2013 IEEE 54th Annual Symposium on Foundations of Computer Science

Quantum 3-SAT is QMA_1-complete

David Gosset
University of Waterloo
dngosset@gmail.com

Daniel Nagaj
University of Vienna and
Institute of Physics, Slovak Academy of Sciences
daniel.nagaj@univie.ac.at

***Abstract*—Quantum satisfiability is a constraint satisfaction problem that generalizes classical boolean satisfiability. In the quantum k-SAT problem, each constraint is specified by a k-local projector and is satisfied by any state in its nullspace. Bravyi showed that quantum 2-SAT can be solved efficiently on a classical computer and that quantum k-SAT with $k \geq 4$ is QMA_1-complete [4]. Quantum 3-SAT was known to be contained in QMA_1 [4], but its computational hardness was unknown until now. We prove that quantum 3-SAT is QMA_1-hard, and therefore complete for this complexity class.**

***Keywords*-Quantum computing; Computational complexity**

I. Introduction

Bravyi introduced a quantum generalization of k-SAT and characterized its complexity for $k = 2$ and $k \geq 4$ [4]. In the quantum k-SAT problem the constraints act on an n-qubit Hilbert space and we are asked to determine if there is a state which satisfies all of them. Each constraint is specified by a k-local[1] projector and is satisfied by any state in its nullspace.

Less is known about quantum k-SAT than is known about its classical counterpart. Random instances of quantum k-SAT have been studied by Laumann et. al. as a function of the clause density α [16], [15]. As in the classical case, it is conjectured that a satisfiability threshold $\alpha_c(k)$ exists, above which the probability that a random instance is satisfiable approaches zero as $n \to \infty$ and below which this probability approaches one [16]. Some bounds on this threshold value have been proven using a quantum version of the Lovász local lemma [2] and by using graph-theoretic techniques [6] but only the case $k = 2$ is fully understood [16], [10]. Other previous work has focused on quantum satisfiability with qudit variables of dimension $d > 2$ [18], [20], [8], [5] or in restricted geometries [18], [7].

Quantum satisfiability is relevant to the study of *frustration-free* Hamiltonians. A frustration-free Hamiltonian is a local Hamiltonian (a sum of k-local Hermitian operators for some constant k) with groundstates that minimize the energy of each local term individually. Such Hamiltonians naturally arise in the study of quantum error correction and play a central role in the field of Hamiltonian complexity [22]. We can view quantum k-SAT as the problem where one is asked to determine if a sum of k-local projectors is frustration-free, that is to say, if its ground energy is zero.

The computational complexity of quantum k-SAT is naturally compared with that of the k-local Hamiltonian problem, which can be viewed as the quantum analogue of MAX k-SAT. In this problem one is given a Hamiltonian which is a sum of k-local operators, along with constants a, b such that $a < b$. One is asked to determine if the ground energy of the given Hamiltonian is less than a (yes instance) or greater than b (no instance), promised that one of these conditions holds. Note that, for yes instances of this problem, a ground state of the Hamiltonian need not have minimal energy for each k-local term; such a system can be frustrated. Because of the possibility of frustration, the k-local Hamiltonian problem can be computationally more difficult than quantum k-SAT. Indeed, the k-local Hamiltonian problem is QMA-complete for $k \geq 2$ [12]. On the other hand, our result that quantum 3-SAT is QMA_1-complete shows that these problems are of comparable difficulty for $k \geq 3$ (putting aside the subtle differences between the definitions of QMA and QMA_1).

In the next Section, we provide the basic definitions, describe our results in more detail and give an overview of this extended abstract. Details which are not included here due to space constraints can be found in the full version [9] of this paper.

II. Definitions and Overview

We first define the complexity class QMA, or Quantum Merlin-Arthur. This class gets its name from a scenario involving Merlin and Arthur, who at the outset are both given an instance of a promise problem encoded as a bit-string X. Arthur wishes to know the correct answer to this problem (which is either yes or no) but his time and space resources are bounded as polynomial functions of $|X|$. Merlin has unbounded computational power and can easily obtain the correct answer. Merlin wants to convince Arthur the answer is "yes", but Arthur doesn't trust Merlin, so he asks for proof. Merlin hands over an n-qubit quantum state $|W\rangle$ (called a witness) that Arthur uses to verify the claim in the following way. He adjoins some number n_a of ancilla qubits each in the state $|0\rangle$ to produce $|W\rangle|0\rangle^{\otimes n_a}$ (the total number $n+n_a$ of qubits in this state must be upper bounded by a polynomial in $|X|$), then applies a polynomial

[1]A k-local operator acts nontrivially on at most k qubits and as the identity on all other qubits.

0272-5428/13 $26.00 © 2013 IEEE
DOI 10.1109/FOCS.2013.86

IEEE computer society

sized verification circuit U_X and then measures the first ancilla qubit in the computational basis. If the measurement outcome is 1, he accepts Merlin's claim that X is a yes instance. Arthur's acceptance probability given the state $|W\rangle$ is therefore

$$\mathrm{AP}\left(U_X, |W\rangle\right) = \left\| \left(\mathbb{I}^{\otimes n} \otimes |1\rangle\langle 1|_{(n+1)} \otimes \mathbb{I}^{\otimes(n_a-1)}\right) U_X |W\rangle |0\rangle^{\otimes n_a} \right\|^2 . \quad (1)$$

For problems in the class QMA, if Merlin is being truthful he can convince Arthur with probability at least $\frac{2}{3}$. On the other hand, if Merlin is lying (i.e., the answer is actually "no") then he can only fool Arthur with probability at most $\frac{1}{3}$.

Definition 1 (**QMA**)**.** A promise problem $L_{\text{yes}} \cup L_{\text{no}} \subset \{0,1\}^*$ is contained in QMA if and only if there exists a uniform polynomial-size quantum circuit family U_X such that

If $X \in L_{\text{yes}}$ there exists a state $|W\rangle$ such that $\mathrm{AP}\left(U_X, |W\rangle\right) \geq \frac{2}{3}$ (completeness).

If $X \in L_{\text{no}}$ then $\mathrm{AP}\left(U_X, |W\rangle\right) \leq \frac{1}{3}$ for any state $|W\rangle$ (soundness).

Here we have defined QMA with constant completeness $\frac{2}{3}$ and soundness $\frac{1}{3}$. Kitaev showed that these parameters can be amplified: we obtain an equivalent definition with soundness $2^{-\Omega(|X|^{\alpha})}$ and completeness $1-2^{-\Omega(|X|^{\alpha})}$ for any constant α [13] (see also [17], [21]).

QMA_1 is defined in a similar way to QMA with two modifications. The first is "perfect" completeness – for $X \in L_{\text{yes}}$, Merlin can convince Arthur with probability exactly equal to 1. The second difference is that Arthur's verification circuit must consist of a sequence of gates from a fixed universal gate set $\mathcal{G}$. The definition of QMA_1 is not known to be independent of the gate set used. In this paper we use the standard choice

$$\mathcal{G} = \{\widehat{H}, T, \mathrm{CNOT}\}, \quad (2)$$

where $\widehat{H}$ is the single-qubit Hadamard gate, $T = \mathrm{diag}(1, e^{i\frac{\pi}{4}})$ and CNOT is the controlled-NOT gate.

Definition 2 (**QMA_1**)**.** A promise problem $L_{\text{yes}} \cup L_{\text{no}} \subset \{0,1\}^*$ is contained in QMA_1 if and only if there exists a uniform polynomial-size quantum circuit family U_X over the gate set $\mathcal{G}$ such that

If $X \in L_{\text{yes}}$ there exists a state $|W\rangle$ such that $\mathrm{AP}\left(U_X, |W\rangle\right) = 1$ (perfect completeness).

If $X \in L_{\text{no}}$ then $\mathrm{AP}\left(U_X, |W\rangle\right) \leq \frac{1}{3}$ for any state $|W\rangle$ (soundness).

Just as with QMA, the soundness of a QMA_1 verification procedure (taken to be $\frac{1}{3}$ in the above) can be amplified so that it is very close to zero [13].

