From quantum circuits to Hamiltonians: analysis of a multi-time construction for QMA

Nikolas P. Breuckmann

November 21, 2013

Master thesis under supervision of
Prof. Dr. B. M. Terhal

Fakultät für Mathematik, Informatik, Naturwissenschaften
Institute for Quantum Information

RWTH RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

First reviewer
Prof. Dr. B. M. Terhal

Second reviewer
Prof. Dr. N. Schuch

Declaration of Authorship

Ich, Nikolas Peter Breuckmann, erkläre hiermit, dass ich diese Arbeit mit dem Thema ‘From quantum circuits to Hamiltonians: analysis of a multi-time construction for QMA’ selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle wörtlichen und sinngemäßen Zitate wurden von mir als solche gekennzeichnet.

Unterschrift: ____________________

Datum: ____________________

Acknowledgements

Foremost, I would like to express my gratitude to my supervisor Barbara Terhal for her guidance, patience and for many insightful discussions. I also want to thank her for making my visit to the QStart conference in Jerusalem possible.

Besides my advisor, I would like to thank my friends and family, foremost my parents, for their unconditional support and encouragement. A special thanks goes to my uncle Heinrich for being so generous to give me the laptop on which this thesis was written on as a gift.

I also would like to thank all people at the IQI in Aachen for contributing to the good atmosphere and for many interesting discussions. I am very much looking forward to continue working here.

Contents

List of Figures

Notation

$\ker(A)$	nullspace of the linear operator A
$\mathrm{tr}(A)$	trace of the linear operator A
$\|\Omega\rangle$	vacuum state
$\{0,1\}^*$	set of all words over $0,1$
$\|x\|$	length of the word x
$\langle\ldots\rangle$	encoding into a word in $\{0,1\}^*$
$x \in A$	x is an instance of the decision problem A, i.e. $x \in A_{yes} \cup A_{no}$
$a \coloneqq b$	a is defined to be equal to b
$A :\Leftrightarrow B$	statement A is equivalent to statement B by definition
$\Pr(E)$	probability of event E
P_i^0	projector into subspace where qubit i is in state $\|0\rangle$
$\mathrm{L}(G)$	Laplacian matrix of the graph G

n	number of qubits
D	depth of the circuit
L	size of the circuit
τ	duration of a computation
T	set of all proper time configurations
N	number of proper time configurations, i.e. $\|T\|$
N_{bound}	number of proper time configurations with one qubit fixed at the final position
$U_{\mathbf{t}}$	unitary operator that is applied on the data register when going from $\mathbf{0}$ to $\mathbf{t}$
S	set of ancilla qubits
q_{out}	output qubit that determines whether the curcuit accepts or rejects

$\mathbf{t}\vert_{\mu,\nu,\ldots} = i$	time configuration $\mathbf{t}$ with qubits $\mu, \nu, \ldots$ at time i, i.e. $t_\mu = t_\nu = \ldots = i$
$\mathcal{H}_{legal}$	nullspace of H_{legal}, all states where clock-qubits correspond to a time
$\mathcal{H}_{caus}$	nullspace of $H_{legal} + H_{caus}$, all states with well-defined clocks where no qubit has undergone a 2-qubit gates without its partner

Chapter 1

Introduction

With the introduction of computer technology the question whether computational problems are solvable with a limited amount of resources became a critical issue. In the 1930s, Turing had already developed a mathematical model that allowed the analysis of algorithms, called *Turing machine*. It was the idea of Hartmanis and Sterns to measure the number of steps (time) and the memory (space) needed as a function of the input size to determine the feasibility of a problem [15]. It was established that a problem is considered to be *efficiently solvable* if the function measuring the required time grows like a polynomial in the size of the input [13]. The class of such problems is called P.

Not efficiently computable in this sense are simulations of quantum mechanical systems, as many-body interactions demand the storage and manipulation of a number of complex amplitudes which is exponential in the size of the system. Feynman proposed that this weakness can be turned into a strength, since it implies that quantum mechanical systems have high computational power [12]. The standard way[1] to represent a computation by a quantum computer is by *quantum circuits* which consist of wires and elementary *quantum gates* to carry and manipulate information stored in quantum states [30]. In analogy to bits in classical computers, quantum information is stored in *qubits* which are 2-level quantum systems. The class of all problems which are efficiently solvable by a quantum computer is called BQP, standing for "bounded error quantum polynomial time". Here, "bounded error" refers to the fact that quantum computation is inherently probabilistic. This does not pose a problem, as the probability of obtaining an incorrect result goes to 0 quickly when repeating the computation [30]. It is known that quantum computers can simulate classical computers efficiently, thus we have $\mathsf{P} \subseteq \mathsf{BQP}$.

[1] There also exists the concept of a *Quantum Turing Machine* introduced by David Deutsch [9]. However, it is equivalent to the circuit model which is more commonly used.

In the mid-90s, Shor showed that not only inherently quantum mechanical problems could be solved faster by a quantum computer; he proved that factoring a number into primes can be done with exponential speed-up compared to a classical computer. Today there are many other known classical problems whose structure can be exploited by a quantum machine, to gain exponential speed-ups over the best known classical algorithms [17]. Therefore, there is a high interest in developing a theory of quantum computational complexity and relating it to known classical complexity classes.

However, in this thesis we will focus on a problem which is inherently quantum mechanical in nature. Namely, the problem of deciding whether a given physically reasonable Hamiltonian has a ground state energy above or below a certain threshold. By physically reasonable we mean that the Hamiltonian does not describe interactions between an arbitrary large number of qubits. Hence, the problem is called LOCAL HAMILTONIAN. Kitaev showed that a solution of this problem is efficiently *verifiable* by a quantum computer, simply by providing the ground state [21]. The class of problems which are efficiently verifiable by a quantum computer is called QMA. It is believed, though not proven, that not all problems in QMA are efficiently *solvable* by a quantum computer.

Kitaev also showed that LOCAL HAMILTONIAN is among the hardest problems in QMA. Hence, there are problems which arise in the analysis of physically reasonable systems which are difficult to solve, even for a quantum computer. Kitaev's proof relied on an abstract mapping from quantum circuits to Hamiltonians that involved the introduction of a clock encoded into qubits. In this thesis we will introduce a different mapping which is physically motivated, as it corresponds to a system of interacting fermions. The idea to use interacting fermions was first presented in a paper by Mizel, Lidar and Mitchell [25]. We show that this model is equivalent to the one introduced by Kitaev, except that we will introduce a clock for each qubit.

The thesis is structured as follows. In Chapter 2 we give an introduction to quantum complexity theory with a focus on the class QMA and Kitaev's proof that LOCAL HAMILTONIAN is among the hardest problems in QMA. We also show the relationship between the circuit-to-Hamiltonian construction used in that proof and alternatives to the quantum circuit model. Finally, we will introduce the construction proposed by Mizel, Lidar and Mitchell. In Chapter 3 we show that the MLM proposal is equivalent to a circuit-to-Hamiltonian construction similar to the one as defined by Kitaev. In Chapter 4 we introduce tools from spectral graph theory to analyze the constructed Hamiltonian. We use our construction in Chapter 5 to prove that LOCAL HAMILTONIAN is a hard problem for a quantum computer. We also show how to reduce the number of qubits involved in interactions by introducing terms in the Hamiltonian which have an energy proportional to the system size. An argument of the proof relies on lower bounding the size of the gap between the two smallest eigenvalues of the constructed Hamiltonian. Unfortunately, we did not find such a lower bound. However, in Chapter 6 we present some numerical results and non-rigorous arguments implying that such a lower bound does exist.

Chapter 2

Quantum Complexity

This chapter is organized as follows. In Sec. 2.1 we will give a review of basic notions of complexity theory. In Sec. 2.2 we define the complexity class QMA and discuss some of its properties. We define the problem Local Hamiltonian in Sec. 2.3 and give a summary of the proof that it is among the hardest problems of QMA in Sec. 2.4. We discuss some further results regarding Local Hamiltonian and the closely related problem Quantum SAT in Sec. 2.5. Finally, we discuss alternative models of quantum computation in Sec. 2.6. We illustrate how to proof that they have the same computational power as quantum circuits using previously introduced ideas from quantum complexity.

2.1 Preliminaries

Complexity theory deals with the inherent *hardness* of algorithmical problems. The word *problem* always refers to the abstract notion. A concrete manifestation of a computational problem is called *instance*. A computational problem can thus be seen as the collection of all of its instances. For example, to decide whether a given number is even is a problem called Evenness. An instance of Evenness is any number $k \in \mathbb{N}$. The hardness of a problem is measured by how much of some ressource, such as time or memory, is needed to find the solution. The demand for a resource is a function depending on the size of a the problem instance. Problems are put into different *complexity classes* which are defined by limiting the available resources of a chosen computational model. Prominent examples for complexity classes are P and NP. The former is the class of problems which can be solved by a deterministic Turing machine (TM) in polynomial time while the latter is the class of problems solvable in polynomial time by a non-deterministic Turing machine (NTM). NTMs are Turing machines which at each point in the computation can choose different actions simultaniously, which means that the computation is not a sequence but a tree. When the NTM reaches a point at which it finds the solution it stops. By performing a search on this tree a TM can simulate a NTM, but only with exponential slow down. Suppose a problem is in NP and we are allowed to give a description of the path going from the root of the NTMs computational tree to the answer node to a TM. Then the TM can perform the computation in the same time as the NTM. Such a description is called a *witness* and NP can also be defined as the class of problems for which a solution can be easily checked by a TM when a witness is provided [27, 32]. The question if P=NP can therefore be reformulated into whether a NTM can be simulated by a TM with only polynomial slow down which seems very unlikely.

Let us formalize the preceding notions.[1] We assume that all problems are encoded over the alphabet $\{0,1\}$. A *word* is a finite sequence of symbols from an alphabet and the set of all words over the alphabet $\{0,1\}$ is denoted by $\{0,1\}^*$. An encoding into a word in $\{0,1\}^*$ is denoted by pointy brackets $\langle\ldots\rangle$. A *decision problem* $A = (A_{yes}, A_{no})$ is defined as a partition of $\{0,1\}^*$ into two subsets called A_{yes} and A_{no}, i.e. $A_{yes} \cap A_{no} = \emptyset$ and $A_{yes} \cup A_{no} = \{0,1\}^*$. Elements of A_{yes} are called *yes-instances* and elements of A_{no} *no-instances*. A function $f : \{0,1\}^* \to \{0,1\}^*$ is said to be *computable in polynomial time* if there exists a TM that outputs $f(x)$ for every input $x \in \{0,1\}^*$ after polynomially many steps in the length of the input $|x|$. The class P is defined as the set of all problems A such that there exists a polynomial p and a TM M which halts after $p(|x|)$ steps on all inputs $x \in \{0,1\}^*$ and outputs 1 if the input x is in A_{yes} and 0 for inputs from A_{no}. The class NP is defined as the set of all problems for which there exist polynomials p and q and a TM M such that M halts on all all inputs (x, y) in $p(|x|)$ steps and for all $x \in A_{yes}$ there exists a $y \in \{0,1\}^*$ with $|y| = q(|y|)$ such that given (x, y) as input, M outputs 1 and for all $x \in A_{no}$ and all y with $|y| \leq q(|x|)$ M outputs 0.

A generalization of decision problems are *promise problems* for which the input is promised to be from a subset of all possible inputs $\{0,1\}^*$, i.e. $A_{yes}, A_{no} \subseteq \{0,1\}^*$ and $A_{yes} \cap A_{no} = \emptyset$ but it is allowed that $A_{yes} \cup A_{no} \neq \{0,1\}^*$. Obviously, all promise problems are decision problems. We will from no on write $x \in A$ for $x \in A_{yes} \cup A_{no}$.

Example 1. A trivial example for a decision problem which is in P is Evenness. Yes-instances are even numbers and no-instances are odd numbers. Since all elements of $\{0,1\}^*$ correspond to a binary encoding of a number the yes- and no-instances exhaust all possible inputs. A constant-time algorithm to decide between a yes- and a no-instance simply checks the least significant bit.

[1] For the definition of a Turing machine consult any textbook on complexity theory such as [27, 32].

A promise problem which is in NP is Hamiltonian Path, where all instances x are binary encodings of graphs. The yes-instances correspond to graphs in which one can find a path which visits each vertex exactly once. The polynomial-size witness for a yes-instance is an encoding of such a path. The number of steps needed to check that a given path is a Hamiltonian path clearly scales linear in the size of the graph.

We will use asymptotic notation to describe the limiting behavior of a function. Let $f, g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$. The notation $f(x) \in O(g(x))$ means that f is bounded above by g asymptotically up to a constant factor, i.e. there exists a constant $c > 0$ and $x_0 \geq 0$ such that $f(x) \leq c \cdot g(x)$ for all $x \geq x_0$. We will also write $O(\text{poly}(x))$ which means that the asymptotic growth scales at most like a polynomial in x. On the other hand, $f(x) \in \Omega(g(x))$ means that f is bounded below by g asymptotically up to a constant factor, i.e. there exists a $c > 0$ and $x_0 \geq 0$ such that $f(x) \geq c \cdot g(x)$ for all $x \geq x_0$.

To compare the hardness of different problems we use *Karp reduction*. We say that a problem A *reduces* to B ($A \leq B$) if there exists a TM which computes a function R in polynomial time such that

$$\begin{aligned} x \in A_{yes} &\Rightarrow R(x) \in B_{yes} \\ x \in A_{no} &\Rightarrow R(x) \in B_{no} \end{aligned} \tag{2.1}$$

for all $x \in A$. Loosely speaking, we can decide the problem A with the same ressources as problem B up to some polynomial overhead. We can define the hardest problem of a complexity class Comp by demanding that all other problems of this class reduce to it. Such a problem is called Comp-*complete*. Comp-complete problems are so general that they capture the structure of all problems in Comp. For the class NP we can easily define such a problem:

Definition 2.1 (Witness Existence)**.** Let $x = \langle M, y, p \rangle$ be the encoding of a TM M, an input y and a polynomial p. Given x decide

$$\begin{aligned} x \in A_{yes} &:\Leftrightarrow \exists w \text{ with } |w| \leq p(|y|) : M \text{ accepts } (y, w) \text{ after } p(|y|) \text{ or fewer steps} \\ x \in A_{no} &:\Leftrightarrow \forall w \text{ with } |w| \leq p(|y|) : M \text{ does not accept } (y, w) \text{ after } p(|y|) \text{ or fewer steps} \end{aligned} \tag{2.2}$$

The problem Witness Existence is trivially NP-complete as it just paraphrases the definition of NP. However, there exist many non-trivial NP-complete problems. The first non-trivial problem proven to be NP-complete is 3-SAT. The proof was found independently by Cook and Levin by reducing Witness Existence to 3-SAT. We give an overview of the proof in Section 2.4.

At present, all algorithms for NP-complete problems take superpolynomial time in the size of the input. The existence of a polynomial time algorithm for a problem that is NP-complete would imply P=NP. However, the opposite is believed to be true and finding a proof for $\mathsf{P} \neq \mathsf{NP}$ is one of the biggest open problems in theoretical computer science.

2.2 The class QMA

The definition of NP can be extended to an analogue definition for quantum computers by considering a notion of a *quantum witness* which was first proposed by Knill [22] and later formalized by Kitaev [21]. A quantum witness is simply a quantum state $|\gamma\rangle$ given to a quantum computer that certifies that some instance of a problem $x \in A$ is a yes-instance. As for NP we want that the quantum computer accepts or rejects the witness in polynomial time. However, the computation of a quantum computer is inherently probabilistic. Therefore, we demand that the quantum computer accepts a yes-instance with a proper witness with high probability $\geq p_1$ and erroneously accepts no-instances only with a low probability $\leq p_0$. As a model for quantum computation we choose quantum circuits. Since a single circuit has a fixed number of input qubits we must take a family of circuits from which we can choose according to the input length. There is a subtlety when we define these families. Nothing prevents us from hard-wiring the solution of computationally hard problems[2] into the circuits. Hence, we demand that a list with the position of all gates in a circuit with n input qubits has to be computable by a TM in $O(\text{poly}(n))$ time. Such families of circuits are also called *uniform*.

Definition 2.2. Let $A = (A_{yes}, A_{no})$ be a promise problem. Then $A \in \mathsf{QMA}$ if and only if there exists a TM which computes in polynomially many steps on input x a description of a quantum circuit U_x acting on n_x qubits and a natural number $m_x \leq n_x$ such that:

$$\begin{aligned} x \in A_{yes} \Rightarrow \exists\, |\gamma\rangle \in \mathbb{C}^{2^{m_x}} &: \Pr(U_x \text{ accepts } |\gamma\rangle) \geq p_1 \\ x \in A_{no} \Rightarrow \forall\, |\gamma\rangle \in \mathbb{C}^{2^{m_x}} &: \Pr(U_x \text{ accepts } |\gamma\rangle) \leq p_0 \end{aligned} \tag{2.3}$$

where

$$\Pr(U_x \text{ accepts } |\gamma\rangle) := |\,\langle 1|_{q_{out}} U_x \,|\gamma, 0^{s_x}\rangle\,|^2, \tag{2.4}$$

$s_x = n_x - m_x$ is the number of ancilla qubits initialized to $|0\rangle$, q_{out} is the designated output qubit and $p_1 - p_0 \in \Omega(|x|^{-\alpha})$ for some $\alpha \in \mathbb{R}_{\geq 0}$.

[2] Or even answers to problems which are impossible to solve algorithmically such as the halting problem.

Note that the number of input qubits n_x and the size L_x of the circuit U_x are polynomial in $|x|$ since U_x is polynomial-time generated [21, 34]. QMA is very robust with regard to the choice of p_1 and p_0. There are equivalent definitions where p_1 and p_0 are functions which are exponentially close to 1 respectively 0 (depending on the size of the input) or constants which are strictly higher respectively lower than $\frac{1}{2}$ [4, 27, 34].

The name QMA stands for "Quantum Merlin Arthur" referring to the game theoretic interpretation of this class; Merlin has unlimited computational power and tries to convince Arthur, who is *only* in possession of a quantum computer, that an instance of a problem is a yes-instance. However, Merlin is not trustworthy and tries to cheat. A problem is in QMA if Merlin can convince Arthur with high probability that an instance is a yes-instance and only succeeds in convincing Arthur to accept a no-instance with low probability.

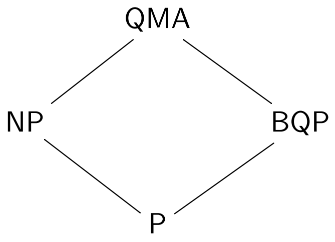

FIGURE 2.1: A diagram illustrating the inclusions between complexity classes discussed in this thesis. The lines indicate containments going upward. The relation between the classes NP and BQP is unknown.

2.3 The 5-Local Hamiltonian problem

The first problem that was shown to be QMA-complete was 5-LOCAL HAMILTONIAN [4, 21]. We call a Hamiltonian H *k-local* if we can write it as a sum of terms $H = \sum_j^m H_j$ where each H_j acts on at most k qubits. Here w.l.o.g. all H_j will be positive-semidefinite.

Definition 2.3 (k-LOCAL HAMILTONIAN)**.** Let $x = \langle H, a, b\rangle$ be the encoding of a k-local Hamiltonian H acting on n qubits and real numbers a, b with $0 \leq a < b$ and $b - a \in \Omega(n^{-\alpha})$ for some $\alpha \in \mathbb{R}_{\geq 0}$. Given x decide

$$x \in A_{yes} :\Leftrightarrow H \text{ has an eigenvalue } \leq a$$
$$x \in A_{no} :\Leftrightarrow \text{all eigenvalues of } H \text{ are} > b.$$

Loosely speaking k-LOCAL HAMILTONIAN asks whether there exists a quantum state which avoids a number of energy penalties defined by the k-local terms H_j.

