StoqMA vs. MA: the power of error reduction

Dorit Aharonov[1,2], Alex B. Grilo[3], and Yupan Liu[4]

[1]School of Computer Science and Engineering, The Hebrew University of Jerusalem
[2]Qedma Quantum Computing Ltd.
[3]Sorbonne Université, CNRS, LIP6
[4]Graduate School of Mathematics, Nagoya University

StoqMA characterizes the computational hardness of stoquastic local Hamiltonians, which is a family of Hamiltonians that does not suffer from the sign problem. Although error reduction is commonplace for many complexity classes, such as BPP, BQP, MA, QMA, etc., this property remains open for StoqMA since Bravyi, Bessen and Terhal defined this class in 2006. In this note, we show that error reduction for StoqMA will imply that StoqMA = MA.

1 Introduction

The local Hamiltonian problem is a cornerstone of quantum complexity theory. The input to the problem consists of a k -local Hamiltonian $H = \frac{1}{m}\sum_{i\in[m]} H_i$, where each term H_i acts non-trivially on k-qubits out of an n qubit system[1], as well as two numbers, α and β. We are asked then to decide if the ground-energy of H is below α or above β, when we are promised that one of the cases hold. This problem is a computational version of the fundamental problem in condensed matter physics, of understanding the ground-energy of many body quantum systems. Kitaev [1] showed that for some α and β such that $\beta - \alpha \geq 1/\mathrm{poly}(n)$, the k-local Hamiltonian problem is complete for QMA, the quantum analog of NP. Many researchers have studied the complexity of the local Hamiltonian problem for restricted families of local Hamiltonians, closer to physical models, e.g., [2–7].

In this work we are interested in a particular subfamily of Hamiltonians called *stoquastic Hamiltonians*.[2] Roughly, stoquastic Hamiltonians are those Hamiltonians whose off-diagonal terms are non-positive. From a physics point of view, stoquastic Hamiltonians arise naturally since they do not exhibit what is known as the *sign problem*, making them more amenable to classical simulations by Monte Carlo methods. Moreover, the first adiabatic algorithms were proposed with stoquastic Hamiltonians [8], and the first models of D-Wave quantum devices were implemented in this model [9, 10].

Dorit Aharonov: doria@cs.huji.ac.il
Alex B. Grilo: Alex.Bredariol-Grilo@lip6.fr
Yupan Liu: yupan.liu@gmail.com

[1]A classical local Hamiltonian could be interpreted as an instance of the Constraint Satisfaction Problem (CSP) problem. In particular, each a local term in Hamiltonian matches a constraint, where variables in the CSP instance correspond to qubits. Moreover, Hamiltonian's ground state is associated with an assignment, and the ground-energy is precisely the maximal violation of such an assignment.

[2]We avoid giving the formal definition of these Hamiltonians here and leave it to Section 2.5.

Several works, led by Bravyi and Terhal [11–13], revealed the important role that stoquastic Hamiltonians play in quantum computational complexity. [12,13] showed that deciding whether a stoquastic Hamiltonian is *frustration-free*, namely (with some normalization) has ground-energy 0, or its ground-energy is at least $1/\text{poly}(n)$, is MA-complete. This is surprising, since it is the *first* natural MA-complete problem – and it is stated using quantum language.[3] Moreover, it was proven by [12] that if we are interested in deciding if a stoquastic Hamiltonian has ground-energy at most α or at least $\alpha+1/\text{poly}(n)$, for some more general non-zero α, then the problem becomes StoqMA-complete, where StoqMA is defined to be a (somewhat artificial) generalization of MA, which sits between MA and QMA.

The class StoqMA is our focal point in this paper; Despite its unnatural definition, which we will review in a moment, it plays a prominent role in Hamiltonian complexity. In particular, it was shown in [7, 14] that it participates in a very interesting classification theorem about quantum local Hamiltonians: for any type of local Hamiltonians,[4] the complexity class of deciding if the ground-energy of Hamiltonians of this type is at most α or at least $\alpha + 1/\text{poly}(n)$, falls in one of four categories: it is either in P, NP-complete, StoqMA-complete or QMA-complete. To put this classification in context, recall Schaefer's dichotomy theorem [15] which is the analog classification theorem for Max-k-SAT. Schaefer's dichotomy theorem states that when we consider classical Hamiltonians (i.e. the Max-k-SAT problem), the problems are either in P or NP-complete. Since Max-k-SAT is exactly a special case of local Hamiltonian problems, it would have been natural to expect that the classification in the quantum case would be to *three* classes, with the only new addition to P and NP being the class QMA. Yet, surprisingly, [7] shows that there is a fourth class which also participates in this classification, namely, StoqMA.

We now devote some time to define StoqMA informally (See Section 2.4 for a formal definition). As in standard proof systems (such as NP, QMA, etc.), in StoqMA we consider a protocol for some problem [5] involving two parties, a computationally unbounded prover and a computationally bounded (usually polynomial time) verifier. In this protocol, the prover sends a quantum state to the verifier. Then the verifier of the StoqMA protocol runs her verification algorithm that has a very particular structure: First, the verifier's computation is given by a classical reversible circuit, viewed as a quantum circuit (i.e., it is performed coherently). Secondly, its input consists of three parts: *i*) the quantum proof provided by the (unbounded) prover; *ii*) auxiliary qubits in the state $|0\rangle$; and *iii*) auxiliary qubits in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. After applying the classical reversible circuit, a certain qubit designated as the output qubit is measured in the $|+\rangle, |-\rangle$ basis, and the verifier accepts iff the output is $|+\rangle$. A problem is then said to be in the complexity class StoqMA(a, b), for some $a > b \geq 0$,[6] if for yes-instances, there is a quantum state that the prover can send that makes the verifier accept with probability at least a, whereas for no-instances, any quantum state provided by the prover makes the verifier accept with probability at most b.

As in other complexity classes with non-perfect completeness and soundness parameters, we would like to understand how does StoqMA(a, b) depend on the parameters a, b. First, it is very easy to see that StoqMA$(a, b) \subseteq$ StoqMA(a', b') if $a' \leq a$ and $b' \geq b$. For several complexity

[3] More precisely, [13] show that such a problem is MA-hard and lies in PromiseMA. For simplicity, we hereafter call such problems MA-complete.

[4] By type of local Hamiltonians, we mean that the local Hamiltonian has special properties. For example, one of the types considered in [7] consists of local Hamiltonians for which there is a tensor product of one-qubit unitaries that diagonalizes all local terms simultaneously.

[5] For us, we consider a problem as a set of two disjoint sets $\mathcal{L}_{yes}$, known as positive instances and $\mathcal{L}_{no}$, known as negative instances. The verifier is then given $x \in \mathcal{L}_{yes} \cup \mathcal{L}_{no}$, and her goal is to decide if $x \in \mathcal{L}_{yes}$ or if $x \in \mathcal{L}_{no}$.