We think of QMA_1 as being very similar to QMA, although the precise relationship between these two classes has yet to be determined (see [1], [11], [14] for recent developments).

Let us now turn our attention to quantum 3-SAT. In this problem we are given a Hamiltonian

$$H = \sum_{i=1}^{r} \Pi_i$$

that is a sum of 3-local projectors Π_i acting on an n-qubit Hilbert space. We are promised that either H has ground state energy zero, or else its ground state energy is greater than a constant (which we take without loss of generality to be 1) and we are asked to decide which is the case.

Note that the matrix elements of a projector Π_i in an instance of quantum 3-SAT cannot be specified as arbitrary complex numbers with unlimited precision. In our definition of quantum 3-SAT we must constrain the set of allowed projectors in some way.

In this work we define quantum 3-SAT with a restricted set of projectors $\mathcal{P}$ given below. While quantum 3-SAT remains in QMA_1 for larger classes of projectors, restricting to a smaller set makes our QMA_1-hardness result stronger. The specific set $\mathcal{P}$ that we use arises from technical considerations.

Definition 3. Let $\mathcal{P}$ be the set of 3-local projectors Π which satisfy one of the following two conditions:

1. Every matrix element of Π in the computational basis has the form

$$\frac{1}{4}\left(a + i\,b + \sqrt{2}\,c + i\sqrt{2}\,d\right) \qquad a,b,c,d \in \mathbb{Z}. \quad (3)$$

2. There is a 3-qubit unitary U with matrix elements of the form (3) (in the computational basis) such that $U \Pi U^{\dagger}$ is equal to

$$\left(\sqrt{\frac{1}{3}}|000\rangle - \sqrt{\frac{2}{3}}|001\rangle\right)\left(\sqrt{\frac{1}{3}}\langle 000| - \sqrt{\frac{2}{3}}\langle 001|\right)$$

on 3 of the qubits tensored with the identity on the remaining qubits.

Definition 4 (**Quantum 3-SAT**)**.** Given a collection $\{\Pi_i : i = 1, \ldots, r\} \subset \mathcal{P}$ of 3-local projectors acting on n qubits, we are asked to decide if they correspond to a yes instance or a no instance (promised that one is the case), where

Yes: There exists an n-qubit state $|\psi\rangle$ satisfying $\Pi_i|\psi\rangle = 0$ for all $i = 1, \ldots, r$.

No: $\sum_i \langle\psi|\Pi_i|\psi\rangle \geq 1$ for all $|\psi\rangle$.

With the definitions given above, we prove that quantum 3-SAT is QMA_1-complete. In reference [9] we provide a proof (following Bravyi [4], [3]) that quantum 3-SAT is contained in QMA_1. Our main result in this paper is QMA_1-hardness of quantum 3-SAT. To prove this, we exhibit an efficiently computable mapping from a g-gate, $(n+n_a)$-qubit verification circuit that implements a unitary U_X to a Hamiltonian

$$H_X = \sum_i \Pi_{i,X}$$

which is a sum of $\Theta\left(n_a+g\right)$ 3-local projectors $\Pi_{i,X} \in \mathcal{P}$ acting on $\Theta(n+n_a+g)$ qubits. Moreover, we prove

Theorem 1 (**Completeness**). *H_X has ground energy 0 if and only if there exists $|W\rangle$ such that $AP\left(U_X, |W\rangle\right) = 1$,*

Theorem 2 (**Soundness**). *If $AP\left(U_X, |W\rangle\right) \leq \frac{1}{3}$ for all $|W\rangle$, then H_X has ground energy $\Omega\left(\frac{1}{g^6}\right)$.*

Note that in our definition of quantum 3-SAT we require that in the "no" case the ground energy is greater than or equal to 1, whereas Theorem 2 gives a bound of $\Omega\left(g^{-6}\right)$. To form an instance of quantum 3-SAT as defined above we repeat each projector $\Pi_{i,X}$ in the instance a suitable number of times (i.e., $\Theta(g^6)$ times). This shows that any promise problem in QMA_1 can be reduced to quantum 3-SAT. Since quantum 3-SAT is also contained in QMA_1 we have proven that it is complete for this complexity class.

Our mapping from the verification circuit U_X to the Hamiltonian H_X relies on two technical innovations. Like many previous works in the field of Hamiltonian complexity, we use a "clock construction". In this work we introduce a new one which has some special properties. In Section III we summarize the relevant properties; details can be found in the full version [9]. Most previous QMA- or QMA_1-hardness results use a circuit-to-Hamiltonian mapping which is an immediate and simple application of the clock construction (the standard approach uses a Hilbert space with a computational register and a clock register). In contrast, in this work we define a novel circuit-to-Hamiltonian mapping where the Hamiltonian H_X acts on a Hilbert space with a computational register along with *two* clock registers. In Section IV we illustrate the main ideas of this mapping, and in Section V we define the Hamiltonian H_X and prove Theorem 1. The proof of Theorem 2 is more involved, and is given in [9].

III. A NEW CLOCK CONSTRUCTION

A clock construction is a local Hamiltonian along with a set of local operators which act on its groundspace in a certain way. It can be used as a set of building blocks to define more complicated Hamiltonians while keeping track of the groundspace.

In this Section we summarize our new clock construction which is presented in full detail in [9]. This extended abstract can be understood using only the properties which we now describe.

For any $N \in \{2, 3, \dots\}$, we present a Hamiltonian $H_{\text{clock}}^{(N)}$ which acts on the Hilbert space of $7N-3$ qubits and which is a sum of 3-local projectors from the set $\mathcal{P}$ given in Definition 3. The zero energy groundspace of $H_{\text{clock}}^{(N)}$ is spanned by orthonormal states

$$|C_i\rangle, \quad i = 1, \dots, N.$$

Now let $\mathcal{H}_{\text{comp}}$ be a computational register containing some (arbitrary) number of qubits, and let U be a unitary acting on this register. We exhibit projectors

$$h_{i,i+1}(U)$$

for $i = 1, \dots, N-1$, which act on

$$\mathcal{H}_{\text{comp}} \otimes \mathcal{H}_{\text{clock}}^{(N)}.$$

These are called the *transition operators* for the clock. They satisfy

$$\begin{aligned} &\left(\mathbb{I} \otimes \Pi_{\text{clock}}^{(N)}\right) h_{i,i+1}(U) \left(\mathbb{I} \otimes \Pi_{\text{clock}}^{(N)}\right) && (4) \\ =&\frac{1}{8}\left(\mathbb{I} \otimes |C_i\rangle\langle C_i| + \mathbb{I} \otimes |C_{i+1}\rangle\langle C_{i+1}|\right) \\ -&\frac{1}{8}\left(U^\dagger \otimes |C_i\rangle\langle C_{i+1}| + U \otimes |C_{i+1}\rangle\langle C_i|\right), && (5) \end{aligned}$$

where $\Pi_{\text{clock}}^{(N)} = \sum_{i=1}^N |C_i\rangle\langle C_i|$ projects onto the clock subspace. The operator $h_{i,i+1}(U)$ is a $(k+2)$-local projector where k is the locality of the unitary U. When U is the identity the projector $h_{i,i+1}(1)$ acts nontrivially only on two qubits of $\mathcal{H}_{\text{clock}}^{(N)}$ and we write

$$h_{i,i+1} \doteq h_{i,i+1}(\mathbb{I}).$$

Thus, for a single-qubit unitary, $h_{i,i+1}(U)$ is only 3-local (this is in contrast with the original clock construction due to Kitaev [13] where the analogous operators are 4-local). Our circuit-to-Hamiltonian mapping, presented in Sections IV and V exploits this feature (it is partly inspired by the railroad switch idea from [19]).