The problem k-Local Hamiltonian is related to the classical problem k-SAT. Let $\phi = C_1 \wedge \cdots \wedge C_m$ be a formula in *conjunctive normal form* k-CNF meaning that each clause C_j consists of a disjunction over k (negated) variables. As a concrete example, let us take $k = 2$ and $\phi(x_1, x_2, x_3) = C_1 \wedge C_2 = (x_1 \vee \neg x_2) \wedge (x_2 \vee x_3)$. For each clause we can define a 2-local Hamiltonians H_j acting on three qubits: $H_1 = |0\rangle \langle 0|_1 \otimes |1\rangle \langle 1|_2$ and $H_1 = |0\rangle \langle 0|_2 \otimes |0\rangle \langle 0|_3$ corresponding to the unsatisfying assignment of their respective clause. We define the full Hamiltonian $H = H_1 + H_2$. Let $\tilde{\mathbf{x}} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3) \in \{0,1\}^3$ be an assignment and $|\tilde{\mathbf{x}}\rangle$ the eigenvector of H which corresponds to that assignment. We see that $\phi(\tilde{\mathbf{x}})$ is true if and only if $(H_1 + H_2)|\tilde{\mathbf{x}}\rangle = 0$. If $\tilde{\mathbf{x}}$ is an unsatisfying assignment for one clause C_j then $|\tilde{\mathbf{x}}\rangle$ is a eigenvector corresponding to eigenvalue 1, i.e. $H_j |\tilde{\mathbf{x}}\rangle = |\tilde{\mathbf{x}}\rangle$. For the general case where we have k-clauses and n variables we can construct a k-local Hamiltonian $H = \sum_{j=1}^{m} H_j$ which has eigenvectors $|\tilde{\mathbf{x}}\rangle$ with $\tilde{\mathbf{x}} \in \{0,1\}^n$. The corresponding eigenvalue λ of $|\tilde{\mathbf{x}}\rangle$ is given by the number of clauses for which $\tilde{\mathbf{x}}$ is an unsatisfying assignment. Asking whether H has an eigenvalue $\lambda = 0$ is equivalent to asking whether ϕ has a satisfying assignment. However, in k-Local Hamiltonian we ask whether there is a low lying eigenvalue. It is therefore more appropriate to think of k-Local Hamiltonian as the quantum analogue of Max-k-SAT where we have to determine the maximum number of satisfiable clauses in a k-CNF formula [21, 34]. The problem of deciding whether there exists a eigenvalue $\lambda = 0$ for a k-local Hamiltonian is called Quantum k-SAT [7].

Theorem 2.4. The problem k-Local Hamiltonian is in QMA.

Proof. We need to show that given a description of H and the numbers a and b which are separated by the inverse of a polynomial, we can find a quantum circuit W which applied to a quantum state produces a result 0 or 1 corresponding to “reject” and “accept”. If the ground state energy of H is lower than a there should exist a witness such that W accepts with high probability. On the other hand if the ground state energy is higher than b then W should reject all inputs with high probability.

We will denote the ground state of H by $|\eta\rangle$ and its corresponding eigenvalue by λ. To illustrate the construction let us first consider the simple case in which all terms H_j are given by projectors $|\alpha^j\rangle \langle \alpha^j|$. Then we have

$$\frac{\lambda}{r} = r^{-1} \sum_{j=1}^{r} \langle \eta | H_j | \eta \rangle = r^{-1} \sum_{j=1}^{r} |\langle \eta | \alpha^j \rangle|^2. \tag{2.5}$$

If we define a measurement in a basis spanned by $|\alpha_j\rangle$ and the orthogonal subspace then $|\langle \eta | \alpha^j \rangle|^2$ is exactly the probability of measuring α^j when the system is in the state $|\eta\rangle$. From this follows that $\frac{\lambda}{r}$ is the probability of measuring α^j when we first pick $j \in \{1, \ldots, r\}$ uniformly at random and then measure in the basis $|\alpha^j\rangle$ and the orthogonal subspace. This procedure can be implemented by a quantum circuit W which will output 0 ("reject") with probability $\frac{\lambda}{r}$ if the result was the randomly chosen α^j and 1 ("accept") otherwise.

The quantum circuit W accepts $|\eta\rangle$ with probability $1 - \frac{\lambda}{r}$. Thus if all eigenvalues of H are bigger than b then any state $|\psi\rangle$ is accepted with probability

$$1 - \frac{\langle\psi| H |\psi\rangle}{r} \leq 1 - \frac{b}{r}. \tag{2.6}$$

Since the probability for accepting any state is upper bounded by $p_0 = 1-\frac{b}{r}$ the reduction is sound. On the other hand if $\lambda \leq a$ then W will accept the ground state $|\eta\rangle$ as input with a probability higher than $p_1 = 1 - \frac{a}{r}$. Note that $p_1 - p_0 \in \Omega(n^{-\alpha})$. This shows that the reduction is complete.

For the more general case where the terms H_j are not just projections we use the spectral decomposition $H_j = \sum_{i \in S_j} \lambda_i^j |\alpha_i^j\rangle \langle\alpha_i^j|$ where $S_j \subseteq \{1, \dots, n\}$. Since each H_j is k-local we have $|S_j| \leq k$. We define the circuit W_j which takes the qubits S_j and one ancilla qubit q_{out} initialized to $|0\rangle$ as input. W_j is defined by its action:

$$W_j |\alpha_i^j\rangle |0\rangle_{q_{out}} = |\alpha_i^j\rangle \left(\sqrt{\lambda_i^j} |0\rangle_{q_{out}} + \sqrt{1 - \lambda_i^j} |1\rangle_{q_{out}} \right) \tag{2.7}$$

We will perform a measurement on the ancilla qubit in the computational basis. Let $|\eta\rangle = \sum_{i \in S_j} y_i |\alpha_i^j\rangle |\beta_i^j\rangle$ be the Schmidt-decomposition of $|\eta\rangle$. The probability for measurement outcome 1 is given by:

$$\begin{aligned} \Pr(W_j \text{ accepts } |\eta\rangle) &= |\langle 1|_{q_{out}} W_j |\eta, 0\rangle|^2 \\ &= \sum_{i \in S_j} (1 - \lambda_i^j) |y_i^j|^2 \\ &= 1 - \langle\eta| H_j |\eta\rangle \end{aligned} \tag{2.8}$$

The procedure is now analogous to the case where we only considered projections. We uniformly choose a random $j \in \{1, \dots, r\}$, apply W_j to $|\eta, 0\rangle$ and measure the ancilla. The circuit will accept with probability

$$\sum_{i=1}^{r} r^{-1} (1 - \langle\eta| H_j |\eta\rangle) = 1 - r^{-1} \langle\eta| H |\eta\rangle = 1 - \frac{\lambda}{r}. \tag{2.9}$$

Note that the size of the W_j and thus the size of the overall circuit does not depend on the number of qubits n respectively on the size of the problem $|x|$. ■

2.4 Kitaev's reduction

Before we sketch the proof of the completeness of 5-Local Hamiltonian let us first give the idea behind Cooks and Levins proof that 3-SAT is NP-complete. Thus, we need to show that an instance of Witness Existence can be reformulated as an instance in 3-SAT. For the reduction we need to construct a Boolean formula ϕ in conjunctive normal form with maximally 3 variables per clause which is satisfiable if and only if the TM accepts the input. First of all let us define variables $b_{i,t}$ and $h_{i,t,s}$. If the variable $b_{i,t}$ is set to 1 it means that at position i and time step t the symbol 1 is written on the tape. If $h_{i,t,s}$ is set to 1 it means that at time t the head of the TM is at position i and the TM is in state s. An assignment of the variables corresponds to a *history* of the computation performed by the TM. The formula ϕ will contain a set of clauses which check that the input is set correctly, e.g. we include $\neg b_{i,0}$ if the ith entry of the input is supposed to be 0. Another set of clauses will check that the computation itself is consistent, i.e. that the change in the symbols on the tape from t to $t+1$ really describes a step in the computation. Finally, we include the clause $\{b_{1,T}\}$ which checks that the output bit at the final time T on the first position on the tape is set to 1. We also need some clauses to check whether the assignment is *legal* meaning that we don't allow the TM to be in different states at the same time and that a symbol on the tape can not change if the head is not at the same position. It is important to note that all these checks can be done *locally* so that we can always express it by a clause of constant size. Finally, using a technical trick we can convert all clauses into ones which contain at most 3 variables.

Kitaev's QMA-reduction uses a similar idea as the Cook-Levin-Theorem. For the reduction we assume that we have some general instance $x \in A$ of a QMA problem A, i.e. we have a circuit $U = U_L \cdots U_1$ which accepts the input $|\gamma\rangle$ with probability $\geq p_1$ if $x \in A_{yes}$ and $|\gamma\rangle$ is a proper witness and rejects with probability $\geq 1 - p_0$ for all $|\gamma\rangle$ if $x \in A_{no}$. W.l.o.g. we assume that all gates U_i are either single or two-qubit gates [30]. Given the circuit U and $|\gamma\rangle$ we will construct a 5-local Hamiltonian and a corresponding ground state $|\eta\rangle$ with ground state energy λ smaller than a if $x \in A_{yes}$. If $x \in A_{no}$ then the ground state energy λ will be higher than b with $b - a \in \Omega(n^{-\alpha})$.

To check the validity of the computation by the quantum circuit we need to "look" at the data and see that it changes at each step t according to the application of the gate U_t. In the proof of the Cook-Levin-Theorem this was done by giving the variables a time index. Kitaev used an idea from Feynman [12] to introduce a register of *time qubits*. We will postpone the exact realization and just assume that we have an extra register

$|t\rangle \in \mathcal{H}_{time} = \mathbb{C}^{L+1}$. We define:

$$|\eta\rangle \coloneqq \frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} (U_t \cdots U_1 |\gamma, \mathbf{0}\rangle) \otimes |t\rangle \in \mathcal{H}_{data} \otimes \mathcal{H}_{time} \tag{2.10}$$

where for $t = 0$ no gate is applied, $\mathcal{H}_{data} = \mathbb{C}^{2^n}$ and $\mathbf{0} = 0 \ldots 0$ are ancilla qubits. The state $|\eta\rangle$ is called the *history state.*

The Hamiltonian has the form

$$H = H_{in} + H_{prop} + H_{out} \tag{2.11}$$

where the terms correspond to the clauses defined in the proof of the Cook-Levin-Theorem. Let $S \subseteq \{1, \ldots, n\}$ be the set of ancilla qubits. The term

$$H_{in} = \sum_{i \in S} |1\rangle \langle 1|_i \otimes |t = 0\rangle \langle t = 0| \tag{2.12}$$

enforces the correct initialization of the ancilla qubits. The validity of the computation is checked by

$$H_{prop} = \sum_{t=1}^{L} H_{prop}^t \tag{2.13}$$

where

$$H_{prop}^t = I \otimes |t\rangle \langle t| + I \otimes |t-1\rangle \langle t-1| - U_t \otimes |t\rangle \langle t-1| - U_t^\dagger \otimes |t-1\rangle \langle t| . \tag{2.14}$$

We call the output qubit of the circuit by $q_{out} \in \{1, \ldots, n\}$. The term

$$H_{out} = |0\rangle \langle 0|_{q_{out}} \otimes |t = L\rangle \langle t = L| \tag{2.15}$$

gives an energy penalty if the quantum circuit rejects.

Note that for correct initialization we have $H_{in} |\eta\rangle = 0$ by construction. We also have $H_{prop}^t |\eta\rangle = 0$ for the following reason: The term $I \otimes |t\rangle \langle t|$ picks the state at time t. The term $U_t \otimes |t\rangle \langle t-1|$ selects the state at $t-1$ and propagates it forward. Both of these terms cancel if and only if in the given state the t state is given by applying U_t to the $t-1$ state. The terms $I \otimes |t-1\rangle \langle t-1|$ and $U_t^\dagger \otimes |t-1\rangle \langle t|$ perform the same check for backwards time propagation and need to be added to make H_{prop}^t Hermitian. Thus we have

$$\lambda = \langle \eta| H_{out} |\eta\rangle = \frac{1}{L+1} \langle \gamma, \mathbf{0}| U^\dagger |0\rangle \langle 0|_{q_{out}} U |\gamma, \mathbf{0}\rangle \leq \frac{1-p_1}{L+1} =: a \tag{2.16}$$

proving that any accepting instance of the original problem is mapped to an accepting instance of 5-Local Hamiltonian, i.e. the reduction is complete. The proof showing that the reduction is also sound is more involved and can be found in [4, 21]. There it is shown that if $x \in A_{no}$ then $\lambda \geq b = \frac{c(1-\sqrt{p_0})}{L^3}$ for some constant $c > 0$. Note that $b - a \in \Omega(n^{-\beta})$ for some $\beta > 0$ since L is polynomial in n.

Up to this point the Hilbert space is given by $\mathbb{C}^{2^n} \otimes \mathbb{C}^{L+1}$. We want to convert this into a space solely consisting of qubits. We could represent the clock by $\log(L)$ qubits, but then the Hamiltonian would only be $\log(L)$-local. Instead, to implement the clock register we use the unary representation of the numbers $0, \ldots, L$, i.e. we set

$$|t\rangle \mapsto |\underbrace{1, \ldots, 1}_{\text{t}}, \underbrace{0, \ldots, 0}_{\text{L-t}}\rangle . \tag{2.17}$$

This realization of a clock is also called *domain wall clock* [28]. In the Hamiltonian (Eqn. 2.11) we replace the following terms:

$$\begin{aligned} |0\rangle\langle 0| &\mapsto |0\rangle\langle 0|_1 \\ |t\rangle\langle t| &\mapsto |10\rangle\langle 10|_{t,t+1} \\ |L\rangle\langle L| &\mapsto |1\rangle\langle 1|_L \end{aligned} \tag{2.18}$$

In H_{prop} (Eqn. 2.13) we also replace

$$\begin{aligned} |0\rangle\langle 1| &\mapsto |00\rangle\langle 10|_{1,2} \\ |t-1\rangle\langle t| &\mapsto |100\rangle\langle 110|_{t-1,t,t+1} \\ |L-1\rangle\langle L| &\mapsto |10\rangle\langle 11|_{L-1,L} \end{aligned} \tag{2.19}$$

and the similarly the Hermitian conjugate terms. Note that all of these terms are 3-local. Together with the 2-qubit gates applied to the data qubits we have that H_{prop} is 5-local. Thus, the full Hamiltonian is $5 - local$ as well.

Since $\mathbb{C}^{2^L}$ is a much larger space than $\mathbb{C}^{L+1}$ there are states which do not correspond to a time t. Those are the states where at some position the sequence “01” occurs. We can penalize those states by adding the 2-local term H_{legal} to the Hamiltonian:

$$H_{legal} = \sum_{t=1}^{L-1} |01\rangle\langle 01|_{t,t+1} \tag{2.20}$$

For a yes-instance this extra term does not change the value of the ground state energy since we have $H_{legal}|\eta\rangle = 0$ by construction of the history state $|\eta\rangle$ (Eqn. 2.10). For a no-instance we note that H commutes with H_{legal}. Thus the action of H leaves the nullspace of H_{legal} called $\mathcal{H}_{legal} := \ker(H_{legal})$ invariant. We will examine the spectrum of H on $\mathcal{H}_{legal}$ and its orthogonal complement $\mathcal{H}_{legal}^{\perp}$ independently. On $\mathcal{H}_{legal}$ we have $\langle\eta| H |\eta\rangle \geq b$. On $\mathcal{H}_{legal}^{\perp}$ we have $H \geq 1$ since $H_{legal} \geq 1$ and all terms in the Hamiltonian are positive-semidefinite. Thus in both cases $H \geq b$.

2.5 Further results on Hamiltonian complexity

Kitaevs result was improved by Kempe and Regev using 3-local terms [20] by modyfying the H_{prop} term to act only on one clock qubit instead of three. Following this Kitaev, Kempe and Regev showed that even 2-Local Hamiltonian is QMA-complete [19]. They achieved a smaller locality using 2-local gadgets which in the subspace of small energies give an effective 3-local interaction. The completeness was a surprise as the classical analogon Max-2-SAT was known not to be NP-complete. Furthermore it was shown by Oliviera and Terhal that 2-Local Hamiltonian remains QMA-complete when the interactions are between qubits which are spatially arranged on a 2D square lattice [31]. It is also possible to achieve QMA-completeness for 1D systems as shown by Aharonov, Gottesmann, Irani and Kempe [2] where they consider interactions between quantum systems with 12 states instead of qubits.

Closely related is the analysis of Quantum k-SAT which is the quantum analog of classical k-SAT (see Sec. 2.3). Bravy showed in [7] that Quantum k-SAT is in P and that Quantum k-SAT is QMA_1-complete for all $k \geq 4$.[3] Recently it was proven by Gosset and Nagaj that also Quantum 3-SAT is QMA_1-complete [14]. Eldar and Regev showed that Quantum SAT with interactions only between three and five-level systems is QMA_1-complete as well [10].

2.6 Relationship to alternative models of QC

Calling a model of computation BQP-universal means that it can solve all problems of BQP efficiently. The ideas presented in Section 2.4 are also used to prove the BQP-universality of two alternatives to the quantum circuit model [3, 28, 34]. They rely on the construction of a time-independent, local Hamiltonian H from a given quantum circuit U.

[3] The class QMA_1 is defined similarly as QMA except that yes-instances are accepted with a probability equal to 1.

2.6.1 Adiabatic quantum computation

We have seen in Section 2.3 that we can encode hard computational problems, such as instances of 3-SAT, into the ground state of a local Hamiltonian. However, we need to cool the system into the ground state of said Hamiltonian. Farhi, Goldstone, Gutmann and Sipser proposed to use the adiabatic theorem for this task [11].

Theorem 2.5 (Adiabatic theorem). Let $s \in [0, \tau]$ and $H(t/\tau)$ be a time-dependent Hamiltonian with ground state energy $\eta(s)$ and ground state $|\eta(s)\rangle$. Assume that all other eigenvalues are larger than $\eta(s) + \lambda$ for any $s \in [0, \tau]$. If we initialize the system in $|\eta(0)\rangle$ and apply the continuously varying Hamiltonian $H(s/\tau)$ for times $s \in [0, \tau]$ then for the resulting state $|\tilde{\eta}\rangle$ it holds that $\| \, |\eta(\tau)\rangle - |\tilde{\eta}\rangle \, \| \leq \delta$ if

$$\tau \geq \frac{10^5}{\delta^2} \max \left(\frac{\|H'\|^3}{\lambda^4}, \frac{\|H'\| \|H''\|}{\lambda^3} \right) \tag{2.21}$$

where H' and H'' are the first and second derivative of H with respect to s, $\|H\| \coloneqq \max_{s \in [0,\tau]} \|H(s/\tau)\|$ and $\| \cdot \|$ is the 2-norm.

The theorem was first stated by Born and Fock and a simplified proof can be found in [5]. To prepare the ground state we use the following scheme: Let H_1 be the Hamiltonian with a ground state which encodes the solution to the problem. Furthermore, let H_0 be a simple Hamiltonian with an easy-to-prepare ground state. We define the time-dependent Hamiltonian as the convex combination

$$H(s/\tau) \coloneqq \left(1 - \frac{s}{\tau}\right) H_0 + \frac{s}{\tau} H_1. \tag{2.22}$$

The duration of the computation τ is chosen according to Theorem 2.5 and the desired accuracy δ.

To simulate the computation of a quantum circuit $U = U_L \cdots U_1$ we assume w.l.o.g. that the input is the all-zero state $|\mathbf{0}\rangle = |0, \ldots, 0\rangle$ since any other input can be generated by the addition of gates to the circuit. The goal is to construct the Hamiltonians H_0 with ground state $|\mathbf{0}\rangle \otimes |t = 0\rangle$ and H_1 with the history state

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} \left(U_t \cdots U_1 |\mathbf{0}\rangle\right) \otimes |t\rangle \tag{2.23}$$

as its ground state. Both Hamiltonians act on the space given by the data register and the clock register $\mathcal{H}_{data} \otimes \mathcal{H}_{time}$ exactly as in Section 2.4.

