# An Efficient Reduction from QMATIME[$n$] to the $k$-Local Hamiltonians Problem

Abhijit S. Mudigonda

January 28, 2021

In this note, we present an efficient reduction from QMATIME[$n$] in the uniform quantum circuit model to the 2-local Hamiltonian problem. The result can be deduced without much difficulty from the proof of QMA-completeness of the 2-local Hamiltonian due to Kempe, Kitaev, and Regev [KKR06] along with an algorithmic version of the Solovay-Kitaev theorem due to van Melkebeek and Watson [vMW12]. As we were unable to find this result in the literature, we present a short proof here. This is motivated by the prospect of extending the lower bound of [MW20] on QCMATIME[$n$] against deterministic small space computation to a lower bound on the $k$-local Hamiltonians problem.

## 1 Preliminaries

### 1.1 Notation

$U(d)$ is the set of $2^d \times 2^d$ unitary matrices. Given a quantum state over $n$ qubits and an operator $A \in U(2^m)$ for $m \leq n$, we write $A_{(i_1,i_2,\ldots,i_m)}$ with $i_1, i_2, \ldots i_m$ distinct to denote the operator in $U(2^n)$ which is applies $A$ to the specified qubits and acts trivially on all other qubits. We will sometimes use superscripts to denote indices rather than powers.

### 1.2 The Computational Model

We use the usual definition of a quantum circuit. The **acceptance probability** of a quantum circuit $\mathcal{Q}$ on a state $|\psi\rangle$ is the probability that measurement of the first qubit of $\mathcal{Q}|\psi\rangle$ is 1. Let $\mathcal{U}$ be a universal set of unitary operators. A **quantum circuit family** is a set $\{\mathcal{Q}_n : n \in \mathbb{N}\}$, where each $\mathcal{Q}_n$ is a quantum circuit with $n$ input bits and some number of ancilla qubits. Note that each $U \in \mathcal{U}$ acts on $O(1)$ qubits (i.e. some fixed constant independent of $n$) because $\mathcal{U}$ is a finite set. The **size** of a quantum circuit family is a function $t : \mathbb{N} \to \mathbb{N}$ where $t(n)$ is the number of tuples in $\mathcal{Q}_n$. Consider $s, u : \mathbb{N} \to \mathbb{N}$. A quantum circuit family is **$(s, u)$-uniform** if there exists a deterministic algorithm that, given as inputs $1^n$ and $i, j, k \in \mathbb{N}$, can print the entry at position $(i, j)$ of the $k^{\text{th}}$ unitary of $\mathcal{Q}_n$ and the list of qubits that this unitary acts on in $u(n)$ time and $s(n)$ space simultaneously.

### 1.3 Universal Sets and the Solovay-Kitaev Theorem

A priori, it may seem that the size of a uniform quantum circuit family which solves a given problem could depend on the universal set $\mathcal{U}$ that is used. However, this turns out not to be the case. This is a consequence of a constructive and space-efficient form of the Solovay-Kitaev theorem due to van Melkebeek and Watson [vMW12].

**Theorem 1.1** (Theorem 4.3 of [vMW12]). *For each constant integer $d \geq 2$ the following holds. Suppose $\mathcal{U} \subseteq U(d)$ is a finite set closed under adjoint such that for every $U \in U(d)$ and every $\epsilon > 0$ there exists a sequence $U_1, \ldots, U_k \in \mathcal{U}$ and a global phase factor $e^{i\theta}$ such that $||U - e^{i\theta} U_k \ldots U_1|| < \epsilon$. Then for every $U \in U(d)$ and every $\epsilon > 0$ there exists a sequence $U'_1, \ldots, U'_{k'} \in \mathcal{U}$ with $k \leq \log^{O(1)}(\frac{1}{\epsilon})$ and a global phase factor $e^{i\theta'}$ such that $||U - e^{i\theta'} U'_{k'} \ldots U'_1|| < \epsilon$. Moreover, such a sequence can be computed by a deterministic algorithm running in $\log^{O(1)}(\frac{1}{\epsilon})$ time and $O(\log \frac{1}{\epsilon})$ space, given as input $\epsilon$ and matrices that are at distance at most $f(\epsilon)$ from $U$ and the gates in $\mathcal{U}$, where $f$ is a certain polynomial depending only on $d$.*

This is a space-efficient form of the classic Solovay-Kitaev theorem, where the deterministic algorithm has the same runtime but uses $\log^{O(1)}(\frac{1}{\epsilon})$ space rather than $O(\log \frac{1}{\epsilon})$ space.