Finally, we also exhibit 1-local (single-qubit) projectors

$$C_{\geq i} \qquad \text{and} \qquad C_{\leq i} \tag{6}$$

for $i = 1, \dots, N$, whose role is to "pick out" clock states $|C_j\rangle$ with $j \geq i$ or $j \leq i$ respectively. They act on the Hilbert space $\mathcal{H}_{\text{clock}}^{(N)}$ and satisfy

$$\Pi_{\text{clock}}^{(N)} C_{\geq i} \Pi_{\text{clock}}^{(N)} = \frac{1}{2}|C_i\rangle\langle C_i| + \sum_{i<j\leq N} |C_j\rangle\langle C_j| \tag{7}$$

$$\Pi_{\text{clock}}^{(N)} C_{\leq i} \Pi_{\text{clock}}^{(N)} = \sum_{1\leq j<i} |C_j\rangle\langle C_j| + \frac{1}{2}|C_i\rangle\langle C_i| \tag{8}$$

with the understanding that when $i = 1$ the first term in (8) is zero and when $i = N$ the second term in (7) is zero. Only the nullspaces of the operators on the RHS of (7) and (8) are important for our purposes. In particular, it is not significant that the $|C_i\rangle\langle C_i|$ terms have different prefactors, since the (positive) value of these coefficients do not affect the nullspace.

IV. Hamiltonians acting on two clock registers

We now develop the main ideas behind our circuit-to-Hamiltonian mapping, using the new clock construction described in the previous section. A key feature of our approach is that we use two clock registers, with Hilbert space

$$\mathcal{H}_{\text{clock}}^{(N)} \otimes \mathcal{H}_{\text{clock}}^{(N)}. \tag{9}$$

Let's consider some local operators which act on this space. The Hamiltonians

$$\mathbb{I} \otimes H_{\text{clock}}^{(N)} \quad \text{and} \quad H_{\text{clock}}^{(N)} \otimes \mathbb{I}$$

are both sums of 3-local projectors as discussed in the previous section. Since $C_{\leq i}$ and $C_{\geq i}$ are 1-local projectors, we can form 2-local projectors by taking tensor products, e.g.,

$$C_{\leq i} \otimes C_{\geq j}.$$

Similarly, since the operators $h_{k,k+1}$ are 2-local projectors, terms such as

$$h_{k,k+1} \otimes C_{\leq i}$$

are 3-local projectors. For convenience and to ease notation later on, we define the following sum of such terms

$$\begin{aligned} S^{(k,k+2)} &= C_{\leq k} \otimes C_{\geq (k+2)} + h_{k,k+1} \otimes C_{\leq (k+1)} \\ &+ h_{(k+1),(k+2)} \otimes C_{\geq (k+1)} + C_{\geq (k+2)} \otimes C_{\leq k} \\ &+ C_{\leq (k+1)} \otimes h_{k,k+1} + C_{\geq (k+1)} \otimes h_{(k+1),(k+2)} \end{aligned} \tag{10}$$

for $k = 1, \ldots, N-2$.

We begin by looking at a simple Hamiltonian which acts in the Hilbert space (9); this example introduces some notation and conventions that we use later on. We then consider two examples where the Hilbert space (9) is tensored with a computational register. These examples contain the essential ideas behind our proof that quantum 3-SAT is QMA$_1$-hard.

A. Warm up example

As a warm-up, consider the following Hamiltonian acting on the space (9) with $N = 9$:

$$\mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + S^{(4,6)}, \tag{11}$$

with $S^{(4,6)}$ given by (10). We will see how the zero energy groundspace of this operator can be represented pictorially.

Recall (from Section III) that $H_{\text{clock}}^{(9)}$ has 9 orthonormal zero energy states $|C_i\rangle$ for $i = 1, \ldots, 9$. The first two terms of (11)

$$\mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} \tag{12}$$

therefore have 81 zero energy ground states which we choose to represent as a set of vertices arranged in a 2D grid, as shown in Figure 1(a). We adopt the convention that the vertex in the top left corner has coordinates $(i, j) = (1, 1)$, the i coordinate increases moving to the right and the j coordinate increases moving downwards. The vertex with coordinate (i, j) is associated with the groundstate $|C_i\rangle|C_j\rangle$.

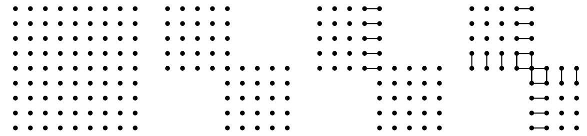


Figure 1. The groundspaces of (a) $\mathbb{I}\otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)}\otimes\mathbb{I}$, (b) $\mathbb{I}\otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)}\otimes\mathbb{I} + C_{\leq 4}\otimes C_{\geq 6} + C_{\geq 6}\otimes C_{\leq 4}$, (c) $\mathbb{I}\otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)}\otimes\mathbb{I} + C_{\leq 4}\otimes C_{\geq 6} + C_{\geq 6}\otimes C_{\leq 4} + h_{4,5}\otimes C_{\leq 5}$, and (d) $\mathbb{I}\otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)}\otimes\mathbb{I} + S^{(4,6)}$. In these graphs each connected component is associated with a ground state of the Hamiltonian.

We add $S^{(4,6)}$ to (12) a few terms at a time. First look at

$$\mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + C_{\leq 4} \otimes C_{\geq 6} + C_{\geq 6} \otimes C_{\leq 4}$$

which is just the first two terms of $S^{(4,6)}$ added to (12). Using the expressions (7) and (8) we see that adding this term assigns an energy penalty to all the states $|C_i\rangle|C_j\rangle$ with either $i \leq 4$ and $j \geq 6$ or $i \geq 6$ and $j \leq 4$. Eliminating the corresponding vertices from Figure 1(a) we get Figure 1(b).

Now look at the next term which is $h_{4,5} \otimes C_{\leq 5}$. Using equations (5) and (8) we get

$$\begin{aligned} &\left(\Pi_{\text{clock}}^{(9)} \otimes \Pi_{\text{clock}}^{(9)}\right)(h_{4,5} \otimes C_{\leq 5})\left(\Pi_{\text{clock}}^{(9)} \otimes \Pi_{\text{clock}}^{(9)}\right) \\ &= \frac{1}{8}(|C_4\rangle - |C_5\rangle)(\langle C_4| - \langle C_5|) \otimes \sum_{j=1}^{5}\left(1 - \frac{1}{2}\delta_{j,5}\right)|C_j\rangle\langle C_j|. \end{aligned}$$

From this we see that states $|C_4\rangle|C_j\rangle$ and $|C_5\rangle|C_j\rangle$ for $j = 1, \ldots, 5$ are not zero energy states for this term although their uniform superpositions $\frac{1}{\sqrt{2}}(|C_4\rangle + |C_5\rangle)|C_j\rangle$ are. We represent the groundspace of

$$\begin{aligned} \mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + C_{\leq 4} \otimes C_{\geq 6} \\ + C_{\geq 6} \otimes C_{\leq 4} + h_{4,5} \otimes C_{\leq 5} \end{aligned} \tag{13}$$

as the graph in Figure 1(c), where now ground states are in one-to-one correspondence with the *connected components* of the graph. The ground state corresponding to a given connected component $\mathcal{J}$ is the uniform superposition

$$\sum_{(i,j)\in\mathcal{J}} |C_i\rangle|C_j\rangle$$

(up to normalization). The next three terms modify the picture in a similar way and the groundspace of $\mathbb{I}\otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + S^{(4,6)}$ is represented as the graph shown in Figure 1(d).

B. A single-qubit unitary

Next, consider an example with two clock registers with $N = 6$ and a computational register containing a single qubit. The Hilbert space is $\mathbb{C}^2 \otimes \mathcal{H}_{\text{clock}}^{(6)} \otimes \mathcal{H}_{\text{clock}}^{(6)}$. Let U be a

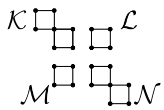


Figure 2. The four groundstates of $H_{\text{clock}}^{(6)} \otimes \mathbb{I} + \mathbb{I} \otimes H_{\text{clock}}^{(6)} + S^{(1,3)} + S^{(4,6)}$ are associated with the four connected components of this graph, which we label $\mathcal{K}, \mathcal{L}, \mathcal{M}, \mathcal{N}$.