We define $H_0 = H_{in} + H_{legal} + H_{start}$ where $H_{in} = \sum_{i=1}^{n} |1\rangle \langle 1|_i \otimes |t = 0\rangle \langle t = 0|$ and $H_{start} = \sum_{t=1}^{L} I \otimes |t\rangle \langle t|$. The term H_{legal} is chosen as in Eqn. 2.20. Note that H_0 has the unique ground state $|\mathbf{0}\rangle \otimes |t = 0\rangle$. Furthermore, we choose H_1 to be the Hamiltonian as constructed by Kitaev, except for the term H_{out}, i.e. $H_1 = H_{prop} + H_{legal} + H_{in}$.

We then use the adiabatic theorem to prepare the ground state of H_1, i.e. the history state $|\eta\rangle$. Finally, we perform a measurement on the time register and if the result is L then we know that the system is in the final state $U\,|\mathbf{0}\rangle \otimes |L\rangle$.

The application of the adiabatic theorem for quantum computation is known as *adiabatic quantum computation* AQC. In [11] Farhi et al. show that a quantum circuit can simulate the the adiabatic model efficiently. The relation to the circuit model via the history state was established later by Aharonov et al. in [3], where they show that the AQC model is polynomially equivalent to the circuit model. This is done by giving a lower bound for the gap λ which scales as the inverse of a polynomial in the number of gates L. From Theorem 2.5 then follows that we can reach a state which is polynomially close to the history state in time $\tau \in O(\text{poly}(L))$. The AQC model provides some robustness against decoherence due to the energy gap λ [8, 24] though it is not proven to be fault-tolerant.

2.6.2 Dynamic Hamiltonian quantum computation

Instead of using the ground state properties as for the AQC model we can also use the Schrödinger dynamics induced by the propagation term H_{prop} (see Eqn. 2.13). The idea to use the dynamical properties of a Hamiltonian for computation was the original proposal of Feynman [12, 28]. For some fixed $|\xi\rangle \in \mathcal{H}_{data}$ we define the states

$$|\tilde{\psi_i}\rangle := (U_i \cdots U_1\,|\xi\rangle) \otimes |i\rangle \in \mathcal{H}_{data} \otimes \mathcal{H}_{time} \tag{2.24}$$

for $i \in \{0, \ldots, L\}$. The states $|\tilde{\psi_i}\rangle$ span a subspace $\mathcal{H}_\xi \leq \mathcal{H}$ which is invariant under the action of H_{prop}. By choosing this basis we can represent H_{prop} on the subspace $\mathcal{H}_\xi$ by the symmetric matrix L.[4]

$$\mathrm{L} := H_{prop}|_{\mathcal{H}_\xi} = \begin{bmatrix} 1 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & -1 & 2 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & 2 & -1 \\ & & & & -1 & 1 \end{bmatrix} \tag{2.25}$$

[4] There is a slight conflict of notation as the size of the circuit is denoted L. However, it will be clear from the context what we mean.

A *continuous time quantum walk* CTQW is defined as the solution of the Schrödinger equation

$$\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}t}\left|\phi(t)\right\rangle = -\mathrm{L}\left|\phi(t)\right\rangle \tag{2.26}$$

which is solved by $|\phi(t)\rangle = \exp(\mathrm{iL}t)\,|\phi(0)\rangle$. If we prepare a system in the state $|\phi(0)\rangle = |\tilde{\psi}_0\rangle$ and let it evolve for some time τ then the probability of finding it in the basis state $|\tilde{\psi}_m\rangle$ is given by

$$p_\tau(m) = |\,\langle\tilde{\psi}_m|\exp(\mathrm{iL}\tau)\,|\psi_0\rangle\,|^2. \tag{2.27}$$

Since $\exp(\mathrm{iL}\tau)$ is unitary, the probability distribution $p_\tau(m)$ does not converge with τ. Thus we define the average probability distribution for some time τ:

$$\bar{p}_\tau(m) \coloneqq \frac{1}{\tau}\int_0^\tau \mathrm{d}\tau'\; p_{\tau'}(m) \tag{2.28}$$

The probability distribution $\bar{p}_\tau(m)$ does converge to a limiting distribution $\pi(m)$. Note that the limiting distribution for a CTQW does depend on the state that we started in, here $|\psi_0\rangle$. This is not the case for classical random walks [1, 28].

To perform a computation we prepare a system in the state $|\phi(0)\rangle = |\tilde{\psi}_0\rangle$ and let it evolve for some time τ. Then we do a measurement on the time register. If the result is L we know that we are in the state $U|\xi\rangle\otimes|L\rangle$. On the other hand, if we measure a $t < L$ we repeat the procedure. We can improve the probability for obtaining $U|\xi\rangle$ by adding identity gates at the end of the circuit. Nagaj shows in [28] that letting the system evolve for some time τ chosen uniformly between 0 and $O(L\log(L)^2)$ the probability to measure a time at which the data register is in the final state of the computation is close to $\frac{2}{3}$. From this follows, that this dynamical model is capable of simulating the circuit model with only polynomial overhead in L. We will discuss the significance of the matrix L and its spectrum for the convergence of the average probability distribution $\bar{p}_\tau(m)$ to the limiting distribution $\pi(m)$ in Section 4.2.

2.7 MLM proposal

In [25] Mizel, Lidar and Mitchell propose an alternative proof for the BQP-universality of the AQC model. In this section we give a review of their alternative circuit-to-Hamiltonian construction.

Assuming a given circuit consists of L gates acting on n qubits. We represent each qubit $\mu \in \{1,\dots,n\}$ by a $2\times(L+1)$-array of quantum dots which we will subsequently refer to as *dual rail.* Each column i of a dual rail corresponds to a pair of fermionic modes $a_i^\dagger(\mu)$ and $b_i^\dagger(\mu)$. The upper row corresponds to the a modes and the lower rail to the b modes.[5] We assume that we are in a sector where there is exactly one fermion per track the basis states take the form $\prod_{\mu=1}^n c_{i_\mu}^\dagger(\mu)\,|\Omega\rangle$ where $|\Omega\rangle$ is the vacuum state, $c_i^\dagger(\mu) \in \{a_i^\dagger(\mu), b_i^\dagger(\mu)\}$ and $i_\mu \in \{0,\dots,L\}$ for all μ.

Let us first consider the case where the quantum circuit U only acts on a single qubit. This means that we have a single dual rail of quantum dots. The ith step in the computation corresponds to the fermion being at the ith position in the dual rail. The state of the circuit system is given by two complex amplitudes represented in the computational base by $U_i \cdots U_1 |0\rangle =: \alpha_i |0\rangle + \beta_i |1\rangle$. Mizel et al. construct in [25] a Hamiltonian of the fermionic system which has a ground state given by the history state

$$\sum_{i=0}^{L} (\alpha_i a_i^\dagger + \beta_i b_i^\dagger)\,|\Omega\rangle\,. \tag{2.29}$$

For readability we will use the following notation. We put the annihilation operators a_i and b_i into columns

$$C_i = \begin{bmatrix} a_i \\ b_i \end{bmatrix} \tag{2.30}$$

so that we can write for some 2×2-matrix A

$$C_i^\dagger A C_j := A_{1,1} a_i^\dagger a_j + A_{1,2} a_i^\dagger b_j + A_{2,1} b_i^\dagger a_j + A_{2,2} b_i^\dagger b_j. \tag{2.31}$$

The Hamiltonian of the system is given by the sum $H = \sum_{i=1}^{L} H_i$, where

$$H_i = [C_i^\dagger - C_{i-1}^\dagger U_i^\dagger][C_i - U_i C_{i-1}]. \tag{2.32}$$

Each term H_i is positive-semidefinite and therefore the full Hamiltonian H is positive-semidefinite as well. Note that H has a two-degenerate ground state spanned by the history states with initial state $|0\rangle$ and $|1\rangle$.

This model generalizes immediately to the case where we have n non-interacting qubits. The Hamiltonian is then simply the sum of the single qubit Hamiltonians:

$$H = \sum_{\mu=1}^{n} H^\mu = \sum_{\mu=1}^{n} \sum_{i=1}^{L} H_i^\mu \tag{2.33}$$

[5] We could alternatively imagine a physical system where the a and b modes correspond to spin up and spin down on a single line instead.

where H^{μ} acts on dual rail μ.

Note that a system of non-interacting fermions can be simulated efficiently on a classical computer. To achieve quantum computational universality we need to introduce two-qubit interactions such as the controlled NOT (CNOT). Let us assume that at the ith step of the computation there is a CNOT-gate with control qubit c and target qubit t. Then we need to add two terms to the Hamiltonian; one for each state of the control qubit c.

The first case is if the control qubit c is set to 0, i.e. if the fermion in rail c is occupying the a-mode. Then we reward hopping of the control qubit c and the target qubit t between the sites $i-1$ and i and put a penalty on not hopping:

$$H^{\mathrm{I}}_{i,c,t} = [a^{\dagger}_{i}(c)C^{\dagger}_{i}(t) - a^{\dagger}_{i-1}(c)C^{\dagger}_{i-1}(t)][C_i(t)a_i(c) - C_{i-1}(t)a_{i-1}(c)] \tag{2.34}$$

In case the control qubit c is set to 1, i.e. fermion on track c occupies b-mode at position i, we reward the hopping of the target qubit t from 0 at $i-1$ to 1 at i and vice versa:

$$H^{\mathrm{N}}_{i,c,t} = [b^{\dagger}_{i}(c)C^{\dagger}_{i}(t) - b^{\dagger}_{i-1}(c)C^{\dagger}_{i-1}(t)X][C_i(t)b_i(c) - XC_{i-1}(t)b_{i-1}(c)] \tag{2.35}$$

We have not yet ensured that the state of the system always corresponds to a specific step in the algorithm. To prevent cases in which one qubit has gone through a CNOT gate without the other we put an energy penalty for each CNOT gate.

$$H^{\mathrm{P}}_{i,c,t} = \sum_{j=0}^{i-1}\sum_{k=i}^{L} C^{\dagger}_{j}(c)C_j(c)C^{\dagger}_{k}(t)C_k(t) + C^{\dagger}_{j}(t)C_j(t)C^{\dagger}_{k}(c)C_k(c) \tag{2.36}$$

Finally, we add for a CNOT gate at the ith step in the computation on qubits c and t the terms

$$H^{\mathrm{CNOT}}_{i,c,t} = H^{\mathrm{ID}}_{i,c,t} + H^{\mathrm{N}}_{i,c,t} + H^{\mathrm{P}}_{i,c,t} \tag{2.37}$$

to the Hamiltonian.

Chapter 3

Circuit to Hamiltonian construction with multiple times

In this chapter we show that the MLM proposal, introduced in Section 2.7, is equivalent to a circuit-to-Hamiltonian construction, similar to the one defined by Kitaev. However, in the MLM proposal there are only few restrictions on how the fermions are allowed to move along the rails. This corresponds to a model in which qubits can undergo the application of gates independently. As the application of a gate means that we make one step in time this means that qubits can be at different times, so that each qubit has its own "clock".

3.1 Fermionic model

In the original proposal [25] Mizel et. al. considered circuits consisting of single qubit gates and CNOT gates without restrictions on their arrangement. To simplify our analysis we consider a class of circuits over a different gate set and with tight constrictions on the circuit structure.

From now on all gates will be controlled-U (CU) gates. A CU gate acts on two qubits. One is called control (c) and the other target (t). If the qubit c is in the state $|0\rangle$ the gate CU acts as the identity on both c and t. If c is in the state $|1\rangle$ then a specified unitary gate U is applied on t. By introducing ancilla qubits initialized to $|1\rangle$ we can perform any single qubit gate. CNOT is a controlled unitary gate anyway. Thus, we can perform any quantum computation. In general, these circuits will also need ancilla qubits initialized to $|0\rangle$. We will denote the set of ancilla qubits $S = S_0 \cup S_1 \subseteq \{1, \ldots, n\}$ where the ones in S_0 are initialized to $|0\rangle$ and the ones in S_1 are initialized to $|1\rangle$.

Furthermore, we assume that at each layer *all* qubits are coupled to a neighbor in an alternating fashion, by introducing controlled-identity gates if necessary. More precisely we assume that if at time step i the qubits μ and $\mu + 1$ are coupled by a CU gate then at time step $i + 1$ the qubits $\mu - 1$ and μ go through a gate together. Hereby we assume periodic boundary conditions, i.e. we identify qubit 0 with qubit n. Note that there are $D + 1$ time steps where D is the depth of the circuit. We demand that the given circuit fulfilling these restrictions has minimal depth. The restriction to the alternating layout still gives a BQP-universal set of circuits, since any general circuit can be put into this form via SWAP gates, which can be implemented using CNOT gates. Note that introducing the SWAP gates increases the circuit depth only proportional to, and hence polynomial in, n.

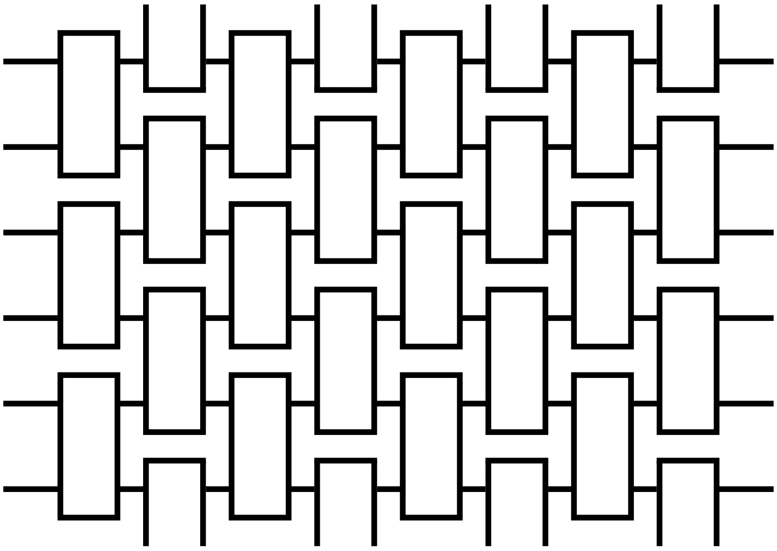

Figure 3.1: Alternating circuit with periodic boundary condition. Each box represents a controlled-U gate and each line is a qubit μ.

Each circuit of the above form is mapped on a Hamiltonian H describing the interactions of n fermions on a 2D lattice of quantum dots, as described in Sec. 2.7. Each fermion is placed in a dual rail which is a $2 \times (D + 1)$ array. The upper row corresponds to the so-called a-modes and the lower row to the b-modes. The columns are labeled by $i \in \{0, \dots D\}$ and each dual rail is labeled by $\mu \in \{1, \dots, n\}$. The Hamiltonian takes the following form:

$$H = H_{in} + H_{out} + H_{prop} + H_{legal} + H_{caus} \tag{3.1}$$

The term H_{in} is meant to enforce the initialization of the ancilla qubits in the input state:

$$H_{in} = \sum_{\mu \in S_0} b_0^\dagger(\mu) b_0(\mu) + \sum_{\mu \in S_1} a_0^\dagger(\mu) a_0(\mu) \tag{3.2}$$

It penalizes the occupation of the $b_0(\mu)$ modes for fermions corresponding to qubits which need to be initialized to $|0\rangle$ and vice versa. As for the output, we have the term

$$H_{out} = a_D^\dagger(q_{out}) a_D(q_{out}) \tag{3.3}$$

which penalizes the output qubit to be in the state $|0\rangle$.

The term H_{prop} defines the propagation of the qubits through the circuit. We have

$$H_{prop} = \sum_{i=1}^{D} \sum_{j=1}^{\frac{n}{2}} H_{prop,i,j} \tag{3.4}$$

where $H_{prop,i,j}$ represents the jth gate at time-step i between the control qubit $c_{i,j}$ and the target qubit $t_{i,j}$. For brevity we will omit the subscripts, if there is no ambiguity. We have $H_{prop,i,j} = H^I_{prop,i,j} + H^U_{prop,i,j}$ with

$$\begin{aligned} H^I_{prop,i,j} =& a_i^\dagger(c) a_i(c) n_i(t) + a_{i-1}^\dagger(c) a_{i-1}(c) n_{i-1}(t) \\ & - \left[a_i^\dagger(c) a_{i-1}(c) \left(a_i^\dagger(t) a_{i-1}(t) + b_i^\dagger(t) b_{i-1}(t) \right) + h.c \right] \end{aligned} \tag{3.5}$$

and

$$\begin{aligned} H^U_{prop,i,j} =& b_i^\dagger(c) b_i(c) n_i(t) + b_{i-1}^\dagger(c) b_{i-1}(c) n_{i-1}(t) \\ & - \Big[b_i^\dagger(c) b_{i-1}(c) \Big(U_{1,1} a_i^\dagger(t) a_{i-1}(t) + U_{1,2} a_i^\dagger(t) b_{i-1}(t) \\ & + U_{2,1} b_i^\dagger(t) a_{i-1}(t) + U_{2,2} b_i^\dagger(t) b_{i-1}(t) \Big) + h.c. \Big] \end{aligned} \tag{3.6}$$

where $n_i(\mu) := C_i^\dagger(\mu) C_i(\mu) = a_i^\dagger(\mu) a_i(\mu) + b_i^\dagger(\mu) b_i(\mu)$ is the number operator for a fermion being on rail μ at site i.

We have

$$H_{legal} = \sum_{\mu=1}^{n} \left(\sum_{i=0}^{D} n_i(\mu) - 1 \right)^2 \tag{3.7}$$

which forces there to be one fermion for every qubit.

Let us define $n_{<j}(\mu) := \sum_{i=0}^{j-1} n_i(\mu)$ and $n_{\geq j}(\mu) := \sum_{i=j}^{D} n_i(\mu)$. In the nullspace $\mathcal{H}_{legal} := \ker(H_{legal})$ we have $n_{\geq j}(\mu) + n_{<j}(\mu) = 1$ as there is one fermion on each rail.

For the causality-term we have $H_{caus} = \sum_{i,j} H_{caus,i,j}$ with

$$H_{caus,i,j} = n_{<i}(c)n_{\geq i}(t) + n_{<i}(t)n_{\geq i}(c). \tag{3.8}$$

This time-ordering penalty $H_{caus,i,j}$ has eigenvalue 0 if and only if $n_{\geq i}(c) = n_{\geq i}(t)$ and both are 0 or 1. Note that H_{legal} and H_{caus} commute with each other and therefore preserve each others eigenspaces.

3.2 Jordan-Wigner transformation

We want to map the fermionic system into a system of qubits (e.g. spin-$\frac{1}{2}$ systems). This can be done using the *Jordan-Wigner transformation* [29]. For fermionic system with modes $c_1, \ldots, c_k$ the Jordan-Wigner transformation into a system of k qubits is defined by the mapping

$$\begin{aligned} c_i^\dagger &\mapsto \left(\bigotimes_{j=1}^{i-1} Z_j \right) \otimes \sigma_i^+ \\ c_i &\mapsto \left(\bigotimes_{j=1}^{i-1} Z_j \right) \otimes \sigma_i^- \end{aligned} \tag{3.9}$$

with $\sigma_i^+ = |1\rangle \langle 0|_i$ and $\sigma_i^- = |0\rangle \langle 1|_i$.

We will label the qubits that we map onto by the dual track μ, the mode a or b and the position on the track i. Note, that the Z_j-operators in Equation 3.9 are problematic since they are non-local. However, for terms of the form $a_i^\dagger(\mu)a_i(\mu)$ and $b_i^\dagger(\mu)b_i(\mu)$ the Zs cancel. Thus the transformed terms

$$H_{in} = \sum_{\mu \in S_0} \sigma_{0,b}^+(\mu)\sigma_{0,b}(\mu) + \sum_{\mu \in S_1} \sigma_{0,a}^+(\mu)\sigma_{0,a}(\mu) = \sum_{\mu \in S_0} P_{0,b}^1(\mu) + \sum_{\mu \in S_1} P_{0,a}^1(\mu) \tag{3.10}$$

and

$$H_{out} = \sigma_{D,a}^+(q_{out})\sigma_{D,a}(q_{out}) = P_{D,a}^1(q_{out}) \tag{3.11}$$

are local.

