# Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation

Dorit Aharonov* Wim van Dam† Julia Kempe‡ Zeph Landau§ Seth Lloyd¶
Oded Regev‖

July 10, 2004

**Abstract**

Adiabatic quantum computation has recently attracted attention in the physics and computer science communities, but its computational power has been unknown. We settle this question and describe an efficient adiabatic simulation of any given quantum algorithm, which implies that the adiabatic computation model and the conventional quantum circuit model are polynomially equivalent. Our result can be extended to the physically realistic setting of particles arranged on a two-dimensional grid with nearest neighbor interactions. The equivalence between the models provides a new vantage point from which to tackle the central issues in quantum computation, namely designing new quantum algorithms and constructing fault tolerant quantum computers. In particular, by translating the main open questions in quantum algorithms to the language of spectral gaps of sparse matrices, the result makes quantum algorithmic questions accessible to a wider scientific audience, acquainted with mathematical physics, expander theory and rapidly mixing Markov chains.

*Computer Science Division, UC Berkeley, CA 94720, and Department of Computer Science and Engineering, Hebrew University, Jerusalem, Israel 91904. doria@cs.huji.ac.il.

†Department of Physics, MIT, Cambridge, MA 02139. vandam@mit.edu

‡Computer Science Division and Department of Chemistry, UC Berkeley, CA 94720, and CNRS-LRI UMR 8623, Université de Paris-Sud, Orsay, France 91405. kempe@lri.fr

§Department of Mathematics, City College of New York. landau@sci.ccny.cuny.edu

¶Department of Mechanical Engineering, MIT, Cambridge, MA 02139. slloyd@mit.edu

‖EECS Department, UC Berkeley, Berkeley, CA 94720. odedr@cs.berkeley.edu

# 1 Introduction

Quantum computation has emerged in the last decade as an exciting and promising direction of research due to several breakthrough discoveries. Shor's quantum algorithm for factorization [1], followed by several other algorithms to solve algebraic and combinatorial problems (see, e.g., [2–5]) have demonstrated the possible exponential advantage of quantum computing systems over classical ones. These discoveries motivated interest in the physical implementation of quantum computation, resulting (to date) in the realization of small-scale quantum computations in various systems (see, e.g., [6–12]). The field now faces two major challenges. The first is to extend the capabilities of quantum algorithms, and in particular, to come up with substantially new algorithmic techniques which go beyond the main quantum tool: the Fourier transform. The second is to improve the current experimental and theoretical methods [13] of protecting the computation against decoherence and errors, thereby addressing the main stumbling blocks in the realization of large-scale quantum computers. Recently, Farhi et al. [14, 15] suggested an ingenious paradigm for quantum algorithms called *adiabatic computation*, which attracted considerable attention [14–21] since it was shown to exhibit promising algorithmic capabilities [16–18], as well as inherent robustness against decoherence and control errors [20].

In the adiabatic paradigm, a combinatorial problem is rephrased as the problem of finding the lowest energy state (namely, the *ground state*) of a "target" Hamiltonian $H_{\rm final}$ (a Hamiltonian is simply a Hermitian matrix). For the Hamiltonian to be physically realistic, we require that it is *local*, i.e., involves only interactions between a constant number of particles. To solve the combinatorial problem, a quantum system is initialized in the ground state of an initial local Hamiltonian $H_{\rm init}$, and then $H_{\rm init}$ is slowly transformed into $H_{\rm final}$. A celebrated theorem from physics called the quantum adiabatic theorem [22, 23] implies that if the transformation is carried out sufficiently slowly, the system tracks the ground state of the time varying Hamiltonian and therefore ends up in the desired ground state of $H_{\rm final}$. Indeed, if the spectral gap of the time varying Hamiltonian is never too small then the entire process can be carried out efficiently. Adiabatic computation can therefore be viewed as a process that takes a quantum state to another. We remark that previous research in the area followed [15] and focused on the case where $H_{\rm final}$ encodes a classical optimization problem and so is diagonal. This means that the final state is a basis state. We observe here that the relevant and natural model from a physical point of view does not require this. Using the same physical resources (namely, local Hamiltonians) one can actually adiabatically generate much more complicated superpositions. Adiabatic computation is thus viewed as a process that takes a tensor product state to a (possibly more general) quantum superposition.

The focus of this paper is the characterization of the computational power of such adiabatic computations. [21] began to address this question when they showed that a related model to adiabatic computation, which used *simulatable* Hamiltonians (i.e., Hamiltonians which are given non explicitly as the result of applying sequences of quantum gates) is as powerful as conventional quantum circuits. [21] left the main question of universality of adiabatic computation with physically realistic (namely, local) Hamiltonians, open. This model might seem at first sight less powerful than standard quantum computation, because of the local, almost explicit, specification of the final state. Indeed, previous results gave only partial answers regarding the computational capabilities of this model. [15] used adiabatic computation to tackle an NP-complete problem. There is mounting evidence [17, 19, 24] that the algorithm of [15] takes exponential time in the worst case for such problems. [19, 25] showed that adiabatic computation can implement Grover's quantum search algorithm [26], and [16–18] showed that adiabatic computation can 'tunnel' through wide energy barriers and thus outperform simulated annealing, the classical counterpart of the adiabatic model. These results demonstrated polynomial speed-ups of adiabatic computation over general classical search algorithms [1]. From the other direction, [15] imply that adiabatic computation is not stronger computationally

[1] In fact, [16, 17] even demonstrated an exponential speed-up of adiabatic computation over classical local search algorithms

than the standard quantum model. Where exactly does the adiabatic model sit on the scale between polynomial advantage over classical computation, and the full quantum computational power, was unclear. In fact, even the question of whether adiabatic computers can simulate general *classical* computations efficiently was unknown.

### 1.1 Results

Our main result clarifies the picture. We show:

**Theorem 1.** *The model of adiabatic computation with local Hamiltonians involving three qubit interactions is polynomially equivalent to the standard model of quantum computation.*

This shows that universal quantum computation can be fully studied and implemented in the adiabatic framework, and so adiabatic computation can be thought of as an alternative model to quantum computation.

We also show that a similar theorem holds when we relax the requirement that the Hamiltonians be local, and allow *sparse* Hamiltonians. These are Hermitian matrices which have at most polynomially many non zero elements at each row and column, where we also require that the matrix is *explicit*, namely each element can be computed efficiently given its indexes. We show

**Corollary 2.** *The model of adiabatic computation with sparse Hamiltonians is polynomially equivalent to the standard model of quantum computation,*

Corollary 2 is potentially more useful in the context of algorithms and complexity, since sparse Hamiltonians seem to be mathematically easier to handle than local ones. One direction follows immediately from Theorem 1 by observing that local Hamiltonians are in particular sparse. The other direction, namely that adiabatic computations with sparse Hamiltonians can be simulated efficiently by standard quantum computers, follows from the implementation of sparse Hamiltonians using quantum circuits presented in [21].

From the algorithmic point of view, these result show that all quantum algorithmic questions can be framed in the language of eigenstates and spectral gaps of local or even sparse Hermitian matrices. The design of quantum algorithms can thus draw on the wide scientific literature on these fundamental objects, in particular expander theory [27], rapidly mixing Markov chains (see, e.g., [28, 29]), and mathematical physics. This raises the hope that tools from these areas might be useful to tackle the difficult challenge of designing new quantum algorithms. Indeed, probability theory was already used in analyzing spectral gaps of Hamiltonians (see, e.g., [30] and references therein, as well as the proofs in this paper). In addition, we note that the adiabatic model appears ideally suited for the task of quantum state generation, which was shown recently to be essential for many important quantum algorithmic problems [21].

As for experimental applications, our result shows that universal quantum computation can in principle be implemented adiabatically. We bring the model one step closer to physical realization by showing that adiabatic computation with a more physically realistic set of Hamiltonians is also quantum universal:

**Theorem 3.** *The model of adiabatic computation with two-body nearest neighbor Hamiltonians operating on six-state particles set on a two dimensional grid, is polynomially equivalent to standard quantum computation.*

Experimentally realizing quantum computation using the adiabatic model has potential advantages from the point of view of fault tolerance, i.e., reliable computation in the presence of noise. [20] argues that if adiabatic computers were cooled below the Hamiltonian's energy gap, decoherence could essentially be ruled out. Furthermore, [20] studies the effect of unitary control errors in the Hamiltonian and conclude that such errors might, in fact, *help* the adiabatic computation. Our result combined with these studies

—such as simulated annealing— though the problem of [16, 17] can be solved efficiently by other classical methods.

indicates that the possibility of fault tolerant adiabatic computation deserves to be further studied, both theoretically and experimentally. Experimental realization of small-scale adiabatic computation was already demonstrated [31].