(single-qubit) unitary acting on the computational qubit and define

$$H_{1\text{q}}(U) = \mathbb{I} \otimes \mathbb{I} \otimes H_{\text{clock}}^{(6)} + \mathbb{I} \otimes H_{\text{clock}}^{(6)} \otimes \mathbb{I} + \mathbb{I} \otimes S^{(1,3)} + \mathbb{I} \otimes S^{(4,6)} + H_U, \tag{14}$$

where

$$H_U = h_{34}(U) \otimes \mathbb{I} + \mathbb{I} \otimes \mathbb{I} \otimes h_{34}. \tag{15}$$

Here $h_{34}(U)$ acts nontrivially on the computational qubit and two qubits of first clock register.

We analyze the groundspace of (14) in two steps. First, we represent the groundspace of the sum of the first four terms using a picture, as in the previous example. Then we consider the action of H_U on this space and obtain the zero energy states for (14).

First, consider

$$\mathbb{I} \otimes H_{\text{clock}}^{(6)} + H_{\text{clock}}^{(6)} \otimes \mathbb{I} + S^{(1,3)} + S^{(4,6)},$$

which acts in the space $\mathcal{H}_{\text{clock}}^{(6)} \otimes \mathcal{H}_{\text{clock}}^{(6)}$ and note (using the graphical representation discussed in the previous example) that its nullspace can be represented as Figure 2. In the Figure we label vertices of the graph as (i,j) with the top left vertex labeled $(1,1)$, i increasing to the right and j increasing downward. A ground state is associated with each connected component $\mathcal{K}, \mathcal{L}, \mathcal{M}, \mathcal{N}$ as shown in the Figure, given by

$$|\mathcal{S}\rangle = \sum_{(i,j) \in \mathcal{S}} |C_i\rangle |C_j\rangle, \tag{16}$$

where $\mathcal{S} \in \{\mathcal{K}, \mathcal{L}, \mathcal{M}, \mathcal{N}\}$. In this paper we will often work with unnormalized states such as these.

The groundstates of $H_{1\text{q}}(U)$ are superpositions of

$$|z\rangle|\mathcal{K}\rangle, \quad |z\rangle|\mathcal{L}\rangle, \quad |z\rangle|\mathcal{M}\rangle, \quad |z\rangle|\mathcal{N}\rangle, \quad z \in \{0,1\}. \tag{17}$$

which have zero energy for H_U. We solve for them as follows. First, note that

$$|z\rangle|\mathcal{K}\rangle, \quad U|z\rangle|\mathcal{L}\rangle, \quad |z\rangle|\mathcal{M}\rangle, \quad U|z\rangle|\mathcal{N}\rangle \tag{18}$$

for $z \in \{0,1\}$ span the same space as (17). This basis is convenient because H_U does not connect states with $z = 0$ to states with $z = 1$. We evaluate the matrix elements of H_U between these unnormalized states using (5). For each $z \in \{0,1\}$, H_U acts as a 4×4 matrix within the space spanned by the four states (18) (since it does not connect states with different z). This matrix is the same for $z = 0$ and $z = 1$ and is given by

$$\frac{1}{4}\begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix},$$

with the ordering of basis states as in (18). The unique zero eigenvector of this matrix is the all-ones vector. This means that the groundspace of $H_{1\text{q}}(U)$ is spanned by the two states

$$|z\rangle|\mathcal{K}\rangle + U|z\rangle|\mathcal{L}\rangle + |z\rangle|\mathcal{M}\rangle + U|z\rangle|\mathcal{N}\rangle, \quad z \in \{0,1\}.$$

Note that to solve for these zero energy eigenvectors it was sufficient to consider the matrix elements of H_U in the unnormalized basis (18).

Now considering superpositions of these two states we see that every state in the groundspace of $H_{1\text{q}}(U)$ has the form

$$|\phi\rangle|\mathcal{K}\rangle + U|\phi\rangle|\mathcal{L}\rangle + |\phi\rangle|\mathcal{M}\rangle + U|\phi\rangle|\mathcal{N}\rangle \tag{19}$$

for some single-qubit state $|\phi\rangle$. In this example we view the state $|C_1\rangle|C_1\rangle$ (corresponding to the top left vertex in Figure 2) as the initial state of the two clocks, and we view the state $|C_6\rangle|C_6\rangle$ (the bottom right vertex) as the final state. We interpret (19) as a history state for the computation that consists of applying U to the state $|\phi\rangle$.

C. A two-qubit unitary

Now consider an example where $N = 9$ and the computational register contains two qubits. The Hilbert space is $(\mathbb{C}^2)^2 \otimes \mathcal{H}_{\text{clock}}^{(9)} \otimes \mathcal{H}_{\text{clock}}^{(9)}$.

Define

$$H_{2\text{q}} = \mathbb{I} \otimes \mathbb{I} \otimes H_{\text{clock}}^{(9)} + \mathbb{I} \otimes H_{\text{clock}}^{(9)} \otimes \mathbb{I} + \mathbb{I} \otimes S^{(1,3)} + \mathbb{I} \otimes S^{(7,9)} + H_V, \tag{20}$$

where

$$H_V = H_{\text{horizontal}} + H_{\text{vertical}} \tag{21}$$

and $H_{\text{horizontal}}$ involves transitions of the first clock register whereas H_{vertical} involves transitions of the second clock register. Labeling the first computational (control) qubit a and the second (target) one b, we define

$$\begin{aligned} H_{\text{horizontal}} &= |0\rangle\langle 0|_a \otimes h_{34} \otimes \mathbb{I} + \mathbb{I} \otimes h_{34} \otimes C_{\geq 7} \\ &+ \mathbb{I} \otimes h_{56} \otimes C_{\leq 3} + h_{45}(B_b) \otimes \mathbb{I} + |0\rangle\langle 0|_a \otimes h_{67} \otimes \mathbb{I} \\ &+ \mathbb{I} \otimes h_{67} \otimes C_{\geq 7} + \mathbb{I} \otimes h_{56} \otimes C_{\geq 7}, \end{aligned} \tag{22}$$

$$\begin{aligned} H_{\text{vertical}} &= |1\rangle\langle 1|_a \otimes \mathbb{I} \otimes h_{34} + \mathbb{I} \otimes C_{\geq 7} \otimes h_{34} \\ &+ \mathbb{I} \otimes C_{\leq 3} \otimes h_{56} + h_{45}(\sigma_b^z) + |1\rangle\langle 1|_a \otimes \mathbb{I} \otimes h_{67} \\ &+ \mathbb{I} \otimes C_{\geq 7} \otimes h_{67} + \mathbb{I} \otimes C_{\geq 7} \otimes h_{56}. \end{aligned} \tag{23}$$

Here the single-qubit unitaries which act on qubit b are

$$\sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{24}$$

In (23) the operator $h_{45}(\sigma_b^z)$ acts nontrivially on the computational qubit b as well as the second clock register (and acts as the identity on the first clock register).

Note that $H_{2\text{q}}$ is a sum of 3-local projectors. We now discuss its groundspace.

Look at the first four terms in (20) which act as

$$\mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + S^{(1,3)} + S^{(7,9)} \tag{25}$$

on the two clock registers. Using our graphical notation, the zero energy groundspace of (25) can be represented as the black graph shown in Figure 3 (a) and (b). A ground state is associated with each of the 25 connected components of this graph (as discussed in the Figure caption). Now adjoining the two-qubit computational register, we get 100 basis vectors for the nullspace of

$$\mathbb{I}\otimes\mathbb{I}\otimes H_{\text{clock}}^{(9)} + \mathbb{I}\otimes H_{\text{clock}}^{(9)} \otimes\mathbb{I} + \mathbb{I}\otimes S^{(1,3)} + \mathbb{I}\otimes S^{(7,9)}, \tag{26}$$

four for each connected component. States in the nullspace of $H_{2\text{q}}$ are superpositions of these 100 basis vectors that also have zero energy for H_V, that is to say, zero eigenvectors of the matrix

$$\langle \mathcal{J}_2 | \langle y' | \langle x' | H_V | x \rangle | y \rangle | \mathcal{J}_1 \rangle \tag{27}$$

where $\mathcal{J}_1$ and $\mathcal{J}_2$ are connected components of the graph in Figure 3 and $x, y, x', y' \in \{0,1\}$. (Here $|\mathcal{J}_1\rangle$ and $|\mathcal{J}_2\rangle$ are defined through (16)). One could now proceed to solve for the nullspace of $H_{2\text{q}}$ by explicitly constructing the matrix elements (27) and analyzing the resulting 100×100 matrix. However, computing the matrix elements (27) is a tedious exercise. To save space and time, we take a different approach here. We provide a Lemma which characterizes the nullspace of $H_{2\text{q}}$, and we describe a simple way that the reader can verify our claim.