H_{prop}^{ID} and H_{prop}^{U} consist of terms of the form

$$a_x^\dagger(c)a_y(c)a_p^\dagger(t)a_q(t) \tag{3.12}$$

where x, y, p, q are positions on the 2D-lattice. After the Jordan-Wigner transformation these operators will take the form

$$\mathbf{Z} \otimes \sigma_x^+(c)\sigma_y^-(c)\sigma_p^+(t)\sigma_q^-(t) \tag{3.13}$$

where $\mathbf{Z}$ is a product of Pauli Z operators which by Eqn. 3.9 has no support on y or q. When we consider the qubits of a state in the nullspace of H_{legal}, i.e. qubits which correspond to the positions on a single dual rail μ, then there is exactly one qubit i which is set to $|1\rangle$. From this follows that for any zero-eigenstate of H_{legal} $|\psi\rangle$ we either have $\sigma_x^+(c)\sigma_y^-(c)\sigma_p^+(t)\sigma_q^-(t)\,|\psi\rangle = 0$ or $\mathbf{Z}\,|\psi\rangle = |\psi\rangle$ Thus we will omit all Z-type operators and obtain

$$\begin{aligned} H^I_{prop,i,j} =& P^1_{i,a}(c)\left(P^1_{i,a}(t) + P^1_{i,b}(t)\right) + P^1_{i-1,a}(c)\left(P^1_{i-1,a}(t) + P^1_{i-1,b}(t)\right) \\ &- \left[\sigma^+_{i,a}(c)\sigma^-_{i-1,a}(c)\left(\sigma^+_{i,a}(t)\sigma^-_{i-1,a}(t) + \sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t)\right) + h.c.\right] \end{aligned} \tag{3.14}$$

and

$$\begin{aligned} H^U_{prop,i,j} =& P^1_{i,b}(c)\left(P^1_{i,a}(t) + P^1_{i,b}(t)\right) + P^1_{i-1,b}(c)\left(P^1_{i-1,a}(t) + P^1_{i-1,b}(t)\right) \\ &- \Big[\sigma^+_{i,b}(c)\sigma^-_{i-1,b}(c)\Big(U_{1,1}\sigma^+_{i,a}(t)\sigma^-_{i-1,a}(t) + U_{1,2}\sigma^+_{i,a}(t)\sigma^-_{i-1,b}(t) \\ &+ U_{2,1}\sigma^+_{i,b}(t)\sigma^-_{i-1,a}(t) + U_{2,2}\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t)\Big) + h.c.\Big]. \end{aligned} \tag{3.15}$$

Thus all terms of the Hamiltonian stay local under the Jordan-Wigner transformation.

3.3 Retrieval of a local clock register

In this section we will only consider states in the nullspace of H_{legal} which we will subsequently denote by $\mathcal{H}_{legal} := \ker(H_{legal})$. Remember that for each rail μ there is exactly one qubit which is set to $|1\rangle$. All other qubits are set to $|0\rangle$. The information about the computational state of qubit μ is encoded into the a and b qubits. In this section we will define a unitary transformation U_{clock} which loosely speaking puts the computational information into the a qubit. The b qubit will encode the information about the position of the qubit in the circuit, i.e. its time.

3.3.1 Time transformation of the states

If we choose one of the original qubits $\mu \in \{1, \dots, n\}$ and a time step $i \in \{0, \dots, D\}$ we are dealing with a two qubit system spanned by states $|x\rangle_{a,i,\mu} \otimes |y\rangle_{b,i,\mu}$ with $x, y \in \{0, 1\}$. Qubit a is in state $|1\rangle$ if and only if the original qubit μ is at time i in state $|0\rangle$ and qubit b is $|1\rangle$ if and only if the original qubit μ is at time i in state $|1\rangle$. If the qubit μ

is not at time step i then a and b are both in state $|0\rangle$. The configuration $x = y = 1$ would correspond to an illegal state and does not occur in $\mathcal{H}_{legal}$.

We want to separate the information about the state of the original qubit and its time. To do this we define $U^{i,\mu}_{clock} := \text{CNOT}_{a,b}\text{CNOT}_{b,a}$. The action of $U^{i,\mu}_{clock}$ is

$$\begin{aligned} U^{i,\mu}_{clock} |10\rangle_{ab} &= |01\rangle_{ab} \\ U^{i,\mu}_{clock} |01\rangle_{ab} &= |11\rangle_{ab} \\ U^{i,\mu}_{clock} |00\rangle_{ab} &= |00\rangle_{ab} \end{aligned} \tag{3.16}$$

where $|xy\rangle_{ab}$ stands for $|x\rangle_{a,i,\mu} \otimes |y\rangle_{b,i,\mu}$. After applying $U^{i,\mu}_{clock}$ we can interpret qubit a as the data qubit as its state is equal to the original qubit. The qubit b can be thought of as the time-qubit since it indicates whether the original qubit is at time step i. We define U_{clock} as the time transformation for all qubits

$$U_{clock} := \prod_{i,\mu} U^{i,\mu}_{clock}. \tag{3.17}$$

3.3.2 Time transformed Hamiltonian

For a fixed qubit μ we have

$$\begin{aligned} U_{clock}\sigma^\dagger_a\sigma_a U^\dagger_{clock} &= U_{clock} |1\rangle \langle 1|_a U^\dagger_{clock} \\ &= |0\rangle \langle 0|_a \otimes |1\rangle \langle 1|_b + |1\rangle \langle 1|_a \otimes |0\rangle \langle 0|_b \end{aligned} \tag{3.18}$$

and

$$\begin{aligned} U_{clock}\sigma^\dagger_b\sigma_b U^\dagger_{clock} &= U_{clock} |1\rangle \langle 1|_b U^\dagger_{clock} \\ &= |1\rangle \langle 1|_a \otimes |0\rangle \langle 0|_b + |1\rangle \langle 1|_a \otimes |1\rangle \langle 1|_b . \end{aligned} \tag{3.19}$$

We will do the transformation in detail for the first term in $H_{prop,i,j}$ (see Eqn. (3.14)). For some fixed site i we have

$$\left(P^0_{a,c}P^1_{b,c} + P^1_{a,c}P^0_{b,c}\right)\left(P^0_{a,t}P^1_{b,t} + P^1_{a,t}P^0_{b,t} + P^1_{a,t}P^0_{b,t} + P^1_{a,t}P^1_{b,t}\right) \tag{3.20}$$

Since we only consider the action on legal states of the form $\otimes^n_{i=1} |x_i, t_i\rangle$ terms such as $|1\rangle \langle 1|_{a,c} \otimes |0\rangle \langle 0|_{b,c}$ have zero eigenvalue on this subspace and can thus be omitted. By throwing out such terms we get $P^0_a(c)P^1_b(c)P^1_b(t)$.

For the full propagation Hamiltonian (Eqn. 3.14 and 3.15) we get:

$$\begin{aligned} H^{I}_{prop} =& P^0_{i,a}(c)P^1_{i,b}(c)P^1_{i,b}(t) + P^0_{i-1,a}(c)P^1_{i-1,b}(c)P^1_{i-1,b}(t) \\ & - \Big[P^0_{i,a}(c)\sigma^+_{i,b}(c)P^0_{i-1,a}(c)\sigma^-_{i-1,b}(c) \\ & \times \Big(P^0_{i,a}(t)\sigma^+_{i,b}(t)P^0_{i-1,a}(t)\sigma^-_{i-1,b}(t) + \sigma^+_{i,a}(t)\sigma^-_{i-1,a}(t)\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t)\Big) + h.c.\Big] \end{aligned} \tag{3.21}$$

and

$$\begin{aligned} H^{U}_{prop} =& P^1_{i,a}(c)P^1_{i,b}(c)P^1_{i,b}(t) + P^1_{i-1,a}(c)P^1_{i-1,b}(c)P^1_{i-1,b}(t) \\ & - \Big[\sigma^+_{i,a}(c)\sigma^-_{i-1,a}(c)\sigma^+_{i,b}(c)\sigma^-_{i-1,b}(c) \\ & \times \Big(U_{1,1}P^0_{i,a}(t)P^0_{i-1,a}(t)\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t) + U_{1,2}P^0_{i,a}(t)\sigma^-_{i-1,a}(t)\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t) \\ & + U_{2,1}\sigma^+_{i,a}(t)P^0_{i,a}(t)\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t) + U_{2,2}\sigma^+_{i,a}(t)\sigma^-_{i-1,a}(t)\sigma^+_{i,b}(t)\sigma^-_{i-1,b}(t)\Big) + h.c.\Big]. \end{aligned} \tag{3.22}$$

For $\mu \in \{1, \dots, n\}$ the unitary U_{clock} transforms the former a, b qubits into states of the form

$$|x\rangle \otimes |i\rangle \coloneqq |0\dots0x0\dots0\rangle \otimes |0\dots010\dots0\rangle \in \mathbb{C}^{2^{D+1}} \otimes \mathbb{C}^{2^{D+1}} \tag{3.23}$$

where x is either 0 or 1, depending on the state of the original qubit μ at time i. As the left hand part of the state $|x\rangle$ spans a two-dimensional space we can interpret it as a single qubit. The right hand part spans the space $\mathbb{C}^{D+1}$, representing the time of the qubit. Note that the clock is realized differently than in Kitaev's construction. Here the clock representation consists of a *cursor* 1 which points to the time, instead of a domain wall 10.

We group all data qubits $|x\rangle_\mu$ together and call the corresponding space *data register* $\mathcal{H}_{data}$. Time qubits are in the *time register* $\mathcal{H}_{time}$. Basis states in the data register are labeled by tuples $\mathbf{x} = (x_1, \dots, x_n) \in \{0,1\}^n$ corresponding to the computational states and the time states by tuples $\mathbf{t} = (t_1, \dots, t_n) \in \{0, \dots, D\}^n$ to their respective times.

Combining the two propagating terms we can write $H_{prop,i,j}$ between qubits c and t as

$$\begin{aligned} H_{prop,i,j} =& |t_c = i\rangle\langle t_c = i|\,|t_t = i\rangle\langle t_t = i| \\ & + |t_c = i-1\rangle\langle t_c = i-1|\,|t_t = i-1\rangle\langle t_t = i-1| \\ & - [CU_{c,t} \otimes |t_c = i\rangle\langle t_c = i-1|\,|t_t = i\rangle\langle t_t = i-1| + h.c.] \end{aligned} \tag{3.24}$$

where $|t_c = i\rangle\langle t_c = i| \coloneqq |i\rangle\langle i|_c$ acts on the time register. We used that a controlled-U gate acting on qubits c and t can be written as $|0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes U_t$.

Similarly we obtain

$$H_{in} = \sum_{\mu \in S_0} |1\rangle \langle 1|_\mu \otimes |t_\mu = 0\rangle \langle t_\mu = 0| + \sum_{\mu \in S_1} |0\rangle \langle 0|_\mu \otimes |t_\mu = 0\rangle \langle t_\mu = 0| \tag{3.25}$$

and

$$H_{out} = |0\rangle \langle 0|_{q_{out}} \otimes |t_{q_{out}} = D\rangle \langle t_{q_{out}} = D| \, . \tag{3.26}$$

For H_{caus} we get the same form as in Eqn. (3.8) with

$$n_{<j}(\mu) = \sum_{i=0}^{j-1} I \otimes |t_\mu = i\rangle \langle t_\mu = i| \tag{3.27}$$

and

$$n_{\geq j}(\mu) = \sum_{i=j}^{D} I \otimes |t_\mu = i\rangle \langle t_\mu = i| \, . \tag{3.28}$$

3.4 Change of basis for time-transformed Hamiltonian

In this section wee will only consider states in the subspace $\mathcal{H}_{caus} = \ker(H_{caus} + H_{legal})$, i.e. states with a correct clock register where all qubits obey the causal constraint. Note that H_{caus} commutes with $H_{legal}, H_{prop}, H_{in}$ and H_{out}. Whether a state is a zero eigenstate of H_{caus} solely depends on the configuration of the time register. Those time configurations which belong to a state in $\mathcal{H}_{caus}$ will be called *proper time configurations.* The set of proper time configurations will be denoted by T.

For each proper time configuration $\mathbf{t} = (t_1, \dots, t_n) \in T$ there exists a unique unitary transformation $U_\mathbf{t}$ which is given by the product of all gates that are applied to the data register when going from the initial state $\mathbf{0} = (0, \dots, 0)$ to $\mathbf{t}$.

We define a unitary transformation

$$W := \sum_{\mathbf{t} \in T} U_\mathbf{t} \otimes |\mathbf{t}\rangle \langle \mathbf{t}| \, . \tag{3.29}$$

The action of W on the term H_{out} is:

$$\tilde{H}_{out} = W^\dagger H_{out} W = \sum_{\mathbf{t} :\, t_{q_{out}} = D} U_\mathbf{t}^\dagger |0\rangle \langle 0|_{q_{out}} U_\mathbf{t} \otimes |\mathbf{t}\rangle \langle \mathbf{t}| \tag{3.30}$$

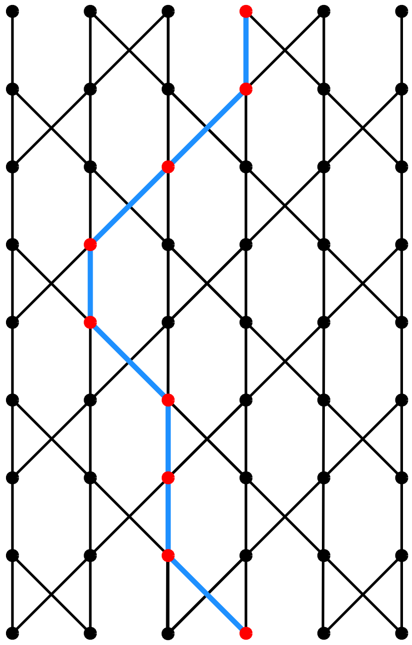

Figure 3.2: Representation of a proper time configurations on a $(n+1) \times (D+1)$-lattice. Each proper time configuration $\mathbf{t} \in T$ is a closed path over the edges of this graph which visits a vertex on each horizontal line once. Each vertex represents the time t_μ for a particular qubit μ and we identify the bottom and top vertices due to the periodic boundary conditions. An edge between two vertices shows that the times of the two qubits obey the causal constraints.

Similarly, the term H_{in} becomes under conjugation with W:

$$\begin{aligned}\tilde{H}_{in} = W^\dagger H_{in} W = &\sum_{\mu \in S_0} \sum_{\mathbf{t}:\, t_\mu = 0} U_{\mathbf{t}}^\dagger \left|1\right\rangle \left\langle 1\right|_\mu U_{\mathbf{t}} \otimes \left|\mathbf{t}\right\rangle \left\langle \mathbf{t}\right| \\ &+ \sum_{\mu \in S_1} \sum_{\mathbf{t}:\, t_\mu = 0} U_{\mathbf{t}}^\dagger \left|0\right\rangle \left\langle 0\right|_\mu U_{\mathbf{t}} \otimes \left|\mathbf{t}\right\rangle \left\langle \mathbf{t}\right|\end{aligned} \tag{3.31}$$

Note that $U_{\mathbf{t}}$ for $\mathbf{t}$ with $t_\mu = 0$ can still be non-trivial, this depends on the interaction structure of the quantum circuit. However, as such unitary $U_{\mathbf{t}}$ does not act on the qubit whose time-coordinate is set to 0, it will drop out, i.e.

$$\tilde{H}_{in} = W^\dagger H_{in} W = \sum_{\mu \in S_0} \sum_{\mathbf{t}:\, t_\mu = 0} \left|1\right\rangle \left\langle 1\right|_\mu \otimes \left|\mathbf{t}\right\rangle \left\langle \mathbf{t}\right| + \sum_{\mu \in S_1} \sum_{\mathbf{t}:\, t_\mu = 0} \left|0\right\rangle \left\langle 0\right|_\mu \otimes \left|\mathbf{t}\right\rangle \left\langle \mathbf{t}\right|. \tag{3.32}$$

Let us check the action of W on $H_{prop,i,j}$ (see Eqn. 3.24). Let

$$Q_{i,j} = \left|i\right\rangle \left\langle i-1\right|_c \otimes \left|i\right\rangle \left\langle i-1\right|_t \tag{3.33}$$

be the time-shift operator at time $i-1$ for qubits c and t. Keep in mind that c and t depend on the time step i and the specific gate j. Each operator $H_{prop,i,j}$ is the sum of four terms. Let us write the action of the conjugation on a hopping-term:

$$W^\dagger \left(CU_{c,t} \otimes |t=i\rangle \langle t=i-1|_c \otimes |t=i\rangle \langle t=i-1|_t \right) W$$

$$\begin{aligned} &= \sum_{\substack{\mathbf{t}'|_{c,t}=i-1 \\ |\mathbf{t}\rangle = Q_{i,j}|\mathbf{t}'\rangle}} U_{\mathbf{t}}^\dagger \mathrm{CU}_{c,t} U_{\mathbf{t}'} \otimes |\mathbf{t}\rangle \langle \mathbf{t}'| \\ &= \sum_{\substack{\mathbf{t}'|_{c,t}=i-1 \\ |\mathbf{t}\rangle = Q_{i,j}|\mathbf{t}'\rangle}} |\mathbf{t}\rangle \langle \mathbf{t}'| \end{aligned} \tag{3.34}$$

In the first step we used that the term

$$|\mathbf{t}\rangle \langle \mathbf{t}| \left(|i\rangle \langle i-1|_c \, |i\rangle \langle i-1|_t \right) |\mathbf{t}'\rangle \langle \mathbf{t}'|$$

is only non-zero if all entries of $\mathbf{t}$ and $\mathbf{t}'$ are identical except that at the entries for c and t we have $i-1$ in $\mathbf{t}'$ and i in $\mathbf{t}$. In the second step we used that $U_{\mathbf{t}}$ and $U_{\mathbf{t}'}$ consist of the same unitary gates except for an additional $\mathrm{CU}_{c,t}$ in $U_{\mathbf{t}}$, i.e. $U_{\mathbf{t}}^\dagger U_{\mathbf{t}'} = \mathrm{CU}_{c,t}$.

The conjugation of the other terms proceeds analogously, so that we obtain:

$$\begin{aligned} \tilde{H}_{prop,i,j} = &\sum_{\mathbf{t}|_{c,t}=i} |\mathbf{t}\rangle \langle \mathbf{t}| + \sum_{\mathbf{t}|_{c,t}=i-1} |\mathbf{t}\rangle \langle \mathbf{t}| \\ &- \sum_{\substack{\mathbf{t}'|_{c,t}=i-1 \\ |\mathbf{t}\rangle = Q_{i,j}|\mathbf{t}'\rangle}} |\mathbf{t}\rangle \langle \mathbf{t}'| - \sum_{\substack{\mathbf{t}'|_{c,t}=i-1 \\ |\mathbf{t}\rangle = Q_{i,j}|\mathbf{t}'\rangle}} |\mathbf{t}'\rangle \langle \mathbf{t}| \end{aligned} \tag{3.35}$$

and $\tilde{H}_{prop} = \sum_{i,j} \tilde{H}_{prop,i,j}$.

3.5 Making constraints local

When we constructed the Hamiltonian in the previous sections we had to impose restrictions on the time configurations of the states to prevent that one qubit has gone through a gate without its partner. However these restrictions are non-local on the lattice. In this section we will fix this problem.

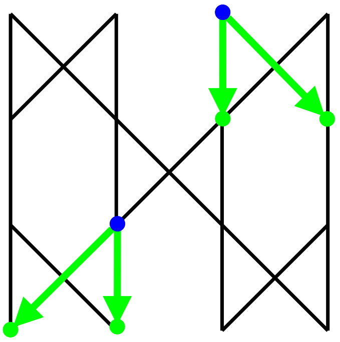

FIGURE 3.3: If the time of a qubit is at one of the blue positions then we know that the next qubit has to be at one of the positions indicated by the green arrow.

For H_{caus} we make use of the alternating structure of the circuit. The idea is that a qubit can not be more than one step ahead of the other one without breaking the causality constraint. This can easily be seen in Figure 3.3: Two neighboring qubits have to be both either before or after a gate where they interact. By checking all neighbor positions for all qubits we can ensure that no qubit passed a gate without its partner.