**Corollary 1.2.** *Let $\mathcal{U}$ and $\mathcal{U}'$ be universal sets of unitaries closed under adjoint, and assume If an $(s, u)$-uniform quantum circuit family $\{\mathcal{Q}_n\}_{n \in \mathbb{N}}$ over $\mathcal{U}$ has size $t(n)$ then there is an $(s', u')$-uniform quantum circuit family $\{\mathcal{Q}'\}_{n \in \mathbb{N}}$ of size $t(n) \log^{O(1)} t(n)$ over a universal set $\mathcal{U}'$. such that the acceptance probability of $\mathcal{Q}'$ on any input $|\psi\rangle$ differs from that of $\mathcal{A}'$ by at most an additive constant.*

This corollary is essentially the same as Theorem 1.2 of [vMW12], but we include a proof because our model for quantum computation is somewhat different from theirs.

*Proof.* Suppose that $\{\mathcal{Q}_n\}$ is a size $t(n)$ quantum circuit family over a universal set $\mathcal{U}$. We'll start by describing the structure of a quantum circuit family $\{\mathcal{Q}'_n\}$ over a finite universal set $\mathcal{U}'$ that is closed under adjoint and subsequently show that we can build the latter from the former while satisfying the uniformity conditions.

By Theorem 1.1, for each $n \in \mathbb{N}$, for any $\epsilon$, each $U \in \mathcal{Q}_n$ can be replaced by a sequence of $\log^{O(1)}(\frac{1}{\epsilon})$ gates from $\mathcal{U}'$ such that the error accrued through replacing $U$ alone is less than $\epsilon$. We will take $\epsilon = O(\frac{1}{t(n)})$ because that way, by the triangle inequality, replacing all $t(n)$ unitaries in $\mathcal{Q}_n$ will not change the acceptance probability by more than an additive constant. Note that the global phase factor is irrelevant because it disappears under measurement.

Theorem 1.1 also tells us that there is a deterministic algorithm that can produce the appropriate sequence of unitaries given a sufficiently accurate description of $U$ and the unitaries in $S'$. The accuracy that we need depends only on the dimension of $U$. Because $U \in S$ and $S \cup S'$ is a finite set, we can hardcode these descriptions in the algorithm as $d$ is a constant. Furthermore, the cost is $\log^{O(1)} n$ time and $O(\log n)$ space per unitary in $\mathcal{Q}_n$, so the runtime stays the same up to polylogarithmic factors. If the initial algorithm was bitwise log-uniform then this one will be as well because given an index $k$, we can compute the $k^{\text{th}}$ unitary from $\mathcal{Q}'_n$ efficiently by figuring out which unitary in $\mathcal{Q}_n$ this corresponds to and running the algorithm that prints the approximation in $\log^{O(1)} n$ time. Note that we can make finding the unitary in $\mathcal{Q}_n$ corresponding to an index $k'$ from $\mathcal{Q}'_n$ easy by approximating each $U \in \mathcal{Q}_n$ with the same number of unitaries from $S'$. □

We will use the universal set of unitary matrices given by the following lemma.

**Lemma 1.3** ([Aar16]). *$\{CNOT, G\}$ is a universal set, where*

$$G := \begin{bmatrix} \frac{3}{5} & \frac{4i}{5} \\ \frac{4}{5} & \frac{-3i}{5} \end{bmatrix}. \tag{1}$$

## 1.4 Quantum Merlin-Arthur

**Definition 1.4.** $\mathsf{QMATIME}[n]_u$ is the class of languages decided by quantum Merlin-Arthur protocols where the verifier is given by an $(s, u)$-uniform quantum circuit family of size $O(n)$.

### 1.5 The $k$-Local Hamiltonians Problem

The $k$-local Hamiltonians problem is a well-known QMA-complete problem, and can be thought of as a quantum analogue of the NP-complete MAX-SAT problem.

**Definition 1.5.** A operator $H$ acting on $n$ qubits is a $k$-local Hamiltonian if it can be written as $\sum_{i=1}^{r} H_i$ where each $H_i$ is Hermitian, acts only on $k$ qubits, and $r = n^{O(1)}$.

**Definition 1.6.** An instance of the $k$-local Hamiltonians (promise) problem consists of two constants $a, b$, with $a < b$, and a representation of a $k$-local Hamiltonian $H$. Without loss of generality, we will expect the representation to consist of tuples of form $(H_i, S)$, where each $H_i$ is a $2^k \times 2^k$ matrix over the complex numbers and $S$ specifies the qubits on which $H_i$ acts. We define the **size** of a $k$-local Hamiltonians instance to be the number of bits required to write down the instance, taking into account bit complexity of $a$, $b$, and the entries of each $H_i$.

