traces out its input and replaces with the maximally-mixed state π_R. This follows because

$$\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} \circ \mathcal{R}^{\pi}_R = \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R \circ \mathcal{R}^{\pi}_R \tag{3.152}$$

$$= \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R \tag{3.153}$$

$$= \mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'}, \tag{3.154}$$

where we have exploited the identity in (3.149) in the first and last lines, and in the second line used the fact that $\mathrm{Tr}_R \circ \mathcal{R}_R^{\pi} = \mathrm{Tr}_R$.

Definition 3.4.2 leads to a consistent resource theory of G-asymmetric unextendibility, in the sense that the free states are G-symmetric extendible states and the output of a G-symmetric extendible channel acting on a G-symmetric extendible state is a G-symmetric extendible state.

Proposition 3.4.2 *A G-symmetric extendible channel $\mathcal{N}_{S\to S'}$ with trivial input system is a G-symmetric extendible state.*

Proof. If the input system S of $\mathcal{N}_{S\to S'}$ is trivial, then it follows that $\mathcal{N}_{S\to S'}$ is a state (call it $\rho_{S'}$); furthermore, we can choose the input system R of the extension channel $\mathcal{M}_{RS\to R'S'}$ to be trivial, in which case $\mathcal{M}_{RS\to R'S'}$ is a state (call it $\omega_{R'S'}$) that extends $\rho_{S'}$. The condition in (3.150) then collapses to $\omega_{R'S'} = \mathcal{V}_{R'S'}(g)(\omega_{R'S'})$ for all $g \in G$. It follows by Definition 1.4.2 that $\rho_{S'}$ is a G-symmetric extendible state. ■

Proposition 3.4.3 *Let $\mathcal{N}_{S\to S'}$ be a G-symmetric extendible channel, and let ρ_S be a G-symmetric extendible state. Then $\mathcal{N}_{S\to S'}(\rho_S)$ is a G-symmetric extendible state.*

Proof. Since ρ_S is a G-symmetric extendible state, by Definition 1.4.1, there exists an extension state ω_{RS} satisfying the conditions stated there. Since $\mathcal{N}_{S\to S'}$ is a G-symmetric extendible channel, by Definition 3.4.2, there exists an extension channel $\mathcal{M}_{RS\to R'S'}$ satisfying the conditions stated there. It follows that $\mathcal{M}_{RS\to R'S'}(\omega_{RS})$ is an extension of $\mathcal{N}_{S\to S'}(\rho_S)$ as

$$\mathrm{Tr}_{R'}[\mathcal{M}_{RS\to R'S'}(\omega_{RS})] = \mathcal{N}_{S\to S'}(\mathrm{Tr}_R[\omega_{RS}]) \tag{3.155}$$

$$= \mathcal{N}_{S\to S'}(\rho_S), \tag{3.156}$$

where the first equality follows from (3.149). Also, consider that the following holds for all $g \in$

G:

$$(\mathcal{V}_{R'S'}(g) \circ \mathcal{M}_{RS\to R'S'})(\omega_{RS}) = (\mathcal{M}_{RS\to R'S'} \circ \mathcal{U}_{RS}(g))(\omega_{RS})$$
$$= \mathcal{M}_{RS\to R'S'}(\omega_{RS}), \tag{3.157}$$

where the first equality follows from (3.150) and the second from (3.2). ■

As a consequence of Proposition 3.4.3 and the data-processing inequality for fidelity, the maximum G-symmetric extendible fidelity is a resource monotone.

Corollary 3.4.3 *Let ρ_S be a state, and let $\mathcal{N}_{S\to S'}$ be a G-symmetric extendible channel. Then the maximum G-symmetric extendible fidelity is a resource monotone,*

$$\max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S) \leq \max_{\sigma_{S'} \in \mathrm{SymExt}_G} F(\mathcal{N}_{S\to S'}(\rho_S), \sigma_{S'}). \tag{3.158}$$

Example 3.4.1 (k-unextendibility) *The resource theory of k-unextendibility, proposed in [KDWW19], is a special case of the resource theory of G-asymmetric unextendibility. To see this, recall that a bipartite channel $\mathcal{N}_{AB\to A'B'}$ is k-extendible if there exists an extension channel $\mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k}$ satisfying*

$$\mathrm{Tr}_{B'_2\cdots B'_k} \circ \mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k} = \mathcal{N}_{AB\to A'B'} \circ \mathrm{Tr}_{B_2\cdots B_k} \tag{3.159}$$

and

$$\mathcal{W}^{\pi}_{B'_1\cdots B'_k} \circ \mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k} = \mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k} \circ \mathcal{W}^{\pi}_{B_1\cdots B_k}, \tag{3.160}$$

for all $\pi \in S_k$, where $\mathcal{W}^{\pi}_{B_1\cdots B_k}$ and $\mathcal{W}^{\pi}_{B'_1\cdots B'_k}$ are unitary permutation channels. Thus, by setting

$$S = AB, \tag{3.161}$$

$$R = B_2 \cdots B_k, \tag{3.162}$$

$$S' = A'B', \tag{3.163}$$

$$R' = B'_2 \cdots B'_k, \tag{3.164}$$

$$U_{RS}(g) = I_A \otimes W_{B_1 \cdots B_k}(\pi), \tag{3.165}$$

$$V_{R'S'}(g) = I_{A'} \otimes W_{B'_1 \cdots B'_k}(\pi), \tag{3.166}$$

we see that a k-extendible channel is a special case of a G-symmetric extendible channel.

3.4.4. Resource Theory of Bose Asymmetric Unextendibility

We finally consider the resource theory of Bose asymmetric unextendibility, with the goal being similar to that of the previous sections; we want to justify the acceptance probability of Algorithm 3 (i.e., the maximum G-BSE fidelity) as a resource monotone. At the same time, we establish a novel resource theory that could have further applications in quantum information.

Once again, let G, $\{U_{RS}(g)\}_{g\in G}$, and $\{V_{R'S'}(g)\}_{g\in G}$ be defined the same way as in Section 3.4.3.

Definition 3.4.3 (G-BSE channel) *A channel $\mathcal{N}_{S\to S'}$ is G-Bose symmetric extendible (G-BSE) if there exists a bipartite channel $\mathcal{M}_{RS\to R'S'}$ such that*

1. *$\mathcal{M}_{RS\to R'S'}$ is a channel extension of $\mathcal{N}_{S\to S'}$:*

$$\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} = \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R, \tag{3.167}$$

2. *$\mathcal{M}_{RS\to R'S'}$ is Bose symmetric:*

$$(\mathcal{M}_{RS\to R'S'})^\dagger(\Pi^G_{R'S'}) \geq \Pi^G_{RS}, \tag{3.168}$$

where Π^G_{RS} and $\Pi^G_{R'S'}$ are defined as in (3.65) *as sums over $U_{RS}(g)$ and $V_{R'S'}(g)$ respectively.*

As discussed in (3.151)–(3.154), the condition in (3.167) can be understood as imposing a no-signaling constraint, from R to S'. Now, with the same line of reasoning given in the proof of Proposition 3.4.2, we conclude the following:

Proposition 3.4.4 *A G-BSE channel $\mathcal{N}_{S\to S'}$ with trivial input system is a G-BSE state.*

The following proposition demonstrates that the resource theory delineated by Definition 3.4.3 is indeed a consistent resource theory.

Proposition 3.4.5 *Let $\mathcal{N}_{S\to S'}$ be a G-BSE channel, and let ρ_S be a G-BSE state. Then $\mathcal{N}_{S\to S'}(\rho_S)$ is a G-BSE state.*

As this proof is similar to that of Proposition 3.4.3, we include it in Appendix B.4. As a consequence of Proposition 3.4.5 and the data-processing inequality for fidelity, it follows that the maximum G-BSE fidelity is a resource monotone.

Corollary 3.4.4 *Let ρ_S be a state, and let $\mathcal{N}_{S\to S'}$ be a G-BSE channel. Then the maximum G-BSE fidelity is a resource monotone in the following sense:*

$$\max_{\sigma_S\in \mathrm{BSE}_G} F(\rho_S,\sigma_S) \leq \max_{\sigma_{S'}\in \mathrm{BSE}_G} F(\mathcal{N}_{S\to S'}(\rho_S),\sigma_{S'}). \tag{3.169}$$

To define the resource theory of k-Bose unextendibility, we establish the notion of a free channel (i.e., a k-Bose extendible bipartite channel) and discuss it in the following example.

Example 3.4.2 (k-Bose unextendibility) *We say that a bipartite channel $\mathcal{N}_{AB\to A'B'}$ is k-Bose-extendible if there exists an extension channel $\mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k}$ satisfying*

$$\mathrm{Tr}_{B'_2\cdots B'_k}\circ\mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k} = \mathcal{N}_{AB\to A'B'}\circ \mathrm{Tr}_{B_2\cdots B_k} \tag{3.170}$$

and

$$(\mathcal{M}_{AB_1\cdots B_k\to A'B'_1\cdots B'_k})^\dagger(\Pi^{\mathrm{Sym}}_{B'_1\cdots B'_k}) \geq \Pi^{\mathrm{Sym}}_{B_1\cdots B_k}, \tag{3.171}$$

where $\Pi^{\mathrm{Sym}}_{B'_1\cdots B'_k}$ and $\Pi^{\mathrm{Sym}}_{B_1\cdots B_k}$ are projections onto symmetric subspaces,

$$\Pi^{\mathrm{Sym}}_{B_1\cdots B_k} := \frac{1}{k!}\sum_{\pi\in S_k} W^\pi_{B_1\cdots B_k}, \tag{3.172}$$

$$\Pi^{\mathrm{Sym}}_{B'_1\cdots B'_k} := \frac{1}{k!}\sum_{\pi\in S_k} W^\pi_{B'_1\cdots B'_k}, \tag{3.173}$$

and $W^{\pi}_{B_1\cdots B_k}$ *and* $W^{\pi}_{B'_1\cdots B'_k}$ *are unitary representations of the permutation* $\pi \in S_k$*. Thus, by setting*

$$S = AB, \tag{3.174}$$

$$R = B_2 \cdots B_k, \tag{3.175}$$

$$S' = A'B', \tag{3.176}$$

$$R' = B'_2 \cdots B'_k, \tag{3.177}$$

$$U_{RS}(g) = I_A \otimes W_{B_1\cdots B_k}(\pi), \tag{3.178}$$

$$V_{R'S'}(g) = I_{A'} \otimes W_{B'_1\cdots B'_k}(\pi), \tag{3.179}$$

we see that a k-Bose-extendible channel is a special case of a G-Bose symmetric extendible channel.

3.5. Conclusion

In summary, we have proposed various quantum computational tests of symmetry, as well as various notions of symmetry like G-symmetric extendibility and G-Bose symmetric extendibility, which include previous notions of symmetry from [MS13, MS14, Wer89, DPS02, DPS04] as a special case. These tests have acceptance probabilities equal to various maximum symmetric fidelities, thus endowing these measures with operational meaning. We have also established resource theories of asymmetry beyond that proposed in [MS13], which put the maximum symmetric fidelities on firm ground in a resource-theoretic sense.

Going forward from here, we will now discuss an expansion of a particular part of this chapter. Namely, we will address unanswered questions in the derivation of acceptance probabilities of bipartite separability tests. Futhermore, we will go on to show that an entire class of separability tests can be generated and compared beyond the full symmetric test prior literature has prepared for us.

Chapter 4. Generalized Separability Tests for Bipartite Pure States

4.1. Introduction

In the previous chapter, we described a specific kind of symmetry test that acts as a separability test for pure bipartite states. Separability and entanglement of quantum states are a topic of high interest throughout quantum information, as might well be expected. (See, for example, quantifiers and measures in [Per96, HHH96, idZHSL98, EP99, VW02, Wer89, DPS02, KDWW19, WWW19, KDWW21].) In this chapter, we will give a recipe for developing separability tests in the vein of k-extendibility [Wer89, DPS02].

The most common quantum computational test of separability of pure states is the swap test, introduced in [BBD+97] and used in quantum fingerprinting [BCWDW01]. To understand it, first recall that a pure bipartite state $|\psi\rangle_{AB}$ is separable if it can be written as a tensor product of two states, as

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B. \tag{4.1}$$

Now, if we take two copies of this separable state, it has the following form:

$$|\psi\rangle_{A_1B_1} \otimes |\psi\rangle_{A_2B_2} = |\phi\rangle_{A_1} \otimes |\varphi\rangle_{B_1} \otimes |\phi\rangle_{A_2} \otimes |\varphi\rangle_{B_2}. \tag{4.2}$$

This state is invariant under a swap of systems A_1 and A_2, as well as a swap of systems B_1 and B_2. Thus, the swap test accepts with certainty in this case; however, if a pure bipartite state is not separable, the two-copy state does not possess the above swap invariance, and the swap test can detect this lack of invariance by means of the well-known phase kickback trick

In Chapter 3 and [LRW21], we proposed a generalization of the swap test as a method for detecting entanglement, based on the observation that multiple copies of the separable state in

(4.1) are invariant under arbitrary permutations of both the A systems and B systems. Indeed, by writing such a state down explicitly as

$$\bigotimes_{i=1}^{k} |\psi\rangle_{A_iB_i} = \bigotimes_{i=1}^{k} |\phi\rangle_{A_i} \otimes |\varphi\rangle_{B_i}, \tag{4.3}$$

it is clear that such a state is invariant as mentioned above; however, if the state $|\psi\rangle_{AB}$ is not separable, then checking for various kinds of permutation invariance of the state $\bigotimes_{i=1}^{k} |\psi\rangle_{A_iB_i}$ leads to more fine-grained tests of entanglement with alternative mathematical expressions for the acceptance probability of the test. This chapter endeavors to understand these expressions in more detail.

For our approach here, we will make liberal use of the framework of G-Bose symmetry tests, as discussed in Section 3.2.1. This method facilitates our discussions of the separability of a pure bipartite state. Specifically, in the framework we consider, we take a pure state $|\psi\rangle_{AB}$ and conduct an S_k-Bose symmetry test on the tensor-power state $|\psi\rangle_{AB}^{\otimes k}$, where S_k denotes the symmetric group on k letters. This tensor-power state realizes the case where we have access to k copies of our state under test. The swap test is recovered as a special case in which $k = 2$.

The G-Bose symmetry tests allow for a generalization of the swap test to more copies of a state of interest and higher-order groups. These algorithms exchange simplicity for certainty, analogous to how fingerprinting is both more accurate and complicated when greater numbers of prints are taken. In choosing to investigate group symmetries, rather than merely the swap test, the separability of a state can be determined more quickly and accurately.

The natural question is, when do these more complex tests merit performing? In [BLW22], the paper this chapter is based upon, we derive the acceptance probability of a generalized separability test, and the end result is included here. In doing so, we present an

inherent reliance on the cycle index polynomial, a particularly important polynomial in Pólya theory [Pó37, Rob09] that encodes the structure of a permutation group by storing the number of elements of a given cycle type as its coefficients. This allows us to compare separability tests generated from various groups, as well as investigate the mathematical relationships inherently present in these tests. We directly show that an arbitrary finite group generates a separability test with its acceptance probability given by the cycle index polynomial of that group. We supplement this by then giving explicit quantum circuit descriptions for groups of interest and counting the number of gates needed to realize each test. Combining our acceptance probability results with resource counting gives us a metric to compare when the relative strictness of the test is outweighed by the benefit of fewer gate resources, and we discuss this factor in more detail in Section 4.4.

In Section 4.2, we revisit the algorithm for the bipartite pure-state separability test in Section 3.3.1. We show that the acceptance probability of this algorithm is given by the cycle index polynomial [Pó37, Rob09] of the symmetric group S_k, which is itself related to the complete Bell polynomials [RR78]. In Section 4.2.1, we prove our conjecture from Section 3.3.1, that the acceptance probability of such algorithms does not increase as $k \to \infty$. In fact, we show that it strictly decreases and converges to zero whenever $\rho_B \coloneqq \mathrm{Tr}_A[|\psi\rangle\langle\psi|_{AB}]$ is not a pure state.

In Section 4.3, we generalize the bipartite pure-state separability test to an algorithm involving any group G, in which a G-Bose symmetry test is performed on the tensor-power state $|\psi\rangle_{AB}^{\otimes k}$. By identifying G with a subgroup of S_k, which is guaranteed to exist by Cayley's theorem, we show, by the same reasoning as in Section 4.2, that the acceptance probability of the algorithm is given by the cycle index polynomial of the group G. We discuss how these generalized tests are in fact separability tests for pure, bipartite states, and they have an interesting con-

nection to combinatorics via the cycle index polynomial.

In Section 4.4, we analyze the resources needed to implement these tests on quantum computers; in doing so, we show that simpler groups can give comparable performance for fewer resources. We also give constructions for tests with respect to the cyclic group C_k and the more typical S_k group, and we compare the resouce costs of these test with respect to their rejection probability.

Finally, we conclude in Section 4.5 with a summary.

4.2. Bipartite Pure-State Separability Test

Let us begin by reviewing the construction of the bipartite pure-state separability test in Chapter 3, which can be viewed as a G-Bose symmetry test. For convenience, we now recall the definition of a G-Bose symmetric state.

Definition 4.2.1 *Let G be a group with a unitary representation $U_S : G \to U(\mathcal{H})$, where $U(\mathcal{H})$ denotes the set of all unitaries that act on a Hilbert space $\mathcal{H}$. Then a state ρ_S is called G-Bose symmetric if*

$$\Pi_S^G \rho_S \Pi_S^G = \rho_S, \tag{4.4}$$

where $\Pi_S^G \coloneqq \frac{1}{|G|} \sum_{g \in G} U_S(g)$ is the group representation projection.