Note that we enumerate the qubits from 1 to n and the times from 0 to D and that for each time i the interaction is either with the left or with the right partner qubit. We assume that at time 0 the qubits 1 and 2 interact. Furthermore we identify $\mu = n + 1$ with $\mu = 1$ and we set $n_i = 0$ for $i = -1$ and $i = D + 1$.

$$\begin{aligned} H_{caus} =& \sum_{\mu=1}^{n} \sum_{\substack{i=0 \\ i+\mu \text{ even}}}^{D} n_i(\mu)\left[1 - (n_{i+1}(\mu+1) + n_i(\mu+1))\right] \\ &+ \sum_{\mu=1}^{n} \sum_{\substack{i=0 \\ i+\mu \text{ odd}}}^{D} n_i(\mu)\left[1 - (n_{i-1}(\mu+1) + n_i(\mu+1))\right] \end{aligned} \tag{3.36}$$

3.6 Construction via domain wall clock

We have seen in Section 3.3 that transforming the model of interacting fermions gives rise to a *cursor clock* where a single qubit is in the state $|1\rangle$ and serves as a pointer indicating the time. The transition from one time to the next in H_{prop} is implemented 2-locally by terms of the form $|t\rangle\langle t-1| = |01\rangle\langle 10|_{t-1,t}$. However, the pulse clock requires initialization and can not be used for a QMA-proof without further ado (see Sec. 5.3). Hence, we will adopt the *domain wall clock* implementation where the time is determined by the position of the domain wall 10 (see Eqn. 2.17).

For a fixed single qubit μ the overall time states are

$$\begin{aligned}
|t_\mu = 0\rangle &= |t_1\rangle \otimes \cdots \otimes |00\ldots0\rangle_\mu \otimes \cdots \otimes |t_n\rangle \\
|t_\mu = 1\rangle &= |t_1\rangle \otimes \cdots \otimes |10\ldots0\rangle_\mu \otimes \cdots \otimes |t_n\rangle \\
&\vdots \\
|t_\mu = D\rangle &= |t_1\rangle \otimes \cdots \otimes |11\ldots1\rangle_\mu \otimes \cdots \otimes |t_n\rangle\,.
\end{aligned} \tag{3.37}$$

A time configuration is legal if and only if the sequence 01 never occurs. We can check the legality of the time register locally by introducing the following 2-local terms into our Hamiltonian:

$$H_{legal} = \sum_{\mu=1}^{n} \sum_{i=0}^{D+1} |0\rangle\langle 0|_{\mu,i} \otimes |1\rangle\langle 1|_{\mu,i+1} \tag{3.38}$$

For $\tilde{H}_{out}$ we can replace $|t_q = D\rangle\langle t_q = D|$ by $|1\rangle\langle 1|_{q_{out},D}$ which gives us 2-local terms:

$$\tilde{H}_{out} = \sum_{\mathbf{t}\colon \mathbf{t}|_{q_{out}}=D} U_{\mathbf{t}}^{\dagger} |0\rangle\langle 0|_{q_{out}} U_{\mathbf{t}} \otimes |1\rangle\langle 1|_{q_{out},D} \tag{3.39}$$

Similarly we get for $\tilde{H}_{in}$:

$$\tilde{H}_{in} = \sum_{\mu\in S_0} |1\rangle\langle 1|_\mu \otimes |0\rangle\langle 0|_{\mu,0} + \sum_{\mu\in S_1} |0\rangle\langle 0|_\mu \otimes |0\rangle\langle 0|_{\mu,0} \tag{3.40}$$

For the causality constraint we introduce the following term in the Hamiltonian:

$$\begin{aligned}
H_{caus} = &\sum_{\mu+i \text{ even}} c_i(\mu)\,(I - (c_{i+1}(\mu+1)) + c_i(\mu+1)) \\
+ &\sum_{\mu+i \text{ odd}} c_i(\mu)\,(I - (c_{i-1}(\mu+1) + c_i(\mu+1))
\end{aligned} \tag{3.41}$$

where

$$c_i(\mu) \coloneqq |1\rangle\langle 1|_{\mu,i} \otimes |0\rangle\langle 0|_{\mu,i+1} \tag{3.42}$$

acts on the time register.

Let $\mathbf{t}$ be a legal time configuration and $\mathbf{t}'$ the time configuration which is equal to $\mathbf{t}$ except that two qubits μ and $\mu+1$ go through a gate such that $\mathbf{t}'_\mu = \mathbf{t}'_{\mu+1} = i+1$. We can substitute the following terms in H_{prop} from Eqn. 3.24:

$$|\mathbf{t}'\rangle\langle \mathbf{t}| = |110\rangle\langle 100|_{\mu,i,i+1,i+2} \otimes |110\rangle\langle 100|_{\mu+1,,i,i+1,i+2} \tag{3.43}$$

Since H_{prop} additionally acts on two qubits in the data register $\mathcal{H}_{data}$ it becomes 8-local compared to 5-local in Kitaev's construction.

Chapter 4

Propagation graph

When we prove the QMA-completeness of the problem Local Hamiltonian with the multi-time construction we need to lower bound the gap between the two lowest eigenvalues of H_{prop} in the subspace $\mathcal{H}_{caus} := \ker(H_{legal} + H_{caus})$. This can be done by analyzing how the proper time configuration are connected. In previous constructions [2, 4, 10, 19–21, 28, 31] this connection is trivial, since there is only one "global" time $t \in \{0, \ldots, L\}$ corresponding to the application of gates. Each time t can be reached by its predecessor and its successor by applying the gate U_t respectively $U_{t+1}^{\dagger}$.

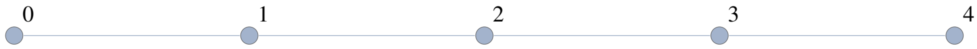

Figure 4.1: The connection between global time steps in a circuit U of size L can be represented by the path graph of lenght $L + 1$.

In the "local time model" however the qubits can go through gates independent of each other as long as they respect causality; no qubit can go through a two-qubit gate without its partner. This makes the connections between the time configurations quite complex as some qubits can be further ahead preventing the propagation of other qubits (see Fig. 4.2).

In this chapter we introduce a family of graphs $G_{n,D}$ which correspond to the controlled-U quantum circuits with alternating structure which we defined at the beginning of Section 3.1. We show how these graphs provide means to analyze the spectrum of the term H_{prop}.

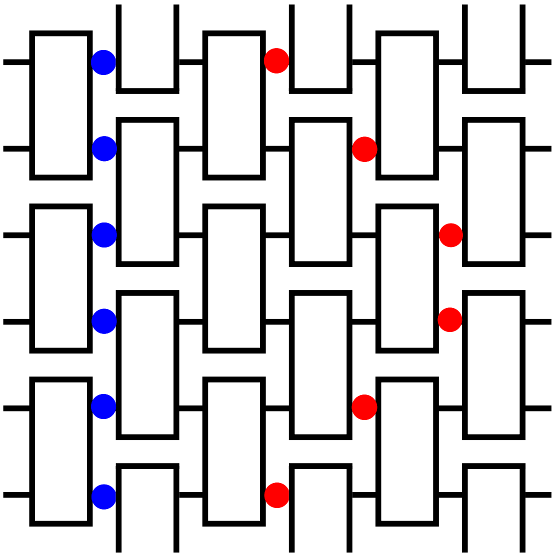

FIGURE 4.2: For the blue qubits there are $n = 6$ gates which can be applied ($\frac{n}{2}$ forward, $\frac{n}{2}$ backward). Therefore the corresponding time configuration is connected to n other time configurations. On the other hand the red qubits can only move to two configurations: One where the first two go backwards or the last two go forwards.

4.1 Definition and properties

Let n be the number of qubits of the circuit U and D its depth. W.l.o.g. we assume that n and D are even and that at the first layer of gates qubits 1 and 2 interact. We define the *propagation graph* $G_{n,D}$ as a graph which has the proper time configuration as vertex set $V = T$ and two vertices $\mathbf{t} \neq \mathbf{t}'$ are connected if there exists a term in the Hamiltonian $\tilde{H}_{prop}$ which maps $|\mathbf{t}\rangle$ to $|\mathbf{t}'\rangle$. In other words, $\mathbf{t}$ and $\mathbf{t}'$ are connected by an edge if $\mathbf{t}'$ only differs from $\mathbf{t}$ by a two-qubit jump through a gate. Since H_{prop} is Hermitian the graph $G_{n,D}$ is *undirected*. In the trivial case where the circuit consists of only two qubits $n = 2$ the propagation graph is simply a path graph of length $D + 1$. However, for larger n the propagation graph will have a much more complicated structure due to the causality constraint.

Let us analyze some of the basic properties of the propagation graphs. The amount of incident edges connecting to a vertex $\mathbf{t}$ is called the *degree* $\deg(\mathbf{t})$. We note that the *synchronized* time configurations which are not the initial or final configuration, i.e. $\mathbf{i} = (i, \dots, i)$ with $i \in \{1, \dots, D - 1\}$, have the maximal degree since all qubits can go through all available gates, i.e. we have

$$\max_{\mathbf{t} \in T} \deg(\mathbf{t}) = n. \tag{4.1}$$

One might suspect that there are cases in which the times of the qubits are arranged in such a way that no hopping is possible, for example when the times for all qubits are different. Such states would not be penalized by H_{prop} and appear as isolated vertices in $G_{n,D}$. The following lemma states that these configurations do not occur, as all qubits interact with some other qubit at all times.

Lemma 4.1. For all proper time configurations it is always possible to jump to another proper time configuration.

Proof. Let $\mathbf{t} \in T - \{\mathbf{D}\}$ be a proper time configuration and let $\mu \in \{1, \dots, n\}$ be a qubit such that its time $t_\mu \leq t_\eta$ for all other qubits $\eta \neq \mu$. Because all qubits interact with some other qubit at all times there is a qubit ν which interacts with μ for $t_\mu \to t_\mu + 1$. Since $\mathbf{t}$ is a proper configuration we have $t_\nu \leq t_\mu$. By choice of μ we thus have $t_\mu = t_\nu$. ■

From the proof it is immediately clear that from all proper time configurations we can reach the final configuration $\mathbf{D}$. Thus we have the following corollary.

Corollary 4.2. All propagation graphs $G_{n,D}$ are *connected*, i.e. there exists a path between any two vertices.

It is also clear from the proof of Lemma 4.1 that for a proper time configuration $\mathbf{t} \neq \mathbf{0}$ we could have chosen a qubit μ with time $t_\mu \geq t_\eta$ for all $\eta \neq \mu$ giving us a partner qubit to apply a gate in reverse $t_\mu \to t_\mu - 1$. Note that for $n \geq 4$ the time configurations $\mathbf{0}$ and D have a degree ≥ 2. This shows that for $n \neq 2$ the minimal degree is given by

$$\min_{\mathbf{t} \in T} \deg(\mathbf{t}) = 2. \tag{4.2}$$

The length of the shortest cycle of the graph is called *girth* g and we have that all propagation graphs have girth $\mathrm{g}(G_{n,D}) = 4$ for $n \geq 2$. For example the configurations $(0,0,0,0,\dots), (1,1,0,0,\dots), (1,1,1,1,\dots)$ and $(0,0,1,1,\dots)$ form a cycle of length 4.[1] To see why this is the minimal cycle length assume that we are given a cycle consisting of the three non-equal vertices $\mathbf{t}^1, \mathbf{t}^2, \mathbf{t}^3$. We further assume w.l.o.g. that $\mathbf{t}^2$ is equal to $\mathbf{t}^1$ except that the first two entries are incremented by 1. Since $\mathbf{t}^2$ and $\mathbf{t}^3$ are connected they differ in exactly two neighboring entries $\mu, \mu + 1$. Due to the causality constraint and our assumption that the gates of the circuit alternate (see Fig. 3.1 and 4.2) we know that either μ or $\mu + 1$ is not one of the first two entries. Hence $\mathbf{t}^1$ and $\mathbf{t}^3$ must differ in at least 3 of their entries and can therefore not be connected.

A connected graph is called *multipartite* with k partitions if we can find k disjoint subsets of vertices $S_i \subseteq V$ such that $(S_i \times S_i) \cap E = \emptyset$ for all $i \in \{0, \dots, k-1\}$. All $G_{n,D}$ are multipartite with $k = \frac{nD}{2} + 1 = L + 1$ partitions. Each partition S_i is given by the set of time configurations $\mathbf{t}$ with $\frac{1}{2}\sum_{j=1}^{n} t_j = i$, i.e. a time configuration in which i gates

[1] All other entries must be equal or else they would not be connected by an edge.

were applied or equivalently a vertex in $G_{n,D}$ where the distance to $\mathbf{0}$ is i. Note that all propagation graphs are symmetric under the the mapping

$$\phi : T \to T,\ (t_1, \ldots, t_n) \mapsto (D - t_2, \ldots, D - t_n, D - t_1). \tag{4.3}$$

To see this assume $\mathbf{t} = (t_1, \ldots, t_n)$ and $\mathbf{t}' = (t'_1, \ldots, t'_n)$ are connected by an edge. This implies that there is a gate acting on qubits μ and $\mu + 1$ such that w.l.o.g. $t'_\mu = t'_{\mu+1} = t_\mu + 1 = t_{\mu+1} + 1$ and $t'_\nu = t_\nu$ for all $\nu \neq \mu, \mu + 1$. Hence,

$$\begin{aligned} \phi(\mathbf{t})_{\mu-1} &= D - t_\mu = D - t'_\mu + 1 = \phi(\mathbf{t}')_{\mu-1} + 1 \\ \phi(\mathbf{t})_\mu &= D - t_{\mu+1} = D - t'_{\mu+1} + 1 = \phi(\mathbf{t}')_\mu + 1 \end{aligned} \tag{4.4}$$

and $\phi(\mathbf{t}')_\nu = \phi(\mathbf{t})_\nu$ for all $\nu \neq \mu - 1, \mu$. Since D is even we know that the time $D - t' + 1$ is odd if and only if t' is even and vice versa. By the alternating structure of the circuit we know that there exists a gate acting on $\mu - 1$ and μ and thus $\phi(\mathbf{t})$ and $\phi(\mathbf{t})$ are connected by an edge in the propagation graph. Since ϕ is a bijection this proves the claim that $(\mathbf{t}, \mathbf{t}') \in E$ if and only if $(\phi(\mathbf{t}), \phi(\mathbf{t}')) \in E$.

From the above follows that for $i \in \{0, \ldots, L\}$ and $\mathbf{t} \in T$ with $\frac{1}{2}\sum_{j=1}^n t_j = i$ we have

$$\frac{1}{2}\sum_{j=1}^{n} \phi(\mathbf{t})_j = \frac{nD}{2} - \frac{1}{2}\sum_{j=1}^{n} t_j = L - i \tag{4.5}$$

and therefore

$$|S_i| = |S_{L-i}|. \tag{4.6}$$

4.2 Spectral graph theory

We will now establish the connection between $G_{n,D}$ and H_{prop}. Let us first consider some undirected graph $G = (V, E)$ with $N = |V|$. We can define a discrete equivalent of the Laplace operator $\mathrm{L}(G) \in \mathbb{Z}^{N \times N}$ by setting

$$\mathrm{L}(G)_{v,u} = \begin{cases} \deg(v) & v = u \\ -1 & (v, u) \in E \\ 0 & \text{else.} \end{cases} \tag{4.7}$$

The rows and columns of the matrix are labeled by the vertices of the graph. Since G is undirected $\mathrm{L}(G)$ is symmetric and has real eigenvalues.

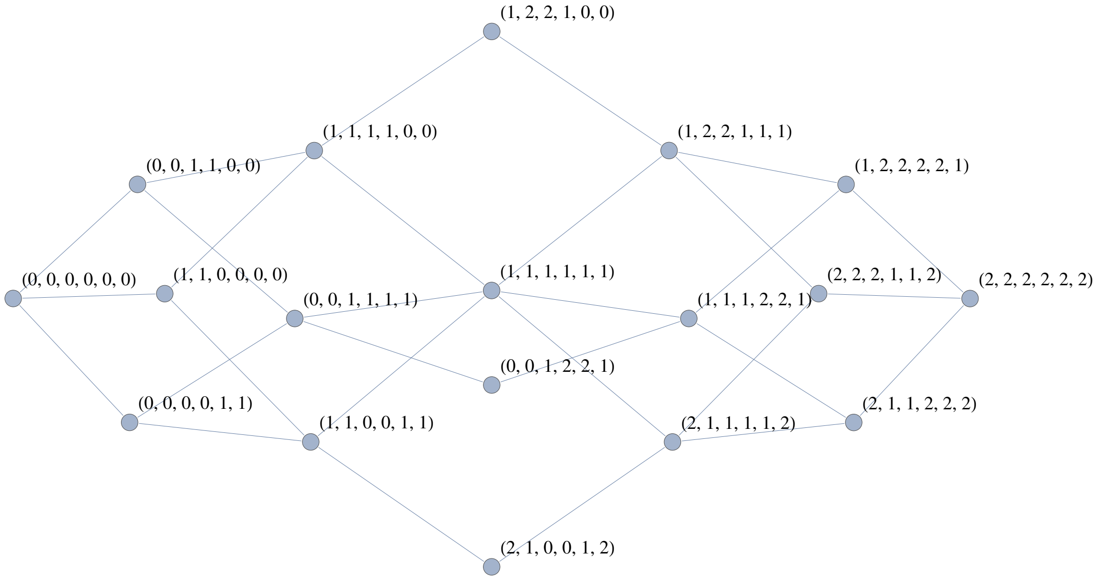

FIGURE 4.3: The graph $G_{n,D}$ for $n = 6$ and $D = 2$.

The Laplace matrix $\mathrm{L}(G)$ describes how the vertices in a graph G are connected. We have already encountered the Laplace matrix of the path graph (Fig. 4.1) in Section 2.6.2 as the generator of a continuous-time quantum walk.

It holds that $\tilde{H}_{prop} = \sum_{\mathbf{t},\mathbf{t}' \in T} \mathrm{L}(G_{n,D})_{\mathbf{t},\mathbf{t}'} \left|\mathbf{t}\right\rangle \left\langle\mathbf{t}'\right|$, i.e. $\tilde{H}_{prop}$ can be represented by the matrix $\mathrm{L}(G_{n,D}) \in \mathbb{Z}^{N \times N}$. This means that the spectrum of $\mathrm{L}(G_{n,D})$ is equal to the spectrum of H_{prop}. We know that H_{prop} is positive semidefinite which is a property all Laplace matrices share. It follows directly from the Courant-Fischer theorem.

Theorem 4.3 (Courant-Fischer). Let G be an undirected graph with N vertices and $x \in \mathbb{R}^N$. It holds that

$$x^{\mathrm{tr}} L(G) x = \sum_{(v,u) \in E} (x_v - x_u)^2. \tag{4.8}$$

By means of Theorem 4.3 we get the following result about the nullspace of the Laplacian matrix.

Lemma 4.4. The nullspace of $\mathrm{L}(G)$ for a connected graph G is non-degenerate and spanned by the ones vector $(1, \ldots, 1)^{\mathrm{tr}}$.

Proof. Let $x \in \ker(\mathrm{L}(G))$ be a vector from the nullspace of $\mathrm{L}(G)$. Due to Theorem 4.3 we have that $0 = \sum_{(v,u) \in E} (x_v - x_u)^2$ from which follows, that $x_u = x_v$ for all $(u, v) \in E$. Since G is connected, all entries of x must be equal and therefore x is a scalar multiple of $(1, \ldots, 1)^{\mathrm{tr}}$. ■

Combining Corollary 4.2 and Lemma 4.4 we get that all ground states of $\tilde{H}_{prop}$ have the form

$$|\eta\rangle = |\xi\rangle \otimes \frac{1}{\sqrt{N}} \sum_{\mathbf{t}\in T} |\mathbf{t}\rangle \tag{4.9}$$

where $|\xi\rangle \in \mathbb{C}^{2^n}$ is some state in the data register.