It will be helpful to use the sets of vertices $\mathcal{R}_0, \mathcal{G}_0, \mathcal{Y}_0, \mathcal{B}_0$ and $\mathcal{R}_1, \mathcal{G}_1, \mathcal{Y}_1, \mathcal{B}_1$ depicted in Figure 3. For each set we define an unnormalized state through (16) (now letting $\mathcal{S}$ be any set of vertices). For example,

$$\begin{aligned} |\mathcal{Y}_0\rangle = &|C_2\rangle|C_7\rangle + |C_3\rangle|C_7\rangle + |C_4\rangle|C_7\rangle \\ &+ |C_2\rangle|C_8\rangle + |C_3\rangle|C_8\rangle + |C_4\rangle|C_8\rangle. \end{aligned}$$

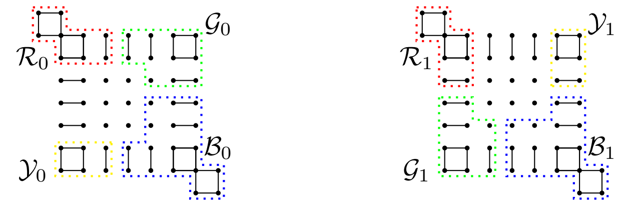
Note that each of the states

$$|\mathcal{R}_0\rangle, |\mathcal{G}_0\rangle, |\mathcal{Y}_0\rangle, |\mathcal{B}_0\rangle, |\mathcal{R}_1\rangle, |\mathcal{G}_1\rangle, |\mathcal{Y}_1\rangle, |\mathcal{B}_1\rangle \tag{28}$$

have zero energy for (25). The following Lemma characterizes the groundspace of $H_{2\text{q}}$.

Lemma 1. *The groundspace of H_{2q} is spanned by*

$$\begin{aligned} |\psi_V^{xy}\rangle = &|x\rangle|y\rangle|\mathcal{R}_x\rangle + (Q|x\rangle|y\rangle)\,|\mathcal{G}_x\rangle \\ &+ \big(\tilde{Q}|x\rangle|y\rangle\big)|\mathcal{Y}_x\rangle + (V|x\rangle|y\rangle)\,|\mathcal{B}_x\rangle \end{aligned}$$



(a) (b)

Figure 3. The black graph (drawn twice for clarity) depicts the groundspace of $\mathbb{I} \otimes H_{\text{clock}}^{(9)} + H_{\text{clock}}^{(9)} \otimes \mathbb{I} + S^{(1,3)} + S^{(7,9)}$. The top left vertex is labeled $(1,1)$ and the bottom right vertex $(9,9)$. Each connected component corresponds to a ground state, given by the uniform superposition of states $|C_i\rangle|C_j\rangle$ with (i,j) in the component. In (a) we have defined sets of vertices $\mathcal{R}_0, \mathcal{G}_0, \mathcal{Y}_0, \mathcal{B}_0$ and in (b) we have defined sets $\mathcal{R}_1, \mathcal{G}_1, \mathcal{Y}_1, \mathcal{B}_1$.

for $x, y \in \{0,1\}$, where the two-qubit unitaries $Q, \tilde{Q}$, and V are given by

$$\begin{aligned} Q &= |0\rangle\langle 0| \otimes B + |1\rangle\langle 1| \otimes \sigma^z, \\ \tilde{Q} &= |0\rangle\langle 0| \otimes \big(B^\dagger \sigma^z B\big) + |1\rangle\langle 1| \otimes (\sigma^z B \sigma^z)\,, \\ V &= |0\rangle\langle 0| \otimes (\sigma^z B) + |1\rangle\langle 1| \otimes (B\sigma^z)\,, \end{aligned} \tag{29}$$

with the single-qubit unitaries B and σ^z as in (24).

Note that, since $|\psi_V^{xy}\rangle$ has support only on states (28) of the clock registers, it has zero energy for (26). Using equations (5), (7), and (8) the reader can verify that each state $|\psi_V^{xy}\rangle$ also has zero energy for H_V. It remains to show that these four states span the groundspace of $H_{2\text{q}}$. We recommend using a computer to verify this fact. To do this, one can numerically diagonalize a specific 324×324 matrix: the restriction of $H_{2\text{q}}$ to the space spanned by $|z_1\rangle|z_2\rangle|C_i\rangle|C_j\rangle$ with $i, j = 1, \ldots, 9$ and $z_1, z_2 \in \{0,1\}$. It is easy to compute the matrix elements of $H_{2\text{q}}$ in this basis using equations (5), (7), and (8). We have included in our arxiv submission [9] an ancillary file (a Matlab script) which numerically diagonalizes this matrix and confirms that the states $|\psi_V^{xy}\rangle$ span the nullspace of $H_{2\text{q}}$.

Using Lemma 1 we see that any state in the groundspace of $H_{2\text{q}}$ is a superposition

$$\sum_{x,y\in\{0,1\}} \alpha_{xy} |\psi_V^{xy}\rangle = |\phi\rangle|C_1\rangle|C_1\rangle + |\text{other}\rangle + V|\phi\rangle|C_9\rangle|C_9\rangle, \tag{30}$$

where

$$|\phi\rangle = \sum_{x,y\in\{0,1\}} \alpha_{xy} |x\rangle|y\rangle,$$

and $|\text{other}\rangle$ has no support on clock states $|C_1\rangle|C_1\rangle$ or $|C_9\rangle|C_9\rangle$. We view $|C_1\rangle|C_1\rangle$ as the initial state of the two clocks and $|C_9\rangle|C_9\rangle$ as the final state of the two clocks, and we interpret (30) as a history state for the computation that consists of applying the two-qubit unitary V from (29) to the state $|\phi\rangle$.

Finally, we show that the two-qubit unitary V is an entangling gate. To see this, note that by multiplying it with single-qubit T and Hadamard gates we obtain the CNOT gate:

$$\left(T^2 \otimes \left(T^6 \hat{H} T^2\right)\right) V = \text{CNOT}. \tag{31}$$

The reader may already see where this is going. In this Section we exhibited Hamiltonians $H_{1\mathrm{q}}(U)$ and $H_{2\mathrm{q}}$ which are sums of 3-local projectors and which have ground states that can be viewed as history states for any one-qubit computation and a specific two-qubit computation respectively. Now we show how to put these ideas together to make a quantum 3-SAT Hamiltonian that is associated with a sequence of one- and two-qubit gates.

V. Quantum 3-SAT is QMA_1-hard

In this Section we exhibit the Hamiltonian H_X and we prove Theorem 1. The proof of Theorem 2 is given in the full version [9] of this paper.

Recall from Section II that we consider a verification circuit which implements a unitary U_X on $n+n_a$ qubits, n_a of which are ancillas initialized to $|0\rangle$ at the beginning of the computation. It is expressed as a product of g gates from the set $\{\widehat{H}, T, \text{CNOT}\}$. We begin by rewriting this circuit in a canonical form.

Equation (31) expresses the CNOT gate as a product of $\hat{H}$ and T gates and the two-qubit gate V (29). Using this identity it is possible [9] to efficiently rewrite the given circuit so that it is a product of $\Theta(g)$ gates from the set $\{\widehat{H}, T, V\}$, with $M = \Theta(g)$ single-qubit gates alternating with M two-qubit V gates:

$$U_X = V_{a_{M-1} b_{M-1}} U^{M-1} \ldots V_{a_1 b_1} U^1 V_{a_0 b_0} U^0, \tag{32}$$

where each single-qubit gate $U^0, U^2, \ldots U^{M-1}$ is either $\widehat{H}$, T or the identity, and where

$$a_0, \ldots, a_{M-1}, b_0, \ldots, b_{M-1} \in [n + n_a]$$

are the labels of the qubits on which the V gates act.

