Computational Complexity of Certain Quantum Theories in $1+1$ Dimensions

by

Saeed Mehraban

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Science in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2015

Author . . . . . .
Department of Electrical Engineering and Computer Science
August 28, 2015

Certified by . . . . . .
Scott Aaronson
Associate Professor of EECS
Thesis Supervisor

Accepted by . . . . . .
Professor Leslie A. Kolodziejski
Chair, Department Committee on Graduate Students

Computational Complexity of Certain Quantum Theories in $1+1$ Dimensions

by

Saeed Mehraban

Submitted to the Department of Electrical Engineering and Computer Science
on August 28, 2015, in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering and Computer Science

Abstract

While physical theories attempt to break down the observed structure and behavior of possibly large and complex systems to short descriptive axioms, the perspective of a computer scientist is to start with simple and believable set of rules to discover their large scale behaviors. Computer science and physics, however, can be combined into a new framework, wherein structures can be compared with each other according to scalar observables like mass and temperature, and also complexity at the same time. For example, similar to saying that one object is heavier than the other, we can discuss which system is more complex. According to this point of view, a more complex system can be interpreted as the one which can be programmed to encode and simulate the behavior of the others within its own degrees of freedom. Within this framework, at the most fundamental layer, physical systems are related to languages. In this thesis, I try to exemplify this point of view through an analysis of certain quantum theories in two dimensional space-time. In simple words, these models are the quantum analogues of elastic scattering of colored balls moving on a line. The models are closely related to each other in both relativistic and non-relativistic regimes. Physical examples that motivate this are the factorized scattering matrix of quantum field theory, and the repulsive delta interactions of quantum mechanics, in $1+1$ dimensions. In classical mechanics, when two hard balls collide, they bounce off and remain in the same order. However, in the quantum setting, during a collision, either the balls bounce off, or otherwise they tunnel through each other, and exchange their configurations. Each event occurs with a certain probability. As a result, moving balls are put in a superposition of being in different color configurations. Thereby, if we consider n distinct balls, the state space is according to their $n!$ possible arrangements, and their collisions act as quantum transpositions. Quantum transpositions can then be viewed as local quantum gates. I therefore consider the general Hilbert space of permutations, and study the space of unitary operators that can be generated by the local permuting gates. I first show that all of the discussed quantum theories can be programmed into an idealized model, the quantum ball permuting model, and then I will try to pin down the language of this model within the already known complexity classes. The main approach is to consider a series of models, as the variations of the ball scattering problem, and then to relate them to each

other, using tools of computational complexity and quantum complexity theory. I find that the computational complexity of the ball permuting model depends on the initial superposition of the balls. More precisely, if the balls start out from the identity permutation, the model can be simulated in a one clean qubit, which is believed to be strictly weaker than the standard model of quantum computing. Given this upper-bound on the ball permuting model, the result is that the model of ball scatterings can be simulated within a one clean qubit, if they start out from an identity permutation. Furthermore, I will demonstrate that if special superpositions are allowed in the initial state, then the ball permuting model can efficiently simulate and sample from the output distribution of standard quantum computers. Next, I show how to use intermediate demolition ball detections to simulate the ball permuting model nondeterministically. According to this result, using post-selection on the outcome of these measurements, one obtains the original ball permuting model. Therefore, the post-selected analogue of ball scattering model can efficiently simulate standard quantum computers, when arbitrary initial superpositions are allowed. In the end, I formalize a quantum computer based on ball collisions and intermediate ball detections, and then I prove that the possibility of efficient simulation of this model on a classical computer is ruled out, unless the polynomial hierarchy collapses to its third level.

Thesis Supervisor: Scott Aaronson
Title: Associate Professor of EECS

Acknowledgments

Above all, I would like to express my utmost gratitude to my advisor Scott Aaronson for his patience, unlimited wisdom, enthusiasm and continuous support during the time I was working on this thesis. He has been a supportive mentor, and I extremely value our discussions. I would like to thank Professor Kuperberg for invaluable discussions. I am specially indebted to Professor Schmidt, my academic advisor for his aspiring guidance, and to Professor Kolodziejski for her kind support throughout. I am thankful to Adam Bouland for valuable discussions and for mentoring me in research. I would like to thank Hamed Pakatchi, Usman Naseer and Hossein Esfandiary for insightful discussions. Last but not least, as I have always been, I am grateful to my family, specially my Parents and my Sisters; I wouldn't be who I am today, if it wasn't because of them.

Contents

List of Figures

Chapter 1

Introduction

1 Motivating lines

What [3] happens when computer science meets physics? The Church-Turing thesis states that *all that is computable in the physical universe is also computable on a Turing machine* [3, 46]. Other than a mathematical statement, this is a conjecture about a fundamental rule in theoretical physics. An outstanding discovery of computability theory was the existence of undecidable problems [51]; problems that are not decidable by Turing machines. Therefore, the Church-Turing thesis can be falsified if there exists a physical model that is programmable to decide an undecidable problem. The Church-Turing thesis was then further extended to another conjecture that: *all that is efficiently computable in the physical universe is also efficiently computable by a probabilistic Turing machine*. An efficient process is defined to be the one which answers a question reliably after polynomial time in the number of bits that specify the question itself. The extended Church-Turing thesis sounds to be defeated by the laws of quantum physics, as the problem of factoring large numbers is efficiently solvable on a quantum computer [44], while yet no polynomial time probabilistic algorithm is not known for it. If this is true, then the revised thesis is that *all that is efficiently computable in the physical universe, is also efficiently computable on a quantum computer*. Given this illustration, a natural approach is to classify the available physical theories with their computational power, both according to the notion of complexity and computability [1]. There are variety of known examples that are equivalent to classical

Turing machines [1, 49, 52, 56], and also other equivalents of the standard quantum computers [26, 40]. Among the available computing models are those that are believed to be intermediate between classical polynomial time and quantum polynomial time [4, 31, 37]. These are models that are probably strictly weaker than standard quantum computers, but they still can solve problems that are believed to be intractable on a classical computer. Besides a theory of decidable languages, complexity theory, as is manifest in its title, provides means to compare objects with respect to their complexity. This is well defined for languages, and is given by reduction from a language to the other. Intuitively, a reduction is of programming an object in to the shape of another object. The language of a physical system can be interpreted both as the relationship between the description of the system and the existence of a property in it, or the relationship between the initial states and a property in the final states. The latter can somehow be viewed as the special case of the first one. Therefore, viewing models as their languages, complexity theory can provide grounds to define a complex system.

In this thesis, I try to apply these ideas to some physical theories, involving scattering of particles. The objective is to realize if these models are efficiently programmable, and if so, what languages? Moreover, I am interested in upper-bounds, i.e., models that can efficiently accept a reduction from these. Scattering amplitudes are central to quantum field theory and quantum theory of scattering particles [10]. They relate the asymptotic initial states of a quantum system to the final states, and therefore they can be viewed as notable observables of quantum theory. While in general scattering amplitudes are sophisticated objects, in integrable theories of $1+1$ dimensions [9, 47] they take simple forms, and can be described by a single diagram with four-particle vertices. These diagrams encode the overall scattering matrix, whose functionality can be placed in one to one correspondence with permutations of finite element sets [55]. A crucial element of these integrable theories is a factorized scattering matrix [57]. In this case, the scattering matrix can be decomposed as a product of local unitary scattering matrices. These local matrices satisfy the well-known Yang-Baxter [14, 55] relations, and it can be demonstrated that Yang-Baxter relations impose special symmetries on the diagrams in a way that each diagram can be consistently assigned to a permutation. Such drastic simplification is directly related to

the existence of an infinite family of conservation rules, first noticed by Zamolodchikov et. al. [58]. In general, a unitary scattering matrix is a manifold of dimension exponential in the number particles. However, it can be shown that the infinite family of conservation rules shrinks the number of degrees of freedom drastically, so that the matrix as a manifold can be embedded in a manifold of linear dimensionality.

2 Methods and Summary of the results

Given these amazing features of the integrable quantum models, it is interesting to use the tools from complexity theory to understand how complex these models are. Specifically, I analyze the situation, where all the particles are distinguishable. In the sense of quantum field theory, this is the situation where infinite colors are allowed. Language within the framework of quantum mechanics is the subject of quantum computation and quantum information, and I will employ these tools over and over. The standard model of language in quantum computation is the class BQP, which is the set of problems that are efficiently verifiable by local quantum circuits, and a quantum model is called BQP-universal if it can recognize the same set of languages. Bits of quantum information are called qubits, the states of a system which can take two states in a superposition. Therefore, in order to have a reference of comparison, I will try to relate the state space of the integrable quantum theory of scattering to bits and qubits. My approach is to define different variations of the scattering model, as new models, and prove reductions between them one by one. Therefore, given a tower of models, I will find corresponding upper-bounds and lower-bounds.

I define the ball permuting model as a quantum models with a Hilbert space consisting of permutations of a finite element set as its orthogonal basis. Then, the gates of ball permuting model act by permuting states like $|x,y\rangle$ according to $|x,y\rangle \rightarrow c|x,y\rangle + is|y,x\rangle$, where x and y are members of a finite element set, and c and s are real numbers with $c^2+s^2=1$. This model is an upper-bound on the particle (ball) scattering model. I prove that if the ball permuting model starts out of an initial state according to $|123\ldots n\rangle$, then the model can be simulated within the one clean qubit [37]. Moreover, I demonstrate that if the model is allowed to start out from arbitrary initial states, then there is a way to simulate BQP within

the ball permuting model. I also consider a variant of the ball permuting model, wherein the action of the gates are according to $|x,y\rangle \rightarrow c_{x,y}|x,y\rangle + is_{x,y}|y,x\rangle$. Here $c_{x,y}$ and $s_{x,y}$ are real numbers that depend on the labels x and y only, and also $c_{x,y}^2 + s_{x,y}^2 = 1$. I will demonstrate that this model can directly simulate BQP on any initial state, including the identity $|123\ldots n\rangle$. After that, I do a partial classification on the power of ball permuting model on different initial states. The classification is according to the Young-Yamanouchi orthonormal basis [30], which form the irreducible representations of the symmetric group. Lastly, I prove that if we allow intermediate demolition measurements on the scattering outcomes of the mentioned integrable quantum models, then the overall scattering matrix can take exponentially large number of degrees of freedom. After that, I use post-selection [2], as a mathematical tool to prove that if the scattering particles are allowed to start from arbitrary initial superpositions, then the model of particle scattering with intermediate demolition particle detections cannot be simulated efficiently with polynomial time probabilistic algorithms, unless a drastic situation occurs in complexity theory: the polynomial hierarchy [11] collapses to its third level.

3 Summary of the Chapters

The thesis consists of three chapters. In chapter 1, I review the essential backgrounds about computability and complexity. I start by defining alphabets, and proceed to the Turing machine as the well-accepted model of computation. After discussing some ingredients of computability theory, I will talk about complexity theory, and bring the definitions for the well-known complexity classes that are related to this thesis. Then I finish the survey on classical computation by circuits, which are essential ingredients of quantum computing.

In chapter two, I quickly review quantum mechanics in a nutshell, and end my discussion with scattering amplitudes and quantum field theory. Given the backgrounds from quantum physics, I talk about quantum complexity theory, as complexity theory written on a background of quantum mechanics. After that, I introduce the integrable models both in quantum field theory, and quantum mechanics.

Chapter 3 is dedicated to the results. As the symmetric group is an important element

of integrable quantum theories, I brought some notes about it in the beginning of the chapter. Before jumping to the computational complexity of the models, I talk a little about a classical analogue of the ball permuting model. After that, I formally define the languages and the variants of the ball permuting model, and pin them down withing the known complexity classes. Specifically, I prove that the model of ball permuting on the initial state $|123\ldots n\rangle$ can be efficiently simulated within the one clean qubit. This immediately gives an upper-bound of one clean qubit on the scattering models on this initial state. Then I introduce a ball scattering computer with intermediate measurements. In order to partially classify ball permuting model on different initial states, I borrow tools from the decoherence free subspaces theory and representation theory of the symmetric group. So I wrote a short review of these at the middle of this chapter. After the classification, I demonstrate explicitly how to program the ball permuting model to simulate models of BQP, if we are allowed to initialize the ball permuting model in any way that we want. Then in the end, I put everything together to demonstrate that the output distribution of the ball scattering computer cannot be simulated efficiently, unless the polynomial hierarchy collapses.

Chapter 2

Computability Theory and Complexity Theory

1 Alphabets

An alphabet Σ is a finite set of symbols. Alphabets can be combined to create strings (sentences). For example, if $\Sigma = \{0,1\}$, then any combination like 01110 is a string over this alphabet. The set of strings (sentences) over an alphabet Σ is denoted by $\Sigma^\star := \{w_1 w_2 \dots w_k : w_j \in \Sigma, k \geq 0\}$. The length of a string $w = w_1 w_2 \dots w_k$ is simply the number of alphabets which construct the string denoted by $|w| := k$. Notice that in the definition of $\Sigma^\star$ the length of a string can be 0 ($k = 0$). An empty string $\varepsilon \in \Sigma^\star$ is thereby defined to be a string of length 0. We can alternatively write $\Sigma^\star := \{\varepsilon\} \cup \{w_1 w_2 \dots w_k : w_j \in \Sigma, k \geq 1\}$. An alphabet of length zero is called an empty alphabet, and the set of strings over this alphabet by definition only contains an empty string. The set of strings over alphabet Σ of length n is denoted by Σ^n. Clearly $|\Sigma^n| = |\Sigma|^n$. An alphabet of length 1 is called a unary alphabet and the sentences over this alphabet are isomorphic to $\{1^n : n \geq 0\} \cong \mathbb{N}$. An alphabet of length 2 is called a binary alphabet. We denote an alphabet of length k by Σ_k. Also, throughout we denote $\mathbb{Z}_t := \{0,1,2,\dots,t-1\}$. All alphabets larger than binary are equivalent in the following sense. In the following sections by $A \cong B$ for two sets A and B, it is meant that there is a one-to-one function which maps the elements of A to B and vice versa.

Proposition 2.1. $\Sigma_0^\star \cong \mathbb{Z}_1$, $\Sigma_1^\star \cong \mathbb{N}$, and for $t \geq 3$, $\Sigma_2^\star \cong \Sigma_t^\star \cong \mathbb{R}$.

Proof. The first two are clear since $\Sigma_0^\star = \{\varepsilon\}$ and $\Sigma_1^\star \cong \{\varepsilon\} \cup \{1^n : n > 0\}$. In order to see the third one, notice that $\Sigma_t \cong \mathbb{Z}_t$. In order to see $\Sigma_2^\star \cong \Sigma_t^\star \cong \mathbb{R}$, first notice that $\Sigma_t^\star \cong \mathbb{Z}_t^\star$. For $w \in \mathbb{Z}_t^\star$, consider the map $w \mapsto 0.w$ as the (base t) decimal representation of a number in $[0,1]$. This map is a bijection between the set of infinite strings and $[0,1] \cong \mathbb{R}$. Also consider a bijection between the set of finite strings and $\mathbb{N}$. Any finite string can be written as $0^l w$ where $l \geq 0$ and w starts with a nonzero element, thereby there is a bijection $0^l w \mapsto (l, w)$, between the set of finite string and $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$. Therefore, for any $t \geq 2$ there is a bijection between $\Sigma_t^\star$ and $[0,1] \cup \mathbb{N} \cong \mathbb{R}$. Consider any such bijections, between $\Sigma_2^\star$ and $\mathbb{R}$, and between $\Sigma_t^\star$ and $\mathbb{R}$, combine them together to get a bijection between $\Sigma_2^\star$ and $\Sigma_t^\star$.

□

2 Turing Machines

A language L over the alphabet Σ is defined as a subset $L \subseteq \Sigma^\star$ i.e. A language is a selection of sentences. A selection is in some sense a mechanical process. Given a language, and any string, we wish to distinguish if the string is contained in the language or not. A machine is thereby an abstract object which is responsible for this mechanical selection. At this point the formal definition of such object is unclear, and we need make an extra assumption: machines are logical or physical. There are two directions to this. Firstly, a computing procedure should go through several causal steps. Like a mathematician writing down a mathematical proof on a piece of paper. The other direction for this is that a machine is a physical system. Physical systems are embedded in space and time and their evolution is causal. The first of these directions was fulfilled by Alan Turing [51], when he introduced the Turing machine. A Turing machine is in some sense a model of a mathematician who is writing down on a proof on a piece of paper.

More formally, a Turing machine (TM) has a set of finite states (control) Q, a one dimensional unbounded tape, and a head (pointer) on the tape which can read/write from/on the tape. We can assume that the tape has a left-most cell and it is unbounded from the right. Initially, the machine is in a specific initial state $q_0 \in Q$, and the tape head is in the left most

cell. The input is initially written on the tape and the rest of the tape is blank. The input might just be blank. We specify an alphabet Σ for the input according to the language we wish to recognize. However a different alphabet Γ can be used for the tape. Γ must contain Σ and an extra letter b as the blank symbol. The machine evolves step by step according to a transition function δ. A transition function inputs the current state ($p \in Q$) of the machine, and the content of the current tape cell x, and based on these, outputs $q \in Q$ as the next state, $y \in \Gamma$ as the content to be written on the current cell, and a direction $Left$ or $Right$ as the next direction of the head. For example $\delta(p,x) = (q,y,L)$, means that if the TM reads x in state p, it'll write y instead of x goes to the state q and the head goes to the left on the tape. If at some point the machine enters a special state q_y, then it will halt with a yes (accepting) answer. There is another state q_n to which if the machine enters, it will halt with a no (rejecting) answer.

Definition 2.1. A (Deterministic) Standard Turing machine is a 7-tuple $(\Sigma, \Gamma, Q, q_0, q_y, q_n, \delta, D := \{L,R\})$. Where Σ is the input alphabet, and $\Gamma \supseteq \Sigma$ is the tape alphabet. Q is the finite set of states of the machine, $q_0 \in Q$ is the unique starting state, q_y and $q_n \in Q$ are the accepting and rejecting halting states, respectively. $\delta : Q \times \Gamma \to Q \times \Gamma \times D$ is the transition function. The Standard Turing machine has a single tape isomorphic to $\mathbb{N}$ with a single head.

Any Turing machine corresponds to a languages, and informally all accessible (enumerable) languages correspond to Turing machines. In computer science this statement is recalled after *Church* and *Turing*:

The Church Turing Thesis: "All that is computable in the Physical Universe is Computable by a Turing machine."

Such statement is a concern of scientific research in the sense that it is falsifiable, and can be rejected if one comes up with architecture of a physical computing device whose language corresponds to a language that is undecidable by Turing machines. Yet, still the *Church-Turing Thesis* has not refused a thought experiment.

We formally classify Languages according to their relation to the class of Turing machines.

Definition 2.2. A language L over the alphabet Σ is called *Turing Recognizable* if there is a single tape Standard Turing machine M such that for every $x \in \Sigma^\star$, $x \in L$ if and only if M accepts x. In this case we say that M recognizes L. The language L is called *Decidable* if there is a Standard Turing machine M which recognizes L and moreover, for any $x \in \Sigma^\star$, M halts. A function $f : \Sigma^\star \to \Sigma^\star$ is called computable if there is a Turing machine M such that M run on x halts with y on its tape iff $f(x) = y$.

We say a Turing machine halts on the input $x \in \Sigma^\star$, if after finite transitions the machine ends up in either state q_y or q_n. We say the Turing machine accepts the input if it ends up in q_y, otherwise, if it does not halt or if it ends at q_n the input is said to be rejected. We can make several conventions for the transition and the structure of a Turing machine. For example, we can think of a Turing machine with multiple finite tapes. Moreover, in the defined version of the Turing machine, we assumed that at each step the tape head either moves left of right. We can think of a Turing machine wherein the head can either move to left or right or stay put. Thereby, we define a transition *stationary* if the tape head stays put, and define it *moving* if it moves. Also the geometry of the tape itself can differ. In the model we discussed the geometry of the tape cell is isomorphic to $\mathbb{N}$ with a single tape head. We can discuss tapes of geometry isomorphic to $\mathbb{Z}$, i.e. a discrete line which is infinite from both sides. Moreover, for any finite $c \geq 1$ we can think of tapes of geometry $\mathbb{Z}^c$ or $\mathbb{N}^c$ with a single tape head. Although these models each can give rise to different complexity classes, in terms of computability, we can show that all of these cases are equivalent.

At this point it is tempting to prove that there exists at least a language that is not decidable by a Turing machine. We mentioned that the space of languages is according to $Lang = \{L \subseteq \Sigma^\star : \Sigma \text{ is finite}\}$. We just proved that for any alphabet Σ larger than unary, $\Sigma^\star \cong \mathbb{R}$. The set of subsets of $\Sigma^\star$ is a set larger than $\mathbb{R}$, meaning that there is no bijection from it to $\mathbb{R}$. The following proposition formalizes this fact:

Proposition 2.2. The set of subsets of any set larger than empty cannot be counted by the original set.

Proof. This true for finite sets, since given any set of n elements the set of subsets has 2^n elements. Suppose that A is an infinite set, and suppose as a way of contradiction that 2^A

(the set of subsets) can be counted by A. Then there is a bijection $f : A \to 2^A$. Given the existence of f consider the subset of A, $P = \{x \in A : x \notin f(x)\}$, and we claim that this subset cannot be counted by A, which is a contradiction. Suppose that P has a pre-image, so $\exists a \in A, f(a) = P$. Then $a \in P$ if and only if $a \notin f(a) = P$. □

Given this nice fact, we observe that the space of languages cannot be counted by $\mathbb{R}$. However, most of the languages are inaccessible to a physical machine, i.e. a physical machine can recognize an input that has finite length. Thereby we consider the set of accessible languages as those that have finite length. This corresponds to the set of subsets of the subset of $\Sigma^\star$ that has all finite sentences. The set of finite sentences can count $\mathbb{N}$ and thereby its subset cannot be counted by $\mathbb{N}$. It suffices to prove that the space of Turing machines is countable by $\mathbb{N}$ and this implies that at least there exists a language that is not captured by Turing machines, or more precisely is not Turing recognizable. Hence a quest for counterexamples to *Church-Turing Thesis* is a concern for us. This is a non-constructive proof, we indeed can mention specific languages that are not decidable by a Turing machine. For example given the description of a Turing machine and its input, the problem of deciding if the machine accepts the input is undecidable. Moreover, given the description of two Turing machines, the problem of deciding whether they recognize the same language is not Turing Recognizable.

Definition 2.3. $\mathbb{N}^{\mathbb{N}} := \{(x_1, x_2, \ldots, x_n) : n \in \mathbb{N}, x_j \in \mathbb{N}, j \in [n]\}$.

We can view $\mathbb{N}^{\mathbb{N}}$ as the space of finite tuples.

Proposition 2.3. (Gödel [28]) $\mathbb{N} \cong \mathbb{N}^{\mathbb{N}}$, with a computable map.

Proof. We give an injection $g : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$. Given any $X = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^{\mathbb{N}}$, construct $f(X) = p_1^{x_1} p_2^{x_2} \ldots p_n^{x_n}$. Clearly, non-equal tuples are mapped to non-equal natural numbers. Also the map is invertible since any natural number is uniquely decomposed into a prime factorization. The map is computable, since given any n-tuple one finds the first n primes and constructs the image as multiplications. □

Proposition 2.4. The Turing machines can be counted by natural numbers.

Proof. It suffices to find a computable one-to-one embedding of TM into $\mathbb{N}^{\mathbb{N}}$. Each Turing machine M is a finite tuple. We need to make a precise convention to distinguish between different machines. We give each imaginable symbol a natural number. These symbols correspond to the input and tape alphabets, name of the machine states, and the left/right (or possibly stay put) symbols. The following is one possible embedding:

$$\begin{aligned} M \quad \mapsto \quad & 2^{|\Sigma|}3^{|\Gamma|}5^{|Q|}p^{\Sigma}\dots p^{\Sigma}p^{\Gamma}\dots p^{\Gamma} \\ & p^{q_0}p^{q_y}p^{q_n}p^{D}p^{q_1,\Gamma_1,q_2,\Gamma_2,D}\dots p^{q_1,\Gamma_1,q_2,\Gamma_2,D} \end{aligned}$$

Here we show the sequence of primes multiplied together with some encoding of the symbols for the set A as powers by $p^A \dots p^A$. In order to avoid adding a new symbol for a delimiter we first specify the size of the sets by $2^{|\Sigma|}3^{|\Gamma|}5^{|Q|}$. Thereby, the next $|\Sigma|$ primes written as $p^{\Sigma}\dots p^{\Sigma}$ as the encoding of the alphabet symbols and so on. Next, the symbol corresponding to the starting, and halting states is specified. Then the map specifies the direction D symbols. Next we need to specify the transition function. A transition function can be specified by a set of 5-tuples of symbols. Each 5-tuple is written as the notation $q_1,\Gamma_1,q_2,\Gamma_2,D$, corresponding to one of the relations $\delta(q_1,\Gamma_1) = (q_2,\Gamma_2,D)$. Therefore, each of these relations is specified by the multiplication of 5 consecutive primes.

Given a Turing machine of symbols clearly there is a Standard Turing machine which converts the description to the discussed standard form and then multiplies the numbers and outputs the binary representation of the image natural number. Given any natural number, a Standard Turing machine can factorize the number and sort it according to the ascending prime power representation, and thereby checks if the description corresponds to a valid Turing machine description. The machine rejects if the description is not valid otherwise it will output the description of the Turing machine into any other computable description.

□

Corollary 2.5. The following statements should be true:

- There is a language that is not recognizable by any Turing machine.

- There is a real number that is not computable.

3 The Complexity Theory of Decidable Languages

By definition, for any decidable language there exists a Turing machine which always halts in certain amount of time and space. One way of classifying these languages is based on the minimum amount of time (space) of a Turing machine that decides the language. In order to classify the languages, then we need a partial (or total order). For this we use the inclusion $\subseteq$ relation among the languages. Inclusion is a partial order and there are those languages that are incomparable. However, the inclusion map has been found to be a natural one [46].

Definition 2.4. For any $f : \mathbb{N} \to \mathbb{N}$, A language L is in time $\mathsf{TIME}(f)$ ($\mathsf{SPACE}(f)$) if there is a Standard Turing machine M which on any input x of size $n := |x|$, it halts using $O(f(n))$ time steps (tape cells of space) and $x \in L$ if and only if M accepts L. For $f, g : \mathbb{N} \to \mathbb{N}$, a language is said to be in $\mathsf{TISP}(f, g)$ ($\mathsf{TIMESPACE}$) if there is a Turing machine which recognizes the language and halts on every input after $O(f(n))$ time using $O(g(n))$ space. We therefore define $\mathsf{P} := \mathsf{TIME}(n^{O}(1))$ and $\mathsf{PSPACE} := \mathsf{SPACE}(n^{O}(1))$.

Next, I mention the concept of nondeterminism:

Definition 2.5. For any $f, g : \mathbb{N} \to \mathbb{N}$ the language $L \in \mathsf{NTIME}(f)$ ($\mathsf{NSPACE}(f)$) with g long witness if there is a Standard Turing machine M, which halts in $\mathsf{TIME}(f)$ and $x \in L$ if and only if there exists a string $|y| \in O(g(|x|))$ such that $M(x, y) = 1$ (accepts). For poly long witnesses, $g \in n^{O(1)}$ we define $\mathsf{NP} := \mathsf{NTIME}(n^{O(1)})$ $\mathsf{PSPACE} := \mathsf{NSPACE}(n^{O(1)})$, and $\mathsf{NL} := \mathsf{NSPACE}(O(\log n))$.

One can think of a nondeterministic version of a Turing machine in which the machine starts out of a unique initial state q_0 on some input $x \in \Sigma^\star$. At each step the computation can branch according to a nondeterministic transition function. At each step depending on the content of the tape head and the current state, the machine can nondeterministically transit to one state, write some symbol and choose a direction among the finitely many available options. A nondeterministic transition function therefore specifies these options at each

point. The running time of a nondeterministic Turing machine is the longest running time among these branches. The machine accepts the input if there exists an accepting branch and rejects otherwise.

Definition 2.6. A standard nondeterministic Turing machine is a 7-tuple $(\Sigma, \Gamma, Q, q_0, q_y, q_n, \delta, D := \{L, R\})$. Everything in the definition is similar to a (Deterministic) Turing machine except for the transition function which is the map to the set of subsets $\delta : Q \times \Gamma \to 2^{Q \times \Gamma \times D}$. Computation starts out in q_0, and at each step if the machine is in state q and reads a symbol a, in the next step it nondeterministically according to one of $(q', a', d) \in \delta(q, a)$ i.e. writes a' on the current cell, goes to state q', and moves the head to right if $d = R$ and to the left otherwise. Each such nondeterministic choice is called a branch of nondeterministic computation. Input is accepted if at least of the branches of the nondeterministic computation transits to q_y state, and is rejected otherwise.

Intuitively, NP is the class of languages that have checkable proof (witness). For example consider the following language:

$$\mathsf{SAT} = \{\phi : \{0,1\}^n \to \{0,1\} | \phi \text{ is in the}$$

$$CNF \text{ form and has a satisfiable assignment}\}$$

A CNF formula consists of a number of clauses $C_1, C_2, \ldots, C_m$ and variables $x_1, x_2, \ldots, x_n$. Each clause consists of a constant number of variables or their negations. For example $(x_1, \neg x_2, x_3)$ is a clause and $\neg$ is the negation of the variable. We can assign the variables with 0 or 1, and a clause is satisfied with this assignment if at least one of its literals is set to 1. In the clause example, an assignment $x_1 = 0, x_2 = 0, x_3 = 0$ satisfies the clause because $\neg x_2 = 1$, but $x_1 = 0, x_2 = 1, x_3 = 0$ does not. A CNF is satisfiable if there is an assignment to its variables that satisfies all of the clauses. SAT is contained in NP. We can see this in a number of ways. Firstly, the language can be phrased in the form $\exists y M(x, y) = 1$. Where x is some encoding of the CNF formula, y is the encoding of an assignment to the formula and M is a Turing machine which reads x and y, and checks if y satisfies x. Secondly, we can think of a nondeterministic polynomial time Turing machine which on input ϕ nondeterministically guesses an assignment in one of its branches and checks if the assignment

satisfies ϕ, if one branch accepts the computation accepts. And thirdly, we can think of the assignment as the witness for containment of ϕ in SAT. We can use any of these views for NP problems.

An oracle is the interface of a language with a machine. Although most of the languages are undecidable, we can think of an imaginary box, the oracle, to which a machine can query some input and it outputs the answer in one step of computation. This can be the answer to a decision problem or computing a function. Based on this concept we can also define different complexity classes:

Definition 2.7. Given a class of computing machines M which can make queries to an oracle A, define M^A to be the class of languages that are decidable by these machines with query access to A.

Each oracle is a language, or in other words they are in one-to-one correspondence with the set of languages. Next, I define a reduction as a crucial element of theory of computing:

Definition 2.8. A reduction is a partial order on the set of languages. Given a class of machines M, and two languages L_1, L_2 over alphabet Σ, we say that $L_1 \leq_M L_2$, or L_1 is reducible to L_2 with M, if there is a function computable in M, such that $x \in L_1$ if and only if $f(x) \in L_2$.

Definition 2.9. A language is called NP hard if all languages in NP are P reducible to it. A language is called NP complete if it is NP hard and is also contained in NP.

Theorem 2.6. *(Cook-Levin [20])* SAT *is complete for* NP.

Lemma 2.7. A language is NP complete if there is a polynomial time reduction from SAT or any other NP complete language to it.

An NP language is in P if there is a reduction from the language to a language in P.

P = NP if and only if SAT $\in$ P (also true for any other NP complete language)

Definition 2.10. #P is the class of functions $f : \Sigma^\star \to \mathbb{N}$ which count the number of accepting branches of an NP machine. Given a nondeterministic Turing machine, M, $f(x)$ is the number of accepting branches of M when run on x. *PP* is the class of problems L for which there exists an NP machine M such that $x \in L$ iff most of the branches of M run on x accept.

So far we have introduced the deterministic and nondeterministic computation in different resources of time and space. An alternative model of computation is the one which is equipped with randomness. In such scheme of computing a Turing machine has access to an unbounded read-once tape consisting of independent true random bits. The transition function can thereby depend on a random bit. Based on such machines we can define new complexity classes.

Definition 2.11. A probabilistic standard Turing machine is defined similar to the deterministic version, with an extra unbounded read-once tape of random bits, as an 8-tuple $(\Sigma, \Gamma, R, Q, q_0, q_y, q_n, \delta, D := \{L, R\})$. Here R is a finite alphabet of random bits, and each element of the alphabet is repeated with equal frequency (probability). The transition function $\delta : Q \times \Gamma \times R \to Q \times \Gamma \times D$.

Therefore, the following two complexity classes are naturally defined as:

- (bounded error probabilistic polynomial time) BPP is the class of languages L for which there is a probabilistic polynomial time Turing machine M such that if $x \in L$, $Pr[M(x) = 1] \geq 2/3$ and otherwise $Pr[M(x) = 0] \geq 2/3$.
- (probabilistic polynomial time) PP is the class of languages L for which there is a probabilistic polynomial time Turing machine M such that if $x \in L$ then $Pr[x = 1] > 1/2$ and otherwise $Pr[x = 0] > 1/2$.

The class PP is related to the counting classes by the following theorem:

Theorem 2.8. $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$ *[11].*

4 The Polynomial Hierarchy

The NP language can be equivalently formulated as the set of languages $L \subseteq \{0,1\}^\star$, for which there is a polynomial time Turing machine $M(\cdot,\cdot)$ and a polynomial $p : \mathbb{N} \to \mathbb{N}$, such that $x \in L$ if and only if there exists $y \in \{0,1\}^{p(|x|)}$ such that $M(x,y)$ accepts. We can just write:

$$x \in L \qquad \text{iff} \qquad \exists y,\ M(x,y) = 1$$

The complement of NP is called *co*NP and is defined as the set of languages $L \subseteq \{0,1\}^\star$ for which there is a polynomial time Turing machine M such that:

$$x \in L \qquad \text{iff} \qquad \forall y,\ M(x,y) = 1$$

The relationship between NP and *co*NP is unknown, but we believe that they are in comparable as set of languages,ı.e. none of them is properly contained in the other. Define the notation $\Sigma_P^0 = \Pi_P^0 = \mathsf{P}$, and $\Sigma_\mathsf{P}^1 = \mathsf{NP}$ and $\Pi_\mathsf{P}^1 = co\mathsf{NP}$, then we can inductively extend the definitions to a Hierarchy of complexity classes. Define Σ_P^j to be the class of languages $L \subseteq \{0,1\}^\star$, for which there is a polynomial time Turing machine M such that:

$$x \in L \qquad \text{iff} \qquad \exists y_1,\ \forall y_2,\ \exists y_3\ \ \ldots Q_i y_i\ \ M(x,y_1,y_2,\ldots,y_i) = 1.$$

Here Q_i is either a $\exists$ or $\forall$ quantifier depending on the parity of i. The complexity class Π_P^i is similarly defined as the class of langauges for which there exists a polynomial time Turing machine M such that:

$$x \in L \qquad \text{iff} \qquad \forall y_1,\ \exists y_2,\ \forall y_3\ \ \ldots\ \ Q_i y_i\ \ M(x,y_1,y_2,\ldots,y_i) = 1.$$

The complexity class polynomial hierarchy is defined as the union $\mathsf{PH} := \cup_{i\geq 0}\Sigma_\mathsf{P}^i$. The relationship between BPP and NP is unknown, however according to Sipser et al. $\mathsf{BPP} \in \Sigma_\mathsf{P}^2$. According to a theorem by Toda [50], PH is contained in $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$. The relationship between the Π^i and Σ^i and also the different levels within PH is unknown. However we know that if $\Sigma_\mathsf{P}^i = \Pi^i\mathsf{P}$ or $\Sigma_\mathsf{P}^i = \Sigma_\mathsf{P}^{i+1}$ for $i > 0$, then PH collapses to the i'th level, that is the hierarchy will consist of finitely many levels [11].

We believe that PH contains infinite levels, and we usually use this assumption to make inference about the containments of complexity classes. For example, the class $\mathsf{BPP}^{\mathsf{NP}}$ is known to be appropriate for efficient approximate counting; in comparison, $\mathsf{P}^{\#\mathsf{P}}$ is the exact counting class. $\mathsf{BPP}^{\mathsf{NP}}$ is contained in the third level of PH. However, because of

Toda's theorem $\mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{BPP}^{\mathsf{NP}}$ which implies $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}} \subseteq \Sigma_{\mathsf{P}}^3$, and then a collapse of PH to the third level. Therefore, we say that there are counting problems that are hard to even approximate within a multiplicative constant, unless PH collapses to the third level [11].