As $G_{n,D}$ is multipartite we get that the corresponding Laplacian $\mathrm{L}(G_{n,D})$ is a tridiagonal block matrix

$$\mathrm{L}(G_{n,D}) = \begin{bmatrix} D_0 & A_{0,1} & & \\ A_{1,0} & D_1 & A_{1,2} & \\ & A_{2,1} & D_2 & \ddots \\ & & \ddots & \ddots \end{bmatrix} \tag{4.10}$$

where each D_i is a diagonal matrix with entries $\deg(\mathbf{t})$ for all $\mathbf{t} \in S_i$.

We are interested in how the gap between the lowest two eigenvalues of H_{prop} scales depending on the number of qubits n and the circuit depth D. As the first eigenvalue of H_{prop} is 0 the gap is given by the second lowest eigenvalue λ_2. The value of λ_2 intuitively tells us how well the graph is connected and is therefore called *algebraic connectivity*. An eigenvector associated to the algebraic connectivity is called *Fiedler vector*. From Theorem 4.3 we get an explicit formula for λ_2:

$$\lambda_2 = \min_{\substack{x\neq 0\\ x\perp \mathbf{1}}} \frac{x^{\mathrm{tr}} L x}{x^{tr}\cdot x} = \min_{\substack{x\neq 0\\ x\perp \mathbf{1}}} \frac{\sum_{(\mathbf{t},\mathbf{t}')\in E}(x_{\mathbf{t}} - x_{\mathbf{t}'})^2}{\sum_{\mathbf{t}\in T} x_{\mathbf{t}}^2} \tag{4.11}$$

Unfortunately the combinatorics involved to compute T and the edge relation E for $G_{n,D}$ is very complex which prevents us from directly using Equation 4.11.

Finding bounds for the algebraic connectivity is of great interest in general as it has applications in the construction of computer networks, random walks, partitioning of graphs, etc. (more background information can be found in [6]). There are many known inequalities for the algebraic connectivity which involve general properties of the graph such as the number of vertices, girth, diameter and the minimal degree (for a good survey see [26]). Unfortunately all lower bounds of this kind known to us are exponential in n and D when applied to $\mathrm{L}(G_{n,D})$.

A better bound on the algebraic connectivity λ_2 of a graph G can be obtained using the *Cheeger constant* $\mathrm{h}(G)$ which is equal to

$$\mathrm{h}(G) \coloneqq \min_{\substack{X \subseteq V \\ 0 < |X| \leq \frac{|V|}{2}}} \frac{|\partial X|}{|X|} \tag{4.12}$$

where $\partial X \coloneqq \{(v,u) \in E \mid v \in X, u \in V - X\}$ is the edge boundary of X. The quotient $\frac{|\partial X|}{|X|}$ can be interpreted as the average boundary degree of X. Intuitively, the Cheeger constant tells us how easy it is to disconnect a large part of the graph. Equivalently we could also say that the Cheeger constant tells us if there are any "bottlenecks" in the graph, due to the max-flow min-cut theorem [27].

Theorem 4.5 (Cheeger inequalities). Let $G = (V, E)$ be a graph. It holds that

$$\frac{\lambda_2}{2} \leq \mathrm{h}(G) \leq \sqrt{2\lambda_2 \max_{v \in V} \deg(v)}. \tag{4.13}$$

Using Eqn. 4.1, the Cheeger inequalities provide the following lower bound on the second lowest eigenvalue of $\mathrm{L}(G_{n,D})$:

$$\frac{\mathrm{h}(G_{n,d})^2}{2n} \leq \lambda_2 \tag{4.14}$$

For both, classical random walks and the continuous-time quantum walks, the spectral gap and the Cheeger constant determine how fast the limiting distribution is reached [1, 18]. This is intuitively clear since both are a measure for how well the graph is connected and random walks converge faster if there are no bottlenecks.

Computing or lower bounding the Cheeger constant for the time propagation graphs $G_{n,D}$ is not trivial and we have not been successful in doing so. However, it appears to be the most promising strategy to obtain a lower bound on the gap of H_{prop}.

4.3 Bounds on time configurations

In this section we will give bounds on the number of proper time configurations N, as well as the number of proper time configurations for which the output qubit q_{out} is at the final position D. Note that for the number of time configurations it does not matter which qubit we fix, due to the periodic boundary condition. Also it does not matter if we fix the time to be D or 0. Thus we will call the number of these time configurations N_{bound}.

Upper bound on the total number of proper time configurations

Remember that the time configurations correspond to paths on the lattice in Figure 3.2. To simplify the analysis we will assume that the lattice has infinite width. If we want to draw a path starting at the top of the graph we see that after each step we always have two different choices which we will mark with the letters X and Y: either we go left (Y) and straight (X) or straight (Y) and right (X), i.e. the leftmost choice is Y and the rightmost choice is X. We assume w.l.o.g. that we start from a position from which we can go left or straight and that the first choice is going straight.[2] Without any further restrictions we have simply 2^{n-1} paths which correspond to the words in $\{X, Y\}^{n-1}$. However, we want the alignment of the qubits to be periodic, i.e. the nth qubit should be a neighbor the first qubit. This means that the paths we consider need to come back to the same vertical position after n steps. Therefore the number of X in the word must be equal to the number of Y in the word. This restriction is necessary but not sufficient since every X coming after Y and vice versa is a straight line (see Fig. 4.4). Therefore words which end with an X will end up one step left of where we started, as the first step was an X.[3] Hence, the number of paths is equal to the number of all the words in $\{X, Y\}^n$ which begin with X and end with Y and have the same number of X and Y. This is the same as saying we choose $\frac{n-2}{2}$ positions in the word where we put X and the rest is filled up with Y. Therefore the number of proper time configurations in which we fix the time of two neighboring qubits is upper bounded by the binomial $\binom{n-2}{\frac{n}{2}-1}$. The exact number will be smaller as we did not consider the case where we reach the left or right boundary of the lattice.

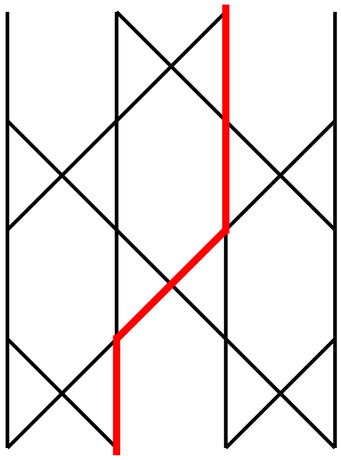

Figure 4.4: Path corresponding to the word $XYYX$.

[2] This is not a restriction since every proper time configuration must have at least two qubits being at the same time.

[3] If we had a word of the form $Y \dots Y$, where the first Y stands for going straight, we would correspondingly end up one step to the right.

To upper bound the total number of time configurations N we take the bound for the number of paths times all possible starting positions of which there are nD many:

$$N \leq nD \cdot \binom{n-2}{\frac{n}{2}-1} \tag{4.15}$$

Lower bound on the number of output configurations

To get the time configurations which lie at the border we can only allow those paths in Figure 3.2 which stay on one side of the starting position. In terms of words from $\{X, Y\}^n$ this means that in addition to the restrictions that we had for the unbounded time configurations we need to restrict to those words in which every initial segment has more Xs than Ys. Note that by fixing the time of one qubit to be at time D the minimal possible time of a proper time configuration is $D - \frac{n}{2}$ due to the periodic boundary condition of the circuit. Hence, we assume that $D \geq \frac{n}{2}$ as all input qubits should contribute to the outcome of the circuit.

To simplify our analysis, let us instead of the lattice from Fig. 3.2 and Fig. 4.4 consider a $k \times k$ square lattice with $k = \frac{n}{2}$ where we go from the lower left corner $(0, 0)$ to the upper right corner (k, k). Now, each occurrence of X shall correspond to going right and each Y shall correspond to going up. Then the restriction that each initial word has more Xs than Ys corresponds to a path on the square lattice going from $(0, 0)$ to (k, k) which never crosses the diagonal.

Theorem 4.6. The number of paths which only move in $(1, 0)$ or $(0, 1)$ direction on a $k \times k$ square lattice which stay below the diagonal connecting $S = (0, 0)$ and $E = (k, k)$ is given by:

$$C_k := \frac{1}{k+1}\binom{2k}{k} \tag{4.16}$$

Proof. First, to count the overall number of possible paths from S to any point (r, s) we observe that by choosing the positions for each move to the right, of which there are r many, we already determine the path as we are forced to fill up all other s positions by moves which go upward. Thus the total number of paths is given by:

$$\binom{r+s}{r} = \binom{r+s}{s} \tag{4.17}$$

Let us now consider a path going from S to E that does cross the diagonal. Let P be the first point of this path which is above the diagonal. We can construct a second path by reflecting all steps which come after the point P (see Fig. 4.5). The newly constructed path will then end at position $Q = (k - 1, k + 1)$. This gives us a bijection between all the paths on a $n \times n$ lattice which cross the diagonal and all paths on a $(k-1) \times (k+1)$ lattice. The number of paths which do not cross the diagonal is thus given by the total number on a $k \times k$ lattice subtracted by the number of paths on a $(k-1) \times (k+1)$ lattice:

$$\binom{2k}{k} - \binom{2k}{k-1} = \frac{(2k)!}{(k!)^2} - \frac{(2k)!}{(k-1)!(k+1)!} = \frac{1}{k+1}\binom{2k}{k} \tag{4.18}$$

■

The numbers C_k are also known as *Catalan numbers* [16, 23]. The proof is from [23].

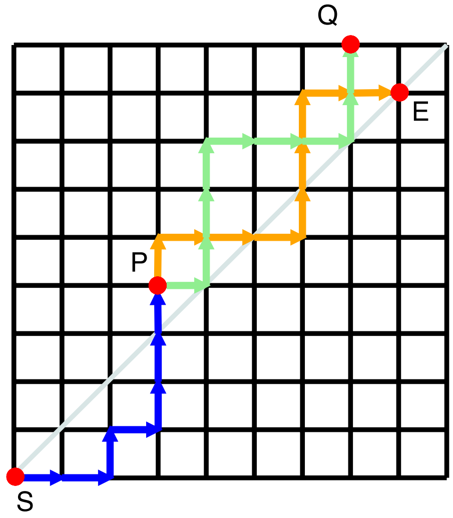

FIGURE 4.5: Reflection priciple: The blue-orange path going from S to E crosses the diagonal at point P. It can be mapped onto the blue-green path which connects the points S and Q.

Thus the number of proper time configurations in a circuit with n qubits and depth $D \geq \frac{n}{2}$ with one qubit fixed at time 0 or time D is given by the Catalan number

$$C_{\frac{n}{2}} = \frac{1}{\frac{n}{2}+1}\binom{n}{\frac{n}{2}}. \tag{4.19}$$

Lower bound on the fraction of output configurations

The following lemma provides a lower bound on the ratio between the number of output configurations N_{bound} and the total number of proper time configurations N, needed for proving QMA-completeness with the multi-time construction in Chapter 5.

Lemma 4.7. Let N be the total number of proper time configurations and N_{bound} the number of proper time configurations where we fix the time of one qubit to be at time

D then the quotient of these numbers can be lower bounded as follows:

$$\frac{N_{bound}}{N} \geq \frac{4\sqrt{2}}{n^{\frac{3}{2}}(n+2)D} \tag{4.20}$$

Proof. We have

$$N_{bound} = \frac{1}{\frac{n}{2}+1}\binom{n}{\frac{n}{2}} \geq \frac{1}{\frac{n}{2}+1}\frac{2^{n-1}}{\sqrt{\frac{n}{2}}} \tag{4.21}$$

due to Stirling's approximation [33]. We can upper bound the number of total time configurations by

$$N \leq nD \cdot \binom{n-2}{\frac{n}{2}-1} \leq nD \cdot 2^{n-2} \tag{4.22}$$

which gives the result. ■

Note, that the fraction of output configurations in Kitaev's model is given by $\frac{1}{L+1}$. It corresponds to the probability of obtaining the final outcome of a computation in the AQC-equivalence proof (Sec. 2.6.1) and in dynamical Hamiltonian quantum computation (Sec. 2.6.2).

Chapter 5

QMA Reduction

We show that using the multi-time construction defined in Chapter 3 we can prove QMA-completeness of the Local Hamiltonian problem. In Sec. 5.3 we use an idea from Kempe and Regev [20] to reduce the locality of the Hamiltonian from 8-local to 4-local. However, this method makes penalty terms in the constructed Hamiltonian dependent on the circuit size.

5.1 Completeness

Completeness for a reduction means that all accepting instances of one problem correspond to accepting instances of the other. In our case this means that if the circuit outputs 1 with probability $p_1 \geq 1 - \epsilon$ then H and equivalently $\tilde{H}$ must have a small eigenvalue.

Let $|\gamma\rangle$ be a quantum witness and U rejects $|\gamma\rangle$ with a probability lower than ϵ. We define

$$|\tilde{\eta}\rangle \coloneqq \frac{1}{\sqrt{N}} \sum_{\mathbf{t} \in T} |\gamma, \mathbf{0}, \mathbf{1}\rangle \otimes |\mathbf{t}\rangle \tag{5.1}$$

and give an upper bound a on $\langle\tilde{\eta}| \tilde{H} |\tilde{\eta}\rangle$. Since all auxiliary qubits are initialized correctly it is easy to see that $\tilde{H}_{in} |\tilde{\eta}\rangle = 0$. The state $|\tilde{\eta}\rangle$ has the same form as given in Eqn. 4.9 and thus $\tilde{H}_{prop} |\tilde{\eta}\rangle = 0$. Because we sum over all time configurations in T we also have $(H_{legal} + H_{caus}) |\tilde{\eta}\rangle = 0$.

Finally, using Eqn. 3.30, we get

$$\begin{aligned}\langle\tilde{\eta}|\,\tilde{H}_{out}\,|\tilde{\eta}\rangle &= \frac{1}{N}\sum_{\mathbf{t}\colon\,\mathbf{t}|_{q_{out}}=D}\langle\gamma,\mathbf{0},\mathbf{1}|\,U_{\mathbf{t}}^{\dagger}\,|0\rangle\,\langle 0|_{q_{out}}\,U_{\mathbf{t}}\,|\gamma,\mathbf{0},\mathbf{1}\rangle\\ &= \frac{1}{N}\sum_{\mathbf{t}\colon\,\mathbf{t}|_{q_{out}}=D}\Pr(U\text{ rejects }|\gamma\rangle) \qquad (5.2)\\ &\leq \frac{N_{bound}}{N}\epsilon\end{aligned}$$

where $N_{bound} := |\{\mathbf{t}\in T \mid t_{q_{out}} = D\}|$. Note that for the proper time configurations $\mathbf{t}$ with $t_{q_{out}} = D$ the operators $U_{\mathbf{t}}$ include the gates in the past causal cone of q_{out}, i.e. all the gates which are logically necessary to produce the output of the circuit. Hence if the original quantum circuit accepted with probability $p \geq 1-\epsilon$ the probability to measure 0 for qubit q_{out} is less than ϵ. We define $a := \epsilon N_{bound}/N$ which is also an upper bound for the ground state energy of the untransformed Hamiltonian H.

5.2 Soundness

For showing the soundness of the reduction we assume that we are in a no-instance where U rejects with a probability higher than $1-\epsilon$, i.e. for all $\mathbf{t}$ with $t_{q_{out}} = D$ and all inputs $|\xi\rangle$ we have

$$\langle\xi,\mathbf{0},\mathbf{1}|\,U_{\mathbf{t}}^{\dagger}\,|0\rangle\,\langle 0|_{q_{out}}\,U_{\mathbf{t}}\,|\xi,\mathbf{0},\mathbf{1}\rangle \geq 1-\epsilon. \qquad (5.3)$$

We have to prove that all eigenvalues of H are lower bounded by some b with $b - a \in \Omega(n^{-\alpha})$ for some $\alpha > 0$.

The minimum eigenvalue of H is the minimum eigenvalue of $H|_{\mathcal{H}_{legal}}$ versus the minimum eigenvalue of $H|_{\mathcal{H}_{legal}^{\perp}}$. We have $H \geq 0$ and the minimum eigenvalue of H restricted to $\mathcal{H}_{legal}^{\perp}$ is 1. The same reasoning holds for the term H_{caus}. So we should now consider the minimum eigenvalue of H on $\mathcal{H}_{legal}\cap\mathcal{H}_{caus}$. We do a unitary rotation to remove the dependence of the logical gates and thus consider the Hamiltonian $\tilde{H}_{in} + \tilde{H}_{out} + \tilde{H}_{prop}$.

The qubits in the set S are all in the past causal-cone of the output qubit q_{out}. If they are not, we could have modified the verification circuit such it is true, as the qubits that are not in the past causal cone of the output qubit do not influence the outcome. For brevity we assume that $S_1 = \emptyset$ ($S = S_0$) and that all ancilla qubits are adjacent, nearest-neighbor qubits.

To obtain a lower bound we define $A := \tilde{H}_{prop}$ and $B := \tilde{H}_{in} + \tilde{H}_{out}$. Note that A and B are positive semidefinite. We have $\ker(A) \cap \ker(B) = \{0\}$ since we are in a no-instance. We will use the following lemma to obtain the lower bound b.

Lemma 5.1. Let A and B be nonnegative operators and $\ker(A)$ and $\ker(B)$ their respective nullspaces, where $\ker(A) \cap \ker(B) = \{0\}$. Suppose further that no nonzero eigenvalue of A or B is smaller than v. Then

$$A + B \geq v \cdot 2 \sin^2 \left(\frac{\theta}{2} \right). \tag{5.4}$$

where $\theta := \angle(\ker(A), \ker(B))$.

For a proof of Lemma 5.1 see [21]. In order to apply the lemma, we need to lower bound the first nonzero eigenvalue of $\tilde{H}_{prop}$ which is not trivial. We conjecture

Conjecture : The first non-zero eigenvalue of $\tilde{H}_{prop}$ is in $\Omega((nD)^{-\alpha})$ with $\alpha > 0$.

In addition, we have $B|_{\ker(B)^\perp} \geq 1$ as B is a sum of projectors.

The nullspace of A is spanned by states of the form $|\psi\rangle = |\xi\rangle \otimes \frac{1}{\sqrt{N}} \sum_{\mathbf{t} \in T} |\mathbf{t}\rangle$ for any n-qubit state $|\xi\rangle$ (see Eqn. 4.9). The nullspace of B is a direct sum $\ker(B) = \ker(B)_1 \oplus \ker(B)_2 \oplus \ker(B)_3$ with

$$\begin{aligned} \ker(B)_1 &= \operatorname{span}\Big(|\xi\rangle \otimes |\mathbf{t}\rangle \,\Big|\, \forall \mu \in S : t_\mu = 0 \to |\xi\rangle_\mu = |0\rangle, \exists \mu \in S : t_\mu = 0 \Big) \\ \ker(B)_2 &= \operatorname{span}\Big(|\xi\rangle \otimes |\mathbf{t}\rangle \,\Big|\, \forall \mu \in S : t_\mu \neq 0, t_{q_{out}} \neq D \Big) \\ \ker(B)_3 &= \operatorname{span}\Big(U_{\mathbf{t}}^\dagger (|1\rangle_{q_{out}} |\xi'\rangle) \otimes |\mathbf{t}\rangle \,\Big|\, t_{q_{out}} = D, |\xi'\rangle \in \mathbb{C}^{2^{n-1}} \Big). \end{aligned} \tag{5.5}$$

Note that these three null-spaces are orthogonal by the orthogonality on the time configurations. It is not possible that $\ker(B)_1 \cap \ker(B)_3 \neq \{0\}$ since then there would be ancilla qubits that don't lie in the past causal-cone of q_{out}. To apply Lemma 5.1 we need the maximal overlap of two normalized states from $\ker(A)$ and $\ker(B)$:

$$\cos^2(\theta) = \max_{\substack{|\psi\rangle \in \ker(A) \\ |\phi\rangle \in \ker(B)}} |\langle \psi \,|\, \phi \rangle|^2 = \max_{|\psi\rangle \in \ker(A)} \left\langle \psi \,\middle|\, \Pi_{\ker(B)} \,\middle|\, \psi \right\rangle \tag{5.6}$$

We have

$$\Pi_{\ker(B)_1} = \sum_{\emptyset \neq \tilde{S} \subseteq S} \mathrm{P}^{\mathbf{0}}_{\tilde{S}} \otimes \sum_{\mathbf{t} \in T(\tilde{S})} |\mathbf{t}\rangle \langle \mathbf{t}| \tag{5.7}$$

where $T(\tilde{S})$ is the set of all time configurations where only the qubits in the set $\tilde{S}$ are at time 0, i.e.

$$T(\tilde{S}) \coloneqq \{\mathbf{t} \in T \mid \forall i \in \tilde{S} : t_i = 0, \forall i \in S - \tilde{S} : t_i \neq 0\}. \tag{5.8}$$

We also introduced the following notation: For a subset of qubits $\tilde{S} = \{\mu_1, \dots, \mu_j\} \subseteq S$ and $\mathbf{x} \in \{0,1\}^j$ we set

$$\mathrm{P}^{\mathbf{x}}_{\tilde{S}} \coloneqq |x_1\rangle \langle x_1|_{\mu_1} \otimes \cdots \otimes |x_j\rangle \langle x_j|_{\mu_j} . \tag{5.9}$$

The operator $\Pi_{\ker(B)_1}$ is a projector because for $\tilde{S} \neq \tilde{S}'$ we have $\langle \mathbf{t}' \mid \mathbf{t}\rangle = 0$ for all $\mathbf{t} \in T(\tilde{S})$ and $\mathbf{t}' \in T(\tilde{S}')$. Now let us w.l.o.g. take the number of ancilla qubits in S to be even with labels $1, 2, \dots, |S|$. Furthermore we assume that the structure of the circuit is such that at the first time-step the qubit pairs $(1,2), (3,4), \dots, (n-1, n)$ interact.