A. The Hamiltonian H_X

We define a Hamiltonian H_X which we associate with the verification circuit (32) and which is a sum of 3-local projectors from the set $\mathcal{P}$ in Definition 3. It acts on the Hilbert space

$$\mathcal{H}_{\text{comp}} \otimes \mathcal{H}_{\text{clock}}^{(9M+3)} \otimes \mathcal{H}_{\text{clock}}^{(9M+3)}, \tag{33}$$

where $\mathcal{H}_{\text{comp}}$ is a computational register containing $n + n_a$ qubits. Note that each of the two clock registers contains $63M + 18$ qubits.

First, consider the Hilbert space $\mathcal{H}_{\text{clock}}^{(9M+3)} \otimes \mathcal{H}_{\text{clock}}^{(9M+3)}$ of the two clock registers and define the following operator acting on this space

$$\begin{aligned} H_{\text{diag}}^{(M)} &= H_{\text{clock}}^{(9M+3)} \otimes \mathbb{I} + \mathbb{I} \otimes H_{\text{clock}}^{(9M+3)} + S^{(9M+1,9M+3)} \\ &+ \sum_{j=0}^{M-1} \left(S^{(9j+1,9j+3)} + S^{(9j+4,9j+6)}\right) \end{aligned} \tag{34}$$

where $S^{(k,k+2)}$ is defined in (10).

Let us pause for a moment and explain why we consider this operator. Using the graphical notation developed in Section IV, the groundspace of (34) can be represented as the graph drawn in black in Figure 4. For the moment, let us focus on the graph drawn in black and ignore all other aspects of the Figure. As described in the caption, a basis for the groundspace is in 1-1 correspondence with the connected components of the graph. Note that the graphs from Figures 2 and 3 each appear M times along the diagonal. This corresponds to the fact that the verification circuit contains M one-qubit gates and M two-qubit gates V.

We obtain H_X by adding terms to $\mathbb{I} \otimes H_{\text{diag}}^{(M)}$. We add terms for each one- and two-qubit gate and we add terms which check the initial and final state of the computation. Specifically, let

$$H_X = \mathbb{I} \otimes H_{\text{diag}}^{(M)} + \sum_{j=0}^{M-1} \left(H_U^j + H_V^j\right) + H_{\text{init}} + H_{\text{end}}, \tag{35}$$

which acts on the Hilbert space (33). Here

$$\begin{aligned} H_{\text{init}} &= \sum_{i=1}^{n_a} |1\rangle\langle 1|_{(i+n)} \otimes C_{\leq 1} \otimes C_{\leq 1}, \\ H_{\text{end}} &= |0\rangle\langle 0|_{(n+1)} \otimes C_{\geq (9M+3)} \otimes C_{\geq (9M+3)} \end{aligned} \tag{36}$$

ensure that each of the ancilla qubits is in the $|0\rangle$ state when the clock state is $|C_1\rangle|C_1\rangle$, and that the first qubit in the ancilla register is in the state $|1\rangle$ when the clock state is $|C_{9M+3}\rangle|C_{9M+3}\rangle$. The operators

$$H_U^j = h_{9j+3,9j+4}(U^j) \otimes \mathbb{I} + \mathbb{I} \otimes \mathbb{I} \otimes h_{9j+3,9j+4} \tag{37}$$

are defined by analogy with (15) and involve the single-qubit unitaries $\{U^j\}$. We also define

$$H_V^j = H_{\text{horizontal}}^j + H_{\text{vertical}}^j \tag{38}$$

by analogy with (21):

$$\begin{aligned} H_{\text{horizontal}}^j &= |0\rangle\langle 0|_{a_j} \otimes h_{9j+6,9j+7} \otimes \mathbb{I} \\ &+ \mathbb{I} \otimes h_{9j+6,9j+7} \otimes C_{\geq 9j+10} + \mathbb{I} \otimes h_{9j+8,9j+9} \otimes C_{\leq 9j+6} \\ &+ |0\rangle\langle 0|_{a_j} \otimes h_{9j+9,9j+10} \otimes \mathbb{I} + \mathbb{I} \otimes h_{9j+9,9j+10} \otimes C_{\geq 9j+10} \\ &+ \mathbb{I} \otimes h_{9j+8,9j+9} \otimes C_{\geq 9j+10} + h_{9j+7,9j+8}(B_{b_j}) \otimes \mathbb{I} \end{aligned} \tag{39}$$

$$\begin{aligned} H_{\text{vertical}}^j &= |1\rangle\langle 1|_{a_j} \otimes \mathbb{I} \otimes h_{9j+6,9j+7} \\ &+ \mathbb{I} \otimes C_{\geq 9j+10} \otimes h_{9j+6,9j+7} + \mathbb{I} \otimes C_{\leq 9j+6} \otimes h_{9j+8,9j+9} \\ &+ |1\rangle\langle 1|_{a_j} \otimes \mathbb{I} \otimes h_{9j+9,9j+10} + \mathbb{I} \otimes C_{\geq 9j+10} \otimes h_{9j+9,9j+10} \\ &+ \mathbb{I} \otimes C_{\geq 9j+10} \otimes h_{9j+8,9j+9} + h_{9j+7,9j+8}(\sigma_{b_j}^z). \end{aligned} \tag{40}$$

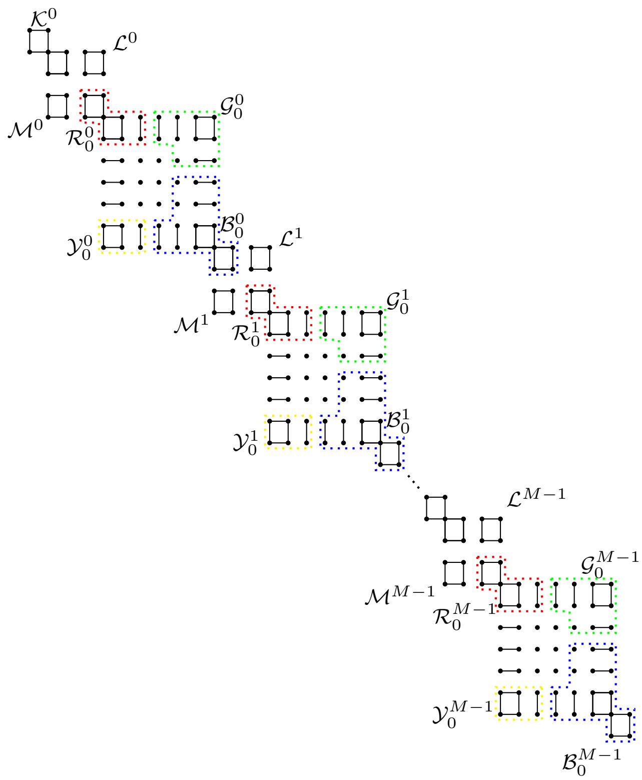


Figure 4. A basis for the groundspace of $H_{\text{diag}}^{(M)}$ is in 1-1 correspondence with the connected components of the graph drawn in black. The vertices are labeled (i, j) with the top left vertex labeled $(1, 1)$ and the bottom right vertex $(9M + 3, 9M + 3)$. The ground state associated with a connected component $\mathcal{J}$ is the uniform superposition $\sum_{(i,j)\in\mathcal{J}} |C_i\rangle|C_j\rangle$.

Note that H_X is a sum of 3-local projectors. We show in [9] that each projector in the sum is of the form given in Definition 3.

We now characterize the groundspace of H_X.