5 Circuits

As a detour consider the set of functions F of the form $\{0,1\}^\star \to \{0,1\}$. Clearly, there is an injective map between F and the set of languages. Given any language L construct a unique function with $f(x) = 1$ if and only if $x \in L$. In other words each such function represents a language. Most of the languages are undecidable, thereby most of these functions are not computable. We can think of a subset of these functions as F_n as the set of functions of the form $\{0,1\}^n \to \{0,1\}$. Consider a lexicographic ordering on the set of strings of n bits, as an injective map between these strings and $[2^n]$ i.e. represent each of these strings with an integer between 1 and 2^n. Given this ordering any function F_n can be specified with a string of 2^n bits, and thereby $|F_n| = 2^{2^n}$. Such an encoding of a function is formalized by a truth table:

Definition 2.12. A truth table tt_f of a function $f : \{0,1\}^n \to \{0,1\}$ is a subset of $\{0,1\}^n \times \{0,1\}$ for which $(x,s) \in tt_f$ if and only if $f(x) = s$.

Definition 2.13. Boolean algebra is a vector space with basis $\Sigma = \{0,1\}$ and two (associative) binary operations (AND) . and (OR) $+ : \Sigma \times \Sigma \to \Sigma$ and a unary operation called negation (NOT) $' : \Sigma \to \Sigma$. Given $x, y \in \Sigma$, $x.y = 1$ if $x = 1$ and $y = 1$, otherwise $x.y = 0$, and $x + y = 0$ only if $x = 0$ and $y = 0$ and otherwise $x + y = 1$. And $x' = 0$ if $x = 1$ and otherwise $x = 1$. We can alternatively use the symbols $\wedge$, $\vee$ and $\neg$ for AND, OR, and NOT operations, respectively.

We can think of the operations as physical gates and $0, 1$ (vectors) as wires, and thereby we formalize a model of computation called circuits. A circuit has n input wires and 1 output wire. The input wires are glued by AND, OR and NOT gates. Each of these gates take input wire(s) and one output wire. Based on the value of the inputs the output bit is set according to the function of the gate. Thereby, following the input wires down to the

output wire a circuit assigns a value in $\{0,1\}$ to an n bit string. Renaming and extending some of these concepts, we can formalize circuits as a subset of directed graphs.

An unbounded AND (OR) gate is a gate with unbounded input wires and unbounded output wires such that all output wires are a copy of the other, and their value is $1(0)$ if and only if all the input wires are $1(0)$, and otherwise the output wires take $0(1)$.

Definition 2.14. A family of circuits $\{C_{m,n}\}$, each with m inputs and n outputs, is called uniform if there is a Turing machine which on input m,n outputs the description $C_{m,n}$. The family is otherwise called nonuniform.

Any boolean function $f : \{0,1\}^n \to \{0,1\}$, can be constructed by a sequence of AND, OR, NOT and COPY. We then call the collection these operations a universal gate set. Therefore, any gate set which can simulate these operations is also universal for Boolean computing. Among these universal gate sets is the gate set consisting of NAND operation only. A NAND operation is the composition of NOT and AND from left to right. We are also interested in universal gate sets which are reversible. That is the gate sets that can generate subsets of invertible functions $f : \{0,1\}^\star \to \{0,1\}^\star$ only. A necessary condition is that each element of the gate set has equal number of inputs and outputs. Examples of reversible gates are controlled not (CNOT) $C : \{0,1\}^2 \to \{0,1\}^2$ which maps $(x,y) \mapsto (x,x \oplus y)$. That is C flips the second bit if the first bit is a 1. Here $\oplus$ is the addition of bits mod 2. Notice that C is an involution and therefore it is its own inverse. Circuits based on C can generate linear functions only and thereby, CNOT is not universal in this sense. However, if a gate operates as NOT controlled by two input bits, then we can come up with gates that are both reversible and universal. More precisely, let $T : \{0,1\}^3 \to \{0,1\}^3$, be a Boolean gate with the map $(x,y,z) \mapsto (x,y,x.y \oplus z)$. Then T is also its own inverse, and one can confirm that composition of T gates can simulate a NAND gate. Notice that we need extra input and output bits to mediate the simulation. The T gate is also known as the Toffoli gate. As another example let $F : \{0,1\}^3 \to \{0,1\}^3$, be a Boolean gate with the maps $(0,x,y) \mapsto (0,x,y)$ and $(1,x,y) \mapsto (1,y,x)$. F is also its own inverse and moreover it can be proved that F is also universal.

Chapter 3

Quantum Theory and Quantum Complexity Theory

In this chapter, I go over the essential backgrounds in quantum mechanics, and quantum computing, and complexity theory. After a short introduction to quantum mechanics and quantum field theory, I discuss the integrable models in $1+1$ dimensions. Quantum computing and quantum complexity theory are discussed later in the second half of the chapter.

1 Quantum Mechanics

There are various interpretations and formulations of quantum mechanics. In this work, we however, focus on one of these, which in simple words views quantum mechanics as a generalization of classical probability theory to operator algebras. In that, a system is described as a quantum state, which is a complex vector in a vector space. These states encode the probability distribution over the possible outcomes of observables. Observables are Hermitian operators on the vector space. Like in classical probability theory, the states of the vector space should be normalized with respect to some norm, and the set of operators that map normalized states to normalized state are the legitimate evolution operators.

A vector space is called a Hilbert space $\mathscr{H}$, if it is complete and has an inner-product. A Hilbert space can have finite or infinite dimension. An inner-product is a function $\langle\cdot,\cdot\rangle : \mathscr{H}\times\mathscr{H}\to\mathbb{C}$, with conjugate symmetry, i.e $\langle\phi_1|\phi_2\rangle^\star = \langle\phi_2|\phi_1\rangle, \forall\phi_1,\phi_2\in\mathscr{H}$, posi-

tive definiteness, that is for all $\phi \in \mathscr{H}$, $\langle \phi | \phi \rangle \geq 0$, with equality if and only if $\phi = 0$, and bilinearity $\langle \phi | a\phi_1 + b\phi_2 \rangle = a\langle \phi | \phi_1 \rangle + b\langle \phi | \phi_2 \rangle$. Here $\bullet^\star$ is the complex conjugation of the $\mathbb{C}$-numbers. Complete means that any Cauchy sequence is convergent with respect to the norm inherent from inner product. We represent vectors $\phi \in \mathscr{H}$ with a ket notation $|\phi\rangle$. If $\mathscr{H}$ is finite dimensional with dimension n, then $\mathscr{H} \cong \mathbb{C}^n$, as a vector space. Otherwise, we denote an infinite dimensional Hilbert space with $\mathbb{C}^\infty$. We call $\{|e_j\rangle : j \in [n]\}$ an orthonormal basis of $\mathbb{C}^n$, if $\langle e_i | e_j \rangle = \delta_{ij}$. δ_{ij} is the Kronecker, which takes the value 1 if $i = j$ and otherwise 0. Let $|\phi\rangle = \sum_{j\in[n]} \phi_j |e_j\rangle$, and $|\psi\rangle = \sum_{j\in[n]} \psi_j |e_j\rangle$, be vectors in $\mathbb{C}^n$, we use the inner product:

$$\langle \phi | \psi \rangle = \sum_{j\in[n]} \phi_j^\star \psi_j$$

Here $\langle \phi | := \sum_{j\in[n]} \phi_j^\star \langle j|$, is the bra notation for the dual vectors. Where, $\langle e_j|$ act as $\langle e_j | e_i \rangle = \delta_{ij}$. More precisely, we call $\mathscr{H}^\star$ the dual of the Hilbert space $\mathscr{H}$, as the set of linear functions : $\mathscr{H} \to \mathbb{C}$. $\mathscr{H}^\star$ is also a vector space isomorphic to $\mathscr{H}$, and thereby has the same dimension as $\mathscr{H}$, and is spanned by $\langle e_j|$. We will not delve into the foundations of infinite dimensional Hilbert spaces. In simple words, such a Hilbert space corresponds to the space of square integrable functions $\phi : \mathbb{R}^m \to \mathbb{C}$, and we call this function square integrable if:

$$\int_{z\in\mathbb{R}^n} d^n z |\phi(z)|^2$$

exists, and the inner product is defined as:

$$(\phi, \psi) = \int_{z\in\mathbb{R}^n} d^n z \phi^\star(z) \psi(z)$$

A vector $|\phi\rangle$ in this Hilbert space is decomposed as $\int_{z\in\mathbb{R}^n} d^n z \phi(z) |z\rangle$, and a normalized state is the one which $\int_{z\in\mathbb{R}^n} d^n z |\phi(z)|^2 = 1$.

Consider the Hilbert space $\mathbb{C}^n$. A quantum state $|\psi\rangle \in \mathbb{C}^n$ is therefore a normalized vector. Any orthonormal basis $|f_j\rangle, j \in [n]$ corresponds to a set of non-intersecting events. The amplitude of measuring the state $|\psi\rangle$ in the state $|f_j\rangle$ is the complex number $\langle f_j | \psi \rangle$,

and is related to a probability with $P_j = |\langle f_j|\psi\rangle|^2$, where $\sum_{j\in[n]} P_j = 1$.

An operator on the Hilbert space is any function : $\mathscr{H} \to \mathscr{H}$. Observables are therefore the linear Hermitian operators. Given a quantum state $|\psi\rangle$, and an observable O with spectrum $\{a, |a\rangle\}$, measuring $|\psi\rangle$ with observable O corresponds to observing the real value a with probability $|\langle a|\psi\rangle|^2$, therefore the expected value of O is $\langle\psi|O|\psi\rangle$. A Hamiltonian is the observable having the allowed energies of the system as its eigenvalues. A Hamiltonian encodes the dynamics of a system.

A legitimate time evolution of a quantum system corresponds to an operator which maps the normalized states to normalized states. A linear operator U with this property is called a unitary operator, and satisfies $U^\dagger U = I$. Each physical system can be described by a Hamiltonian H. The Hamiltonian is responsible for the unitary evolution in time. Such an evolution is described by a Schrödinger equation:

$$i\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle.$$

Where $|\psi(t)\rangle$ is the state of the system at time t. If H is time-independent, then the unitary evolution is $|\psi(t)\rangle = \exp(-iHt)|\psi(0)\rangle$.

1.1 A word on Special Relativity

Lorentz transformations are those which preserve length with respect to the metric $\eta = \text{diag}(-1,1,1,1)$. The basis is $(t,\mathbf{x}) = (x^0,x^1,x^2,x^3)$; time and three space coordinates. The Greek letters $(\mu,\nu,\ldots)$ run from 0 to 3, the ordinary letters $(a,b,\ldots)$ run from 1 to 3. An infinitesimal length should be conserved according to this metric, and therefore $\eta_{\mu\nu}dx^\mu dx^\nu = \eta_{\mu\nu}dx'^\mu dx'^\nu$. If we define the matrix elements of the Lorentz transform as $L^\mu{}_\nu = \partial x'^\mu/\partial x^\nu$. So the general transforms are of the form $x'^\mu = L^\mu{}_\nu x^\nu + a^\mu$, and the transforms must satisfy:

$$\eta_{\mu\nu}L^\mu{}_\alpha L^\nu{}_\beta = \eta_{\alpha\beta}$$

or equivalently using the matrix form:

$$L^T \eta L = \eta$$

This equation tells us that $Det(L) = \pm 1$. In general the representation of the Lorentz transforms on quantum states are $T(L,a)$. These in general construct the *Poincaré* group. Any representation U of the general Poincaré group for quantum states should satisfy:

$$U(L_1,a_1)U(L_2,a_2) = U(L_1L_2, L_1a_2 + a_1) \tag{3.1}$$

1.2 The Scattering Matrix

Let $\mathscr{H}$ be a possibly infinite dimensional Hilbert space, and h_0 be the Hamiltonian responsible for the time evolution of vectors in $\mathscr{H}$. N copies of the Hilbert space can be combined into $\mathscr{H}^{\otimes N}$. Refer to $\mathscr{H}_i$ as the i'th copy of this combined Hilbert space, and h_0^i as its corresponding Hamiltonian, i.e., h_0^i acts as h_0 on $\mathscr{H}_i$, and acts trivially on the others. The natural time evolution of the states in this Hilbert space is then governed by $\sum_{j\in[N]} h_0^j =: H_0$. This Hamiltonian acts on each copy independently, and we call it the free Hamiltonian. Let S_1 and S_2 be subsets of $[N]$. An interaction between S_1 and S_2 subsystems of the Hilbert space is a Hermitian operator H_{S_1,S_2}, which maps the vectors of $\mathscr{H}_{S_1} \oplus \mathscr{H}_{S_2}$ to itself, and acts as identity on the rest of the Hilbert space. A general form of an interaction is then according to $\sum_{S,S'\subseteq[N]} H_{S,S'}$. Let V be any such interaction. The Hamiltonian describing the overall time evolution is then $H = H_0 + V$. At this point we assume that all of the operators are time-independent. Let Ψ_t be the time dependent quantum state in $\mathscr{H}^{\otimes N}$, then the unitary time evolution is according to $U(t,\tau) = \exp(-iH(t-\tau))$, which maps $|\Psi_\tau\rangle \mapsto |\Psi_t\rangle$. Let $|\Phi_t\rangle := \exp(iH_0t)|\Psi_t\rangle$, be the interaction picture of wave-functions. The evolution of $|\Phi_\tau\rangle$ is then given by the unitary operator:

$$\Omega(t,\tau) = \exp(iH_0t)\exp(-iH(t-\tau))\exp(-iH_0\tau), \tag{3.2}$$

that is $|\Phi_t\rangle = \Omega(t,\tau)|\Phi_\tau\rangle$. Scattering matrix is a unitary operator which relates $\Phi_{-\infty}$ to $\Phi_{+\infty}$, and is given according to $S = \Omega(+\infty,-\infty)$. That is, the scattering matrix relates the states in far past to the states in far future. The interaction picture for the observables is

defined as $V(t) = \exp(iH_0 t)V\exp(-iH_0 t)$. The scattering matrix is then:

$$S = \mathrm{T}\exp\left(-i\int_{-\infty}^{+\infty} V(t)dt\right), \tag{3.3}$$

where T is the time ordering operator sorting the operators in decreasing order from left to right, given by:

$$S = 1 + \sum_{n=1}^{\infty} \frac{(-i)^n}{n!} \int_{-\infty}^{\infty} dt_1 dt_2 \ldots dt_n \theta(t_n, \ldots, t_2, t_1) V(t_1) V(t_2) \ldots V(t_n)$$

where $\theta : \mathbb{R}^n \to \{0,1\}$, is the indicator of the event $t_1 > t_2 > \ldots > t_n$. Or we can just write:

$$S = 1 + \sum_{n=1}^{\infty} \frac{(-i)^n}{n!} \int_{-\infty}^{\infty} dt_1 dt_2 \ldots dt_n \mathrm{T}\Big(V(t_1) V(t_2) \ldots V(t_n)\Big)$$

This expansion is known as the Dyson series. There is also a similar expression for the scattering matrix of quantum field theory. Here, I sketch the logic given in [53]. We need to first revisit the Hilbert space slightly. Consider the decomposition of a Hilbert space according to the number of particles $\bigoplus_{i=0}^{\infty} \mathscr{H}_i$. The zeroth term $\mathscr{H}_0$ consists of a single vector $|0\rangle$, which is called the vacuum state. This corresponds to the minimum energy state. The other terms $\mathscr{H}_i$ for $i \geq 1$, corresponds to i particles, each with a four momentum $p_j = (p^0, \boldsymbol{p})$ and A_j a set of discrete internal degrees of freedom, for $j \in [i]$. The discrete degrees of freedom are internal degrees of freedom like spin. Denote the vectors in the combined Hilbert space with Greek letter $\alpha, \beta, \ldots$. The amplitude of scattering for state with label α to state with label β is then $S_{\beta,\alpha} = \langle \Psi_\beta | S | \Psi_\alpha \rangle$. A creation operator $a_\alpha^\dagger$ is naturally defined as the operator which maps vacuum state to the state with α ingredients in its corresponding block of the Hilbert space, i.e., $|\Psi_\alpha\rangle = a_\alpha^\dagger |\Psi_0\rangle$.

We need a theory that poses both locality and unitarity. Unitarity is simply captured by choosing Hermitian interactions. By locality it is meant that the Lorentz group is a symmetry of this theory. Or in other words, the observables, i.e., the scattering amplitudes are Lorentz invariant. We can hardly imagine how to define operators that only depend on time in a way that they are invariant according to Lorentz space and time transformations. Therefore, a necessary condition is that there exist a well defined interaction density in spatial

coordinates, in the sense that $V(t) = \int d^3x \mathscr{H}(\mathbf{x},t)$. Cluster decomposition in quantum field theory relates the structure of the interaction density to a seemingly obvious logic: if two physical processes occur independently the amplitude of the combined process products of separate amplitudes in each subsystem. This is something like statistical independence in probability theory. Then cluster decomposition forces the interaction densities to be composed of integration over creation and annihilation (the Hermitian conjugate of the creation operator) operators, in such a way that all the creation operators appear on the left hand side of annihilation operators, and the arguments in these integrals contain at most one Dirac delta like singularity. Therefore, in short, the interactions should be specific combinations of the annihilation and creation operators in such a way that they are local and transform according to Lorentz symmetry. That is:

$$U(L,a)\mathscr{H}(x)U^{-1}(L,a) = \mathscr{H}(Lx+a)$$

and locality,

$$[\mathscr{H}(0,\boldsymbol{x}),\mathscr{H}(0,0)] = 0 \qquad |\boldsymbol{x}| > 0$$

If we take a close look at the Greek letter α we see that these are momentum, and other discrete quantum numbers. So the interaction density depends on several (creation and annihilation) operators which they themselves depend on a finite number of momentum species. How can we impose Lorentz scalars when your interaction density depends only on finite numbers of momenta. The solution is the quantum field, an operator that depends on space time and carries all possible creation and annihilation operators in a suitable superposition:

$$\Psi_i^\dagger(x) = \sum_\sigma \int d^3p A_i(p,x,\sigma)a^\dagger(p,\sigma)$$

where $A_l(\cdot,\cdot,\cdot)$ is a suitable function, that can be a vector or scalar and so on. A quantum field is then a proper combination of annihilation and creation operators in such a way that they respect the Lorentz transformation as operators:

$$U(L,a)\Psi_i^\dagger(x)U^{-1}(L,a) = \sum_i M_{ij}\Psi_j^\dagger(Lx+a)$$

Therefore, the quantum fields are building blocks of the quantum field theory, operators that each are Lorentz invariant independently. The legitimate interaction densities then correspond to all the ways that we can combine quantum fields to a Hermitian operator. Represent points of space-time with $x = (t,\boldsymbol{x})$. Expanding equation 3.3 we get:

$$S_{\beta,\alpha} = \sum_{N=0}^{\infty} \frac{(-i)^N}{N!} \int d^4x_1 d^4x_2 \ldots d^4x_N \langle 0|a_\beta T\{\mathscr{H}(x_1)\ldots\mathscr{H}(x_N)\}a_\alpha^\dagger|0\rangle \tag{3.4}$$

The zeroth term in the summation is 1, by convention. Each argument in the integral is a combination of creation and annihilation operators and quantum fields which are integrations over creation and annihilation operators themselves, and these along with their (anti-) commutation relations pose a combinatorial structure and correspond to a set of Feynman diagrams, which we will not delve into. Thereby, given the interaction density of a theory, we construct sequences of Feynman diagrams each amounting to a complex number, and then the summation over them gives the overall amplitude of an interaction.

2 Some Quantum Models in $1+1$ Dimensions

In this section, I am going to review some basic quantum models of two dimensional space-time. As it turns out, both relativistic and non-relativistic versions of the models pose similar structures. For the purpose of this thesis, it is sufficient to focus on one of these, and the same results immediately apply to the others. More specifically, these are integrable quantum models of $1+1$ dimensions [25,27,47]. Integrability is translated as a model which has an exact solution, that is, the perturbation terms in the expression of scattering amplitudes amount to an expressible shape. In order to understand this point, view each perturbation term as a piece among the pieces of a broken vase. While these pieces look unstructured and unrelated, in an integrable world, they can be glued together and integrated in a way that the whole thing amounts to a vase. The solution to an integrable model is simple to describe, and indeed the relation between the problem and its solution can be formalized

as a language, as I will do later. For example, given some initial configuration of particles, I can ask if the amplitude of observing a specific outcome for a measurement is nonzero. Therefore, the mission is to pin down the locus of languages of this form among the already known languages.

The situation in two dimensional space-time is that in far past, a number of free particles are initialized on a line, moving towards each other, and in far future, an experimenter measures the asymptotic wave-function that is resulted from scattering. In the following, I first review models of quantum field theories with factorized scattering matrices. The structure of the interactions is described, and then it is explained how the entries of the scattering matrix are obtained. Next, I review the repulsive delta interactions model, as a non-relativistic model of scattering of free particles. The structure of the two models resemble each other, and I am going to focus on the second model throughout.

Zamolodchikov and Zamolodchikov [57, 58] studied models of two dimensional quantum field theory that give rise to factorized scattering matrices. A scattering matrix is called factorized, if it is decomposable into the product of $2 \to 2$ scattering matrices. They found that the factorization property is related to an infinite family of conservation rules for these theories. More specifically, suppose that the initial quantum state of n particles with momenta $p_1, p_2, \ldots, p_n$, and masses $m_1, m_2, \ldots m_n$ is related to an output state of l particles with momenta $p'_1, p'_2, \ldots, p_l$, and masses $m'_1, m'_2, \ldots, m'_l$, then an example of these conservation rules is according to:

$$\sum_{j\in[n]} p_j^{2N+1} = \sum_{j\in[l]} p_j'^{2N+1} \qquad N = 0, 1, 2, 3, \ldots$$

and,

$$\sum_{j\in[n]} p_j^{2N} \sqrt{p_j^2 + m_j^2} = \sum_{j\in[n]} p_j'^{2N} \sqrt{p_j'^2 + m_j'^2} \qquad N = 0, 1, 2, 3, \ldots$$

These equations directly impose selection rules on the scattering process. According to these selection rules, $n = l$, $\{m_1, m_2, \ldots, m_n\} = \{m_1, m_2, \ldots, m_l\}$, and that the particles of different mass do not interact, and the output momenta among the particles of the same mass are permutations of the input momenta. In this case, the conservation rules put drastic

constraints on the structure of the scattering amplitudes, and this directly imply factorization of the scattering matrix, and thereby integrability of the scattering matrix. Indeed, particles do not actually interact, and instead they only exchange their internal degrees of freedom and their momenta. Thereby, the process resembles pairwise elastic collisions quantum hard balls.

In their paper, the authors find actual examples of quantum field theories that satisfy the factorization condition and are thereby integrable. These models include the quantum sine-Gordon [43], the massive Thirring model, and quantum chiral field [58]. All of these models pose an $O(n)$ isotopic symmetry. Let $\phi_1, \phi_2, \ldots, \phi_n$ be n fields. A model is said to have $O(n)$ isotopic symmetry, if its Lagrangian density and the constraints are both invariant under the application of orthogonal matrices on the fields. Consider a model with Lagrangian density $\mathscr{L}(\phi_1, \phi_2, \ldots, \phi_n)$, subject to a series of constraints $g_j(\phi_1, \phi_2, \ldots, \phi_n) = 1$. For any $n \times n$ orthogonal matrix $O \in O(n)$, define the rotated fields as $\phi_i' := \sum_{j\in[n]} O_{ij}\phi_j$. Then the model has $O(n)$ symmetry if $\mathscr{L}(\phi_1, \phi_2, \ldots, \phi_n) = \mathscr{L}(\phi_1', \phi_2', \ldots, \phi_n')$, and, $g_j(\phi_1, \phi_2, \ldots, \phi_n) = g_j(\phi_1', \phi_2', \ldots, \phi_n')$. For example, the Lagrangian $\mathscr{L} = \sum_{i\in[n]} \partial_\mu \phi_i \partial^\mu \phi_i$, and the constraint $\sum_{i\in[n]} \phi_i^2 = 1$, has the desired symmetry.

In the following, I sketch the general structure of a factorized relativistic scattering matrix. Suppose that n particles of the same mass m are placed on a line, where each one is initialized with a two momentum $(p^0, p^1) =: m(\cosh\theta, \sinh\theta)$, and an internal degree of freedom with a label in $[n]$. In $1+1$ dimensions, the two momentum $p = (p^0, p^1)$ should satisfy ${p^0}^2 - {p^1}^2 = m^2$, where m is the mass of the particle. So any momenta can be specified with a single real parameter, θ called the rapidity, which is related to p as $p = (p^0, p^1) = m(\cosh\theta, \sinh\theta)$. Therefore, we can mark the entries of the scattering matrix by n discrete labels $i_1, i_2, i_3, \ldots, i_n$ of $[n]^n$, and rapidities $\theta_1, \theta_2, \ldots, \theta_n$. Let π be the permutation for which $\theta_{\pi(1)} \geq \theta_{\pi(2)} \geq \ldots \geq \theta_{\pi(n)}$. Denote the scattering matrix by S, then given the conservation rules the entries corresponding to $I := i_1, i_2, i_3, \ldots, i_n \to J := j_1, j_2, j_3, \ldots, j_n$ and $\tilde{\theta} := \theta_1, \theta_2, \theta_3, \ldots, \theta_n \to \tilde{\theta}' := \theta_1', \theta_2', \theta_3', \ldots, \theta_n'$ of S has the following form:

$$S_{I,J}^{\tilde{\theta},\tilde{\theta}'} = \delta(\tilde{\theta}' - \pi(\tilde{\theta}))\mathscr{A}_{I,J}.$$

Where $\pi(\theta_1,\theta_2,\ldots,\theta_n)=(\theta_{\pi(1)},\theta_{\pi(2)},\ldots,\theta_{\pi(n)})$. That is, the only nonzero entries are the ones where the rapidities are reordered in a non-ascending order. We are interested in the computation of the amplitudes $\mathscr{A}_{I,J}$. From now on, we recall the scattering matrix by the entries $\alpha_{I,J}$.

Zamalodchikov et. al. invented an algebra, which demonstrates how to compute the amplitudes of a factorized model. This is now known as the Zamalodchikov algebra. The algebra is generated by non-commutative symbols that encode initial rapidities and labels of the particles before scattering. Suppose that n particles are initialized with rapidities $\theta_1,\theta_2,\ldots,\theta_n$, and labels $i_1,i_2,\ldots,i_n\in[n]$. We are interested in the amplitude $\mathscr{A}_{i_1\ldots,i_n\to j_1\ldots,j_n}$. Define a symbol $A_{i_j}(\theta_j)$ for each particle j. Here, the labels i_j can be possibly repeated. The multiplication rules between these symbols are according to:

$$A_i(\theta)A_j(\phi)=\alpha(\theta,\phi)A_i(\phi)A_j(\theta)+\beta(\theta,\phi)A_j(\phi)A_i(\theta)$$

for $i\neq j$. This case corresponds to the scatterings $i+j\to i+j$ and $i+j\to j+i$, where either the particles bounce off or otherwise they simply tunnel through each other. Here α and β are complex numbers that depend on the rapidities, and the number of particles. For $i=j$ the replacement rule is an annihilation-creation type $i+i\to j+j$:

$$A_i(\theta)A_i(\phi)=e^{i\phi(\theta,\phi)}\sum_{j\in[n]}A_j(\phi)A_j(\theta),$$

and the overall process obtains a global phase. Now in order to compute the amplitude $\mathscr{A}_{i_1\ldots,i_n\to j_1\ldots,j_n}$, multiply the symbols according to:

$$A_{i_1}(\theta_1)A_{i_2}(\theta_2)\ldots A_{i_n}(\theta_n),$$

and read the coefficient of $A_{j_1}(\theta_{\pi(1)})A_{j_2}(\theta_{\pi(2)})\ldots A_{j_n}(\theta_{\pi(n)})$ as the desired amplitude. We also want that the final amplitude be independent from the order that we multiply the symbols together, that is, we want the algebra to be associative:

$$\ldots A_{i_1}(\theta_1)\Big(A_{i_2}(\theta_2)A_{i_3}(\theta_3)\Big)\ldots=\ldots\Big(A_{i_1}(\theta_1)A_{i_2}(\theta_2)\Big)A_{i_3}(\theta_3)\ldots$$

Intuitively, this asserts that as long as the rapidities are reordered in a suitable way, the order of multiplications is not important. This is also known as the factorization condition, also known as the Yang-Baxter equation [14, 55]. I am going to describe this point in detail in the context of the non-relativistic repulsive model, and later in section ... . See Figure **??**: the total scattering process is decomposed into pairwise 4-particle interactions, as demonstrated with the red circles. The reconfiguration of the rapidities is represented by lines flowing upwards. In this case, the scattering matrix is the product of smaller matrices, each corresponding to one of the red circles.

The scattering matrix S has a separate block corresponding to the matrix entries indexed by all distinct labels as permutations of $1,2,3,\ldots,n$. In this case, the scattering of the form $1+1 \to 2+2$ does not occur at all. This separate block is fairly large and has dimension $n!$. I am specifically interested in computational complexity of finding matrix elements of this block.

The non-relativistic analogue of the factorized scattering is given by the repulsive delta interactions model [55] of quantum mechanics. In this model, also elastic hard balls with known velocities are scattered from each other. The set of conserved rules are closely related to the relativistic models. If we denote the initial momenta of the balls with $p_1, p_2, \ldots, p_n$, then the conserved quantities are $\sum_j p_j^{2k+1}$, and $\sum_j p_j^2/m_j$, for $k \geq 0$. Where m_j are the mass of the balls. Again, the selection rules assert that balls with different mass do not interact with each other, and the final momenta among the balls of same mass are permutation of the initial momenta.

In the repulsive delta interactions model, n asymptotically free balls in one spatial dimension and time interact and scatter from each other. I am interested to find the amplitude of each output configuration as a function of the input configuration and momenta of the balls. Asymptotic freedom means that except for a trivially small spatial range of interactions between each two balls, they move freely and do not interact until reaching to the short range of contact. Denote the position of these balls by $x_1, x_2, \ldots, x_n$ and the range of interaction as r_0, then for the asymptotic free regime, we assume $|x_i - x_j| \gg r_0$. The interaction consists of $\dfrac{n(n-1)}{2}$ terms, one for each pair of balls. For each pair of balls, the interaction is modeled by the delta function of the relative distance between them. If no

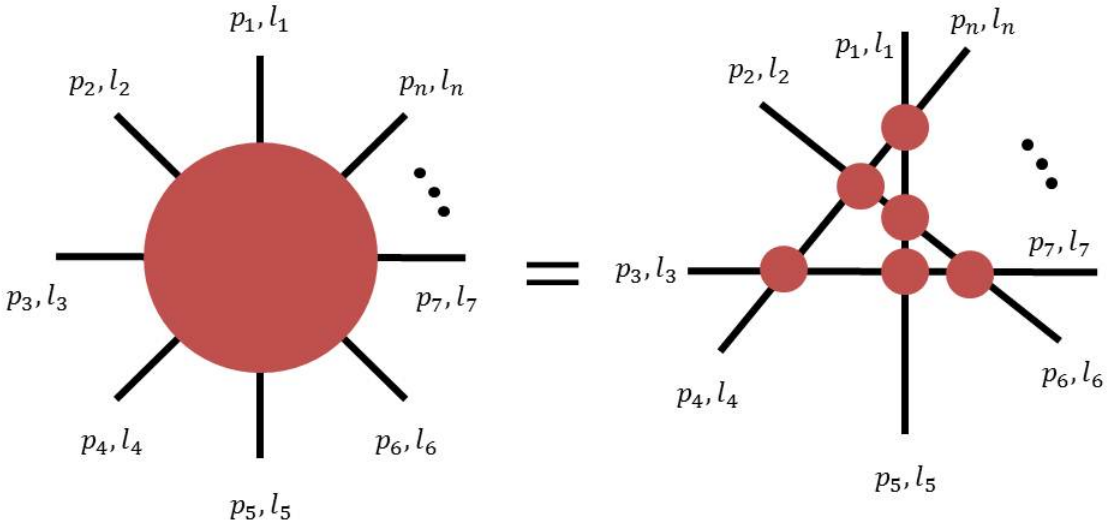


Figure 3-1: Factorization of the S-Matrix into two particle interactions. Any such nonzero amplitude diagram has even number of legs, and for 2*n* legs, the factorization is according to intersections of *n* straight lines.

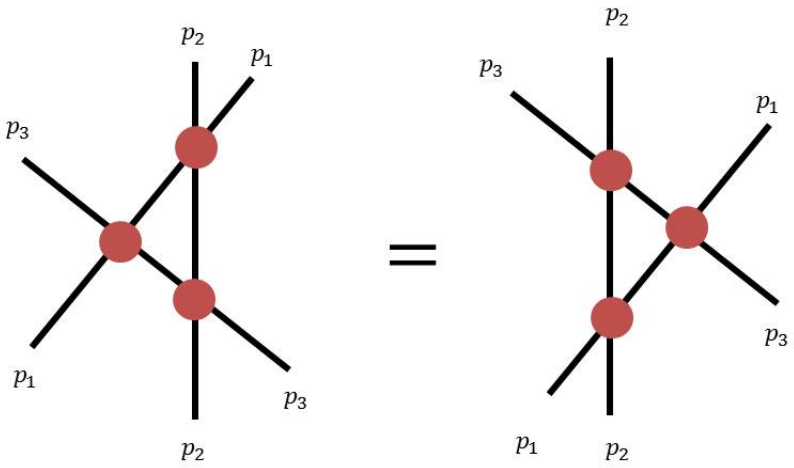


Figure 3-2: Three particle symmetry, known as the Yang-Baxter equation.

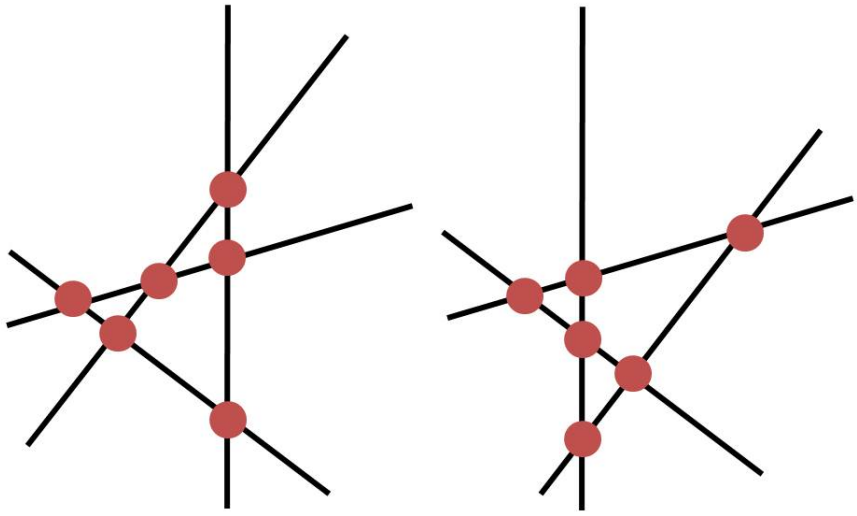


Figure 3-3: Two equivalent diagrams with Yang-Baxter Symmetry. The right hand diagram can be obtained from the left hand diagram by moving some of the straigth lines parallel to themselves.

balls are in contact, then the action of such Hamiltonian is just a free Hamiltonian, and each contact is penalized by a delta function. The functional form of the Schrödinger's equation is written as:

$$i\hbar\frac{\partial}{\partial t}\psi(x_1,x_2,\ldots,x_n,t)=\Big[\sum_{j=1}^{n}-\frac{\partial^2}{\partial x_j^2}+2c\sum_{i<j}\delta(x_i-x_j)\Big]\psi(x_1,x_2,\ldots,x_n,t)$$

Here $c>0$ is the strength of the interactions. As the species of unequal mass do not interact, only balls of same mass are considered. The Hilbert space is indeed $(\mathbb{C}^\infty)^{\otimes n}\times\mathbb{R}$. One can write down a general solution like:

$$|\psi\rangle=\int\frac{dp_1\ldots dp_n}{(2\pi)^{n/2}}\mathscr{A}(p_1,\ldots,p_n,t)|p_1,p_2,\ldots,p_n\rangle.$$

Where $\langle x|p\rangle=\exp(ipx)$. Inspired by Bethe ansatz [**?**] for spin chain models, one can guess a solution for the eigenfunction with the following form:

$$\psi(x_1,\ldots,x_n)=\sum_{\tau,\pi\in S_n}\mathscr{A}_\pi^\tau\theta_\tau(x_1,\ldots,x_n)\exp\left[i(x_{\tau_1}p_{\pi_1}+\ldots+x_{\tau_n}p_{\pi_n})\right]$$

$\theta_\pi:\mathbb{R}^n\to\{0,1\}$ is an indicator function. It gives the output 1 if the input satisfies $x_{\pi(1)}<x_{\pi(2)}<\ldots<x_{\pi(n)}$, and otherwise zero. p_j for $j\in[n]$ are constant parameters, and can be viewed as the momenta. The proposed solution must be a continuous function of the positions and also one can impose a boundary condition for $x_{\pi(t)}=x_{\pi(t+1)}$ for $t\in[n]$ on the derivative of the wave-function. Applying these boundary conditions, one can get linear relations between the amplitudes:

$$\mathscr{A}_\pi^{t\circ\tau}=\frac{-ic\mathscr{A}_\pi^\tau+V_{\tau,t}\mathscr{A}_{t\circ\pi}^\tau}{ic+V_{\tau,t}}$$

Here $t\circ\pi$ is a new permutation resulted from the swapping of the t and $t+1$'th labels in the permutation π. $V_{\tau,t}=p_{\tau(t)}-p_{\tau(t+1)}$. The above linear map has a simple interpretation: two balls with relative velocity V collide with each other with amplitude $\dfrac{-ic}{ic+V}$, the momenta are exchanged and they are reflected, or otherwise, with amplitude $\dfrac{V}{ic+V}$ they

tunnel through without any interaction. In any case, the higher momentum passes through the lower momentum and starting from a configuration $x_1 < x_2 < \ldots < x_n$ for n balls with momenta are in a decreasing order $p_1 > p_2 > \ldots > p_n$, the wave-function will end up in a configuration with momenta in the increasing order $p_n < p_{n-1} < \ldots < p_1$.