Building on ideas of Feynman, Kitaev showed that the 5-local Hamiltonian problem is QMA-complete [KSV02]. The value of $k$ was reduced further, first in [KR03] to 3 and finally in [KKR06] to 2. The 1-local Hamiltonian problem is in P, so this is as far as we can go.

**Lemma 1.7** ([KSV02])**.** *For $k = O(1)$, the $k$-local Hamiltonians problem on $n$ qubits is contained in $\mathsf{QMATIME}_{s,u}[n]$ for some $s(n) = O(\log n)$, $u(n) = \log^{O(1)} n$.*

*Sketch.* Our algorithm will be the same as that in [KSV02] with an amplification step at the end. We refer the reader to [KSV02] for a proof of correctness, and here will just check that it has the requisite time and space complexity. Given the description of $H_i$, we first perform singular-value decomposition to write it as $\sum_{j=0}^{k} \lambda_j^i |\psi_j^i\rangle \langle\psi_j^i|$, where the eigenvalues and eigenvectors are computed to whatever accuracy is needed. A priori, it could be the case that some entries of the matrix are represented with $O(n)$ bits. However, all we will need is an approximation of $H_i$ up to an $O(\frac{1}{k})$ error, which is $O(1)$ since $k = O(1)$. Therefore, if we take the input to be in (say) binary scientific notation, we see that we can consider just a constant number of bits per entry of $H_i$. Thus, we can write down the operator $W_i$, where

$$W_i := \sum_j |j\rangle \langle j| \otimes \left( \sqrt{\lambda_j^i} |0\rangle \langle 0| + \sqrt{1-\lambda_j^i} |1\rangle \langle 0| - \sqrt{1-\lambda_j^i} |0\rangle \langle 1| + \sqrt{\lambda_j^i} |1\rangle \langle 1| \right). \tag{2}$$

$W_i$ is some matrix in $U(k)$. Applying the deterministic algorithm from Theorem 1.1 with sufficiently small constant error, we can implement $W$ in $O(1)$ time and $O(\log n)$ space.

As in [KSV02], our algorithm – given the $n$ qubit state $|\eta\rangle$ from Merlin – consists of picking a random $i$, computing $W_i |\eta\rangle$, measuring the first qubit, and accepting if it is $|1\rangle$. The runtime so far is $O(\log n)$ because drawing a random $j \in [r]$ requires $\lceil \log r \rceil = O(\log n)$ measurements. Our current soundness gap is $\frac{1}{r}$. We may apply Marriot-Watrous in-place amplification to increase the soundness gap to $\Omega(1)$. The length of the requisite proof string remains $O(n)$, the space complexity remains the same (the additional steps in Marriot-Watrous amplification are simple to describe), and the runtime increases to $O(n \log n)$. □

## 2 A Tight Reduction from a subset of QMATIME$[n]$ to 2-local Hamiltonians

We will exhibit an efficient reduction from $\mathsf{QMATIME}[n]_{s,t}$ in the uniform quantum circuit model to the 2-local Hamiltonians problem. The reduction, applied to an $n$-bit input, will yield an instance

of 2-local Hamiltonians of length at most $n \log^{O(1)} n$. Furthermore, a given bit of the reduction can be computed in $s(n) + O(\log n)$ space and $t(n) + \log^{O(1)} n$ time. Our result follows as a corollary of the aforementioned proof of QMA-completeness of the 2-local Hamiltonian problem.

**Theorem 2.1** ([KKR06])**.** *Suppose a size $t$ quantum circuit $\mathcal{Q}$ with $n$ inputs has the following properties.*

1. *Given a tuple $(i, j, k, l)$, the $l^{th}$ bit of the $(j, k)^{th}$ entry of the $i^{th}$ unitary can be computed in $u(n)$ time and $s(n)$ space simultaneously.*
2. *The circuit consists only of single-qubit gates and the controlled phase gate $C_\phi$.*
3. *Each $C_\phi$ gate is preceded and followed by two $Z$ gates, one on each qubit.*
4. *The $C_\phi$ gates occur at regular intervals, with the same number of single-qubit gates in between any two consecutive $C_\phi$ gates.*

*Then, there exists a 2-local Hamiltonian $H$ with $O(n + t)$ 2-local terms such that*

- *If $\mathcal{Q}$ accepts with probability more than $1 - \epsilon$ on some input then $H$ has an eigenvalue smaller than $\epsilon$.*
- *If $\mathcal{Q}$ accepts with probability less than $\epsilon$ for all inputs then all eigenvalues of $H$ are larger than $\frac{1}{2} - \epsilon$.*