[6] We can assume that the soundness parameter b is at least $\frac{1}{2}$, WLOG, as argued in Remark 2.4.

classes such as BPP, BQP, MA, QMA, etc., much more can be said about the dependence on parameters: the class stays the same as long as the completeness and soundness differ by at least some inverse polynomial. This is done by what is called *error reduction*, where we repeat the verification in parallel and do majority vote on the parallel output qubits. Peculiarly, it is not known how to do error reduction for StoqMA! The standard approach does not seem to work for StoqMA (at least not in a straightforward way) because the majority vote between the output of the parallel runs needs to be done in the Hadamard basis, which is not (known to be) possible using a classical circuit, as required in StoqMA.[7] Yet, we conjecture here:

Conjecture 1.1 (Error reduction for StoqMA)**.** *For any a, b such that $1/2 \leq b < a \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$,*

$$\mathsf{StoqMA}(a,b) \subseteq \mathsf{StoqMA}\left(1 - 2^{-l(n)}, \frac{1}{2} + 2^{-l(n)}\right),$$

where $l(n)$ is a polynomial of n.

If this conjecture holds, we could write StoqMA without specifying the parameters (as is done for example in BPP and BQP); essentially that would mean $\mathsf{StoqMA}(a,b)$ with any a, b such that $a - b > 1/\mathrm{poly}(n)$.

The main result in this paper is that surprisingly, if this natural property of error reduction holds for StoqMA, this would imply a very interesting conclusion: that StoqMA is equal to MA. In fact, we show this already follows from a much weaker version of error reduction. We state this implication as another conjecture:

Conjecture 1.2. *For any a, b such that $1/2 \leq b < a \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$, we have that $\mathsf{StoqMA}(a,b) = \mathsf{MA}$.*

Before stating our result connecting Conjectures 1.1 and 1.2 more formally, let us try to argue why Conjecture 1.2 is a natural conjecture, independently. To this end, let us compare StoqMA to other better understood complexity classes. First, [12] showed that $\mathsf{StoqMA}(a,b)$ is contained in AM for every $a - b \geq 1/\mathrm{poly}(n)$[8]. Notice that this puts a strong upper bound on StoqMA, when compared with the belief that BQP, the class of problems solved in quantum polynomial-time, is not included in the polynomial hierarchy [17].

From the other side, it follows that $\mathsf{StoqMA}(1, \frac{1}{2} + \mathrm{negl}(n))$ contains MA. To see this, let us use the fact we can consider MA with perfect completeness and $\mathrm{negl}(n)$ soundness error WLOG. If we consider the coherent version of MA verifier, we can modify it to perform a controlled-SWAP where the control wire is the MA output wire, and it swaps an auxiliary qubit $|0\rangle$ and an auxiliary qubit $|+\rangle$ and uses the first of these registers as the StoqMA output. For completeness, the SWAP is always performed (due to perfect completeness for MA) so we also have perfect completeness in the StoqMA verifier. For no-instances, with $1 - \mathrm{negl}(n)$ probability the MA verifier's output is 0 and therefore there is no SWAP between $|0\rangle$ and $|+\rangle$. When this happens, the acceptance probability is $\frac{1}{2}$.

Notice that the two containments above mean that under the commonly believed complexity theoretical assumption,[9] AM = NP, we have AM = StoqMA = MA = NP. Conjecture 1.2 is, of course, weaker. We notice that this conjecture would also follow from another natural property

[7] See Remark 2.5 for more details.

[8] Recall [16] that AM is a two-message randomized generalization of NP, in which the message from the verifier consists of random bits

[9] Namely, the derandomization assumption [18, 19] which states that: for some $\epsilon > 0$, some language in $\mathsf{NE} \cap \mathsf{coNE}$ requires non-deterministic circuit of size $2^{\epsilon n}$.

of complexity classes, which many classes, including MA, AM [20] and QCMA [21] possess: the property of being closed under perfect completeness (namely, that the class does not change if we require the verifier to accept yes-instances with probability 1). By the results of [12, 13], if StoqMA turns out to be closed under perfect completeness, this would imply it is equal to MA.

1.1 Results

Our main technical contribution concerns a problem that we call *projection uniform stoquastic Local Hamiltonian*. This problem is a restricted variant of the stoquastic local Hamiltonian problem proposed by [12, 13]. First, we require each local term to be a projection. Secondly, as in [22] (in the case of frustration-free Hamiltonians), we require that the terms are *uniform*; by this we mean that the groundspace of each local term is spanned by an orthonormal basis of quantum states, each being a *uniform* superposition of strings (see Definition 2.10).

Our main technical result then states that deciding whether a projection uniform stoquastic Local Hamiltonian has ground-energy at most $\mathrm{negl}(n)$ or at least $1/\mathrm{poly}(n)$ (we denote this as the $\mathsf{ProjUSLH}(\mathrm{negl}(n), 1/\mathrm{poly}(n))$ problem), is in MA.

Theorem 1.3. $\mathsf{ProjUSLH}(\mathrm{negl}(n), 1/\mathrm{poly}(n))$ *is in* MA.

We argue in Lemma 2.12 that the StoqMA-hardness proof of [12] can be easily patched to hold also with the restriction of the terms being projections and uniform; more precisely, their proof can be easily strengthened to show that $\mathsf{ProjUSLH}(\mathrm{negl}(n), 1/\mathrm{poly}(n))$ is $\mathsf{StoqMA}(1-\mathrm{negl}(n), 1-1/\mathrm{poly}(n))$-hard. Therefore, we have the following important implication of Theorem 1.3:

Corollary 1.4. $\mathsf{StoqMA}\left(1-\mathrm{negl}(n), 1-\frac{1}{\mathrm{poly}(n)}\right) \subseteq \mathsf{MA}$.

This result has a surprising consequence for the general $\mathsf{StoqMA}(a, b)$ vs. MA question: it implies that if we have error reduction for StoqMA (in other words, if Conjecture 1.1 holds), then StoqMA = MA (Figure 1b)

Corollary 1.5 (StoqMA = MA is equivalent to error reduction for StoqMA)**.** *Conjecture 1.1 is true iff Conjecture 1.2 is true.*

In fact, a weaker version of Conjecture 1.1, in which the error is reduced not exponentially but rather just to being negligibly small (namely, for any $a - b \geq 1/\mathrm{poly}(n), \mathsf{StoqMA}(a, b)) \subseteq \mathsf{StoqMA}\left(1-\mathrm{negl}(n), 1-1/\mathrm{poly}(n)\right)$), would already imply Conjecture 1.2. Interestingly, it suffices here that only the error in the completeness is reduced; this also appears in the proof of $\mathsf{MA} = \mathsf{MA}_1$ [20].

Optimistically, our result shows a possible path towards StoqMA = MA. An analogous phenomenon holds for QMA(2): [23] showed that the ability to perform error reduction for QMA(2) would imply QMA(2) = QMA(k), where k indicates k unentangled provers. In this case, it turned out to be a successful story: Harrow and Montanaro [24] indeed proved such an equivalence a few years later.