Finally, we consider further the possible relevance of the above results to fault tolerance. If the Hamiltonian of the adiabatic evolution leaves a certain subspace invariant, it actually suffices to lower bound the spectral gap of the Hamiltonian *restricted* to that subspace. (This is the case in Subsection 3.1) However, the *full* spectral gap, namely the gap in the entire Hilbert space, may be important in the context of noise, especially thermal fluctuations (see [20]) [2]. It turns out that

**Theorem 4.** *The above results hold with Hamiltonians with inverse polynomial "full" spectral gap.*

## 1.2 Key Ideas

Given a quantum circuit [35], we associate with it a corresponding adiabatic computation. Without loss of generality we will assume that the input to the quantum circuit consists of $n$ qubits all initialized to $|0\rangle$'s [3]. Then, a sequence of $L$ unitary gates, $U_1, \ldots, U_L$, each operating on one or two qubits, is applied to the state. The system's state after the $\ell$'th gate is $|\alpha(\ell)\rangle$. The output of the quantum circuit is in general a complicated quantum state $|\alpha(L)\rangle$ of $n$ qubits, which is then measured in the standard basis.

A natural attempt to design an adiabatic computation that mimics the circuit's computation would be to define $H_{\rm final}$ to be a local Hamiltonian with $|\alpha(L)\rangle$ as its ground state. This poses a difficulty: we want to explicitly specify the Hamiltonian *without knowing* the complicated output of the quantum circuit in advance.

The key to solving this problem is based on an idea by Kitaev [36] and Feynman [37]. Instead of designing a Hamiltonian that has the final unknown state of the circuit as its ground state, a task that seems impossible, one can define $H_{\rm final}$ to be a *local* Hamiltonian whose ground state is the entire *history* of the quantum computation, in *superposition*:

$$|\eta\rangle \quad := \quad \frac{1}{\sqrt{L+1}} \sum_{\ell=0}^{L} |\alpha(\ell)\rangle \otimes |1^{\ell}0^{L-\ell}\rangle^{c}. \tag{1}$$

The right ($L$ qubits) register is a clock which counts the steps by adding 1s from left to right. The superscript $c$ denotes clock qubits. For simplicity, denote $|\gamma_\ell\rangle := |\alpha(\ell)\rangle \otimes |1^{\ell}0^{L-\ell}\rangle^{c}$. Kitaev [36] defined a Hamiltonian $H_{\rm final}$ involving five body interactions (three clock particles and two computation particles) that has $|\eta\rangle$ as its ground state. The idea is that the unary representation of the clock enables a local verification of correct propagation of the computation from one step to the next. For the initial Hamiltonian $H_{\rm init}$ we require that it has $|\gamma_0\rangle$ as its unique ground state. $H(t)$ is taken to be a convex combination of $H_{\rm init}$ and $H_{\rm final}$.

A technical problem lies in showing that the spectral gap of the intermediate Hamiltonian $H(t)$ is larger than $1/L^2$. To do this, we use a mapping of the Hamiltonian to a Markov chain corresponding to a random walk on the time steps. We then apply the conductance bound from the theory of rapidly mixing Markov chains [28] to bound the spectral gap of this chain. We note that in general, applying the conductance bound requires knowing the limiting distribution of the chain, which in our case is hard since it corresponds to knowing the coefficients of the ground state at all times. We circumvent this problem by noticing that it is actually sufficient in our case to know very little about the limiting distribution of the Markov chains, namely that it is monotone (in a certain sense to be defined later.). This allows us to apply the conductance bound, and deduce that the spectral gap is $\Omega(1/L^2)$. From this is follows that if $T \gg L^4$, the adiabatic system

[2] The importance of non-negligible spectral gaps to fault tolerance appeared already in geometric and topological quantum computation [32–34]. Note that these models differ from adiabatic computation in that the entire computational space has the same energy, and hence the spectral gap is irrelevant from an *algorithmic* point of view

[3] Otherwise, the first $n$ gates can be used to flip the qubits to the desired input.

will end up close to the history state $|\eta\rangle$. Extracting the output of the quantum circuit from the history state efficiently is easy: Measure all qubits and if the clock is at state $|1^l\rangle$, the computational qubits carry the result of the circuit. Otherwise, start from scratch [4].

This scheme would not suffice to prove Theorem 3. The basic problem lies in arranging sufficient interaction between the computational and the clock particles, since if the particles are set on a grid, each clock particle can only interact with four neighbors. We circumvent this problem as follows. Instead of having separate clock and computational particles, we now assign to each particle both clock and computational degrees of freedom (this is what makes our particles six-states). We then construct a computation that propagates locally over the entire set of particles, snaking up and down each column of the lattice. The adiabatic evolution would now end up in the history state of this snake-like sequence of states.

**Organization of Paper:** In Section 2 we describe the model and state some relevant facts about Markov chains. Section 3 shows how adiabatic systems with local Hamiltonians allowing five- and later three-body interactions, can simulate efficiently conventional quantum computations. Section 4 shows how to adapt the construction to a two-dimensional grid. We conclude with open questions.

# 2 Preliminaries

## 2.1 The Adiabatic Computation Model

For background on $n$-qubit systems, quantum circuits and Hamiltonians, see [35]. Consider a quantum system composed of $n$ particles, governed by Schrödinger's equation: $-i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$. $H(t)$, called the *Hamiltonian* of the system, is a Hermitian matrix. It's eigenvalues are called energies. We require that $H(t)$ is local, i.e., $H(t) = \sum_A H^A(t)$ where $A$ runs over constant size subsets of the particles, and $H^A(t)$ operates trivially on all but $A$ (i.e., it is a tensor product of a Hamiltonian on $A$ with identity on the particles outside of $A$). The system is initialized in a tensor product state, the ground state (lowest energy eigenstate) of the initial Hamiltonian $H_{\text{init}} = H(0)$. One then slowly modifies the Hamiltonian over a time of length $T$ from $H_{\text{init}}$ to $H_{\text{final}} = H(T)$ by setting $H(t) := (1 - t/T)H_{\text{init}} + (t/T)H_{\text{final}}$ (from now on we use $s = t/T$). In the limit of large $T$ we are guaranteed by the adiabatic theorem [22, 23] that the final state will be very close to the final ground state. Just how large $T$ should be is determined by the *spectral gap* of the time dependent Hamiltonian $H(s)$, denoted $\Delta(H(s))$, which is the difference between the Hamiltonian's lowest and next to lowest eigenvalue. More precisely, the adiabatic theorem requires that

$$T = \Omega\left(\frac{\|\frac{dH}{ds}\|}{\min_{s\in[0,1]}\{\Delta^2(H(s))\}}\right). \tag{2}$$

In fact, if there exists a subspace $\mathcal{S}$ such that $H(t)$ leaves $\mathcal{S}$ invariant for all $t$, and the initial groundstate belongs to $\mathcal{S}$, then it is sufficient that the above condition holds for $H(t)$ restricted to $\mathcal{S}$. For the adiabatic algorithm to be efficient, we require that $T$ is polynomial in $n$, i.e., bounded by $n^c$ for some constant $c$. Typically, the norm of $\frac{dH}{ds}$ is bounded by some small constant (2, in the cases we study). We therefore require that for all $s \in [0, 1]$ the spectral gaps $\Delta(H(s))$ are at least $1/n^c$ for some (preferably small) constant $c$. If this condition holds, the final state is close to the ground state of $H_{\text{final}}$, which can be thought of as the outcome of the computation. In the end, the particles are measured to give the result of the computation.

## 2.2 Markov Chains and Hermitian Matrices

Under certain conditions, there exists a standard mapping of Hermitian matrices to Markov chains (i.e., stochastic matrices). Let $G$ be a Hermitian matrix operating on an $L+1$ dimensional Hilbert space. Assume

[4] This gives an overhead factor of $L$, which can be avoided by adding, say, $10L$ identity gates to the quantum circuit at the end, so that most of the history state is concentrated on the final state $|\alpha(L)\rangle$)

that all the entries of $G$ are non-negative. Consider the eigenvector $(\alpha_0, \ldots, \alpha_L)$ of $G$, with the largest eigenvalue $\mu$. Assume $\mu > 0$ and $\alpha_i > 0$ for all $0 \leq i \leq L$. We can now define the matrix $P$ by:

$$P_{ij} := \frac{\alpha_j}{\mu \alpha_i} G_{ij}. \tag{3}$$

$P$ is well defined and is stochastic because all its entries are non-negative and each of its rows sums up to one. It is easy to verify the following fact:

**Fact 1.** *$(v_0, \ldots, v_L)$ is an eigenvector of $G$ with eigenvalue $\delta$ if and only if $(\alpha_0 v_0, \ldots, \alpha_L v_L)$ is a left eigenvector of $P$ with eigenvalue $\delta/\mu$.*