B. The zero energy groundspace of H_X (Proof of Theorem 1)

We now show that a zero-energy ground state of H_X exists if and only if there exists a witness $|W\rangle$ which the original verifier U_X accepts with certainty. We begin by defining some sets of vertices in the graph from Figure 4. For each copy $j = 0, \ldots, M-1$ of the graph in Figure 3 that appears in Figure 4, we define sets $\mathcal{R}_0^j, \mathcal{G}_0^j, \mathcal{Y}_0^j, \mathcal{B}_0^j, R_1^j, \mathcal{G}_1^j, \mathcal{Y}_1^j, \mathcal{B}_1^j$. Likewise, for each copy $j = 0, \ldots, M-1$ of the graph in Figure 2 that appears in Figure 4 we define sets $\mathcal{L}^j, \mathcal{M}^j$in Figure 4, and for the copy with $j = 0$ (in the top left) we also define $\mathcal{K}^0$ as shown in the Figure. For each of these sets, we define an associated (unnormalized) state through (16).

To analyze the groundspace of H_X, we add the terms in equation (35) one at a time, computing the zero energy states of the resulting operator at each step.

We start with $\mathbb{I} \otimes H_{\text{diag}}^{(M)}$, which (as discussed in the previous Section) has nullspace spanned by states of the form

$$|z\rangle|\mathcal{J}\rangle = |z\rangle \sum_{(i,j)\in\mathcal{J}} |C_i\rangle|C_j\rangle, \tag{41}$$

where $\mathcal{J} \subset [9M+3]\otimes[9M+3]$ is a connected component of the graph drawn in black in Figure 4 and z is an $(n + n_a)$-bit string.

Now consider

$$\mathbb{I} \otimes H_{\text{diag}}^{(M)} + \sum_{j=0}^{M-1} H_V^j. \tag{42}$$

As the reader might expect, we are going to use Lemma 1 to solve for the zero energy states. We begin by considering the action of H_V^j in the basis (41).

Look at the graph in black in Figure 3 and note that there are M copies of this graph along the diagonal in Figure 4. Each copy $j = 0, \ldots, M-1$ contains 25 connected components $\mathcal{J}$. The operator H_V^j only has support on states $|z\rangle|\mathcal{J}\rangle$ when $\mathcal{J}$ is one of the 25 connected components in the jth copy. This implies that the matrix element

$$\sum_{j=0}^{M-1} \langle\mathcal{J}_2|\langle z_2|H_V^j|z_1\rangle|\mathcal{J}_1\rangle \tag{43}$$

is nonzero only when $\mathcal{J}_1$ and $\mathcal{J}_2$ are both contained in the same copy j. The matrix with entries (43) is therefore block diagonal with a nonzero block for each $j = 0, \ldots, M-1$. In addition to these blocks, there are "blocks" of size 1 – the states

$$|z\rangle|\mathcal{K}^0\rangle, \qquad |z\rangle|\mathcal{M}^j\rangle, \qquad |z\rangle|\mathcal{L}^j\rangle \tag{44}$$

for $j = 0, \ldots, M-1$ and $z \in \{0,1\}^{n+n_a}$ which have zero energy for (42). Let us now solve for the zero eigenvectors of (42) within each nonzero block. The block corresponding to a given value j is a $(2^{n+n_a} \cdot 25) \times (2^{n+n_a} \cdot 25)$ matrix with entries

$$\langle\mathcal{J}_2|\langle z_2|H_V^j|z_1\rangle|\mathcal{J}_1\rangle,$$

where $\mathcal{J}_1$ and $\mathcal{J}_2$ are from the corresponding set of 25 connected components. Recall that H_V^j acts nontrivially on qubits a_j and b_j and as the identity on the remaining 2^{n+n_a-2} qubits of the first register. Using this fact we see that the above matrix (the block labeled by j) further decomposes into 2^{n+n_a-2} identical blocks each of which has size $4 \cdot 25 \times 4 \cdot 25$. Each of these 100×100 blocks is a matrix that we have already encountered in Section IV, the matrix with entries given by (27). Lemma 1 characterizes the zero energy eigenvectors of this matrix. Applying Lemma 1, we get zero eigenvectors of (42)

$$\sum_{x,y\in\{0,1\}}\Bigg[\left(|xy\rangle\langle xy|_{a_jb_j}\right)|z\rangle|\mathcal{R}_x^j\rangle+\left(Q|xy\rangle\langle xy|_{a_jb_j}\right)|z\rangle|\mathcal{G}_x^j\rangle$$
$$+\left(\tilde{Q}|xy\rangle\langle xy|_{a_jb_j}\right)|z\rangle|\mathcal{Y}_x^j\rangle+\left(V|xy\rangle\langle xy|_{a_jb_j}\right)|z\rangle|\mathcal{B}_x^j\rangle\Bigg]. \tag{45}$$

Here the projector $|xy\rangle\langle xy|_{a_jb_j}$ acts nontrivially only on qubits a_j and b_j of the computational register and z is an $(n+n_a)$-bit string. Note that since $|z\rangle$ is a computational basis state, only one of the terms in the sum over x,y is nonzero; we have written the state in this way to ease understanding later on. Letting z range over all $(n+n_a)$-bit strings and $j=0,\ldots,M-1$, the states (44) and (45) span the groundspace of (42).

Now consider

$$\mathbb{I}\otimes H_{\text{diag}}^{(M)}+\sum_{j=0}^{M-1}H_V^j+\sum_{j=0}^{M-1}H_U^j. \tag{46}$$

The third term in (46) couples the ground states of (42). To solve for the zero energy states of (46), we compute the action of

$$\sum_{j=0}^{M-1}H_U^j \tag{47}$$

within the groundspace of the first two terms. We now exhibit a basis for the ground space of (42) in which the operator (47) has a simple form. Define unitaries $O^0=\mathbb{I}$ and

$$O^k=\ V_{a_{k-1}b_{k-1}}U^{k-1}V_{a_{k-2}b_{k-2}}U^{j-2}\ldots U^0$$

for $k=1,\ldots,M-1$ and states

$$|\mathcal{K}^0(\phi)\rangle=|\phi\rangle|\mathcal{K}^0\rangle \tag{48}$$
$$|\mathcal{M}^j(\phi)\rangle=O^j|\phi\rangle|\mathcal{M}^j\rangle\qquad|\mathcal{L}^j(\phi)\rangle=U^jO^j|\phi\rangle|\mathcal{L}^j\rangle, \tag{49}$$

and

$$|\psi_V^j(\phi)\rangle=\sum_{x,y\in\{0,1\}}\Bigg[\left(|xy\rangle\langle xy|_{a_jb_j}\right)U^jO^j|\phi\rangle|\mathcal{R}_x^j\rangle$$
$$+\left(Q|xy\rangle\langle xy|_{a_jb_j}\right)U^jO^j|\phi\rangle|\mathcal{G}_x^j\rangle$$
$$+\left(\tilde{Q}|xy\rangle\langle xy|_{a_jb_j}\right)U^jO^j|\phi\rangle|\mathcal{Y}_x^j\rangle$$
$$+\left(V|xy\rangle\langle xy|_{a_jb_j}\right)U^jO^j|\phi\rangle|\mathcal{B}_x^j\rangle\Bigg]. \tag{50}$$

Here we let $|\phi\rangle$ range over some (arbitrary) complete orthonormal basis Λ for the $(n+n_a)$ qubit register and $j=0,\ldots,M-1$. The states (48)-(50) (with $j=0,\ldots,M-1$ and $|\phi\rangle\in\Lambda$) are linearly independent superpositions of (44) and (45) and therefore span the groundspace of (42). Their normalizations are:

$$\begin{aligned}\langle\mathcal{K}^0(\phi)|\mathcal{K}^0(\phi)\rangle&=7,\\ \langle\mathcal{M}^j(\phi)|\mathcal{M}^j(\phi)\rangle=\langle\mathcal{L}^j(\phi)|\mathcal{L}^j(\phi)\rangle&=4,\\ \langle\psi_V^j(\phi)|\psi_V^j(\phi)\rangle&=43.\end{aligned} \tag{51}$$

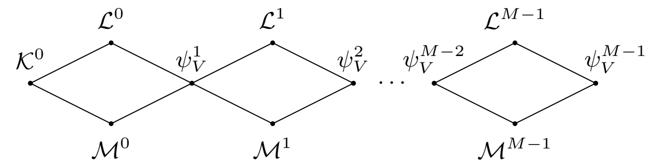


Figure 5. The Hamiltonian (47) is block diagonal when written in the basis (49)-(50). Each of the 2^{n+n_a} blocks corresponds to a different $(n+n_a)$-qubit state $|\phi\rangle$ from an orthonormal basis Λ. The matrix for each block is the same, equal to $\frac{1}{4}L$ where L is the Laplacian of this graph, which has $3M+1$ vertices.