We discussed in Section 3.3.1 how this framework can be used to test for the separability of a bipartite pure state ψ_{AB}. To do so, we suppose that k copies of the state ψ_{AB} are available, which we write as $\psi_{AB}^{\otimes k}$. We also identify the A systems by $A_1 \cdots A_k$ and the B systems by $B_1 \cdots B_k$. We then perform an S_k-Bose symmetry test on the state $\psi_{AB}^{\otimes k}$ by identifying S with $A_1 B_1 \cdots A_k B_k$ and $U_S(\pi)$ with $I_{A_1 \cdots A_k} \otimes W_{B_1 \cdots B_k}(\pi)$, where $\pi \in S_k$ and $W_{B_1 \cdots B_k} : S_k \to U(\mathcal{H}_{B_1 \cdots B_k})$ is the standard unitary representation of S_k that acts on $\mathcal{H}_{B_1 \cdots B_k} \equiv \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_k}$

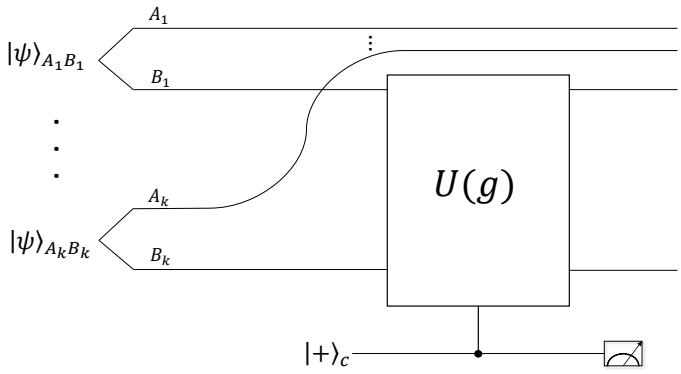


Figure 4.1. Quantum circuit to implement a G-Bose symmetry test. We take k copies of an initial bipartite state $|\psi\rangle_{AB}$ and consider the reduced state $\rho_B = \mathrm{Tr}_A[|\psi\rangle\langle\psi|_{AB}]$. The collection of these reduced states are then subjected to the separability test determined by the group, where $|+\rangle_C$ is defined in (3.10), and $U(g)$ is an element of the group representation.

by permuting the Hilbert spaces according to the corresponding permutation. Define $\rho_B :=$ $\mathrm{Tr}_A[\psi_{AB}]$. By applying (4.4), the acceptance probability for the bipartite pure-state separability algorithm is given by

$$p^{(k)} := \mathrm{Tr}[\Pi_{B_1\cdots B_k}\rho_B^{\otimes k}]\,, \tag{4.5}$$

where

$$\Pi_{B_1\cdots B_k} := \frac{1}{k!}\sum_{\pi\in S_k} W_{B_1\cdots B_k}(\pi)\,. \tag{4.6}$$

Figure 4.1 reviews the G-Bose symmetry test. The circuit begins with k copies of an initial bipartite state $|\psi\rangle_{AB}$. The B_i subsystems are collected and subject to a controlled unitary gate whose mathematical description involves each unitary $U(g)$. The control register is initialized to the state $|+\rangle_C$, as defined in (3.10). Under the separability test circuit, $G = S_k$, and the unitary representation is a permutation of the B_i subsystems.

Our first main result is a formula for the acceptance probability $p^{(k)}$ in (4.5) as a sum over the partitions of k of a product of traces of ρ_B and its powers and certain scaling factors.

Theorem 4.2.1 *Let ψ_{AB} denote a pure bipartite state and define $\rho_B \coloneqq \mathrm{Tr}_A[\psi_{AB}]$. Then the acceptance probability $p^{(k)}$ for the bipartite pure-state separability test is given by*

$$p^{(k)} = \sum_{a_1+2a_2+\cdots+ka_k=k} \prod_{j=1}^{k} \frac{(\mathrm{Tr}[\rho_B^j])^{a_j}}{j^{a_j} a_j!}, \tag{4.7}$$

where the sum is taken over the partitions of k.

Proof. Let $\pi \coloneqq (1\ 2\ \cdots\ k)$ and consider the representation $W_{B_1\cdots B_k}(\pi)$. It was shown in [EAO+02] that $\mathrm{Tr}[W_{B_1\cdots B_k}(\pi)\rho_B^{\otimes k}] = \mathrm{Tr}[\rho_B^k]$, but we include a proof here for completeness. Expanding ρ in the standard basis as $\rho = \sum_{i,j} p_{i,j}|i\rangle\langle j|$, we have

$$\begin{aligned}
&\mathrm{Tr}[W_{B_1\cdots B_k}(\pi)\rho_B^{\otimes k}] \\
&= \mathrm{Tr}\left[W_{B_1\cdots B_k}(\pi) \sum_{\substack{i_1,\ldots,i_k \\ j_1,\ldots,j_k}} p_{i_1 j_1}\cdots p_{i_k j_k}|i_1\rangle\langle j_1| \otimes |i_2\rangle\langle j_2| \otimes \cdots \otimes |i_k\rangle\langle j_k|\right] && (4.8)\\
&= \mathrm{Tr}\left[\sum_{\substack{i_1,\ldots,i_k \\ j_1,\ldots,j_k}} p_{i_1 j_1}\cdots p_{i_k j_k}|i_k\rangle\langle j_1| \otimes |i_1\rangle\langle j_2| \otimes \cdots \otimes |i_{k-1}\rangle\langle j_k|\right] && (4.9)\\
&= \sum_{\substack{i_1,\ldots,i_k \\ j_1,\ldots,j_k \\ t_1,\ldots,t_k}} p_{i_1 j_1}\cdots p_{i_k j_k}\delta_{t_1 i_k}\delta_{j_1 t_1}\cdots\delta_{t_k i_{k-1}}\delta_{j_k t_k} && (4.10)\\
&= \sum_{t_1,\ldots,t_k} p_{t_2 t_1} p_{t_3 t_2}\cdots p_{t_k t_{k-1}} p_{t_1 t_k}. && (4.11)
\end{aligned}$$

Meanwhile,

$$\begin{aligned}
\mathrm{Tr}[\rho^k] &= \mathrm{Tr}\left[\sum_{i_1,\ldots,i_k,j_1,\ldots,j_k} p_{i_1 j_1}\cdots p_{i_k j_k}|i_1\rangle\langle j_1|i_2\rangle\langle j_2|\cdots|i_k\rangle\langle j_k|\right] && (4.12)\\
&= \sum_{i_1,i_2,\ldots,i_k} p_{i_1 i_2} p_{i_2 i_3}\cdots p_{i_{k-1} i_k} p_{i_k i_1}. && (4.13)
\end{aligned}$$

Thus, by relabeling the indices, we see that

$$\mathrm{Tr}[W_{B_1\cdots B_k}(\pi)\rho_B^{\otimes k}] = \mathrm{Tr}[\rho^k]. \tag{4.14}$$

Similarly, we can show for every m-cycle $\pi_m \in S_k$ that

$$\mathrm{Tr}[W_{B_1\cdots B_k}(\pi_m)\rho_B^{\otimes k}] = \mathrm{Tr}[\rho^m]. \tag{4.15}$$

Now suppose π_m and π_n are disjoint m- and n-cycles, respectively. Then they act on different Hilbert spaces and so the trace of the product of their representations acting on $\rho_B^{\otimes k}$ splits into the product of traces. That is,

$$\mathrm{Tr}[W_{B_1\cdots B_k}(\pi_m)W_{B_1\cdots B_k}(\pi_n)\rho^{\otimes k}] = \mathrm{Tr}[\rho^m]\,\mathrm{Tr}[\rho^n]. \tag{4.16}$$

Now, since every m-cycle yields a factor of $\mathrm{Tr}[\rho^m]$ and products of disjoint cycles split the trace, we have

$$\begin{aligned} p^{(k)} &= \mathrm{Tr}[\Pi_{B_1\cdots B_k}\rho_B^{\otimes k}] && (4.17)\\ &= \mathrm{Tr}\left[\frac{1}{k!}\sum_{\pi\in S_k} W_{B_1\cdots B_k}(\pi)\rho_B^{\otimes k}\right] && (4.18)\\ &= \frac{1}{k!}\sum_{\pi\in S_k}\mathrm{Tr}[W_{B_1\cdots B_k}(\pi)\rho_B^{\otimes k}] && (4.19)\\ &= \frac{1}{k!}\sum_{a_1+2a_2+\cdots+ka_k=k} c(a_1,\ldots,a_k)\prod_{j=1}^{k}\mathrm{Tr}[\rho_B^j]^{a_j} && (4.20) \end{aligned}$$

where $c(a_1,\ldots,a_k)$ is the number of cycles in S_k with cycle type $(a_1,\ldots,a_k)$, which is known to be $\frac{k!}{\prod_{j=1}^k j^{a_j}a_j!}$ (see [vLW01, Eq. (13.3)]). Thus, the equality in (4.7) follows. ■

We assert now that the formula is identical to that of the cycle index polynomial of the symmetric group S_k, with each variable x_j taking the value $\mathrm{Tr}[\rho^j]$. The cycle index polynomial of a permutation group G is defined by

$$Z(G)(x_1,\ldots,x_n) \coloneqq \frac{1}{|G|}\sum_{g\in G} x_1^{c_1(g)}\cdots x_n^{c_n(g)}, \tag{4.21}$$

where $c_j(g)$ denotes the number of cycles of length j in the disjoint cycle decomposition of g. Setting $x_j = \mathrm{Tr}[\rho_B^j]$, we see that the acceptance probability of the separability test is given by the

cycle index polynomial of the symmetric group S_k (see [vLW01, Chapter 37, pg. 526]), so that it satisfies the recurrence relation

$$p^{(k)} = \frac{1}{k} \sum_{j=1}^{k} \mathrm{Tr}[\rho^j] p^{(k-j)} \,. \tag{4.22}$$

Furthermore, the cycle index polynomial of the symmetric group S_k is equivalent to

$$\frac{1}{k!} B_k(x_1, x_2, 2!\, x_3, 3!\, x_4, \ldots, (k-1)!\, x_k) \,, \tag{4.23}$$

where $B_k(x_1, \ldots, x_k)$ is the complete Bell polynomial [Com74]. From this perspective, the acceptance probability can be interpreted as the k^{th} raw moment of a probability distribution with the first k cumulants given by $1, \mathrm{Tr}[\rho^2], \ldots, \mathrm{Tr}[\rho^k]$. See [Mac95, Chapter 1, Section 2] for more information on (4.22).

Thus we have addressed one of the two open questions purposed in Section 3.3.1. Now we move on to the second.

4.2.1. Strictly Decreasing Acceptance Probability

In Chapter 3, we made reference to a conjecture from [LRW21] that the acceptance probability of the bipartite pure-state separability test is monotone non-increasing in k. We answer this conjecture in the affirmative as a corollary of the following lemma about complete Bell polynomials. In fact, this inequality is strict, and the acceptance probability approaches zero in the limit $k \to \infty$ whenever ρ_B is not a pure state.

The full proof of this is given in [BLW22] and is beyond the scope of this thesis, but we list the results here. By first proving a relevant relationship between Bell polynomials, we are able to show the following theorem.

Theorem 4.2.2 *The acceptance probability $p^{(k)}$ is strictly decreasing and $\lim_{k\to\infty} p^{(k)} = 0$ when ρ_B is not a pure state.*

These results indicate that as k goes to infinity, fewer repetitions of the test are needed to determine whether a given pure state is entangled. There is a trade-off, however, between increasing k and the computational resources needed to conduct a single test. As k increases, one might suspect that the resources needed will increase in such a way that a large enough k is not feasible. Indeed, as one of our results, we discuss the scaling in this claim in Section 4.4.

4.3. Generalization of the Algorithm

The previous sections address results and conjectures of the archetypal k-Bose extendibility tests, but we now present a generalization of the bipartite pure-state separability algorithm to groups other than the symmetric group S_k. Furthermore, these algorithms are also separability tests. As always, let G be a finite group, and let ψ_{AB} be a pure state. Recall that Cayley's theorem [DF04] guarantees that every finite group is isomorphic to a subgroup of a permutation group. Thus, there exists a representation of G such that every $g \in G$ is mapped to an element $\pi \in S_k$ for some $k \in \mathbb{N}$. In turn, there exists a map from π to the operator that permutes the Hilbert spaces in the composite Hilbert space $\mathcal{H}^{\otimes k}$. Then a generalization of the bipartite pure-state separability algorithm is given by performing a G-Bose symmetry test on the state $\psi_{AB}^{\otimes k}$.

By the argument in the proof of Theorem 4.2.1, we see that one simply has to count the number of cycles of any given cycle type in the permutation subgroup isomorphic to G to obtain a formula for the acceptance probability of the algorithm. That is, the argument in Theorem 4.2.1, combined with Cayley's theorem, proves the following theorem:

Theorem 4.3.1 *Let p_G denote the acceptance probability with respect to the group G for the generalization of the bipartite pure-state separability algorithm. Then*

$$p_G = Z(G)(1, \ldots, \mathrm{Tr}[\rho^k]) \,. \tag{4.24}$$

That is, the acceptance probability p_G is given by the cycle index polynomial (4.21) *of G evaluated at $x_j = \mathrm{Tr}[\rho^j]$ for $j \in \{1, \ldots, k\}$.*

As an aside, we note that (4.24) has an interesting combinatorial meaning. Let $\{\lambda_i\}_{i=1}^r$ denote the eigenvalues of ρ. By Pólya's enumeration theorem [Bru10, Tuc95], we can interpret (4.24) as a generating function for the number of nonequivalent colorings of a set S with the r colors $\{\lambda_i\}_{i=1}^r$. The role of G here is to define the equivalence between colorings through its action on S.

We would now like to give two relevant examples to demonstrate the above result. Specifically, we show the already discussed case of S_k but also the cyclic group C_k, as these two examples will be of interest to us in later sections.

Example 4.3.1 *We consider the example already discussed in Theorem 4.2.1. Let $G = S_k$ be the symmetric group, which is already a permutation group. Then the acceptance probability is given by the cycle index polynomial of S_k. That is,*

$$p_{sym}^{(k)} = \sum_{a_1+2a_2+\cdots+ka_k=k} \prod_{j=1}^{k} \frac{(\mathrm{Tr}[\rho_B^j])^{a_j}}{j^{a_j} a_j!}. \tag{4.25}$$

□

Example 4.3.2 *In this example, we generalize the cyclic test to products of cyclic groups. Let $G = \mathbb{Z}_m^k$ be the product of k copies of the group $\mathbb{Z}_m$. We represent G as a permutation subgroup by labeling its elements and letting them act on the group to construct a permutation. For example, if $k = 1$, then $G = \{0, 1, \ldots, m-1\}$. Since 0 has no effect on any element of the group, we map it to the identity element e. Meanwhile, 1 acts on each element of the group by sending 0 to 1, 1 to 2, and so on. So we identify 1 with the cycle $(1 \cdots m)$. The remaining permutations are defined similarly.*

Returning to the more general setting, we see that the elements of each order n correspond to products of n-cycles. Now, for an element of G to have order n, each component must contain an element of an order that divides n, with at least one component filled by an element of order n. So the number of elements of order n is given by

$$\sum_{i=1}^{k}\binom{k}{i}(\phi(n))^i\left(\sum_{\substack{l|n\\ l<n}}\phi(l)\right)^{k-i} = \left(\phi(n)+\sum_{\substack{l|n\\ l<n}}\phi(l)\right)^{k} - \left(\sum_{\substack{l|n\\ l<n}}\phi(l)\right)^{k} \tag{4.26}$$

$$= n^k - (n-\phi(n))^k, \tag{4.27}$$

where ϕ denotes the Euler ϕ-function. The acceptance probability given by the cycle index polynomial of $\mathbb{Z}_m^k$ is then

$$p_{\mathbb{Z}_m^k}^{(k)} = \frac{1}{m^k}\sum_{n|m}(n^k-(n-\phi(n))^k)(\mathrm{Tr}[\rho_B^n])^{\frac{m^k}{n}}. \tag{4.28}$$

□

Finally, we claim that the above nontrivial examples, as well as any other example involving a nontrivial finite group, are tests for separability of a pure bipartite state. Thus, we have produced an entire class of separability tests.

Theorem 4.3.2 *Let ψ_{AB} denote a pure bipartite state. Then the generalized bipartite pure-state separability algorithm is, in fact, a faithful test for separability of ψ_{AB} for any nontrivial finite group G, meaning that the acceptance probability is equal to one if and only if the pure state is a separable state.*

Once again, the proof of this theorem is given in [BLW22], but we include it here for completeness.

Proof. Suppose ψ_{AB} is separable. That is, $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B$ for some states $|\phi\rangle_A \in \mathcal{H}_A$ and

$|\varphi\rangle_B \in \mathcal{H}_B$. Then

$$\rho_B \coloneqq \mathrm{Tr}_A[\psi_{AB}] \tag{4.29}$$

$$= \mathrm{Tr}_A[|\phi\rangle\langle\phi|_A \otimes |\varphi\rangle\langle\varphi|_B] \tag{4.30}$$

$$= |\varphi\rangle\langle\varphi|_B. \tag{4.31}$$

That is, ρ_B is a pure state. From Theorem 4.3.1, the acceptance probability of the algorithm is given by the cycle index polynomial evaluated at the traces of increasing powers of ρ_B. But since ρ_B is pure, $\mathrm{Tr}[\rho_B^j] = 1$ for all $j \in \{1, \ldots, n\}$. Then the acceptance probability is equal to the cycle index polynomial at $x_j = 1$ for all $j \in \{1, \ldots, n\}$. That is,

$$p_G = Z(G)(1, \ldots, \mathrm{Tr}[\rho^n]) \tag{4.32}$$

$$= Z(G)(1, \ldots, 1) \tag{4.33}$$

$$= \frac{1}{|G|} \sum_{g \in G} 1^{c_1(g)} \cdots 1^{c_n(g)} \tag{4.34}$$

$$= \frac{1}{|G|} \sum_{g \in G} 1 \tag{4.35}$$

$$= 1 \tag{4.36}$$

where $c_i(g)$ denotes the number of cycles of length i in the disjoint cycle decomposition of g. Thus, ψ_{AB} separable implies that the acceptance probability is identically one.

Now suppose ρ_B is a mixed state. Then $\mathrm{Tr}[\rho_B^j] < 1$ for all $j > 1$ and we have

$$p_G = Z(G)(1, \mathrm{Tr}[\rho_B^2], \ldots, \mathrm{Tr}[\rho_B^n]) \tag{4.37}$$

$$= \frac{1}{|G|} \sum_{g \in G} 1^{c_1(g)} (\mathrm{Tr}[\rho_B^2])^{c_2(g)} \cdots (\mathrm{Tr}[\rho_B^n])^{c_n(g)} \tag{4.38}$$

$$< \frac{1}{|G|} \sum_{g \in G} 1^{c_1(g)} \cdots 1^{c_n(g)} \tag{4.39}$$

$$= \frac{1}{|G|} \sum_{g \in G} 1 \tag{4.40}$$

$$= 1, \tag{4.41}$$

where we have used the assumption that G is nontrivial to guarantee that at least one of the $c_j(g)$ is nonzero so that the inequality holds. Thus, the test is faithful. ■

4.4. Resource Comparison of Symmetry Tests

Given the generalization in Section 4.3, we can now compare the performance of these separability tests. There are two practical concerns to consider when implementing such a test: the rate at which the acceptance probability decays and the resources required to construct it. The cycle index polynomial results described above allow for direct analysis of the former topic, but the latter requires additional consideration before it can be adequately addressed. First, we will specify how resources are counted for each algorithm. Then we compare the resource cost for each algorithm given this framework. We accompany this with a discussion of the acceptance probability of the compared methods.

We now clarify what is meant by resources in this context. For the G-Bose symmetry test described in Chapter 3 and tests of that nature, the two primary resources are the number of gates used to construct the test and how many qubits are needed in the control register. An alternate consideration is the depth of the circuit, which we will mention where appropriate. We begin with a discussion of gate counting.