We will consider Hermitian matrices of the form $G = cI - H$ for some constant $c$ and some Hamiltonian $H$. The above fact implies that if $(\alpha_0, \ldots, \alpha_L)$ is the groundstate of $H$ with eigenvalue $\lambda$ then $(\alpha_0^2, \ldots, \alpha_L^2)$ is the limiting distribution of $P$ (i.e., left eigenvector with maximal eigenvalue 1), and the gap between $P$'s largest and second largest eigenvalues is equal to $\Delta(H)/(c - \lambda)$. Another useful fact is the following; its proof is based on the Perron-Frobenius theorem:

**Fact 2.** *[38] Let $G$ be Hermitian, with non-negative entries, and $\exists k < \infty$ s.t. all entries of $G^k$ are strictly positive. Then $G$'s largest eigenvalue is positive and non-degenerate. Moreover, all entries of the corresponding eigenvector are positive.*

### 2.3 Spectral Gaps of Markov Chains

Numerous techniques were developed to bound the spectral gap of a Markov chain matrix, as it is related [29] to the important quantity of the *mixing time* of the chain. In this paper we use the conductance bound [28]. Given a stochastic matrix $P$ with limiting distribution $\pi$, and a subset $B \subseteq \{0, \ldots, L\}$, the *flow* from $B$ is given by: $F(B) := \sum_{i \in B, j \notin B} \pi_i P_{ij}$. For each $B$, define the $\pi$-weight as $\pi(B) := \sum_{i \in B} \pi_i$. The *conductance* of $P$ is defined by

$$\varphi(P) \quad := \quad \min_B \frac{F(B)}{\pi(B)},$$

where we minimize over all non-empty subsets $B \subseteq \{0, \ldots, L\}$ with $\pi(B) \leq \frac{1}{2}$.

**Theorem 5. (The conductance bound [28])***: The eigenvalue gap of $P$ is $\geq \frac{1}{2}\varphi(P)^2$.*

## 3 Equivalence of Adiabatic and Quantum Computation

We show here how to simulate a quantum circuit with $L$ two-qubit gates on $n$ qubits by adiabatic computation on $n + L$ qubits. The initial ground state in the adiabatic evolution is $|\gamma_0\rangle = |0^n\rangle \otimes |0\rangle$, and the final state is, as explained in the introduction, the *history* state defined in Equation 1. We start by allowing *five* qubit interactions, and later show how to reduce it to three.

### 3.1 Universality of Adiabatic Computation with Five Qubit Interactions

#### 3.1.1 The Hamiltonian

We would like to define a Hamiltonian $H_{\text{init}}$ that has as its ground state $|\gamma_0\rangle$, and $H_{\text{final}}$ that has as its ground state $|\eta\rangle$. To do this, we construct local Hamiltonians which "check" that the ground states are the correct

ones, and assign energy penalty whenever this is not the case. The following Hamiltonian checks that the clock's state is indeed $\ell = 0$ in the beginning

$$H_{\text{clockinit}} = |1\rangle\langle 1|_1^c,$$

where the subscript indicates which clock qubits the projection operates on. We also define $H_{\text{clock}}$, which checks that the clock's state is always of the form of $|1^\ell 0^{L-\ell}\rangle^c$ by assigning an energy penalty to any basis state on the clock qubits that contains the sequence $01$:

$$H_{\text{clock}} \quad := \quad \sum_{\ell=1}^{L-1} |01\rangle\langle 01|_{\ell,\ell+1}^c,$$

The ground space $\mathcal{S}$ of $H_{\text{clock}}$ is spanned by exactly those states that represent a legal clock state. Next consider $H_{\text{input}}$, which checks that the input of the computational qubits is all zeroes, by penalizing all states with clock state $\ell = 0$ whose computation qubits are not all zero:

$$H_{\text{input}} \quad := \quad \sum_{i=1}^{n} |1\rangle\langle 1|_i \otimes |0\rangle\langle 0|_1^c.$$

We define:

$$H_{\text{init}} \quad := \quad H_{\text{clockinit}} + H_{\text{input}} + H_{\text{clock}} \tag{4}$$

**Claim 6.** *$|\gamma_0\rangle$ is a ground state of $H_{\text{init}}$ with eigenvalue $0$.*

*Proof.* The fact that $H_{\text{init}}|\gamma_0\rangle$ is easy to verify. All eigenvalues of $H_{\text{init}}$ are non negative since all terms in $H_{\text{init}}$ are positive semi definite. □

$H_{\text{final}}$ is defined by checking that the propagation from step $\ell - 1$ to $\ell$ is correct, i.e., corresponds to the application of the gate $U_\ell$:

$$H_{\text{final}} \quad := \quad \frac{1}{2}\sum_{\ell=1}^{L} H_\ell + H_{\text{input}} + H_{\text{clock}} \tag{5}$$

where for $1 < \ell < L$, the following Hamiltonian corresponds to the desired check:

$$H_\ell \quad := \quad \begin{array}{rcl} I \otimes |100\rangle\langle 100|_{\ell-1,\ell,\ell+1}^c & - & U_\ell \otimes |110\rangle\langle 100|_{\ell-1,\ell,\ell+1}^c \\ -U_\ell^\dagger \otimes |100\rangle\langle 110|_{\ell-1,\ell,\ell+1}^c & + & I \otimes |110\rangle\langle 110|_{\ell-1,\ell,\ell+1}^c \end{array}. \tag{6}$$

The three-qubit terms in $H_l$ can be seen as $|l\rangle\langle l|$, $|l-1\rangle\langle l-1|$, $|l\rangle\langle l-1|$ and $|l-1\rangle\langle l|$ respectively, i.e., corresponding to moving one step forward or backwards. For the boundary cases $\ell = 1, L$, we omit one clock qubit from these terms:

$$\begin{aligned} H_1 \quad &:= \quad I \otimes |10\rangle\langle 10|_{1,2} + I \otimes |00\rangle\langle 00|_{1,2} - U_1 \otimes |10\rangle\langle 00|_{1,2} - U_1^\dagger \otimes |00\rangle\langle 10|_{1,2} \\ H_L \quad &:= \quad I \otimes |11\rangle\langle 11|_{L-1,L} + I \otimes |10\rangle\langle 10|_{L-1,L} - U_L \otimes |11\rangle\langle 10|_{L-1,L} - U_L^\dagger \otimes |10\rangle\langle 11|_{L-1,L}. \end{aligned} \tag{7}$$

We remark that for the results in this subsection (and only here) the terms $H_{\text{clock}}$ and $H_{\text{input}}$ can be completely omitted. We introduce them here for the sake of consistency with the rest of the paper.

**Claim 7.** *$|\eta\rangle$ is the ground state of $H_{\text{final}}$ with eigenvalue $0$.*

*Proof.* Same as that of Claim 6. □

### 3.1.2 The Spectral Gap

It remains to show that the spectral gap of $H(s)$ is non-negligible. It is easy to verify that:

**Claim 8.** *The subspace $\mathcal{S}_0$, spanned by $|\gamma_0\rangle, \ldots, |\gamma_L\rangle$ is invariant under $H(s)$, i.e., $H(s)(\mathcal{S}_0) \subseteq \mathcal{S}_0$*

Hence, by Subsection 2.1, Theorem 1 follows from

**Claim 9.** $\Delta(H_{\mathcal{S}_0}(s)) = \Omega(L^{-2})$ *for all* $s \in [0,1]$.

(Here and later we use the notation $H_{\mathcal{A}}$ to denote the Hamiltonian restricted to a subspace $\mathcal{A}$.)

*Proof.* Let us write the Hamiltonians $H_{\mathcal{S}_0,\text{init}}$ and $H_{\mathcal{S}_0,\text{final}}$ in the basis $|\gamma_0\rangle, \ldots, |\gamma_L\rangle$ of $\mathcal{S}_0$. $H_{\text{clock}}$ and $H_{\text{input}}$ are 0 on $\mathcal{S}_0$ and can thus be ignored. We have the following $(L+1) \times (L+1)$ matrices:

$$H_{\mathcal{S}_0,init} = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}, \tag{8}$$

$$\begin{aligned} H_{\mathcal{S}_0,\text{final}} &= \tfrac{1}{2}|\gamma_0\rangle\langle\gamma_0| - \tfrac{1}{2}|\gamma_0\rangle\langle\gamma_1| - \tfrac{1}{2}|\gamma_L\rangle\langle\gamma_{L-1}| + \tfrac{1}{2}|\gamma_L\rangle\langle\gamma_L| \\ &\quad + \sum_{l=1}^{L-1}(-\tfrac{1}{2}|\gamma_l\rangle\langle\gamma_{l-1}| + |\gamma_l\rangle\langle\gamma_l| - \tfrac{1}{2}|\gamma_l\rangle\langle\gamma_{l+1}|) \\ &= \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 & & \cdots & & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & \ddots & & \vdots \\ 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & \ddots & \vdots \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \\ \vdots & & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & 0 \\ & & & 0 & -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & & \cdots & & 0 & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}. \end{aligned} \tag{9}$$

We now lower bound $\Delta(H_{\mathcal{S}_0})$. We consider two cases:

**The case** $s < 1/3$**:** Here, $H_{\mathcal{S}_0}(s)$ is sufficiently close to $H_{\mathcal{S}_0,\text{init}}$ which has a spectral gap of 1, and we can use standard techniques (Gerschgorin's Circle Theorem [39]) to show that the gap of $H_{\mathcal{S}_0}(s)$ is larger than $1/3$. Let $R_i = \sum_{j \neq i} |H_{\mathcal{S}_0}(s)_{ij}|$. The Circle Theorem states that for each $i$ there is an eigenvalue in the disk of radius $R_i$ around $H_{\mathcal{S}_0}(s)_{ii}$. For $s < 1/3$, $H_{\mathcal{S}_0}(s)_{0,0} \leq 1/6$ and $R_0 < 1/6$, so the corresponding eigenvalue is less than $1/3$. Similarly, we obtain that the eigenvalue corresponding to $H_{\mathcal{S}_0}(s)_{L,L}$ is at least $2/3$. For all $0 < i < L$, $R_i < 1/3$, and $H_{\mathcal{S}_0}(s)_{ii} = 1$, and so the remaining eigenvalues are also at least $2/3$. Hence the gap is larger than $1/3$.