The operator (47) acts on this basis in a simple way. It only connects states with the same $|\phi\rangle\in\Lambda$ and is therefore block diagonal (with 2^{n+n_a} blocks).

We compute the matrix elements within a block using equations (37) and (5). For example,

$$\begin{aligned}\sum_{j=0}^{M-1}\langle\mathcal{K}^0(\phi)|H_U^j|\mathcal{M}^0(\phi)\rangle&=\langle\mathcal{K}^0(\phi)|\left(\mathbb{I}\otimes\mathbb{I}\otimes h_{3,4}\right)|\mathcal{M}^0(\phi)\rangle\\&=-\frac{1}{4}.\end{aligned}$$

Continuing in this manner, we compute all matrix elements of (47) between states (49)-(50). The resulting matrix is the same for each $|\phi\rangle$ and is equal to $\frac{1}{4}L$ where L is the Laplacian matrix of the graph in Figure 5. The Laplacian matrix of a connected graph has a unique eigenvector with eigenvalue zero: the all ones vector. This fact means that for each $|\phi\rangle\in\Lambda$ there is a unique zero energy state of (46) given by the uniform superposition

$$|\text{Hist}(\phi)\rangle=$$
$$\frac{1}{F_M}\left(|\mathcal{K}^0(\phi)\rangle+\sum_{j=0}^{M-1}\left(|\mathcal{L}^j(\phi)\rangle+|\mathcal{M}^j(\phi)\rangle+|\psi_V^j(\phi)\rangle\right)\right), \tag{52}$$

where we use (51) to compute the normalizing factor $F_M=\sqrt{51M+7}$. Letting $|\phi\rangle$ range over all states in the basis Λ we get a spanning basis for the groundspace of (46). Moreover, *every* state in the groundspace of (46) is of the form $|\text{Hist}(\psi)\rangle$ for some $(n+n_a)$-qubit state $|\psi\rangle$, by linearity of $|\text{Hist}(\psi)\rangle$.

Now consider the conditions under which a state $|\text{Hist}(\psi)\rangle$ in the groundspace of (46) also has zero energy for both H_{init} and H_{end}, the final two terms in (35).

We have

$$\langle \text{Hist}(\psi)|H_{\text{init}}|\text{Hist}(\psi)\rangle$$
$$= \frac{1}{(F_M)^2}\langle \mathcal{K}^0(\psi)|\sum_{i=1}^{n_a}|1\rangle\langle 1|_{n+i}\otimes C_{\leq 1}\otimes C_{\leq 1}|\mathcal{K}^0(\psi)\rangle$$
$$= \frac{1}{(F_M)^2}\langle \psi|\langle C_1|\langle C_1|\sum_{i=1}^{n_a}|1\rangle\langle 1|_{n+i}\otimes C_{\leq 1}\otimes C_{\leq 1}|\psi\rangle|C_1\rangle|C_1\rangle$$
$$= \frac{1}{4\,(F_M)^2}\langle \psi|\sum_{i=1}^{n_a}|1\rangle\langle 1|_{n+i}|\psi\rangle,$$

where in the last line we used (8). This is equal to zero if and only if $|\psi\rangle = |W\rangle|0\rangle^{\otimes n_a}$ for some n-qubit state $|W\rangle$. Similarly,

$$\langle \text{Hist}(\psi)|H_{\text{end}}|\text{Hist}(\psi)\rangle = \frac{1}{4\,(F_M)^2}\langle \psi|U_X^\dagger\left(|0\rangle\langle 0|_{n+1}\right)U_X|\psi\rangle,$$

which is zero if and only if the $(n+1)$th qubit of $U_X|\psi\rangle$ is in the state $|1\rangle$ with certainty. We have therefore proven that H_X has a zero energy eigenstate if and only if there exists an $n-$qubit state $|W\rangle$ satisfying

$$\left\|\left(\mathbb{I}^{\otimes n}\otimes|0\rangle\langle 0|_{(n+1)}\otimes\mathbb{I}^{\otimes(n_a-1)}\right)U_X|W\rangle|0\rangle^{\otimes n_a}\right\|^2 = 0. \tag{53}$$

This establishes Theorem 1.

VI. Acknowledgment

We thank Sergey Bravyi, Daniel Gottesman, Rajat Mittal, and John Watrous for helpful discussions. DG was supported in part by NSERC. DN gratefully acknowledges support by the EU project QUERG.

References

[1] S. Aaronson. On perfect completeness for qma. *Quantum Info. Comput.*, 9(1):81–89, January 2009.

[2] A. Ambainis, J. Kempe, and O. Sattath. A quantum lovász local lemma. In *Proceedings of the 42nd ACM symposium on Theory of computing*, pages 151–160. ACM, 2010.

[3] S. Bravyi. Personal communication.

[4] S. Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. *eprint arXiv:quant-ph/0602108*, February 2006. Published in *Contemporary Mathematics* Volume 536, 2011.

[5] S. Bravyi, L. Caha, R. Movassagh, D. Nagaj, and P. W. Shor. Criticality without frustration for quantum spin-1 chains. *Phys. Rev. Lett.*, 109:207202, Nov 2012.

[6] S. Bravyi, C. Moore, and A. Russell. Bounds on the quantum satisfiability threshold. In *ICS*, pages 482–489, 2010.

[7] M. Coudron and R. Movassagh. Unfrustration Condition and Degeneracy of Qudits on Trees. *e-print arXiv:1209.4395*, September 2012.

[8] L. Eldar and O. Regev. Quantum sat for a qutrit-cinquit pair is qma1-complete. In *ICALP (1)*, pages 881–892, 2008.

[9] D. Gosset and D. Nagaj. Quantum 3-SAT is QMA_1-complete. *eprint arXiv:1302.0290*, February 2013.

[10] Z. Ji, Z. Wei, and B. Zeng. Complete characterization of the ground-space structure of two-body frustration-free hamiltonians for qubits. *Phys. Rev. A*, 84:042338, Oct 2011.

[11] S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. Achieving perfect completeness in classical-witness quantum merlin-arthur proof systems. *Quantum Info. Comput.*, 12(5-6):461–471, May 2012.

[12] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, May 2006.

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

[14] H. Kobayashi, F. Le Gall, and H. Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. *4th ACM Innovations in Theoretical Computer Science conference (ITCS 2013)*, 2013.

[15] C. R. Laumann, A. M. Läuchli, R. Moessner, A. Scardicchio, and S. L. Sondhi. Product, generic, and random generic quantum satisfiability. *Phys. Rev. A*, 81:062345, Jun 2010.

[16] C.R. Laumann, R. Moessner, A. Scarddichio, and S. L. Sondhi. Random quantum satisfiability. *Quantum Information & Computation*, 10(1&2):1–15, 2010.

[17] C. Marriott and J. Watrous. Quantum arthur—merlin games. *Comput. Complex.*, 14(2):122–152, June 2005.

[18] R. Movassagh, E. Farhi, J. Goldstone, D. Nagaj, T. J. Osborne, and P. W. Shor. Unfrustrated qudit chains and their ground states. *Phys. Rev. A*, 82(1):012318, July 2010.

[19] D. Nagaj. Fast universal quantum computation with railroad-switch local Hamiltonians. *Journal of Mathematical Physics*, 51(6):062201, June 2010.

[20] D. Nagaj and S. Mozes. New construction for a QMA complete three-local Hamiltonian. *Journal of Mathematical Physics*, 48(7):072104, July 2007.

[21] D. Nagaj, P. Wocjan, and Y. Zhang. Fast amplification of qma. *Quantum Information & Computation*, pages 1053–1068, 2011.

[22] T. J. Osborne. Hamiltonian complexity. *Reports on Progress in Physics*, 75(2):022001, February 2012.