4.4.1. Resource Counting of Quantum Gates

The unitary representation in this context is always formed from a collection of SWAP gates used to permute the subsystems. SWAP gates can be realized by a sequence of three CNOT gates in alternating direction. Often, the literature commonly counts the number of CNOT gates

used as a resource (see, e.g., [GB00]); however, particular architectures may have more efficient realizations of the SWAP gate. Furthermore, this algorithm actually calls for controlled-SWAP gates, which may have vastly different compilations between architectures. For the purposes of this discussion, we will be counting the necessary number of controlled-SWAPs alone. Additionally, we do not restrict to swapping between consecutive Hilbert spaces although in principle this could be a limitation of particular systems.

Here, we give an explicit construction for two example groups. The first is the cyclic group test, which is a simple Abelian subgroup of the symmetric group and therefore of interest as a point of comparison. Although constructions of cyclic shifts exist in the literature, our construction follows binary encoding procedures [BGB+18, LC19] and uses fewer gates than a naïve implementation and thus warrants discussion. The second construction given describes a recursive implementation of the full permutation test. Similarly, although the quantum Schur transform [BCH06, BCH07, Kro19] gives a recipe for implementing the symmetric group in principle, the gate construction is abstract and thus difficult to use for accurate gate counts compared to other approaches. As such, we utilize the construction given in [BBD+97]. In the following two subsections, we show that a cyclic group test can be implemented with $O(k \log(k))$ controlled-SWAP gates and a full symmetric group test (also known as a permutation test) with $O(k^2)$ controlled-SWAP gates.

Cyclic Group

Analysis of the cyclic group benefits from established literature. Any cyclic permutation can be achieved in constant depth with $k-1$ gates, where k is the order of the cycle [GB00]. We will now show that any cyclic group test can be generated by implementing solely the elements

in that cycle that are powers of two. This means that the resource cost of implementing the cyclic test of order k is $(k-1)\log_2(k)$, and the constant depth condition above from [GB00] gives a corresponding depth of $O(\log_2(k))$ in the separability test.

To see this, first recall that the k-order cyclic group is isomorphic to the set $\mathbb{Z}_k$ of integers modulo k under addition. This will allow us to symbolically represent each element by a single number, understood in this context to be modulo k.

Since the case of $k = 1$ is trivial, let us first consider the base case of $k = 2$. This example illustrates the general construction of cyclic tests and recreates the well-established swap test [BBD+97, BCWDW01]. The controlled-SWAP element corresponds to the element $1 = 2^0$, and is the sole gate needed, and the identity element is naturally 0. (Note that 1 is the sole power of two in $\mathbb{Z}_2 = \{0, 1\}$.) The control state for this test is given by a single qubit state of

$$|+\rangle_{C(2)} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,, \tag{4.42}$$

where we employ the computational basis. It is clear that each element in the ancillary basis will give rise to its corresponding group element with this test.

How does this construction generalize? For each given k, we follow a similar recipe as above. As C_k is isomorphic to $\mathbb{Z}_k$, start by identifying each cycle in C_k with a number in $\mathbb{Z}_k$. If we always map the first k-cycle to one, then this map follows simply by mapping cycle composition to integer addition by one. Consider, for instance, the case of C_5. Then the first cycle is (1 2 3 4 5). Map this to 1. Then the next element, (1 3 5 2 4) = (1 2 3 4 5)(1 2 3 4 5) maps to $1 + 1 = 2$. After we have identified each element of C_k with an element of $\mathbb{Z}_k$, we can always rewrite these numbers in binary. The beauty of binary construction, as is well appreciated in computer science, is that only elements corresponding to powers of two need to be individually

defined, and every other number can be generated from combinations of them. Thus, after this second rewrite, we have a mapping between every cycle in C_k and a binary number. Now to construct the circuit, we only need to implement controlled gates that correspond to cycles that have mapped to a power of two. For C_5, this would be gates that have mapped to 001, 010, and 100 (in decimal: 1, 2, and 4, respectively).

To show how this construction grows, it is most convenient to denote the gates by which power of two they implement. In Figure 4.2, we label gates as 2^j where j ranges from 0 to $\lfloor \log_2(k-1) \rfloor$. To see why $\lfloor \log_2(k-1) \rfloor$ is the final gate, recall the convention that $\mathbb{Z}_k$ always contains 0 instead of k. Then the bound falls out from inspection. Revisiting our above example of $k = 5$, the gates we identified as necessary can be equivalently represented as $001 = 2^0$, $010 = 2^1$, and $100 = 2^2$.

This construction can also be achieved by considering the labeling of the control state. If the computational basis is read as a number in binary, we can clearly define the relationship between the computational basis and the group element construction as $|g\rangle = |g_{\text{binary}}\rangle = |g_{\text{decimal}}\rangle$, where the abstract construction is equivalent to a computational basis in binary, which equivalently realizes the familiar group element in decimal. For example, following the above convention, the basis state for $k = 5$ given by $|(1\ 3\ 5\ 2\ 4)\rangle = |10\rangle = |2\rangle$ indicates that the element (1 3 5 2 4) can be labeled as the 2 element of the group. As 2 is obviously a power of 2, this group element must be encoded in the circuit. This construction is shown generally in Figure 4.2 and for our specific example of $k = 5$ in Figure 4.3. Note that all elements of C_k will take at most $k - 1$ SWAP gates to implement.

Furthermore, note that cyclic permutations can be implemented in a constant depth of two

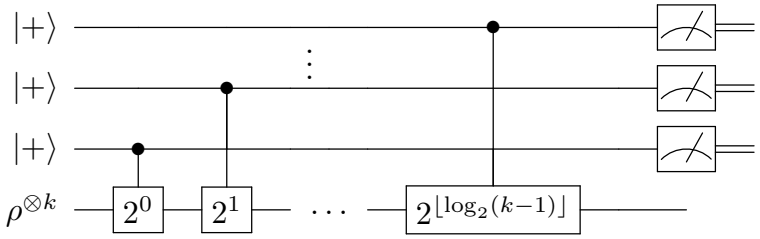


Figure 4.2. Figure demonstrating how to systematically generate a test for the cyclic group of order k. The notation (2^j) indicates the unitary representation of the element in C_k labeled by the j-th power of two. Alternatively, this element is obtained by the full k-cycle $(1, 2, \ldots, k)$ acting on itself 2^j times. Note that the final power is always given by $\lfloor \log_2(k - 1) \rfloor$. Also, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ in the circuit diagram above and the final measurements are performed in the Hadamard basis, accepting if all +1 outcomes occur.

[GB00]. To maintain this depth even for the controlled gates, a GHZ state, $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes m} + |1\rangle^{\otimes m})$, where $m = \lfloor k/2 \rfloor$, can be used instead of a single plus state, similar to the approach employed in [QWK22]. Then the controls can act on different qubits of the state, and the final measurement is taken by projecting back to the GHZ state. This state preparation and the corresponding measurement may add complexity to the ancilla register; however, since the circuit to prepare a k-qubit GHZ state has depth $O(\log_2(k))$ (with the circuit to project onto it being its inverse), this gives the cyclic group test a depth that grows as $O(\log_2(k))$.

To see that this circuit is capable of generating every element of the cyclic group, we again refer to the isomorphism between C_k and $\mathbb{Z}_k$. Writing every element of $\mathbb{Z}_k$ in binary, it becomes obvious that every element can be written as an addition of powers of 2 that form the basis of binary numbers. As such, only elements corresponding to new "digits" need to be considered.

Symmetric Group

We now review a recursive algorithm for the construction of the symmetric group. Necessary to this construction is the proof that the entire group S_k can be generated in a convenient

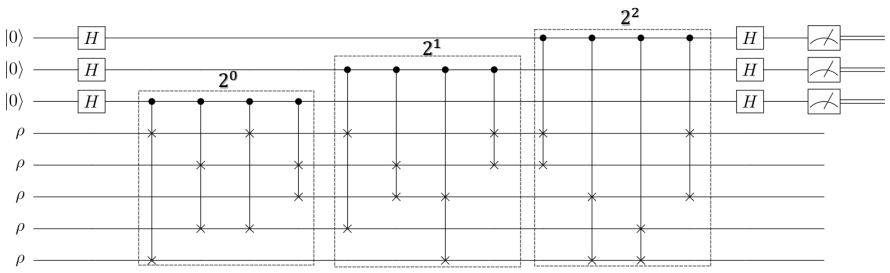


Figure 4.3. An example of the cyclic group test for $k = 5$. The notation (2^j) indicates the unitary representation of the element in C_k labeled by the j-th power of two. For this case, only the elements corresponding to 2^0, 2^1, and 2^2 contribute. Notice that, if the gates are not controlled on the same qubit, each individual cycle collapses to a depth of two with $k - 1$ gates.

way, using solely transpositions. This construction is equivalent to that given in [BBD+97], but we explain it here for convenience.

Observe that S_2 can be generated by the element $(1\ 2)$. To generate S_3, we need only act on this element from the left by $(1\ 3)$ and $(2\ 3)$. Indeed, the remaining elements of S_3 are given by $(1\ 2\ 3) = (1\ 3)(1\ 2)$ and $(1\ 3\ 2) = (2\ 3)(1\ 2)$. This serves as our base case, and we now proceed by induction. Suppose we can generate every element of S_{k-1} in this way. We must show that the remaining elements of S_k are given by acting on S_{k-1} from the left by the transpositions of the form $(i\ k)$ for $i \in \{1, 2, \ldots, k-1\}$. To see this, let $(i_1\ i_2\ \cdots\ i_m)$ be an arbitrary m-cycle in S_{k-1}. Then acting from the left by $(i_j\ k)$ for some $j \in \{1, \ldots, m\}$ yields $(i_j\ k)(i_1\ i_2\ \cdots\ i_m) = (i_1\ i_2\ \cdots\ i_{j-1}\ k\ i_j\ \cdots\ i_m)$. In this way, we can generate every cycle in S_k. Since every element of S_k can be decomposed into a product of disjoint cycles, we can now generate every element of S_k recursively by appending only transpositions of the form $(i\ k)$. We can visualize this construction by the circuit given in Figure 4.4 for an example when $k = 4$.

Given a way to generate S_k, we now need an appropriate control state to implement these elements. By supposition, the identity can always be implemented via the state $|0\rangle$ tensored with

itself to some power. What then for the remaining states? Consider only one 'layer' of the recursive construction of S_k. It suffices to only ever use one transposition at a time. Thus the control state for every i-th layer of transpositions should take the form

$$|+\rangle_{S_i} = \frac{1}{\sqrt{i+1}}(|0\rangle^{\otimes i} + |10\cdots0\rangle + |01\cdots0\rangle + \cdots + |00\cdots1\rangle)\,, \tag{4.43}$$

as given in [BBD+97]. These individual control states should be concatenated together to form the control register for the entire algorithm. For a quick sanity check, when considering the tensor product of such states as i ranges from 1 to k, the normalization constant out in front becomes $\sqrt{k!} = \sqrt{|S_k|}$.

However, a question remains; can the control register for such a circuit also be generated recursively? Observe, in Figure 4.4, that we denote a series of gates A_j that act on the control register to create superpositions. Furthermore, notice that we have arranged the transpositions in a consistent manner such that each gate is appended in ascending order of transposition. Then we define the gate A_j to act as such:

$$A_j|0\rangle^{\otimes j-1} = \frac{1}{\sqrt{j}}(|0\rangle^{\otimes j-1} + |W_{j-1}\rangle)\,, \tag{4.44}$$

where $|W_{j-1}\rangle = \frac{1}{\sqrt{j-1}}\sum_{i=1}^{j-1}|2^i\rangle$ is the W-state on $j-1$ qubits. Here $|2^i\rangle$ is the state with a one in the i-th component and a zero elsewhere. (This is equivalent to the one-hot encoding commonly used in literature.) We can observe by inspection that this action, when taken recursively from $j = 2$ to $j = k$, will generate a superposition over $k!$ basis elements. An example of this construction can be seen in Figure 4.4 for $k = 4$.

There are several choices available to construct these A_j gates. We review two here. One recursive approach is to begin by designing the circuit for A_i; then the next gate A_{i+1} is given by

adding $i+1$ control qubits, initializing the first qubit to a superposition of $(\frac{1}{\sqrt{i}}|0\rangle + \frac{\sqrt{i-1}}{\sqrt{i}}|1\rangle)$, then controlling off of this state, implement A_i on the remaining new qubits. However, this naïve approach will use numerous gates and quickly grow in size. In [BBD+97], they assume the first i qubits are initialized, then add $i+1$ qubits for the recursive step. The $(i+1)$-th qubit can be acted on by a one-qubit gate U_i given by

$$U_i := \frac{1}{\sqrt{i+1}} \begin{pmatrix} 1 & -\sqrt{i} \\ \sqrt{i} & 1 \end{pmatrix}. \tag{4.45}$$

Following this, act simultaneously on the $i+1$ qubit and the remaining qubits with a series of two-qubit gates given by

$$T_{j,j+1} := \frac{1}{\sqrt{i-j+1}} \begin{pmatrix} \sqrt{i-j+1} & 0 & 0 & 0 \\ 0 & 1 & \sqrt{i-j} & 0 \\ 0 & -\sqrt{i-j} & 1 & 0 \\ 0 & 0 & 0 & \sqrt{i-j+1} \end{pmatrix}, \tag{4.46}$$

where j ranges from 1 to $i-1$. This will give the desired control state. In all likelihood, there are even more ways to generate the desired control register. Whichever approach is chosen, the control state should remain the same. Note that the ancilla cost of the control state should be at least $O(k \log_2 k)$ ancilla qubits regardless simply from the magnitude of the symmetric group, $|S_k| = k!$.

Given this construction, it is easy to see the number of controlled-SWAP gates needed to perform the symmetric group test. Indeed, from Figure 4.4, we see that the number of controlled-SWAPs needed when $k = 4$ is $1+2+3 = 6$, where the 1 corresponds to the permutation (1 2) needed to generate S_2, the 2 corresponds to the permutations (2 3) and (1 3) needed to generate S_3 from S_2, and the 3 corresponds to the permutations (3 4), (2 4), and (1 4) needed to generate

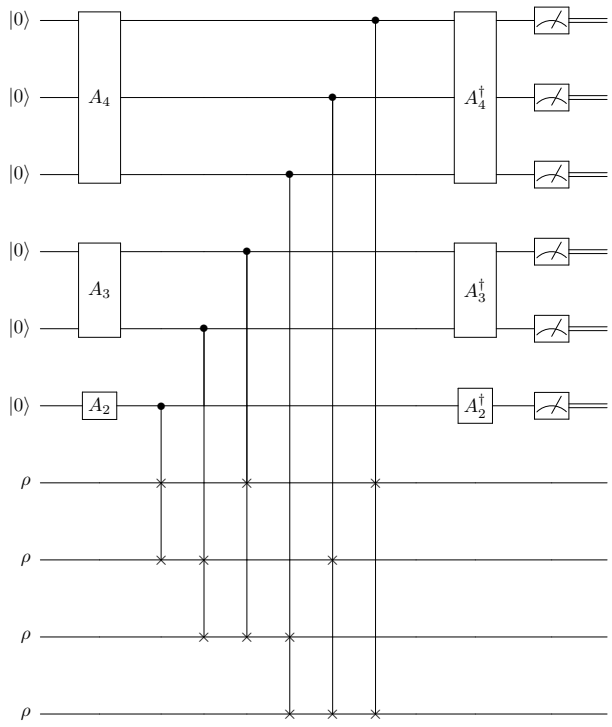


Figure 4.4. Figure demonstrating how to systematically generate a test for the symmetric group of order four.

S_4 from S_3. By induction, the number of controlled-SWAP's needed to perform the k-th symmetric group test is the sum of the first k integers, or $k(k-1)/2$, thus leading to the claimed $O(k^2)$ gate complexity.

Dihedral Group

The dihedral group, D_k is isomorphic to the semi-direct product of $\mathbb{Z}_k$ with $\mathbb{Z}_2$, with $\mathbb{Z}_2$ acting on $\mathbb{Z}_k$ by inversion. As such, it can be formed in a faithful way using a cyclic group generator and a non-commuting action that squares to identity. Using just the generators of the group, it is clear that the unitary flip action adds a factor of two to the number of cyclic gates needed, plus the additional instance of the flip element acting alone. In this manner, the full dihedral group requires at most $2k\log_2(k)$ gates to implement.

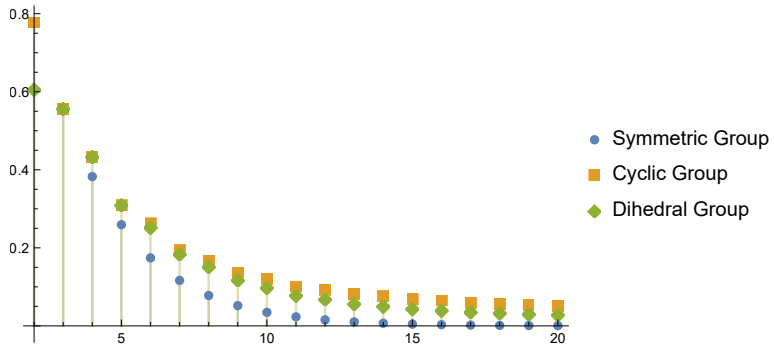


Figure 4.5. Plot of the acceptance probabilities of each separability test as k increases, for the symmetric group S_k, the cyclic group C_k, and the dihedral group D_k. For this example, we use a reduced W-state as an example to illustrate the algorithmic scaling for an unextendible state. For a separable state, all acceptance probabilities are equal to one.

4.4.2. Comparison between Subgroups of the Symmetric Group

Now that we have given a method to count the number of quantum gates necessary for these separability tests, we consider if there is any advantage to using a simpler group as k increases. Essentially, when is the trade-off between additional gates and acceptance probability favorable towards the various tests?

The inherent motivation behind increasing k is to obtain a smaller acceptance probability, prompting the need for Theorem 4.2.2. Clearly, the symmetric test provides the most stringent bound (see Figure 4.5), yet it grows quickly in terms of gate resources needed (see Figure 4.6). The cyclic group, however, benefits from the simplest construction but does not decay as quickly as the full symmetric group.

To visualize this trade-off, we consider the quantity $\frac{R_{\text{test}}}{1-P_{\text{acc}}}$, where R_{test} is the number of resources needed to perform the test via the counting methods described above and P_{acc} is the acceptance probability of the test. We employ the quantity $1 - P_{\text{acc}}$ in the denominator, as we would like the test to have a lower acceptance probability for non-separable states, and thus the denominator will converge to one for better algorithms. This quantifier is very closely aligned

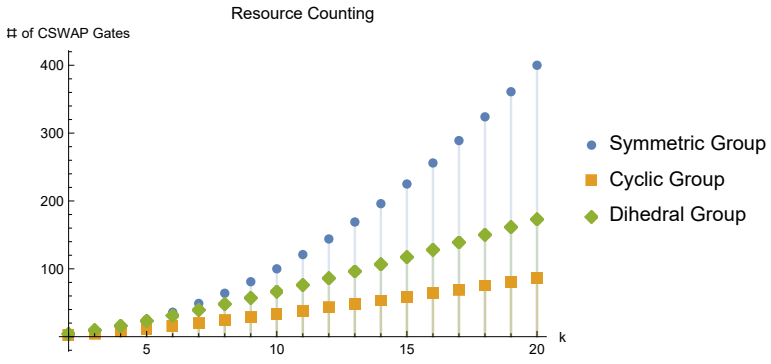


Figure 4.6. Plot of the resource scaling in terms of the number of controlled-SWAP gates used for each group test as k increases. We consider the symmetric group S_k, the cyclic group C_k, and the dihedral group D_k, and we use the gate counting methods described in the text.