**The case** $s \geq 1/3$**:** We note that $H_{\mathcal{S}_0,\text{final}}$ is the Laplacian of the simple random walk [29] of a particle on a line of length $L+1$. A standard result in Markov chain theory implies $\Delta(H_{\mathcal{S}_0,\text{final}} = \Omega(1/L^2)$ [29]. For large enough $s$, the matrix has enough weight of a random walk to apply Markov chain techniques.

Let $(\alpha_0, \ldots, \alpha_L)$ be the ground state of $H_{\mathcal{S}_0}(s)$ with the eigenvalue $\lambda$. Since the spectral norm of $H_{\mathcal{S}_0}(s)$ is at most 2, $\lambda$ is at most 2 in absolute value. Define the Hermitian matrix $G(s) = 4I - H_{\mathcal{S}_0}(s)$. Clearly, $G(s)$ has non-negative entries and for large enough $k$, all entries of $G(s)^k$ are strictly positive. Hence, following Fact 2, we obtain that the largest eigenvalue $\mu = 4 - \lambda$ of $G(s)$ is positive and non-degenerate and the corresponding eigenvector $(\alpha_0, \ldots, \alpha_L)$ has positive entries. We can now map the matrix $G(s)$ to a stochastic matrix $P(s)$ as described in Subsection 2.2. The transition matrix $P(s)$ describes a random walk on the line of $L+1$ sites:

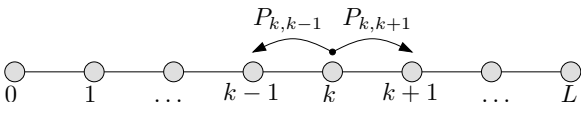


Figure 1: The random walk corresponding to $P(s)$

**Fact 3.** *For all $s > 0$, the ground state of $H_{\mathcal{S}_0}(s)$ is monotone, namely $\alpha_0 \geq \alpha_1 \geq \ldots \geq \alpha_L > 0$.*

*Proof.* It is easy to check that $G(s)$ preserves positivity and monotonicity, and $(\alpha_0, \ldots, \alpha_L)$ is the limit of the application of $G(s)/\mu$ on the monotone vector $(1, \ldots, 1)$ infinitely many times. (This is because all other eigenvalues of $G(s)$ are strictly smaller than $\mu$ in absolute value, so their contribution decays to 0.) □

Hence, the limiting distribution of $P(s)$, $\pi = (\alpha_0^2, \ldots, \alpha_L^2)$, is monotone. We use this and simple combinatorial arguments to prove the following claim, the proof of which can be found in Appendix A:

**Claim 10.** $\varphi(P(s)) \geq \frac{1}{36(L+1)}$

By Theorem 5, we have that the spectral gap of $P(s)$ is larger than $\frac{1}{2\cdot(36)^2\cdot(L+1)^2}$. We have by Subsection 2.2 that $\Delta(H_{\mathcal{S}_0}) \geq \frac{\mu}{2\cdot(36)^2(L+1)^2}$. Finally, notice that $\mu = 4 - \lambda \geq 2$ since $\lambda \leq 2$. □

**Remark** In fact, we can prove a lower bound on the full gap: $\Delta(H(s)) = \Omega(L^{-3})$, using the terms $H_{\text{clock}}$ and $H_{\text{input}}$. The proof follows the first part of the proof of Claim 11 and is omitted here.

### 3.2 From Five Qubits to Three

To move to three-body interactions, we modify $H_l$ in Equations 6,7, by leaving in the expressions corresponding to clock qubits only those terms which correspond to the current time step $\ell$:

$$H'_\ell := I \otimes |0\rangle\langle 0|^c_\ell - U_\ell \otimes |1\rangle\langle 0|^c_\ell - U^\dagger_\ell \otimes |0\rangle\langle 1|^c_\ell + I \otimes |1\rangle\langle 1|^c_\ell. \tag{10}$$

This introduces terms in the Hamiltonian which interact between legal and non-legal clock states, and so $H(s)$ no longer leaves the subspace $\mathcal{S}_0$ invariant. To this end, we assign a much larger energy penalty to states outside of the legal clock states. Set $J = O(L^9)$ and define:

$$H'_{\text{init}} := H_{\text{clockinit}} + J \cdot H_{\text{clock}} + H_{\text{input}} \quad , \quad H'_{\text{final}} := \frac{1}{2}\sum_{\ell=1}^{L} H'_\ell + J \cdot H_{\text{clock}} + H_{\text{input}} \tag{11}$$

Clearly, the new Hamiltonians have the same ground states as the old ones. Theorem 1 follows from:

**Claim 11.** $\Delta(H'(s)) = \Omega(L^{-3})$ *for all* $s \in [0, 1]$.

*Proof.* (Sketch. See appendix.) The proof builds on the proof of Claim 9, with two additional ideas. First, we restrict attention to states with legal clock states, i.e., states in $\mathcal{S}$, and observe that the Hamiltonian $H'_{\mathcal{S}}(s)$ can be block diagonalized, where one of the blocks is exactly $H_{\mathcal{S}_0}(s)$ from Claim 9. We show that the lowest eigenvalue in the other blocks is $\Omega(L^{-3})$ because of $H_{\text{input}}$ which is non zero there. This shows the desired spectral gap for $H'_{\mathcal{S}}(s)$. Since $\mathcal{S}$ is not invariant, we need to consider states outside of $\mathcal{S}$. We use similar ideas to those used in [40] in the context of quantum NP-complete problems: since the energy given to states outside of $\mathcal{S}$ by $H_{\text{clock}}$ is at least $J$, they cannot appear in the ground state of the Hamiltonian with large weights, and the interaction with them does not effect the lower energy states that much. □

# 4 Two-Body Local Interactions on a Two-Dimensional Lattice

In this section we prove Theorem 3. First, assume without loss of generality that the quantum circuit consists of $R$ rounds, where each round is composed of $n$ gates (some can be the identity gate), as in Figure 2. This can be done by introducing extra identity gates.

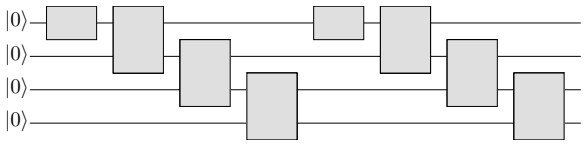


Figure 2: The first gate in each round is a one-qubit gate applied to the first qubit. For $i = 2, \ldots, n$, the $i$'th gate is a two-qubit gate applied to qubits $i-1$ and $i$.

The adiabatic computation is performed on 6-dimensional particles, arranged on a two-dimensional square lattice with $n$ rows and $R+1$ columns. Each column will correspond to a round of the computation of the circuit. The six internal states of each particle are divided to four groups, corresponding to four "clock" degrees of freedom: "unborn": $|\bigcirc\rangle$, "first phase":$|\updownarrow\rangle, |\updownarrow\rangle$, "second phase": $|\updownarrow\rangle, |\updownarrow\rangle$, and "dead":$|\otimes\rangle$. The two "first phase" states and two "second phase" states correspond to computational degrees of freedom, namely to the "zero" and "one" state of a qubit. We write $|\updownarrow\rangle$ (and similarly $|\updownarrow\rangle$) to denote a general state that belongs to the subspace spanned by $|\updownarrow\rangle$ and $|\updownarrow\rangle$.