Each of these pairwise scatterings can be viewed as a local quantum gate, and the collection of scatterings as a quantum circuit. In order to see this, consider an $n!$ dimensional Hilbert space for n particles with orthonormal basis $\{|\sigma\rangle : \sigma \in S_n\}$. Assume an initial state of $|1,2,3,\ldots,n\rangle$, with defined momenta $p_1, p_2, \ldots, p_n$. These momenta and the initial distance between the particles specify in what order the particles will collide. It is instructive to view the trajectory of the particles as n straight lines for each of these particles in an $x-t$ plane. Time goes upwards and the intersection between each two lines is a collision. In each collision, either the label of the two colliding balls is swapped or otherwise left unchanged. The tangent of each line with the time axis is proportional to the momentum of the ball that the line is assigned to in the first place. Balls with zero relative velocity do not interact, as lines with equal slope do not intersect. Suppose that the first collision corresponds to the intersection of line t with line $t+1$. Such a collision occurs when $p_t > p_{t+1}$. Then the initial state is mapped to:

$$\Big|1,2,\ldots,n\Big\rangle \rightarrow \frac{-ic}{ic+V_{t,t+1}}\Big|1,2,\ldots t,t+1,\ldots,n\Big\rangle + \frac{V_{t,t+1}}{ic+V_{t,t+1}}\Big|1,2,\ldots t+1,t,\ldots,n\Big\rangle$$

Where, $V_t = p_t - p_{t+1}$. This map can be viewed as a $n! \times n!$ unitary matrix:

$$H(p_t - p_{t+1}, t) := H(p_t, p_{t+1}, t) := \frac{-ic}{ic+V_{t,t+1}} I + \frac{V_{t,t+1}}{ic+V_{t,t+1}} L_{(t,t+1)}$$

Here I is the $n! \times n!$ identity matrix, $L_{(t,t+1)}$ is the $n! \times n!$ matrix which transposes the t and the $t+1$'th labels of the basis states. $H(u,t)$ acts only on the t and the $t+1$'th balls only. u is the velocity of the t'th ball relative to the $t+1$'th balls. From now on I refer to these unitary gates as the ball permuting gates. One can check that these gates are unitary:

$$H(u,t)H^{\dagger}(u,t) = H(u,t)H(-u,t) = I.$$

Given n particles, with labels $i_1, i_2, \ldots, i_n$, and momenta $p_1, p_2, \ldots, p_n$, we can obtain a quantum circuit with gates $H(u_1,t_1), H(u_2,t_2), \ldots, H(u_m,t_m)$, one for each intersection of the straight lines. The scattering matrix in this theory is then given by the product $S = H(u_m,t_m), H(u_{m-1},t_{m-1}), \ldots, H(u_1,t_1)$. In general, the label of the balls can be repeated, and the matrix S has a block diagonal form. For each tuple $I = i_1, i_2, \ldots, i_n$, assign a vector $X_I = (x_1, x_2, \ldots, x_n)$, where x_j is the number of times that the index j appears in I. Clearly, $\sum_j x_j = n$. Given this description, the blocks of S are marked by vectors X, that is, the block $X = (x_1, x_2, \ldots, x_n)$, consists of basis entries for which the index 1 appears for x_1 times, the index 2 for x_2 times and so on. S is an $n^n \times n^n$ matrix, and the dimension of the block X is given by $\frac{n!}{x_1! x_2! \ldots x_n!}$. For the purpose of this thesis, I am interested in the block $(1,1,1,\ldots,1)$, where the entries of the S matrix are marked by permutations of the numbers $\{1,2,3,\ldots,n\}$. The product of symbols with distinct labels $A_1(\theta_1)A_1(\theta_1)\ldots A_n(\theta_n)$ can be formulated similarly using product of two-local unitary gates.

An important ingredient of these quantum gates is the so called Yang-Baxter equation [**?**, **?**], which is essentially the factorization condition, and is the analogue of the associativity of Zamalodchikov algebra. The Yang-Baxter equation is a three ball condition, and is according to:

$$H(u,t)H(u+v,t+1)H(v,t) = H(v,t+1)H(u+v,t)H(u,t+1).$$

Basically, the Yang-Baxter equation asserts that the continuous degrees of freedom like the initial position of the particles does not change the outcome of a quantum process, and all that matters is the relative configuration of them. In order to see the line representation of the Yang-Baxter equation, see Figure **??**. Also, the Yang-Baxter equation imposes overall symmetries on the larger diagrams, see Figure **??** for an example. Consider three balls with labels $1,2,3$, initialized with velocities $+u$, 0 and $-u$, respectively. If we place the middle ball very close to the left one, the order of collisions would be $1-2 \to 2-3 \to 1-2$. However, if the middle one is placed very close to the third ball, the order would be $2-3 \to 1-2 \to 2-3$. The Yang-Baxter equation asserts that the output of the collisions is the same for the two cases. Therefore, the only defining pa-

rameters are the relative configurations, and the relationships between the initial velocities. The Yang-Baxter equation has an important role in many disciplines [**?**], these range from star-triangle relations in analog circuits to lattice models of statistical mechanics. Also it can be related to the braiding of n tangles, in the sense that a collision corresponds to the braiding of two adjacent tangles. Braid [**?**] group is defined by B_n generated by elements b_j for $j \in [n-1]$. The defining feature of the braid group is the two conditions: $[b_i, b_j] = 0$ for $|i-j| \geq 2$, and $b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}$ for $i \in [n-2]$. The first property is readily satisfied for the ball permuting gates, and the second property corresponds somehow to the Yang-Baxter equation.

2.1 Semi-classical Approximation to the Model

It is not conventional to do a measurement at the middle of a scattering process. However, in the discussed integrable model, it sounds that the two particle interactions occur independently from each other, and the scattering matrix is a product of smaller scattering matrices. Moreover, in the regime that I am going to consider, no particle creation or annihilation occurs. Therefore, it sounds reasonable to assume that at the middle of interactions the particles (balls) are independent from each other, and no interactions occur unless two particles collide. So, in the following sections, I assume that balls start out from far distances and the nondeterminism in the momentum variable is small. So it is plausible to assume that the balls move according to actual trajectories, and it is possible to track them in between and stop the process whenever we want at the middle of collisions. Also, I am going to use intermediate demolition measurements at the middle of interactions. In such a measurement, a ball is detected by a detector, and then it is taken away from the system. In such a measurement only the classical post-measurement outcome is available to an experimentalist. As a matter of fact, this is a semi-classical approximation on the quantum model.

3 Quantum Complexity Theory

As discussed we compare the complexity of the models using reductions; this is translated in the question of which system can efficiently simulate the other ones. Therefore, in this subsection we review the definition of BQP, as the standard complexity class for quantum computing, and will use this model and its variations as the point of reference in reductions. A qubit as the extension of a bit to quantum systems, is a quantum state in $\mathbb{C}^2$. Let $|0\rangle$ and $|1\rangle$ be an orthonormal basis state for $\mathbb{C}^2$, and we assume that an experimenter can measure the qubit in these basis whenever (s)he wants to. Such a basis state is called the computational basis. The extension of strings to quantum computing is given by quantum superpositions over $(\mathbb{C}^2)^{\otimes n}$, for some $n \geq 1$. Therefore, a quantum computing can create a probability distribution over strings of qubits, through a quantum superposition like $\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$, for complex amplitudes α_x, amounting to $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$. A quantum algorithm then is a way of preparing a quantum superposition from which a measurement reveals nontrivial information about the output of a computing task. Therefore, we use a quantum circuit to produce such a superposition. A quantum circuit is a sequence of local unitary operators each of which affect constant number of degrees of freedom at a time. Each such unitary operator is called quantum gate, and the size of a quantum circuit is the number of local gates in it.

A local quantum gate set is a set of unitary operators G, each of which affecting a constant number of qubits at a time. A quantum circuit on n qubits is then a way of composing the gates in G on n qubits. G as gate-set is called dense or BQP-universal if for any $n > 0$, for any unitary operator U on n qubits and any $\varepsilon > 0$, there is a quantum circuit in G which amounts to a unitary that is ε-close to U.

Theorem 3.1. *(Solovay-Kitaev [35]) all* BQP*-universal gate sets are equivalent: if G and G' are two* BQP*-universal gate sets, then for any quantum circuit C of size d in G, there is a quantum circuit C' of size $O(d)\log^{O(1)}(1/\varepsilon)$ in G' that is ε-close to C.*

also it is worth to mention that:

Theorem 3.2. *(Dawson-Nielsen [21]) there is an algorithm which takes ε and the description of C in theorem 3.1 as input, and outputs the description C' in a time that grows like*

$O(d)\log^{O(1)} 1/\varepsilon$.

Definition 3.1. A group $(G,\cdot)$ is a set G and a binary operation $\cdot$ with the associative map map $(g_1,g_2)\mapsto g_1\cdot g_2$, with the following structures: 1)G is closed under $\cdot$, 2) there is an element $e\in G$ with $e\cdot g = g\cdot e = g, \forall g\in G$, and 3) for all $g\in G$ there exists g^{-1} such that $g^{-1}\cdot g = g\cdot g^{-1} = e$.

The set of $n\times n$ real and invertible matrices with the matrix multiplication create a group, which we call it the general linear group, $GL(n,\mathbb{R})$. Let $O(n)$ be the set orthogonal matrices, i.e., matrices that send orthonormal (real) vectors to orthogonal vectors. These are matrices with orthonormal columns and rows. $O(n)$ is a subgroup of $GL(n,R)$. The determinant of an orthogonal matrix is either 1 or -1. Determinant of a matrix is a homomorphism with respect to matrix multiplication, thereby the subset of $GL(n,\mathbb{R})$ corresponding to determinant 1 is a subgroup called the special orthogonal group $SO(n)$. It can be confirmed that $SO(n)$ is indeed connected. Similarly, we can define the same groups with matrices over the field of complex numbers. These are $GL(n,\mathbb{C})$, $U(n)$ and $SU(n)$. The determinant of a unitary matrix is a phase, i.e., a complex number of the form $e^{i\phi}, \phi\in\mathbb{R}$. $SU(n)$ is thereby the (connected) proper subgroup of $U(n)$ with determinant 1. See the containments of figure.

From a computing perspective, we are interested in programming a quantum gate set into the unitary group. That is we wish to find a local quantum gate set along with a classical algorithm which given the description of a unitary in $U(n)$ outputs a sequence of gates in the gate set, whose composition, with respect to some measure, is arbitrarily close to the input unitary. The final output of such computing scheme is a probability distribution over the qubit strings. Denseness of the gate set in $U(n)$ is a sufficient condition. However, this is not a necessary condition for universal computing. As a first input, the overall phase of a unitary matrix is not an observable in the output probability distribution. Therefore, a gate set that is dense in $SU(n)$ would suffice for universal computation.

Let $\phi : GL(n,\mathbb{C})\to GL(2n,\mathbb{R})$, be the map which replace each entry $M_{ij} = me^{i\theta}$ of $M\in GL(n,C)$ with a 2×2 real matrix:

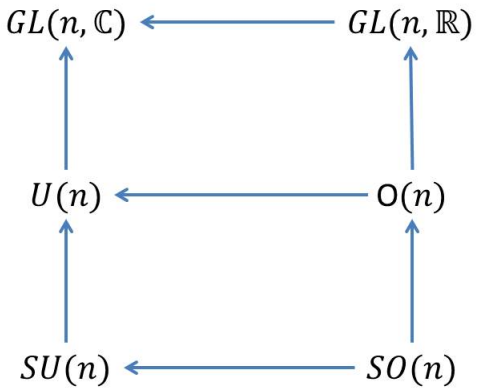


Figure 3-4: Containment relations between general linear, unitary, orthogonal, special unitary and special orthogonal groups groups.

$$m\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.$$

ϕ is a homomorphism and respects the group action. Let $\{|j\rangle : j \in [n]\}$ and $\{|j_1\rangle, |j_2\rangle : j \in [n]\}$ be basis for $GL(n,\mathbb{C})$, and $GL(2n,\mathbb{R})$, respectively. Then if $M \in GL(n,\mathbb{C})$ maps $\sum_{j\in[n]} \alpha_j|j\rangle$ to $\sum_{j\in[n]} \beta_j|j\rangle$, then $\phi(M)$ maps $\sum_{j\in[n]} \Re\alpha_j|j_1\rangle + \Im\alpha_j|j_2\rangle$ to $\sum_{j\in[n]} \Re\beta_j|j_1\rangle + \Im\beta_j|j_2\rangle$. If M is a unitary matrix, $\phi(M)$ is an orthogonal matrix. Moreover, the determinant of $\phi(M)$ is 1. In order to see this write $M = VDV^\dagger$, where D is a diagonal matrix consisting of phases only, and V is a unitary matrix. Then $\phi(M) = \phi(V)\phi(D)\phi(V^\dagger) = \phi(V)\phi(D)\phi(V)^T$. Thereby, $\det(M) = \det(\phi(V))^2\det(\phi(D)) = \det(\phi(D))$. $\phi(D)$ has a block diagonal structure, and the determinant of each block is individually a 1. Therefore ϕ sends $U(n)$ to a subset of $SO(2n)$. From this we conclude that denseness in $SO(n)$ is a more relaxed sufficient condition for universal quantum computing. See Figure 3-4 for the relationship between these.

As a first step we need to program a qubit; that is, we need universal gates that act on $Q = \mathbb{C}^2$. A qubit is a normal vector in $\mathbb{C}^2$, therefore, any such complex vector can be specified using three real parameters:

$$|(\psi,\theta,\phi)\rangle = \exp(i\psi)(\cos\theta/2|0\rangle + \sin\theta_2 e^{i\phi}|1\rangle)$$

The overall phase ψ is unobservable and we can drop it, and qubits can be represented by $|(\theta,\phi)\rangle$. In other words, we take two states equivalent if and only if they are equal modulo a global phase. $|(\theta+2\pi,\phi)\rangle = -|(\theta,\phi)\rangle$ are projectively equivalent. The choice of $\theta/2$ is important, and with this choice the space of qubits (modulo overall phase) is isomorphic to points (θ,ϕ) on a unit 2-sphere, corresponding to the surface $(\cos\theta\cos\phi, \cos\theta\sin\phi, \cos\theta)$. This sphere is referred to as the Bloch Sphere. Therefore, a qubit is programmable if given any two points on the Bloch sphere there is a way to output a unitary operator which maps one point to the other.

Define the Pauli operators on the Hilbert space $\mathbb{C}^2$ as:

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.5}$$

These operators are Hermitian, unitary, traceless and have determinant equal to -1. They anti-commute with each other and each of them squares to the identity operator. We say that two operators A,B anti-commute if $\{A,B\} = AB + BA = 0$, or in other words $AB = -BA$. Moreover they satisfy the commutation relation:

$$[\frac{1}{2}\sigma_i, \frac{1}{2}\sigma_j] = i\frac{1}{2}\sum_{k\in\{x,y,z\}} \varepsilon_{ijk}\sigma_k, \ \forall . i,j \in \{x,y,z\}$$

$[\cdot,\cdot]$, is the commutator operator and maps $A,B \mapsto AB - BA$. ε_{ijk} is the Levi Civita symbol, amounts to zero if any pair in i,j,k are equal, otherwise gives a 1 if the order of (i,j,k) is right-handed, and otherwise takes the value -1. A triple (i,j,k) is called right-handed if it is equal to $(1,2,3)$, and is called left-handed if the order is $(2,1,3)$, modulo cyclic rotation. We usually drop the summation for simplicity. In short the Pauli operators satisfy $\sigma_i\sigma_j = \delta_{ij} + i\varepsilon_{ijk}\sigma_k$.

Any 2×2 unitary operator with unit determinant, can be decomposed as $R(v) = v_0 + i(v_1\sigma_x + v_2\sigma_y + v_3\sigma_z)$, where $v := (v_0,v_1,v_2,v_3) =: (v_0,\mathbf{v}) \in \mathbb{R}^{\mathbf{4}}$, and pose the structure

$v_0^2 + v_1^2 + v_2^2 + v_3^2 = 1$. We can thereby use equivalent parameterization $(v_0, v_1, v_2, v_3) = (\cos\theta, \sin\theta\mathbf{n})$, where $\mathbf{n} \in \mathbb{R}^3$ is a unit vector. Two points $(v_0, \mathbf{v})$ and $(w_0, \mathbf{w})$ act on each other as:

$$(v_0, \boldsymbol{v}).(w_0, \boldsymbol{w}) = (v_0.w_0 - \boldsymbol{v}.\boldsymbol{w},\ w_0\boldsymbol{v} + v_0\boldsymbol{w} - \boldsymbol{v} \times \boldsymbol{w}),$$

If we define the exponential map as the limit of $M \mapsto \exp(M) := \sum_{j=0}^{\infty} \frac{M^j}{j!}$, then $R(v) = \exp(i\theta\mathbf{n}.\sigma)$. Where, $\sigma = (\sigma_\mathbf{x}, \sigma_\mathbf{y}, \sigma_\mathbf{z})$, and $\mathbf{n}.\sigma$ is the usual inner product of the two objects. The object sitting in the argument of the exponential map has the structure of a vector space, with $\sigma_x, \sigma_y, \sigma_z$ as its linearly independent basis. Along with the commutation relation as the vector-vector action it has the structure of an algebra. This algebra is called the Lie algebra $\mathfrak{su}(2)$. The exponential map is an isomorphism between $SU(2)$ and $\mathfrak{su}(2)$. The element $R_j(\theta) := \exp(i\theta\sigma_j)$ is called the single qubit rotation along the j axis, for $j \in \{x, y, z\}$. Indeed, any element in $SU(2)$, can be decomposed as a composition of two rotations R_x, R_y, only.

We can extend this to larger dimensions. Any unitary matrix A with unit determinant can is related to a traceless Hermitian operator H with the exponential map $\exp(iH)$. Let $\mathfrak{su}(n)$ the vector space over $\mathbb{R}$, with $n \times n$ traceless Hermitian matrices as its linearly independent basis. Again the exponential map is an isomorphism between $SU(n)$ and $\mathfrak{su}(n)$. $\mathfrak{su}(n)$ as a vector space has dimension $n^2 - 1$. Also, we know that elements of the set of $n \times n$ unitary matrices with unit determinant can be specified with $n^2 - 1$ real parameters.

Other well known qubit operations are Hadamard H and $\pi/8$ gate P:

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad P := \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \tag{3.6}$$

The importance of a Hadamard gate is that its action $H^{\otimes n}$ in parallel maps $|0\rangle^{\otimes n}$ to an equal superposition over n bit strings, i.e, $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$.

Let $\mathbb{C}^d$ be a Hilbert space, with orthonormal basis $\{|e_j\rangle\}_{j \in [d]}$. Consider the Lie algebra

g_{ij} generated by the operators:

$$|e_i\rangle\langle e_j| + |e_j\rangle\langle e_i|, \quad -i|e_i\rangle\langle e_j| + i|e_j\rangle\langle e_i|, \quad |e_i\rangle\langle e_i| - |e_j\rangle\langle e_j|,$$

for $i < j$. Clearly, g_{ij} is closed under Lie commutation, and is isomorphic to $\mathfrak{su}(2)$. Its image under the exponential map, G_{ij}, is isomorphic to $SU(2)$, and corresponds to quantum operators (with unit determinant) that impose rotations on the subspace spanned by $|e_i\rangle$ and $|e_j\rangle$, and acts as identity of the rest of the Hilbert space. Such set of operation is called a two level gate. If we allow operations from G_{ij} for all $i < j$, then the corresponding gate set is called a two-level system. A two level system is universal, and is dense in $SU(d)$:

Theorem 3.3. *Let g be the vector space generated by $\cup_{i<j} g_{ij}$ then $g = \mathfrak{su}(d)$.*

Proof. $g \subseteq \mathfrak{su}(d)$, since elements of g_{ij} are traceless and Hermitian. Pick any Hermitian matrix M with vanishing trace. Then:

$$\begin{aligned} M &= \sum_{i<j\in[d]} m_{ij}|e_i\rangle\langle e_j| + m_{ij}^\star|e_j\rangle\langle e_i| + \sum_{i\in[d]} m_{ii}|e_i\rangle\langle e_i| \\ &= \sum_{i<j\in[d]} \Re m_{ij}(|e_i\rangle\langle e_j| + |e_j\rangle\langle e_i|) + \Im m_{ij}(i|e_i\rangle\langle e_j| - i|e_j\rangle\langle e_i|) \\ &\quad + \sum_{i\in[d]} m_{ii}|e_i\rangle\langle e_i| \end{aligned}$$

with $\sum_{i\in[d]} m_{ii} = 0$. The off-diagonal terms are manifestly constructible with g_{ij} basis. The last term is also constructible with g basis:

$$\begin{aligned} \sum_{i\in[d]} m_{ii}|e_i\rangle\langle e_i| &= \sum_{i\in[d-1]} m_{ii}|e_i\rangle\langle e_i| + m_{dd}|e_d\rangle\langle e_d| \\ &= \sum_{i\in[d-1]} m_{ii}(|e_i\rangle\langle e_i| - |e_d\rangle\langle e_d|) \end{aligned}$$

□

Corollary 3.4. A two level system on $\mathbb{C}^d$ can generate elements of $SU(d)$.

Corollary 3.5. The following d^2-1 elements create a linearly independent basis for $\mathfrak{su}(d)$:

$$|e_i\rangle\langle e_j| + |e_j\rangle\langle e_i|,$$

$$-i|e_i\rangle\langle e_j| + i|e_j\rangle\langle e_i|,$$

for all $i < j \in [d]$, and:

$$|e_d\rangle\langle e_d| - |e_i\rangle\langle e_i|,$$

for $i \in [d-1]$.

Any $d \times d$ unitary matrix with unit determinant can be decomposed as the composition of $\frac{d(d-1)}{2}$ two level gates. For computation purpose we want to program a gate set to act on multi-qubit systems, that is the Hilbert space $Q^{\otimes n}$, which has dimension 2^n. Therefore a two-level system on $Q^{\otimes n}$ consists of exponentially many elements, and is not an efficient choice for computing. Therefore, we are looking for gates that act on constant number of qubits at a time and generate a dense subgroup of $SU(Q^{\otimes n})$.

An important two qubit gate is the controlled not (CNOT) gate [42], which maps the basis $|x,y\rangle$ to $|x,x\oplus y\rangle$, for $x,y \in \{0,1\}$. That is it flips the second bit if the first bit is set to 1. Indeed, we can discuss a controlled-U gate as $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ for any unitary U. Therefore, a CNOT gate is the controlled σ_x gate. A controlled phase gate is the one with $U = \sigma_z$. CNOT is also related to the classical reversible circuits, that is a boolean gate which flips the second bit conditioned on the status of the first bit. Among these, CNOT has a classical circuit analogue as we discussed previously. Also inspired by the classical reversible gates, we can discuss three qubit gates. Among these are the quantum Fredkin and Toffoli gates. A Fredkin gate is a swap controlled on two qubits controlled by a third qubit, that is the maps $|0,x,y\rangle \to |0,x,y\rangle$ and $|1,x,y\rangle \to |1,y,x\rangle$. A Toffoli or controlled-controlled not or CCNOT is the gate which acts as σ_x a qubit controlled on the status of two other bits; it gives the map $|x,y,z\rangle \to |x,y,x.y \oplus z\rangle$. Here $x.y$ is the logical AND of x and y.

As described two level systems are universal, but not efficiently programmable. There are a number of well known universal gate sets. CNOT with arbitrary qubit rotation are BQP universal by simulating the two level systems. Moreover, for any unitary U, there is a way of assigning real angles to the rotations, such that the composition of gates in this gate set simulates U exactly. However, given finite rotation gates with irrational rotation angles, along with CNOT generate a dense subset of $SU(Q^{\otimes}(n))$. CNOT and X rotations can simulate any special orthogonal matrix, and by the discussion of embedding complex matrices into real ones these are still universal for quantum computing. There are other known BQP-universal gate set. For example, Hadamard with Toffoli generate a dense subset of the orthogonal group (see [5] for a proof), and also $\pi/8$ phase gate, Hadamard with CNOT are also universal for BQP. However, the composition of Hadamard and CNOT gates generate a sparse subset of unitary matrices and the output of any such quantum circuit can be simulated in polynomial time.

A quantum computer works in three steps, initialization, evolution and measurement. The initialization is due to a polynomial time Turing machine which on the size of the input outputs the description of a quantum circuit in some universal gate set. Evolution is simply the action of the quantum circuit on the input $|x\rangle \otimes |00\ldots0\rangle$. The $|x\rangle$ part is the string in computational basis and the state $|00\ldots0\rangle$ is a number of extra bits which mediate the computation. These extra bits are called ancilla qubits. Measurement is basically sampling from the output distribution of $C|x00\ldots0\rangle$ in the computational basis. Moreover, for a decision problem, we can deform C in such a way that measuring the first bit is sufficient to obtain a non-trivial answer.

Definition 3.2. (Bounded-error quantum polynomial time [16]) a language $L \subset \{0,1\}^{\star}$ is contained in BQP, if there a polynomial time Turing machine M, which on the input $1^{|}x|$, outputs the description of a quantum circuit C in some universal gate set, such that if $x \in L$, the probability of measuring a 1 in the first qubit is $\geq 2/3$ and otherwise $\leq 1/3$.

There are variety of definitions for the state norms and operator norms; however, in the context of this research, they all give similar results. More specifically, if $|\psi\rangle$ is a vector, the L_k norm of this vector is defined as:

$$\||\psi\rangle\|_k := \left(\sum_j |\psi_j|^k\right)^{1/k}$$

A valid distance between two operators U and V is then defined as [42]:

$$d(U,V) := sup_{\||\psi\rangle\|=1}\|(U-V)|\psi\rangle\|$$

Specifically, the following theorem is crucial. It basically says that if we can approximate each unitary operator in a quantum circuit, then the error in approximation of the overall circuit grows linearly in its size:

Theorem 3.6. *(Bernstein-Vazirani [15]) if $U_1U_2\ldots U_n$ and $V_1V_2\ldots V_n$ be two sequences of unitary operators such that the distance between each pair U_i and V_i is at most ε, then the distance between $U_1U_2\ldots U_n$ and $V_1V_2\ldots V_n$ is at most $n\varepsilon$.*

4 The One Clean Qubit

While state of a quantum system is a pure vector in a Hilbert space, most of the time the actual quantum state is unknown; instead, all we know is a classical probability distribution over different quantum states, i.e., the given quantum state is either $|\psi_1\rangle$ with probability p_1, or $|\psi_2\rangle$ with probability p_2, and so on. In other words, the state is an ensemble of quantum states $\{(p_1,|\psi_1\rangle),(p_2,|\psi_2\rangle),\ldots,(p_n,|\psi_n\rangle)\}$, for $p_1+p_2+\ldots p_n = 1$. Such an ensemble is a mixture of quantum probability and classical probability distributions at the same time, it is also called a mixed state, and is described by a density matrix ρ:

$$\rho = \sum_{j\in[n]} p_j|\psi_j\rangle\langle\psi_j|.$$

A density matrix is a Hermitian operator, with non-negative eigenvalues and unit trace. A quantum state is called pure, if it has a density matrix of the form $|\psi\rangle\langle\psi|$. In other words, a quantum state ρ is pure if and only if $tr(\rho^2) = 1$.

If some quantum state is initially prepared in the mixed state ρ_0, then given a unitary evolution U, the state is mapped to $U\rho_0U^\dagger$. Let $\{|j\rangle : j\in[n]\}$ be some orthonormal basis of

a Hilbert space. The maximally mixed state of this Hilbert space has the form $\frac{1}{n}\sum_j |j\rangle\langle j| = \frac{I}{n}$, is a quantum state which contains zero quantum information in it. That is, the outcome of any measurement can be simulated by a uniform probability distribution on n numbers. Also, a maximally mixed state is independent of the selection of the orthonormal basis. Quantum computing on a maximally mixed state is hopeless, since $\frac{I}{n}$ is stable under any unitary evolution.

Consider the situation where we can prepare a pure qubit along with n maximally mixed qubits to get $|0\rangle\langle 0| \otimes \frac{I}{n}$. The state $|0\rangle\langle 0|$ is also referred to as a clean qubit. In this case, the quantum state has one bit of quantum information in it. It is also believed that there are problems in DQC1 that are not contained in the polynomial time. One example of such problem, is the problem of deciding if the trace of a unitary matrix is large or small. No polynomial time algorithm is known for this problem. I am going to point out to the trace computing problem later in section ... . Moreover, if we consider the version of DQC1 where we are allowed to measure more than one qubits, then it is shown that there is no efficient classical simulation in this case, unless the polynomial Hierarchy collapses to the third level. In the version of my definition, since I used a polynomial Turing machine as a pre-processor, DQC1 immediately contains P. Pre-processing can be tricky for one clean qubit. For example, as it appears, if instead of P, we used NC^1, the class P and DQC1 are incomparable.

Definition 3.3. (One clean qubit [37]) let DQC1 be the class of decision problems that are efficiently decidable with bounded probability of error using one clean qubit and arbitrary amount of maximally mixed qubits. More formally, these are the class of languages $L \subseteq \{0,1\}^\star$, for which there is a polynomial time Turing machine M, which on any input $x \in \{0,1\}^\star$, outputs the description of a unitary matrix $\langle U \rangle$ with the following property: if $x \in L$, the probability of measuring a $|0\rangle$ on the first qubit of $U|0\rangle\langle 0| \otimes \frac{I}{n} U^\dagger$ is $\geq 2/3$, and otherwise $\leq 1/3$. Here U is an $n+1 \times n+1$ unitary matrix.

Notice that if we allow intermediate measurements we will obtain the original BQP; just measure all qubits in $\{|0\rangle, |1\rangle\}$ basis, and continue on a BQP computation. Clearly, DQC1 is contained in BQP; in order to see this, just use Hadamrds and intermediate measurements

to prepare the maximally mixed state, and continue on a DQC1 computation. It is unknown whether $\mathsf{BQP} \subseteq \mathsf{DQC}_1$, however, we believe that this should not be true.

5 Complexity Classes with Post-Selection

Here we define the complexity classes with post-selection. Intuitively, these are the complexity classes with efficient verifiers with free retries. That is an algorithm which runs on the input, and in the end will tell you whether the computation has been successful or not. The probability of successful computation can be exponentially small.

Definition 3.4. Fix an alphabet Σ. PostBQP (PostBPP) is the class of languages $L \subset \Sigma^\star$ for which there is a polynomial time quantum (randomized) algorithm $\mathscr{A} : \Sigma^\star \to \{0,1\}^2$, which takes a string $x \in \Sigma^\star$ as an input and outputs two bits, $\mathscr{A}(x) = (y_1, y_2)$, such that:

- $1) \forall x \in \Sigma^\star, Pr(y_1(x) = 1) > 0.$
- If $2) x \in L$ then $Pr(y_2(x) = 1 | y_1(x) = 1) \geq \frac{2}{3}$
- If $3) x \notin L$ then $Pr(y_2(x) = 1 | y_1(x) = 1) \leq \frac{1}{3}$

Here y_1 is the bit which tells you if the computation has been successful or not, and y_2 is the actual answer bit. The conditions $2)$ and $3)$ say that the answer bit y_2 is reliable only if $y_1 = 1$. In this work, we are interested in the class PostBQP. However, PostBPP is interesting on its own right, and is equal to the class BPP_{path}, which a modified definition of BPP, where the computation paths do not need to have identical lengths. PostBPP is believed to be stronger than BPP, and is contained in $\mathsf{BPP}^{\mathsf{NP}}$, which is the class of problems that are decidable on a BPP machine with oracle access to NP or equivalently SAT.

Due to a seminal result by Aaronson, PostBQP is related to the complexity class PP:

Theorem 3.7. *(Aaronson [37])* $\mathsf{PostBQP} = \mathsf{PP}$.

Firstly, because of $\mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}}$ as a corollary to the theorem, with oracle access to PostBQP, P can solve intricate counting tasks, like counting the number of solutions to an NP complete problem. The implication of this result for the current work is that if a quantum model,

combined with post-selection is able to efficiently sample from the output distribution of a PostBQP computation, then the existence of a randomized scheme for approximating the output distribution of the model within constant multiplicative factor is ruled out unless PH collapses to the third level. This point is going to be examined in section ... .

6 Some Remarks on Lie Algebras

Let $a_1, a_2, \ldots, a_n$ be Hermitian operators. These can be Hamiltonians of a physical interaction. We are interested in the Lie group generated by operators like $A_k(t) := \exp(ia_k t)$, for $k \in [n]$ and $t \in \mathbb{R}$, as a manifold G. The Lie group is fairly complicated, and it is worth looking at the space tangent to the identity element. Such a space is a vector space, and moreover, it is an alternative definition of a Lie algebra. I denote this Lie algebra by g. Since the exponential map is an isomorphism, the dimension of a Lie algebra, as a vector space, matches the dimension of the manifold G. In addition, for some vector space V, the containment of $\mathfrak{su}(V)$ in g, implies denseness of G in $SU(V)$. Starting with $A_1(t), A_2(t), \ldots, A_n(t)$, it is well-known that the corresponding Lie algebra consists of all the elements that can be ever generated by taking the Lie commutators $i[\cdot,\cdot] : g \times g \to g$ of the elements, and Linear combination of the operators over $\mathbb{R}$.

In order to obtain an intuition about what is going on, it is worth mentioning the following remarks that are followed from [22, 23, 40]. Notice that this is far from being a proof. The Trotter formula states that for any two operators H and V:

$$\exp\left(i(H+V)\right) = \lim_{m\to\infty} \left(\exp(iH/m)\exp(iV/m)\right)^m, \tag{3.7}$$

and the rate of convergence is according to:

$$\exp\left(i(H+V)\right) = \left(\exp(iH/m)\exp(iV/m)\right)^m + \mathrm{O}(1/m).$$

Therefore, this implies that if two elements H and V in g can be approximated within arbitrary accuracy, then $H+V$ can also be approximated efficiently. Next, observe the following identity:

$$\exp([H,V]) = \lim_{m\to\infty} \left(\exp(iH/\sqrt{m})\exp(iV/\sqrt{m})\exp(-iH/\sqrt{m})\exp(-iV/\sqrt{m})\right)^m, \quad (3.8)$$

with the rate of convergence:

$$\left(\exp(iH/\sqrt{m})\exp(iV/\sqrt{m})\exp(-iH/\sqrt{m})\exp(-iV/\sqrt{m})\right)^m = exp([U,V]) + \mathrm{O}(1/\sqrt{m})$$

Therefore this explains the commutator. Lastly, we need to take care of the scalar multiplications. Notice that if an element $\exp(iH)$ is approximated in G, then for any $k \geq 1$, $\exp(iHk)$ can be approximated similarly by repeating the process for k times. Now assume that the sequence $\prod_i A_i(t_i)$ approximates the element with the desired accuracy, then the process $(\prod_i A_i(t_i/km))^m$ can approximate $\exp(iH/k)$ in any way that we want by tuning m.

Chapter 4

Computational Complexity of Particle Scattering and Ball Permuting Models

In this chapter, I borrow tools from pervious chapters to examine the computational complexity of the integrable models. In the beginning, I describe a classical motivation for the problem. After that I formally express the languages, and the goal of the rest of this chapter is to pin down the complexity of these languages.

1 Classical Computation with Probabilistic Swaps

Suppose that n distinct colored balls are placed on a straight line. Label the initial configuration of the balls from left to right with ordinary numbers $1,2,3,\ldots,n$. Clearly, each configuration of the balls can be (uniquely) represented by a permutation as a rearrangement of the elements of an n-element set $[n] := \{1,2,3,\ldots,n\}$. Therefore, the ball permuting model of n-balls has $n!$ distinct states. In general, the transition rules are given by the set of bijections : $[n] \to [n]$. These bijections along with their compositions correspond to the well-known symmetric group, which is the subject of the next section.

1.1 The Symmetric Group

Here is a formal definition of the set of bijections as a group:

Definition 4.1. *(The Symmetric Group)* Given a finite element set X of n elements, let $S(X) \cong S([n])$ be the set of bijections : $X \to X$. The bijections of $S[n]$ along with $\circ : S[n] \times S[n] \to S[n]$ as the composition of functions of functions from right-to-left, create a group $S_n := (S[n], \circ, e)$, with identity e as the identity function.