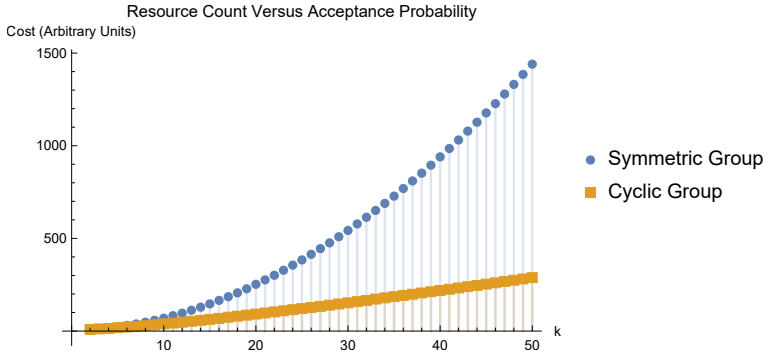


Figure 4.7. We show the ratio of the resources required to rejection probability as k increases. We consider here the cyclic group of k elements as an example of a simple Abelian group and show it gives an advantage in terms of the resources-to-rejection metric over the test generated by the full symmetric group.

with the expected runtime of the algorithm until getting a failure (it would be exactly equal to the expected runtime if we instead used circuit depth over $1 - P_{\text{acc}}$ as the figure of merit). Thus, in comparing this quantity for the various tests, smaller values correspond to more ideal behavior from the algorithms. In Figure 4.7, we show this quantity for algorithms generated by the cyclic group and the symmetric group.

Examining Figure 4.7, we see a clear difference in the performance between the tests generated by the cyclic group and the symmetric group. The plotted ratio can be thought of as resources-to-rejection, in the sense that $1 - P_{\text{acc}}$ is the probability that a non-separable state is

correctly identified—or rather, the failure rate of the algorithm for such a state. Although Figure 4.5 makes it appear that the standard test generated from S_k would always be preferable, we determine from this comparison that the C_k algorithm gives more benefit per gate resource.

From this analysis, we can assert that the simpler test for separability is more cost-efficient than the full permutation test. We show in Figure 4.5 that both tests show a decrease in acceptance probability as k increases, a desirable trait. However, Figure 4.6 shows how quickly circuit sizes grow as k increases, particularly for S_k, which can be considered the standard test. Figure 4.7 bridges these notions to show that the comparative growth in gate resources of S_k outweighs the relative decrease in acceptance probability given over the C_k test. We thus determine that the cyclic group C_k suffices as a separability test of this nature.

4.5. Conclusion

In this chapter, we have presented several separability tests for bipartite pure states, and we have established analytical expressions for their acceptance probabilities. These expressions invariably rely on the cycle index polynomial of the group. Indeed, from a mathematical point of view, this relationship seems natural, due to the inherent combinatorics present in the algorithms. Nonetheless, these expressions give us direct insight into the performance of any separability tests generated from a finite group—which we have shown can be feasibly constructed. Using this perspective, we demonstrate that when utilizing more copies of the state under test, these tests become more stringent. Additionally, we observe that the full symmetric test using a representation of the symmetric group gives a quickly decreasing acceptance probability for an entangled state; however, for the given implementations of these algorithms, other tests can use fewer resources and still show great efficiency.

Here, we have limited ourselves to pure bipartite states; however, we believe multipartite tests may yield results in a similar vein. For instance, a trivial implementation would be to separate all parties into individual tests and then multiply the results. There is a question, however, if more elegant algorithms exist for multipartite cases, and if interesting mathematics arise in the study of such systems.

Data Availability Statement

The datasets generated during and/or analysed during the current study are available in the GitHub repository, https://github.com/mlabo15/GeneralizedSeparability.

Chapter 5. Lagniappe

5.1. Introduction

In Louisiana French, "lagniappe" (pronounced "lan-yap") means some extra inclusion or gift beyond what is strictly necessary. It is often translated as "a little something extra", and this chapter aims to be exactly that. In what follows, we represent three results not yet published or presented in another medium, for whatever reason. The first investigates the use of density matrix exponentiation to obtain a normalized commutator. Second, we consider the impact of using all measurement outcomes in the Hamiltonian symmetry test when the group is Abelian. This is then supplemented with an alternate construction of the Hamiltonian symmetry test from Chapter 2 using block encoding. These findings, all resulting from joint work with Dr. Mark Wilde, are included below as lagniappe.

5.2. Density Matrix Exponentiation and Symmetry Testing

We begin with an approach combining two concepts previously presented in this work—namely, testing the symmetries of quantum states from Chapter 3 and the nested commutator result procured in Chapter 2. We do so by employing density exponentiation [LMR14] as an alternative to the algorithm presented in Section 2.4 previously used to test Hamiltonian symmetry.

Here, we do not delve into the details of density matrix exponentiation but will instead view it as a 'black box' that can be called upon. Following Theorem 1 of [KLL+17], the process of density matrix exponentiation can be summarized thusly: by using $O(\frac{t^2}{\delta})$ copies of a state ρ, one can simulate the unitary channel $(\cdot) \to e^{-i\rho t}(\cdot)e^{i\rho t}$ up to δ-error in diamond distance. That is, there exists a quantum algorithm described by the channel $\mathcal{A}_{SB_1\cdots B_n\to S}$ such that

$$\sup_{\sigma_{RS}} \frac{1}{2} \left\| \mathcal{A}_{SB_1\cdots B_n\to S}(\sigma_{RS} \otimes \rho_{B_1} \otimes \cdots \otimes \rho_{B_n}) - \left(I_R \otimes e^{-i\rho t}\right) \sigma_{RS} \left(I_R \otimes e^{-i\rho t}\right)^\dagger \right\|_1 \leq \delta, \tag{5.1}$$

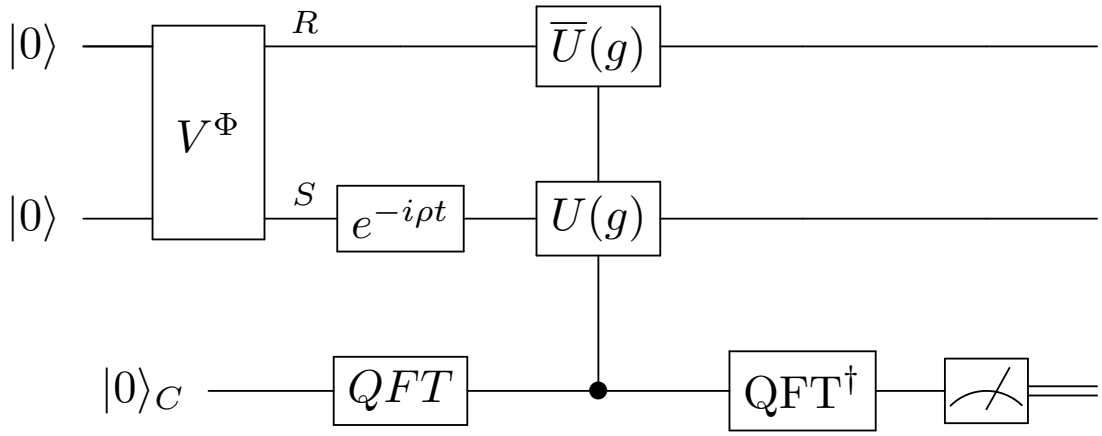


Figure 5.1. Quantum circuit to test for the symmetry of a state via density matrix exponentiation channel. The unitary V^Φ generates the state $|\Phi\rangle_{RS}$, the maximally-entangled state on RA. The exponentiation is achieved via by $e^{-i\rho t}$, and the $U(g)$ gates are controlled on a superposition over all of the elements $g \in G$, as in (2.4).

where the optimization is over every state σ_{RS}, with reference system R arbitrarily large. Observe that this is a method for Hamiltonian simulation where the Hamiltonian in this case is the quantum state ρ. (Indeed, every state is a legitimate Hamiltonian as every state is guaranteed to be Hermitian.)

Given this computational tool, we can now discuss how density matrix exponentiation can be utilized to test a state ρ for symmetry with respect to a group G with projective unitary representation $\{U(g)\}_{g\in G}$. Recall the algorithm from Chapter 2, Section 2.4. This algorithm had an acceptance probability, via (2.15), of

$$\mathrm{Tr}[\Pi^G \left(I_R \otimes e^{iHt}\right) \Phi_{RS} \left(I_R \otimes e^{-iHt}\right)^\dagger] = \frac{1}{d\,|G|} \sum_{g\in G} \mathrm{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}], \tag{5.2}$$

where $\tau = \|H\|_\infty t$. Our goal now is to replace the operator e^{iHt} with the density matrix exponentiation black box previously described, as shown in Figure 5.1.

First, assume that the density matrix exponentiation is ideal. Then the acceptance proba-

bility is found by simply plugging $e^{i\rho t}$ into the above equation, giving

$$\mathrm{Tr}[\Pi^G \left(I_R \otimes e^{i\rho t}\right) \Phi_{RS} \left(I_R \otimes e^{-i\rho t}\right)^\dagger] \,. \tag{5.3}$$

Invoking (5.1), we find that

$$\left|\mathrm{Tr}[\Pi^G \left(I_R \otimes e^{i\rho t}\right) \Phi_{RS} \left(I_R \otimes e^{-i\rho t}\right)^\dagger] - \widetilde{P}_{\mathrm{acc}}\right| \leq \delta \,, \tag{5.4}$$

where

$$\widetilde{P}_{\mathrm{acc}} = \mathrm{Tr}[\Pi^G \mathcal{A}_{SB_1\cdots B_n \to S}(\Phi_{RS} \otimes \rho_{B_1} \otimes \cdots \otimes \rho_{B_n})] \,. \tag{5.5}$$

Then, by plugging in the above, employing the expansion in (2.36), and choosing $\delta = t^4$ such that the error from density matrix exponentiation is of fourth order, we conclude that

$$\widetilde{P}_{\mathrm{acc}} = 1 - \frac{t^2}{2d\,|G|} \sum_{g \in G} \|[U(g), \rho]\|_2^2 + O(t^4), \tag{5.6}$$

given that $\tau = \|H\|_\infty t \leq t$ and $H = \rho$ in this case, so that $\|H\|_\infty \leq 1$.

Thus, the acceptance probability, in this case, includes the measure of asymmetry, the normalized commutator norm $\frac{1}{d|G|} \sum_{g \in G} \|[U(g), \rho]\|_2^2$. Furthermore, the number of copies of ρ needed to realize the expression in (5.6) is $O(t^2/\delta) = O(1/t^2)$.

5.3. Hamiltonian Symmetry Measurement with Abelian Groups

In all of our algorithms, we take as a success only one potential outcome and reject all others. A natural question is whether we can make any use of these other measurement outcomes. To investigate this situation, consider the case of Hamiltonian symmetry described in Chapter 2.

Imagine we construct a control register in the manner we have become accustomed to, as a superposition over group elements $g \in G$, and let us consider as input the maximally-entangled state $|\Phi\rangle$ of dimension d. Then the initial state of the system is

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |\Phi\rangle \,. \tag{5.7}$$

Now perform the controlled unitary $|g\rangle\langle g| \otimes U^\dagger(g)e^{-iHt}U(g)$ to create the state

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle (U^\dagger(g)e^{-iHt}U(g) \otimes \mathbb{I})|\Phi\rangle \,. \tag{5.8}$$

(As for how to implement e^{-iHt}, allow us to borrow arguments given in Chapter 2.) So far, we have not ventured far from our original algorithm; let's remedy that. Instead of the usual measurement, we will measure in the Fourier basis given by

$$|\tilde{g}\rangle \coloneqq \frac{1}{\sqrt{|G|}} \sum_{g\in G} e^{\frac{2\pi i g\tilde{g}}{|G|}} |g\rangle \,. \tag{5.9}$$

Now we must pause to address a difficulty. We have unceremoniously assumed that placing group elements into exponents is an unproblematic step. In fact, this step needs to be approached cautiously. Case in point, those familiar with Lie groups and Lie algebras may think by the factor $e^{\frac{2\pi i g\tilde{g}}{|G|}}$ we are loosely appropriating that structure here—emphatically, this is not the case as we do not assume any sort of Lie group structure. There is an inherent assumption we make in declaring this a measurement, however, that our final outcome will be a real number. We would like to use (5.9) to employ some phase estimation approach, but this requires that $e^{\frac{2\pi i g\tilde{g}}{|G|}}$ not be an operator. To facilitate this, we must require that G is Abelian. Then there exists a one-dimensional representation of G as discussed in Section 1.2.2. We require that the group operation denoted by addition $g + \tilde{g}$ be an equivalent representation to the unitary representation $\{U(g)\}_{g\in G}$ such that

$$g + \tilde{g} \cong U(g)U(\tilde{g}) \,. \tag{5.10}$$

Since we have assumed a one-dimensional representation in the exponent, the product $g\tilde{g}$ will arise from the structure of the complex numbers.

The probability of measuring the state in (5.8) to be in the state $|\tilde{g}\rangle$ is given by

$$\left\| (\langle \tilde{g}|_C \otimes \mathbb{I}) \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C (U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I}) |\Phi\rangle \right) \right\|_2^2$$

$$= \left\| \left(\frac{1}{\sqrt{|G|}} \sum_{g' \in G} e^{-2\pi i g' \tilde{g}/|G|} \langle g'|_C \otimes \mathbb{I} \right) \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C (U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I}) |\Phi\rangle \right) \right\|_2^2 \tag{5.11}$$

$$= \frac{1}{|G|^2} \left\| \sum_{g,g' \in G} e^{-2\pi i g' \tilde{g}/|G|} \langle g'|g\rangle_C \left((U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I}) |\Phi\rangle \right) \right\|_2^2 \tag{5.12}$$

$$= \frac{1}{|G|^2} \left\| \sum_{g \in G} e^{-2\pi i g \tilde{g}/|G|} \left((U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I}) |\Phi\rangle \right) \right\|_2^2 \tag{5.13}$$

$$= \frac{1}{|G|^2} \left(\sum_{g' \in G} e^{2\pi i g' \tilde{g}/|G|} \langle \Phi| \left(U^\dagger(g') e^{iHt} U(g') \otimes \mathbb{I} \right) \right) \left(\sum_{g \in G} e^{-2\pi i g \tilde{g}/|G|} \left(U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I} \right) |\Phi\rangle \right) \tag{5.14}$$

$$= \frac{1}{|G|^2} \sum_{g,g' \in G} e^{2\pi i \tilde{g}(g'-g)/|G|} \langle \Phi| \left(U^\dagger(g') e^{iHt} U(g') U^\dagger(g) e^{-iHt} U(g) \otimes \mathbb{I} \right) |\Phi\rangle \tag{5.15}$$

$$= \frac{1}{d|G|^2} \sum_{g,g' \in G} e^{2\pi i \tilde{g}(g'-g)/|G|} \operatorname{Tr}[U^\dagger(g') e^{iHt} U(g') U^\dagger(g) e^{-iHt} U(g)] \tag{5.16}$$

$$= \frac{1}{d|G|^2} \sum_{g,g' \in G} e^{2\pi i \tilde{g}(g'-g)/|G|} \operatorname{Tr}[U^\dagger(g'-g) e^{iHt} U(g'-g) e^{-iHt}] \tag{5.17}$$

Now we use the assumptions in (5.10) to allow us to rewrite (5.17) in terms of $h \coloneqq g' - g$, giving us

$$\frac{1}{d|G|^2} \sum_{g,h \in G} e^{2\pi i \tilde{g} h/|G|} \operatorname{Tr}[U^\dagger(h) e^{iHt} U(h) e^{-iHt}]$$

$$= \frac{1}{d|G|} \sum_{h \in G} e^{2\pi i \tilde{g} h/|G|} \operatorname{Tr}[U^\dagger(h) e^{iHt} U(h) e^{-iHt}] \tag{5.18}$$

$$= \frac{1}{d|G|} \sum_{g \in G} e^{2\pi i \tilde{g} g/|G|} \operatorname{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] \,. \tag{5.19}$$

Thus, we have derived the probability of observing outcome $|\tilde{g}\rangle$ as

$$\Pr[\tilde{g}] = \frac{1}{d|G|} \sum_{g \in G} e^{2\pi i \tilde{g} g/|G|} \operatorname{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] \,. \tag{5.20}$$

This result bears some resemblance to the case where we only consider the outcome $|0\rangle$, which serves as a nice sanity check. We can also note that the inverse Fourier transform of $\Pr[\tilde{g}]$ is given by

$$\left\{ \frac{1}{d} \operatorname{Tr}[U^\dagger(h) e^{iHt} U(h) e^{-iHt}] \right\}_{h \in G} , \tag{5.21}$$

where each element of (5.21) is a group-averaged out-of-time-order correlator (OTOC) [dMKHMVZ19, SBSSH16, HMY17].

Now, how can such a result be used practically? Suppose we perform this measurement many times, say for N trials, and keep track of the number of times each $|\tilde{g}\rangle$ detection as $N(\tilde{g})$. Then the empirical distribution of $\frac{N(\tilde{g})}{N}$ will converge to $\Pr[\tilde{g}]$ as N becomes large. Of course, we need to determine how large N should be for this to happen. For this purpose, allow us to assign a random variable Y_j^h, taken as a value $e^{-2\pi i \tilde{g} h/|G|}$, if the outcome of the j-th trial is equal to $\tilde{g}$. This generates a set of $|G|$ random variables $\{Y_j^h\}_{h \in G}$ for each trial, $N|G|$ in total. The expectation of the random variable Y_j^h is

$$\begin{aligned}
\mathbb{E}[Y_j^h] &= \sum_{\tilde{g} \in G} \Pr[\tilde{g}] e^{-2\pi i \tilde{g} h/|G|} \\
&= \frac{1}{d|G|} \sum_{g, \tilde{g} \in G} e^{-2\pi i \tilde{g} g/|G|} \operatorname{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] e^{-2\pi i \tilde{g} h/|G|} && (5.22) \\
&= \frac{1}{d} \sum_{g \in G} \operatorname{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] \frac{1}{|G|} \sum_{\tilde{g} \in G} e^{-2\pi i \tilde{g}(g-h)/|G|} && (5.23) \\
&= \frac{1}{d} \sum_{g \in G} \operatorname{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] \delta_{g,h} && (5.24) \\
&= \frac{1}{d} \operatorname{Tr}[U^\dagger(h) e^{iHt} U(h) e^{-iHt}] \,. && (5.25)
\end{aligned}$$

Following the same procedure as in Section 2.5, this can be expanded explicitly in terms of the commutator to show that

$$\begin{aligned}\mathbb{E}[Y_j^h] &= 1 + \frac{t^2}{d}(\mathrm{Tr}[HU(h)^\dagger HU(h)] - \mathrm{Tr}[H^2]) \\ &\quad + \frac{it^3}{2}(\mathrm{Tr}[U(h)^\dagger H^2 U(h) H] - \mathrm{Tr}[U(h)^\dagger HU(h)H^2]) + O(\tau^4) \qquad (5.26) \\ &= 1 - \frac{t^2}{2d}\,\|[U(h), H]\|_2^2 + O(\tau^4)\,, \qquad (5.27)\end{aligned}$$

with $\tau := \|H\|_\infty t < 1$. Then the average $\overline{Y_N^h} := \frac{1}{N}\sum_{j=1}^N Y_j^h$ is an unbiased estimator of the corresponding OTOC from (5.21). The Hoeffding Bound [Hoe94] tells us that to obtain

$$\Pr[|\overline{Y_N^h} - \mathbb{E}[Y_j^h]| \leq \epsilon] \geq 1 - \delta \qquad (5.28)$$

N must satisfy

$$N \geq \frac{4}{\epsilon^2}\ln(\frac{4}{\delta})\,. \qquad (5.29)$$

In such a manner, we can estimate the variables Y_j^h. Unlike the results presented in Chapter 2, this procedure requires a further restriction to Abelian groups, as that allows for a natural one-dimensional representation. However, an interesting future question would be to examine if certain non-Abelian groups (for example, the dihedral groups) might allow for an analogous procedure.