With a more negative perspective, our result indicates that (dis)proving error reduction procedures for StoqMA might be a difficult task.

1.2 Implications of our results

We discuss now the implications of our result to the relation between the complexity classes NP, MA, StoqMA, AM and QMA, and to the corresponding landscape of local Hamiltonians problems. We first recall that the known relation between these complexity classes is the following:

$$\mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{StoqMA} \subseteq \mathsf{AM} \quad \text{and} \quad \mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{StoqMA} \subseteq \mathsf{QMA} \quad \text{(Figure 1a)}.$$

However, under strong derandomization assumptions (see Footnote 9), we have that NP = AM and therefore

$$\mathsf{NP} = \mathsf{MA} = \mathsf{StoqMA} = \mathsf{AM} \subseteq \mathsf{QMA} \quad \text{(Figure 1d)}.$$

Notice that this assumption simplifies the landscape of the complexity of the local Hamiltonian problem by collapsing the hierarchy proposed in [7]: the complexity of the local Hamiltonian problem with inverse polynomial promise gap is either in P, NP-complete or QMA-complete.

The interesting consequences of our result apply when such strong derandomization assumptions do not hold (or are not proven). More concretely, we show that if error reduction for StoqMA is proven (Conjecture 1.1), then StoqMA = MA (Figure 1b) and the four classes of local Hamiltonian problems in [7] become: P, NP-complete, MA-complete or QMA-complete. We notice that MA is a much more natural complexity class than StoqMA, so while this does not collapse any of these categories, it qualitatively simplifies their landscape.

But if on top of Conjecture 1.1, we also assume weak derandomization (i.e. MA = NP), then StoqMA = NP (Figure 1c), and we also have that the complexity of the local Hamiltonian problem with inverse polynomial promise gap is either in P, NP-complete or QMA-complete.

1.3 Proof overview

The starting point of the proof of Theorem 1.3 (given in Section 3) is the random walk used in [12, 13], to prove that the frustration-free stoquastic k-Local Hamiltonians problem is in MA.

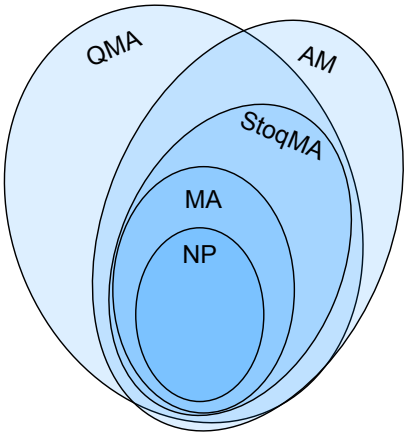
More concretely, the input to the problem is a stoquastic local Hamiltonian $H = \frac{1}{m}\sum_{i\in[m]} H_i$, where each H_i has norm at most 1, and acts on at most k out of an n qubit system. Then, we have to decide if there exists a quantum state $|\psi\rangle$ such that $\langle\psi|H|\psi\rangle = 0$, in which case we say that H is frustration-free, or for all possible quantum states $|\psi\rangle$, $\langle\psi|H|\psi\rangle \geq \frac{1}{\text{poly}(n)}$.

To prove containment in MA, [12, 13] define a random walk associated with H, which can be viewed as a walk on the following exponential-size (multi)graph $G(H)$. The vertices in the graph are all the possible n-bit strings, and the edges are defined as follows: for each $i \in [m]$, we connect the two nodes (strings) x, y iff $\langle x|H_i|y\rangle \neq 0$. [12, 13] also define the notion of a *bad string*, which is a string that does not appear in the support of any of the groundstates of some local term, i.e., x is bad if there exists some i such that $\langle x|H_i|x\rangle = 0$ (and as expected, if x is not bad, we say it is good).

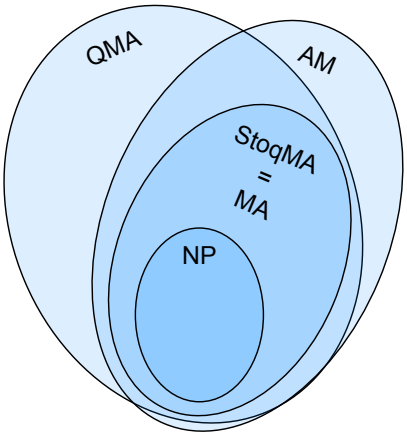
The MA-verification consists of running a random walk on $G(H)$ for polynomially many steps, starting at an n-bit string x_0 provided by the prover and rejecting if at any point along the walk a bad string is encountered.[10] [12, 13] showed that if the stoquastic Hamiltonian is frustration-free, then the connected component of any string in the support of any groundstate of the Hamiltonian, does not contain bad strings, and so any walk on the above defined graph, which starts from some string in a groundstate, does not reach bad strings. On the other hand, if the Hamiltonian is at least $\frac{1}{p(n)}$ frustrated, for some polynomial p, then there exists some polynomial q such that a $q(n)$-step random walk starting from any initial string reaches a bad string with high probability.

In this work, we will keep the soundness part of the proof of [13], showing that for negative instances, no matter what string you start with, a random walk will reach a bad string after polynomially many steps with constant probability. However, we need a stronger statement for completeness. In the case of perfect completeness, it was true that *any* string x in the support of a groundstate, would be a good witness, namely a random walk starting at x will never reach a bad string. Once we relax the perfect completeness requirement, this is no longer the case:

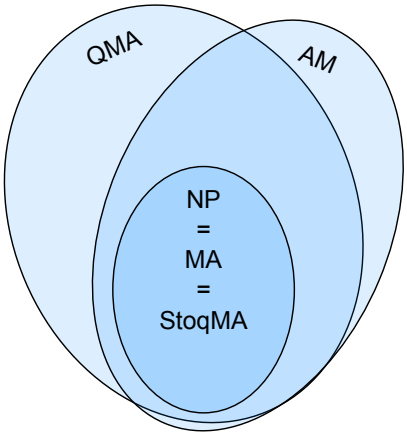
[10] Notice that such a walk can be implemented efficiently since we since we can compute the neighbors of each string in polynomial-time given H.



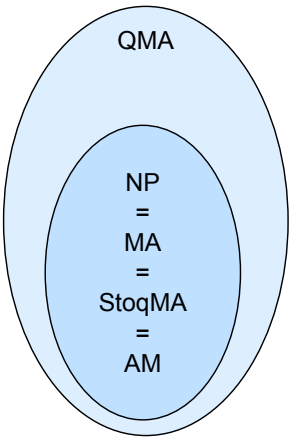
(a) The currently known relation between the complexity classes.



(b) Relation between the complexity classes if error reduction is possible for StoqMA.



(c) Relation between the complexity classes if error reduction is possible for StoqMA and we assume weak derandomization assumptions.



(d) Relation between the complexity classes under strong derandomization assumptions.