S_n is a group because each element of $S[n]$ is a bijection, and thereby is invertible. Also, the composition of functions $\circ$ is associative. For any $\pi \in S_n$ construct the structure $\Big\{\{1, \pi(1), \pi\circ\pi(1), \ldots\}, \{2, \pi(2), \pi\circ\pi(2), \ldots\}, \ldots, \{n, \pi(n), \pi\circ\pi(n), \ldots\}\Big\} =: \{C_\pi(1), C_\pi(2), \ldots, C_\pi(n)\} =: C_\pi$. This structure is called the set of cycles of permutation π, and each element $C_\pi(j) := \{\pi(j), \pi\circ\pi(j), \ldots\}$ is the cycle corresponding to element j. The number of cycles in C_π can vary from 1 to $n!$ (corresponding to e). $[n]$ is finite set, and for each $\pi \in S_n$ and $j \in [n]$ there is a number $n \geq k \geq 1$, which depends on π and j and $\pi^k(j) = j$. Therefore the size of the cycle is the minimum $|C_\pi(j)| = \min\{k > 0 : \pi^k(j) = j\}$. The set $[n]$ is therefore partitioned into the union of disjoint cycles $C_1, C_2, \ldots, C_N$. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N$ be the size of these cycles, clearly $\lambda_1 + \lambda_2 + \ldots + \lambda_N = n$.

Definition 4.2. For each positive integer n, a partition of n is a non-ascending list of positive integers $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N)$ such that $\lambda_1 + \lambda_2 + \ldots + \lambda_N = n$. Denote $\lambda!$ with $\lambda_1!\lambda_2!\ldots\lambda_N!$.

For any cycle structure of partition (size of cycles) $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_N$ there is a subgroup of S_n that is isomorphic to $S[\lambda] := S_{\lambda_1} \times S_{\lambda_2} \times \ldots \times S_{\lambda_n}$. In other words the subgroup consists of the product of N permutations each acting on a distinct cycle. Any such subgroup has $\lambda!$ elements. There are $n!/\lambda!$ ways to construct a subgroup isomorphic to $S[\lambda]$.

The symmetric group is indeed the mother of all groups, and any group can be embedded in an instance of a symmetric group. In other words, any group G is isomorphic to a subgroup of $S[G]$. However, such an embedding is not efficient since $S[G]$ has $|G|!$ elements, and is exponentially larger than the original group itself. However, the observation of this embedding had been the prime motivation for the definition of S_n as a group.

Theorem 4.1. *(Cayley) Any group G is isomorphic to a subgroup of S_G.*

Proof. We give an isomorphism between the elements of G and a subset of bijections on G. Consider the following set of bijections:

$$R_G := \{\rho_g : G \to G | x \mapsto g.x, \forall x \in G\}$$

We claim that $h : G \to R_G \leq S_G$ with the map $g \mapsto \rho_g$ is an isomorphism. For any $a,b \in G$, $\rho_g(a) = \rho_g(b)$ if and only if $g.a = g.b$ which is true if and only if $a = b$. And for all $a \in G$ there is an element $b = g^{-1}.a$ that $\rho_g(b) = a$. Therefore, for all $g \in G$, ρ_g is a bijection. Also $\forall x,y,a \in G$, $\rho_x(\rho_y(a)) = x.y.a = \rho_{x.y}(a)$ and thereby $\rho_x\rho_y = \rho_{x.y}$. Now $h(a) = h(b)$, if and only if $a(x) = b(x)$ for all $x \in G$, and for $x = e$, $a = b$. Since R_G has at most $|G|$ elements, the map must be onto too. So h is an isomorphism. Moreover, $\forall x,y \in G$, $h(x).h(y) = \rho_x\rho_y = \rho_{x.y} = h(x.y)$.

In order to complete the proof we must show that $R_G \leq S_G$. Clearly, $R_G \subseteq S_G$. R_G is associative with function composition and contains the identity bijection ρ_e. Since any h is an isomorphism, for any $f \in R_G$ there is a unique g that $f = \rho_g$, and has the inverse $\rho_{g^{-1}}$. Also for any $f_1, f_2 \in R_G$ there are unique $g_1, g_2 \in G$ such that $f_1 = \rho_{g_1}$ and $f_2 = \rho_{g_2}$ and thereby $f_1 f_2 = \rho_{g_1 g_2} \in R_G$ which is the closure property. □

Two permutations might have same cyclic structures. Indeed, corresponding to a cyclic structure with cycles of sizes $\lambda_1, \lambda_2, \ldots, \lambda_m$, there are $(\lambda_1 - 1)!(\lambda_2 - 1)! \ldots (\lambda_m - 1)!$ permutations. For example, there are two permutations with a single cycle of size 3, and these are the maps $(1,2,3) \to (3,1,2)$, and $(1,2,3) \to (2,3,1)$.

In order to address each permutation π uniquely, we can use an alternative representation for the cycles as an ordered list (tuple) $(y_1, y_2, \ldots, y_k)$, with $\pi(y_t) = y_{t+1 \mod k}$. Therefore, each permutation π can be represented by its cycles $\pi \cong (C_1, C_2, \ldots, C_k)$. We can define two different actions of the symmetric group S_n on an ordered list $(x_1, x_2, \ldots, x_n)$. The first one of these is called the left action where a permutation π acts on a tuple $X = (x_1, x_2, \ldots, x_n)$ as $(\pi, X) \mapsto (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) =: l(\pi)$. The left action rearranges the location of the symbols. The right action is defined by $(\pi, X) \mapsto (\pi(x_1), \pi(x_2), \ldots, \pi(x_n)) =: r(\pi)$. Throughout by permutation we mean left action, unless it is specified otherwise.

A permutation is called a swap of i, j if it has a nontrivial cycle (i, j) and acts trivially on the other labels. A swap is called a transposition (i) for $i \in [n-1]$ if it affects two adjacent labels $i, i+1$ with a cycle $(i, i+1)$. There are $n-1$ transpositions in S_n and the

group is generated by them. We use the notations (i, j) or $b_{i,j}$ for swaps and b_i and (i) for transpositions, interchangeably. Any permutation can be generated by at most $\frac{n(n-1)}{2}$ transpositions or n swaps. Indeed, we can define a distance between permutations as $d : S_n \times S_n \to \mathbb{N}$, with $d(\pi, \tau)$ being the minimum number of transpositions whose application on π constructs τ. Like any finite group S_n is also compact, and it is indeed isomorphic to a hypercube of dimension $n-1$, or a regular graph of degree $n-1$. Therefore, the problem of permutation generation has a reduction to the search problem on a hypercube. Given a distance on the permutations we can classify the permutations into even and odd ones.

Definition 4.3. A sign of a permutation $sgn : S_n \to \{-1, 1\}$ is a homomorphism, with the map $\sigma \mapsto 1$ if $d(\sigma, e)$ is even and gives -1 otherwise.

It is not hard to see that sign is a homomorphism. Given this, we can think of $E_n \leq S_n$ as a subgroup of S_n consisting of $\sigma \in S_n$ with $sgn(\sigma) = 1$. Clearly, E_n includes the identity permutation, inverse and closure.

Proposition 4.2. For $n \geq 2$, any group $(G, ., e)$ generated by $b_1, b_2, \ldots, b_{n-1}$ is isomorphic to S_n if and only if the following is satisfied:

- $b_i.b_j = b_j.b_i$ for $|i - j| > 1$
- $b_i^2 = e$ for $i \in [n-1]$
- $b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}$ for $i \in [n-2]$

1.2 The Classical Ball Permuting Model

Consider the following problem:

*"(*BALL*) The input is given as a target permutation $\pi \in S_n$ along with a $m = \mathsf{poly}(n)$ long list of swaps $(i_1, j_1), (i_2, j_2), \ldots, (i_m, j_m)$, and a list of independent probabilities $p_1, p_2, \ldots, p_m$. We apply the swaps in order to the list $(1, 2, 3, \ldots, n)$ in order each with its corresponding probability. That is we first apply (i_1, j_1) with probability p_1, (and with probability $1 - p_1$ we do nothing), then we apply (i_2, j_2) with probability p_2 and so on. Given the promise that*

the probability of target permutation is $\geq 2/3$ *or* $\leq 1/3$*, The problem is to decide which one is the case."*

The above process creates a probability distribution over the permutations of S_n and the problem is to decide if there is nonzero support on the target permutation. What is the computational complexity of deciding this problem? Is the complexity of the problem different if all the input swaps are adjacent ones? We can start with the identity permutation and add the permutations that get nonzero probability support at each step and check if the target permutation appears at the end of the process. If at some step τ appears in the list, after applying the next swap (i, j) we should update the list by adding $(i, j) \circ \tau$, and we should do the same thing for all of the permutations in the list. However, the size of the list can be as large as $n!$, and this suggests an upper-bound of $\mathsf{TIME}(n!) \subset \mathsf{EXP}$. However, we observe that this problem can be decided by a polynomial time nondeterministic Turing machine, where the short proof (witness) of the nonzero probability support is the sub list of swaps which creates the target permutation. However, the number of alternative witnesses can be as large as 2^m. Therefore, the first question is to see where in NP does BALL. It can be anywhere ranging from P to NP complete.

Next, we can think about the computational complexity of finding the exact probability of the target permutation. This can be viewed as a (enumerative) counting process. For example if all the probabilities are equal to $1/2$, then the probability of a target permutation is equal to the number of ways that one can produce the permutation with the given swaps divided by 2^m. Usually the counting problems are captured by the complexity class #P, which is the class of functions that compute the number of witnesses for an NP complete problem. However, even if the BALL problem itself is in P, the counting version can be as complex as #P complete. For example, deciding if an undirected graph has an Euler path is in P, but counting the number of Euler paths is known to be #P complete. Moreover, we can ask if one can approximate (known as *PTAS*) the target probability. However, if the exact counting is #P complete, a *PTAS* is also ruled out unless $\mathsf{P} = \mathsf{NP}$.

Notice that a BPP machine can sample from the output probability distribution over the permutations, by just tossing coins whenever a probabilistic swap is needed. However, the converse is not true and as we will see in the next section, there is an upper bound of

a class called AlmostL. Although the exact computation of the probabilities sounds like an intricate counting task, finding the marginal probability distribution of the location of each color in the end can be done in polynomial time.

Theorem 4.3. *Starting with the list* $(1,2,3,\ldots,n)$*, given a list of swaps* $(i_1,j_1),(i_2,j_2),\ldots,(i_m,j_m)$ *with corresponding probabilities* $p_1,p_2,\ldots,p_m$*, there is a polynomial time (in n and m) procedure to compute the marginal probability distribution over the locations for each (ball) color* $\in [n]$.

Proof. We give the procedure for the first color. We construct a vector V of size n, whose entries V_j for $j \in [n]$ is the probability of finding the first ball in the j'th location in the end of ball permutation. The vector is initialized at $(1,0,0,0,\ldots,0)$. For steps $t = 2,3,\ldots,m$, let $V_k \leftarrow V_k$ if $k \neq i_t, j_t$, and otherwise map:

$$V_{i_t} \leftarrow p_t V_{j_t} + (1-p_t)V_{i_t}$$

and,

$$V_{j_t} \leftarrow p_t V_{i_t} + (1-p_t)V_{j_t}$$

This can be done in $O(m.n)$ number of operations. □

1.3 The Yang-Baxter Equation

Alternatively, this process can be viewed as the action of probabilistic swaps can be captured by multiplication of stochastic matrices. Consider the probability simplex $\mathbb{V}_n := \{V \in \mathbb{R}^{n!}, \sum_j V_j = 1\}$. Each entry of V corresponds to a permutation, and its content is the probability that the permutation appears in the process. Consider an orthonormal basis for this vector space as $\{|\sigma\rangle : \sigma \in S_n\}$. The basis $|\sigma\rangle$ has probability support 1 on σ and 0 elsewhere. Now a swap can be viewed as the homomorphism $L : S_n \to End(\mathbb{V}_n)$ with the map $L(\pi)|\sigma\rangle = |\pi \circ \sigma\rangle$, that is the left action of the symmetric group on the vector space. Here $End(\mathbb{V}_n)$ is the set of operators which map the simplex $\mathbb{V}_n$ to itself. Denote the swap operator by $L_{i,j} := L(i,j)$. Notice that the symmetry operators of the simplex $\mathbb{V}_n$

is the set of stochastic matrices of size $n!$, that is the matrices whose rows sum up to 1. A probabilistic swap (i, j) with probability p is therefore given by the matrix:

$$R_{i,j}(p) = (1-p) + pL_{i,j}$$

So this clearly gives a reduction to matrix multiplication. A matrix description of the problem allows us to formalize the Yang-Baxter symmetry of three labels (balls). As discussed in the quantum ball permuting model, a Yang-Baxter (YB) symmetry is a restriction on probabilities in such a way that the swaps in order $(1,2),(2,3),(1,2)$ give the same probability distribution as the swaps $(2,3),(1,2),(2,3)$. We can view this as the solution to the following equation:

$$R_1(p_1)R_2(p_2)R_1(p_3) = R_2(p'_1)R_1(p'_2)R_2(p'_3) \tag{4.1}$$

We want to find the class of probabilities $1 \geq p_1, p_2, \ldots, p'_6 \geq 0$ which the equation is satisfied. If we rewrite $R_{i,j}(p)$ with the parameter $x \in [0,\infty)$:

$$R_{i,j}(x) = \frac{1+xL_{i,j}}{1+x}$$

We can observe that there is a solution of the form:

Theorem 4.4. *The following is a solution to equation 4.1:*

$$p_1 = \frac{x}{1+x} \qquad p_2 = \frac{x+y}{1+x+y} \qquad p_1 = \frac{y}{1+y}$$
$$p'_1 = \frac{y}{1+y} \qquad p'_2 = \frac{x+y}{1+x+y} \qquad p'_3 = \frac{x}{1+x}$$

Proof. First I need to show that these are indeed a solution to YB equation. Expanding the equation $R_1(x)R_2(x+y)R_1(y)$ we get:

$$\frac{1+xy+(x+y)(L_1+L_2)+(x+y)(xL_1L_2+yL_2L_1)+xy(x+y)L_1L_2L_1}{(1+x)(1+x+y)(1+y)} \tag{4.2}$$

Exchanging L_1 with L_2 and x with y in the left hand side of equation 4.2 gives the right hand side. Using the identity $L_1L_2L_1 = L_2L_1L_2$, however equation 4.2 is invariant under

these exchanges. □

2 General Hilbert Space of Permutations

In the previous section I discussed several quantum models, whose evolution is governed by local gates responsible for exchanging the order of internal degrees of freedom. My approach was to introduce a formal model, as I will call it the quantum ball permuting model, which captures all of the others. That is the quantum ball permuting model is more complex than the others, in the sense that with some feasible encodings, it can simulate the evolution of the other examples. In this model, all degrees of freedom are distinguishable, and the Hilbert space is described by the order of these labels; that is the basis of the Hilbert space is marked by the permutations of a finite-element set. We can think of these labels, as colors, distinguishable particles (balls), or internal degrees of freedom like qudits.

Let $\mathscr{H}_n = \mathbb{C}[S_n]$ be an $n!$ dimensional Hilbert space, with permutations of n symbols as its orthonormal basis. I consider a finite unitary gate set with all 2-local permuting gates acting on $\mathscr{H}_n$. I am interested in the set of local gates according to:

$$X(\theta,k) = \cos\theta I + i\sin\theta L_{(k,k+1)},$$

where θ is a free parameter, and I is the identity operator on the Hilbert space. $L_{(k,k+1)}$ is called the left transposition with the map:

$$|x_1,x_2,\ldots,x_k,x_{k+1},\ldots,x_n\rangle \mapsto |x_1,x_2,\ldots,x_{k+1},x_k,\ldots,x_n\rangle$$

for any permutation $x_1,x_2,\ldots,x_n$ of the labels $1,2,3,\ldots,n$.

For example, consider $\mathbb{C}S_2$, spanned by the basis $|12\rangle$ and $|21\rangle$. The matrix form of $X(\theta,1)$ on these basis according to:

$$X(\theta,1) = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}.$$

This has one free parameter, and moreover, each column is a permutation of the other.

However, the general form of a unitary on a two dimensional orthonormal Hilbert space has four parameters with the form:

$$U(\theta,\psi,\delta_1,\delta_2) = e^{i\psi}\begin{pmatrix} \cos\theta & i\sin\theta e^{i\delta_1} \\ i\sin\theta e^{i\delta_2} & \cos\theta e^{i(\delta_1+\delta_2)} \end{pmatrix}.$$

The $X(\cdot,\cdot)$ operator is a special case of U where all the phases $\psi,\delta_1,\delta_2 = 0$. Moreover, U is expressible by permutations on two labels only, only if $\delta_1 = \delta_2$ and $\delta_1 + \delta_2 = 0$ modulo 2π, which implies that $\delta_1,\delta_2 \propto \pi$. Therefore, this suggests that other than some arbitrary overall phase ψ, X is the most general form to express a local permuting unitary gate.

The operator L can be thought of as a homomorphism : $S_n \to\to U(\mathbb{C}S_n)$, I call it a left action because it lets a member τ of S_n act on a basis state $|\sigma\rangle, \sigma \in S_n$ according to:

$$L(\tau)|\sigma\rangle = |\tau\circ\sigma\rangle$$

However, the transpositions and swaps in general of the form $L_{(ij)}$ are both Hermitian and unitary, that is the image of a swap under L is an involution (a map that is its own inverse). Indeed, one can observe the following simple fact, which I am going to use in a later section:

Proposition 4.5. If L is unitary and also an involution, projecting out the overall phase, the operator $\alpha + \beta L$ for $\alpha,\beta \in \mathbb{C}$ is unitary if and only if $\alpha = c, \beta = is$ for some real valued parameters c,s, with $c^2 + s^2 = 1$.

We can also talk about a right action : $S_n \to U(\mathbb{C}S_n)$ with a corresponding map:

$$R(\tau)|\sigma\rangle = |\sigma\circ\tau\rangle$$

While a left action rearranges the physical location of the labels, a right action relabels them, and as it is mentioned in a later section, the unique commutant of the associative algebra generated by left actions is the algebra of right actions. Therefore, it is worthwhile to introduce a right permuting version of a local gate:

$$Y(\theta,k) = \cos\theta I + i\sin\theta R_{(k,k+1)}$$

A Y operator simply exchanges the labels k with $k+1$, independent of their actual location, and is not local in this sense. As a first input, the following theorem can be observed.

Theorem 4.6. *Let $U = X(\theta_m,k_m)\dots X(\theta_2,k_2)X(\theta_1,k_1)$ be any composition of the X operators, then columns of U as a matrix in S_n basis, are obtainable by permuting the entries of the top-most column.*

Proof. Consider the first column of U spanned by:

$$U|123\dots n\rangle = \sum_{\sigma\in S_n} \alpha_\sigma|\sigma\rangle$$

Where α_σ's are the amplitudes of the superposition. Now consider any other column marked by π:

$$U|\pi\rangle = \sum_{\sigma\in S_n} \beta_\sigma|\sigma\rangle$$

Clearly, $|\pi\rangle = R(\pi)|123\dots n\rangle$, and since $[U,R(\pi)] = 0$:

$$\sum_{\sigma\in S_n} \beta_\sigma|\sigma\rangle = \sum_{\sigma\in S_n} \alpha_\sigma|\sigma\circ\pi\rangle,$$

which is the desired permutation of columns, and in terms of entries $\beta_{\sigma\circ\pi} = \alpha_\sigma$.

□

The same conclusion can be made for the composition of Y operators. Let G be the group of unitary operators that can ever be generated by the compositions of X operators. While the unitary group $U(\mathscr{H})$ is a Lie group of dimension $n!^2$, as the corollary of the above theorem $G \subset U(\mathscr{H})$ as a Lie group, has dimension $n!$ which is polynomially smaller than $n!^2$. This is suggestive of the fact that G is not a dense subgroup of the unitary group.

In the definition of $X(\cdot,\cdot)$ and $Y(\cdot,\cdot)$ operators, the angle θ is independent of the labels that are being swapped. In fact the property observed in theorem 4.6 was a consequence

of this independence. Therefore, I introduce another local unitary, $Z(\tilde{\theta},k)$, wherein the transposition angles depend on the color of the labels. Here $\tilde{\theta} = \{\theta_{ij}\}$ is a list of angles, one element per each $i \neq j \in [n]$. By definition $Z(\tilde{\theta},k)$ acts on the labels $|ab\rangle$ in the locations k and $k+1$ with the following map:

$$Z(\tilde{\theta},k)|ab\rangle = \cos\theta_{ab} I + i \sin\theta_{ab} L_{(a,a+1)}$$

If we assume real valued angles with $\theta_{ij} = \theta_{ji}$, then the operator Z becomes unitary. Clearly, the X operators are the special case of the Z operators. In order to see this, consider any basis $|\sigma\rangle, \sigma \in S_n$, and suppose $\sigma(k) = a, \sigma(k+1) = b$ then:

$$\begin{aligned} Z^{\dagger}(\tilde{\theta},k) Z(\tilde{\theta},k)|\sigma\rangle = \\ (\cos\theta_{ab} - i\sin\theta_{ab} L_{(k,k+1)})(\cos\theta_{ab} + i\sin\theta_{ab} L_{(k,k+1)})|\sigma\rangle = |\sigma\rangle \end{aligned}$$

Now the composition of Z operators give rise to a subgroup $U(\mathscr{H})$ whose dimension can exceed $n!$. We can also define $W(\tilde{\theta},k)$ as an analogue of the Z operators. Such a W map is according to the following:

$$|\ldots \overset{a}{k} \ldots \overset{b}{k+1} \ldots\rangle \rightarrow \cos\theta_{ab} |\ldots \overset{a}{k} \ldots \overset{b}{k+1} \ldots\rangle + i \sin\theta_{ab} |\ldots \overset{a}{k+1} \ldots \overset{b}{k} \ldots\rangle.$$

The superscripts demonstrate the location of the labels. However, W is not a dual to Z, like X and Y's, since these operators do not commute in general. In general, we can confirm the following properties for the discussed operators:

- $X^{\dagger}(\theta,k) = X^{-1}(\theta,k) = X(-\theta,k)$, and the similar relations are true for the Y and Z operators.
- $[X(\theta,k), X(\theta',k')] \neq 0$ if and only if $|k-k'| = 1$, this is also true for the Y operators.
- $[Z(\tilde{\theta},k), Z(\tilde{\theta}',k')] \neq 0$ if and only if $|k-k'| = 1$, this is also true for the W operators.
- $[X(\theta,k), Y(\theta',k')] = 0$ for all values of k,k' and θ,θ'.

- $[Z(\tilde{\theta},k),R(\pi)]$ can be nonzero. Therefore if U is a composition of Z operators, the columns of can be different modulo permutation.

The last property suggests that the Lie group generated by Z operators is larger than G, and I am going to prove that with slight encodings one obtains a BQP-universal model.

2.1 The Yang-Baxter Equation

We can discuss the restriction on the angles of the X operators in such a way that they respect Yang-Baxter equation (YBE) of three particles. Therefore, this restricted version can capture the scattering matrix formalism of particles on a line. YBE in the scattering models asserts that the amplitudes depend only on the initial configuration and momenta of the particles.

Given a vector space $\mathbb{V}^{\otimes n}$, let R_{ij} for $i<j\in[n]$ be a family of two-local operators in $GL(\mathbb{V}^{\otimes n})$ such that each R_{ij} only affects the ij slot of the tensor product, and acts trivially on the rest of the space. Then, R is said to satisfy the parameter independent YBE if they are constant and:

$$R_{ij}R_{jk}R_{ij}=R_{jk}R_{ij}R_{jk}$$

Sometimes, I refer to the following as the YBE:

$$(R\otimes I)(I\otimes R)(R\otimes I)=(I\otimes R)(R\otimes I)(I\otimes R)$$

Both sides of the equation act on the space $\mathbb{V}\otimes\mathbb{V}\otimes\mathbb{V}$, and $R\otimes I$ acts effectively on the first two slots, and trivially on the other one. Similarly, I can define a parameter dependent version of the YBE, wherein the operator $R:\mathbb{C}\to GL(\mathbb{V}\otimes\mathbb{V})$ depends on a scalar parameter, and R is said to be a solution to the parameter dependent YBE is according to:

$$(R(z_1)\otimes I)(I\otimes R(z_2))(R(z_3)\otimes I)=(I\otimes R(z_1'))(R(z_2')\otimes I)(I\otimes R(z_3'))$$

for some $z_1,z_2,\ldots,z_3'$. I am interested in a solution of parameter dependent YBE with $X(\cdot,\cdot)$ operators. For simplicity of notations, in this part, I use the following operator:

$$R(z,k) := \frac{1}{\sqrt{1+z^2}} + \frac{iz}{\sqrt{1+z^2}} L_{(k,k+1)} = X(\tan^{-1}(z),k)$$

instead of the X operators. The following theorem specifies a solution to the parameter dependent YBE:

Theorem 4.7. *Constraint to $z_1 z_2 \ldots z_3' \neq 0$, the following is the unique class of solutions to the parameter dependent YBE, with the $R(\cdot,\cdot) = X(\tan^{-1}(\cdot),\cdot)$ operators:*

$$R(x,1)R(x+y,2)R(y,1) = R(y,2)R(x+y,1)R(x,2),$$

for all $x, y \in \mathbb{R}$.

Proof. We wish to find the class parameters $z_1, z_2, \ldots, z_3'$ such that the following equation is satisfied:

$$R(z_1,1)R(z_2,2)R(z_3,1) = R(z_1',2)R(z_2',1)R(z_3',2) \tag{4.3}$$

It is straightforward to check that if $z_1 = z_3'$, $z_3 = z_1'$ and $z_2 = z_2' = z_1 + z_2$, then the equation is satisfied. I need to prove that this is indeed the only solution. Let:
$\Gamma := \sqrt{\frac{(1+z_1'^2)(1+z_2'^2)(1+z_3'^2)}{(1+z_1^2)(1+z_2^2)(1+z_3^2)}}$.
If equation 4.3 is satisfied, then the following are equalities inferred:

1) $\Gamma.(1 - z_1 z_3) = (1 - z_1' z_3')$

2) $\Gamma.(z_1 + z_3) = z_2'$

3) $\Gamma.z_2 = (z_1' + z_3')$

4) $\Gamma.z_1 z_2 = z_2' z_3'$

5) $\Gamma.z_2 z_3 = z_1' z_2'$

6) $\Gamma.z_1 z_2 z_3 = z_1' z_2' z_3'$

Suppose for now that all of the parameters are nonzero; I will take care of these special cases later. If so, dividing 6) by 5) and 6) by 4) reveals:

$$\begin{aligned} z_1 &= z_3' \\ z_3 &= z_1'. \end{aligned} \tag{4.4}$$

Again suppose that $z_1 z_3 \neq 1$ and $z_1' z_3' \neq 1$. Then using the equivalences of 4.4 in 2), one gets $\Gamma = 1$, from 2) and 3):

$$z_2 = z_2' = z_1 + z_3,$$

which is the desired solution. Now suppose that $z_1 z_3 = 1$. This implies also $z_1' z_3' = 1$. Using these in 6) one finds $\Gamma . z_2 = z_2'$ and substituting this in 2) and 3) reveals $\Gamma = 1$ as the only solution, and inferring from equations $2), 3), \ldots, 6)$ reveals the desired solution. □

If one of the parameters is indeed 0, I can find other solutions too, but all of these are trivial solutions. The following is the list of such solutions:

- If $z_1 = 0$, then:
  - either $z_3' = 0$, which implies $z_3 = z_2'$ and $z_2 = z_1'$
  - or $z_2' = 0$ that implies $z_3 = 0$ and $\tan^{-1}(z_2) = \tan^{-1}(z_1') + \tan^{-1}(z_3')$.
- If $z_2 = 0$ then $z_1' = z_3' = 0$ and $\tan^{-1}(z_{,2}) = \tan^{-1}(z_1) + \tan^{-1}(z_3)$.
- If $z_3 = 0$, then:
  - either $z_1' = 0$, which implies $z_1 = z_2'$ and $z_2 = z_3'$
  - or $z_2' = 0$ that implies $z_1 = 0$ and $\tan^{-1}(z_2) = \tan^{-1}(z_1') + \tan^{-1}(z_3')$.

The solutions corresponding to $z_j' = 0$ are similar, and I can obtain them by replacing the primed rapidities with the unprimed rapidities in the above table. There is another corresponding to the limit $z_j \to \infty$:

$$X(0,1)X(0,2)X(0,1) = X(0,2)X(0,1)X(0,2)$$

Which corresponds to the property $L_{(1,2)}L_{(2,3)}L_{(1,2)} = L_{(2,3)}L_{(1,2)}L_{(2,3)}$ of the symmetric group. From now on, I use the following form of the R-matrices:

$$R(v_1, v_2, k) := R(v_1 - v_2, k),$$

for real parameters v_1, v_2, and the YBE is according to:

$$R(v_1, v_2, 1)R(v_1, v_3, 2)R(v_2, v_3, 1) = R(v_2, v_3, 2)R(v_1, v_3, 1)R(v_1, v_2, 2).$$

The parameters v_j can be interpreted as velocities in the scattering model. I can now extend the three label Yang-Baxter circuit to larger Hilbert spaces.

Definition 4.4. An m gate Yang-Baxter circuit over n labels is a collection of n smooth curves $(x_1(s), s), (x_2(s), s) \ldots (x_n(s), s)$ where $s \in [0,1]$, with m intersections, inside the square $[0,1]^2$, such that, $0 < x_1(0) < x_2(0) < \ldots < x_n(0) < 1$, and $x_i(1)$ are pairwise non-equal.

If $\sigma \in S_n$, and $x_{\sigma(1)}(1) < x_{\sigma(2)}(1) < \ldots < x_{\sigma(n)}(1)$, then σ is called the permutation signature of the circuit.

I can assume that all the intersections occur in different s parameters. Then one can enumerate the intersections from bottom to the top with the parameters $s_1 < s_2 < \ldots < s_m$. Let $\varepsilon < \min\{s_{t+1} - s_t : t \in [m-1]\}$, then for each intersection $s \in \{s_1, s_2, \ldots, s_m\}$, there is a permutation $\pi \in S_n$ such that:

$$x_{\pi(1)}(s-\varepsilon) < \cdots < x_{\pi(k)}(s-\varepsilon) < x_{\pi(k+1)}(s-\varepsilon) < \ldots < x_{\pi(n)}(s-\varepsilon)$$

and,

$$x_{\pi(1)}(s+\varepsilon) < \cdots < x_{\pi(k+1)}(s+\varepsilon) < x_{\pi(k)}(s+\varepsilon) < \ldots < x_{\pi(n)}(s+\varepsilon).$$

Then the intersection at s maps the order of lines from the permutation π to the per-

mutation $\tau := (k, k+1) \circ \pi$, which is the adjacent transposition of the k and $k+1$'th line. Thereby, I can say that the intersection corresponds to the transposition $(k, k+1)$, and the permutation signature of the Yang-Baxter circuit after this intersection is τ. Intuitively, the permutation signature at each section is the rearrangement of lines at that section. Indeed, each Yang-Baxter circuit represents a permutation, as its permutation signature. Two isotopic[1] Yang-Baxter circuits have the same permutation signature, but the converse is not necessarily true.

Definition 4.5. Let C be a Yang-Baxter circuit of m gates, each corresponding to a transposition $(k_t, k_t+1), t \in [m]$, and the permutation signature $\pi_t, t \in [m]$ at each of these gates. Then if one assigns a real velocity v_j to each line, then the Yang-Baxter quantum circuit for C is a composition of $R(\cdot,\cdot,\cdot)$ operators:

$$R(v_{\pi_m(k_m)} - v_{\pi_m(k_m)+1}, k_m) \ldots R(v_{\pi_2(k_1)} - v_{\pi_2(k_1+1)}, k_2) R(v_{k_1} - v_{k_1+1}, k_1).$$

Each of these unitary R-matrices is a quantum gate.

2.2 The Class of Quantum Ball-Permuting Languages

Now that I have specified the quantum gate sets, I make an attempt to formalize these models according to classes of languages they recognize, and then in a later section I will try to pin down their complexities. In general, I am interested in a form of quantum computing where one starts with some initial state in $\mathbb{C}S_n$, applies a polynomial size sequence of ball permuting gates, and then in the end samples from the resulting probability distribution in the permutation basis of S_n. An initial state of the form $|123\ldots n\rangle$ sounds natural, however, for the reasons that we are going to see later, I believe that the model in this case is going to be strictly weaker than the situation where the model is allowed to start with arbitrary initial states. Therefore, I study the case where the model has access to arbitrary initial states separately:

[1] we call two objects isotopic if there exists a smooth function which maps one to the other.

Definition 4.6. Let XQBALL be the class of languages $L \subseteq \{0,1\}^\star$ for which there exists a polynomial time Turing machine M which on any input $x \in \{0,1\}^\star$, outputs the description of a ball permuting quantum circuit C as a composition of X operators, such that if $x \in L$, $|\langle 123\ldots n|C|123\ldots n\rangle|^2 \geq 2/3$ and otherwise $\leq 1/3$. Also, define YQBALL and ZQBALL similarly with the ball permuting circuits as the composition of Y and Z operators, respectively. Define HQBALL in the same way with the H operators with (possibly non-planar) Yang-Baxter circuits.

Let XQBALL_{adj}, YQBALL_{adj}, ZQBALL_{adj}, and HQBALL_{adj} as the corresponding subclasses where all operators act on adjacent labels $\mathsf{XQBALL}^\star_{adj}$, $\mathsf{YQBALL}^\star_{adj}$, and $\mathsf{ZQBALL}^\star_{adj}$ as further restricted subclasses with all nonzero transposition angles.

For later sections, by XQBALL I mean the model that starts out from $|123\ldots n\rangle$, otherwise it is mentioned that the initial state is arbitrary. In any case, the final measurement is done in the ball label basis. Here I defined different variants of the model. It is conventional to consider such variations for a computational model, to see if the computing power is robust under these variations.

2.3 A Flash-forward to the Final Results

As I am going to define it later, PostHQBALL is the class of problems that are decidable on the ball scattering model with H operators when we are allowed to post select on the outcomes of intermediate demolition measurements. As we are going to see, the following upper-bounds can be obtained on the models:

Model	$\|123\ldots n\rangle$ initial state	arbitrary initial state
XQBALL	DQC1	BQP
ZQBALL	BQP	BQP
PostHQBALL	DQC1	BQP

The following lower-bounds are obtained:

Model	$\|123\ldots n\rangle$ initial state	arbitrary initial state
XQBALL	?	BQP
ZQBALL	BQP	BQP
PostHQBALL	?	BQP

3 Upper-bounds

Some of these models are the special cases of the others and as the first input, the following containments are immediate:

- $\mathsf{HQBALL} \subseteq \mathsf{XQBALL} \subseteq \mathsf{ZQBALL}$
- $\mathsf{XQBALL}^{\star}_{adj} \subseteq \mathsf{XQBALL}_{adj} = \mathsf{XQBALL}$, similar relations are true for H, Y and Z classes.

Clearly, models with arbitrary initial states immediately contain their corresponding model with initial state $|123\ldots n\rangle$. In order to see all the containments in BQP, it is sufficient to prove that $\mathsf{ZQBALL} \subseteq \mathsf{BQP}$.

Theorem 4.8. $\mathsf{ZQBALL} \subseteq \mathsf{BQP}$.

Proof. Let $L \in \mathsf{ZQBALL}$. Then, on any input $x \in \{0,1\}^{\star}$, there exists a polynomial time Turing machine that outputs the description of a Z ball permuting circuit. We simulate the Hilbert space of permutations with bits, by just representing each label of $[n]$ with its $\lceil \log n \rceil$ long binary representation. Therefore, we use $n\lceil \log n \rceil$ bits to encode the permutations of S_n. Although this is not an optimal encoding, it works in this case. The computation consists of three steps: at first we should simulate the initial state quantum states over binary bits, then we need to simulate the Z operators, and in the end we need to demonstrate how to sample from the output states.

1) Initialization: the BQP quantum circuit first applies enough not gates to the $|0\rangle^{\otimes n\lceil \log n \rceil}$ to prepare the encoded initial state $|123\ldots n\rangle$ with binary representations.

2) Evolution: it is sufficient to show how to simulate one of the $Z(\tilde{\theta})$ operators on two labels. The list $\tilde{\theta}$ consists of coefficients θ_{ij}. So for each pair of indices $i < j$ we

add a control ancilla bit. We initialize all of the ancilla bits with zeros. We first apply enough controlled operations to the binary encodings of the k and $k+1$ slots, to flip the i, j control bit if and only if the contents of k and $k+1$ slots are i and j, then controlled with the i, j control bit we apply the unitary $\cos\theta_{ij} + i\sin\theta_{ij}S$, where S is the operator which swaps all the bits in the k slot with all the bits in $k+1$. Notice the operator S acts on at most $O(\log n)$ qubits, and because of the Solovay-Kitaev theorem, it can be efficiently approximated by a quantum computer. We continue this for all of the indices $i < j$. Since we are using several ancilla bits, we need to uncompute their contents, at the end of each Z simulation. Therefore, a Z ball permuting quantum circuit can be simulated by a qubit quantum circuit with polynomial (in n) blow-up in its size, and a Hilbert space consisting of $O(n\log n + mn^2) = O(m.n^2)$, where m is the size of the original circuit.