5.4. Block-Encoded Hamiltonian Symmetry

Once again, let us revisit the Hamiltonian symmetry test given in Chapter 2. Suppose, instead of a Trotterization, we have a block-encoding of a Hamiltonian into a unitary matrix. This formalism is a useful tool used to generalize how matrices can be implemented for use in quantum algorithms [LC19, GSLW19], and so we review it briefly here.

Block-encoding allows a complex matrix A with $\|A\|_\infty \leq 1$ to be represented as the upper-left block of a unitary matrix. That is,

$$U = \begin{pmatrix} A & \cdot \\ \cdot & \cdot \end{pmatrix}, \tag{5.30}$$

or, equivalently, $A = (\langle 0| \otimes \mathbb{I})U(|0\rangle \otimes \mathbb{I})$. Then U is called a block-encoding of A. The unitary U can be thought of as a probabilistic implementation of the linear map realized by A. Suppose A acts on a qubits; then, given an a-qubit input state $|\phi\rangle$, acting with U on the state $|0\rangle|phi\rangle$ and post-selecting on a measurement of $|0\rangle$ on the first system will guarantee that the second system contains a state proportional to $A|\psi\rangle$.

Now, let us consider a unitary B a block-encoding of a Hamiltonian H of the form

$$B = \begin{pmatrix} H & \cdot \\ \cdot & \cdot \end{pmatrix}, \tag{5.31}$$

such that

$$(\langle 0|_A \otimes \mathbb{I})B(|0\rangle_A \otimes H)\,, \tag{5.32}$$

where we require that $\|H\|_\infty \leq 1$.

How can we test the symmetry of H using this construction? Let us begin by creating an analogous block encoding of our unitary representation. This can be done via the new representation $\hat{U}(g)$ such that

$$\hat{U}(g) \coloneqq |0\rangle\langle 0|_A \otimes U(g) + (\mathbb{I}_A - |0\rangle\langle 0|_A) \otimes \mathbb{I}\,. \tag{5.33}$$

Next, promote $\hat{U}(g)$ to a controlled unitaries V, with the control state $|+\rangle_C \coloneqq \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle$ such that

$$V \coloneqq \sum_{g\in G} |g\rangle\langle g|_C \otimes (\hat{U}(g))\,. \tag{5.34}$$

Now we can construct a quantum algorithm to test the symmetry of this approach in much the same vein as in Chapter 2 and achieve familiar results. Once again, we consider the initial state of the system to consist of a control register initialized to $|+\rangle_C$ and an input of the maximally-entangled state $|\Phi\rangle$, but we augment this with an ancillary state $|0\rangle_A$. Then the initial state of the system is

$$|+\rangle_C|0\rangle_A|\Phi\rangle\,. \tag{5.35}$$

Then we mimic the action of the algorithm in Chapter 2 replacing $U(g)$ with V and e^{iHt} with $\mathbb{I}_C \otimes B$. That is, we act first with V then $\mathbb{I}_C \otimes B$ then $V^\dagger$. Then the state of the system is

$$V^\dagger(\mathbb{I}_C \otimes B)V|+\rangle_C|0\rangle_A|\Phi\rangle\,. \tag{5.36}$$

Finally, measure C and A, and accept only if the outcome $|+\rangle_C|0\rangle_A$ is observed. This means the acceptance probability is given by

$$\begin{aligned}
&\left\|\langle+|_C\langle 0|_A V^\dagger(\mathbb{I}_C \otimes B)V|+\rangle_C|0\rangle_A|\Phi\rangle\right\|_2^2 \\
&= \left\|\frac{1}{\sqrt{|G|}}\sum_{g'\in G}\langle g'|_C\langle 0|_A V^\dagger(\mathbb{I}_C \otimes B)V\left(\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C|0\rangle_A|\Phi\rangle\right)\right\|_2^2 &(5.37)\\
&= \frac{1}{|G|^2}\left\|\sum_{g,g'\in G}\langle g'|_C\langle 0|_A V^\dagger(\mathbb{I}_C \otimes B)V|g\rangle_C|0\rangle_A|\Phi\rangle\right\|_2^2\,. &(5.38)
\end{aligned}$$

Now, in (5.38), we can substitute in the definition of V from (5.34). (Respectively, we can also easily implement the Hermitian conjugate of (5.34) for $V^\dagger$.) In doing so, we will gain two more summations over the group elements of G; however, using the assumption of orthogonality in our basis states $|g\rangle$, these all can be combined and simplified into a single sum over g. Furthermore, we can easily collapse the measurement over the A system using (5.32). This procedure will thus

simplify (5.38) into

$$\frac{1}{|G|^2}\left\|\sum_{g,g'\in G}\langle g'|_C\langle 0|_A V^\dagger(\mathbb{I}_C\otimes B)V|g\rangle_C|0\rangle_A|\Phi\rangle\right\|_2^2$$

$$=\frac{1}{|G|^2}\left\|\sum_{g\in G}U^\dagger(g)HU(g)|\Phi\rangle\right\|_2^2 \tag{5.39}$$

$$=\frac{1}{|G|^2}\langle\Phi|\left(\sum_{g'\in G}U^\dagger(g')HU(g')\right)\left(\sum_{g\in G}U^\dagger(g)HU(g)\right)|\Phi\rangle \tag{5.40}$$

$$=\frac{1}{|G|^2}\sum_{g,g'\in G}\langle\Phi|U^\dagger(g')HU(g')U^\dagger(g)HU(g)|\Phi\rangle \tag{5.41}$$

$$=\frac{1}{d|G|^2}\sum_{g,g'\in G}\mathrm{Tr}[U^\dagger(g')HU(g')U^\dagger(g)HU(g)] \tag{5.42}$$

$$=\frac{1}{d|G|^2}\sum_{g,g'\in G}\mathrm{Tr}[U(g)U^\dagger(g')HU(g')U^\dagger(g)H]\,, \tag{5.43}$$

where in the last step we use cyclicity of trace. Next, we will use the group homomorphism property of representations and the group operation $g'g^{-1}=h\ \in G$ to continue.

$$=\frac{1}{d|G|^2}\sum_{g,g'\in G}\mathrm{Tr}[U^\dagger(g'g^{-1})HU(g'g^{-1})H] \tag{5.44}$$

$$=\frac{1}{d|G|^2}\sum_{g,h\in G}\mathrm{Tr}[U^\dagger(h)HU(h)H] \tag{5.45}$$

$$=\frac{1}{d|G|}\sum_{h\in G}\mathrm{Tr}[U^\dagger(h)HU(h)H]\,. \tag{5.46}$$

Finally, we arrive at the result that our acceptance probability P_{acc} is given by

$$P_{\text{acc}}=\frac{1}{d|G|}\sum_{g\in G}\mathrm{Tr}[U^\dagger(g)HU(g)H]\,, \tag{5.47}$$

where d is the dimension as usual. This result in (5.47) should look very familiar, as it bares great resemblance to our original result in (2.15); however, without the exponential present, this equation only provides the second order term of 2.40, which is the lowest-order term in which the

commutator appears. As an additional note, whenever H is unitary, no block-encoding is necessary. Thus, we have given an alternate approach to our algorithm in Chapter 2 when the Hamiltonian simulation is available via block encoding.

5.5. Conclusion

With this, we conclude the lagniappe section of this work. In this chapter, we have given an additional test for asymmetry of a quantum state and two expansions on the work of Chapter 2. While not major contributions independently, these results are nonetheless interesting in their own right, and we hope to continue expanding upon these findings in the future. For the time being, however, we can now progress to the conclusion of this work.

Chapter 6. Conclusion

Throughout this thesis, we have demonstrated the intersection of symmetry property testing and quantum computational algorithms. We have introduced various types of symmetry and given their relevant algorithmic tests. We have shown that these tasks can be computationally difficult for classical computers and sometimes quantum computers as well. Nonetheless, we maintain that these results are of interest to both quantum information applications in particular and the field of physics in general.

In Chapter 1 of this thesis, we began with an introduction to background terminology in mathematics and quantum computation. We defined relevant terms in group theory, representation theory, and quantum information in order to make this work self-contained. We further defined some notions of symmetry to be used in future chapters.

In Chapter 2, we gave a quantum computing algorithm to test Hamiltonian dynamics for symmetry with respect to a group. The acceptance probability of this algorithm depended explicitly on the familiar expression of symmetry from quantum mechanics. Furthermore, we were able to show that this algorithm is DQC1-complete, making it unlikely to be efficiently calculable on classical computers. We further expand on these results by giving examples of relevant Hamiltonians calculated using the IBM quantum simulator.

In Chapter 3, we proposed algorithms to test for various notions of symmetry, including G-symmetric extendibility and G-Bose extendibility. The acceptance probabilities of these algorithms are equal to the maximum symmetric fidelity of their respective symmetry, thus endowing these measures with operational meaning. Furthermore, we established resource theories of asymmetry corresponding to the symmetries we have tested.

In Chapter 4, we followed up on a specific subject introduced in the previous chapter—

that of separability tests for pure bipartite states. We established acceptance probabilities for a general class of separability tests derived from G-Bose symmetric extendible tests, specifically showing a reliance on the cycle index polynomial of the group. This result then allowed us to compare the traditional separability test to a simpler cyclic group test, which was shown to be more resource efficient in terms of both depth and number of gates.

Finally, in Chapter 5, we included three additional but related results. We invoked density matrix exponentiation to test the symmetry of a quantum state. We discussed reconsidered the test of Hamiltonian symmetry in which an Abelian group is being used and all measurement outcomes are considered. For the former, we showed that a simple alteration to the permutation symmetry test would suffice to account for this change. For the latter, we demonstrated how such an approach could be used to estimate out-of-time-order correlators. Finally, we gave an alternate approach to the algorithm in Chapter 2 when a block encoding of a Hamiltonian is available.

Further detailed calculations for the primary chapters can be found in the appendices, and all code used for the various projects contained within can be found at the appropriate links at the end of the respective chapters.

Appendix A. Supplementary Material for Chapter 2

The appendices serve primarily to imprison long proofs. Importantly, these proofs give context and credence to the results presented therein. As such, we include them here.

A.1. Acceptance Probability of the First Hamiltonian Symmetry Test

To see that the acceptance probability of the first Hamiltonian symmetry test in Figure 2.1 is given by $\mathrm{Tr}[\Pi^G \Phi^t_{RB}]$, consider that the state just before the measurement is as follows:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C \left(\overline{U}_R(g) \otimes U_B(g) \right) |\Phi^t\rangle_{RB}. \tag{A.1}$$

Then the acceptance probability is given by

$$\begin{aligned}
&\left\| \begin{array}{c} (\langle +|_C \otimes \mathbb{I}_{RB}) \times \\ \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C \left(\overline{U}_R(g) \otimes U_B(g) \right) |\Phi^t\rangle_{RB} \right) \end{array} \right\|_2^2 \\
&= \left\| \begin{array}{c} \left(\frac{1}{\sqrt{|G|}} \sum_{g' \in G} \langle g'|_C \otimes \mathbb{I}_{RB} \right) \times \\ \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C \left(\overline{U}_R(g) \otimes U_B(g) \right) |\Phi^t\rangle_{RB} \right) \end{array} \right\|_2^2 && \text{(A.2)} \\
&= \left\| \frac{1}{|G|} \sum_{g', g \in G} \langle g'|g\rangle_C \left(\overline{U}_R(g) \otimes U_B(g) \right) |\Phi^t\rangle_{RB} \right\|_2^2 && \text{(A.3)} \\
&= \left\| \frac{1}{|G|} \sum_{g \in G} \left(\overline{U}_R(g) \otimes U_B(g) \right) |\Phi^t\rangle_{RB} \right\|_2^2 && \text{(A.4)} \\
&= \left\| \Pi^G |\Phi^t\rangle_{RB} \right\|_2^2 && \text{(A.5)} \\
&= \mathrm{Tr}[\Pi^G \Phi^t_{RB}]. && \text{(A.6)}
\end{aligned}$$

Now we show that

$$P_{\text{acc}} = \mathrm{Tr}[\Pi^G \Phi^t_{RB}] \tag{A.7}$$

is equal to the following expression:

$$P_{\text{acc}} = \frac{1}{d|G|} \sum_{g \in G} \text{Tr}[U^\dagger(g) e^{iHt} U(g) e^{-iHt}] \,. \tag{A.8}$$

To see this, we begin with equation (A.7) and note that, using the cyclicity of the trace, it can be rewritten as

$$\text{Tr}[(\mathbb{I}_R \otimes e^{iHt}) \Pi^G (\mathbb{I}_R \otimes e^{-iHt}) \Phi_{RA}]. \tag{A.9}$$

We can now substitute the definition of the projector given in (1.76), giving

$$\begin{aligned} &\frac{1}{|G|} \text{Tr}[(\mathbb{I}_R \otimes e^{iHt}) \sum_{g \in G} \overline{U}_R(g) \otimes U_A(g) (\mathbb{I}_R \otimes e^{-iHt}) \Phi_{RA}], \\ &\qquad = \frac{1}{|G|} \sum_{g \in G} \text{Tr}[(\mathbb{I}_R \otimes e^{iHt}) \overline{U}_R(g) \otimes U_A(g) (\mathbb{I}_R \otimes e^{-iHt}) \Phi_{RA}], \end{aligned} \tag{A.10}$$

where the second equality follows from the linearity of the trace.

We now want to employ the transpose trick:

$$\mathbb{I}_R \otimes U_A |\Phi\rangle_{RA} = U_R^T \otimes \mathbb{I}_A |\Phi\rangle_{RA}, \tag{A.11}$$

where T denotes the transpose. The description of this action can be easily interpreted through the language of tensor networks [BB17]. Using this relation, we can rewrite the above as

$$\frac{1}{|G|} \sum_{g \in G} \text{Tr}[U_A^\dagger(g) (\mathbb{I}_R \otimes e^{iHt}) U_A(g) (\mathbb{I}_R \otimes e^{-iHt}) \Phi_{RA}]. \tag{A.12}$$

We can now evaluate the trace as a composition of partial traces ($\text{Tr}[\cdot] = \text{Tr}_{RA}[\cdot] = \text{Tr}_A[\text{Tr}_R[\cdot]]$). Computing the trace on R first, we obtain

$$\frac{1}{d|G|} \sum_{g \in G} \text{Tr}[U_A^\dagger(g) e^{iHt} U_A(g) e^{-iHt}], \tag{A.13}$$

which is exactly (2.15).

A.2. Exact Expansion of the Acceptance Probability of the First (Efficient) Hamiltonian Symmetry Test

Here we first prove that the following equality holds:

$$\frac{1}{d\,|G|}\sum_{g\in G}\mathrm{Tr}[U^{\dagger}(g)e^{iHt}U(g)e^{-iHt}] = \frac{1}{d}\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}t^{2n}f(n,k,H,G), \tag{A.14}$$

where

$$f(n,k,H,G) \coloneqq \sum_{k=0}^{n}\binom{2n}{k}\left(2-\delta_{k,n}\right)(-1)^k\,\mathrm{Tr}[\mathcal{T}_G(H^{2n-k})H^k] \tag{A.15}$$

and the group twirl $\mathcal{T}_G$ is defined as

$$\mathcal{T}_G(X) \coloneqq \frac{1}{|G|}\sum_{g\in G}U(g)XU^{\dagger}(g). \tag{A.16}$$

After that, we establish the expansion in (2.42).

Consider that

$$\frac{1}{|G|}\sum_{g}\mathrm{Tr}[U^{\dagger}(g)e^{iHt}U(g)e^{-iHt}] = \mathrm{Tr}[\mathcal{T}_G(e^{iHt})e^{-iHt}] \tag{A.17}$$

$$= \sum_{\ell=0}^{\infty}\frac{(it)^{\ell}}{\ell!}\,\mathrm{Tr}[\mathcal{T}_G(H^{\ell})e^{-iHt}] \tag{A.18}$$

$$= \sum_{\ell,m=0}^{\infty}\frac{(it)^{\ell}\,(-it)^{m}}{\ell!m!}\,\mathrm{Tr}[\mathcal{T}_G(H^{\ell})H^{m}] \tag{A.19}$$

$$= \sum_{\ell,m=0}^{\infty}\frac{(it)^{\ell+m}\,(-1)^{m}}{\ell!m!}\,\mathrm{Tr}[\mathcal{T}_G(H^{\ell})H^{m}] \tag{A.20}$$

$$= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{(it)^{n}\,(-1)^{k}}{n-k!k!}\,\mathrm{Tr}[\mathcal{T}_G(H^{n-k})H^{k}] \tag{A.21}$$

$$= \sum_{n=0}^{\infty}(it)^{n}\sum_{k=0}^{n}\frac{(-1)^{k}}{n-k!k!}\,\mathrm{Tr}[\mathcal{T}_G(H^{n-k})H^{k}] \tag{A.22}$$

Let us consider the term

$$\sum_{k=0}^{n}\frac{(-1)^{k}}{n-k!k!}\,\mathrm{Tr}[\mathcal{T}_G(H^{n-k})H^{k}]. \tag{A.23}$$

Suppose that n is odd. Then consider, with the substitution $\ell = n - k$, that

$$\sum_{k=0}^{n} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] = \sum_{k=0}^{(n-1)/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{k=(n+1)/2}^{n} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.24}$$

$$= \sum_{k=0}^{(n-1)/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{\ell=0}^{(n-1)/2} \frac{(-1)^{n-\ell}}{\ell!n-\ell!} \operatorname{Tr}[\mathcal{T}_G(H^{\ell})H^{n-\ell}] \tag{A.25}$$

$$= \sum_{k=0}^{(n-1)/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{\ell=0}^{(n-1)/2} \frac{(-1)^{n-\ell}}{\ell!n-\ell!} \operatorname{Tr}[\mathcal{T}_G(H^{n-\ell})H^{\ell}] \tag{A.26}$$

$$= \sum_{k=0}^{(n-1)/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{k=0}^{(n-1)/2} \frac{(-1)^{n-k}}{k!n-k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.27}$$

$$= \sum_{k=0}^{(n-1)/2} \frac{(-1)^k + (-1)^{n-k}}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.28}$$

$$= 0. \tag{A.29}$$

The second-to-last line follows from the fact that the twirl is its own adjoint and from cyclicity of trace. For the last line, consider that $(-1)^k + (-1)^{n-k} = 0$ for all $k \in \{0, \ldots, (n-1)/2\}$ when n is odd.