Figure 1: Relation between the complexity classes NP, MA, StoqMA, AM and QMA.

for example the groundstate could contain a bad string $\hat{x}$, and any random walk starting at $\hat{x}$ rejects. However, we are able to show that if H has *negligible* frustration, then there must exist *some* initial string x_0 such that the probability that a polynomial-time random walk starting from x_0 reaches a bad string, is negligibly small.

The main idea to prove this result is to use a central result of [22], connecting the amount of frustration of the Hamiltonian, to a certain quantity of *expansion* in the graph. More precisely, the result we use says that if the Hamiltonian has only negligible frustration, then there must exist a non-empty set of nodes S in $G(H)$ (recall that nodes correspond to n-bit strings) such that i) all strings in the set are good strings, and ii) the set has negligible expansion. The existence of such a set is proven in Lemma 3.5.

Given such a set, we prove in Lemma 3.8 that there exists one node in the set from which bad strings are hard to reach. To show this, we apply results about *escaping probabilities* of random walks [25]: if we start on a uniformly random element of the weakly expanding set of

good strings S, then the probability that we leave this set is negligibly small. We can then apply an averaging argument, to deduce that there must exist *some* initial string x_0 with the same property that starting the random walk from it, the probability to escape the set within polynomially many times steps of the walk, is negligible; this proves our result.

1.4 Conclusions and open questions

In this work, we prove a simple result which somewhat unexpectedly connects two problems; one, the question of the relation between MA and StoqMA, and the other, the question of error reduction for StoqMA. This connection might lead to a clarification of the peculiar class StoqMA; hopefully, it can point at a path by which it can be proven that StoqMA=MA.

Of course, the main open problem that is highlighted by our work is whether error reduction for StoqMA is possible.

We mention also a related interesting question: this is the study of StoqMA (and the stoquastic Local Hamiltonian problem) with constant gap between completeness and soundness. In particular, if this problem can be solved in NP, as is the case for its frustration-free variant [22], then there would be a stronger connection between the Quantum PCP conjecture and the derandomization conjecture than the one proved in [22]: a slightly weaker gap amplification procedure for stoquastic Hamiltonians would already imply MA=NP.[11]

2 Preliminaries

2.1 Notation

For $n \in \mathbb{N}^+$, we denote $[n] = \{0, ..., n-1\}$. We we say that $f(n) = \text{negl}(n)$ if $f = o\left(\frac{1}{n^c}\right)$ for every constant c.

2.2 Graph theory and random walks

For some undirected graph $G = (V, E)$, and $v \in V$, let $d_G(v) = |\{u \in V : \{v, u\} \in E\}|$ be the degree of v. For some set of vertices $S \subseteq V$, we define the edge boundary of S as $\partial_G(S) = \{\{u, v\} \in E : u \in S, v \notin S\}$, the neighbors of S as $N_G(S) = \{u \in \overline{S} : v \in S, \{u, v\} \in E\}$ (where $N_G(u)$ for some $u \in V$ is shorthand for $N_G(\{u\})$); and finally the volume of S $vol_G(S) = |\{\{u, v\} : u \in S, v \in N_G(u)\}|$ and the conductance of S, $\phi_G(S) = \frac{|\partial_G(S)|}{vol_G(S)}$.

We define notions related to random walks on graphs; definitions are taken from [26]. One step in the random walk on the graph G starting on vertex v is defined by moving to vertex u with probability $p_{v,u} = \begin{cases} \frac{1}{d_G(v)}, & \text{if } \{u, v\} \in E \\ 0, & \text{otherwise} \end{cases}$.

A *lazy* random walk stays put with probability half, and with probability half applies a step of the above random walk. A lazy random walk on a connected undirected graph always converges to a unique *limiting distribution*; we denote this distribution over the vertices by π. It is well known that $\pi(v)$ is proportional to the degree of v, $d_G(v)$.

We denote by $x_1, ..., x_t \sim \text{RW}(G, x_0, t)$ the distribution over t-tuple of variables, $x_1, ..., x_t$, derived from running a t-step random walk on G starting at x_0.

[11] More precisely, Let us consider a gap amplification procedure ϕ that maps stoquastic Hamiltonians to stoquastic Hamiltonians such that: *a*) if the ground-energy of H is 0, then the ground-energy of $\phi(H)$ is negl(n); and *b*) if the ground-energy of H is at least $1/\text{poly}(n)$, then the ground-energy of $\phi(H)$ is at least some constant ε. [22] proves that if such ϕ exists, then MA = NP. The weaker version of the gap amplification that we mention would allow $\phi(H)$ ground-energy to be some constant ε', for $\varepsilon' < \varepsilon$, if H is frustration-free. See [22] for a more details on the gap amplification procedure.

Lemma 2.1 (Escaping probability, Proposition 3.1 in [25]). *Let $G(V, E)$ be a graph. For any $S \subseteq V$ and integer t, we have that a t-step lazy random walk starting at a randomly chosen vertex $v \in S$, where v is chosen with probability $\pi(v)$ restricted to S, leaves the set S with expected probability at most $1 - (1 - \phi_G(S)/2)^t$.*

2.3 Quantum computing

We review now the concepts and notation of Quantum Computation that are used in this work. We refer to Ref. [27] for a detailed introduction of these topics.

A pure quantum state of n qubits is a unit vector in the Hilbert space $\left\{\mathbb{C}^2\right)^{\otimes n}$, where $\otimes$ is the Kroeneker (or tensor) product. The basis for such Hilbert space is $\{|i\rangle\}_{i\in\{0,1\}^n}$. For some quantum state $|\psi\rangle$, we denote $\langle\psi|$ as its conjugate transpose. The inner product between two vectors $|\psi\rangle$ and $|\phi\rangle$ is denoted by $\langle\psi|\phi\rangle$ and their outer product as $|\psi\rangle\langle\phi|$.

We now introduce some notation which is somewhat less commonly used and more specific for this paper: the support of $|\psi\rangle$, $supp(|\psi\rangle) = \{i \in \{0,1\}^n : \langle\psi|i\rangle \neq 0\}$, is the set strings with non-zero amplitude. We call quantum state $|\psi\rangle$ *non-negative* if $\langle i|\psi\rangle$ is real and $\langle i|\psi\rangle \geq 0$ for all $i \in \{0,1\}^n$. For any $S \subseteq \{0,1\}^n$, we define the state $|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{i\in S} |i\rangle$ as the subset-state corresponding to the set S [28].

2.4 Complexity classes

A (promise) problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ consists of two non-overlapping subsets $\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}} \subseteq \{0,1\}^*$. We hereby define the main complexity classes that are considered in this work.