3) Measurement: at the end of the computation we only need to measure the output bits, and interpret them as a permutation. Therefore the output of the Z ball permuting circuit can be sampled efficiently. We can also use enough controlled operations to flip a single bit if and only if the $n\lceil\log n\rceil$ bits encode the identity permutation. □

This readily demonstrates that all of the discussed models are contained in BQP. Next, I use the following theorem to prove that the models with X and Y operators

Theorem 4.9. *Let G and H be the unitary groups generated by X and Y operators, respectively. Then $G \cong H$.*

Proof. We show an isomorphism $T : G \to H$, as a linear map, with $T(L_\sigma) = R_{\sigma^{-1}}$, and the (linear) inverse $T^{-1} : H \to G$, with $T^{-1}(R_\sigma) = L_{\sigma^{-1}}$. Let U be any element in A, then U can be decomposed as a sequence of X operators $U_m = X(\theta_m, k_m)X(\theta_{m-1}, k_{m-1})\ldots X(\theta_1, k_1) =: \sum_{\sigma\in S_n}\alpha_\sigma L_\sigma$, we need to prove that $T(U_m) \in B$. I use induction to show that $T(U)$ is simply $Y(\theta_m, k_m)Y(\theta_{m-1}, k_{m-1})\ldots Y(\theta_1, k_1) \in B$. Clearly, $T(X(\theta_1, k_1)) = Y(\theta_1, k_1)$, since the inverse of each transposition is the same transposition. For $t < m$, let $U_t = X(\theta_t, k_t)X(\theta_{t-1}, k_{t-1})\ldots X(\theta_1, k_1)) =: \sum_{\sigma\in S_n}\alpha'_\sigma L_\sigma$. By induction hypothesis suppose that $T(U_t) =: V_t = Y(\theta_t, k_t)Y(\theta_{t-1}, k_{t-1})\ldots Y(\theta_1, k_1) = \sum_{\sigma\in S_n}\alpha'_\sigma R_{\sigma^{-1}}$. For simplicity let $c := \cos\theta_{t+1}$ and $s := \sin\theta_{t+1}$ and the transposition $k := (k_t, k_t + 1)$, then:

$$\begin{aligned} U_{t+1} &= X(\theta_{t+1},k_{t+1})U_t = \sum_{\sigma\in S_n} c\alpha'_\sigma L_\sigma + is\alpha'_\sigma L_{k\circ\sigma} \\ &= \sum_{\sigma\in S_n} (c\alpha'_\sigma + is\alpha'_{k\circ\sigma})L_\sigma \end{aligned}$$

and,

$$\begin{aligned} V_{t+1} &= Y(\theta_{t+1},k_{t+1})V_t = \sum_{\sigma\in S_n} c\alpha'_\sigma R_{\sigma^{-1}} + is\alpha'_\sigma R_{\sigma^{-1}\circ k^{-1}} \\ &= \sum_{\sigma\in S_n} c\alpha'_\sigma R_{\sigma^{-1}} + is\alpha'_\sigma R_{(k\circ\sigma)^{-1}} = \sum_{\sigma\in S_n} (c\alpha'_\sigma + is\alpha'_{k\circ\sigma})R_{\sigma^{-1}} \\ &= T(U_{t+1}) \end{aligned}$$

□

And more generally,

Theorem 4.10. *Let A and B be the associative algebras generated by L and R operators over the field* $\mathbb{C}$*, respectively. Then* $A \cong B$.

Proof. The isomorphism T of theorem 4.9 works. □

Corollary 4.11. XQBALL = YQBALL

Proof. I use the isomorphism result of theorem 4.9: suppose that after application of several gates $X(\theta_m,k_m)X(\theta_{m-1},k_{m-1})\ldots X(\theta_1,k_1)$ to the state $|123\ldots n\rangle$ one obtains the quantum state $|\psi\rangle = \sum_{\sigma\in S_n}\alpha_\sigma|\sigma\rangle$, then the application of the corresponding Y operators $Y(\theta_m,k_m)Y(\theta_{m-1},k_{m-1})\ldots Y(\theta_1,k_1)$ to the same initial state, one obtains $|\psi\rangle = \sum_{\sigma\in S_n}\alpha_\sigma^{-1}|\sigma\rangle$, where σ^{-1} is the inverse of the permutation σ. Any X computation can be deformed in a way that in the end the computation just reads the amplitude corresponding to the identity permutation, i.e., $\alpha_{123\ldots n}$. Since the inverse of the identity permutation is identity itself, X computation can be simulated by a Y computation, by just applying the same quantum circuit with Y operators and read the identity amplitude in the end. A similar reduction also works from X to Y computations. □

Next, I demonstrate that adjacent swaps and nonadjacent swaps do not change the computational power of the ball permuting model:

Theorem 4.12. $\mathsf{XQBALL}^{\star}_{adj} = \mathsf{XQBALL}_{adj} = \mathsf{XQBALL}$*, also the same equalities are true for Y and Z operators.*

Proof. The direction $\mathsf{XQBALL}^{\star}_{adj} \subseteq \mathsf{XQBALL}_{adj} \subseteq \mathsf{XQBALL}$ is immediate. Now in order to see $\mathsf{XQBALL} \subseteq \mathsf{XQBALL}^{\star}_{adj}$, consider any gate $X(\theta)$, if θ is a multiple of 2π, then composing X with itself for a constant number of times reveals the pure swap operator. Otherwise, if it is an irrational multiple of 2π, because of equidistribution theorem for any $\varepsilon > 0$, there is a number $N = O(1/\varepsilon)$, such that composing X with itself for N times, reveals an operator that is ε-close to the pure swap operator. Given this observation, any computation in XQBALL_{adj} can be simulated by a computation $\mathsf{XQBALL}^{\star}_{adj}$, where all the X operators are different from swaps. Finally, I will prove $\mathsf{XQBALL} \subseteq \mathsf{XQBALL}_{adj}$. This should be also true, since any non-adjacent swap can be simulated with a sequence of adjacent swaps. See the proof of theorem ??. The same arguments also work for Y and Z operators. □

The general definition of HQBALL involves possibly non-planar circuits. Although this is not physical, it is interesting to show that the model is equivalent to XQBALL itself:

Theorem 4.13. $\mathsf{XQBALL} = \mathsf{HQBALL}$.

Proof. The direction $\mathsf{HQBALL} \subseteq \mathsf{XQBALL}$ is immediate; R gates are special cases of X gates. To see the other direction, given any ball permuting quantum circuit as a composition $C = X(\theta_m, k_m)X(\theta_{m-1}, k_{m-1})\dots X(\theta_1, k_1)$, we construct an HQBALL quantum circuit with non-planar Yang-Baxter circuit C', which can efficiently sample from the output of C. I use non-planarity (in a tricky way) to compose a two particle R quantum gate with itself over and over. As it can be seen in the next theorem, non-planarity is indeed necessary for this simulation. Suppose that C acts on n labels, then one can choose the velocities of C' to be $v_1 = n\pi, v_2 = (n-1)\pi, \dots, v_n = \pi$. Given this choice of velocities, the rapidity $v_i - v_j \propto \pi$ for all i, j and the angle $\phi_{ij} \tan -1(v_i - v_j)$ is an irrational multiple of π. From Gibb's equidistribution theorem, for any $\varepsilon > 0$ and angle $\theta \in [0, 2\pi]$, there is a number $N = O(1/\varepsilon)$

such that $|N\phi_{ij} - \theta| < \varepsilon, \mod 2\pi$. So given any gate $X(\theta_t, k_t)$, we approximate it with accuracy ε/m with $O(m/\varepsilon)$ compositions of the operator $R(z, k_t)$ with itself. Thereby, we approximate all of the local gates with accuracy ε/m, and given the linear propagation of error in quantum circuits, the unitary C' is ε-close to C, with respect to some matrix norm.

□

Corollary 4.14. XQBALL = HQBALL, on arbitrary initial states.

Proof. Given that the unitary C' described in the proof of 3 can approximate the unitary C with arbitrary precision, we can conclude that given any initial state $|\psi\rangle$, the quantum state $C|\psi\rangle$ is arbitrary close to $C'|\psi\rangle$. □

Theorem 4.15. *Let Q_n be the Lie group generated by planar Yang-Baxter quantum circuits over n labels, then Q_n as a manifold is isomorphic to the union of n! manifolds, each with dimension at most n.*

Proof. Fix the velocities $v_1, v_2, \ldots, v_n$. The idea is to demonstrate an embedding of the group generated with these fixed velocities into the symmetric group S_n. Consider any two planar Yang-Baxter quantum circuits C and C', with permutation signatures σ and τ, respectively. I show that if $\sigma = \tau$, then $C = C'$.

The underlying circuit of C corresponds to a sequence of transpositions $k_1, k_2, \ldots, k_M$ and C' corresponds to another sequence $l_1, l_2, \ldots, l_N$, such that $k_M \circ \ldots \circ k_2 \circ k_1 = \sigma$, and $l_N \circ \ldots \circ l_2 \circ l_1 = \tau$. Then the unitary operators C and C' can be written as a sequence of R operators:

$$C = R(z_M, k_M) \ldots R(z_2, k_2) R(z_1, k_1)$$

and,

$$C' = R(z'_N, l_N) \ldots R(z'_2, l_2) R(z'_1, l_1).$$

Where the z parameters are the suitable rapidities assigned to each two-particle gate based on the velocities $v_1, v_2, \ldots, v_n$, and the underlying Yang-Baxter circuits. From propo-

sition 4.2 if two sequence of transpositions $k_M \circ \ldots \circ k_2 \circ k_1$ and $l_N \circ \ldots \circ l_2 \circ l_1$ amount to the same permutation, then there is a sequence of substitution rules among:

1) $b_i^2 \Leftrightarrow e$

2) $b_i b_j \Leftrightarrow b_j b_i$ if $|i-j| > 1$

3) $b_i b_i + 1 b_i \Leftrightarrow b_i + 1 b_i b_i + 1$, for all $i \in [n-1]$

Such that if we start with the string $k_M \circ \ldots \circ k_2 \circ k_1$ and apply a sequence of substitution rules, we end up with $l_N \circ \ldots \circ l_2 \circ l_1$. All I need to do is to prove that the sequences of unitary gates are invariant under each of the substitution rules. The invariance under each rule is given in the below:

1) If we apply two successive quantum transpositions on the labels $i, i+1$ we will end up with the identity operator. This follows from unitarity $R(z)R(-z) = I, \forall z \in \mathbb{R}$, and planarity of the circuits. Suppose that in the first transposition the left strand has velocity v_1 and the right strand has velocity v_2, then the first unitary gate is $R(p1-p2,i)$, now applying another transposition on i and $i+1$'th label corresponds to the unitary $R(p2-p1,i)$, which is the inverse of the first one. This is true since after the first application of R_i the order of velocities is exchanged, and because of planarity the only way to compose the unitary with itself is with $R(p2-p1,i)$.

2) Clearly $R(\cdot,i)R(\cdot,j) = R(\cdot,j)R(\cdot,i)$ for $|i-j| > 1$, since these are 2-local gates.

3) This part also follows from the Yang-Baxter equation.

We can then start with the unitary $C = R(z_M,k_M)\ldots R(z_2,k_2)R(z_1,k_1)$ and apply the same substitution rules and end up with $C = R(z'_N,l_N)\ldots R(z'_2,l_2)R(z'_1,l_1)$.

Now let $Q_n(\sigma)$ be the Lie group corresponding to all Yang-Baxter quantum circuits with permutation signature σ. For each choice of velocities, there is exactly one unitary in this group, so $Q_n(\sigma)$ is locally diffeomorphic to $\mathbb{R}^n$, and $Q_n = \cup_{\sigma \in S_n} Q_n(\sigma)$. □

In the following I show that even with post-selection in the end, a quantum planar Yang-Baxter circuit still generates a sparse subset of unitary group.

Theorem 4.16. *The set of unitary operators generated by* HQBALL_{adj} *with post-selection in particle label basis in the end of computation, correspond to the union of (discrete)* $n!^{O(1)}$ *manifolds, each with linear dimension.*

Proof. We follow the proof of theorem 4.16. Consider the planar YB circuits on n labels. If the input velocities are fixed, then the unitary operators generated by the model constitute a finite set of size at most $n!$. There are finite $n!^{O(1)}$ to do a post-selection on the output labels of each circuit. So for each fixed set of velocities, the unitary matrices obtained by post-selection and proper normalization still constitute a set of size $n!^{O(1)}$. Therefore, label the manifolds with the permutation signature of the circuits and the type of final post-selection. Then the points in each of these manifolds are uniquely specified by n velocity parameters, which is an upper-bound on the dimension for each of them. □

Notice that result of these theorems still hold if we allow the circuit models to start with arbitrary initial states.

3.1 XQBALL on Separable States

The result of this section was obtained in joint collaboration with Greg Kuperberg. In this section, I find an upper-bound for the class XQBALL; that is computing with the $|123\ldots n\rangle$ initial state. I provide evidence that it is unlikely to do universal quantum computation with this initialization of states.

XQBALL can alternatively be defined as the class of decision problems that are polynomial time reducible to the following problem:

"The input is a polynomial $m = n^{O(1)}$ long list of swaps $(i_1, j_1), (i_2, j_2), \ldots, (i_m, j_m)$ on n labels, and an independent list of rotations $\theta_1, \theta_2, \ldots, \theta_m \in [0, 2\pi]$. Let $C = X_{i_m,j_m}(\theta_m)X_{i_{m-1},j_{m-1}}(\theta_{m-1})\ldots X_{i_1,j_1}$ be the corresponding ball permuting quantum circuit. Given the promise that $|\langle 123\ldots n|C|123\ldots n\rangle|$ is either $\geq 2/3$ or $\leq 1/3$, decide which one is the case."

XQBALL(σ, τ) can be defined in a similar way, except that the initialization and finalization is according to $\langle\sigma|C|\tau\rangle$. Clearly, there are linear time reductions between the two complexity classes in both ways. For example, given any instance C of XQBALL(σ, τ), the reduction is just to add pure swaps $L(\sigma)$ and $L(\tau)$ to obtain $C = L^{-1}(\tau)CL(\sigma)$ as the equivalent instance in XQBALL. The reduction in the other direction is similar. This is indeed due to the fact that unitary matrices of the XQBALL have at most $n!$ degrees of freedom, compared to $n!^2$ number of degrees of freedom of the unitary group. This is because, as dis-

cussed, each column of any such unitary can be obtained by permuting the other columns. This is indeed a special property and we believe that it makes this complexity class a weak one. Indeed, the situation can be phrased according to the trace of the unitary matrices generated in this class:

Lemma 4.17. Given any ball permuting quantum circuit C over $\mathbb{C}S_n$, the trace $Tr(C) = n!\langle 123\ldots n|C|123\ldots n\rangle$.

Proof. A quantum ball permuting circuit, by definition, consists of left permuting actions only, and it commutes with a right action $R(\sigma)$ (relabeling) for any $\sigma \in S_n$. Thereby $\langle 123\ldots n|C|123\ldots n\rangle = \langle 123\ldots n|R^{-1}(\sigma)CR(\sigma)|123\ldots n\rangle = \langle \sigma|C|\sigma\rangle$. From this, $Tr(C) = \sum_{\sigma\in S_n}\langle \sigma|C|\sigma\rangle = n!\langle 123\ldots n|C|123\ldots n\rangle$. □

This suggests that all the amplitudes are closely related to the trace of a ball permuting operator. I also used the observation of commutation with the right actions (relabeling) to obtain a non-universality criterion in section 9.1.

At this point, it is crucial to be precise about they way XQBALL is simulated in BQP. Consider the following simulation: given a circuit C over $\mathbb{C}S_n$, simulate the ball permuting model with qubits. Represent each number in $[n]$ with $\log n$ bits of binary representation and let the initial state be the encoding of $123,\ldots n$. We just need to simulate each local ball permuting gate with corresponding gates on qubits. I demonstrate such a simulation for $X_{1,2}(\theta)$ the construction of the rest of the operators is similar. Let $T_{i,j}$ be the swap operator in the qubit basis, i.e. the operator which swaps the content of the i and j'th qubits. Then clearly $\tilde{T}_{12} := T_{1,\log n}T_{2,1+\log n}\ldots T_{\log n,2\log n}$ is Hermitian and moreover (an involution) $\tilde{T}_{12}^2 = I$. From this we conclude that $\exp(i\theta\tilde{T}_{12}) = \cos(\theta)I + \sin(\theta)\tilde{T}_{12}$ is a unitary operator, and can be approximated with a polylog(n) size circuit of a universal gate set.

As discussed, the one clean qubit model is an example of a problem which is intermediate between P and BQP. The major motivation for the definition of this complexity class has been the physics of nuclear magnetic resonance. In such a model most of the qubits are in a highly mixed state, and an experimenter has control over a few qubits. Although one bit of quantum information does not sound like a high computational power, it has been

shown that this model is able to solve promise problems that are believed to be hard for the class P. One these problems which is relevant to the current work is computing the trace of a large unitary matrix.

Definition 4.7. (Trace) given as input the poly(n) size description of a unitary circuit U over n qubits, and the promise that either $\frac{1}{2^n}|Tr(U)| \geq 2/3$ or $\leq 1/3$, decide which one is the case. I assume that U is generated from a BQP universal gate set.

Theorem 4.18. *(Jordan-Shor [45])* Trace $\in$ DQC1. *Moreover,* Trace *is a complete promise problem for* DQC1*, i.e.,* DQC1 *can be defined as the class of decision problems that are polynomial time reducible* Trace*.*

Given any ball permuting circuit C, it is sufficient to prove that deciding if $\langle 123\ldots n|C|123\ldots n\rangle$ is large or small is a problem decidable in DQC1. In order to do this, I give a polynomial time algorithm which takes the description of C as input, and outputs the description of a unitary U from a BQP-universal gate set, such that $Tr(U) \propto \langle 123\ldots n|C|123\ldots n\rangle$ with a known proportionality constant. The algorithm goes according to the following: given n, specify $n\lceil \log n\rceil$ qubits to represent each label in $1,2,3,\ldots,n$, and $\frac{n(n-1)}{2}$ more (flag register) qubits, and label them by $f_{ij}, i<j \in [n]$. The quantum circuit U consists of two parts. The initial part of U, for each $i<j\in[n]$, using sequences of $CNOT$, compares the qubits $(i-1)\lceil \log n\rceil +1$ to $i.\lceil \log n\rceil$ with the qubits $(i-1)\lceil \log n\rceil +1$ to $i.\lceil \log n\rceil$, bit by bit, and applies the Pauli gate σ_x to the register $f_{i,j}$ if the corresponding bits are all equal to each other. The second half of U is given by the BQP-simulation of Theorem **??**. Then U is fed into the Trace computation. It suffices to show that $Tr(U) \propto \langle 123\ldots n|C|123\ldots n\rangle$. Let $N := n\lceil \log n\rceil + n(n-1)/2$. The trace $Tr(U) = \sum_{x\in\{0,1\}^N}\langle x|U|x\rangle$. Given the described construction, the term $\langle x|U|x\rangle = \langle \sigma|C|\sigma\rangle$, if and only if the label part of x is the correct encoding of the permutation σ, and if x is not a correct encoding of a permutation it gives 0. There are $2^{n(n-1)/2}$ strings like x which encode σ correctly, therefore:

$$1/2^N Tr(U) = \frac{2^{n(n-1)/2}}{2^N} Tr(C) = \frac{n!}{2^{n\lceil \log n\rceil}}\langle 123\ldots n|C|123\ldots n\rangle.$$

This is still problematic, since the coefficient $\frac{n!}{2^{n\lceil \log n\rceil}}$ can be exponentially small, and thereby using polynomial iterations of the DQC1 computation wouldn't reveal sufficient

information bout the desired amplitude. Taking a close look at the this coefficient, it is observed that:

$$\frac{n!}{dimV}$$

where V is the Hilbert space that is used to encode permutations in it. In the discussed, I used $O(n\log n)$ bits to encode permutations of n labels. We need a more compressed way of encoding these permutations, and more precisely we need an encoding which uses $\log_2(n!n^{O(1)}) = \log_2(n!) + O(n)$ number of bits. Therefore, the existence of an encoding with the following properties implies $\mathsf{XQBALL} \subseteq \mathsf{DQC1}$:

- 1) the encoding uses $\log_2(n!) + O(n)$ number of bits.
- 2) for any transposition τ, there is a polynomial size reversible circuit C_τ which inputs the encoding of any permutation $\langle\pi\rangle$ and outputs $\langle\tau\circ\pi\rangle$.
- 3) it is verifiable, in the sense that there is a reversible circuit which inputs any string of size $\log_2(n!) + O(n)$ bits (the same size as the size of the encoding) and an extra flag bit f, and outputs the first $\log_2(n!) + O(n)$ bits without altering them, and flips f if the string is not a correct encoding of a permutation.

The requirement is to find a lexicographic ordering on the permutations of n labels. Based on this lexicographic ordering, one can think of a bijection between S_n and the numbers of $[n!]$, which is efficiently computable in $S_n \to [n!]$ and also in $[n!] \to S_n$ direction. Call this bijection g, and g^{-1} as its inverse. Indeed efficient computation of such a bijection exists [19] [2]. Then the first condition is satisfied. Also the verifiability condition is relaxed, since we are dealing with bijections. In order to see the implementation of condition 2, notice that if we can implement C_τ for each transposition τ, then the circuit is reversible since $C_\tau^2 = C_{\tau^2}$ is equal to the identity circuit, which is clearly reversible. Given reversible circuits for g and g^{-1} one can implement C_τ. Just use g^{-1} to map the input number to any (even less compressed) encoding of the permutations. We can use polynomial amount of

[2] Also see http://stackoverflow.com/questions/12146910/finding-the-lexicographic-index-of-a-permutation-of-a-given-array and http://stackoverflow.com/questions/8940470/algorithm-for-finding-numerical-permutation-given-lexicographic-index

ancilla bits. Then apply the transposition in this encoded basis, and finally use g to invert the permutation back to a binary number in $[n!]$. Suppose that we use N number of ancilla bits, then an interaction of DQC1 reveals:

$$\frac{1}{2}+\frac{1}{2}\frac{n!}{(n!+O(1))2^N}2^N\langle 123\ldots n|C|123\ldots n\rangle$$

which proves the desired result:

Theorem 4.19. XQBALL $\subseteq$ DQC1.

4 The Scattering Quantum Computer with Demolition Intermediate Measurements

In the previous section, I showed that the quantum circuit model with planar Yang-Baxter symmetry, even with post-selection in the end, generates discrete Lie groups each of linear dimension in n, and therefore I believe that it probably fails to generate a dense subgroup of $U(n!)$. The model with planar YB quantum circuits is an upper bound on the models of particle scattering in $1+1$ dimension, so the same result for the complexity of these models; this is basically the following corollary:

Corollary 4.20. (Of theorem 4.16) let S be the set of unitary scattering operators generated by n particle scattering with any of the models in section 2. Then S corresponds to a manifold of dimension at most n.

Proof. The proof of theorem 4.16 still works here, with a tiny difference. In the scattering problem, the signature of the corresponding planar YB quantum circuit is fixed by the velocities, therefore, for any set of velocities, the model can generate at most one unitary, and hence the points in the set of scattering matrices combined together is parameterized with n real numbers, as velocities. □

Moreover, as another corollary of theorem 4. 16, we find out that probably a proof for post-selected BQP universality of particle scattering does not exist, if we post-select in the particle label basis in the end of computation:

Corollary 4.21. (Of theorem **??**) let S be the set of unitary scattering operators generated by n particle scattering with any of the models in section 2, with and without post-selection in the particle label basis in the end of computation. Then S corresponds to $n!^{O(1)}$ manifolds each with dimension at most n.

Proof. Following the proof of 4.16, if the velocity parameters are fixed, then the model can generate exactly one unitary operator, and there are (discrete) $n!^{O(1)}$ ways to do post-selection on the output of this unitary matrix. Therefore, given a set of particles initialized with fixed velocities, the model can generate at most $n!^{O}(1)$ number of unitary scattering matrices. □

Here I add another ingredient to the scheme of computing with particle scattering; that is intermediate measurement. The idea is to use intermediate measurements to simulate X operators of class XQBALL, and then because of the equivalence between XQBALLwith arbitrary initial states and BQP, particle scattering with intermediate measurement can also efficiently sample from the output of a BQP computation and then from a PostBQP, if it is allowed to start out with arbitrary initial states. There are two ways to do an intermediate measurement. The first of these is to measure, intermediately, in the particle label basis, in a way that the outcome of the measurement is the post measurement quantum state. In this way, because of the planarity of circuits in one spatial dimension, I have to use the post-measurement state over and over. In a later section I will discuss how to nondeterministically simulate X operators with non-adaptive use Yang-Baxter gate. Here nondeterministic simulation I mean a simulation that succeeds with a certain probability. However, this model of computing is not realistic, and moreover, because of the multiple use of the post-measurement states it disallows one to use post-selection hardness result in this case.

The second scheme of intermediate measurement is a non-adaptive demolition measurement due to a particle detector. That is a measurement which reveals the classical output of measurement but not the post-measurement quantum state. In other words the detection throws the measured label to a second Hilbert space, which is inert and no quantum operation can affect it anymore.

4.1 Programming the Scattering Amplitudes with Intermediate Particle Detections

The goal is to come up with a quantum algorithm based on particle scattering in $1+1$ dimension, which takes the description $\langle C \rangle$ of a general X quantum ball permuting model as an input, and outputs the description of a sequence of particle scatterings and a sequence of intermediate non-adaptive demolition particle measurements, in a way that the overall process efficiently samples from the output of C. The construction of this section is very similar to the nondeterministic gates of [36, 38]. For a review of quantum computing with intermediate measurements see [18, 39, 48].

For example, consider the X ball-permuting gate of FIG. 1., where we let the two input wires interact with arbitrary amplitudes, and in the end we measure the label locations of A and B. The objective is to have a particle scattering gadget that can simulate the output distribution of circuit in FIG. 1. Therefore, we can use the four particle gadget of FIG. 2. to accomplish this. The overall scattering process acts as a nondeterministic gate, in the sense that the gadget succeeds in a successful simulation, only with a certain probability, and an experimenter can verify, in the end of the scattering, if the gadget has succeeded in its simulation. In FIG. 2. the lines represent particle trajectories, and the red circles are interactions between them. The rectangles are particle detectors, which measure the particles intermediately, and output the classical measurement outcome, and not the post-measurement quantum states. Indeed, the measured particle is thrown away in a second inert Hilbert space, as the detectors' internal degrees of freedom, upon which no particle scattering can make any further affections. The experimenter, then post-selects on measuring the labels a and b, in the left and right detectors, respectively. Then (s)he lets the particles collide, and in the end reads the actual measurement outcomes. If the outcomes match the post-selected labels, (s)he makes sure that the scattering has succeeded in producing the desired swap. The velocities v_1, v_2, v_a and v_b can be tuned in such a way that the desired swap is obtained. The probability of success, thereby, depends on these velocity parameters. More precisely, conditioned on a successful simulation, the overall action of the scattering gadget is the swap $X(\tan^{-1} z_{eff}, 1)$, where:

$$\tan^{-1} z_{eff} = \tan^{-1} z_1 + \tan^{-1} z_2$$

with $z_1 = v_1 - v_2$ and $z_2 = v_a - v_b$. As a result of this, the left and right black output particles will have velocities v_b and v_a, respectively. Moreover, as described, in this model of scattering the particles move on straight line in time-space place, and they do not naturally change their directions. We thereby can use a two particle gadget of FIG. 3. to navigate the particles' trajectories. In FIG. 3. the two particles collide from left to right, and the left particle is measured in the end. Conditioned on the detector measures the label a, the navigation is successful, and the outcome of this process is particle with its original label 1 moves to the right direction with velocity v_a. One can match $v_a = v_1$, so that the overall action of the nondeterministic gadget is a change of direction. The success probability, then depends on v_1 and v_a. Notice that all of these results still hold if the black particles start out of arbitrary initial superpositions. However, one should make sure that the ancilla particles start out of states with definite distinct labels; labels that are not in a superposition with any other labels.

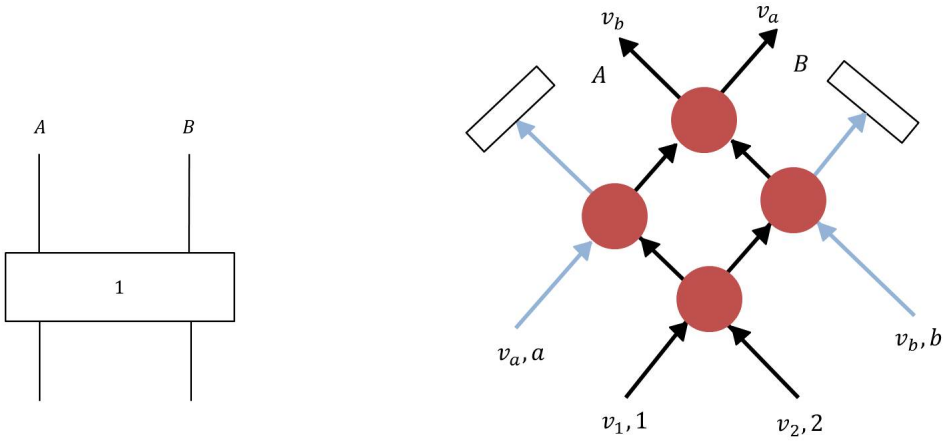
As another example consider the X quantum ball permuting circuit of FIG. 4. This circuit consists of X gates, $1,2$ and 3, and they permute labels of the four input wires. In the end we measure the output wires A,B,C and D, in the particle label basis. We use the particle scattering sequences of FIG. 5. to simulate this circuit. Again the blue particles are ancilla, and the black particles correspond to the wires, and the labels $1,2$ and 3, correspond to the simulation of gates $1,2$ and 3 in FIG. 4., respectively. Each of the detectors measure in the particle label basis, and in the end the experimenter measures the particle locations A,B,C and D, corresponding to the output wires A,B,C and D, in FIG. 4., respectively. The overall scattering process succeeds in its simulation only if the detectors measure the ancilla particles with their initial labels. That is, conditioned on all blue particles successfully pass through their intermediate interactions and bouncing off the last interaction, the scattering process simulates the circuit of FIG. 4. successfully. This is true, because the particles move on straight lines, and the only event corresponding to detecting an ancilla particle with its original label is the one where it never bounces

off in its intermediate interactions, and bounces off its final collision before moving to its corresponding detector. For an example of a larger simulation see the simulation of the X quantum circuit of FIG 6. with the scattering process of FIG. 8. This example specially, demonstrates that during the scattering, blue (ancilla) particles can experience many intermediate interactions, and the number of these interactions can scale linearly in the number of particles being used. Therefore, the event corresponding to a successful simulation can have exponentially small probability.

It is important to mention that because of the Yang-Baxter equation, braiding of two particles is impossible. Braiding means that two particles can interact with each other over and over, however, because of the expression of unitarity, $H(u)H(-u) = I$, two successive collisions is equivalent to no collision. The role of the intermediate measurements is to allow two particles interact over and over without ending up with identity.

4.2 Stationary Programming of Particle Scatterings

The simulations of last section are both intuitive and instructive. However, they have a drawback. The slope of the lines corresponding to particle trajectories, depend on the velocities of the particles. So for large simulations, we need to keep the track of the architecture of collisions, and the amplitudes of interactions at the same time, and this can be both messy and difficult in the worst cases. In this section, I try to present a better simulation scheme where one only needs to keep track of amplitudes, and the architecture of collisions can be tuned easily. The philosophy is to have steady particles, in the beginning, and whenever we want a ball permuting gate, a number of ancilla particles are fired to the target steady particles. Then the intermediate detections are used, and then post-selections on their outcomes enables the model to simulate an arbitrary X quantum ball permutation. By stationary particle I mean a particle that is not moving. In order to fulfill this purpose, I use the stationary gadget of FIG. 8. The objective is to impose a desired permutation on the input black particles. And I want the black particles to stay stationary in the end of the simulation. In order to do this, two other stationary ancillas are put at the left and right of the black particles. Then, two other ancilla particles, the desired velocities, are fired from



(a) (b)

Figure 4-1: (a) The representation of an X operator. The gate permutes the input labels, and in the end we measure the labels of output wires A and B. (b) Four particle scattering gadget gadget to simulate X rotation of FIG. 1. Lines represent the trajectories of particles, red circles demonstrate interactions, and white rectangles are detectors. Blue particles are ancillas which mediate computation, and black particles are the particles that we wish to implement the actual quantum swap on. The gate is nondeterministic in the sense that it succeeds in producing the desired superposition on labels $|1\rangle$ and $|2\rangle$ only if the left and right detectors detect $|a\rangle$ and $|b\rangle$ labels in the particle label basis, respectively. The probability of success, thereby, depends on the velocities. That is conditioned on both ancilla particles bounce off the black particles, the gate operates successfully.

left and right, and post-selection is made on them bouncing off from the black particles. Then the two black particles interact and exchange momenta, and then they collide with the two stationary ancillas. In the end, we measure and post-select on the ancilla particles bouncing off the black particles. Therefore, in the end of the process, the stationary black particles are left stationary, and the desired superposition is obtained. In order to see an example for the implementation of the stationary programming in larger circuits, see the simulation of XQBALL circuit of FIG. 9. with stationary particle programming of FIG. 10.

Here I demonstrate that using intermediate post selection, even with the planar Yang-Baxter symmetry one can simulate the unitary operators generated by XQBALL. The main idea is to pick a planar Yang-Baxter circuit C and use local intermediate post selections which projects the quantum states to the one where all i'th colors in the superposition being seated at the j'th position, thereby for the Hilbert space $\mathbb{C}S_N$ there are N^2 choices for such

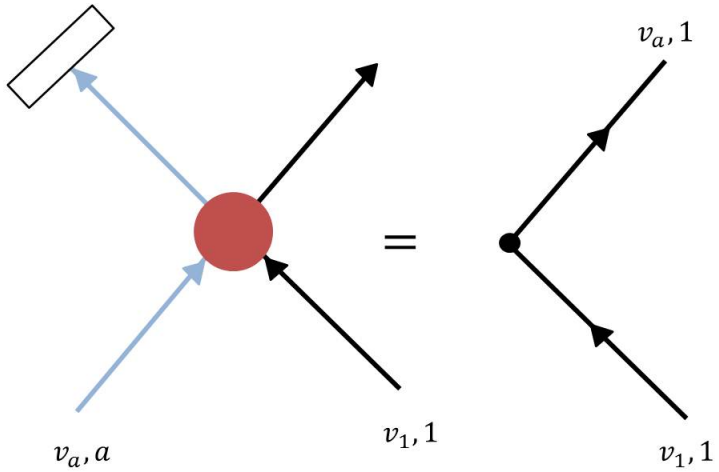


Figure 4-2: Two particle gadget to navigate the trajectory of a single particle. In this setting the particles move on straight line, therefore, I use this gadget to change the particle's trajectory, that is, the particle moving towards left with velocity v_1, changes direction to right with velocity v_a, if the detector on the left detects label $|a\rangle$. If the velocities match, $v_a = v_1$, the overall action is a change of direction. The success probability depends on v_1 and v_a.

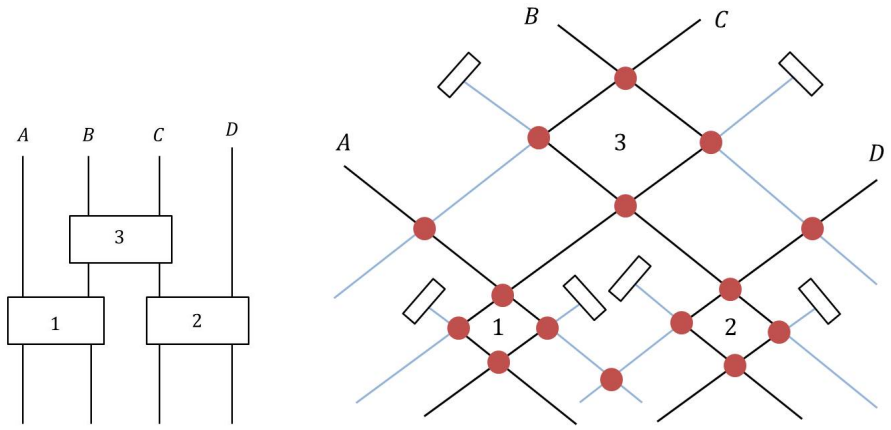
post selection. Moreover, in my approach the choice of the sequence of post-selections is made non-adaptively. I therefore use polynomial size three particle gadgets with planar Yang-Baxter circuits combined with post-selection which can simulate an arbitrary X rotation with arbitrary accuracy.