Suppose instead that n is even. Then setting $\ell = n - k$ we find that

$$\sum_{k=0}^{n} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k]$$

$$= \sum_{k=0}^{n/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{k=n/2+1}^{n} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.30}$$

$$= \sum_{k=0}^{n/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{\ell=0}^{n/2-1} \frac{(-1)^{n-\ell}}{\ell!n-\ell!} \operatorname{Tr}[\mathcal{T}_G(H^\ell)H^{n-\ell}] \tag{A.31}$$

$$= \sum_{k=0}^{n/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{k=0}^{n/2-1} \frac{(-1)^{n-k}}{k!n-k!} \operatorname{Tr}[\mathcal{T}_G(H^k)H^{n-k}] \tag{A.32}$$

$$= \sum_{k=0}^{n/2} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] + \sum_{k=0}^{n/2-1} \frac{(-1)^{n-k}}{k!n-k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.33}$$

$$= \frac{(-1)^{n/2}}{(n/2!)^2} \operatorname{Tr}[\mathcal{T}_G(H^{n/2})H^{n/2}] + \sum_{k=0}^{n/2-1} \frac{(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k]$$
$$+ \sum_{k=0}^{n/2-1} \frac{(-1)^{n-k}}{k!n-k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.34}$$

$$= \frac{(-1)^{n/2}}{(n/2!)^2} \operatorname{Tr}[\mathcal{T}_G(H^{n/2})H^{n/2}] + \sum_{k=0}^{n/2-1} \frac{(-1)^k + (-1)^{n-k}}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.35}$$

$$= \frac{(-1)^{n/2}}{(n/2!)^2} \operatorname{Tr}[\mathcal{T}_G(H^{n/2})H^{n/2}] + \sum_{k=0}^{n/2-1} \frac{2\,(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k] \tag{A.36}$$

$$= \sum_{k=0}^{n/2} \frac{\left(2-\delta_{k,n/2}\right)(-1)^k}{n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{n-k})H^k]\,. \tag{A.37}$$

Then the overall formula is given by

$$\frac{1}{d\,|G|} \sum_{g\in G} \operatorname{Tr}[U^\dagger(g)e^{iHt}U(g)e^{-iHt}]$$
$$= \frac{1}{d} \sum_{n=0}^{\infty} (-1)^n\, t^{2n} \sum_{k=0}^{n} \frac{\left(2-\delta_{k,n}\right)(-1)^k}{2n-k!k!} \operatorname{Tr}[\mathcal{T}_G(H^{2n-k})H^k] \tag{A.38}$$

$$= \frac{1}{d} \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} t^{2n} \sum_{k=0}^{n} \binom{2n}{k} \left(2-\delta_{k,n}\right)(-1)^k \operatorname{Tr}[\mathcal{T}_G(H^{2n-k})H^k]. \tag{A.39}$$

Now let us establish the expansion in (2.42). By applying the Baker–Campbell–Hausdorff formula and the nested commutator in (2.43), consider that

$$\operatorname{Tr}[U^\dagger(g)e^{iHt}U(g)e^{-iHt}] = \operatorname{Tr}\left[U^\dagger(g) \sum_{n=0}^{\infty} \frac{[(iHt)^n, U(g)]}{n!}\right] \tag{A.40}$$

$$= \sum_{n=0}^{\infty} \frac{(it)^n}{n!} \operatorname{Tr}\left[U^\dagger(g)\,[(H)^n, U(g)]\right] \tag{A.41}$$

As derived above, it is only necessary to consider even powers in t when including the sum over $g \in G$, and so we consider the following:

$$= \sum_{n=0}^{\infty} \frac{(it)^{2n}}{2n!} \operatorname{Tr}\left[U^\dagger(g)\left[(H)^{2n}, U(g)\right]\right] = \sum_{n=0}^{\infty} \frac{(-1)^n t^{2n}}{2n!} \operatorname{Tr}\left[U^\dagger(g)\left[(H)^{2n}, U(g)\right]\right]. \tag{A.42}$$

Then we find that

$$\begin{aligned}
&\operatorname{Tr}\left[U^\dagger(g)\left[(H)^{2n}, U(g)\right]\right] \\
&= \operatorname{Tr}\left[U^\dagger(g)\left[H, \left[(H)^{2n-1}, U(g)\right]\right]\right] && \text{(A.43)} \\
&= \operatorname{Tr}\left[U^\dagger(g)\left(H\left[(H)^{2n-1}, U(g)\right] - \left[(H)^{2n-1}, U(g)\right]H\right)\right] && \text{(A.44)} \\
&= \operatorname{Tr}\left[\left(U^\dagger(g)H - HU^\dagger(g)\right)\left[(H)^{2n-1}, U(g)\right]\right] && \text{(A.45)} \\
&= \operatorname{Tr}\left[\left[U^\dagger(g), H\right]\left[(H)^{2n-1}, U(g)\right]\right] && \text{(A.46)} \\
&= \operatorname{Tr}\left[\left[U^\dagger(g), H\right]\left(H\left[(H)^{2n-2}, U(g)\right] - \left[(H)^{2n-2}, U(g)\right]H\right)\right] && \text{(A.47)} \\
&= \operatorname{Tr}\left[\left[\left[U^\dagger(g), H\right], H\right]\left[(H)^{2n-2}, U(g)\right]\right] && \text{(A.48)} \\
&= \operatorname{Tr}\left[\left[\left[U^\dagger(g), H\right], H\right]\left(H\left[(H)^{2n-3}, U(g)\right] - \left[(H)^{2n-3}, U(g)\right]H\right)\right] && \text{(A.49)} \\
&= \operatorname{Tr}\left[\left[\left[\left[U^\dagger(g), H\right], H\right], H\right]\left[(H)^{2n-3}, U(g)\right]\right] && \text{(A.50)} \\
&= \operatorname{Tr}\left[\left[U^\dagger(g), (H)^n\right]\left[(H)^n, U(g)\right]\right] && \text{(A.51)} \\
&= \operatorname{Tr}\left[\left(\left[(H)^n, U(g)\right]\right)^\dagger\left[(H)^n, U(g)\right]\right] && \text{(A.52)} \\
&= \left\| \left[(H)^n, U(g)\right] \right\|_2^2. && \text{(A.53)}
\end{aligned}$$

The third-to-last line follows from induction and the second-to-last from the fact that

$$\left[Y^\dagger, (X)^n\right]^\dagger = \left[(X)^n, Y\right], \tag{A.54}$$

for Hermitian X and by using the convention that

$$\left[Y^\dagger, (X)^n\right] \equiv [\cdots[[Y^\dagger, \underbrace{X], X]\cdots, X}_{n \text{ times}}], \tag{A.55}$$

$$\left[Y^\dagger, (X)^0\right] \equiv Y^\dagger. \tag{A.56}$$

Eq. (A.54) follows from applying $[A, B]^\dagger = [B^\dagger, A^\dagger]$ inductively. Plugging back in above, we find that

$$\frac{1}{d\,|G|}\sum_{g\in G}\mathrm{Tr}[U^\dagger(g)e^{iHt}U(g)e^{-iHt}] = \sum_{n=0}^{\infty}\frac{(-1)^n\,t^{2n}}{d\,|G|\,(2n!)}\sum_{g\in G}\left\|\left[(H)^n, U(g)\right]\right\|_2^2. \tag{A.57}$$

A.3. Derivation of Acceptance Probability of the Second (Variational) Hamiltonian Symmetry Test

Here we present an alternative derivation of (2.15), as well as a derivation of (2.45) and (2.46). Suppose that the input to the circuit in Figure 2.2 is a pure state $|\psi\rangle$, rather than the maximally mixed state. Then the initial state of the algorithm is given by

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C|\psi\rangle. \tag{A.58}$$

After the first controlled unitary, the Hamiltonian evolution e^{-iHt}, and the second controlled unitary, the state becomes

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C U(g)e^{-iHt}U^\dagger(g)|\psi\rangle. \tag{A.59}$$

The acceptance probability is then given by

$$\begin{aligned}
&\left\| \begin{array}{c} (\langle +|_C \otimes \mathbb{I})\times \\ \left(\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C U(g)e^{-iHt}U^\dagger(g)|\psi\rangle\right)\end{array}\right\|_2^2 \\
&= \left\| \begin{array}{c} \left(\frac{1}{\sqrt{|G|}}\sum_{g'\in G}\langle g'|_C \otimes \mathbb{I}\right)\times \\ \left(\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C U(g)e^{-iHt}U^\dagger(g)|\psi\rangle\right)\end{array}\right\|_2^2 \qquad (A.60)\\
&= \left\|\frac{1}{|G|}\sum_{g',g\in G}\langle g'|g\rangle_C U(g)e^{-iHt}U^\dagger(g)|\psi\rangle\right\|_2^2 \qquad (A.61)
\end{aligned}$$

$$= \left\| \frac{1}{|G|} \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) |\psi\rangle \right\|_2^2 . \tag{A.62}$$

First let us suppose that the maximally mixed state is input. This is equivalent to picking a pure state $|\psi_x\rangle$ from an orthonormal basis, with probability $1/d$. Then in this case, the acceptance probability is given by

$$\begin{aligned}
&\frac{1}{d} \sum_{x=1}^{d} \left\| \frac{1}{|G|} \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) |\psi_x\rangle \right\|_2^2 \\
&= \frac{1}{d} \sum_{x=1}^{d} \left(\frac{1}{|G|} \sum_{g' \in G} \langle \psi_x | U(g') e^{iHt} U^\dagger(g') \right) \left(\frac{1}{|G|} \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) |\psi_x\rangle \right) && \text{(A.63)} \\
&= \frac{1}{d\,|G|^2} \sum_{x=1}^{d} \sum_{g',g \in G} \langle \psi_x | U(g') e^{iHt} U^\dagger(g') U(g) e^{-iHt} U^\dagger(g) |\psi_x\rangle && \text{(A.64)} \\
&= \frac{1}{d\,|G|^2} \sum_{x=1}^{d} \sum_{g',g \in G} \mathrm{Tr}[U^\dagger(g) |\psi_x\rangle\langle\psi_x| U(g') e^{iHt} U^\dagger(g') U(g) e^{-iHt}] && \text{(A.65)} \\
&= \frac{1}{d\,|G|^2} \sum_{g',g \in G} \mathrm{Tr}\left[U^\dagger(g) U(g') e^{iHt} U^\dagger(g') U(g) e^{-iHt} \right] && \text{(A.66)} \\
&= \frac{1}{d\,|G|^2} \sum_{g',g \in G} \mathrm{Tr}\left[U^\dagger(g' \circ g) e^{iHt} U(g' \circ g) e^{-iHt} \right] && \text{(A.67)} \\
&= \frac{1}{d\,|G|} \sum_{g \in G} \mathrm{Tr}\left[U^\dagger(g) e^{iHt} U(g) e^{-iHt} \right] . && \text{(A.68)}
\end{aligned}$$

The second-to-last equality follows from the group property and the fact that $U(g)$ is a representation of g. So this provides an alternate proof of (2.15).

Now let us prove the expansion in (2.44). Consider that

$$\begin{aligned}
&\left\| \frac{1}{|G|} \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) |\psi\rangle \right\|_2^2 \\
&= \left\| \mathcal{T}_G(e^{-iHt}) |\psi\rangle \right\|_2^2 && \text{(A.69)} \\
&= \langle \psi | \mathcal{T}_G(e^{iHt}) \mathcal{T}_G(e^{-iHt}) |\psi\rangle && \text{(A.70)}
\end{aligned}$$

$$= \langle\psi|\mathcal{T}_G\left(\mathbb{I} + iHt - H^2t^2/2 + O(\tau^3)\right)\mathcal{T}_G\left(\mathbb{I} - iHt - H^2t^2/2 + O(\tau^3)\right)|\psi\rangle \tag{A.71}$$

$$= \langle\psi|\left(\mathbb{I} + it\mathcal{T}_G(H) - \left(t^2/2\right)\mathcal{T}_G(H^2) + O(\tau^3)\right)\left(\mathbb{I} - it\mathcal{T}_G(H) - \left(t^2/2\right)\mathcal{T}_G(H^2) + O(\tau^3)\right)|\psi\rangle \tag{A.72}$$

$$= 1 + t^2\langle\psi|\left(\mathcal{T}_G(H)\right)^2|\psi\rangle - t^2\langle\psi|\mathcal{T}_G(H^2)|\psi\rangle + O(\tau^3) \tag{A.73}$$

$$= 1 - t^2\langle\psi|\left(\mathcal{T}_G(H^2) - \left(\mathcal{T}_G(H)\right)^2\right)|\psi\rangle + O(\tau^3) \tag{A.74}$$

$$= 1 - t^2\left\langle\mathcal{T}_G(H^2) - \left(\mathcal{T}_G(H)\right)^2\right\rangle_\psi + O(\tau^3). \tag{A.75}$$

The Kadison–Schwarz inequality [Bha07, Theorem 2.3.2] implies the following operator inequality:

$$\mathcal{T}_G(H^2) \geq \left(\mathcal{T}_G(H)\right)^2. \tag{A.76}$$

As a consequence, the following inequality holds for every state $|\psi\rangle$:

$$\left\langle\mathcal{T}_G(H^2) - \left(\mathcal{T}_G(H)\right)^2\right\rangle_\psi \geq 0. \tag{A.77}$$

If we perform a maximization of the acceptance probability over every input state $|\psi\rangle$, then it is equal to

$$\max_{|\psi\rangle:\||\psi\rangle\|_2=1}\left\|\frac{1}{|G|}\sum_{g\in G}U(g)e^{-iHt}U^\dagger(g)|\psi\rangle\right\|_2^2$$

$$= \left\|\frac{1}{|G|}\sum_{g\in G}U(g)e^{-iHt}U^\dagger(g)\right\|_\infty^2 \tag{A.78}$$

$$= \left\|\frac{1}{|G|}\sum_{g\in G}\left(\left[U(g), e^{-iHt}\right] + e^{-iHt}U(g)\right)U^\dagger(g)\right\|_\infty^2 \tag{A.79}$$

$$= \left\|\frac{1}{|G|}\sum_{g\in G}\left(\left[U(g), e^{-iHt}\right]U^\dagger(g) + e^{-iHt}\right)\right\|_\infty^2 \tag{A.80}$$

$$= \left\|e^{-iHt} + \frac{1}{|G|}\sum_{g\in G}\left[U(g), e^{-iHt}\right]U^\dagger(g)\right\|_\infty^2 \tag{A.81}$$

$$\geq \left(\left\| e^{-iHt} \right\|_\infty - \left\| \frac{1}{|G|} \sum_{g \in G} \left[U(g), e^{-iHt} \right] U^\dagger(g) \right\|_\infty \right)^2 \tag{A.82}$$

$$= \left(1 - \left\| \frac{1}{|G|} \sum_{g \in G} \left[U(g), e^{-iHt} \right] U^\dagger(g) \right\|_\infty \right)^2 \tag{A.83}$$

$$\geq \left(1 - \frac{1}{|G|} \sum_{g \in G} \left\| \left[U(g), e^{-iHt} \right] U^\dagger(g) \right\|_\infty \right)^2 \tag{A.84}$$

$$= \left(1 - \frac{1}{|G|} \sum_{g \in G} \left\| \left[U(g), e^{-iHt} \right] \right\|_\infty \right)^2 \tag{A.85}$$

$$\geq 1 - \frac{2}{|G|} \sum_{g \in G} \left\| \left[U(g), e^{-iHt} \right] \right\|_\infty . \tag{A.86}$$

The first inequality follows from the reverse triangle inequality. The next equality follows because $\left\| e^{-iHt} \right\|_\infty = 1$. The second inequality follows from the triangle inequality. The final equality follows from the unitary invariance of the spectral norm. Thus we have established (2.45).

Now suppose that $\|H\|_\infty t < 1$. Then we find that

$$\left\| \left[U(g), e^{-iHt} \right] \right\|_\infty$$

$$= \left\| \left[U(g), \mathbb{I} - iHt + \sum_{n=2}^{\infty} \frac{(-iHt)^n}{n!} \right] \right\|_\infty \tag{A.87}$$

$$= \left\| -it \left[U(g), H \right] + \left[U(g), \sum_{n=2}^{\infty} \frac{(-iHt)^n}{n!} \right] \right\|_\infty \tag{A.88}$$

$$\leq t \left\| [U(g), H] \right\|_\infty + \left\| \left[U(g), \sum_{n=2}^{\infty} \frac{(-iHt)^n}{n!} \right] \right\|_\infty \tag{A.89}$$

$$\leq t \left\| [U(g), H] \right\|_\infty + 2 \left\| \sum_{n=2}^{\infty} \frac{(-iHt)^n}{n!} \right\|_\infty \tag{A.90}$$

$$\leq t \left\| [U(g), H] \right\|_\infty + 2 \sum_{n=2}^{\infty} \frac{(\|H\|_\infty t)^n}{n!} \tag{A.91}$$

$$\leq t \left\| [U(g), H] \right\|_\infty + 2 (\|H\|_\infty t)^2 \sum_{n=2}^{\infty} \frac{1}{n!} \tag{A.92}$$

$$= t \left\| [U(g), H] \right\|_\infty + 2 \left(\|H\|_\infty t \right)^2 (e - 2) \tag{A.93}$$

$$\leq t \left\| [U(g), H] \right\|_\infty + 2 \|H\|_\infty^2 t^2, \tag{A.94}$$

where the second-to-last inequality follows from the assumption that $\|H\|_\infty t < 1$. This implies that

$$\frac{1}{|G|^2} \max_{|\psi\rangle} \left\| \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) |\psi\rangle \right\|_2^2 \geq 1 - \frac{2t}{|G|} \sum_{g \in G} \left\| [U(g), H] \right\|_\infty - 4 \|H\|_\infty^2 t^2, \tag{A.95}$$

thus establishing (2.46).