We now define the states $|\gamma_l\rangle$. See Figure 4 for illustration. Once again, $|\gamma_0\rangle$ corresponds to the all $|0\rangle$ input to the quantum circuit. Here, it is the state in which the particles in the leftmost column are in $|\updownarrow\rangle$ whereas the rest are "unborn": $|\bigcirc\rangle$. $|\gamma_\ell\rangle$ transforms to $|\gamma_{\ell+1}\rangle$ by changing the particles on the lattice in the following order (which resembles a propagation of a snake): first, we modify the particles in the left most column from top to bottom, by applying the first round of computation on their internal qubit degree of freedom, while simultaneously changing the particle's state from a first-phase state to a second-phase state. Once we reach the last particle in the column, we start moving up the same column, copying the qubit's state of the particle one site to the right, leaving the copied particle in the "dead" phase, while the particle to the right is now in its first phase. When we reach the topmost particle in the column, all particles in this column are dead and the particles in the next column are ready for the next round of computation. Finally, in $|\gamma_L\rangle$ all columns but the last one are "dead", and the $n$ qubits in the right column are in the superposition corresponding to the final state of the quantum circuit, i.e., the superposition obtained by mapping $|0\rangle$ to $\updownarrow$ and $|1\rangle$ to $\updownarrow$. We get $L = 2(R+1)n$ states (two for each site in the lattice), plus the initial state.

As in the non-geometrical adiabatic computation, we now use the $|\gamma_\ell\rangle$ to define the initial and final groundstates: the initial groundstate of the adiabatic computation is $|\gamma_0\rangle$ and the final one is the history state $|\eta\rangle$ defined by $|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{\ell=0}^{L} |\gamma(\ell)\rangle$.

## 4.1 The Hamiltonian

The notion of a legal clock state now means a state whose clock degrees of freedom has the same *shape* as one of the states in Figure 4. The following claim is easy verification (see also Table 1).

**Claim 12.** *A state of $n \times R+1$ six state particles set in an $n \times (R+1)$ grid is of one of the shapes as in Figure 4 if none of the following forbidden configurations appear in the state:*

$\bigcirc\updownarrow$, $\bigcirc\updownarrow$, $\bigcirc\otimes$, $\updownarrow\otimes$, $\updownarrow\otimes$, $\otimes\bigcirc$, $\updownarrow\updownarrow$, $\updownarrow\updownarrow$, $\updownarrow\updownarrow$, $\updownarrow\updownarrow$

$$\begin{matrix}\bigcirc\\ \updownarrow\end{matrix}, \begin{matrix}\updownarrow\\ \updownarrow\end{matrix}, \begin{matrix}\otimes\\ \updownarrow\end{matrix}, \begin{matrix}\updownarrow\\ \bigcirc\end{matrix}, \begin{matrix}\updownarrow\\ \otimes\end{matrix}, \begin{matrix}\bigcirc\\ \otimes\end{matrix}, \begin{matrix}\otimes\\ \bigcirc\end{matrix}, \begin{matrix}\updownarrow\\ \bigcirc\end{matrix}, \begin{matrix}\otimes\\ \updownarrow\end{matrix}.$$

We define a two body nearest neighbor Hamiltonian which forbids the above configurations. For example, if the rule forbids $A = (i, j)$ in state $\bigcirc$ to the left of $B = (i, j + 1)$ in state $\bigotimes$, then the corresponding term in the Hamiltonian is $(|\bigcirc, \bigotimes\rangle\langle\bigcirc, \bigotimes|)_{A,B}$. Summing over all the forbidden configurations in Claim 12 applied to all pairs of particles, We have

$$H_{\text{clock}} \quad := \quad J \sum_{r \in \text{rules}} H_r$$

where $J = O(L^{-9})$. $H_{\text{input}}$ checks that none of particles in the leftmost column are in $|\Downarrow\rangle$:

$$H_{\text{input}} := \sum_{i=1}^{n} (|\Downarrow\rangle\langle\Downarrow|)_{i,1}.$$

We can now define the initial Hamiltonian to be:

$$H_{\text{init}} := (I - |\Uparrow\rangle\langle\Uparrow| - |\Downarrow\rangle\langle\Downarrow|)_{1,1} \quad + \quad H_{\text{input}} \quad + \quad H_{\text{clock}}.$$

The first term checks that the top left particle is in a $|\Updownarrow\rangle$ state. For $H_{\text{final}}$ we have:

$$H_{\text{final}} \quad := \quad \frac{1}{2} \sum_{\ell=1}^{L} H_\ell \quad + \quad H_{\text{input}} \quad + \quad H_{\text{clock}}.$$

As before, the terms $H_\ell$ check the propagation from $|\gamma_\ell\rangle$ to $|\gamma_{\ell+1}\rangle$. Since $|\gamma_\ell\rangle$ differs from $|\gamma_{\ell+1}\rangle$ only in two adjacent lattice sites, this is a two-body nearest neighbor Hamiltonian. There are two types of steps: an "upward" step and a "downward" step, and thus $H_\ell := H_\ell^{(u)} + H_\ell^{(d)}$. For the upward step, in which all that is supposed to happen is that the particle moves to the right and does not change its internal qubit state, the Hamiltonian is:

$$\begin{aligned} H_\ell^{(u)} \quad := \quad & |\bigotimes, \Uparrow\rangle\langle\bigotimes, \Uparrow| + |\circledast, \bigcirc\rangle\langle\circledast, \bigcirc| - |\bigotimes, \Uparrow\rangle\langle\circledast, \bigcirc| - |\circledast, \bigcirc\rangle\langle\bigotimes, \Uparrow| + \\ & |\bigotimes, \Downarrow\rangle\langle\bigotimes, \Downarrow| + |\circledast, \bigcirc\rangle\langle\circledast, \bigcirc| - |\bigotimes, \Downarrow\rangle\langle\circledast, \bigcirc| - |\circledast, \bigcirc\rangle\langle\bigotimes, \Downarrow|. \end{aligned}$$

where the left particle is followed by the right particle. The first line corresponds to changing the state $|\circledast, \bigcirc\rangle$ into $|\bigotimes, \Uparrow\rangle$. The second line is similar for $|\circledast, \bigcirc\rangle$ and $|\bigotimes, \Downarrow\rangle$.

For the downward step, $H_\ell^{(d)}$ needs to check that a two-qubit gate is applied correctly. We denote the upper particle involved in this gate first, followed by the lower particle in the gate. Restricted to the four $|\circledast, \Updownarrow\rangle$ states and to the four $|\circledast, \circledast\rangle$ states, $H_\ell^{(d)}$ is the following $8 \times 8$ matrix:

$$H_\ell^{(d)} \quad := \quad \begin{pmatrix} I & -U \\ -U^\dagger & I \end{pmatrix}$$

(cf. Equation 6); everywhere else $H_\ell^{(d)}$ is zero.

The Hamiltonians $H_\ell$ for the edge cases, i.e., the top most and bottom most particles of each column, are defined similarly, where the only difference is that the first gate of a round in the quantum circuit is a one-qubit gate, and so $H_\ell$ operates only on one particle. Formally, if $U$ is the corresponding gate, we define $H_l$ as the $4 \times 4$ matrix

$$H_l := \begin{pmatrix} I & -U \\ -U^\dagger & I \end{pmatrix}$$

operating on the two states $|\Updownarrow\rangle$ and the two states $|\circledast\rangle$. It is easy to check that

**Claim 13.** *$|\gamma_0\rangle$,$|\eta\rangle$ are the ground states of $H_{\text{init}}$, $H_{final}$, respectively, with eigenvalues $0$.*

It remains to prove that the spectral gap is non-negligible:

**Claim 14.** *$\Delta(H(s)) \geq 1/L^3$ for all $s \in [0, 1]$*

*Proof.* The proof is essentially identical to that of Claim 11. Note that here too $\mathcal{S}$ is not invariant. □

## 5 Conclusions and Open Questions

This paper demonstrates that quantum computation, its strengths and weaknesses, can be studied and implemented entirely within the adiabatic computation model, without losing its computational power. These results raise many open questions in various directions. Can the connections to new pools of techniques, in particular Markov chain Monte Carlo methods and adiabatic evolutions, be helpful in improving our understanding of the computational power of quantum systems, and in designing new algorithms? An important intermediate question is to try to understand known quantum algorithms in the adiabatic language; as we showed all known algorithms have efficient adiabatic representations.

A full fault tolerance theory for the adiabatic computation model is yet to be developed. In particular, experimental study of the susceptibility of adiabatic computations to decoherence and errors might be of great importance. Improving the parameters presented in this work, and in particular, making the simulation of quantum systems by adiabatic evolutions linear instead of polynomial, as well as decreasing the dimensionality of the particles from six to two or three, might be very important for implementation applications.

## 6 Acknowledgments

We wish to thank Dave Bacon, Ed Farhi, Leonid Gurvitz and Umesh Vazirani for inspiring discussions. DA's effort is supported in part by ARO grant number DAAD19-03-1-0082, NSF ITR grant number CCR-0121555. WvD work is supported in part by funds provided by the U.S. Department of Energy (DOE) and cooperative research agreement DF-FC02-94ER40818, by a CMI postdoctoral fellowship, and by an earlier HP/MSRI fellowship. JK's effort is partly sponsored by the Defense Advanced Research Projects Agency (DARPA) and Air Force Laboratory, Air Force Material Command, USAF, under agreement number F30602-01-2-0524 and FDN00014-01-1-0826. OR's effort is supported by the Army Research Office grant DAAD19-03-1-0082 and NSF grant CCR-9987845. Part of this work was done while DA, WvD, JK, ZL were members of the Mathematical Sciences Research Institute, Berkeley, CA, and OR was at the Institute for Advanced Study, Princeton, NJ.