4.3 3-particle Gadgets with Non-demolition Measurements

Here I give a version of a three particle gadget with fixed velocities v_1, v_2, v_3, can in turn generate an arbitrary X rotation on two labels. Like before, let the rapidities $z_1 = v_1 - v_2$ and $z_2 = v_2 - v_3$, and consider a Yang-Baxter circuit with permutation signature (13), i.e., the permutation which maps $(1,2,3) \to (3,2,1)$:

$$C(v_1, v_2, v_3) = R(z_2, 1).R(z_1 + z_2, 2).R(z_1, 1) =: C(z_1, z_2)$$

The corresponding unitary operation amounts to:



(a) (b)

Figure 4-3: (a) A combination of X operators in a circuit. The circuit consists of three gates, 1, 2, and 3, and in the end we measure the wires A, B, C, and D, in the label basis. (b) An architecture of quantum ball permuting circuit based on particle scattering and intermediate particle detections to simulate quantum ball permuting circuit of FIG. 4. The circuit consists of 6 ancilla particles which mediate the computation and are detected intermediately with detectors. The labels 1, 2, and 3 demonstrate the simulation of gates 1, 2, and 3, of FIG. 4, respectively. In the end we measure the particle locations A, B, C, and D. The overall circuit operates successfully only if the detectors measure the the initial label of ancilla particles. That is conditioned on all ancilla particles succeed in passing through all of the intermediate interactions and bouncing off the last interaction, the scattering process succeeds in its simulation.

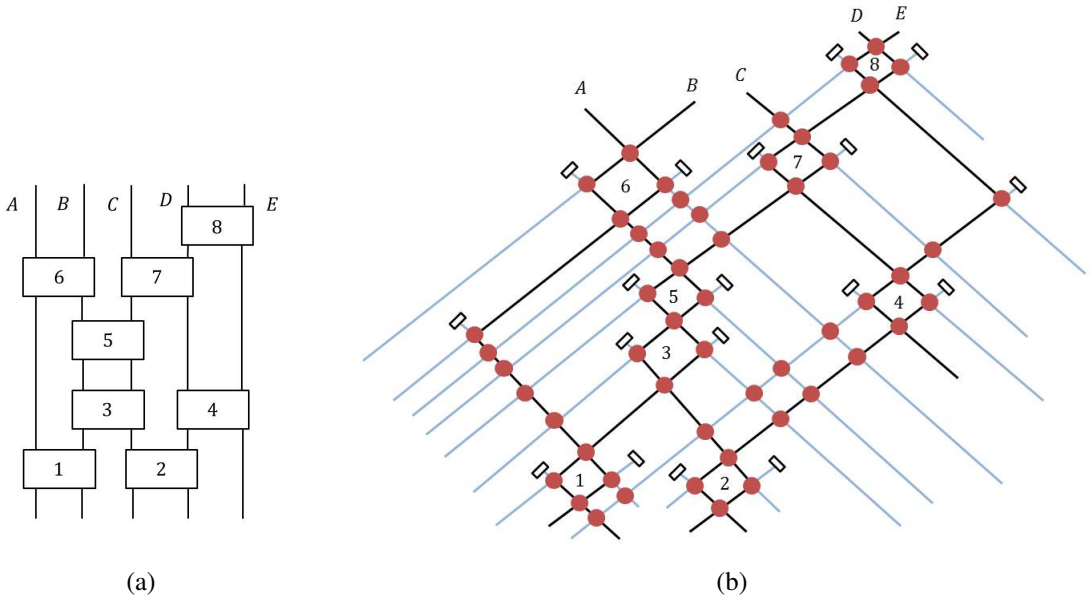


Figure 4-4: (a) Another example of a quantum circuit with X gates, 1, 2, ..., 8, on five labels. In the end we measure the wires A, B, C, D and E, in the particle label basis. (b) Programming particle scattering with intermediate measurements to simulate the X quantum ball permuting circuit of FIG. 6. The labels $1, 2, \ldots, 8$ correspond to the simulation of gates $1, 2, \ldots, 8$ in FIG. 6., respectively. Notice that in this example, the ancilla particles can experience many intermediate interactions. This example demonstrates that the overall process succeeds in successful simulation, only with small probability, and in general simulations, the probability of success can be exponentially small in the number of particles being used. Therefore, post-selecting on the outcome of the measurements, one can successfully simulate any X ball permuting quantum circuit. In the end the experimenter will measure the particle locations A, B, C, D and E, corresponding to wires A, B, C, D and E, of FIG. 6., respectively. A drawback of this scheme of programming is that, it is hard to program the velocities as we proceed to higher layers of the quantum circuit, and we might need to use particles with higher and higher velocity, as we proceed to the top of the circuit.

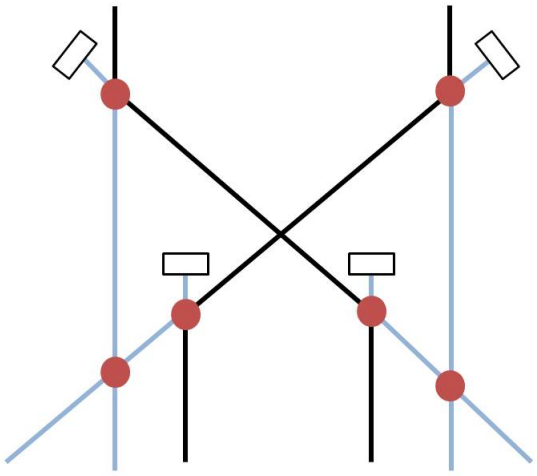
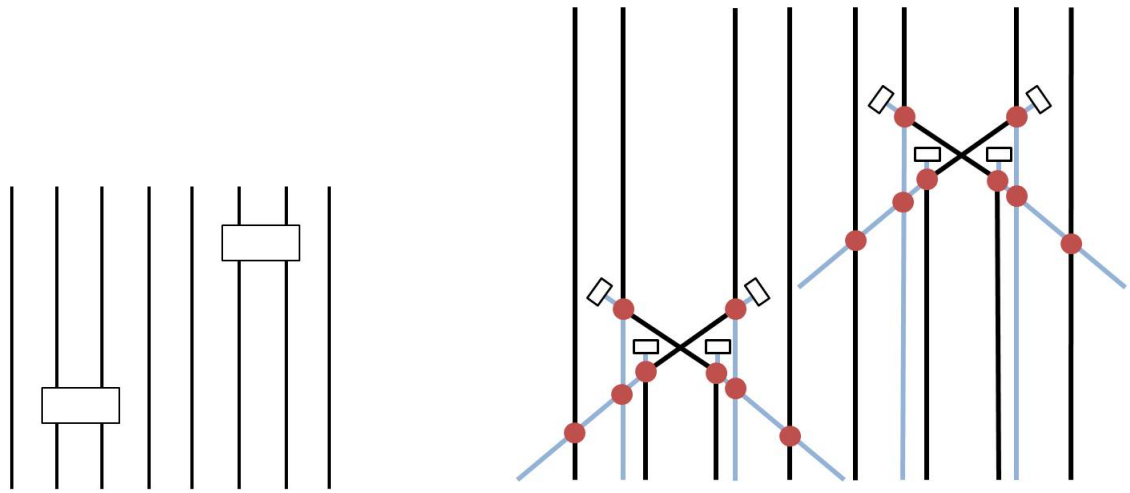


Figure 4-5: Four particle gadgets for stationary programming of particle scattering with detectors and intermediate particle collisions. The overall gadget simulates the two label permutation of FIG. 1. The objective is to impose superpositions on black particles which are stationary, in the sense that they do not move. Initially two black particles are stationary in the beginning, and we put two more stationary ancilla particles next to them. Then we shoot two ancilla particles from left and right and measure and post-select on them being bounced off the black particles. Then the two black particles collide with the two stationary ancilla particles and we measure and post-select on the ancilla particles being bounced off in the end. In this scheme it is easier to program the particle scatterings, and it has the advantage of inducing arbitrary permutation amplitudes on any two labels.



(a) (b)

Figure 4-6: (a) Stationary programming of particle scattering. We have used gadgets of FIG. 7. for this purpose. The overall scattering with intermediate post-selections simulates the X ball permuting circuit of FIG. 8. (b) A three particle gadget with RQBALL_{adj} quantum gates to simulate arbitrary rotations on the left (red) and right (blue) wires. P_{ij} means post-selection on label i being measured in the location j. The z parameters are the rapidities. The construction is done in three steps. First we let three wires to interact with three intersections. Then we measure the middle wire and post-select on measuring label $|2\rangle$. Then in step 2, we let the two left wires to interact and post select on the left most wire being label 2. Then in step 3), we let the right most wires interact, and finally in step 4) the two left wires have an interaction and we post-select on measuring the label $|2\rangle$ on the middle wire. In this scheme of programming, the post-measured label is being used over and over.

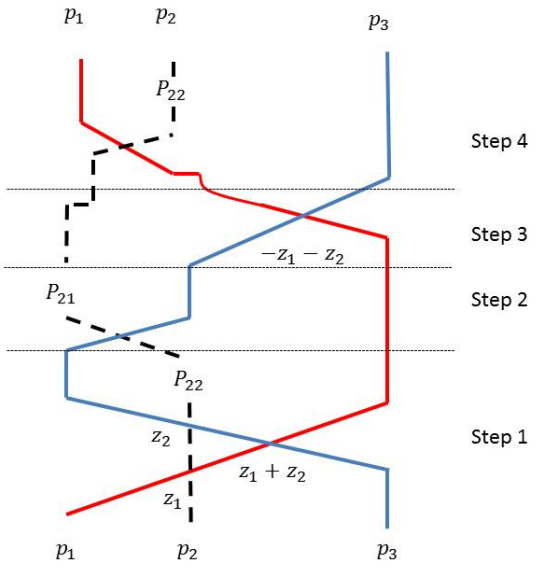


Figure 4-7: Nondeterministic three particle gadget to simulate an X operator with non-demolition measurements. The underlying model is the one where amplitudes are selected according to the Yang-Baxter equation. Measured labels are being used over and over in this computing scheme.

$$\frac{(1-z_1z_2)+i(z_1+z_2)(L_1+L_2)-(z_1+z_2)(z_1L_2L_1+z_2L_1L_2)-iz_1z_2(z_1+z_2)L_1L_2L_1}{\sqrt{(1+z_1^2)(1+z_2^2)(1+(z_1+z_2)^2)}}$$

There are $3\times 3=9$ choices for a post-selection. Let P_{ij} to be the corresponding post-selection of label i being located at the j'th location. Modulo a normalization factor, this is indeed the projection:

$$P_{ij}=\sum_{\sigma\in S_3:\sigma(j)=i}|\sigma\rangle\langle\sigma|.$$

The following is the list of the normalized out-come of post-selections. I will drop the overall phases throughout:

- $P_{11}C(z_1,z_2)|123\rangle=\dfrac{(1-z_1z_2)|123\rangle+i(z_1+z_2)|132\rangle}{\sqrt{(1-z_1z_2)^2+(z_1+z_2)^2}}$

- $P_{12}C(z_1,z_2)|123\rangle = \dfrac{|213\rangle + iz_2|312\rangle}{\sqrt{1+z_2^2}}$
- $P_{13}C(z_1,z_2)|123\rangle = \dfrac{|231\rangle + iz_2|321\rangle}{\sqrt{1+z_2^2}}$
- $P_{21}C(z_1,z_2)|123\rangle = \dfrac{|213\rangle + iz_1|231\rangle}{\sqrt{1+z_1^2}}$
- $P_{22}C(z_1,z_2)|123\rangle = \dfrac{(1-z_1z_2)|123\rangle - iz_1z_2(z_1+z_2)|321\rangle}{\sqrt{(1-z_1z_2)^2+(z_1z_2(z_1+z_2))^2}}$
- $P_{23}C(z_1,z_2)|123\rangle = \dfrac{|132\rangle + iz_2|312\rangle}{\sqrt{1+z_2^2}}$
- $P_{31}C(z_1,z_2)|123\rangle = \dfrac{|312\rangle + iz_1|321\rangle}{\sqrt{1+z_1^2}}$
- $P_{32}C(z_1,z_2)|123\rangle = \dfrac{|132\rangle + iz_1|231\rangle}{\sqrt{1+z_1^2}}$
- $P_{33}C(z_1,z_2)|123\rangle = \dfrac{(1-z_1z_2)|123\rangle + i(z_1+z_2)|213\rangle}{(1-z_1z_2)^2+(z_1+z_2)^2}$

After the first iteration, the configuration of the velocities changes from v_1, v_2, v_3 to v_3, v_2, v_1. Several of these post-selection are need to make sure about two things: first that the configuration of the momenta is back to v_1, v_2, v_3, and second that the middle label 2 is back to middle. The latter is because we want to use this label as an ancilla, and we want to make sure that it is not entangled to any other label. These gadgets are problematic and one needs more operations since, for instance, implementing the protocol $P_{11}C(z_1,z_2)$ first maps $|123\rangle$ to $(1-z_1z_2)|123\rangle + i(z_1+z_2)|132\rangle$ and if we implement it for the second time, because of the exchange of velocities the operation is forced to be $P_{11}C_3(-z_2,-z_1)$ which maps $|123\rangle$ back to itself.

In order to resolve the problem to recover a general rotation, we need to use a three particle gadget with the property that after each of its iterations, the configuration of the velocities is unchanged, and that the overall action is a rotation on two desired labels. I claim that the three particle gadget of Figure 5.1 does this task. The gadget consists of

two circuits, the first of which is a single P_{22} iteration of the discussed post-selection, and induces a rotation on the first and the third labels, and the second circuit makes sure that the velocities are arranged back to their primary locations. Let x and y be the labels of the first and the third locations, respectively. We add a third ancilla color, with a new label 2, and through each step of the protocol I will make sure that the ancilla label does not superimpose with the other labels.

I go through the steps of the protocol one by one. For simplicity, I drop the normalization factor for the intermediate steps and the states are normalized in the end. Let $z_1 = v_1 - v_2$ and $z_2 = v_2 - v_3$ and $z_3 = v_1 - v_3$ also let the label of the middle particle be 2:

- Step 1: $|x2y\rangle \to (1 - z_1.z_2)|x2y\rangle - iz_1.z_2z_3|y2x\rangle$. And the configuration of velocities in the end is: v_3, v_2, v_1.

- Step 2: let the first and second label locations interact, and after that, post select on the first particle to have the label 2. Then:

$$|123\rangle \to (1 - z_1.z_2)|2xy\rangle - iz_1.z_2z_3|2yx\rangle,$$

  and the configuration of velocities is v_2, v_3, v_1.

- Step 3: let the second and the third label locations interact, and that is going to be with rapidity $-z_1 - z_2$. Then:

$$|123\rangle \to (1 - z_1.z_2 - z_1z_2z_3^2)|2xy\rangle - iz_3|2yx\rangle,$$

  and the configuration of the velocities is v_2, v_1, v_3.

- Step 4: finally, let the first and the second label locations interact, and after that post-select on label 2 to be at the second location, which maps:

$$|123\rangle \to (1 - z_1.z_2 - z_1z_2(z_1 + z_2)^2)|x2y\rangle - i(z_1 + z_2)|y2x\rangle,$$

and the configuration of velocities is now back to v_1, v_2, v_3.

The overall action of the protocol is:

$$|123\rangle \rightarrow \cos(\phi_{z_1,z_2})|x2y\rangle + i\sin(\phi_{z_1,z_2})|y2x\rangle$$

With:

$$\phi_{z_1,z_2} = \tan^{-1}\left(\frac{-(z_1+z_2)}{1-z_1.z_2-z_1.z_2(z_1+z_2)^2}\right)$$

Now it is easy to check that the output state after t iterations of this gadgets is going to be:

$$|123\rangle \rightarrow \cos(t.\phi_{z_1,z_2})|x2y\rangle + i\sin(t.\phi_{z_1,z_2})|y2x\rangle.$$

The rapidity v_2 is a free parameter and can be set in a way that the angle ϕ_{z_1,z_2} is an irrational multiple of 2π, so using $O(1/\varepsilon)$ iterations, one can simulate any of the X rotations with accuracy ε.

Given these three particle gadgets, I wish to prove that any model with X operators can be efficiently approximated by a post-selected instance of planar Yang-Baxter R operators. I therefore use the discussed three particle gadgets to create arbitrary rotations on two labels, whenever we need them. Any circuit X operators can be represented by a normal form like Figure 5. 2. Where, each of the boxes is a unitary two particle gate, with some specific arbitrary amplitudes c, is. Consider any such circuit C of n particles and m gates, then we use a modified circuit of Figure 5. 3. In Figure 3, each gate of C is replaced by a three particle gadget. The ancilla labels are represented with dashed lines; each of them has a new label and an arbitrary velocity. The circles above the gates represent post-selection. The velocities (v_a), for each ancilla label a, should be selected in such a way that for all velocities v, v' of the original circuit, the rotation angles $(\phi v - v_a, v_a - v')$ are irrational multiples of 2π. In each gadget of the modified circuit, one should repeat the base gadget of Figure 5. 3. a sufficient number of times so that the parameters c, is for each gate of C is approximated with the desired accuracy. Given this background, I summarize this result in the following theorem:

Theorem 4.22. $\mathsf{XQBALL} \subseteq \mathsf{PostHQBALL}_{adj}$.

Proof. I prove the inclusion of XQBALL_{adj}, and since $\mathsf{XQBALL} \subseteq \mathsf{XQBALL}_{adj}$, the inclusion of XQBALL is implied. Given the description of any adjacent X ball permuting circuit C, with n labels and m gates, in polynomial time (in n and m), one can convert it to a normal form of Figure 3. This can be done layer by layer: in each layer, whenever two labels interact, a box with the desired amplitudes is placed, otherwise, we put boxes with amplitudes $c = 1, is = 0$, for each non-interacting adjacent labels. For each of the boxes with nonzero rotation angles, we add a three particle gadget, each with a new ancilla label and proper velocity such that the rotation angles are irrational multiples of 2π. Suppose that we want to approximate the output of C with accuracy ε, then we need the gadget to approximate its corresponding X operator with accuracy ε/m. If so, we will obtain a unitary which is ε-close to C. So each gadget will have size $O(m/\varepsilon)$, and will have $O(m/\varepsilon)$ number of intermediate post-selections. Therefore, the final circuit will have $O(n)$ labels, $O(m^2/\varepsilon)$ size and $O(m^2/\varepsilon)$ number of intermediate post-selections.

This proves an efficient approximation of XQBALL. However, I can also do better, and by adding m new ancilla labels, one per each gate of C, to tune the ancilla velocities in such a way that X operators are simulated exactly. Like the previous construction, I construct a circuit in HQBALL_{adj}, with the same gate configurations of C, with velocities $v_1, v_2, \ldots, v_n$. Then I replace each two particle gate with amplitudes c and is, with a three particle gadget with a new ancilla label a of velocity v_a. Therefore, the input momenta of the gadget are now v_i, v_a, v_j, and one needs to choose v_a in a way that the angle ϕ of the gadget satisfies $\cos(\phi) = c, \sin(\phi) = s$. Here, v_i and v_j are the proper choices of velocities according to the base Yang-Baxter circuit. The only issue is that the new particle a can superimposed to other particles whenever the line corresponding to v_a intersects another line. In order to fix this issue, I add a new two-particle gadget (see Figure 5. 4), which avoids such an interference. Suppose that at some point, the label in location $j+1$ interacts with the ancilla label a at location j then do a post-selection $\mathscr{P}_{a,j+1}$ to make sure that the particle a is located at $j+1$ after the interaction, and thereby, the overall action of the gadget is a mere swap, and rearrangement of velocities. Therefore, for each gate, I add a proper ancilla label, and using the discussed post-selected swap gadget, it gets passed through all

the intermediate lines until it is located at the bottom of its designed gadget. Then the gadget is implemented, and again the ancilla label is moves passed through the rest of the lines in the circuit, so that the ancilla label does not interact with any of the other labels anymore. Using this second approach, adding m ancilla labels to the Hilbert space, and doing $O(m)$ number of post-selections, C is simulated exactly. □

5 Lower-bounds

5.1 ZQBALL = BQP

In this part I use a simple encodings of qubits using labels $1,2,3\ldots,n$, and the Z operators to operate on them as single and two qubit gates. More specifically, I prove that using a sequence of Z operators, one can encode any element in the special orthogonal group. For an example of encoded universality see [12, 29]. I encode each qubit using two labels. Given two labels $a < b$ I define the encoded (logical) qubits as:

$$|0\rangle := |ab\rangle$$

and,

$$|1\rangle := i|ba\rangle.$$

Using simple $X(\theta,1)$ we can apply arbitrary rotation of the following form:

$$|0\rangle \to \cos\theta|0\rangle + \sin\theta|1\rangle$$

and,

$$|1\rangle \to \cos\theta|1\rangle - \sin\theta|0\rangle.$$

We are dealing with orthogonal matrices which are represented over the field or real numbers. Using the Z operators, we can discuss a controlled swap of the form:

$$S(i,j,k,l) := Z(\pi/2\delta_{i,j},k,l).$$

In simple words, $S(i,j,k,l)$ applies the swap $iL_(k,l)$, on the k and l'th labels if and only if the content of these label locations are i and j (j and i). We can also extend it to the following form:

$$S(\{(i_1,j_1)^{s_1},(i_2,j_2)^{s_2},\ldots,(i_t,j_t)^{s_t}\},k,l) := Z(\pi/2\delta_{i,j},k,l).$$

Where s_m can be a symbol $\star$ or nothing. Given $(i_m,j_m)^\star$ in the list means that the swap $(iL_{(k,l)})^\dagger = -iL_{(k,l)}$ is applied if the content of k and l are i_m and j_m. And given plain (i_m,j_m) in the list means $iL_{(k,l)}$ if the content of k and l are i_m and j_m.

Suppose that one encodes one qubit with labels $a<b$ and another one with $x<y$, we wish to find a unitary operator which applies a *controlled not* on the two qubits, that is the following map:

$$\begin{aligned}
|00\rangle &:= |a,b,x,y\rangle \to |a,b,x,y\rangle = |00\rangle \\
|01\rangle &:= i|a,b,y,x\rangle \to i|a,b,y,x\rangle = |01\rangle \\
|10\rangle &:= i|b,a,x,y\rangle \to -|b,a,y,x\rangle = |11\rangle \\
|10\rangle &:= -|b,a,y,x\rangle \to i|b,a,x,y\rangle = |10\rangle
\end{aligned}$$

It can be confirmed that the following operator can do this:

$$C := S(\{(a,x),(a,y)^\star\},1,3)S(\{(a,x),(a,y)\},2,3)S(\{(a,x),(a,y)\},1,2)$$

Given these two operators, one can simulate special orthogonal two-level systems, that is for each orthonormal $|\psi\rangle$ and $|\phi\rangle$ in the computational basis of n qubits we can apply an operator which acts as:

$$|\psi\rangle \to \cos\theta|\psi\rangle + \sin\theta|\phi\rangle$$

and,

$$|\phi\rangle \to \cos\theta|\phi\rangle - \sin\theta|\psi\rangle$$

5.2 Arbitrary Initial States

As mentioned in theorem 4.6, the columns of a ball permuting operator as a unitary matrix are all permutations of each other, and as a result of this constraint, I believe that the model starting with $|123\ldots n\rangle$ initial state is strictly weaker than the standard BQP model of computation. Moreover, one can observe the following property:

Lemma 4.23. If C is any composition of X ball permuting operators over $\mathbb{C}S_n$, then $C|123\ldots n\rangle = |123\ldots n\rangle$ if and only if $C = I$.

Proof. One direction is clear, that is if $C = I$ then $C|123\ldots n\rangle = |123\ldots n\rangle$. In order to see the other direction, suppose that $C|123\ldots n\rangle = |123\ldots n\rangle$, then act $R(\sigma)$ for all $\sigma \in S_n$ to the both sides to obtain $R(\sigma)C|123\ldots n\rangle = R(\sigma)|123\ldots n\rangle$. Since any ball permuting circuit commutes with a right (relabeling) action, we get $C|\sigma\rangle = |\sigma\rangle, \forall\sigma \in S_n$, which readily implies $C = I$. □

The lemma is another way of phrasing theorem **??**, and states that the group of ball permuting operators that stabilize $|123\ldots n\rangle$ is trivial. Also, one can extend this to all states like $|\sigma\rangle$ for $\sigma \in S_n$, and indeed all states that are reachable by an X ball permuting circuit from $|123\ldots n\rangle$. This suggests that the set of ball permuting gates is contained in a subgroup $SU(n!)$ as manifold of lower dimension. However, although this does not rule out encoded universality, because of the following corollary there is some evidence, supporting that even encoded BQP universality and therefore BQP universality is impossible for ball permuting circuits in this case:

Corollary 4.24. Let $|0_L\rangle = C_0|123\ldots n\rangle$ and $|1_L\rangle = C_1|123\ldots n\rangle$, with C_0 and C_1 being ball permuting circuits, be any logical encoding of a qubit. Then for any $N \geq 1$ and any string $x \in \{0,1\}^N$, a ball permuting unitary U is a stabilizer of the encoded $|x\rangle$, if and only if $U = I$.

Proof. Again, one direction of the proof is clear, that is if $U = I$, then $U|x\rangle = |x\rangle$. Now suppose that $U|x\rangle = |x\rangle$. Then $UC_{x_1} \otimes C_{x_2} \otimes \ldots \otimes C_{x_N}|12,3,\ldots,nN\rangle = C_{x_1} \otimes C_{x_2} \otimes \ldots \otimes C_{x_N}|12,3,\ldots,nN\rangle$. Since C_{x_j} are unitary ball permuting circuits, they have inverses, and $G_x := C_{x_1} \otimes C_{x_2} \otimes \ldots C_{x_N}$ is also a ball permuting gate and has an inverse G_x^{-1} which is also a ball permuting circuit. Therefore, $G_x^{-1}UG_x|123\ldots nN\rangle = |123\ldots nN\rangle$. From lemma 4.24, $G_x^{-1}UG_x = I$ which implies $U = I$. □

In the proof, I used two facts: first that C_0 and C_1 have inverses, and that they commute with the relabeling R operators. Indeed, the lemma applies to non-unitary C_0 and C_1, as long as they have the commuting and the inverse properties. I finally conclude the following general non-universality criterion:

Corollary 4.25. The result of corollary 4.24 remains true if C_0 and C_1 have inverses and commute with the relabeling operators.

While computing with the $|123\ldots n\rangle$ initial state, results in a presumably week model, one can use other initial states to break the conditions of lemma 4.24. For example, if one allows the initial state $|\psi\rangle = \frac{1}{n!}\sum_{\sigma\in S_n}|\sigma\rangle$ then the application of any operator of the form $X(\theta_1,\cdot)X(\theta_2,\cdot)\ldots X(\theta_p,\cdot)$ results in the state $\exp(i(\theta_1+\theta_2+\ldots+\theta_p))|\psi\rangle$, so as long as the angles sum up to zero the operator stabilizes $|\psi\rangle$. Indeed, the projection $\frac{1}{n!}\sum_{\sigma\in S_n}R(\sigma)$ maps any state in $\mathbb{C}S_n$ to a state proportional to $|\psi\rangle$.

In this section I provide evidence for encoded universality of the ball permuting model, in the case where initial states other than $|123\ldots n\rangle$ are allowed. This requires three considerations: first, we need to find a subspace $V \subseteq \mathscr{H}$, that is invariant under ball permuting operators, and that also scales exponentially in n in dimension. Secondly, we need to find a way of composing the X operators to act densely in $SU(V)$. Thirdly, we need to find a way to sample from the output states in V, in the color basis, to extract non-trivial information about these states. In order to achieve the second goal, I find a reduction from a model that is already known to be BQP universal. See section .

Theory of decoherence free subspaces and the BQP universality of the exchange interactions

The theory of decoherence free subspaces was originally motivated by the following problem [32]. Let $\mathscr{H}$ be a Hilbert space, and let N be the set of Hamiltonians, as the unwanted noise interactions. The objective is to find a large enough subspace $V \subseteq \mathscr{H}$ that is unaffected by the noise operators. Such a subspace is called a decoherencce free subspace. It is tempting to find a set of local and feasible quantum Hamiltonians, E, which commute with N and affect the decoherence free subspace only. Then universal quantum computation is possible if E acts as a universal gate set on V.

Ideally, the Hilbert space is decomposable into two separate subsystems $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$, and the action of N affects $\mathscr{H}_2$ only, and acts trivially on $\mathscr{H}_1$. Then, any universal gate set acting on $\mathscr{H}_1$ can reliably do universal quantum computing. However, in general, N can mix all local degrees of freedom of the available subsystems at the same time. Thereby, instead of subsystems, one can think about subspaces which mimic the structure of decoupled subsystems. Intuitively, this can be interpreted as subspaces of a Hilbert space simulating decoupled subsystems.

In order to find such a decomposition, it is helpful to consider a larger structure, A, as the matrix algebra generated by operators of N, by matrix composition and scalar linear combinations. This is a vector space of matrices, with matrix multiplication as the vector on vector action. Then, under certain conditions, A is isomorphic to the decomposition of smaller irreducible matrix algebras:

$$A \cong \bigoplus_{\lambda=1}^{D} \bigoplus_{j=1}^{n_\lambda} M(d_\lambda) \cong \bigoplus_{\lambda} I(n_\lambda) \otimes M(d_\lambda).$$

Here λ enumerates the type of the matrix blocks. $M(d_\lambda)$ denotes the algebra of matrices with dimension d_λ, and $\bigoplus_{j=1}^{n_\lambda} M(d_\lambda)$ is the same algebra repeated for d_λ times, and n_λ is therefore the multiplicity of this block. This means that there is a change of basis, on which the element of A acts as the block diagonal structure $M_1 \times M_1 \times \ldots \times M_1 \times \ldots \times M_D \times M_D \times \ldots \times M_D$; each matrix M_j is repeated for n_j times in the product series. These basis states are indeed the desired subspaces, and the Hilbert space also decomposes accordingly:

$$\mathscr{H} = \bigoplus_{\lambda} n_\lambda X(d_\lambda) \cong \bigoplus_{\lambda} V(n_\lambda) \otimes X(d_\lambda).$$

Here $n_\lambda X_{d_\lambda}$ means n_λ isomorphic subspaces each with dimension d_λ, and therefore $\dim \mathscr{H} = \sum_\lambda n_\lambda d_\lambda$. Given these decompositions, the operators of each block λ in the decomposition of A acts non-trivially on $X(\lambda)$ only, and leaves the subspace $V(n_\lambda)$ unaffected. It remains to find operators that act only on the V species and leave the X parts unaffected. The most general such structure is the matrix algebra B which commutes with all of A. B has the unique decomposition according to:

$$B \cong \bigoplus_{\lambda} M(n_\lambda) \otimes I(d_\lambda).$$

Let E be a gate set in B. Then, universal quantum computation on a decoherence free subspace $V(n_\lambda)$ is translated to first zooming into a subspace $V(n_\lambda) \otimes |\psi\rangle$, for some $|\psi\rangle \in X(d_\lambda)$, and then denseness of E in $SU(V(n_\lambda))$, and finally zooming out from $V(n_\lambda)$, by sampling bits of information from the output of computation.

Most of the mathematical review is borrowed from [30] We are interested in two mathematical structures, the group algebra of the symmetric group $\mathbb{C}S_n$, and the unitary regular representation of the symmetric group. As it turns out, the two structures are closely related to each other, and also to the group generated by the ball permuting gates. Group algebra is an extension of a group to an algebra, by viewing the members of the group as linearly independent basis of a vector space over the field $\mathbb{C}$. Therefore, in addition to the group action an action of $\mathbb{C}$ on S_n is needed, by the map $(\alpha, \sigma) \mapsto \alpha S_n$, and also addition of vectors in the usual sense. Therefore, a group algebra consists of all elements that can ever be generated by vector on vector composition and linear combination of vectors over $\mathbb{C}$. Any element of $\mathbb{C}S_n$ can be uniquely written as $\sum_{\sigma \in S_n} \alpha_\sigma \sigma$, with $\mathbb{C}$ coefficients α_σ. If we add a conjugation convolution † with maps $\sigma^\dagger = \sigma^{-1}$, and $\alpha^\dagger = \alpha^\star$, then for any element $v \in \mathbb{C}S_n$, $v^\dagger v = 0$, if and only if, $v = 0$. In order to see this, let $v = \sum_{\sigma \in S_n} \alpha_\sigma \sigma$. Then, $v^\dagger v = \sum_\sigma |\alpha_\sigma|^2 e + \ldots = 0$. A zero on the right hand side implies zeroth of all the vector components, including the component along e, which implies $\alpha_\sigma = 0$ for all $\sigma \in S_n$, and therefore $v = 0$. Let e be the identity element of S_n, consider an element $p \in \mathbb{C}S_n$ to

be a projector if it has the property $p^2 = p$. Two projectors p and q are called orthogonal if $p.q = 0$. Then $(e-p)^2 = e-p$ is also a projector, and also $p(e-p) = 0$ are orthogonal projectors. 0 is trivially a projector. Therefore, the group algebra decomposes as:

$$\mathbb{C}S_n = \mathbb{C}S_n e = \mathbb{C}S_n(e-p) + p = \mathbb{C}S_n(e-p) \oplus \mathbb{C}S_n p.$$

A projector is called minimal if it cannot be written as the sum of any two others projectors other than 0 and itself. Let p^μ be a list of minimal projectors summing $\sum_\mu p^\mu = e$, then the decomposition of the group algebra into minimal parts is according to:

$$\mathbb{C}S_n = \bigoplus_\mu \mathbb{C}S_n p^\mu.$$

p^μ are known as Young symmetrizers, and I am going to mention them later.

A (finite) representation ρ of a group G is a homomorphism from G to the group of isomorphisms of a linear space : $G \to GL(V,\mathbb{C})$, for some vector space V. Let g be any element of G, with its inverse g^{-1}, and e and 1 as the identity elements of G and $GL(V,\mathbb{C})$, respectively. Given the definition, $\rho(g^{-1}) = \rho(g)^{-1}$, and $\rho(e) = 1$ are immediate. One can observe that $\rho : G \to \{I \in GL(V,\mathbb{C})\}$, is immediately a representation, and is called the trivial representation of V. A dual representation of G is a homomorphism from G into the group of linear maps : $V \to \mathbb{C}$. As I discussed before, this is called the dual space $V^\star$, and V is viewed as the space of column vectors, then its dual space is a row space. For any vector spaces V and W, the two can be combined into a larger linear structure, $V \otimes W^\star$, as the set of linear maps from W to V. Let M_1 and M_2 be two elements of $GL(V,\mathbb{C})$ and $GL(W,\mathbb{C})$, respectively. Then, viewing $V \otimes W^\star$ as a vector space, the object (M_1, M_2) acts on $x \in V \otimes W^\star$ with $M_1 x M_2^{-1}$. Then, if M_1 and M_2 are two representations of G on V and W, then (M_1, M_2) is a representation of G on $V \otimes W^\star$, as a vector space. Notice that the inverse on M_2 is needed in order to have (M_1, M_2) act as a homomorphism. The dual representation M of V is then the representation on $\mathbb{C} \otimes V^\star$, when $M_2 = M$, and M_1 is the one dimensional trivial representation. This is just saying that the dual representation $M^\star$ of M on $V^\star$, maps $\langle\psi|$ to $\langle\psi|M(g^{-1})$, if we view the dual space as the usual row space. If we define an inner product as the action of the dual of a vector on itself, then G, as a representation, sends

orthonormal basis to orthonormal basis. This suggests that every representation of a finite group is isomorphic to a unitary representation. That is, any non-unitary representation becomes unitary after a change of basis. Let M be a representation on V. Then, we say $W \subseteq V$ is called stable under M, if for any $x \in W$, $Mx \in W$. Then, M restricted to W is called a sub-representation. A representation M on V is called an irreducible representation (irrep), if it has no stable subspaces other than 0 and V. Two representations M_1 and M_2 on V_1 and V_2 are isomorphic if M_1 resembles M_2 after a suitable change of basis within V_1. Then, if V is reducible, it can be decomposed as $V_1 \oplus V_2 \oplus \ldots \oplus V_n$, for $n > 1$. Some of the sub-representations can be isomorphic, and the multiplicity of a sub-representation is the number of sub-representations isomorphic to it. Then, the isomorphic subspaces can be grouped together to $V \cong m_1V_1 \oplus m_2V_2 \oplus \ldots m_kV_k$. Then $\dim V = \sum_j m_j \dim V_j$. The structure of such decomposition is isomorphic to $\bigoplus_j V_j \otimes X_j$, where X_j is the multiplicity space of V_j and is a vector space of dimension m_j. Decomposition of a representation onto the irreducible ones is unique up to isomorphism and multiplicities and dimensionality of irreducible representations do not depend on the decomposition. Canonical ways to find a decomposition are also known.