Definition 2.2 (MA). *A promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in$ MA iff there exist a polynomial $p(n)$ and a probabilistic polynomial-time verifier $V(x, w)$ where V takes as input a string $x \in \{0,1\}^*$ and a $p(n)$-bit witness w, and decides on acceptance or rejection of x such that*

Completeness. *If $x \in \mathcal{L}_{\text{yes}}$, then there exists w such that $\Pr[V$ accepts $(x, w)] \geq 2/3$;*

Soundness. *If $x \in \mathcal{L}_{\text{no}}$, for any witness w, $\Pr[V$ accepts $(x, w)] \leq 1/3$.*

It is worth mentioning that [11] provides an alternative quantum-mechanical definition of MA, namely, the verifier is a polynomial-size quantum circuit which uses only classical reversible gates (NOT, CNOT, Toffoli gate). This circuit receives a quantum witness, on top of auxiliary qubits, each of which is initialized either to the $|0\rangle$ or the $|+\rangle$ state. The verifier applies on this state the circuit, and then measures the output qubit in the computational basis and decides on acceptance/rejection.

By replacing the computational basis of the final measurement in the above definition, with a measurement in the Hadamard basis (arriving at the so-called *stoquastic verifier*), this leads to the complexity class StoqMA:

Definition 2.3 (StoqMA(a, b), adapted from [12]). *A stoquastic verifier is a tuple $V = (n, n_w, n_0, n_+, U)$, where n is the number of input bits, n_w the number of input witness qubits, n_0 the number of input auxiliary qubits $|0\rangle$, n_+ the number of input auxiliary qubits $|+\rangle$ and U is a quantum circuit on $n+n_w+n_0+n_+$ qubits with NOT, CNOT, and Toffoli gates. The acceptance probability of a stoquastic verifier V on input string $x \in \{0,1\}^n$ and n_w-qubit witness state $|\psi\rangle$ is defined as $\Pr[V$ accepts $(x, |\psi\rangle)] = \langle\psi_{\text{in}}|U^\dagger \Pi_{\text{out}} U|\psi_{\text{in}}\rangle$. Here $|\psi_{\text{in}}\rangle = |x\rangle \otimes |\psi\rangle \otimes |0\rangle^{\otimes n_0} \otimes |+\rangle^{\otimes n_+}$ is the initial state and $\Pi_{\text{out}} = |+\rangle\langle+|_1 \otimes I_{\text{else}}$ projects the first qubit onto the state $|+\rangle$.*
A promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in$ StoqMA(a,b) iff there exists a uniform family of stoquastic verifiers, such that for any fixed number of input bits n the corresponding verifier V uses at most $p_1(n)$ qubits, $p_2(n)$ gates where both p_1 and p_2 are polynomials; and obeys the following:

Completeness. *If $x \in \mathcal{L}_{\text{yes}}$, then there is some $|\psi\rangle$ s.t.* $\Pr[V \text{ accepts } (x, |\psi\rangle)] \geq a$;

Soundness. *If $x \in \mathcal{L}_{\text{no}}$, then for any $|\psi\rangle$,* $\Pr[V \text{ accepts } (x, |\psi\rangle)] \leq b$.

Remark 2.4. *We notice that we can assume $b \geq \frac{1}{2}$, WLOG: Notice that for a quantum circuit composed solely by classical reversible gates, if its input state is non-negative, so is its output, since classical gates do not modify the phases of the quantum state. In this case, the final state of the* StoqMA *verifier's circuit on any non-negative witness is $\alpha_0|0\rangle|\psi_0\rangle + \alpha_1|1\rangle|\psi_1\rangle$, where $\alpha_b \in \mathbb{R}$ and $|\psi_b\rangle$ is a non-negative state and therefore, the acceptance probability is at least*

$$\frac{1}{2}\left(\alpha_0^2\langle\psi_0|\psi_0\rangle + 2\alpha_0\alpha_1\langle\psi_0|\psi_1\rangle + \alpha_1^2\langle\psi_1|\psi_1\rangle\right) \geq \frac{1}{2}\left(\alpha_0^2 + \alpha_1^2\right) = \frac{1}{2}.$$

Remark 2.5. *As mentioned in Section 1, error reduction for* StoqMA(a, b) *remains an open question since majority voting does not work (at least not in a straightforward way). To see this, notice that in order to perform such a majority voting, one would need to compute ℓ parallel runs of the original* StoqMA *verifier, measure the output qubit of each one of such runs in the Hadamard basis, and then compute the majority of the outcomes. But, unfortunately, this requires ℓ measurements in the Hadamard basis, whereas we are only allowed to perform a single one of such measurements by the definition of* StoqMA *verifiers.*

2.5 Stoquastic Hamiltonians

The goal of this section is to describe the projection uniform stoquastic Local Hamiltonian problem. We start with the definition of local Hamiltonians.

Definition 2.6 (k-Local Hamiltonian)**.** *A* Hamiltonian *on n qubits is a Hermitian operator on $\mathbb{C}^{2^n}$, namely, a complex Hermitian matrix of dimension $2^n \times 2^n$. A Hamiltonian on n qubits is called* k-Local *if it can be written as $H = \sum_{i=1}^{m} H_i$, where each H_i can be written in the form $H_i = \tilde{H}_i \otimes I$, where $\tilde{H}_i$ acts on at most k out of the n qubits.*

We remark that WLOG we assume that each term H_i is positive semi-definite since we could just add a constant cI to the term to make it PSD; this only causes a constant shift in the eigenstates of the total Hamiltonian, hence does not change the nature of the problems we discuss here. We describe now the properties of the Hamiltonian in which we are interested.

Definition 2.7 (Ground-energy, frustration)**.** *The ground-energy of a Hamiltonian H acting on n qubits is defined as $\min_{|\psi\rangle}\langle\psi|H|\psi\rangle$, where the minimum is over all possible n-qubit states (of norm 1), a groundstate of H is a state which achieves such a minimum, i.e., $\operatorname{argmin}_{|\psi\rangle}\langle\psi|H|\psi\rangle$, and the groundspace of H is the subspace spanned by its groundstates. We say that a H is ε-frustrated if its ground-energy is at least ε and we say that H is frustration-free if its ground-energy is 0.*

We restrict ourselves to stoquastic Hamiltonians, which lie in between classical (diagonal) Hamiltonians and general quantum ones.

Definition 2.8 (Stoquastic Hamiltonian [11])**.** *A k-Local Hamiltonian $H = \sum_{i=1}^{m} H_i$ is called* stoquastic *in the computational basis if for all i, the off-diagonal elements of H_i (the local terms) in this basis are non-positive*[12]*.*

[12]Klassen and Terhal [29] have a different nomenclature. They call a matrix Z-symmetric if the off-diagonal elements of the local terms are non-positive and they call a Hamiltonian stoquastic if all local terms can be made Z-symmetric by local rotations.

Notice that the definition of stoquasticity is basis dependent, and in our definition we assume that the stoquastic Hamiltonian is *given* in the basis where each of the *local* terms is stoquastic, i.e., has non-positive off-diagonal elements.

A property of a stoquastic local Hamiltonian is that the groundspace of the local terms can be decomposed as a sum of orthogonal non-negative rank-1 projectors.