We consider

$$\begin{aligned} &\max_{|\psi\rangle \in \ker(A)} \langle\psi| \Pi_{\ker(B)_1} + \Pi_{\ker(B)_2} + \Pi_{\ker(B)_3} |\psi\rangle \\ &= \max_{|\xi\rangle} \frac{1}{N} \langle\xi| \left(\sum_{\emptyset \neq \tilde{S} \subseteq S} |T(\tilde{S})| \mathrm{P}^{\mathbf{0}}_{\tilde{S}} + N_{int} + \sum_{\mathbf{t}: t_{q_{out}} = D} U^\dagger_{\mathbf{t}} \mathrm{P}^1_{q_{out}} U_{\mathbf{t}} \right) |\xi\rangle \end{aligned} \tag{5.10}$$

where $N_{int} = |\{\mathbf{t} \in T \mid \forall \mu \in S : t_\mu \neq 0 \text{ and } t_{q_{out}} \neq D\}|$. The first part of this expression can be analyzed as follows. We can write

$$\sum_{\emptyset \neq \tilde{S} \subseteq S} |T(\tilde{S})| \mathrm{P}^{\mathbf{0}}_{\tilde{S}} \eqqcolon \sum_{\mathbf{x} \in \{0,1\}^{|S|}} p_{\mathbf{x}} \prod_{\mu \in S : \mathbf{x}_\mu = 0} \mathrm{P}^0_\mu \tag{5.11}$$

where $p_{\mathbf{x}}$ is the number of time configurations $\mathbf{t} \in T$ with $t_\mu = 0$ if $x_\mu = 0$, i.e.

$$p_{\mathbf{x}} \coloneqq \sum_{\emptyset \neq \tilde{S} \subseteq S :\ \mathbf{x}|_{\tilde{S}} = \mathbf{0}} |T(\tilde{S})|. \tag{5.12}$$

We have $p_{max} \coloneqq \max_{\mathbf{x}} p_{\mathbf{x}} = p_{\mathbf{0}}$ as it includes the most subsets. The next largest $p_{\mathbf{x}}$ is $p_{\mathbf{e}_1} = p_{10\dots0} \eqqcolon p_{max-1}$.

Lemma 5.2. It holds that

$$p_{max-1} = p_{max} - N_{bound}. \tag{5.13}$$

Proof. We have

$$\begin{aligned} p_{max-1} &= |\{\mathbf{t} \in T \mid (\exists \mu \in S - \{1\} : t_\mu = 0) \wedge t_1 \neq 0\}| \\ &= |\{\mathbf{t} \in T \mid \exists \mu \in S : t_\mu = 0\} - \{\mathbf{t} \in T \mid t_1 = 0\}| \\ &= |\{\mathbf{t} \in T \mid (\exists \mu \in S : t_\mu = 0)\}| - |\{\mathbf{t} \in T \mid t_1 = 0\}| \\ &= p_{max} - N_{bound} \end{aligned} \tag{5.14}$$

since for sets $Y \subseteq X$ we have $|X - Y| = |X| - |Y|$ and obviously it holds that

$$\{\mathbf{t} \in T \mid t_1 = 0\} \subseteq \{\mathbf{t} \in T \mid \exists \mu \in S : t_\mu = 0\}. \tag{5.15}$$

■

Let $s = |S|$. We upper bound Eqn. 5.10 by considering the general state

$$|\xi\rangle = \alpha_0 |\mathbf{0}, \xi_0\rangle + \alpha_1 \sum_{\substack{x \in \{0,1\}^s \\ x \neq \mathbf{0}}} \beta_x |\mathbf{x}, \xi_x\rangle \tag{5.16}$$

with $|\alpha_0|^2 + |\alpha_1|^2 = \sum_{x \neq \mathbf{0}} |\beta_x|^2 = 1$ and $|\xi_y\rangle \in \mathbb{C}^{2^{n-s}}$. We have

$$\begin{aligned} \langle\psi| \Pi_{\ker(B)_1} |\psi\rangle &= \frac{1}{N} \left(|\alpha_0|^2 + |\alpha_1|^2 \sum_{x \neq \mathbf{0}} |\beta_x|^2 p_x \right) \\ &\leq \frac{1}{N} \left(|\alpha_0|^2 p_{max} + |\alpha_1|^2 p_{max-1} \right) \end{aligned} \tag{5.17}$$

since the maximum of a convex combination is given by the maximal element and $\max_{x \neq \mathbf{0}} p_x = p_{max-1}$. This gives

$$\langle\psi| \Pi_{\ker(B)} |\psi\rangle \leq \frac{|\alpha_0|^2 p_{max} + |\alpha_1|^2 p_{max-1}}{N} + \frac{N_{int}}{N} + \frac{\langle\psi| \Pi_{\ker(B)_3} |\psi\rangle}{N} \tag{5.18}$$

To upper bound the third term in Eqn. 5.18 we use the following lemma.

Lemma 5.3. Given a projector Π and a state of the form

$$|\psi\rangle = \alpha_0 |\psi_0\rangle + \alpha_1 |\psi_1\rangle \tag{5.19}$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$, $\langle\psi_0 \mid \psi_1\rangle = 0$ and

$$|\psi_0\rangle = \sqrt{1-\epsilon} |\psi_0^{\Pi=0}\rangle + \sqrt{\epsilon} |\psi_0^{\Pi=1}\rangle \in \ker(\Pi) \oplus \ker(\Pi)^\perp \tag{5.20}$$

the expectation value of Π can be upper bounded as follows:

$$\langle\psi|\,\Pi\,|\psi\rangle \leq |\alpha_0|^2\epsilon + |\alpha_1|^2 + 2|\alpha_0||\alpha_1|\sqrt{\epsilon(1-\epsilon)} \tag{5.21}$$

Proof. Let

$$|\psi_1\rangle = \sqrt{1-\delta}\,|\psi_1^{\Pi=1}\rangle + \sqrt{\delta}\,|\psi_1^{\Pi=0}\rangle\,. \tag{5.22}$$

Since

$$0 = \langle\psi_0 \mid \psi_1\rangle = \sqrt{\epsilon(1-\delta)}\langle\psi_0^{\Pi=1} \mid \psi_1^{\Pi=1}\rangle + \sqrt{(1-\epsilon)\delta}\langle\psi_0^{\Pi=0} \mid \psi_1^{\Pi=0}\rangle \tag{5.23}$$

we have that

$$\sqrt{\epsilon(1-\delta)}|\langle\psi_0^{\Pi=1} \mid \psi_1^{\Pi=1}\rangle| = \sqrt{(1-\epsilon)\delta}|\langle\psi_0^{\Pi=0} \mid \psi_1^{\Pi=0}\rangle| \tag{5.24}$$

which can be upper bounded by $\sqrt{\epsilon(1-\epsilon)}$. Thus

$$\begin{aligned}\langle\psi|\,\Pi\,|\psi\rangle &\leq |\alpha_0|^2\epsilon + |\alpha_1|^2(1-\delta) + 2|\alpha_0||\alpha_1|\sqrt{\epsilon(1-\delta)}|\langle\psi_0^{\Pi=1} \mid \psi_1^{\Pi=1}\rangle| \\ &\leq |\alpha_0|^2\epsilon + |\alpha_1|^2 + 2|\alpha_0||\alpha_1|\sqrt{\epsilon(1-\epsilon)}.\end{aligned} \tag{5.25}$$

■

Using Lemma 5.2 and Lemma 5.3 we obtain

$$\begin{aligned}\max_{|\psi\rangle\in\ker(A)} \langle\psi|\,\Pi_{\ker(B)}\,|\psi\rangle \leq& 1 - \frac{N_{bound}}{N}\left(1 - |\alpha_0|^2\epsilon - 2|\alpha_0|\sqrt{1-|\alpha_0|^2}\sqrt{\epsilon(1-\epsilon)}\right) \\ =&: 1 - \frac{N_{bound}}{N}f(\epsilon,|\alpha_0|).\end{aligned} \tag{5.26}$$

The function $f(\epsilon,|\alpha_0|)$ can be lower bounded by $f(\epsilon) := f(\epsilon,\hat{\alpha})$ with

$$\hat{\alpha} := \sqrt{\frac{4-3\epsilon+\sqrt{\epsilon(4-3\epsilon)}}{2(4-3\epsilon)}}. \tag{5.27}$$

This shows that

$$2\sin^2\left(\frac{\theta}{2}\right) \in \Omega\left(\frac{N_{bound}}{N}f(\epsilon)\right). \tag{5.28}$$

For the fraction of output configurations we have $\frac{N_{bound}}{N} \in \Omega(n^{-2.5}D^{-1})$, see Lemma 4.7.

Note that $f(\epsilon = 1) = 0$, resulting in a lower bound $b = 0$ as we would expect, since this corresponds to the case where the circuit accepts with probability 1.

5.3 Improving the locality

The Hamiltonian H is 8-local (see Sec. 3.6). We can improve this to 4-local by modifying the terms in H_{prop} and putting a higher energy penalty on non-legal states, i.e. states in $\mathcal{H}_{legal}^{\perp}$. We use the same idea as Kempe and Regev in [20].

We modify the construction of the Hamiltonian H in the following way. We denote the interacting qubits as c and t, keeping in mind that they depend on i and j.

For $i \in \{2, \dots, D-1\}$ we set

$$\begin{aligned} H_{prop,i,j} =& I \otimes |10\rangle\langle 10|_{i,i+1}^{c} \otimes |10\rangle\langle 10|_{i,i+1}^{t} + I \otimes |10\rangle\langle 10|_{i-1,i}^{c} \otimes |10\rangle\langle 10|_{i-1,i}^{t} \\ &- \left[CU_{c,t}^{i} \otimes |1\rangle\langle 0|_{i}^{c} \otimes |1\rangle\langle 0|_{i}^{t} + h.c. \right] \end{aligned} \tag{5.29}$$

and

$$\begin{aligned} H_{prop,1,j} =& I \otimes |10\rangle\langle 10|_{1,2}^{c} \otimes |10\rangle\langle 10|_{1,2}^{t} + I \otimes |0\rangle\langle 0|_{1}^{c} \otimes |0\rangle\langle 0|_{1}^{t} \\ &- \left[CU_{c,t}^{1} \otimes |1\rangle\langle 0|_{1}^{c} \otimes |1\rangle\langle 0|_{1}^{t} + h.c. \right] \end{aligned} \tag{5.30}$$

$$\begin{aligned} H_{prop,D,j} =& I \otimes |1\rangle\langle 1|_{D}^{c} \otimes |1\rangle\langle 1|_{D}^{t} + I \otimes |10\rangle\langle 10|_{D-1,D}^{c} \otimes |10\rangle\langle 10|_{D-1,D}^{t} \\ &- \left[CU_{c,t}^{D} \otimes |1\rangle\langle 0|_{D}^{c} \otimes |1\rangle\langle 0|_{D}^{t} + h.c. \right]. \end{aligned} \tag{5.31}$$

Note that H_{prop} is not positive semidefinite anymore. Let b from the soundness proof in the previous section be lower-bounded by $\frac{c}{(nD)^{\beta}}$ for some $\beta \in \mathbb{N}$ and constant $c > 0$. We define $g := 4nD$ and set

$$H_{legal} = g^{2\beta+6} \left[\sum_{\mu=1}^{n} \sum_{i=0}^{D+1} |0\rangle\langle 0|_{\mu,i} \otimes |1\rangle\langle 1|_{\mu,i+1} + \sum_{\mu=1}^{n} \Big(|0\rangle\langle 0|_{\mu,0} + |1\rangle\langle 1|_{\mu,D+1} \Big) \right]. \tag{5.32}$$

All terms in the Hamiltonian H are now 4-local. However, we need to revise our proof of the soundness of the QMA-reduction. For $H' := H_{in} + H_{out} + H_{prop} + H_{caus}$ we have

$$\begin{aligned} \|H'\| &\leq \|H_{in}\| + \|H_{out}\| + \sum_{i,j} \|H_{prop,i,j}\| + \|H_{caus}\| \\ &\leq |S| + 1 + nD + nD \leq g. \end{aligned} \tag{5.33}$$

Assume we are in a no-instance. Let $|\eta\rangle = \alpha_1 |\eta_1\rangle + \alpha_2 |\eta_2\rangle$ with $|\eta_1\rangle \in \mathcal{H}_{legal}$ and $|\eta_2\rangle \in \mathcal{H}_{legal}^{\perp}$ and $\alpha_1^2 + \alpha_2^2 = 1$. We have to show two cases:

The first case is $\alpha_2 \geq \frac{1}{g^{\beta+2}}$. Then we have

$$\begin{aligned}\langle\eta| H |\eta\rangle &\geq \langle\eta| H_{legal} |\eta\rangle - \|H'\| \\ &\geq \alpha_2^2 \cdot g^{2\beta+6} - g = g^2 - g > 1\end{aligned} \tag{5.34}$$

since $g = 4nD > 1$.

In the second case we have $\alpha_2 < \frac{1}{g^{\beta+2}}$ and thus

$$\begin{aligned}\langle\eta| H |\eta\rangle &\geq \langle\eta| H' |\eta\rangle \\ &\geq \langle\eta_1| H' |\eta_1\rangle - \alpha_2^2 \langle\eta_1| H' |\eta_1\rangle + 2\alpha_1\alpha_2 \mathrm{Re}(\langle\eta_1| H' |\eta_2\rangle) + \alpha_2^2 \langle\eta_2| H' |\eta_2\rangle \\ &\geq \langle\eta_1| H' |\eta_1\rangle - 2\alpha_2^2\|H'\| - 2\alpha_2\|H'\| \\ &\geq \langle\eta_1| H' |\eta_1\rangle - \frac{2}{g^{2\beta+1}} - \frac{2}{g^{\beta+1}}.\end{aligned} \tag{5.35}$$

Note that the for both the cursor clock and the domain wall clock the legal space is N dimensional. Thus the term $\langle\eta_1| H' |\eta_1\rangle$ is equal to the one we dealt with in Section 5.2 up to renaming the basis elements of the time register. Hence, Eqn. 5.35 is asymptotically lower bounded by a function in $\Omega((nD)^{-\beta})$ which concludes the proof.

Chapter 6

Numerical analysis

6.1 Numerical values of the gap

We implemented a program in Mathematica to analyze the spectrum of the term H_{prop} numerically. The program constructs the propagation graph $G_{n,D}$ via a depth-first traversal. From the graph it computes the corresponding Laplacian matrix and the second lowest eigenvalue λ_2. However, the number of steps that he algorithm takes to construct the graph scales badly in n and D, so we were only able to compute λ_2 for $n \in \{2, \ldots, 14\}$ and $D \in \{1, \ldots, 10\}$ in a reasonable amount of time (see Fig. 6.1).

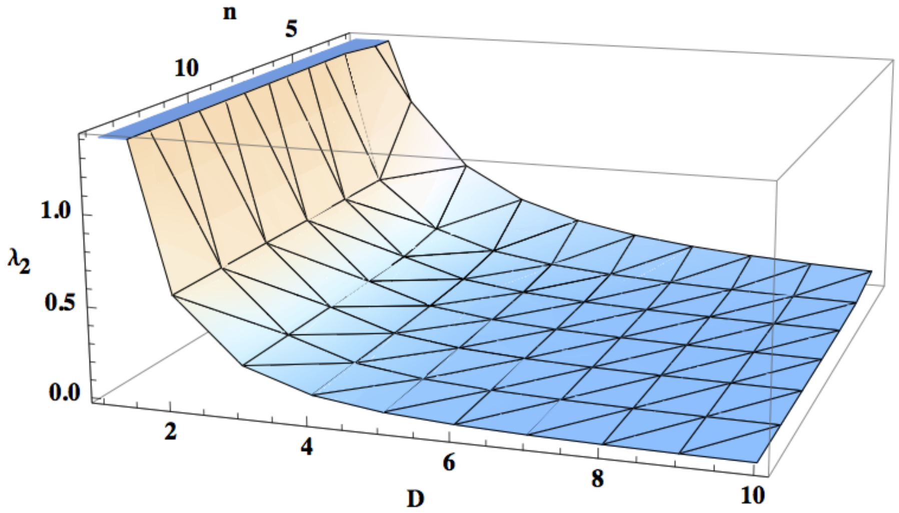

FIGURE 6.1: Dependence of λ_2 on $n \in \{2, \ldots, 14\}$ and $D \in \{1, \ldots, 10\}$.

In Figure 6.2 we see the dependence of λ_2 on n, if we fix D for non-periodic boundary in time. The curve does not seem to depend exponentially on n, though it is not justified to draw any conclusions from such a small set of data.

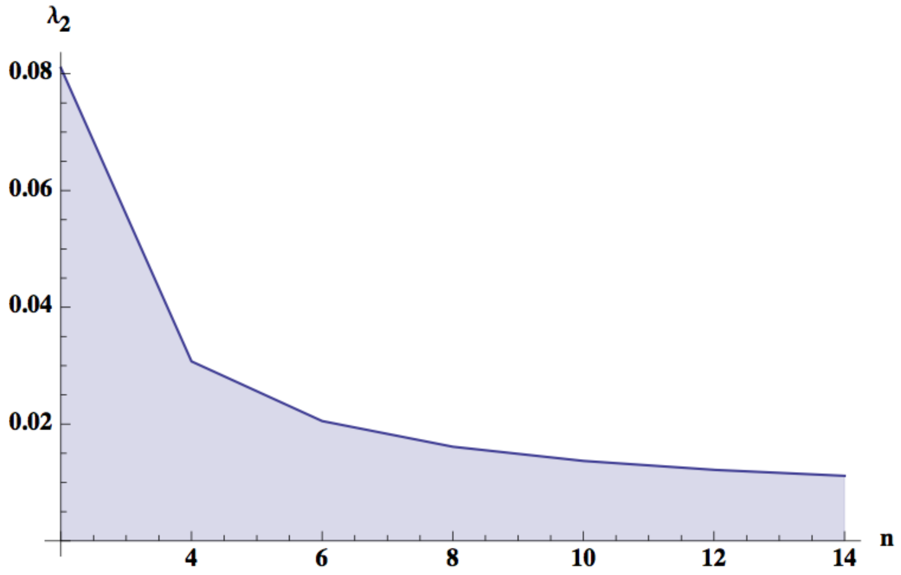

FIGURE 6.2: Dependence of λ_2 on $n \in \{2, \ldots, 14\}$ for $D = 10$.

On the other hand, if we fix n we get a curve as in Figure 6.3. From the limited set of data it is hard to tell whether this curve is described by a function which falls like the inverse of a polynomial or exponentially.