The regular representation of S_n, also denoted by $\mathbb{C}S_n$, is the unitary representation of S_n onto the usual Hilbert space $\mathbb{C}S_n$ spanned by the orthonormal basis $\{|\sigma\rangle : \sigma \in S_n\}$. It is well known that for any regular representation, the dimension of each irrep is equal to the multiplicity of the irrep, and therefore $\mathbb{C}S_n$ decomposes into irreducible representations of the following form:

$$\mathbb{C}S_n \cong \bigoplus_{\lambda} V_\lambda \otimes X_\lambda,$$

with $\dim X_\lambda = \dim V_\lambda =: m_\lambda$, and indeed $\sum_\lambda m_\lambda^2 = n!$. Here X_λ is again the multiplicity space, and V_λ corresponds to each irrep. It is tempting to make a connection between the group algebra and regular representation of the symmetric group. As described earlier, S_n can act on the Hilbert space $\mathbb{C}S_n$ in two ways; the left and right, $L, R : S_n \to U(\mathbb{C}S_n)$, unitary regular representation, with the maps $L(\sigma)|\tau\rangle = |\sigma \circ \tau\rangle$ and $R(\sigma)|\tau\rangle = |\tau \circ \sigma^{-1}\rangle$. Also, similar left and right structure can be added to the group algebra. Clearly, L and R

representations commute, and it can be shown that the algebra generated by L is the entire commutant of the algebra generated by R. Putting everything together, inspired by the theory of decoherence free subspaces, and the defined structures, one can show that the left (A) and right (B) algebras and the Hilbert space $\mathbb{C}S_n$ decompose according to:

$$A \cong \bigoplus_{\lambda} M(m_\lambda) \otimes I(m_\lambda),$$

$$B \cong \bigoplus_{\lambda} I(m_\lambda) \otimes M(m_\lambda),$$

and,

$$\mathbb{C}S \cong \bigoplus_{\lambda} V(m_\lambda) \otimes X(m_\lambda).$$

This is indeed a nice and symmetric structure. Indeed each irrep V_λ is an invariant subspace of the X operators, and it cannot be reduced further. It remains to demonstrate the structure of the irreps λ, and to study the action of X operators on these subspaces.

The irreducible representations of the symmetric group S_n are marked by the partitions of n. Remember that a partition of n is a sequence of non-ascending positive numbers $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \ldots \lambda_k$ summing to n, i.e., $\sum_j \lambda_j = n$. The number of partitions of n grows like $\exp\Theta(\sqrt{n})$. Each as described earlier each partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ is related to a diagram, called the Young diagram, which consists of k horizontal rows of square boxes $r_1, r_2, \ldots, r_k$. The Young diagram is then created by paving the left-most box of r_1 to the left-most box of r_2, and so on. For a Young diagram λ, the dual diagram $\tilde{\lambda}$, is another Young diagram, whose rows are the columns of λ. A Young tableau t^λ with the shape λ, is a way of bijective assigning of the numbers in $[n]$ to the boxes of λ. I will use t^λ and simply t with the shape λ interchangeably. A permutation $\pi \in S_n$ can act on a Young tableau t^λ by just replacing the content of each box to the its image under π, i.e., if a box contains j, after the action of π it will be replaced with $\pi(j)$. A tableau is called standard, if the numbers in each row and column are all in ascending orders. The number of standard tableau for each partition of shape λ is denoted by f^λ.

Let t be a tableau with shape λ. Define $P(t)$ and $Q(t) \subseteq S_n$ to be sets of permutations that leave each row and column invariant, respectively. Then the projectors of the $\mathbb{C}S_n$ group algebra are according to the Young symmetrizers, one for each standard tableau:

$$p^t = \frac{1}{f^\lambda} \sum_{\pi \in C(t)} \sum_{\sigma \in R(t)} sgn(\pi) \pi \circ \sigma.$$

These subspaces correspond to all of the irreducible invariant subspaces of S_n. The dimension for each of these subspaces is the number of standard tableaus of each partition, and it is computable using the hook lengths. The hook of each box in a partition of shape λ is consists of the box itself along with all boxes below and at the right of the box. The hook length of each box is the number of boxes contained in that hook, and the hook length h^λ of the shape λ is the multiplication of these numbers for each box. Then, the dimension of the irrep corresponding to λ is according to $f^\lambda = n!/h^\lambda$.

In order to talk about quantum operations subspaces with orthonormal basis are needed. It would be nice if we have a more lucid description of the basis, in a way that the action of X operators on these subspaces is clear. Moreover, I seek for an inductive structure for the orthonormal basis of the irreps that is adapted to the nested subgroups $S_1 \subset S_2 \subset \ldots \subset S_n$. By that I mean states that are marked with quantum numbers like $|j_1, j_2, j_3, \ldots, j_k\rangle$, such that while elements of S_n affect all the quantum numbers, for any $m_1 < n$, elements of S_n restricted to the first m_1 labels affects the first k_1 quantum numbers only, and act trivially on the rest of the labels. Also, for any $m_2 < m_1 < n$, the elements of S_n restricted to the first m_2 labels affect the first $j_2 < j_1 < k$ quantum numbers only, and so on.

Fortunately, such a bases exist, and are known as the subgroup adapted Young-Yamanouchi (YY) bases [30]. These bases are both intuitive and easy to describe: for any partition of shape λ, mark an orthonormal basis with the standard Young Tableaus of shape. Agree on a lexicographic ordering of the standard tableaus, and denote these basis corresponding to the partition λ, by a $\{|\lambda_j\rangle\}_{j=1}^{f^\lambda}$. Denote the action of a swap (i, j) on $|\lambda_l\rangle$ by $|(i, j).\lambda_l\rangle$, to be the basis of a tableau that is resulted by exchanging location of i and j in the boxes. Suppose that for such tableau t, the number j (i) is located at the r_j and c_j (r_i and c_i) row and column of t, respectively. Then, define the axial distance d_{ij} of the label i from label

j of on each tableau to be $(c_j - c_i) - (r_j - r_i)$. Or in other words, starting with the box containing i walk on the boxes to get to the box j. Whenever step up or right is taken add a -1, and whenever for a step down or left add a 1. Starting with the number 0, the resulting number in the end of the walk is the desired distance. Given this background, the action of $L_{(k,k+1)}$ on the state $|\lambda_i\rangle$, is according to:

$$L_{(k,k+1)}|\lambda_i\rangle = \frac{1}{d_{k+1,k}}|\lambda_i\rangle + \sqrt{1-\frac{1}{d_{k+1,k}^2}}|(k,k+1).\lambda_i\rangle$$

Three situations can occur: either k and $k+1$ are in the same column or row, or they are not. If they are in the same row, since the tableau is standard, k must come before $k+1$, then the axial distance is $d_{k+1,k} = 1$, and the action of $L_{(k,k+1)}$ is merely:

$$L_{(k,k+1)}|\lambda_i\rangle = |\lambda_i\rangle.$$

If the numbers are not in the same column, k must appear right at the top of $k+1$, and the action is:

$$L_{(k,k+1)}|\lambda_i\rangle = -|\lambda_i\rangle.$$

Finally, if neither of these happen, and the two labels are not in the same row or column, then the tableau is placed in the superposition of itself, and the tableau wherein k and $k+1$ are exchanged. Notice that if the tableau $|\lambda_i\rangle$ is standard the exchanged tableau $|\lambda_i\rangle$ is also standard. This can be verified by checking the columns and rows containing k and $k+1$. For example, in the row containing k, all the numbers at the left of k are less than k, then if we replace k with $k+1$, again all the numbers on the left of $k+1$ are still less than $k+1$. Similar tests for the different parts in the two rows and columns will verify $(k,k+1)\lambda_i$, as a standard tableau. The action of $L_{k,k+1}$ in this case is also an involution. This is obvious for the two cases where k and $k+1$ are in the same row or column. Also, in the third case if the action of $L_{(k,k+1)}$ maps $|\lambda\rangle$ to $\frac{1}{d}|\lambda\rangle + \sqrt{1-\frac{1}{d^2}}|t\circ\lambda\rangle$ then a second action maps $|t\circ\lambda\rangle$ to $\frac{-1}{d}|t\circ\lambda\rangle + \sqrt{1-\frac{1}{d^2}}|\lambda\rangle$, and therefore:

$$L^2_{(k,k+1)}|\lambda\rangle = \frac{1}{d}(\frac{1}{d}|\lambda\rangle + \sqrt{1-\frac{1}{d^2}}|t\circ\lambda\rangle) + \sqrt{1-\frac{1}{d^2}}(\frac{-1}{d}|t\circ\lambda\rangle + \sqrt{1-\frac{1}{d^2}}|\lambda\rangle) = |\lambda\rangle.$$

Given this description of the invariant subspaces, I wish to provide a partial classification of the image of the ball permuting gates on each of these irreps. The hope is to find denseness in $\prod_\lambda SU(V_\lambda)$, on each of the irreps V_λ, with an independent action on each block. In this setting, two blocks λ and μ are called dependent, if the action on λ is a function of the action on μ, i.e., the action on the joint block $V_\lambda \oplus V_\mu$ resembles $U \times f(U)$, for some function f. Then, independence is translated to decoupled actions like $I \times U$ and $U \times I$.

Throughout, the $\lambda \vdash n$, means that λ is a partition of n. We say $\mu \vdash n+1$ is constructible by $\lambda \vdash n$, if there is a way of adding a box to λ to get μ. We say a partition $\mu \vdash m$ is contained in $\lambda \vdash n$, for $m < n$, if there is a sequence of partitions $\mu_1 \vdash m+1$, $\mu_2 \vdash m+2, \ldots, \mu_{n-m-1} \vdash n-1$, such that μ_1 is constructible by μ, λ is constructible by μ_{n-m-1}, and finally for each $j \in [n-m-2]$, μ_{j+1} is constructible by μ_j. I also call μ a sub-partition of λ. A box in a partition λ is called removable, if by removing the box the resulting structure is still a partition. Also, define a box to be addable if by adding the box the resulting structure is a partition.

Theorem 4.26. *The Young-Yamanouchi bases for partitions of n are adapted to the chain of subgroups* $\{e\} = S_1 \subset S_2 \subset \ldots \subset S_n$.

Proof. Let $\lambda \vdash n$, and t be any standard tableau of shape λ. I construct some enumeration of states in the Young-Yamanouchi basis of λ which is adapted to the action of subgroups. For any $m < n$, since t is a standard tableau, the numbers $1,2,3,\ldots,m$, are all contained in a sub-partition $\mu \vdash m$ of λ. This must be true, since otherwise the locus of numbers $1,2,3,\ldots,m$ do not shape as a sub-partition of λ. Let ν be the smallest sub-partition of n that contains these numbers. Clearly, $|\nu| > m$. The pigeonhole principle implies that, there is a number $k > m$ contained somewhere in ν. The box containing k is not removable from ν, since otherwise you can just remove it to obtain a sub-partition smaller than ν that contains all of the numbers in $[m]$. Therefore, if k is in the bulk of ν, then both the row

and column containing k are not in the standard order. If k is on a vertical (horizontal) boundary, then the column (row) of the box containing k is not standard.

Let λ_k be the smallest sub-partition of λ that contains $[k]$. Then the enumeration of the basis is according to $|\lambda_1, \lambda_2, \ldots, \lambda_n\rangle$. Here, $\lambda_n = \lambda$, and λ_1 is a single box. From before, for any $j < n$, λ_{j+1} is constructible by λ_j. For $m < n$, let S_m be the subgroup of S_n, that stabilizes the numbers $m+1, m+2, \ldots, n$. For any $k \leq m$, $L_{(k,k+1)}$ just exchanges the content of boxes withing λ_m, and therefore leaves the quantum numbers $\lambda_{m+1}, \lambda_{m+2}, \ldots, \lambda_n$ invariant. Moreover, the box containing m is somewhere among the removable boxes of λ_m, since otherwise, as described in the last paragraph, the tableau λ_m is not standard. The box containing $m-1$ is either right above or on the left side of m, or it is also a removable box. In the first two cases, the action of $L_{(m-1,m)}$ is diagonal, and the quantum numbers are intact. In the third case, the only quantum numbers that are changed are λ_{m-1} and λ_m. □

Consider now the action of S_{n-1} on an element $|\lambda_1, \lambda_2, \ldots, \lambda_n = \lambda\rangle$. In any case λ is constructible by λ_{n-1}, and the construction is by adding an addable box to λ_{n-1}. In other words, λ_{n-1} can be any partition $\vdash n-1$, that is obtained by removing a removable box from λ. These observations, all together, lead to a neat tool:

Lemma 4.27. (Branching.) Under the action of S_{n-1}, $V_\lambda \cong \bigoplus_{\substack{\mu \vdash n-1 \\ \mu \subset \lambda}} V_\mu$.

Proof. Choose an orthonormal basis according to YY. Enumerate the removable boxes of λ by $1, 2, \ldots, p$. Clearly, in any standard tableau of λ, the box containing n is a removable one. Group the tableaus according to the location of n. Clearly, each subspace corresponds to a partition $\mu \vdash n-1 \subset \lambda$. Call these partitions $\mu_1, \mu_2, \ldots, \mu_p$, according to the enumeration of removable boxes. Also denote the space V_{μ_j} correspondingly. For any μ_j, any element of S_{n-1}, acted on V_{μ_j}, generates a vector within V_{μ_j}. In other words, these subspaces are stable under S_{n-1}. □

Partial classification of arbitrary initial states

In the following, I first prove denseness in some special class of Young tableaus. As described, the Hilbert space $\mathbb{C}S_n$ has the decomposition:

$$\mathbb{C}S_n \cong \bigoplus_{\lambda \vdash n} V_\lambda \otimes X_\lambda$$

In this section, I will work on the Lie algebra and the unitary Lie group generated by X operators, interchangeably. That is if the dimension of the Lie algebra as a vector space is large enough, then the Lie group is dense in some background group, and vice versa. As a first input, the element $X(\theta,k)$ can be written as:

$$X(\theta,k) = \exp(i\theta L_{(k,k+1)}).$$

Let G be the unitary group generated by these X operators. As described earlier, the space tangent to the identity element of G is a Lie algebra, g, which contains $L_{(k,k+1)}$ for all $k \in [n-1]$, and is close under linear combination over $\mathbb{R}$, and the Lie commutator $i[\cdot,\cdot]$. The objective is to show that for any $\lambda \vdash n$ with two rows or two columns, and any element U of $SU(V_\lambda)$, there is an element of G that is arbitrarily close to U.

The proof is presented inductively. First of all, for any n, the irreps V_n and $V_{1,1,1,\ldots,n}$ are one dimensional, and the action of $x \in G$ is to add an overall phase. However, observing the structure of YY basis for these irreps, the action of G on the joint blocks $V_n \oplus V_{(1,1,1,\ldots,1)}$ cannot be decoupled, and the projection of G onto these subspaces is diagonal, and moreover isomorphic to the group $e^{i\theta} \times e^{-i\theta} : \theta \in \mathbb{R}$. Intuitively, these are Bosonic and Fermionic subspaces, where an exchange $L_{(k,k+1)}$ of particles results in a $+1$ and -1 overall phase, respectively.

For $n = 2$, the only invariant subspaces are V_2 and $V_{(1,1)}$, and we know the structure of these irreps from the last paragraph:

$$\mathbb{C}S_2 \cong V_2 \oplus V_{(1,1)}, \qquad G \twoheadrightarrow e^{i\theta} \times e^{-i\theta} : \theta \in \mathbb{R}.$$

For $n = 3$, the decomposition is according to:

$$\mathbb{C}S_3 \cong V_3 \oplus V_{(1,1,1)} \oplus V_{(2,1)} \otimes X(2).$$

Here, $X(2)$ is a two dimensional multiplicity space. There are two standard $(2,1)$

tableaus and therefore $V_{(2,1)}$ is also two dimensional. Observing the YY basis the two generators $L_{(1,2)}$ and $L_{(2,3)}$ take the matrix forms:

$$L_{(1,2)} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and,

$$L_{(2,3)} = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}.$$

The basis of the matrix are marked with the two standard Young tableaus of shape $(2,1)$. The first basis corresponds to the numbering $(1,2;3)$ and the second one corresponds to $(1,3;2)$. Here, the rows are separated by semicolons. The following elements of the Lie algebra g generate $\mathfrak{su}(V_{(2,1)})$ and annihilate the two Bosonic and Fermionic subspaces:

$$\frac{1}{2\sqrt{3}}[L_{(1,2)},[L_{(1,2)},L_{(2,3)}]] = 0 \oplus 0 \oplus \sigma_x \otimes I,$$

$$\frac{i}{\sqrt{3}}[L_{(1,2)},L_{(2,3)}] = 0 \oplus 0 \oplus \sigma_y \otimes I,$$

and,

$$\frac{1}{6}[[L_{(1,2)},[L_{(1,2)},L_{(2,3)}]],[L_{(1,2)},L_{(2,3)}]] = 0 \oplus 0 \oplus \sigma_z \otimes I.$$

This implies the denseness of G in $1 \times 1 \times SU(V_{(2,1)})$. Therefore, we obtain a qubit coupled to the multiplicity space, placed in a superposition of the one dimensional Bosonic and Fermionic subspaces. So, projecting onto a subspace like $V_{(2,1)} \otimes |\psi\rangle$, for $|\psi\rangle \in X(2)$, we obtain a qubit.

I use this result as the seed of an induction. The upshot is to add boxes to $(2,1)$ one by one, in a way that the partitions remain with two rows or two columns. At each step, I use the branching rule to combine the blocks together to larger and larger special unitary groups. In the course of this process, I use two powerful tools, called the bridge lemma, and decoupling lemma:

Lemma 4.28. (Aharonov-Arad [6]) let A and B be two orthogonal subspaces, with *non-equal* dimensions, $\dim A < \dim B$:

- (Bridge) if there is some state $|\psi\rangle \in A$, and a (bridge) operator $V \in SU(A \oplus B)$, such that the projection of $V|\psi\rangle$ on B is nonzero, then the combination of $SU(A)$, $SU(B)$, and V is dense in $SU(A \oplus B)$.

- (Decoupling[3]) suppose for any elements $x \in SU(A)$ and $y \in SU(B)$, there are two corresponding sequences I_x and I_y in G, arbitrarily close to x and y, respectively, then the action of G on $A \oplus B$ is non-diagonal, i.e., $SU(A) \times SU(B) \subseteq G$.

See [7,8] for more similar results. Intuitively, what bridge lemma says is that given two subspaces, with one of them larger than the other, dense action each, along with a bridge between them, implies denseness on the combined subspace. That is a bridge glues them to a larger special group. The condition of different dimensions is a crucial requirement for the application of this lemma. The decoupling lemma, on the other hand, states that given dense action on two subspaces, as long as they have different dimensionality, there is way of acting on the two subspaces independently. Again, in this case non-equal dimensionality is important. For example, suppose that $\dim A = \dim B$, then the action $x \times x^\dagger : x \in SU(A)$, cannot be decoupled. In order to see this, just notice that after finite compositions, the general form of elements generated in this way is $(x_1 x_2 \ldots x_n) \times (x_n \ldots x_2 x_1)^\dagger$, and an identity action in the left part implies identity action in the right part of the Cartesian product.

Next, I show that the lemma along with the branching rule, force denseness on all irreps corresponding to partitions of two rows or two columns. I will take care of the case with two rows. The situation with two columns is similar. As a way of induction, suppose that, for any $m < n$, for any $\lambda = (\lambda_1 \geq \lambda_2) \vdash m$, the projection of G on λ is dense in $SU(V_\lambda)$. The objective is to prove denseness for any partition $\mu \vdash n$.

This is true for $(2,1)$, as showed above. For the sake of illustration, I prove this for $n = 4$. The partitions (4) is immediate, because this is one dimensional. Also, the partition $(2,2)$ is immediate, since the branching rule, under the action of S_3 is:

[3] I wrote an alternative formulation of Aharonov-Arad's original lemma that is consistent with the ball permuting group G.

$$V_{(2,2)} \cong V_{(2,1)},$$

That is the only removable box from $(2,2)$ is the last box, and in the YY basis for $(2,2)$, this last box can contain the symbol 4 only. So, the same operators of S_3 act densely on this subspace.

The situation with the partition $(3,1)$ is a little different. Analyzing the hook lengths, $V_{(3,1)}$ has dimension 3, and the branching rule involves the direct sum of partitions $(2,1)$ and (3):

$$V_{(3,1)} \cong V_{(2,1)} \oplus V_{(3)}.$$

Where, $V_{(2,1)}$ is two dimensional, and $V_{(3)}$ is one dimensional, and therefore, they have non-equal dimensions, and also their direct sum adds up to dimension 3. From, the analysis of S_3 we know that independent $SU(2)$, and $SU(1) = \{1\}$ is possible on these irreps. It suffices to find a bridge operator in $SU(V_{(2,1)} \oplus V_{(3)})$. In the first glance, the operator $L_{3,4} \in g$ sounds like a suitable choice. However, there is a problem with this: the restriction of $L_{3,4}$ on $V_{(3,1)}$ is not traceless, and therefore the image under exponentiation does not have unit determinant. Therefore, a wise choice for a bridge operator is $i[L_{(2,3)}, L_{(3,4)}]$. Looking at the actual matrices, restricted to the YY basis of $(3,1)$, one finds $i[L_{(2,3)}, L_{(3,4)}]$, as a suitable bridge, that is nice and traceless:

$$i \begin{pmatrix} 0 & \sqrt{2} & -\sqrt{\frac{2}{3}} \\ -\sqrt{2} & 0 & \sqrt{\frac{1}{3}} \\ \sqrt{\frac{2}{3}} & -\sqrt{\frac{1}{3}} & 0 \end{pmatrix}.$$

Here the matrix is written in the basis corresponding to the tableaus $(1,2,3;4), (1,2,4;3)$ and $(1,3,4;2)$. The bridging is between the $(1,2)$ and $(2,1)$ elements of the matrix. Thereby, the bridge lemma implies the desired denseness.

For general n, two situations can happen, either the partition under analysis is of the form $(\nu,\nu) = (n/2, n/2)$ (for even n of course), or not. In the first case, the situation is

similar to the partition $(2,2)$ of $n=4$. Thereby, restricted to S_{n-1}:

$$V_{(\nu,\nu)} \cong V_{(\nu,\nu-1)},$$

and based on the induction hypothesis the image of G is already dense in the subspace. In the second case, also two cases can happen: either the partition has the form $\mu=(\nu+1,\nu)$, with $2\nu+1=n$, or not. In the first case, the branching rule is according to:

$$V_{(\nu+1,\nu)} \cong V_{(\nu,\nu)} \oplus V_{(\nu+1,\nu-1)}$$

The space $V_{(\nu,\nu)}$ corresponds to all YY basis corresponding to tableaus, wherein the index n is located in the last box of the first row. Therefore, the index $n-1$ in all of the tableaus of (ν,ν) is located in the last box of the second column, because this is the only removable box available. For simplicity, let's call this space V_1. The YY bases of $V_{(\nu+1,n-1)}$ correspond to all the tableaus of $(\nu+1,\nu)$, where the index n is located in the last box of the second row. In this space, the location of the index $n-1$ is either in the last box in the first row or in the box right at the left of the last box in the second row. A coarser stratification of the states in $V_{(\nu+1,\nu-1)}$ is by grouping the YY basis according to the location of $n-1$. Let V_2 be the first one, and V_3 the second one. Therefore, YY bases of $V_{(\nu+1,\nu)}$ can be grouped in three ways, V_1,V_2,V_3, corresponding to all the ways that one can remove two boxes from the original $V_{(\nu+1,\nu)}$. Again, a neat candidate for a bridge is $L_{(n-1,n)}$. Taking a closer look at the operator $L_{(n-1,n)}$, it can be decomposed according to:

$$L_{(n-1,n)} = \sum_{|j\rangle\in V_3} |j\rangle\langle j| + \frac{1}{2} \sum_{\substack{k':k \\ |k\rangle\in V_1 \\ |k'\rangle\in V_2}} |k\rangle\langle k| - |k'\rangle\langle k'| + \sqrt{\frac{3}{2}} \sum_{\substack{k':k \\ |k\rangle\in V_1 \\ |k'\rangle\in V_2}} |k\rangle\langle k'| + |k'\rangle\langle k|$$

$|j\rangle$, $|k\rangle$, and $|k'\rangle$, of V_1, V_2, and V_3 are the corresponding orthonormal basis in the spaces. Notice that the space V_1 is isomorphic to V_2, and $k:k'$, refers to this isomorphism. Clearly, the restriction of $L_{(n-1,n)}$ to this block is not traceless, and indeed $tr_{V_{(\nu+1,\nu)}} = \dim V_3 = \dim V_{(\nu+1,\nu-2)}$.

Now, I use the decoupling lemma of Aharonov-Arad. $V_{(\nu+1,\nu)}$ and $V_{(\nu,\nu)}$ have different dimensionality, and also, due to the induction hypothesis the operators can act as the special unitary group on each of them. Thereby, there is a way to act as $x \oplus 0$ on the joint space $V_{(\nu,\nu)} \oplus V_{(\nu+1,\nu-1)}$, for some traceless element $x \in \mathfrak{su}(V_{(\nu,\nu)})$. Therefore, $x|j\rangle = 0$ and $x|k'\rangle$, for all $|j\rangle \in V_3$, $|k'\rangle \in V_2$. And denote $|xk\rangle := x|k\rangle$, for $|k\rangle \in V_1$. Taking the commutator $i[x, L_{(n-1,n)}]$:

$$i[x, L_{(n-1,n)}] = \frac{i}{2} \sum_{\substack{k':k \\ |k\rangle \in V_1 \\ |k'\rangle \in V_2}} |xk\rangle\langle k| - |k\rangle\langle xk| + i\sqrt{\frac{3}{2}} \sum_{\substack{k':k \\ |k\rangle \in V_1 \\ |k'\rangle \in V_2}} |xk\rangle\langle k'| - |k'\rangle\langle xk|.$$

Clearly, this operator is traceless, Hermitian, and also one can choose x in such a way that the bridging term in the second sum is nonzero.

Given the above proof for the case $V_{(\nu+1,\nu)}$, I will use a similar technique to take care of the situation $V_{(p,q)}$, where $p > q+1$, and $p+q = n$. Again, the branching rule is:

$$V_{(p,q)} = V_{(p,q-1)} \oplus V_{(p-1,q)}.$$

The space $V_{(p,q-1)}$ corresponds to all YY bases that correspond to the tableaus where the index n is located at the last box of the first row. In this space, the index $n-1$ is either located at the left side of the box containing n, or it is located in the last box of the second row. Call the space corresponding to the first (second) one V_1 (V_3). $V_{(p-1,q)}$ corresponds to all YY bases of tableaus with index n is located at the last box of the second row. In this space, the index $n-1$ is either located at the left side of the box containing n, or it is located in the last box of the first row. Call the first space V_2 and the second one V_4. Again, write the decomposition of $L_{(n-1,n)}$, accordingly:

$$L_{(n-1,n)} = \sum_{|j\rangle \in V_1} |j\rangle\langle j| + \sum_{|j\rangle \in V_2} |j\rangle\langle j| + \alpha(p,q) \sum_{\substack{k':k \\ |k\rangle \in V_3 \\ |k'\rangle \in V_4}} |k\rangle\langle k| - |k'\rangle\langle k'| + \beta(p,q) \sum_{\substack{k':k \\ |k\rangle \in V_3 \\ |k'\rangle \in V_4}} |k\rangle\langle k'| + |k'\rangle\langle k|$$

Here:

$$\alpha(p,q) = \frac{1}{p-q+1}$$

and,

$$\beta(p,q) = \sqrt{1 - \frac{1}{(p-q+1)^2}}.$$

Once again, V_2 is isomorphic to V_3, and $k : k'$ denotes the correspondence between elements of the two spaces. Once again, I use the decoupling lemma, which asserts the existence of elements like $X := x \oplus 0$, and $Y := 0 \oplus y$, on $V_{(p,q-1)} \oplus V_{(p-1,q)}$, for every $x \in \mathfrak{su}(V_{(p,q-1)})$ and $y \in \mathfrak{su}(V_{(p,q-1)})$. A bridge between V_3 and V_4 is needed, in such a way that the bridge annihilates both V_1 and V_2. A candidate for a bridge is $[Y,[X,L_{(n-1,n)}]]$. However, it can be easily shown that the element $i[X,L_{(n-1,n)}]$ will also work. The operator X annihilates everything in V_2 and V_4. Therefor, taking the commutator, the second sum is annihilated, and also, all the remaining terms are trace-less and one can find x in such a way that the bridge part is nonzero. All the above results also apply to the tableaus with two columns.

Programmability: reduction from exchange interactions

In the last section, I demonstrated denseness of G in special unitary groups over some specific invariant subspaces of $\mathbb{C}S_n$. However, this is a nonconstructive statement, and it is desirable to have an explicit description of BQP simulations in this model. Suppose that we can prepare an arbitrary initial state. For example, suppose that we can initialize the ball permuting model in one of the YY bases of an irrep $V_{(n,n)}$. We can view $V_{(n,n)}$ as a single giant qudit of exponential size. Analyzing the hook lengths, indeed one obtains the dimensionality:

$$\dim V_{(n,n)} = \frac{(2n)!}{(n+1)!n!} = 2^{\Omega(n)},$$

which is exponential, and can hold $\Omega(n)$ bits of quantum information in it. Even so, it is not clear how to efficiently program the states of $V_{(n,n)}$, using a polynomial time Turing

preprocessor. Moreover, in the way that I described the model, the final measurements can be done in the ball labels basis only, and given an output state in $V_{(n,n)}$, it is not obvious how one can sample from it to extract bits of information. Given this motivation, in this section I show how to use arbitrary initial states to obtain a programmable BQP universal model. This is done by demonstrating a reduction from the exchange interaction model of quantum computation which is already known to be BQP universal.

Here, I first review the exchange interaction model [12, 32, 33], and then describe how to do a reduction from the computation in this model to the ball permuting model of computing on arbitrary initial states. Next, I sketch the proof of universality for the exchange interaction model, which in turn results in BQP universality of ball permuting model on arbitrary initial states. Consider the Hilbert space $(\mathbb{C}^2)^{\otimes n} =: \mathbb{C}\{0,1\}^n$, with binary strings of length n, $\mathscr{X}_n := \{|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle : x_j \in \{0,1\}\}$, as the orthonormal computational basis. I am interested in the group generated by the unitary gates $T(\theta,i,j) = \exp(i\theta E_{(i,j)}) = \cos\theta I + i\sin\theta E_{(i,j)}$, where the operator, $E_{(i,j)}$, called the exchange operator, acts as:

$$E = \frac{1}{2}(I + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z)$$

on the i,j slots of the tensor product, and acts as identity on the other parts. More specifically, E is the map:

$$\begin{aligned} |00\ \rangle &\to |00\rangle, \\ |01\ \rangle &\to |10\rangle, \\ |10\ \rangle &\to |01\rangle, \\ |11\ \rangle &\to |11\rangle. \end{aligned}$$

The action of E_{ij} is very similar to the permuting operator $L_{(i,j)}$, except that E operates on bits rather than the arbitrary labels of $[n]$. These operators are also known as the Heisenberg couplings, related to the Heisenberg Hamiltonian for spin-spin interactions:

$$H(t) = \sum_{i<j\in[n]} a^x_{ij}(t)\sigma^i_x \otimes \sigma^j_x + a^y_{ij}(t)\sigma^i_y \otimes \sigma^j_y + a^z_{ij}(t)\sigma^i_z \otimes \sigma^j_z.$$

Here a^l_{ij} are time dependent real valued couplings. The Heisenberg Hamiltonian models pairwise interaction of spin $\frac{1}{2}$ particles, on a network. If one considers zero couplings for the nonadjacent locations with $|i-j|>1$, what the model describes is a chain of spins, with spin-spin interaction of the particles located on a line, or circle if the boundary condition of $a_{i,i+1} = a_{j,j+1}$ is considered for $i = j \mod n$. These are both one dimensional geometries. An isotropic Heisenberg Hamiltonian is the one for which the coefficients satisfy $a^x_{ij}(t) = a^y_{ij}(t) = a^z_{ij}(t) = a(t)_{ij}$, at all times. The isotropic Hamiltonian is expressible by the exchange operators according to:

$$H(t) = \sum_{i<j\in[n]} a(t)_{ij}(2E_{(i,j)} - 1).$$

If one further restricts the $a(t)_{ij}$ couplings to be piecewise constant in time, and that at most one nonzero coupling at a time, in the summation above, $H(t)$ imposes a general form of unitary evolution, according to:

$$U = T(\theta_m, i_m, j_m)\dots T(\theta_2, i_2, j_2)T(\theta_1, i_1, j_1). \tag{4.5}$$

Given $(\theta_1, i_1, j_1), (\theta_2, i_2, j_2), \dots, (\theta_m, i_m, j_m)$ as the description of U, and special initial states $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, I will demonstrate how to use X operators with arbitrary initial state to simulate U, and then sample from the output distribution of $U|\psi\rangle$. After that, I consult a previously known result, which asserts that exchange interactions are sufficient for universal quantum computing.

Definition 4.8. Define $\mathscr{X}^k_n := \{|x\rangle : x \in \{0,1\}^n, |x|_H = k\}$ to be the subset of $\mathscr{X}_n$, containing strings of Hamming distance $k \leq n$. Here, $|.|_H$ is the Hamming distance, which is the number of 1's in a string. Also, let $\mathbb{C}\mathscr{X}^k_n$ [4] be the corresponding Hilbert space spanned by these basis.

Theorem 4.29. *Given a description of U (in equation 4.5), and an initial state* $|\psi\rangle \in \mathbb{C}\mathscr{X}^k_n$,

[4] Usually $\mathbb{C}G$ refers to a group algebra, however, here I just use $\mathbb{C}\mathscr{X}^k_n$ just for the simplicity of notations.

there exists an initial $|\psi'\rangle \in \mathbb{C}S_n$, and a ball permuting circuit, with X operators, that can sample from the output of $U|\psi'\rangle$, exactly.

Proof. I show how to encode any state of $\mathbb{C}\mathscr{X}_n^k$ with states of $\mathbb{C}S_n$. Let $S_{k,n-k}$ be the subgroup of S_n according to the cycles $\{1,2,\ldots,k\}$ and $\{k+1,k+2,\ldots,n\}$, and denote $|\phi_0\rangle = \frac{1}{\sqrt{k!(n-k)!}} \sum_{\sigma \in S_{k,n-k}} R(\sigma)|123\ldots n\rangle$ be an encoding of the state $|1^k 0^{n-k}\rangle$. Here, 1^k means 1's repeated for k times. This is indeed a quantum state that is symmetric on each the labels of $\{1,2,\ldots,k\}$ and $\{k+1,k+2,\ldots,n\}$, separately. Any string of Hamming distance k can be obtained by permuting the string $0^k 1^{n-k}$. For any such string x let π_x be such a permutation, and encode $|x\rangle$ with $|\phi(x)\rangle := L_{\pi_x}|\phi_0\rangle$. Therefore, given any initial state $|\psi\rangle := \sum_{x \in \mathscr{X}_n^k} \alpha_x |x\rangle$, pick an initial state $|\psi'\rangle := \sum_{x \in \mathscr{X}_n^k} \alpha_x |\phi(x)\rangle$ in $\mathbb{C}S_n$. Now, given any unitary $U = T(\theta_m, i_m, j_m)\ldots T(\theta_2, i_2, j_2)T(\theta_1, i_1, j_1)$ with T operators, pick a corresponding ball permuting circuit $U' = X(\theta_m, i_m, j_m)\ldots X(\theta_2, i_2, j_2)X(\theta_1, i_1, j_1)$. It can be confirmed that for any $i < j \in [n]$ if $E_{(i,j)}|x\rangle = |x'\rangle$, then $E_{(i,j)}|\phi(x)\rangle = |\phi(x')\rangle$. From this, if $U|\psi\rangle = \sum_{x \in \mathscr{X}_n^k} \beta_x |x\rangle$, then $U'|\psi'\rangle = \sum_{x \in \mathscr{X}_n^k} \beta_x |\phi(x)\rangle$.

It remains to show that given access to the output of $U'|\psi'\rangle$, one can efficiently sample from $U|\psi\rangle$. Suppose that $U'|\psi'\rangle$ is measured in the end, and one obtains the permutation $\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n))$. Then, by outputting a string x by replacing all the labels of $\{1,2,\ldots,k\}$ in σ with ones and the other labels with zeros the reduction is complete. The probability of obtaining any string x with this protocol is exactly equal to $|\langle x|U|\psi\rangle|^2$. □

Indeed, in this simulation, the space is going to be projected onto a subspace of $\mathbb{C}S_n$ that is invariant under X operators. Moreover, this subspace is isomorphic to the strings of bits with certain Hamming distances. One can formally extend this idea to other similar subspaces. As before, let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_t)$ be a partition of n, and $S_\lambda \cong S_{\lambda_1} \times S_{\lambda_2} \times \ldots S_{\lambda_t}$, be the subgroup of S_n as the set of permutations with cycles $\{1,2,\ldots,\lambda_1\}, \{\lambda_1 + 1, \ldots, \lambda_2\}, \{\lambda_{t-1}+1, \ldots, \lambda_t\}$. Then it can be seen that $P(\lambda) := \frac{1}{\lambda!} \sum_{\sigma \in S_\lambda} R(\sigma)$ is a projection, i.e., it is Hermitian and also $P(\lambda)^2 = P(\lambda)$. $P(\lambda)$ is Hermitian, since $R(\cdot)$ is a Hermitian operator. S_λ is a group, and R is a homomorphism, therefore for any $\tau \in S_\lambda$, $R(\tau)\sum_{\sigma \in S_\lambda} R(\sigma) = \sum_{\sigma \in S_\lambda} R(\sigma)$, which is implied by the closure of $R(S_\lambda)$ as a group. Therefore:

$$P(\lambda)^2 = \frac{1}{\lambda!^2} \sum_{\tau \in S_\lambda} R(\tau) \sum_{\sigma \in S_\lambda} R(\sigma) = \frac{|S_\lambda|}{\lambda!^2} \sum_{\sigma \in S_\lambda} R(\sigma) = P(\lambda).$$

Indeed, looking at the Young symmetrizers, it can be confirmed that the subspace V_λ is contained in the space resulted under this projection, and the subspace is further reducible. I need to show that for any partition λ, $P(\lambda)\mathbb{C}S_n$ is a subspace that is invariant under the X operators. Let $W_\lambda := \{|\psi\rangle \in \mathbb{C}S_n : (I - P(\lambda))|\psi\rangle = 0\}$ be the subspace obtained by this projection, and W'_λ as its complement in $\mathbb{C}S_n$. Choose any $|\psi\rangle \in W_\lambda$, I claim that for any operator X, $X|\psi\rangle \in W_\lambda$. This is true, because the projection $P(\lambda)$ commutes with X, and $(I - P(\lambda))X|\psi\rangle = X(I - P(\lambda))|\psi\rangle = 0$. However, as it is going to be mentioned in a later section, these subspaces are further reducible. More specifically, in the proof of theorem 4.29, I used the partition $\lambda = (k, n-k)$, and constructed the subspace $W_\lambda := P(\lambda)\mathbb{C}S_n \subset \mathbb{C}S_n$ as the encoding of $\mathbb{C}\mathscr{X}_n^k$; in other words $W_{(k,n-k)} \cong \mathbb{C}\mathscr{X}_n^k$.