Lemma 2.9 (Groundspace of stoquastic Hamiltonians, Proposition 4.1 of [13])**.** *Let H be a stoquastic Hamiltonian and let P be the projector onto its groundspace. It follows that*

$$P = \sum_j |\phi_j\rangle\langle\phi_j|, \tag{1}$$

where for all j, $|\phi_j\rangle$ is non-negative and for $j \neq j'$, $\langle\phi_{j'}|\phi_j\rangle = 0$.

2.5.1 Projection Uniform Stoquastic Hamiltonians

We now restrict ourselves to stoquastic Local Hamiltonians whose local terms have groundspaces which are much simpler, namely, the groundspace is spanned by orthogonal subset-states. In addition, we also require each H_i to be itself a projection.

Definition 2.10 (projection uniform stoquastic Local Hamiltonian)**.** *A stoquastic Local Hamiltonian $H = \frac{1}{m}\sum_{i=1}^{m} H_i$ is called projection uniform if for all i: a) H_i is a projection and b) when considering the groundspace projector $P_i = I - H_i$, there exist disjoint sets $S_{i,j} \subseteq \{0,1\}^n$ such that $P_i = \sum_j |S_{i,j}\rangle\langle S_{i,j}|$, namely, the groundspace can be spanned by subset states on the disjoint sets $S_{i,j}$.*[13]

We can finally define the projection uniform stoquastic k-Local Hamiltonian problem.

Definition 2.11 (projection uniform stoquastic k-Local Hamiltonian problem ($\mathsf{ProjUSLH}(\alpha,\beta)$)**.** *We are given three parameters: $k \in \mathbb{N}^*$ which is called the locality, $\alpha, \beta : \mathbb{N} \to [0,1]$ which are a non-decreasing functions with $\alpha(n) < \beta(n)$. The* projection uniform stoquastic k-Local Hamiltonian *problem with completeness α and soundness β, and with parameters k, ε, is the following promise problem. Let n be the number of qubits of a quantum system. The input is a set of $m(n)$ uniform stoquastic Hamiltonians $H_1, \ldots, H_{m(n)}$ where m is a polynomial, s.t. $\forall i \in [m(n)] : H_i$ is a projection which acts on k qubits out of the n qubit system. Let $H = \frac{1}{m}\sum_{i=1}^{m} H_i$. We are promised that one of the following two conditions hold, and we need to decide which one:*
Yes. *There exists a n-qubit quantum state $|\psi\rangle$ such that $\langle\psi|H|\psi\rangle \leq \alpha$*
No. *For all n-qubit quantum states $|\psi\rangle$ it holds that $\langle\psi|H|\psi\rangle \geq \beta$.*

It turns out that considering this restricted family of Hamiltonians does not harm the StoqMA hardness:

Lemma 2.12 ($\mathsf{ProjUSLH}(\text{negl}, 1/\text{poly})$ is $\mathsf{StoqMA}(1-\text{negl}, 1-1/\text{poly})$-hard)**.** *For any polynomial $p_1(n)$ and negligible function $\varepsilon(n)$, there exists a polynomial $p_2(n)$ such that the problem $\mathsf{ProjUSLH}\left(\varepsilon(n), \frac{1}{p_2(n)}\right)$ is $\mathsf{StoqMA}\left(1-\varepsilon(n), 1-\frac{1}{p_1(n)}\right)$-hard.*

Proof. The proof is analogous to the MA-hardness proof of stoquastic 6-SAT (Appendix B in [13]), in which Kitaev's circuit to Hamiltonian construction is used to devise a local Hamiltonian whose ground state is the history of the verification computation. Given a StoqMA verifier with

[13] Notice that while there are multiple ways of decomposing the groundspace of H_i, there is at most one way of doing it if we require that all vectors in the decomposition are non-negative. In this case, the partition $\{S_{i,j}\}_j$ is unique.

completeness $1-\varepsilon(n)$ and soundness $1-\frac{1}{p_1(n)}$, we end up with a projection uniform stoquastic Hamiltonian H by following the construction in [13], except we replace the output constraint $\Pi_{out} := |0\rangle\langle 0|_1$ in [13] by $|+\rangle\langle +|_1$. More concretely, for a StoqMA circuit consisting of T gates $G_1, ..., G_T$ acting on a P-qubit proof, A auxiliary qubits $|0\rangle$ and R auxiliary qubits $|+\rangle$, we consider the terms:

$$\begin{aligned}
H_i^{aux0} &= |01\rangle\langle 01|_{1,T+P+i}, \forall i \in [A] \\
H_i^{aux+} &= |0-\rangle\langle 0-|_{1,T+P+A+i}, \forall i \in [R] \\
H_t^{clock} &= |01\rangle\langle 01|_{t,t+1}, \forall t \in [T] \\
H_t^{prop} &= I - \sum_z \left(|100\rangle|z\rangle + |110\rangle G_t|z\rangle\right)\left(\langle 100|\langle z| + \langle 110|\langle z|G_t\right)_{t-1,t,t+1,W(t)}, \forall t \in [T] \\
H^{out} &= |1-\rangle\langle 1-|_{T,T+1},
\end{aligned}$$

where $W(t)$ is the set of qubits on which the t-th gate acts. Notice that each of these terms are projections, that H_i^{aux0}, H_i^{aux+}, and H_t^{clock} are diagonal, and that all of the off-diagonal elements of H_t^{prop} and H^{out} are non-negative. Therefore, the sum of all of these terms is a projection uniform stoquastic Hamiltonian.

As is typically the case in the circuit to Hamiltonian construction proofs, the completeness parameter is preserved, namely, the ground-energy of H is upper-bounded by $\varepsilon(n)$ - this is because the history state $|\eta\rangle$ for the witness which is rejected with probability at most $\varepsilon(n)$, satisfies $\langle\eta|H_{out}|\eta\rangle = \|H_{out}|\eta\rangle\|^2 \leq \varepsilon(n)$.

For soundness, since the StoqMA verifier accepts any witness state with probability at most $1-1/p_1(n)$, the statement at the beginning of Section 14.4.4 in [1] (with ϵ in [1] being equal to $1-1/p_1(n)$) implies that the ground-energy of H is lower-bounded by

$$\lambda_{\min}(H) \geq \frac{C_0\left(1-\sqrt{1-1/p_1(n)}\right)}{L^3} \geq \frac{C_0\left(1-(1-1/2p_1(n))\right)}{L^3} = \frac{C_0}{2p_1(n)L^3} := \frac{1}{p_2(n)},$$

where C_0 is some positive constant, L is the number of clock qubits which is a polynomial, and $p_2(n)$ is clearly a polynomial. It completes the proof. □

3 Proof of main result

In this section we prove Theorem 1.3. To prove that ProjUSLH(negl, 1/poly) is in MA, it suffices to show that there exists a negligible function ε and some value $t = \text{poly}(n)$ such that:

Completeness. If H is a *yes*-instance, then there exists a string x such that any t-step random walk starting at x will reach a bad string with probability at most $\varepsilon(n)$;

Soundness. If H is a *no*-instance, then all t-step random walk will reach a bad string with constant probability.