## References

[1] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26(5):1484–1509, 1997.

[2] S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In *Proc. 34th STOC*, pages 653–58, 2002.

[3] W. van Dam and S. Hallgren. Efficient quantum algorithms for shifted quadratic character problems. Technical report, lanl-arXive quant-ph/0011067, 2000.

[4] J. Watrous. Quantum algorithms for solvable groups. In *Proc. 33rd STOC*, pages 60–67, 2001.

[5] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proc. 35th STOC*, pages 59–68, 2003. quant-ph/0209131.

[6] I.L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*', 80:3408–3411, 1998.

[7] J.A. Jones, M. Mosca, and R.H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. *Nature*, 393:344–346, 1998.

[8] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393:143–146, 1998.

[9] D.G. Cory, A.F. Fahmy, and T.F. Havel. Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing. *PhysComp96, Proceedings of the Fourth Workshop on Physics and Computation,T. Toffoli, M. Biafore, J. Leão, eds., (New England Complex Systems Institute, Boston)*, 1996.

[10] Q.A. Turchette, C.J. Hood, W. Lange, H. Mabuchi, and H.J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75:4710–4713, 1995.

[11] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, 75:4714–4717, 1995.

[12] Y. Nakamura, Yu. A. Pashkin, and J.S. Tsai. Coherent control of macroscopic quantum state in a single-cooper-pair box. *Nature*, 398:305, 1999.

[13] J. Preskill. Fault-tolerant quantum computation. In *Introduction to quantum computation and information*, pages 213–269. World Sci. Publishing, River Edge, NJ, 1998.

[14] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science*, 292(5516):472–476, 2001.

[15] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution. Technical report, lanl-arXive quant-ph/0001106, 2000.

[16] E. Farhi, J. Goldstone, and S. Gutmann. Quantum adiabatic evolution algorithms versus simulated annealing. Technical report, lanl-arXive quant-ph/0201031, 2002.

[17] B. Reichardt. The quantum adiabatic optimization algorithm and local minima. In *Proc. 36th STOC*, 2004.

[18] G.E. Santoro, R. Martonak, E. Tosatti, and R. Car. Theory of quantum annealing of an Ising spin glass. *Science*, 295:2427–30, 2002.

[19] W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? In *42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001)*, pages 279–287. IEEE Computer Soc., Los Alamitos, CA, 2001.

[20] A. Childs, E. Farhi, and J. Preskill. Robustness of adiabatic quantum computation. *Phys. Rev. A*, 65:012322, 2002. quant-ph/0108048.

[21] D. Aharonov and A. Ta-Shma. Adiabatic quantum state generation and statistical zero-knowledge. In *Proc. 35th STOC*, pages 20–29, 2003.

[22] T. Kato. On the adiabatic theorem of quantum mechanics. *J. Phys. Soc. Jap.*, 5:435–439, 1951.

[23] A. Messiah. *Quantum Mechanics*. John Wiley & Sons, New York, 1958.

[24] W. van Dam and U. Vazirani. More on the power of adiabatic computation. unpublished, 2001.

[25] J. Roland and N. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, 2002.

[26] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Letters*, 79:325, 1997. LANL preprint quant-ph/9706033.

[27] J. Friedman. *Expanding Graphs*. Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 1993.

[28] A. Sinclair and M. Jerrum. Approximate counting, uniform generation and rapidly mixing Markov chains (extended abstract). In *Graph-theoretic concepts in computer science (Staffelstein, 1987)*, volume 314 of *Lecture Notes in Comput. Sci.*, pages 134–148. Springer, Berlin, 1988.

[29] L. Lovász. Random walks on graphs: a survey. In *Combinatorics, Paul Erdős is eighty, Vol. 2 (Keszthely, 1993)*, volume 2 of *Bolyai Soc. Math. Stud.*, pages 353–397. János Bolyai Math. Soc., Budapest, 1996.

[30] W.L. Spitzer and S. Starr. Improved bounds on the spectral gap above frustration-free ground states of quantum spin chains. *Lett. Math. Phys.*, 63(2):165–177, 2003. lanl-arXive math-ph/0212029.

[31] M. Steffen, W. van Dam, T. Hogg, G. Breyta, and I. Chuang. On the adiabatic theorem of quantum mechanics. *Phys. Rev. Lett.*, 90, 2003.

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

[33] J. Pachos and P. Zanardi. Quantum holonomies for quantum computing. *Int.J.Mod.Phys. B*, 15:1257–1286, 2001.

[34] J. A. Jones, V. Vedral, A. Ekert, and G. Castagnoli. Geometric quantum computation with NMR. *Nature*, 403:869–871, 2000.

[35] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[36] A.Y. Kitaev, A.H. Shen, and M.N. Vyalyi. *Classical and Quantum Computation*. Number 47 in Graduate Series in Mathematics. AMS, Providence, RI, 2002.

[37] R. Feynman. Quantum mechanical computers. *Optics News*, 11:11–21, February 1985.

[38] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1985.

[39] R. Bhatia. *Matrix Analysis*. Number 169 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[40] J. Kempe and O. Regev. 3-local Hamiltonian is QMA-complete. *Quantum Inf. Comput.*, 3(3):258–264, 2003.

# A Proof of Claim 10

For the proof, we consider two cases, depending on whether the set $B$ contains $0$ or not.

- If $0 \in B$: Let $k$ be the smallest index such that $k \in B$ but $k+1 \notin B$. Clearly, $F(B) \geq \pi_k P(s)_{k,k+1} = \alpha_k \alpha_{k+1} G(s)_{k,k+1}/(4-\lambda)$. We bound each of these terms. We have $\alpha_{k+1}, \alpha_k \geq \frac{1}{\sqrt{2(L+1)}}$, since by $\pi(B) \leq \frac{1}{2}$ and the monotonicity of $\alpha_i^2$, we have the bound $\frac{1}{2} \leq \alpha_{k+1}^2 + \cdots + \alpha_n^2 \leq (L+1)\alpha_{k+1}^2$. Also, using the definition of $G$ and the assumption that $s \geq 1/3$ we get that $G(s)_{k,k+1} \geq \frac{1}{6}$, which gives the lower bound $F(B) \geq \frac{1}{12(4-\lambda)(L+1)}$, and since $2 \leq 4-\lambda \leq 6$, $F(B)/\pi(B) \geq \frac{1}{36(L+1)}$.

- If $0 \notin B$, we let $k$ be the smallest index such that $k \notin B$ but $k+1 \in B$. Because of the monotonicity of $\alpha_i^2$, we know that $\pi(B) \leq \alpha_{k+1}^2 + \cdots + \alpha_L^2 \leq \alpha_{k+1}^2(L+1)$. Again, we have $F(B) \geq \alpha_k \alpha_{k+1} G(s)_{k,k+1}/(4-\lambda)$ and hence $F(B)/\pi(B) \geq \frac{1}{6}\alpha_k\alpha_{k+1}/((4-\lambda)\alpha_{k+1}^2(L+1)) \geq \frac{1}{6(4-\lambda)(L+1)} \geq \frac{1}{36(L+1)}$.

Together these show the desired bound.

# B Proof of Spectral Gap For Three Qubit Interactions

Here we prove Claim 11. We first consider $H'_{\mathcal{S}}(s)$. From now on we omit the prime. This Hamiltonian is block diagonal as in Figure 3.

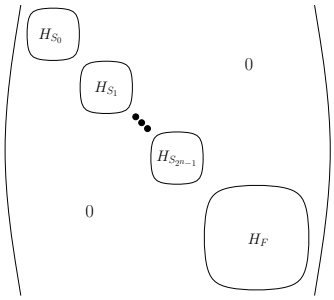


Figure 3: The Hamiltonian $H(s)$ can be block diagonalized as above.