We now prove (2.47). Consider that

$$\left\| \frac{1}{|G|} \sum_{g \in G} U(g) e^{-iHt} U^\dagger(g) \right\|_\infty^2$$

$$= \left\| \frac{1}{|G|} \sum_{g \in G} e^{iHt} U(g) e^{-iHt} U^\dagger(g) \right\|_\infty^2 \tag{A.96}$$

$$= \left\| \frac{1}{|G|} \sum_{g \in G} \sum_{n=0}^{\infty} \frac{[(iHt)^n, U(g)]}{n!} U^\dagger(g) \right\|_\infty^2 \tag{A.97}$$

$$= \left\| \sum_{n=0}^{\infty} \frac{(it)^n}{n!} \frac{1}{|G|} \sum_{g \in G} [(H)^n, U(g)] \, U^\dagger(g) \right\|_\infty^2 \tag{A.98}$$

$$= \left\| \mathbb{I} + \sum_{n=1}^{\infty} \frac{(it)^n}{n!} \frac{1}{|G|} \sum_{g \in G} [(H)^n, U(g)] \, U^\dagger(g) \right\|_\infty^2 \tag{A.99}$$

$$\geq \left(\|\mathbb{I}\|_\infty - \left\| \sum_{n=1}^{\infty} \frac{(it)^n}{n!} \frac{1}{|G|} \sum_{g \in G} [(H)^n, U(g)] \, U^\dagger(g) \right\|_\infty \right)^2 \tag{A.100}$$

$$= \left(1 - \left\| \sum_{n=1}^{\infty} \frac{(it)^n}{n!} \frac{1}{|G|} \sum_{g \in G} [(H)^n, U(g)] \, U^\dagger(g) \right\|_\infty \right)^2 \tag{A.101}$$

$$\geq \left(1 - \sum_{n=1}^{\infty} \frac{t^n}{n!} \frac{1}{|G|} \sum_{g \in G} \left\| [(H)^n, U(g)] \, U^\dagger(g) \right\|_\infty \right)^2 \tag{A.102}$$

$$= \left(1 - \sum_{n=1}^{\infty} \frac{t^n}{n!} \frac{1}{|G|} \sum_{g \in G} \| [(H)^n, U(g)] \|_\infty \right)^2 . \tag{A.103}$$

In the above, we employed unitary invariance of the spectral norm, the Baker–Campbell–Hausdorff formula, and the triangle inequality.

Appendix B. Supplementary Material for Chapter 3

B.1. Proof of Theorem 3.2.1

Let ψ_{RS} be an arbitrary purification of ρ_S, and consider that

$$\operatorname{Tr}[\Pi_S^G \rho_S] = \operatorname{Tr}[(I_R \otimes \Pi_S^G)\psi_{RS}] \tag{B.1}$$

$$= \left\| \left(I_R \otimes \Pi_S^G \right) |\psi\rangle_{RS} \right\|_2^2 . \tag{B.2}$$

Recall the following property of the norm of an arbitrary vector $|\varphi\rangle$:

$$\| |\varphi\rangle \|_2^2 = \max_{|\phi\rangle : \| |\phi\rangle \|_2 = 1} |\langle \phi | \varphi \rangle|^2 . \tag{B.3}$$

This follows from the Cauchy–Schwarz inequality and the conditions for saturating it. This implies that

$$\left\| \left(I_R \otimes \Pi_S^G \right) |\psi\rangle_{RS} \right\|_2^2 = \max_{|\phi\rangle : \| |\phi\rangle \|_2 = 1} \left| \langle \phi |_{RS} \left(I_R \otimes \Pi_S^G \right) |\psi\rangle_{RS} \right|^2 \tag{B.4}$$

Let us also recall Uhlmann's theorem [Uhl76]: For positive semi-definite operators ω_A and τ_A and corresponding rank-one operators ψ_{RA}^{ω} and ψ_{RA}^{τ} satisfying

$$\operatorname{Tr}_R[\psi_{RA}^{\omega}] = \omega_A, \tag{B.5}$$

$$\operatorname{Tr}_R[\psi_{RA}^{\tau}] = \tau_A, \tag{B.6}$$

Uhlmann's theorem [Uhl76] states that

$$F(\omega_A, \tau_A) = \left\| \sqrt{\omega_A} \sqrt{\tau_A} \right\|_1^2 \tag{B.7}$$

$$= \max_{V_R} |\langle \psi^{\omega} |_{RA} \left(V_R \otimes I_A \right) |\psi^{\tau}\rangle_{RA}|^2 , \tag{B.8}$$

where the optimization is over every unitary V_R acting on the reference system R. We also implicitly defined fidelity more generally for positive semi-definite operators. Considering that

$$\rho_S = \operatorname{Tr}_R[\psi_{RS}], \qquad \sigma_S := \operatorname{Tr}_R[\phi_{RS}], \tag{B.9}$$

so that

$$\Pi_S^G \sigma_S \Pi_S^G = \mathrm{Tr}_R[\Pi_S^G \phi_{RS} \Pi_S^G], \tag{B.10}$$

we conclude that

$$\begin{aligned}\max_{|\phi\rangle:\||\phi\rangle\|_2=1} \left|\langle\phi|_{RS}\left(I_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right|^2 &= \max_{|\phi\rangle:\||\phi\rangle\|_2=1} \max_{U_R} \left|\langle\phi|_{RS}\left(U_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right|^2 \\ &= \max_{\sigma_S \in \mathcal{D}(\mathcal{H}_S)} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G). \end{aligned} \tag{B.11}$$

where the last equality follows from Uhlmann's theorem with the identifications $|\psi^\omega\rangle \leftrightarrow (I \otimes \Pi^G)|\phi\rangle$ and $|\psi^\tau\rangle \leftrightarrow |\psi\rangle$. Clearly, we have that

$$\begin{aligned}\max_{\sigma_S \in \mathcal{D}(\mathcal{H}_S)} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G) &\geq \max_{\sigma \in \text{B-Sym}_G} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G) \\ &= \max_{\sigma \in \text{B-Sym}_G} F(\rho_S, \sigma_S), \end{aligned} \tag{B.12}$$

because $\text{B-Sym}_G \subset \mathcal{D}(\mathcal{H})$. Now let us consider showing the opposite inequality. Let $\sigma \in \mathcal{D}(\mathcal{H})$. If $\Pi^G \sigma \Pi^G = 0$, then this is a suboptimal choice as it follows that the objective function $F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G) = 0$ in this case. So, let us suppose this is not the case. Then define

$$\sigma' := \frac{1}{p} \Pi^G \sigma \Pi^G, \tag{B.13}$$

$$p := \mathrm{Tr}[\Pi^G \sigma], \tag{B.14}$$

and observe that $\sigma'_S \in \text{B-Sym}_G$. Consider that

$$F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G) = p F(\rho_S, \sigma'_S) \tag{B.15}$$

$$\leq F(\rho_S, \sigma'_S) \tag{B.16}$$

$$\leq \max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S). \tag{B.17}$$

We have thus proved the opposite inequality, concluding the proof.

B.2. Proof of Theorem 3.2.3

Following the same reasoning given in (3.34)–(3.41), by using Uhlmann's theorem, we conclude that

$$\max_{V_{S'E\to RE'}} \left\| \Pi^G_{RS} V_{S'E\to RE'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS} \sigma_{RS} \Pi^G_{RS}]), \tag{B.18}$$

where the optimization is over every state σ_{RS} and Π^G_{RS} is defined in (3.65). The next part of the proof shows that

$$\max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS} \sigma_{RS} \Pi^G_{RS}]) = \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S) \tag{B.19}$$

and is similar to (3.42)–(3.59). To justify the inequality $\geq$, let σ_S be an arbitrary state in BSE_G. Then by Definition 1.4.2, this means that there exists a state ω_{RS} such that $\mathrm{Tr}_R[\omega_{RS}] = \sigma_S$ and $\Pi^G_{RS} \omega_{RS} \Pi^G_{RS} = \omega_{RS}$. This means that

$$F(\rho_S, \sigma_S) = F(\rho_S, \mathrm{Tr}_R[\omega_{RS}]) \tag{B.20}$$

$$= F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS} \omega_{RS} \Pi^G_{RS}]) \tag{B.21}$$

$$\leq \max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS} \sigma_{RS} \Pi^G_{RS}]), \tag{B.22}$$

which implies that

$$\max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS} \sigma_{RS} \Pi^G_{RS}]) \geq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S) \tag{B.23}$$

To justify the inequality $\leq$, let σ_{RS} be an arbitrary state. If $\Pi^G_{RS} \sigma_{RS} \Pi^G_{RS} = 0$, then the desired inequality trivially follows. Supposing then that this is not the case, let us define

$$\sigma'_{RS} := \frac{1}{p} \Pi^G_{RS} \sigma_{RS} \Pi^G_{RS}, \tag{B.24}$$

$$p := \mathrm{Tr}[\Pi^G_{RS} \sigma_{RS}]. \tag{B.25}$$

We then find that

$$F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) = pF(\rho_S, \mathrm{Tr}_R[\sigma'_{RS}]) \tag{B.26}$$

$$\leq F(\rho_S, \mathrm{Tr}_R[\sigma'_{RS}]). \tag{B.27}$$

Consider that $\sigma'_S \coloneqq \mathrm{Tr}_R[\sigma'_{RS}]$ is G-Bose symmetric extendible because σ'_{RS} is an extension of it that satisfies $\Pi^G_{RS}\sigma'_{RS}\Pi^G_{RS} = \sigma'_{RS}$. We conclude that

$$F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \leq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S). \tag{B.28}$$

Since this inequality holds for every state σ_{RS}, we surmise the desired result

$$\max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \leq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S). \tag{B.29}$$

B.3. Proof of Theorem 3.2.4

Following the same reasoning given in (3.34)–(3.41), by using Uhlmann's theorem, we conclude that

$$\max_{V_{S'E\to R\hat{R}\hat{S}E'}} \left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right\|_2^2 = \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]), \tag{B.30}$$

where the optimization is over every state $\sigma_{RS\hat{R}\hat{S}}$ and $\Pi^G_{RS\hat{R}\hat{S}}$ is defined in (1.46). The next part of the proof shows that

$$\max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) = \max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S) \tag{B.31}$$

and is similar to (3.42)–(3.59). To justify the inequality $\geq$, let σ_S be a state in SymExt_G. Then by Theorem 1.4.1, there exists a purification $\varphi_{RS\hat{R}\hat{S}}$ of σ_S satisfying $\varphi_{RS\hat{R}\hat{S}} = \Pi^G_{RS\hat{R}\hat{S}}\varphi_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}$. We find that

$$F(\rho_S, \sigma_S) = F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\varphi_{RS\hat{R}\hat{S}}]) \tag{B.32}$$

$$= F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}} \varphi_{RS\hat{R}\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}]) \tag{B.33}$$

$$\leq \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}]). \tag{B.34}$$

Since the inequality holds for all $\sigma_S \in \mathrm{SymExt}_G$, we conclude that

$$\max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S) \leq \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}]). \tag{B.35}$$

To justify the inequality $\leq$, let $\sigma_{R\hat{R}S\hat{S}}$ be an arbitrary state. If $\Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}} \Pi^G_{RS\hat{R}\hat{S}} = 0$, then the desired inequality follows trivially. Suppose this is not the case, then define

$$\sigma'_{R\hat{R}S\hat{S}} \coloneqq \frac{1}{p} \Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}, \tag{B.36}$$

$$p \coloneqq \mathrm{Tr}[\Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}}]. \tag{B.37}$$

Then we find that

$$F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}} \sigma_{R\hat{R}S\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}]) = pF(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]) \tag{B.38}$$

$$\leq F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]) \tag{B.39}$$

$$= F(\rho_S, \tau_S), \tag{B.40}$$

where $\tau_S \coloneqq \mathrm{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]$. We now aim to show that $\tau_S \in \mathrm{SymExt}_G$. To do so, it suffices to prove that $\sigma'_{RS} = U_{RS}(g) \sigma'_{RS} U_{RS}(g)^\dagger$ for all $g \in G$. Abbreviating $U \otimes \overline{U} \equiv U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)$, consider that

$$\sigma'_{RS} = \mathrm{Tr}_{\hat{R}\hat{S}}[\sigma'_{RS\hat{R}\hat{S}}] \tag{B.41}$$

$$= \mathrm{Tr}_{\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}} \sigma'_{RS\hat{R}\hat{S}} \Pi^G_{RS\hat{R}\hat{S}}] \tag{B.42}$$

$$= \mathrm{Tr}_{\hat{R}\hat{S}}[(U \otimes \overline{U}) \Pi^G_{RS\hat{R}\hat{S}} \sigma'_{RS\hat{R}\hat{S}} \Pi^G_{RS\hat{R}\hat{S}} (U \otimes \overline{U})^\dagger] \tag{B.43}$$

$$= U \, \mathrm{Tr}_{\hat{R}\hat{S}}[\overline{U} \Pi^G_{RS\hat{R}\hat{S}} \sigma'_{RS\hat{R}\hat{S}} \Pi^G_{RS\hat{R}\hat{S}} \overline{U}^\dagger] U^\dagger \tag{B.44}$$

$$= U \operatorname{Tr}_{\hat{R}\hat{S}}[\overline{U}^{\dagger}\overline{U}\Pi^{G}_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^{G}_{RS\hat{R}\hat{S}}]U^{\dagger} \tag{B.45}$$

$$= U \operatorname{Tr}_{\hat{R}\hat{S}}[\Pi^{G}_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^{G}_{RS\hat{R}\hat{S}}]U^{\dagger} \tag{B.46}$$

$$= U \operatorname{Tr}_{\hat{R}\hat{S}}[\sigma'_{RS\hat{R}\hat{S}}]U^{\dagger} \tag{B.47}$$

$$= U_{RS}(g)\sigma'_{RS}U_{RS}(g)^{\dagger}. \tag{B.48}$$

It follows that $\tau_S \in \text{SymExt}_G$, and we conclude that

$$F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^{G}_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^{G}_{RS\hat{R}\hat{S}}]) \leq \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S). \tag{B.49}$$

Since the inequality holds for every state $\sigma_{R\hat{R}S\hat{S}}$, we conclude that

$$\max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^{G}_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^{G}_{RS\hat{R}\hat{S}}]) \leq \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S). \tag{B.50}$$

B.4. Proof of Proposition 3.4.5

The idea of the proof is similar to that for Proposition 3.4.3. Since ρ_S is a G-BSE state, by Definition 1.4.2, there exists an extension state ω_{RS} satisfying the conditions stated there. Since $\mathcal{N}_{S\to S'}$ is a G-BSE channel, by Definition 3.4.3, there exists an extension channel $\mathcal{M}_{RS\to R'S'}$ satisfying the conditions stated there. It follows that $\mathcal{M}_{RS\to R'S'}(\omega_{RS})$ is an extension of $\mathcal{N}_{S\to S'}(\rho_S)$ because

$$\operatorname{Tr}_{R'}[\mathcal{M}_{RS\to R'S'}(\omega_{RS})] = \mathcal{N}_{S\to S'}(\operatorname{Tr}_R[\omega_{RS}]) \tag{B.51}$$

$$= \mathcal{N}_{S\to S'}(\rho_S), \tag{B.52}$$

where the first equality follows from (3.167). Also, consider that the following holds

$$1 \geq \operatorname{Tr}[\Pi^{G}_{R'S'}\mathcal{M}_{RS\to R'S'}(\omega_{RS})]$$

$$= \operatorname{Tr}[(\mathcal{M}_{RS\to R'S'})^{\dagger}(\Pi^{G}_{R'S'})\omega_{RS}] \tag{B.53}$$

$$\geq \mathrm{Tr}[\Pi^{G}_{RS}\omega_{RS}] \tag{B.54}$$

$$= 1. \tag{B.55}$$

The first inequality follows because $\mathcal{M}_{RS\to R'S'}(\omega_{RS})$ is a state and $\Pi^{G}_{R'S'}$ is projection. The first equality follows from the definition of channel adjoint. The second inequality follows from (3.168). where the first equality follows from (3.150) and the second from (3.2). We conclude that $\mathrm{Tr}[\Pi^{G}_{R'S'}\mathcal{M}_{RS\to R'S'}(\omega_{RS})] = 1$, which by (3.16), implies that $\mathcal{M}_{RS\to R'S'}(\omega_{RS})$ is a G-Bose symmetric state. It then follows that $\mathcal{N}_{S\to S'}(\rho_S)$ is G-Bose symmetric extendible.

Appendix C. Copyright Information

This dissertation uses material from a previously published article in which the dissertation writer was an author.

C.1. Chapter 2

Chapter 2 contains material from the article "Quantum Algorithms for Testing Hamiltonian Symmetry" by Margarite L. LaBorde and Mark M. Wilde. This article is published in *Physical Review Letter* by publisher American Physical Society (APS) and is copyrighted by American Physical Society as of 2022.

Below is the response by APS to a request for written permission to include this work in the dissertation:

Margarite LaBorde
Apr 23, 2023, 6:04 PM EDT

To whom it may concern:

I am writing to request written permission to include portions of the article "Quantum Algorithms for Testing Hamiltonian Symmetry" by Margarite L. LaBorde and Mark M. Wilde, published in Physical Review Letters, in my PhD dissertation.

The dissertation will be available through LSU Digital Commons, an open-access digital repository. LSU asserts prior claim on theses and dissertations to the extent that LSU "reserves a nonexclusive, paid-up, royalty-free right to distribute copies of Course Materials, theses and dissertations, both internally and to third parties, whether by electronic means, microfilm, and otherwise."

In the chapter of the dissertation containing the material, an acknowledgement will be given using your (the publisher's) preferred phrasing.

Best regards,
Margarite LaBorde
PhD Candidate
Department of Physics and Astronomy
Louisiana State University

Figure C.1.

APS Help Desk <help@aps.org>
Mon 4/24/2023 8:23 AM
To: Margarite LaBorde <margaritelaborde@hotmail.com>
Cc: mlabo15@lsu.edu <mlabo15@lsu.edu>

Tydria Clarke-Kittrell (APS)
Apr 24, 2023, 9:23 AM EDT

Hello,

Thank you for writing. Kindly refer to our Copyright FAQ located at https://journals.aps.org/copyrightFAQ.html, specifically:

Q) - "As the author of an APS-published article, may I include my article or a portion of my article in my thesis or dissertation?"

A) - "Yes, the author has the right to use the article or a portion of the article in a thesis or dissertation without requesting permission from APS, provided the bibliographic citation and the APS copyright credit line are given on the appropriate pages."

I hope this is helpful to you.

Warm Regards,
Tydria
Help@aps.org

Figure C.2.

Bibliography

[Aar13] Scott Aaronson. *Quantum computing since Democritus*. Cambridge University Press, 2013.

[AS67] Yakir Aharonov and Leonard Susskind. Charge superselection rule. *Physical Review*, 155(5):1428–1431, March 1967.

[BACS07] Dominic W. Berry, Graeme Ahokas, Richard Cleve, and Barry C. Sanders. Efficient quantum algorithms for simulating sparse hamiltonians. *Communications in Mathematical Physics*, 270(2):359–371, 2007.

[BB17] Jacob Biamonte and Ville Bergholm. Tensor networks in a nutshell. 2017. arXiv:1708.00006.