We need to find t which satisfies both conditions. In Lemma 3.3, which is proven in Section 3.1, we derive the soundness: we show that there exists some $t = \text{poly}(n)$ which satisfies the soundness condition. This part in fact follows almost exactly the proof of [13]. We will later (in Sections 3.2 and 3.3) show that the completeness condition is satisfied for *any* polynomial t, which completes the proof of Theorem 1.3.

3.1 Soundness: Recalling the random walk argument from [13]

We describe now the random walk approach of [12,13] to show that the stoquastic frustration-free Hamiltonian problem is in MA. As in [22], we restrict ourselves to the simplified version of their result that works for projection uniform stoquastic Hamiltonian, which is sufficient for our purposes given that this problem is StoqMA-hard as proven in Lemma 2.12. We start with defining the configuration graph for a given projection uniform stoquastic Hamiltonian.

Definition 3.1 (Graph from projection uniform stoquastic Hamiltonian)**.** *Let $H = \frac{1}{m}\sum_i H_i$ be a projection uniform stoquastic k-local Hamiltonian on n qubits. We define the undirected multi-graph $G(H) = (\{0,1\}^n, E)$ where E is defined as follows. Let $M = (2^k)!$ and for each $i \in [m]$, let $S_i^x = \{y : \langle x|P_i|y\rangle > 0\} \cup \{x\}$.[14] For each $i \in [m]$, if $S_i^x \neq \emptyset$, for each $y \in S_i^x$ we add $\frac{M}{|S_i^x|}$ edges between (x, y).*

We now argue that the lazy random walk [15] on the above configuration graph is the same walk as used in [12, 13]. The random walk in [12, 13] is defined in the following way: first we pick a term H_i uniformly at random out of the m terms, and then we move from x to a random y such that $\langle y|H_i|x\rangle \neq 0$ (we say in this case that y and x are neighbors via H_i). As usual, we consider the lazy version of this walk. We note that the number of edges leaving a node x is

$$\sum_{i\in[m]} |S_i^x| \cdot \frac{M}{|S_i^x|} = mM,$$

and therefore the probability to move the string x to a string y in this walk is

$$\frac{M/|S_i^x|}{mM} = \frac{1}{m|S_i^x|},$$

summed over all i's such that x, y are neighbors via H_i. This gives the same ratio between probabilities to move to different y's from a given x, as in the lazy simple random walk induced on the graph in Definition 3.1, and thus we have an equivalent lazy random walk.

We note that in order to use known results in the literature regarding simple random walks, such as Lemma 2.1 we take from [25], we prefer to stick to the multi-graph notation and we add multiple edges that correspond to the weight of the random walk described in [12,13].

[12, 13] also define a notion of bad strings, which are strings that do not belong to any groundstate of some of the local terms.

Definition 3.2 (Bad strings [13])**.** *Given a local Hamiltonian $H = \frac{1}{m}\sum_i H_i$, we say that x is bad for H if there exists some $i \in [m]$ such that $\langle x|H_i|x\rangle = 0$.*

The random walk starts from some initial string x_0 sent by the prover, runs for T steps on this graph and at the end accepts iff no bad string was encountered in the walk. We remark that given some string x, one can compute in polynomial time all neighbors of x in $G(H)$ as well as decide whether x is bad for H, by just inspecting the groundspace of each local term.

[14] The forced inclusion of x in S_i^x guarantees that all vertices have self-loops and it does not change the random walk because, as we will see later, if $\langle x|P_i|x\rangle = 0$, the random walk halts.

[15] We use the term lazy random walk to highlight the fact that in Definition 3.1, we added self-loops for every node. We notice that since $x \in S_i^x$ for every i and $1 \leq |S_i^x| \leq k$, this is equivalent to the standard notion of lazy random walk where we stay in the same vertex with constant probability $\frac{1}{k}$.

1. Let x_0 be the initial string.
2. Repeat for $t = 0, ..., T-1$:
   (a) If x_t is bad for H, reject
   (b) Pick $i \in [m]$ uniformly at random
   (c) Pick a neighbor x_{t+1} of x_t via H_i uniformly at random
3. Accept

Figure 2: Random Walk from [13] (simplified to the uniform case)

Lemma 3.3 (Soundness, adapted from Section 6.2 of [13])**.** *For every polynomial p, there exists some polynomial q such that if H is at least $\frac{1}{p(n)}$-frustrated, then for every string x, for $T = q(n)$, the random walk from Figure 2 reaches a bad string (and thus rejects) with constant probability.*

This completes the soundness part. The intuition of the proof is easier to explain in the projection uniform case: as noticed by [30], in this case, the frustration of a uniform stoquastic Hamiltonian H is related to the expansion of the graph $G(H)$. Therefore, with inverse polynomial lower-bounds on the expansion of the graph and on the fraction of bad strings, one can show that there exists a polynomial q such that a $q(n)$-step random walk on $G(H)$ starting at any vertex must encounter a bad string with high probability.

3.2 Negligible frustration implies weakly expanding set of good strings

In [13], completeness was proven for the case of frustration-free Hamiltonian.

Lemma 3.4 (Completeness, adapted from Section 6.1 of [13])**.** *If H is frustration-free, then there exists some string x such that there are no bad-strings in the connected component of x.*

To prove this, [12, 13] show that if H is frustration-free, the set of strings in the support of any of its groundstates, form a union of connected components of $G(H)$. Since H is frustration-free, any such connected component must contain only good strings, since bad strings exhibit non-zero energy. Therefore any path starting at a vertex in this connected component never finds a bad string, and the verifier will always accept.

Here, we do not have frustration-freeness, so we have to work harder. Due to the negligible frustration in the yes case, we have the following "approximation" of the situation of connected components of good strings (the next subsection uses this lemma to prove completeness, by a random walk argument):

Lemma 3.5 (Weakly expanding set of good strings)**.** *For every negligible function ε, there exists a negligible function ε' such that the following holds. If a projection uniform stoquastic k-local Hamiltonian H has ground-energy at most $\varepsilon(n)$, then there exists some set $S \subseteq \{0,1\}^n$ of good strings such that $|\partial_{G(H)}(S)| < \varepsilon'(n)|S|$.*

In order to prove Lemma 3.5, we first list two auxiliary lemmas from [22].