In the first subspace is $\mathcal{S}_0$ we get exactly the same Hamiltonian which we have dealt with in Claim 9. In addition, we have many subspaces, denoted $\mathcal{S}_j$, which can be viewed as the analogues of $\mathcal{S}_0$. $\mathcal{S}_0$ consists of the set of states which the quantum circuit reaches starting from the all zero input. $\mathcal{S}_j$ consists of the set of states which the quantum circuit reaches starting from the $j$'th input, i.e., the $n$ bit binary representation of $j \in \{0, \ldots, 2^n - 1\}$. The $\mathcal{S}_j$'s span $\mathcal{S}$. We first show

**Claim 15.** *The spectral gap of $H_{\mathcal{S}}(s)$ is $\Omega(1/L^3)$.*

*Proof.* By Claim 9, it suffices to argue that the energy of $H_{\mathcal{S}}(s)$ on each of the $\mathcal{S}_j$ for $j \neq 0$ is at least $1/L^3$. This is true because of the penalty assigned by $H_{\text{input}}$, but the argument is slightly subtle since $H_{\text{input}}$ applies only for the first clock's state. We have $H_{\mathcal{S}_j}(s) = H_{\mathcal{S}_0}(s) + H_{\mathcal{S}_j,\text{input}}$. $H_{\mathcal{S}_j,\text{input}}$ is diagonal, with its top left element at least 1 (it actually equals the number of 1's in the binary representation of $j$) and all other diagonal elements are zero. Hence, we can lower bound the ground energy of $H_{\mathcal{S}_j}(s)$ with the ground energy of the Hamiltonian $H_{\mathcal{S}_0}(s) + H'$ where

$$H' := \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

We can now use a geometrical lemma by Kitaev (Lemma 14.4 in [36]) that bounds the ground energy of the sum of two Hamiltonians. It states that if the spectral gaps of both Hamiltonians are larger than $\Lambda$, and the angle between the two ground spaces is $\theta$, then the ground energy of the sum is at least $2\Lambda \sin^2(\theta/2)$. In our case, the spectral gaps are $\Omega(L^2)$ by Claim 9. Moreover, the angle between the ground states satisfies $\cos(\theta) \leq 1 - 1/L$ by the monotonicity of the ground state of $H_{\mathcal{S}_0}(s)$. It follows that the ground energy of $H_{\mathcal{S}_j}(s)$ is $\Omega(1/L^3)$ for all $\mathcal{S}_j$ with $j \neq 0$. □

We now want to consider the entire Hilbert space, including states outside of $\mathcal{S}_0$. We use similar ideas to those used in [40] in the context of quantum NP-complete problems. The following lemma allows us to eliminate the interaction between $\mathcal{S}$ and its orthogonal space which we denote $\mathcal{F}$, and essentially consider only the Hamiltonian restricted to the space $\mathcal{S}$ while ignoring the $\mathcal{F}$ space completely. Once restricted to the space $\mathcal{S}$, the spectral gap analysis follows from Claim 15.

We would like to say that since the energy given to states in $\mathcal{F}$ is so high, they cannot appear in the ground state of the Hamiltonian with large weights, and the interaction with them does not effect the lower energy states that much. This is captured by the following general lemma, where we assume that $J$, the penalty for being in the forbidden subspace, is much larger than the size of the interaction between the forbidden subspace and the valid subspace. $K$ in the following upper bounds this interaction, and thus we assume $J \gg K$ in the following lemma.

**Lemma 16.** *Let $H = H_1 + H_2$ be the sum of two Hamiltonians operating on some Hilbert space $\mathcal{H} = \mathcal{S} + \mathcal{F}$. The Hamiltonian $H_2$ is such that all its eigenvectors are inside either $\mathcal{S}$ or $\mathcal{F}$. Moreover, the eigenvalues of eigenvectors in $\mathcal{S}$ are $0$ and those of eigenvectors in $\mathcal{F}$ are at least $J$. Also, assume that $\|H_1\| \leq K$ for some $K \geq 1$. Assume that the Hamiltonian $H_{\mathcal{S},1}$, i.e., the restriction of $H$ to the space $\mathcal{S}$, has an eigenvector $|\eta\rangle \in \mathcal{S}$ with eigenvalue 0 and all other eigenvectors are with eigenvalues at least 1. Then, the Hamiltonian $H$ has an eigenvector $|\eta'\rangle$ with eigenvalue at most 0 such that $\||\eta'\rangle - |\eta\rangle\| \leq 8K^{3/4}/J^{1/4}$ and all other eigenvectors are with eigenvalues at least $1 - 70K^{3/2}/\sqrt{J}$.*

*Proof.* Any vector $|v\rangle \in \mathcal{H}$ can be written as $|v\rangle = \alpha_1|v_1\rangle + \alpha_2|v_2\rangle$ with $|v_1\rangle \in \mathcal{S}$, $|v_2\rangle \in \mathcal{F}$, $\alpha_1, \alpha_2 \in \mathcal{R}$, $\alpha_1 \geq 0$ and $\alpha_1^2 + \alpha_2^2 = 1$.
**Fact 1:**

$$\alpha_2^2 \leq \frac{\langle v|H|v\rangle + K}{J}$$

*Proof:* $\langle v|H|v\rangle \geq \langle v|H_2|v\rangle - \|H_1\| \geq J\alpha_2^2 - K$.
**Fact 2:**

$$\langle v|H|v\rangle \geq \langle v_1|H_1|v_1\rangle - 4K|\alpha_2|$$

*Proof:* Write

$$\begin{aligned} \langle v|H|v\rangle &\geq \langle v|H_1|v\rangle = (1-\alpha_2^2)\langle v_1|H_1|v_1\rangle + 2\alpha_1\alpha_2 Re\langle v_1|H_1|v_2\rangle + \alpha_2^2\langle v_2|H_1|v_2\rangle \\ &\geq \langle v_1|H_1|v_1\rangle - K(2\alpha_2^2 + 2|\alpha_2|) \end{aligned}$$

using $\alpha_1 \leq 1$. The result follows with $|\alpha_2| \geq \alpha_2^2$.

In the first part of the proof we will show that $|\eta'\rangle$ exists and that it's very close to $|\eta\rangle$. First,

$$\langle \eta|H|\eta\rangle = \langle \eta|H_1|\eta\rangle + \langle \eta|H_2|\eta\rangle = \langle \eta|H_1|\eta\rangle = 0$$

where we used $|\eta\rangle \in \mathcal{S}$. Therefore, the Hamiltonian $H$ must have an eigenvector $|\eta'\rangle$ whose eigenvalue is at most $0$. Write

$$|\eta'\rangle = \alpha_1|\eta_1'\rangle + \alpha_2|\eta_2'\rangle$$

with $|\eta_1'\rangle \in \mathcal{S}$, $|\eta_2'\rangle \in \mathcal{F}$, $\alpha_1, \alpha_2 \in \mathcal{R}$ such that $\alpha_1 \geq 0$, $\alpha_1^2 + \alpha_2^2 = 1$ and use Fact 1 to obtain $|\alpha_2| \leq \sqrt{\frac{K}{J}}$ and then Fact 2 together with $|\eta_1'\rangle \in \mathcal{S}$ to get

$$4\frac{K^{3/2}}{\sqrt{J}} \geq \langle \eta_1'|H_1|\eta_1'\rangle = \langle \eta_1'|\Pi H_1 \Pi|\eta_1'\rangle.$$

Write

$$|\eta_1'\rangle = \gamma_1|\eta\rangle + \gamma_2|\eta^\perp\rangle$$

and let us assume that we have chosen the phase of $|\eta'\rangle$ such that $\gamma_1 \geq 0$. Then $\langle\eta'_1|\Pi H_1 \Pi|\eta'_1\rangle = \gamma_2^2 \langle\eta^\perp|\Pi H_1\Pi|\eta^\perp\rangle \geq \gamma_2^2$ using $\Pi H_1 \Pi|\eta\rangle = 0$ and the assumption on $\Pi H_1 \Pi$.

Finally, we get that

$$\begin{aligned} \||\eta'\rangle - |\eta\rangle\| &\leq \||\eta'\rangle - \alpha_1|\eta'_1\rangle\| + \|\alpha_1|\eta'_1\rangle - |\eta'_1\rangle\| + \||\eta'_1\rangle - \gamma_1|\eta\rangle\| + \|\gamma_1|\eta\rangle - |\eta\rangle\| \leq \\ &\sqrt{K/J} + K/J + 2K^{3/4}/J^{1/4} + 4K^{3/2}/\sqrt{J} \leq 8K^{3/4}/J^{1/4} \end{aligned}$$

where we used $\alpha_1 \geq \alpha_1^2 \geq 1 - K/J$ and $\gamma_1 \geq \gamma_1^2 \geq 1 - 4K^{3/2}/\sqrt{J}$.