[BBC+95] Adriano Barenco, Charles Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computing. *Physical Review A*, 52:5, 1995.

[BBD+97] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997.

[BCH06] Dave Bacon, Isaac L. Chuang, and Aram W. Harrow. Efficient quantum circuits for Schur and Clebsch-Gordan transforms. *Physical Review Letters*, 97:170502, October 2006.

[BCH07] Dave Bacon, Isaac L. Chuang, and Aram W. Harrow. The quantum Schur and Clebsch-Gordan transforms: I. efficient qudit circuits. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07, page 1235–1244, USA, 2007. Society for Industrial and Applied Mathematics.

[BCLK+21] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek, and Alán Aspuru-Guzik. Noisy intermediate-scale quantum (NISQ) algorithms. 2021. arXiv:2101.08448.

[BCP14] Tillman Baumgratz, Marcus Cramer, and Martin B. Plenio. Quantifying coherence. *Physical Review Letters*, 113(14):140401, September 2014. arXiv:1311.0275.

[BCWDW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[BCY11a] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750.

[BCY11b] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. A quasipolynomial-time algorithm for the quantum separability problem. *Proceedings of ACM Symposium on Theory of Computation*, pages 343–351, June 2011. arXiv:1011.2751.

[Ben80] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[BGA+21] George S. Barron, Bryan T. Gard, Orien J. Altman, Nicholas J. Mayhall, Edwin Barnes, and Sophia E. Economou. Preserving symmetries for variational quantum eigensolvers in the presence of noise. *Physical Review Applied*, 16:034003, September 2021.

[BGB+18] Ryan Babbush, Craig Gidney, Dominic W. Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. Encoding electronic spectra in quantum circuits with linear T complexity. *Physical Review X*, 8(4):041015, 2018.

[BGCC21] Jacob L. Beckey, N. Gigena, Patrick J. Coles, and M. Cerezo. Computable and operationally meaningful multipartite entanglement measures. April 2021. arXiv:2104.06923.

[BGNP01] David Beckman, Daniel Gottesman, Michael A. Nielsen, and John Preskill. Causal and localizable quantum operations. *Physical Review A*, 64(5):052309, October 2001. arXiv:quant-ph/0102043.

[BGT21] Adam Bouland and Tudor Giurgica-Tiron. Efficient universal quantum compilation: An inverse-free Solovay-Kitaev algorithm. *arXiv preprint arXiv:2112.02040*, 2021.

[BH13] Fernando G. S. L. Brandão and Aram W. Harrow. Quantum de Finetti theorems under local measurements with applications. In *Proceedings of the 45th annual ACM Symposium on the Theory of Computing*, pages 861–870, Palo Alto, California, USA, June 2013. arXiv:1210.6367.

[Bha07] Rajendra Bhatia. *Positive Definite Matrices*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, New Jersey, USA, 2007.

[BLW22] Zachary P. Bradshaw, Margarite L. LaBorde, and Mark M. Wilde. Cycle index polynomials and generalized quantum separability tests. *arXiv preprint*

arXiv:2208.14596, 2022.

[BR12] Rainer Blatt and Christian F. Roos. Quantum simulations with trapped ions. *Nature Physics*, 8(4):277–284, 2012.

[BRS07] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Reviews of Modern Physics*, 79(2):555–609, April 2007. arXiv:quant-ph/0610030.

[Bru10] R. A. Brualdi. *Introductory Combinatorics*. Pearson/Prentice Hall, 2010.

[CAB+20] M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. Variational quantum algorithms. December 2020. arXiv:2012.09265.

[CBC21] Laura Clinton, Johannes Bausch, and Toby Cubitt. Hamiltonian simulation algorithms for near-term quantum hardware. *Nature Communications*, 12(1):1–10, 2021.

[CCH+20] Benjamin Commeau, M. Cerezo, Zoë Holmes, Lukasz Cincio, Patrick J. Coles, and Andrew Sornborger. Variational Hamiltonian diagonalization for dynamical quantum simulation. September 2020. arXiv:2009.02559.

[CDP09] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Realization schemes for quantum instruments in finite dimensions. *Journal of Mathematical Physics*, 50(4):042101, April 2009.

[CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2):025001, April 2019. arXiv:1806.06107.

[CHM+16] Tom Cooney, Christoph Hirche, Ciara Morgan, Jonathan P. Olson, Kaushik P. Seshadreesan, John Watrous, and Mark M. Wilde. Operational meaning of quantum measures of recovery. *Physical Review A*, 94(2):022310, August 2016. arXiv:1512.05324.

[CJW06] James A Carlson, Arthur Jaffe, and Andrew Wiles. *The millennium prize problems*. Citeseer, 2006.

[CKMR07] Matthias Christandl, Robert Koenig, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, July 2007. arXiv:quant-ph/0602130.

[CMN+18] Andrew M. Childs, Dmitri Maslov, Yunseong Nam, Neil J. Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proceedings of the*

National Academy of Sciences, 115(38):9456–9461, 2018.

[CMP18] Toby S. Cubitt, Ashley Montanaro, and Stephen Piddock. Universal quantum Hamiltonians. *Proceedings of the National Academy of Sciences*, 115(38):9497–9502, 2018.

[Com74] L. Comtet. *Advanced Combinatorics: The Art of Finite and Infinite Expansions*. Springer Netherlands, 1974.

[CSZW21] Ranyiliu Chen, Zhixin Song, Xuanqiang Zhao, and Xin Wang. Variational quantum algorithms for trace distance and fidelity estimation. *Quantum Science and Technology*, 7(1):015019, dec 2021. arXiv:2012.05768.

[Dav69] Edward B. Davies. Quantum stochastic processes. *Communications in Mathematical Physics*, 15(4):277–304, 1969.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3rd edition, 2004.

[Die82] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92:271, 1982.

[dMKHMVZ19] Robert de Mello Koch, Jia-Hui Huang, Chen-Te Ma, and Hendrik JR Van Zyl. Spectral form factor as an OTOC averaged over the Heisenberg group. *Physics Letters B*, 795:183–187, 2019.

[DN06] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Info. Comput.*, 6(1):81–95, jan 2006.

[DPS02] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88(18):187904, April 2002. arXiv:quant-ph/0112007.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69(2):022308, February 2004. arXiv:quant-ph/0308032.

[DPS05] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Detecting multipartite entanglement. *Physical Review A*, 71(3):032333, March 2005. arXiv:quant-ph/0407143.

[EAO+02] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Micha l Horodecki, Pawe l Horodecki, and L. C. Kwek. Direct estimations of linear and nonlinear functionals of a quantum state. *Physical Review Letters*, 88(21):217901, May 2002.

[EP99] Jens Eisert and Martin B. Plenio. A comparison of entanglement measures. *Journal of Modern Optics*, 46(1):145–154, July 1999.

[ESW02] T. Eggeling, D. Schlingemann, and Reinhard F. Werner. Semicausal operations are semilocalizable. *Europhysics Letters*, 57(6):782–788, March 2002. arXiv:quant-ph/0104027.

[FKM+18] Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. Impossibility of classically simulating one-clean-qubit model with multiplicative error. *Physical Review Letters*, 120:200502, May 2018. arXiv:1409.6777.

[FKS21] Steph Foulds, Viv Kendon, and Tim Spiller. The controlled SWAP test for determining quantum entanglement. *Quantum Science and Technology*, 6(3):035002, April 2021. arXiv:2009.07613.

[FR96] Ugo Fano and A. Ravi P. Rau. *Symmetries in Quantum Physics*. Academic Press, 1996.

[GAH+22] Michael R. Geller, Andrew Arrasmith, Zoë Holmes, Bin Yan, Patrick J. Coles, and Andrew Sornborger. Quantum simulation of operator spreading in the chaotic ising model. *Phys. Rev. E*, 105:035302, Mar 2022.

[GB00] Markus Grassl and Thomas Beth. Cyclic quantum error–correcting codes and quantum shift registers. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 456(2003):2689–2706, 2000.

[GHMW15] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. Quantum interactive proofs and the complexity of separability testing. *Theory of Computing*, 11(3):59–103, 2015. arXiv:1308.5788.

[GL21] Mark Girard and Jeremy Levick. Twirling channels have minimal mixed-unitary rank. *Linear Algebra and its Applications*, 615:207–227, 2021.

[GLX+21] Xue-Yi Guo, Shang-Shu Li, Xiao Xiao, Zhong-Cheng Xiang, Zi-Yong Ge, He-Kang Li, Peng-Tao Song, Yi Peng, Kai Xu, Pan Zhang, Lei Wang, Dong-Ning Zheng, and Heng Fan. Thermal variational quantum simulation on a superconducting quantum processor. July 2021. arXiv:2107.06234.

[Gro96] David J. Gross. The role of symmetry in fundamental physics. *Proceedings of the National Academy of Sciences*, 93(25):14256–14259, December 1996.

[GS08] Gilad Gour and Robert W. Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics*,

10:033023, March 2008. arXiv:0711.0043.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019.

[GZB+20] Bryan T. Gard, Linghua Zhu, George S. Barron, Nicholas J. Mayhall, Sophia E. Economou, and Edwin Barnes. Efficient symmetry-preserving state preparation circuits for the variational quantum eigensolver algorithm. *NPJ Quantum Information*, 6(1):10, 2020.

[Har05] Aram W. Harrow. *Applications of coherent classical communication and the Schur transform to quantum information theory*. PhD thesis, Massachusetts Institute of Technology, December 2005. arXiv:quant-ph/0512255.

[Har13] Aram W. Harrow. The church of the symmetric subspace. 2013. arXiv:1308.6595.

[HHH96] Micha l Horodecki, Pawe l Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, November 1996.

[HHHH09] Ryszard Horodecki, Pawe l Horodecki, Micha l Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225.

[HM10] Aram Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum Merlin-Arthur games. In *Proceedings of the 51st Annual IEEE Symposium on the Foundations of Computer Science (FOCS)*, pages 633–642, Las Vegas, Nevada, USA, October 2010. arXiv:1001.0017.

[HMW13] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. In *Proceedings of the 28th IEEE Conference on Computational Complexity*, pages 156–167, 2013.

[HMW14] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Information and Computation*, 14(5–6):384–416, April 2014. arXiv:1211.6120.

[HMY17] Koji Hashimoto, Keiju Murata, and Ryosuke Yoshii. Out-of-time-order correlators in quantum mechanics. *Journal of High Energy Physics*, 2017(10):1–31, 2017.

[Hoe94] Wassily Hoeffding. Probability inequalities for sums of bounded random vari-

ables. In *The collected works of Wassily Hoeffding*, pages 409–426. Springer, 1994.

[Hol02] Alexander S. Holevo. Remarks on the classical capacity of quantum channel. December 2002. arXiv:quant-ph/0212025.

[idZHSL98] Karol Życzkowski, Pawe l Horodecki, Anna Sanpera, and Maciej Lewenstein. Volume of the set of separable states. *Physical Review A*, 58(2):883–892, August 1998.

[Jor70] Camille Jordan. *Traite des substitutions et des equations algebriques par m. Camille Jordan*, volume 1. Gauthier-Villars, 1870.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, August 2019. arXiv:1803.10710.

[KDWW21] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource theory of unextendibility and nonasymptotic quantum capacity. *Physical Review A*, 104:022401, August 2021. arXiv:1803.10710.

[KL98] Emanuel Knill and Raymond Laflamme. Power of one bit of quantum information. *Physical Review Letters*, 81:5672–5675, December 1998.

[KLL+17] Shelby Kimmel, Cedric Yen-Yu Lin, Guang Hao Low, Maris Ozols, and Theodore J. Yoder. Hamiltonian simulation with optimal sample complexity. *NPJ Quantum Information*, 3(1):1–7, 2017.

[KLP+19] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T Sornborger, and Patrick J Coles. Quantum-assisted quantum compiling. *Quantum*, 3:140, 2019.

[Kro19] Hari Krovi. An efficient high dimensional quantum Schur transform. *Quantum*, 3:122, 2019.

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 608–617, 2000.

[KW20] Sumeet Khatri and Mark M. Wilde. *Principles of Quantum Communication Theory: A Modern Approach*. November 2020. arXiv:2011.04672v1.

[LC19] Guang Hao Low and Isaac L. Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019.

[Llo96] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.

[LMR14] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631–633, 2014.

[LRW21] Margarite L. LaBorde, Soorya Rethinasamy, and Mark M. Wilde. Testing Symmetry on Quantum Computers. 2021. arXiv:2105.12758v2.

[LSM61] Elliott Lieb, Theodore Schultz, and Daniel Mattis. Two soluble models of an antiferromagnetic chain. *Annals of Physics*, 16(3):407–466, 1961.

[LW22] Margarite L. LaBorde and Mark M. Wilde. Quantum algorithms for testing hamiltonian symmetry. *Phys. Rev. Lett.*, 129:160503, Oct 2022. arXiv preprint arXiv:2203.10017.

[LXYB22] Chufan Lyu, Xusheng Xu, Manhong Yung, and Abolfazl Bayat. Symmetry enhanced variational quantum eigensolver. March 2022. arXiv:2203.02444.

[Mac95] I. G. Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford mathematical monographs. Clarendon Press, 1995.

[Mar12] Iman Marvian. *Symmetry, asymmetry and quantum information*. PhD thesis, University of Waterloo, 2012. http://hdl.handle.net/10012/7088.

[MFF14] Tomoyuki Morimae, Keisuke Fujii, and Joseph F. Fitzsimons. Hardness of classically simulating the one-clean-qubit model. *Physical Review Letters*, 112:130502, April 2014. arXiv:1312.2496.

[MPRP21] Lorenzo Moro, Matteo GA Paris, Marcello Restelli, and Enrico Prati. Quantum compiling by deep reinforcement learning. *Communications Physics*, 4(1):1–8, 2021.

[MS13] Iman Marvian and Robert W. Spekkens. The theory of manipulations of pure state asymmetry: I. basic tools, equivalence classes and single copy transformations. *New Journal of Physics*, 15(3):033001, March 2013. arXiv:1104.0018.

[MS14] Iman Marvian and Robert W. Spekkens. Modes of asymmetry: The application of harmonic analysis to symmetric quantum dynamics and quantum reference frames. *Physical Review A*, 90(6):062110, December 2014. arXiv:1312.0680.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[Nic12] W Keith Nicholson. *Introduction to abstract algebra*. John Wiley & Sons, 2012.

[Noe18] Emmy Noether. Invariante variationsprobleme. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1918:235–257, 1918.

[ON07] Tomohiro Ogawa and Hiroshi Nagaoka. Making good codes for classical-quantum channel coding via quantum hypothesis testing. *IEEE Transactions on Information Theory*, 53(6):2261–2266, June 2007.

[Par70] James L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, March 1970.

[Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413–1415, August 1996.

[PHHH06] Marco Piani, Micha l Horodecki, Pawe l Horodecki, and Ryszard Horodecki. Properties of quantum nonsignaling boxes. *Physical Review A*, 74(1):012305, July 2006. arXiv:quant-ph/0505110.

[Pó37] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen. *Acta Mathematica*, 68:145–254, 1937.

[QWK22] Yihui Quek, Mark M. Wilde, and Eneet Kaur. Multivariate trace estimation in constant quantum depth. June 2022. arXiv:2206.15405.

[Rob09] Fred Roberts. *Applied Combinatorics*. CRC Press, Boca Raton, 2009.

[RR78] Steven M. Roman and Gian-Carlo Rota. The Umbral Calculus. *Advances in Mathematics*, 27(2):95–188, 1978.

[SAP17] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. Colloquium: Quantum coherence as a resource. *Reviews of Modern Physics*, 89(4):041003, October 2017. arXiv:1609.02439.

[SBSSH16] Brian Swingle, Gregory Bentsen, Monika Schleier-Smith, and Patrick Hayden. Measuring the scrambling of quantum information. *Physical Review A*, 94(4):040302, 2016.

[Sch05] I. Schur. *Neue Begründung der Theorie der Gruppencharaktere*. Sitzungsberichte der Königlich-Preussischen Akademie der Wissenschaften zu Berlin. 1905.

[Sen11] Ambar N Sengupta. *Representing finite groups: a semisimple introduction*.

Springer Science & Business Media, 2011.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994.

[SJ08] Peter W. Shor and Stephen P. Jordan. Estimating Jones polynomials is a complete problem for one clean qubit. *Quantum Information and Computation*, 8(8):681–714, September 2008. arXiv:0707.2831.

[SKCC20] Kunal Sharma, Sumeet Khatri, Marco Cerezo, and Patrick J Coles. Noise resilience of variational quantum compiling. *New Journal of Physics*, 22(4):043006, 2020.

[Som16] Rolando D. Somma. A Trotter–Suzuki approximation for Lie groups with applications to Hamiltonian simulation. *Journal of Mathematical Physics*, 57(6):062202, 2016.

[SSY20] Kazuhiro Seki, Tomonori Shirakawa, and Seiji Yunoki. Symmetry-adapted variational quantum eigensolver. *Physical Review A*, 101:052340, May 2020.

[Ste09] Benjamin Steinberg. Representation theory of finite groups. *School of Mathematics and Statistics, Carleton University*, 2009.

[Suz76] Masuo Suzuki. Generalized Trotter's formula and systematic approximants of exponential operators and inner derivations with applications to many-body problems. *Communications in Mathematical Physics*, 51(2):183–190, 1976.

[Ter04] Barbara M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, January 2004. arXiv:quant-ph/0307120.

[Tro59] Hale F. Trotter. On the product of semi-groups of operators. *Proceedings of the American Mathematical Society*, 10(4):545–551, 1959.

[Tuc95] A. Tucker. *Applied Combinatorics*. Wiley, 1995.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, April 1976.

[vdV96] F. J. M. van den Ven. Multidimensional NMR in liquids: Basic principles and experimental methods, 1996.

[vLW01] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2001.

[VW02] Guifre Vidal and Reinhard F. Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, February 2002. arXiv:quant-ph/0102117.

[VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends in Theoretical Computer Science*, 11(1–2):1–215, March 2016. arXiv:1610.01664.

[Wat09] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and System Science*, 2009. arXiv:0804.3401.

[Wer89] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, May 1989.

[Wil17] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, USA, 2nd edition, 2017.

[Win99] Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, November 1999. arXiv:1409.2536.

[WWW52] G. C. Wick, A. S. Wightman, and E. P. Wigner. The intrinsic parity of elementary particles. *Physical Review*, 88(1):101–105, October 1952.

[WWW19] Kun Wang, Xin Wang, and Mark M. Wilde. Quantifying the unextendibility of entanglement, November 2019. arXiv:1911.07433.

[WZ82] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

Vita

Margarite L. LaBorde was born in 1995 in Baton Rouge, Louisiana. She attended Port Allen High School in Baton Rouge and graduated in May of 2014. She obtained dual degrees in physics and mathematics at Louisiana State University in May 2018, obtaining Latin honors in both and earning the College Honors distinction for her physics degree. She received her Masters of Science in Physics in 2022 and is currently a candidate for the degree of Doctorate of Philosophy in Physics, which is to be awarded in May 2023.