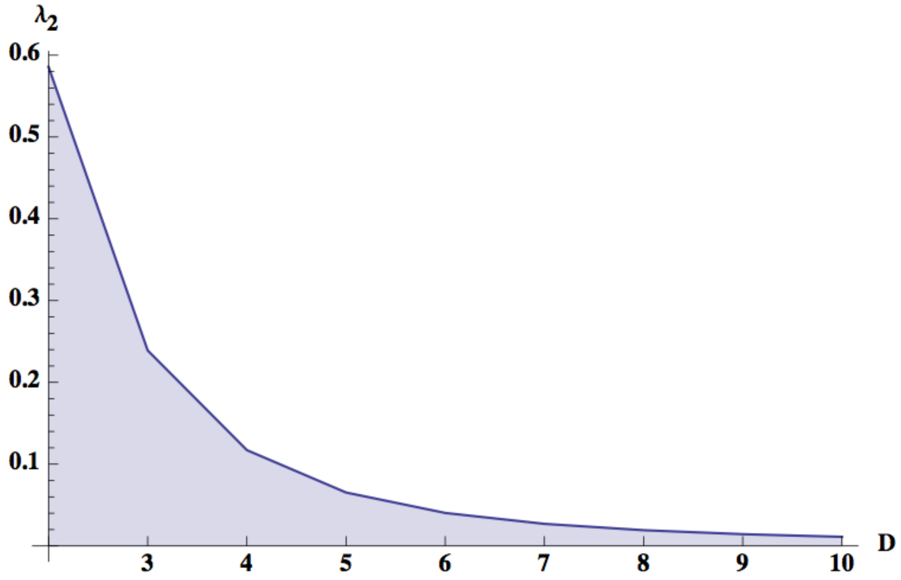

FIGURE 6.3: Dependence of λ_2 on $D \in \{2, \ldots, 10\}$ for $n = 14$.

6.2 Approximation of a low-lying state

We want to construct an approximation of the Fiedler vector, i.e. a low-lying state of H_{prop}. In loose terms, to minimize the quotient in Eqn. 4.11 we need to make the difference between the amplitudes for connected time configurations as small as possible while making the overall variation of the amplitudes large.

We do this by assigning each time configuration $\mathbf{t}$ of one partition S_i the same amplitude (see Sec. 4.1). By doing this we effectively obtain a path graph with $L+1$ vertices. The Fiedler vector for a path graph is known. If $\{v_1, \ldots, v_{L+1}\}$ are the vertices of a path graph of length $L+1$ then the amplitudes of the Fiedler vector $\mathbf{x}$ are

$$x_{v_i} = \cos\left(\frac{\pi i}{2L}\right). \tag{6.1}$$

Thus, for a time propagation graph $G_{n,D}$ we define the vector $\mathbf{x}' \in \mathbb{R}^N$ by

$$x'_{\mathbf{t}} = \cos\left(\frac{\pi \sum_{j=1}^{n} t_j}{nD}\right). \tag{6.2}$$

Note that the vector $\mathbf{x}'$ is orthogonal to the all-one vector $\mathbf{1}$:

$$\begin{aligned}
\mathbf{x}' \cdot \mathbf{1} &= \sum_{\mathbf{t}\in T} \cos\left(\frac{\pi \sum_{j=1}^{n} t_j}{nD}\right) \\
&= \sum_{r=0}^{\frac{nD}{2}} |S_r| \cos\left(\frac{2\pi r}{nD}\right) \\
&= \sum_{r=0}^{\frac{nD}{4}} |S_r| \cos\left(\frac{2\pi r}{nD}\right) + \sum_{r=0}^{\frac{nD}{4}} |S_r| \cos\left(\pi - \frac{2\pi r}{nD}\right) = 0
\end{aligned} \tag{6.3}$$

We used that n and D are even and that $|S_r| = |S_{L-r}|$ which follows from the symmetry of the graph (see Eqn. 4.6).

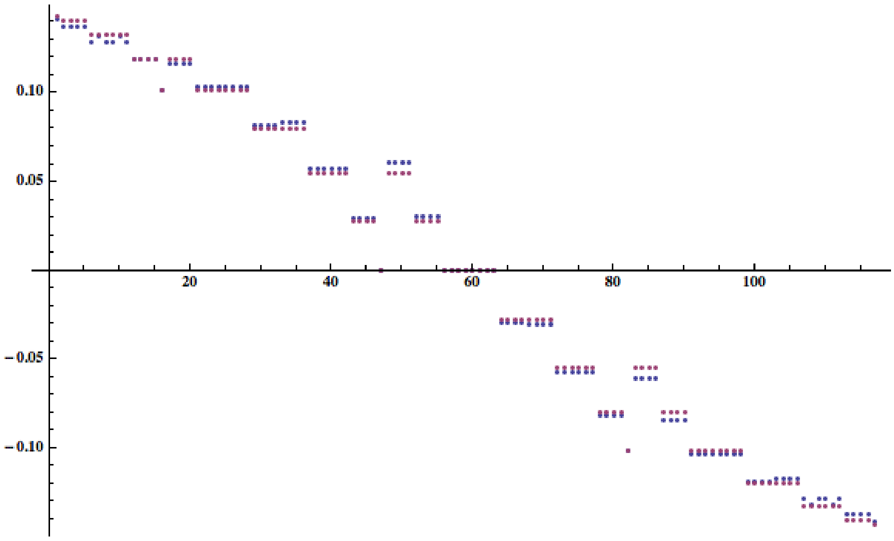

Figure 6.4: Approximation of the amplitudes of the Fiedler vector for $n = 8$ and $D = 4$. Blue are the amplitudes obtained by the Mathematica program and purple are the approximations via Eqn. 6.2.

We can use this method of getting a low-lying state to get an approximation for the second eigenvalue $\tilde{\lambda}_2$ using the Courant-Fischer formula (see Eqn. 4.11). The results are listed in Fig. 6.5. The relative errors do not seem to diverge.

n	$\tilde{\lambda}_2$	λ_2	$\lvert\tilde{\lambda}_2 - \lambda_2\rvert$	$\frac{\lvert\tilde{\lambda}_2 - \lambda_2\rvert}{\lambda_2}$
2	0.03415	0.03405	0.0001057	0.003103
4	0.01232	0.01232	0.0000072201835	0.000586
6	0.007905	0.007902	0.0000031998598	0.0004049
8	0.005995	0.005985	0.000009262097	0.001547
10	0.004928	0.00491	0.00001682	0.00342

Figure 6.5: Approximation of λ_2 for $D = 16$ via Eqn. 6.2 and by computing the Laplacian matrix with Mathematica.

Encouraged by this result we want to lower bound λ_2 using the approximation and Eqn. 4.11. We know that if $(\mathbf{t}, \mathbf{t}') \in E$ then they only differ in two positions by 1. However, we do not know the number of edges connecting from earlier times and edges connecting to later times. To circumvent this problem we identify the time 0 with time D, i.e. we assume periodic boundary conditions in time. Equivalently, we can imagine the circuits wrapped around the surface of a torus. For consistency we additionally to n and D being even we demand that n divides D or D divides n, depending on which is larger.

Lemma 6.1. For periodic bounday in time we have that for any proper time configuration $\mathbf{t}$ there are as many time configurations which jump onto $\mathbf{t}$ as there are time configurations which jump away from $\mathbf{t}$.

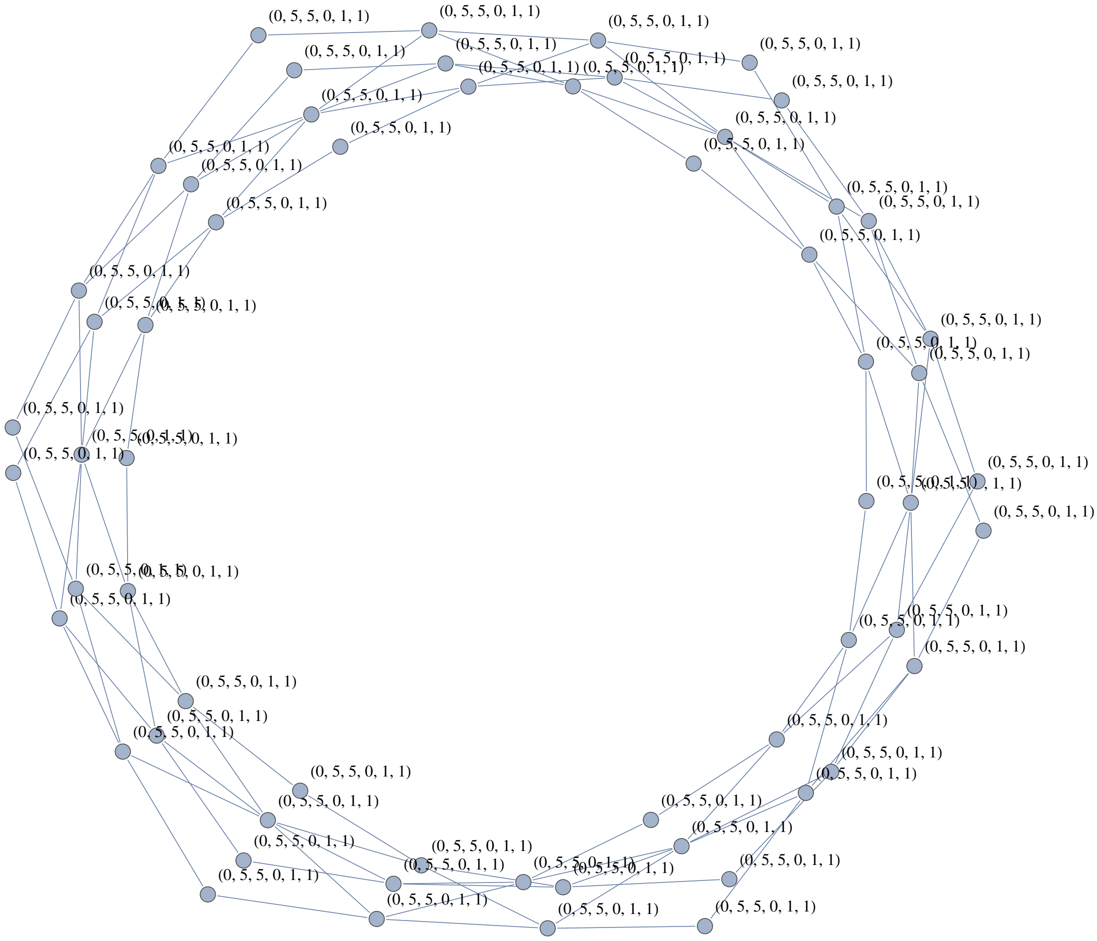

FIGURE 6.6: The time propagation graph with periodic boundary in time for $n = 6$ and $D = 6$.

Proof. Intuitively this is true because a path in Fig. 3.2, corresponding to a proper time configuration, must have the same number of left and right turns. More formally let us assume that we are given a proper time configuration $\mathbf{t}$. Since it is in T there exist, by a similar argument as for Lemma 4.1, two partner qubits $\mu, \mu+1$ which are at the same time after the gate where they interacted. We know that the qubit $\mu+2$ is either at the same time as $\mu+1$ or one before. If it is at the same time then the neighbors $\mu+1, \mu+2$ can jump forward. If not we follow the path downwards until we arrive at a position where two neighbors are at the same time and both can jump forward. These qubits must exist or else one qubit must have gone through a gate without its partner. Thus we can pair up all forward jumps with backward jumps which proves our claim. ■

Using Lemma 6.1 and the known amplitudes for a cycle graph[1] we obtain for large circuits the following approximate lower bound:

$$\begin{aligned}\lambda_2 \approx &\sum_{(\mathbf{t},\mathbf{t}')\in E} (x_{\mathbf{t}} - x_{\mathbf{t}'})^2 \\ =&\frac{1}{N}\sum_{\mathbf{t}\in T}\sum_{\mathbf{t}':(\mathbf{t},\mathbf{t}')\in E}\left[\cos\left(\frac{2\pi\sum_j t_j}{nD}\right) - \cos\left(\frac{2\pi\sum_j t'_j}{nD}\right)\right]^2 \\ =&\frac{1}{N}\sum_{\mathbf{t}\in T}\left[\frac{\deg(\mathbf{t})}{2}\left(\cos\left(\frac{2\pi\sum_j t_j}{nD}\right) - \cos\left(\frac{2\pi\sum_j t_j}{nD} + \frac{4\pi}{nD}\right)\right)^2\right. \\ &+\left.\frac{\deg(\mathbf{t})}{2}\left(\cos\left(\frac{2\pi\sum_j t_j}{nD}\right) - \cos\left(\frac{2\pi\sum_j t_j}{nD} - \frac{4\pi}{nD}\right)\right)^2\right] \\ \gtrapprox&\frac{32\pi^2}{Nn^2D^2}\sum_{\mathbf{t}\in T}\sin\left(\frac{2\pi\sum_j t_j}{nD}\right)^2 \geq \frac{16\pi^2}{n^2D^2}\end{aligned} \tag{6.4}$$

where we did a Taylor expansion in $\frac{1}{nD}$ and used $\deg(\mathbf{t}) \geq 2$ for all $\mathbf{t} \in T$.

In Figure 6.7 we compare the approximation with the results obtained by the Mathematica program. We see that for $n = 16$ the relative error increases suddenly by a factor of 4. Since we can not go to higher circuit sizes it is hard to say whether the approximation is good.

n	$\tilde{\lambda}_2$	λ_2	$\lvert\tilde{\lambda}_2 - \lambda_2\rvert$	$\frac{\lvert\tilde{\lambda}_2-\lambda_2\rvert}{\lambda_2}$
4	0.781049	0.76393	0.0171166	0.022
8	0.347979	0.34141	0.0065729	0.019
12	0.223031	0.21978	0.0032484	0.014
16	0.163664	0.15183	0.0118337	0.078

FIGURE 6.7: Approximation of λ_2 for $D = 4$ for the periodic case via Eqn. 6.2.

[1] A path graph where the two terminal vertices are identified.

Chapter 7

Conclusion

Summary

We have shown that the proposal by Mizel et. al. to map a circuit onto a Hamiltonian describing interacting fermions is equivalent to a similar construction as introduced by Kitaev with multiple time registers. The transformation naturally gives rise to a cursor clock (Ch. 3). By restricting the considered class of circuits to consist of controlled-unitary gates arranged in an alternating fashion we made the necessary causality checks local on the 2D lattice. We introduced the time propagation graphs $G_{n,D}$ and derived some of their properties (Ch. 4). This family of graphs makes it possible to analyze the spectrum of the term H_{prop}. Our main result is the proof that 8-Local Hamiltonian is QMA-complete, using the multi-time circuit to Hamiltonian construction with a domain wall representation of the clock (Ch. 5). We also show that we can reduce the locality to 4-local by implementing a cursor clock. This is done by introducing energy penalties on non-legal states, which scale with the system size. Note that these penalties are not necessary when using the multi-time construction for adiabatic or dynamical quantum computing, since the Hamiltonian H preserves the legal space and we can prepare the initial state of the system. Unfortunately, we were not able to provide a lower bound of the term H_{prop} needed to prove that the QMA-reduction is sound. We implemented a program in Mathematica to compute the values of the gap numerically (Ch. 6). However, we were only able to run the program for small circuit sizes, making the numerical analysis not conclusive. Furthermore, we gave a non-rigorous argument for a polynomial sized gap.

Future work

The most important open problem is to find a lower bound for the gap of H_{prop}, as it is the missing piece in the completeness proof. This would also give a rigorous proof of the equivalence between AQC and the circuit model as proposed in [25]. We consider the most promising approach to be the analysis via the time propagation graphs and spectral graph theory. Having the degree of the polynomial would also enable us to find bounds on the mixing time of a quantum walk on the time propagation graphs, which in turn can be used for dynamical quantum computation.

Bibliography

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, STOC '01, pages 50–59, New York, NY, USA, 2001. ACM.

[2] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The power of quantum systems on a line. *Communications in Mathematical Physics*, 287(1):41–65, 2009.

[3] D. Aharonov, J. Kempe, S. Lloyd, W. van Dam, Z. Landau, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM Journal on Computing*, 2007.

[4] D. Aharonov and T. Naveh. Quantum NP - A Survey, 2002, arXiv:quant-ph/0210077.

[5] A. Ambainis and O. Regev. An Elementary Proof of the Quantum Adiabatic Theorem, 2004, arXiv:quant-ph/0411152.

[6] B. Bollobás. *Modern Graph Theory.* Graduate texts in mathematics. Springer, Heidelberg, corrected edition, 1998.

[7] S. Bravyi. Efficient algorithm for a quantum analogue of 2-SAT, 2006, arXiv:quant-ph/0602108.

[8] A. M. Childs, E. Farhi, and J. Preskill. Robustness of adiabatic quantum computation. Phys.Rev. A65 (2002) 012322, 2001, arXiv:quant-ph/0108048.

[9] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Royal Society of London Proceedings Series A*, 400:97–117, July 1985.

[10] L. Eldar and O. Regev. Quantum SAT for a Qutrit-Cinquit Pair Is QMA1-Complete. In *Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part I*, ICALP '08, pages 881–892, Berlin, Heidelberg, 2008. Springer-Verlag.

[11] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution, 2000, arXiv:quant-ph/0001106.

[12] R. P. Feynman. Quantum mechanical computers. *Foundations of physics*, 16(6):507–531, 1986.

[13] L. Fortnow and S. Homer. A short history of computational complexity. *Bulletin of the EATCS*, 80:95–133, 2003.

[14] D. Gosset and D. Nagaj. Quantum 3-SAT is QMA1-complete, 2013, arXiv:1302.0290.

[15] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Transactions of the American Mathematical Society*, 117:285–306, 1965.

[16] S. Heubach and T. Mansour. *Combinatorics of compositions and words*. CRC Press, 2010.

[17] S. Jordan. Quantum Algorithm Zoo. `http://math.nist.gov/quantum/zoo/`, 2013.

[18] J. Kempe. Quantum random walks: an introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.

[19] J. Kempe, A. Kitaev, and O. Regev. The Complexity of the Local Hamiltonian Problem. In *In Proc. of 24th FSTTCS*, pages 372–383, 2004.

[20] J. Kempe and O. Regev. 3-Local Hamiltonian is QMA-complete. Quantum Computation and Information, Vol. 3(3), p. 258-64, 2003, 2003, arXiv:quant-ph/0302079.

[21] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, Boston, MA, USA, 2002.

[22] E. Knill. Quantum Randomness and Nondeterminism, Oct. 1996, arXiv:quant-ph/9610012.

[23] T. Koshy. *Catalan Numbers with Applications*. Oxford University Press, Oxford, 2009.

[24] D. A. Lidar. Towards Fault Tolerant Adiabatic Quantum Computation. Phys. Rev. Lett. 100, 160506 (2008), 2007, arXiv:0707.0021.

[25] A. Mizel, D. Lidar, and M. Mitchell. Simple proof of equivalence between adiabatic quantum computation and the circuit model. *Phys Rev Lett*, 99(7):070502, 2007.

[26] B. Mohar. The Laplacian spectrum of graphs. In *Graph Theory, Combinatorics, and Applications*, pages 871–898. Wiley, 1991.

[27] C. Moore and S. Mertens. *The Nature of Computation.* Oxford University Press, Inc., New York, NY, USA, 2011.

[28] D. Nagaj. Fast universal quantum computation with railroad-switch local Hamiltonians. *Journal of Mathematical Physics*, 51:062201, 2010.

[29] M. A. Nielsen. The Fermionic canonical commutation relations and the Jordan-Wigner transform.

[30] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge university press, 2010.

[31] R. Oliveira and B. M. Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Information & Computation*, 8(10):900–924, 2008.

[32] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1990.

[33] P. Stănică. Good lower and upper bounds on binomial coefficients. *JIPAM. Journal of Inequalities in Pure & Applied Mathematics*, 2(3):Paper No. 30, 5 p., 2001.

[34] J. Watrous. Quantum Computational Complexity. *Encyclopedia of Complexity and Systems Science*, pages 7174–7201, 2009.