*Furthermore, any local term can be computed in $u(n)$ time and $s(n)$ space simultaneously.*

Theorem 2.1 is implicit in [KKR06], although the authors do not expressly discuss time and space uniformity. Observe that Theorem 2.1 gives a reduction from any quantum Merlin-Arthur protocol whose verifier is in the specified form to 2-local Hamiltonians. We shall show the following:

**Corollary 2.2.** *2-local Hamiltonians is hard, under (deterministic) reductions in $s(n) + O(\log n)$ space and $n(u(n) + \log^{O(1)} n)$ time simultaneously, for $\mathsf{QMATIME}_{s,u}[n]$. Furthermore, each bit of the reduction can be computed in $u(n) + \log^{O(1)} n$ time and $s(n)$ space simultaneously.*

It suffices to show that an arbitrary linear-time quantum verifier can be converted into one satisfying the conditions of Theorem 2.1.

*Proof of Corollary 2.2.* Take $\mathcal{Q}_0$ in Theorem 2.1 to be the verifier of the QMA protocol with the input fixed, and suppose it is given over some universal set $\mathcal{U}$. We may apply Corollary 1.2 to obtain an equivalent circuit over the set $\mathcal{U}' := \{C_\phi, H, G, G^{\dagger,Z}$ — $\mathcal{U}'$ is universal and closed under adjoint by Lemma 1.3 because applying a Hadamard gate before and after the target qubit of $\mathbb{C}_\phi$ yields a CNOT gate. $\mathcal{U}'$ satisfies the condition 2 by definition. It also satisfies condition 1 because all the entries of the single qubit operators in $\mathcal{U}'$ have finite decimal representations[1]. It remains to show that we can uniformly convert this circuit to a form satisfying conditions 3 and 4.

We first add two ancilla qubits to $\mathcal{Q}$, which we label with indices $-1, -2$. Let $C'_{\phi,(i,j)}$ denote the sequence of operators $Z_{(i)}Z_{(j)}C_{\phi,(i,j)}, Z_{(i)}, Z_{(j)}$, and let $C'_{\phi,-} := C'_{\phi,(-1,-2)}$. Observe that $C'_{\phi,(i,j)}$ is equivalent to $C_{\phi,(i,j)}$ because $Z_iZ_j$ and $C_{\phi,(i,j)}$ commute (they are both diagonal matrices). We replace each $C_{\phi,(i,j)}$ in $\mathcal{Q}$ by the sequence $C'_{\phi,-}, I, C'_{\phi,(i,j)}, I$. Each single qubit unitary $A_{(i)}$ in $\mathcal{Q}$ is replaced by the sequence $C'_{\phi,-}, A_i, C'_{\phi,-}, I$. Lastly, we append a single $C'_{\phi,-}$ to the circuit to make

[1]This doesn't really matter as long as we can get arbitrarily good approximation to the entries of single qubit entries in our chosen universal set time and space efficiently.

the total number of applications of $C'_\phi$ even (if it would otherwise be odd). The point of this is that now the $C'_\phi$ occur at regular intervals but the $C'_{\phi,\_}$ do not change the result of the computation as in the end they all cancel out. Each unitary in the initial circuit is replaced with twelve gates in the new circuit. We can now apply Theorem 2.1 to finish. □

It's worth noting that Corollary 2.2 does not immediately imply that the lower bound of [MW20] extends to a lower bound on $k$-local Hamiltonians because that lower bound is against $\mathsf{QCMATIME}[n]$ on quantum random-access machines. The missing piece is a tight (up to polylogarithmic factors) relationship between $\mathsf{QCMATIME}[n]$ on quantum random-access machines and $\mathsf{QCMATIME}[n]$ in the uniform circuit model, analogous to the corresponding result for nondeterministic linear time due to Gurevich and Shelah [GS89].

## References


[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes. 2016.

[GS89] Yuri Gurevich and Saharon Shelah. Nearly linear time. In *Logic at Botik '89 (Pereslavl -Zalesskiy, 1989)*, volume 363 of *Lecture Notes in Comput. Sci.*, pages 108–118. Springer, Berlin, 1989.

[KKR06] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local Hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, 2006.

[KR03] Julia Kempe and Oded Regev. 3-local Hamiltonian is QMA-complete. *Quantum Inf. Comput.*, 3(3):258–264, 2003.

[KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002. Translated from the 1999 Russian original by Lester J. Senechal.

[MW20] Abhijit Mudigonda and R. Ryan Williams. Time-space lower bounds for simulating proof systems with quantum and randomized verifiers. *CoRR*, abs/2012.00330, 2020.

[vMW12] Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory Comput.*, 8:1–51, 2012.