In the second part of the proof we will show that for any vector $|\xi\rangle$ orthogonal to $|\eta'\rangle$, $\langle\xi|H|\xi\rangle \geq 1 - 70K^{3/2}/\sqrt{J}$. As before, we write

$$|\xi\rangle = \beta_1|\xi_1\rangle + \beta_2|\xi_2\rangle$$

with $|\xi_1\rangle \in \mathcal{S}$, $|\xi_2\rangle \in \mathcal{F}$, $\beta_1, \beta_2 \in \mathcal{R}$ such that $\beta_1^2 + \beta_2^2 = 1$. Then from Fact 1,

$$\beta_2^2 \leq \frac{\langle\xi|H|\xi\rangle + K}{J}$$

Therefore, if $\beta_2^2 \geq 2K/J$ we are done. Assume that $\beta_2^2 < 2K/J$. From Fact 2 and our assumptions on $\Pi H_1 \Pi$ it follows that

$$\begin{aligned} \langle\xi|H|\xi\rangle &\geq \langle\xi_1|H_1|\xi_1\rangle - 4\sqrt{2K^3/J} \\ &= \langle\xi_1|\Pi H_1\Pi|\xi_1\rangle - 4\sqrt{2K^3/J} \\ &\geq 1 - |\langle\eta|\xi_1\rangle|^2 - 4\sqrt{2K^3/J} \end{aligned}$$

Now, using $\langle\eta'|\xi\rangle = 0$ and $|\eta\rangle \in \mathcal{S}$:

$$|\langle\eta|\xi_1\rangle| = |\langle\eta|\xi\rangle| = |\langle\eta|\xi\rangle| - |\langle\eta'|\xi\rangle| \leq |\langle\eta - \eta'|\xi\rangle| \leq \||\eta\rangle - |\eta'\rangle\| \leq 8\frac{K^{3/4}}{J^{1/4}}$$

Finally, by combining the inequalities above, we obtain

$$\langle\xi|H|\xi\rangle \geq 1 - 64K^{3/2}/\sqrt{J} - 4\sqrt{2}K^{3/2}/\sqrt{J} \geq 1 - 70K^{3/2}/\sqrt{J}$$

□

**Corollary 17.** *Let $H = H_1 + H_2$ be the sum of two Hamiltonians operating on some Hilbert space $\mathcal{H} = \mathcal{S} + \mathcal{F}$. The Hamiltonian $H_2$ is such that all its eigenvectors are inside either $\mathcal{S}$ or $\mathcal{F}$. Moreover, the eigenvalues of eigenvectors in $\mathcal{S}$ are $0$ and those of eigenvectors in $\mathcal{F}$ are at least $J$. Also, assume that $\|H_1\| \leq K$ for some $K \geq 1$. Assume that the Hamiltonian $H_{\mathcal{S},1}$ has an eigenvector $|\eta\rangle \in \mathcal{S}$ with eigenvalue $a$ and all other eigenvectors are with eigenvalues at least $b$. Then, the Hamiltonian $H$ has an eigenvector $|\eta'\rangle$ with eigenvalue at most $a$ such that*

$$\||\eta'\rangle - |\eta\rangle\| \leq 8\frac{(K+a)^{3/4}}{J^{1/4}\sqrt{b-a}}$$

*and all other eigenvectors are with eigenvalues at least $b - 70(K+a)^{3/2}/\sqrt{J}$.*

*Proof.* Define $H'_1 = (H_1 - a \cdot I)/(b-a)$, $H'_2 = H_2/(b-a)$ and $H' = H'_1 + H'_2$. Notice that $\|H'_1\| \leq (K+a)/(b-a)$ and that $H'_2$ eigenvalues on $\mathcal{F}$ are at least $J/(b-a)$. Then, using the above lemma, we obtain that $H'$ has an eigenvector with eigenvalue at most $0$ whose distance from $|\eta\rangle$ is at most $8((K+a)/(b-a))^{3/4}/(J/(b-a))^{1/4}$. Moreover, all other eigenvectors of $H'$ are with eigenvalues at least $1 - 70((K+a)/(b-a))^{3/2}/\sqrt{J/(b-a)}$. We now complete the proof by translating these results back to $H$. □

We apply Corollary 17 by taking $H_2$ to be $H_{clock}$ and $H_1$ to be the remaining terms such that $H(s) = H_1 + H_2$. Notice that $\|H_1\| \leq O(L)$ because it consists of $O(L)$ terms, each of constant norm. Also note that the ground energy $a$ of $H_{\mathcal{S},1} = H_{\mathcal{S}}(s)$ is at most $\frac{1}{2}$. Moreover, we have $b - a \geq 1/L^3$ by the same proof as in the spectral gap of the non-geometrical Hamiltonian. Hence, Corollary 17 implies that the spectral gap decreases by at most

$$70(K+a)^{3/2}/\sqrt{J} = O(L^{3/2}/\sqrt{J}).$$

Moreover, the distance between the ground state of $H(1)$ and $|\eta\rangle$ is at most

$$8\frac{(K+a)^{3/4}}{J^{1/4}\sqrt{b-a}} = O(L^{3/4}/J^{1/4}).$$

By choosing $J = O(L^9)$ we obtain that the spectral gap of $H(s)$ is at least $1/(2L^3)$ and that the ground state of $H(1)$ is close to $|\eta\rangle$. Hence, adiabatic simulation in time $O(L^6)$ is possible.

## C The States $|\gamma_\ell\rangle$ For the Two Dimensional Construction

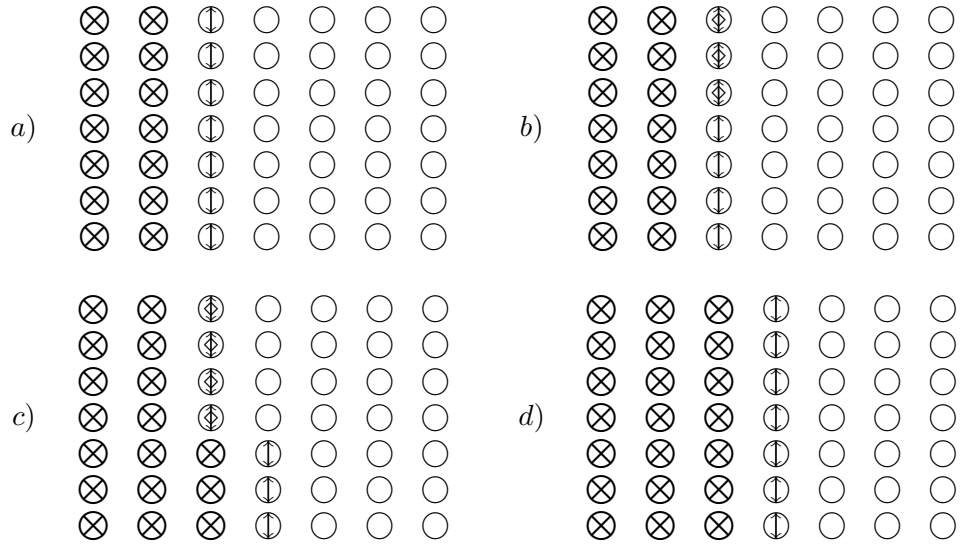


Figure 4: a) The state at the beginning of the $r$'th round. The $n$ particles in the $r$th column are in their "first phase", where their computational degrees of freedom are in the state of the circuit's qubits in the beginning of the $r$th round. b) Next, the gates of the $r$th round of the circuit are applied on the qubits from top to bottom. The particles on which the gates have been applied are now in their "second phase." c) Next, the particle's computational state are moved one column to the right, and their phase becomes "first" again. The internal qubit-state of the particles does not change in this phase. d) Once this phase is over, we are back to a state of the same shape we had in a), one column (and one round) further.

## D Rules for the Clock Hamiltonian on the Lattice

| Forbidden configuration | Guarantees that |
|---|---|
| $\bigcirc\updownarrow, \bigcirc\Updownarrow, \bigcirc\otimes$ | $\bigcirc$ is to the right of all other qubits |
| $\bigcirc\otimes, \updownarrow\otimes, \Updownarrow\otimes$ | $\otimes$ is to the left of all other qubits |
| $\bigcirc\otimes, \otimes\bigcirc$ | $\bigcirc$ and $\otimes$ are not horizontally adjacent |
| $\updownarrow\updownarrow, \updownarrow\Updownarrow, \Updownarrow\updownarrow, \Updownarrow\Updownarrow$ | only one of $\updownarrow$, $\Updownarrow$ per row |
| $\begin{matrix}\bigcirc\\ \Updownarrow\end{matrix}$ , $\begin{matrix}\updownarrow\\ \Updownarrow\end{matrix}$ , $\begin{matrix}\otimes\\ \Updownarrow\end{matrix}$ | only $\Updownarrow$ above $\Updownarrow$ |
| $\begin{matrix}\updownarrow\\ \bigcirc\end{matrix}$ , $\begin{matrix}\updownarrow\\ \Updownarrow\end{matrix}$ , $\begin{matrix}\updownarrow\\ \otimes\end{matrix}$ | only $\updownarrow$ below $\updownarrow$ |
| $\begin{matrix}\bigcirc & \otimes\\ \otimes & \bigcirc\end{matrix}$ | $\bigcirc$ and $\otimes$ are not vertically adjacent |
| $\begin{matrix}\Updownarrow & \otimes\\ \bigcirc & \updownarrow\end{matrix}$ | no $\bigcirc$ below $\Updownarrow$ and no $\updownarrow$ below $\otimes$ |

Table 1: Local rules that guarantee that a basis state is in $\mathcal{S}$