For any $k \in [n]$, $\mathbb{C}\mathscr{X}_n^k$ is an invariant subspace of the group, G_T, generated by T operators. This is because the exchange operators do not change the Hamming distance of the computational basis. So the decomposition $\mathbb{C}\{0,1\}^n \cong \bigoplus_k \mathbb{C}\mathscr{X}_n^k$ is immediate. Consider the standard total Z direction angular momentum operator:

$$J_Z := \frac{1}{2}(\sigma_z^1 + \sigma_z^2 + \ldots + \sigma_z^n).$$

Then $[J_Z, E_{(i,j)}] = 0$ for all i and j. Here, the superscript j in A^j for operator A means $I \otimes I \otimes \ldots \otimes \overset{j}{\overset{\downarrow}{A}} \otimes \ldots \otimes I$, the action of the operator on the j'th slot of the tensor product. J_Z indeed counts the Hamming distance of a string, and more precisely, for any $|\psi\rangle \in \mathbb{C}\mathscr{X}_n^k$, $J_Z|\psi\rangle = (\frac{n}{2} - k)|\psi\rangle$. Therefore, the eigenspace corresponding to each eigenvalue of J_Z is an invariant subspace of G_T. For each eigenvalue $n/2 - k$ the multiplicity of this space is $\binom{n}{k}$, the number of n bit strings of Hamming distance k. One can also define the X and Y direction total angular momentum operators in the same way:

$$J_X := \frac{1}{2}(\sigma_x^1 + \sigma_x^2 + \ldots + \sigma_x^n),$$

and,

$$J_Y := \frac{1}{2}(\sigma_y^1 + \sigma_y^2 + \ldots + \sigma_y^n).$$

Indeed, consulting the decoherence free subspaces theory of the exchange operators, the algebra generated by the operators J_X, J_Y and J_Z, is the unique commutant of the exchange operators, and vice versa. Indeed, for any positive algebra that is closed under the conjugation map, the commutant relation is an involution [30], i.e., the commutant of the commutant of any such algebra is the algebra itself.

The decomposition of $\mathbb{C}\{0,1\}^n$, of n spin $\frac{1}{2}$ particles, is well known, and can be characterized by total angular momentum, and the Z direction of the total angular momentum. The total angular momentum operator is:

$$J^2 = (\sum_{j\in[n]} \frac{1}{2}\sigma_x^j)^2 + (\sum_{j\in[n]} \frac{1}{2}\sigma_y^j)^2 + (\sum_{j\in[n]} \frac{1}{2}\sigma_z^j)^2.$$

Indeed, using a minimal calculation one can rewrite J^2 as:

$$J^2 = n(n-1/4) + \sum_{i<j\in[n]} E_{(i,j)},$$

and it can be confirmed that for all $k < l \in [n]$, $[E_{(k,l)}, J^2] = 0$. In other words, the exchange operators do not change the total and Z direction angular momentum of the a system of spin $1/2$ particles. The decomposition of $\mathbb{C}\{0,1\}^n$ can be written down according to these quantum numbers. Let $V(s) \subset \mathbb{C}\{0,1\}^n$, be the set of states $|\psi\rangle$ in $\mathbb{C}\{0,1\}^n$ such that $J^2|\psi\rangle = s(s+1/2)|\psi\rangle$, and $V(s,m) \subset V(s) \subset \mathbb{C}\{0,1\}^n$, as the subspace with states $|\phi\rangle$ such that $J_Z|\phi\rangle = m/2|\phi\rangle$. If n is even, $\mathbb{C}\{0,1\}^n$ decomposes according to:

$$\mathbb{C}\{0,1\}^n \cong V(0) \oplus V(1) \oplus \ldots \oplus V(n/2),$$

and each of these subspaces further decomposes to:

$$V(s) \cong V(s,-s) \oplus V(s,-s+1) \oplus \ldots \oplus V(s,s).$$

For odd n the only difference is in the decomposition $\mathbb{C}\{0,1\}^n \cong V(\frac{1}{2}) \oplus V(\frac{3}{2}) \oplus \ldots \oplus$

$V(n/2)$. From what is described in the context of decoherence free subspaces theory, the exchange interaction can affect the multiplicity space of each subspace $V(s,m)$. I am interested in the subspaces of the form $V(s,0)$ for even n, and $V(s,\pm\frac{1}{2})$, for odd n, which correspond to the decomposition of $\mathscr{X}_n^{n/2}$, and $\mathscr{X}_n^{(n\pm1)/2}$, based on the total angular momentum, respectively.

There is a neat connection between the multiplicity space of these subspaces, and the subgroup adapted YY bases. For $k \in [n]$, define the following series of operators:

$$J_k^2 = k(k-1/4) + \sum_{i<j\in[k]} E_{(i,j)}.$$

Clearly, $J_k^2 = J^2$. These are indeed the total angular momentum measured by just looking at the first k particles. Using a minimal calculation one gets $[J_k^2, J_l^2] = 0$ for all k,l. That is they are all commuting, and they can be mutually diagonalized. For $x_j \in [n]$, let $|x_1,x_2,\ldots,x_n\rangle$, be such basis with $J_j^2|x_1,x_2,\ldots,x_n\rangle = x_j(x_j+\frac{1}{2})|x_1,x_2,\ldots,x_n\rangle$. These are appropriate candidates as a basis for the multiplicity space of $V(s,0)(V(s,1/2)$ for odd n). Then, $x_n = s$. Analyzing these operators more carefully, it is realized that for each $l < n$, either $x_{l+1} = x_l + 1/2$ or $x_{l+1} = x_l - 1/2$. Intuitively, this is saying that adding a new spin $1/2$ particle $Q = \mathbb{C}^2$ to $V(x_j)$:

$$V(x_j) \otimes Q \cong V(x_j + \frac{1}{2}) \oplus V(x_j - \frac{1}{2}),$$

for $x_j > 0$, and otherwise:

$$V(0) \otimes Q \cong V(\frac{1}{2}),$$

This is similar to the branching rule of the symmetric group representation theory. The second form is directly related to the branching rule of $V_{(n,n)} \cong V_{(n,n-1)}$. For simplicity, here I consider the twice of the J operators instead, so that the branching rule takes the form:

$$V(x_j) \otimes Q \cong V(x_j + 1) \oplus V(x_j - 1),$$

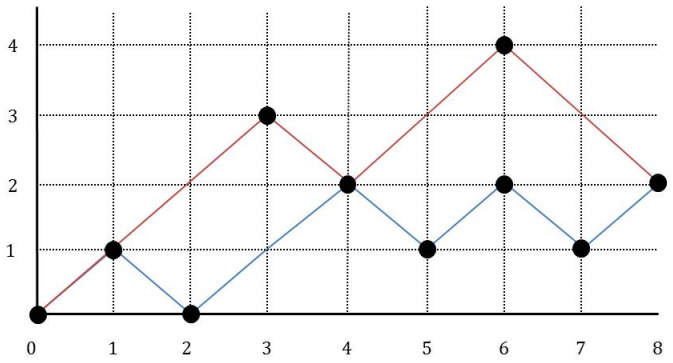


Figure 4-8: An example of a path model. The blue and red paths start out of $(0,0)$ and end up with the point $(8,2)$. YY basis corresponding to tableaus that two rows are closely related to the path model.

for $x_j > 0$ and,

$$V(0) \otimes Q \cong V(1),$$

otherwise. Applying this rule recursively, the path model is obtained. See Figure 4-8 for an example. A path model P_s is the set of paths between two points $(0,0)$ and (n,s) in a two dimensional discrete Cartesian plane $\{0,1,2,3,\ldots,n\}^2$, where no path is allowed to cross the $(x,0)$ line, and at each step the path will move either one step up or one step down. Path up/down from the point (x,y) is the connection from this point to $(x+1,y+1)/(x+1,y-1)$. See FIG for an example of a path model. Therefore, the Hilbert space $V(s)$ corresponds to the orthonormal basis labeled by the Paths to the point $(n,2s)$.

Indeed, I could agree on a path model for the YY basis of the tableaus with two rows. Let λ be the Young diagram of shape $\lambda = (n,m)$. The path model is constructed in the following way: map each tableau t to a symbol, $M_t = y_1 y_2 \ldots y_{n+m}$, where y_j is the row index of the box containing the number j. Starting at the point $(0,0)$ then the path corresponding to t is constructed by taking a step up, whenever a 1 is read in M, and a step down otherwise. Thereby, P_0 corresponds to (n,n), and P_{2n} corresponds to the partition $(2n)$.

Given this background, universal quantum computing is possible by encoding a qubit using three spin $1/2$ particles. Suppose that the following initial states are given in $\mathbb{C}\mathscr{X}_3^1$:

$$|0_L\rangle := \frac{|010\rangle - |100\rangle}{\sqrt{2}}$$

and,

$$|1_L\rangle := \frac{2|001\rangle - |010\rangle - |100\rangle}{\sqrt{6}},$$

as some logical encoding of a qubit using three quantum digits. I claim that there is a way to distinguish $|0_L\rangle$ from $|1_L\rangle$ with perfect soundness. These mark the multiplicity space of the space with half Z direction angular momentum and half total angular momentum. First, we should find a way to distinguish between these two states using measurement in the computational basis. Suppose that we have access to k copies of an unknown quantum state, and we have the promise that it is either $|0_L\rangle$ or $|1_L\rangle$, and we want to see which one is the case. The idea is to simply measure the third bit of each copy, and announce it to be 0_L if the results of the k measurements are all 0 bits. If the state has been $|0_L\rangle$, the probability of error in this decision is zero, because $|0_L\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \otimes |0\rangle$. Otherwise, we will make a wrong decision with probability at most $(1/3)^k$, which is exponentially small. This is because the probability of reading a 0 in the third bit of $|1_L\rangle$ is $1/3$.

Theorem 4.30. *There is a way of acting as encoded $SU(2)$ on the span of $\{|0_L\rangle, |1_L\rangle\}$, and also $SU(4)$ on the concatenation of two encoded qubits.*

Proof. (Sketch) according to the analysis of [24, 32], one can look at the Lie algebra of the exchange operators to find encoded $\mathfrak{su}(2)$ algebra on the encoded qubit. Also, we need to take enough commutations such that the action of the designed operators annihilates the two one dimensional spaces spanned by $|000\rangle$ and $|111\rangle$. The authors of [32] prove that there is a way to act as $SU(V(s,m))$ on each invariant subspace $V(s,m)$. Moreover, they prove that the action on two subspaces $V(s_1,m_1)$ and $V(s_2,m_2)$ can be decoupled, unless $s_1 = s_2$, and $m_2 = -m_1$, where the two subspaces are isomorphic. It is almost enough to prove that the state $|0_L\rangle \otimes |0_L\rangle$ is contained in non-isomorphic invariant subspaces. However, this is also true, since $|0_L\rangle \otimes |0_L\rangle$ is completely contained in subspaces with $m = 2$. □

See [13, 34, 54] for similar models with encoded universality. Therefore, this is a non-constructive proof for the existence of an encoded entangling quantum gate; CNOT for example. Indeed, the actual construction of a CNOT is given in [24] . Notice that for a decision problem, one can formulate quantum computation in such a way that only one qubit needs to be measured in the end, and this can be done by distinguishing $|0_L\rangle$ and $|1_L\rangle$ using measurement in the computational basis. The probability of success in distinguishing between the two bits can also be amplified by just repeating the computation for polynomial number of times, and taking the majority of votes. Also, taking the majority of votes can be done with encoded CNOTs and single qubits gates on a larger circuit, and without loss of generality we can assume that one single measurement on one single qubit is sufficient.

6 Evidence for the Hardness of Classical Simulation of the Scattering Quantum Computer

In this section, I combine some of the results from last sections with known facts in complexity theory to give substantial evidence that it is hard to sample from the output probability distribution of the ball scattering model when we allow intermediate particle detections and arbitrary initial states. The approach is to demonstrate that the existence of a feasible sampling scheme results in falsification of statements that are believed to be true. These are statements that have not been proved, but yet no counter examples are known to them. An example is the well-known P versus NP question. Most of the researchers in computer science believe that these two objects are not equal. However, a proof of equivalence or a separation does not exist yet, and it might be the case that this problem is an undecidable problem itself. Another example of this kind is the problem of deciding if the polynomial hierarchy is finite or infinite. Indeed, in this section I show that efficient sampling from the output distribution of the ball scattering problem directly implies finiteness of the polynomial hierarchy (PH). As described, the polynomial hierarchy is an extension of nondeterministic polynomial time, NP, to a tower of complexity classes with the form $\mathsf{NP}^{\mathsf{NP}^{\cdots^{\mathsf{NP}}}}$; more precisely PH is the union of Σ_{P}^{j} for $j \geq 1$, where $\Sigma_{\mathsf{P}}^{1} = \mathsf{P}$, $\Sigma_{\mathsf{P}}^{2} = \mathsf{NP}$, and

$\Sigma_{\mathsf{P}}^{j+1} = \Sigma_{\mathsf{P}}^{j\,\mathsf{NP}}$, for $j \geq 2$. Remember that A^B is the machine of class A with oracle access to B. It is widely believed that the polynomial hierarchy is infinite, and recently, it has been proved that relative to a random oracle PH is infinite.

The objective of this section is to demonstrate that it is hard to sample from the output distribution of the ball scattering model, unless the polynomial hierarchy collapses to its third level. Similar proof techniques already exist, for example see [4, 41]. In sections 4.1 and 4.2 of this chapter, I showed that one can use intermediate demolition measurements on the ball scattering problem of section 2 to come up with a sequence of nondeterministic gates that are able simulate quantum circuits of XQBALL. The gates are nondeterministic, in the sense that they will succeed in their simulation, only if certain measurement outcomes are obtained, and this can happen with exponentially small probability. Also, the proof still holds on arbitrary initial states. After that, in section 5.2, I proved that on arbitrary initial states, the model XQBALL is equal to the standard BQP. Moreover, I discussed that in order to simulate a standard quantum circuit model C of BQP in XQBALL, the form of the desired initial state depends on the number n of qubits in C only. I denote this initial state by $|\psi_n^\star\rangle$, or just simply by $|\psi^\star\rangle$. Putting these results together, we observe that the model of ball scattering with intermediate demolition post-selection is equal to BQP, if we allow arbitrary initial states. For the sake of clarity, I define PostXQBALL with the following definition to capture the discussed ingredients in the model of ball scattering:

Definition 4.9. Let PostHQBALL be the class of decision problems that are efficiently solvable using the following resources:

- Yang-Baxter ball collision circuits, similar to section 4.2,
- initial states of the form $|\psi^\star\rangle \otimes |c_1, c_2, \ldots, c_m\rangle$,
- post-selection on demolition intermediate measurement outcomes.

Here, $|\psi^\star\rangle$ is the discussed special inital, and $c_1, c_2, \ldots, c_m$ are distinct colors that are also distinct from color species of $|\psi^\star\rangle$. More precisely, this is the class of languages $L \subset \{0,1\}^\star$, for which there is a polynomial time Turing machine M that on any input $x \in \{0,1\}^\star$ outputs the description of a ball scattering setup like in section 4.2, and a polynomial

size set of ball colors $\tilde{c}$, along with a special output ball register c'_0, with the following properties:

- 1) for all $x \in \{0,1\}^\star$, $Pr[c'_1 = c_1, c'_2 = c_2, \ldots, c'_m = c_m] > 0$, where c'_l is the outcome of the l'th intermediate measurement. Denote this event by C.
- 2) if $x \in L$, $Pr[c'_0 \in \tilde{c}|C] \geq 2/3$. Here $c'_j \in \tilde{c}$ is the event where the color of the ball measured in location j, in the end of scattering, is among the colors of the set $\tilde{c}$.
- 3) if $x \notin L$, $Pr[c'_0 \in \tilde{c}|C] \leq 1/3$.

Condition 1 states that the probability of the event that the classical outcomes of the intermediate measurements match the guessed outcomes $c_1, c_2, c_3, \ldots, c_m$ is nonzero. Notice that as discussed in the section 4 of this chapter, this probability can be exponentially small, but since we are dealing with conditional probabilities, a nonzero probability is sufficient. Conditions 2 and 3 state that the probability of error is bounded. Here $\tilde{c}$ is a set of colors among the colors of $|\psi^\star\rangle$, which correspond to the accepting ball colors. The ball register c'_0, is a special location of a ball in the output of ball scattering; c'_0 can be viewed as an answer register.

A major observation is the following theorem, stating that although the ball scattering model might be strictly weaker than BQP, the post-selected version is equal to PostBQP, and to PP because of Aaronson's PostBQP = PP.

Theorem 4.31. PostHQBALL = PostBQP = PP.

Proof. PostBQP = PP is given by the result of Aaronson. Also, PostHQBALL $\subseteq$ PostBQP. In order to see this, observe that the BQP machine first prepares the initial state $|\psi^\star\rangle \otimes |c_1, c_2, \ldots, c_m\rangle$, encoded with binary strings. Then, whenever an intermediate measurement is done, it just leaves the state along and postpones the measurement to the end of computation. This might give rise to a non-planar quantum circuit, but it is fine, since we are working with BQP. The BQP measurements are done in a proper basis that encodes the ball color basis. For example, if we encode ball colors with binary representations, then it is sufficient to measure in binary basis and confirm if the digital representation of the

ball color (number) is correct. Notice that in the simulation, we are not going to use the balls that have already been measured intermediately again. All the swap gates are applied accordingly. Then in the end we post select on the desired demolition measurements and in the end we measure the encoded location of the j'th ball and confirm if it is among $\tilde{c}$. We can also use CNOT gates to shrink the number of post-selections down to one.

In order to see the more interesting direction PostHQBALL $\supseteq$ PostBQP, just we follow the post-selected universality result of section 4.2 and 5.2 of this chapter, to simulate any computation in BQP. Then notice that any PostBQP computation can be deformed in a way that one only needs to post-select on one qubit, and also measure one qubit in the end. PostHQBALL uses this deformed PostBQP protocol, instead, and uses one of its demolition measurements in the end of computation to simulate post selection of the actual PostBQP circuit. □

In section 4.2.2, I defined HQBALL as a variation of the ball permuting model with planar Yang-Baxter circuits. Later, in section 4.4.2 , I demonstrated how to use intermediate non-demolition measurements to come up with nondeterministic three particle gadgets that simulate the two particle gates of XQBALL. Thereby, I define the formal model with post-selection:

Definition 4.10. Let PostHQBALL* to be the class of decision problems that are efficiently solvable using initial states of the form $|\psi^\star\rangle$, and non-adaptive planar Yang-Baxter circuits with post-selection on non-demolition intermediate measurements. The details of the definition is similar to definition 4.9.

This model does not immediately have a corresponding physical example, but it is interesting that the same result of theorem 4.31 is applicable to it:

Theorem 4.32. PostHQBALL* = PostBQP = PP.

Proof. The proof of both directions is similar to the proof theorem 4.31, except that now in the direction PostBQP $\supseteq$ PostHQBALL*, the BQP simulation uses *CNOT* gates to postpone all intermediate measurements to the end. □

The equivalence of these quantum models and PP is already and interesting connection, however, we are two steps away from the major results, that is the connection to the collapse of polynomial hierarchy. In order to achieve this goal, I recapitulate amazing tools from complexity theory in the following theorem:

Theorem 4.33. *The following relationships are true for the complexity classes* $\mathsf{PP}, \mathsf{PostBPP}, \mathsf{NP}, \mathsf{PH}, \mathsf{PostBQP}$ *and* Σ_{P}^3*:*

- $\mathsf{PostBPP} \subseteq \mathsf{BPP}^{\mathsf{NP}} \subseteq \Sigma_{\mathsf{P}}^3 \subseteq \mathsf{PH}$ *[11].*
- $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$ *[11]*
- *(Toda [50])* $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$
- $\mathsf{PostBPP} \subseteq \mathsf{PostBQP}$
- *(Aaronson)* $\mathsf{PostBQP} = \mathsf{PP}$ *[2]*

A direct corollary to these containment relations is the following:

Corollary 4.34. $\mathsf{PostHQBALL} \subseteq \mathsf{PostBPP}$ implies the collapse of PH to the third level Σ_{P}^3.

Proof. Putting the relations in theorem 4.33, along with the result of theorem 4.31 together we obtain:

$$\mathsf{PostBPP} \subseteq \mathsf{BPP}^{\mathsf{NP}} \subseteq \Sigma_{\mathsf{P}}^3 \subseteq \mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\mathsf{PostBQP}} = \mathsf{P}^{\mathsf{PostHQBALL}}$$

If $\mathsf{PostHQBALL} \subseteq \mathsf{PostBPP}$, then $\mathsf{P}^{\mathsf{PostHQBALL}} \subseteq \mathsf{P}^{\mathsf{PostBPP}} \subseteq \mathsf{P}^{\Sigma_{\mathsf{P}}^3}$, and thereby $\mathsf{PH} \subseteq \Sigma_{\mathsf{P}}^3$, which results in the collapse of PH to the third level. □

Given this corollary, the existence of a randomized classical procedure to *exactly* sample from the output of the ball scattering problem, immediately results in the collapse of PH. However, we can even proceed further to come up with a somehow stronger result. Here, I borrow definitions from the notions of randomized simulation from computational complexity theory:

Definition 4.11. Let P be the output a computational (or physical) model, as a probability distribution on n variables $x := (x_1, x_2, \ldots, x_n)$, we say a randomized algorithm R simulates P within multiplicative constant error, if R produces a probability distribution $\tilde{P}$ on the variables, with the property that there is a constant number $\alpha > 1$, which for all x:

$$\frac{1}{\alpha} P(x) < \tilde{P}(x) < \alpha P(x).$$

The following theorem states that the existence of a randomized simulation of ball scattering with multiplicative error immediately results in PostHQBALL $\subseteq$ PostBPP:

Theorem 4.35. *The existence of a* BPP *algorithm to create a probability distribution with-ing multiplicative error to the actual distribution on $c_1, c_2, \ldots, c_m$ and c_0 of definition 4.9 implies* PostHQBALL $\subseteq$ PostBPP.

Proof. The proof is similar to the proof of theorem 2 in [17]. Suppose that there is a procedure which outputs the numbers $x_1, x_2, \ldots, x_m, y$ such that:

$$1/\alpha Pr[c'_0 = c_0; c'_1 = c_1, c'_2 = c_2, \ldots, c'_m = c_m] < Pr[y = c_0; x_1 = c_1, x_2 = c_2, \ldots, x_m = c_m] < \alpha Pr[c'_0 = c_0; c'_1 = c_1,$$

for every list of colors $c_1, c_2, \ldots, c_m$ and c_0. Notice that if this is true, it should also be true for all marginal probability distributions. Denote the vector $(c'_1, c'_2, \ldots, c'_m, c'_0)$ by $(\tilde{c'}, c'_0)$, and $(x_1, x_2, \ldots, x_m, y)$ by $(\tilde{x}, y)$. Then the conditional probabilities also satisfy:

$$1/\alpha^2 Pr[c'_0 = c_0 | \tilde{c'} = \tilde{c}] < Pr[y = c_0 | \tilde{x} = \tilde{c}] < \alpha^2 Pr[c'_0 = c_0 | \tilde{c'} = \tilde{c}].$$

Now let L be any language in PostHQBALL. Then if $x \in L$, $Pr[d' = d|C] \geq 2/3$ and otherwise $\leq 1/3$. Suppose that $x \in L$, then in order for $Pr[y = d|\tilde{x} = \tilde{c}] > 1/2$, it is required that:

$$1/2 < 1/\alpha^2 (2/3)$$

which means if $1 < \alpha < \sqrt{4/3} - O(1)$, then the PostBPP algorithm recognizes x with

bounded probability of error. The probability of success can be increased by using the majority of votes' technique.

□

Putting it all together, I finally mention the result of this section in the following corollary:

Corollary 4.36. There exists no polynomial time randomized algorithm to simulate ball scattering models of section 4.4.2 and 4.4.3 within multiplicative constant error, unless PH collapses to its third level.

7 Open Problems and Further Directions

- The actual model of particle scattering corresponds to a unitary scattering matrix with at most n degrees of freedom. Therefore, as a manifold, the dimension of the unitary group that is generated by the Yang-Baxter scatterings have small dimension. Although I proved that with intermediate measurements the structure of the group will expand to exponential dimension, it is still unknown if classical simulation is allowed for the problem without intermediate measurements. There examples [31] of models that generate discrete number of unitary operators, and still they are believed to be able to solve problems that are hard for classical computation. Moreover, the structure of the described manifold, as a mathematical object is interesting.

- No physical example for the model ZQBALL is mentioned. Since the model is proved to be equivalent to BQP it is interesting to see if there are actual physical models that capture the dynamics of ZQBALL. This might be a model for molecular dynamics with exchange interactions for which the coupling terms depend on the type of molecules being exchanged.

- While we hope to find a lower bound of $\prod_{\lambda \vdash n} SU(V_\lambda)$ for G, on $\bigoplus_{\lambda \vdash n} V_\lambda$, there is some evidence supporting correlated action of G on pairs of subspaces V_λ and $V_{\lambda^\star}$, whenever λ is dual to $\lambda^\star$. As a first input, the subspaces of dual partitions have equal dimensions, therefore, even dense action on each, separately, does not immediately imply decoupling of the two subspaces.

If we enumerate the YY basis of λ, by $|i_1\rangle, |i_2\rangle, \ldots, |i_d\rangle$, where d is the dimension of V_λ. Each element of these bases, $|i_j\rangle$, have a corresponding tableau, and the transpose of that tableau is a tableau of $\lambda^\star$, and it is bijectively related to a YY base element, $|i'_j\rangle$, of $V_{\lambda^\star}$. Let X be an element of the Lie algebra of G, whose action on V_λ has the form:

$$X \overset{\lambda}{\twoheadrightarrow} \sum_{j\in d} \alpha_j |j\rangle\langle j| + \sum_{i<j} \beta_{ij}(|i\rangle\langle j| + |i\rangle\langle j|) + i\delta_{ij}(|i\rangle\langle j| - |i\rangle\langle j|).$$

By $\overset{\lambda}{\twoheadrightarrow}$, I mean the restriction of X on V_λ, by projecting out everything else from other subspaces. It is believable that the similar action on the dual block is according to:

Claim 1. The projection of X on $\lambda^\star$ is according to:

$$X \overset{\lambda^\star}{\twoheadrightarrow} \sum_{j\in d} \pm\alpha_j |j'\rangle\langle j'| + \sum_{i'<j'} \pm\beta_{ij}(|i'\rangle\langle j'| + |i'\rangle\langle j'|) \pm i\delta_{ij}(|i'\rangle\langle j'| - |i'\rangle\langle j'|).$$

If this is the case, then it immediately implies the mentioned coupling. In order to see this, notice that $X \overset{\lambda}{\twoheadrightarrow} 0$ implies $X \overset{\lambda^\star}{\twoheadrightarrow} 0$, and vice versa. Checking the situation for the dual partitions $(2,1,1)$ and $(3,1)$ for four labels, one can confirm that this is true. However, even in this case, quantum efficient computation is not ruled out. For example, consider the situation where the initial state is according to $\frac{1}{\sqrt{2}}(|x\rangle + |x'\rangle)$. Then a coupled action of the form $U \oplus U^\star$ maps $\frac{1}{\sqrt{2}}(|x\rangle + |x'\rangle)$ to $\frac{1}{\sqrt{2}}(U|x\rangle + U^\star|x'\rangle)$. Then finalizing with the same state we get $\frac{1}{2}(\langle x|U|x\rangle + \langle x'|U^\star|x'\rangle) = \Re\langle x|U|x\rangle$. However, the problem of reading an entry of a quantum circuit is already known to be BQP-complete.

- It is not clear if there is a way to act as $SU(V_\lambda)$ on all of the partitions of n. The bridge lemma works if two orthogonal subspaces are being joined together. Therefore, it is interesting to extend the bridge lemma to more subspaces. Moreover, there cases where two subspaces of equal dimensionality take part in a single branching rule. Therefore, the bridge lemma is not applicable. For example consider the partition

$(3,2,1)$. The branching rule for this partition involves decomposition into the direct sum of three subspaces corresponding to $(2,2,1)$, $(3,1,1)$, and $(3,2)$. However, not only the subspaces corresponding partitions $(2,2,1)$ and $(3,2)$ have the same dimensions, but also they are dual partitions, and it might be the case that even the action of G cannot be decoupled from the two.

8 Conclusion

I applied some of the ideas from complexity theory and quantum complexity theory to a small regime of theoretical physics, the problem of particle scattering in integrable theories of $1+1$ dimensions. I found that the complexity of the model essentially depends on the initial superpositions that the particles start out from. The theory can be simulated within the one clean qubit if no initial superposition is allowed. However, I proved that if special initial superpositions are allowed, then in the model equipped with demolition intermediate measurements, it is hard to sample from the output distribution on a classical computer, unless the polynomial hierarchy collapses to the third level.

Bibliography

[1] Scott Aaronson. Guest column: Np-complete problems and physical reality. *ACM Sigact News*, 36(1):30–52, 2005.

[2] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005.

[3] Scott Aaronson. *Quantum computing since Democritus*. Cambridge University Press, 2013.

[4] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2011.

[5] Dorit Aharonov. A simple proof that toffoli and hadamard are quantum universal. *arXiv preprint quant-ph/0301040*, 2003.

[6] Dorit Aharonov and Itai Arad. The bqp-hardness of approximating the jones polynomial. *New Journal of Physics*, 13(3):035019, 2011.

[7] Dorit Aharonov, Itai Arad, Elad Eban, and Zeph Landau. Polynomial quantum algorithms for additive approximations of the potts model and other points of the tutte plane. *arXiv preprint quant-ph/0702008*, 2007.

[8] Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the jones polynomial. *Algorithmica*, 55(3):395–421, 2009.

[9] Changrim Ahn and Rafael I Nepomechie. Review of ads/cft integrability, chapter iii. 2: exact world-sheet s-matrix. *Letters in Mathematical Physics*, 99(1-3):209–229, 2012.

[10] Nima Arkani-Hamed, Jacob L Bourjaily, Freddy Cachazo, Alexander B Goncharov, Alexander Postnikov, and Jaroslav Trnka. Scattering amplitudes and the positive grassmannian. *arXiv preprint arXiv:1212.5605*, 2012.

[11] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[12] D Bacon, J Kempe, DP DiVincenzo, DA Lidar, and KB Whaley. Encoded universality in physical implementations of a quantum computer. *arXiv preprint quant-ph/0102140*, 2001.

[13] Bela Bauer, Claire Levaillant, and Michael Freedman. Universality of single quantum gates. *arXiv preprint arXiv:1404.7822*, 2014.

[14] Rodney J Baxter. Partition function of the eight-vertex lattice model. *Annals of Physics*, 70(1):193–228, 1972.

[15] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[16] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20. ACM, 1993.

[17] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20100301. The Royal Society, 2010.

[18] HJ Briegel, DE Browne, W Dür, R Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

[19] William H Campbell. Indexing permutations. *Journal of Computing Sciences in Colleges*, 19(3):296–300, 2004.

[20] Stephen A Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158. ACM, 1971.

[21] Christopher M Dawson and Michael A Nielsen. The solovay-kitaev algorithm. *arXiv preprint quant-ph/0505030*, 2005.

[22] David Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 449, pages 669–677. The Royal Society, 1995.

[23] David P DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015, 1995.

[24] David P DiVincenzo, Dave Bacon, Julia Kempe, Guido Burkard, and K Birgitta Whaley. Universal quantum computation with the exchange interaction. *Nature*, 408(6810):339–342, 2000.

[25] LD Faddeev. Two-dimensional integrable models in quantum field theory. *Physica Scripta*, 24(5):832, 1981.

[26] Michael Freedman, Alexei Kitaev, Michael Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin of the American Mathematical Society*, 40(1):31–38, 2003.

[27] Subir Ghoshal and Alexander Zamolodchikov. Boundary s matrix and boundary state in two-dimensional integrable quantum field theory. *International Journal of Modern Physics A*, 9(21):3841–3885, 1994.

[28] Kurt Gödel. Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i. *Monatshefte für mathematik und physik*, 38(1):173–198, 1931.

[29] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64(1):012310, 2001.

[30] Gordon James and Adalbert Kerber. The representation theory of the symmetric group. *Reading, Mass*, 1981.

[31] Stephen P Jordan. Permutational quantum computing. *arXiv preprint arXiv:0906.2508*, 2009.

[32] Julia Kempe, Dave Bacon, Daniel A Lidar, and K Birgitta Whaley. Theory of decoherence-free fault-tolerant universal quantum computation. *Physical Review A*, 63(4):042307, 2001.

[33] Julia Kempe, David Bacon, David P DiVincenzo, and K Brigitta Whaley. Encoded universality from a single physical interaction. *Quantum Information & Computation*, 1(4):33–55, 2001.

[34] Julia Kempe and K Birgitta Whaley. Exact gate sequences for universal quantum computation using the xy interaction alone. *Physical Review A*, 65(5):052330, 2002.

[35] A Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[36] E Knill, R Laflamme, and G Milburn. Efficient linear optics quantum computation. *arXiv preprint quant-ph/0006088*, 2000.

[37] Emanuel Knill and Raymond Laflamme. Power of one bit of quantum information. *Physical Review Letters*, 81(25):5672, 1998.

[38] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46–52, 2001.

[39] Debbie W Leung. Quantum computation by measurements. *International Journal of Quantum Information*, 2(01):33–43, 2004.

[40] Seth Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346, 1995.

[41] Tomoyuki Morimae, Keisuke Fujii, and Joseph F Fitzsimons. Hardness of classically simulating the one-clean-qubit model. *Physical review letters*, 112(13):130502, 2014.

[42] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[43] B Schroer, TT Truong, and P Weisz. Towards an explicit construction of the sine-gordon field theory. *Physics Letters B*, 63(4):422–424, 1976.

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

[45] Peter W Shor and Stephen P Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Information & Computation*, 8(8):681–714, 2008.

[46] Michael Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 2012.

[47] Matthias Staudacher. Review of ads/cft integrability, chapter iii. 1: Bethe ansätze and the r-matrix formalism. *Letters in Mathematical Physics*, 99(1-3):191–208, 2012.

[48] Barbara M Terhal and David P DiVincenzo. Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games. *arXiv preprint quant-ph/0205133*, 2002.

[49] Barbara M Terhal and David P DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. *Physical Review A*, 65(3):032325, 2002.

[50] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[51] Alan Mathison Turing. On computable numbers, with an application to the entscheidungsproblem. *J. of Math*, 58(345-363):5, 1936.

[52] Leslie G Valiant. Classical simulation of quantum computations. Technical report, DTIC Document, 2005.

[53] Steven Weinberg. *The quantum theory of fields*, volume 2. Cambridge university press, 1996.

[54] L-A Wu and DA Lidar. Power of anisotropic exchange interactions: Universality and efficient codes for quantum computing. *Physical Review A*, 65(4):042318, 2002.

[55] Chen-Ning Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Physical Review Letters*, 19(23):1312, 1967.

[56] Andrew Chi-Chih Yao. Classical physics and the church–turing thesis. *Journal of the ACM (JACM)*, 50(1):100–105, 2003.

[57] Alexander B Zamolodchikov and Alexey B Zamolodchikov. Relativistic factorized s-matrix in two dimensions having o (n) isotopic symmetry. *Nuclear Physics B*, 133(3):525–535, 1978.

[58] Alexander B Zamolodchikov and Alexey B Zamolodchikov. Factorized s-matrices in two dimensions as the exact solutions of certain relativistic quantum field theory models. *Annals of physics*, 120(2):253–291, 1979.