Lemma 3.6 (Projection on boundary lower bounds energy - Lemma 5.2 from [22])**.** *Let H be a projection uniform stoquastic Hamiltonian and $|\psi\rangle = \sum_x \alpha_x |x\rangle$ be a positive state. Let N be the set $\{x \in supp(|\psi\rangle : \exists i \in [m], y \notin supp(|\psi\rangle), \langle x|P_i|y\rangle > 0\}$. Then $\langle\psi|H|\psi\rangle \geq \frac{1}{2^k m} \sum_{x \in N} \alpha_x^2$.*

To get a rough intuition behind this lemma, we consider two strings $x \in supp(|\psi\rangle)$ and $y \notin supp(|\psi\rangle)$ that are neighbors via some term H_i. The contribution of y to $\langle\psi|H_i|\psi\rangle$ is, on one hand, at least (some function of) α_x, the amplitude of x in $|\psi\rangle$, and, on the other hand, we expect a factor of $\frac{1}{2^k}$ to appear, corresponding to the fact that if $\langle y|P_i|x\rangle > 0$ it must be at least $1/2^k$ since the subset states comprising the groundspace of H_i have at most 2^k strings in their support.

Lemma 3.7 (Existence of a "nice" low energy state - Lemma 5.3 of [22])**.** *Let H be a projection uniform stoquastic Hamiltonian with non-zero ground-energy at most $\frac{1}{f(n)}$. Then for any $g(n) > 0$, there exists some non-negative state $|\psi\rangle$ that does not contain bad strings for H, contains only strings with amplitude at least $\delta = \frac{1}{\sqrt{g(n)|S|}}$ and has frustration at most $\frac{1}{f(n)(1-\frac{m}{f(n)}-\frac{1}{g(n)})}$, where $S = supp(|\psi\rangle)$.*

The proof of this lemma follows by starting from the true groundstate of H, and then removing all bad strings and strings with amplitude smaller than δ. The result follows by a simple calculation of the frustration of the remaining (renormalized) state. With these lemmas, we can prove Lemma 3.5

Proof of Lemma 3.5. Let $|\psi\rangle$ be the state that comes from Lemma 3.7, by picking $f(n) = 1/\varepsilon(n)$ and $g(n) = 1/\sqrt{\varepsilon(n)}$. As stated by Lemma 3.7, $|\psi\rangle$ does not contain bad strings, all the amplitudes are at least $\delta = \sqrt{\frac{\sqrt{\varepsilon(n)}}{|S|}}$, where $S = supp(|\psi\rangle)$, and this state has frustration

$$\langle\psi|H|\psi\rangle < \frac{\varepsilon(n)}{1 - m\varepsilon(n) - \sqrt{\varepsilon(n)}} \leq 2\varepsilon(n). \tag{2}$$

As in Lemma 3.6, let us define $N = \{x \in S : \exists y \notin S, i \in [m] \text{ s.t. } \langle x|P_i|y\rangle > 0\}$. We first show that $|N| \leq m2^{k+1}\sqrt{\varepsilon(n)} \cdot |S|$. Let us assume towards contradiction that

$$\frac{|N|}{|S|} > m2^{k+1}\sqrt{\varepsilon(n)}. \tag{3}$$

We have that

$$2\varepsilon(n) > \langle\psi|H|\psi\rangle \geq \frac{1}{m2^k}\sum_{x\in N}\alpha_x^2 \geq \frac{|N|\delta^2}{m2^k} > 2\delta^2\sqrt{\varepsilon(n)}|S| = 2\varepsilon(n),$$

where the first inequality holds from Equation (2), the second inequality holds from Lemma 3.6, the third inequality comes from the fact that $\alpha_x \geq \delta$, the fourth inequality comes from the assumption on $|N|$ and the last equality comes from the definition of δ. This is a contradiction and therefore Equation (3) does not hold.

We now notice that N counts vertices in the boundary of S in $G(H)$, whereas to finish the proof of Lemma 3.5, we need to upper bound on the number of edges. By the definition of $G(H)$ (Definition 3.1), each vertex is connected to at most $m2^k(2^k)!$ edges. Therefore, the result follows from the negation of Equation (3) by choosing $\varepsilon'(n) = m^2 2^{2k+1}(2^k)!\sqrt{\varepsilon(n)}$. □

3.3 The existence of a witness in the negligible frustration case

Using Lemma 3.5, we show that if a stoquastic Hamiltonian is negligibly frustrated, then there exists a string which is a "good starting point" for the random walk, i.e., there exists a vertex x^* such that for any polynomial p, a $p(n)$-step random walk starting from x^* finds a bad string with negligible probability.

Lemma 3.8. *For every negligible function ε, there exists a negligible function $\hat{\varepsilon}(n)$ such that the following holds. If a projection uniform stoquastic k-local Hamiltonian H has ground-energy at most $\varepsilon(n)$, then there exists a string $x_0 \in \{0,1\}^n$ such that for any polynomial p, the probability that a $p(n)$-step -random-walk starting at x_0 finds a bad string is bounded from above by $\hat{\varepsilon}(n)$.*

Proof. From Lemma 3.5, there exists some set $S \subseteq \{0,1\}^n$ of good strings such that $|\partial_{G(H)}(S)| < \varepsilon'(n)|S|$, for some $\varepsilon'(n) = \text{negl}(n)$.

In particular, this implies that $\phi(S) = \frac{|\partial_{G(H)}(S)|}{vol(S)} \leq \frac{|\partial_{G(H)}(S)|}{|S|} < \varepsilon'(n)$, where in the first inequality we use the fact that every $x \in S$ has a neighbor (not necessarily in S).[16] Therefore, if we pick $x_0 \in S$ at random with probability π_S (namely the probability proportional to the limiting distribution restricted to S), and perform a $p(n)$-step random walk starting from $x_0 \sim \pi_S$, we have by Lemma 2.1 that the expected probability of leaving the set S during this walk is at most

$$\mathop{\mathbb{E}}_{x_0 \sim \pi_S} \Pr_{x_1,\ldots,x_t \sim \text{RW}(G,x_0,t)} [\exists i \in [t] \text{ s.t. } x_i \notin S] \leq 1 - (1-\varepsilon'(n))^{p(n)} \leq p(n)\varepsilon'(n) := \hat{\varepsilon}(n). \tag{4}$$

Notice that if Equation (4) is true, then there must exist some value x_0 such that

$$\Pr_{x_1,\ldots,x_t \sim \text{RW}(G,x_0,t)} [\exists i \in [t] \text{ s.t. } x_i \notin S] \leq \hat{\varepsilon}(n), \tag{5}$$

by an averaging argument. Since all strings in S are good, we have that a random walk starting at x_0 finds a bad string with probability at most $\hat{\varepsilon}(n)$. □

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. As in [13], the verification algorithm consists of the random walk described in Figure 2 for $T = q(n)$, where q is the polynomial from Lemma 3.3.

Since q is a polynomial, we have from Lemma 3.8 that if H is a *yes*-instance of ProjUSLH(negl(n), 1/poly(n)), then there exists some x_0 such that the random walk rejects with probability at most $\hat{\varepsilon}(n)$, for some negligible function $\hat{\varepsilon}$.

From Lemma 3.3, we have that for any *no*-instance H of ProjUSLH(negl(n), 1/poly(n)) and any initial string x_0, the probability that the random walk in Figure 2 rejects is bounded from below by a constant > 0. □

Acknowledgements

D.A. and Y.L. were gratefully supported by ISF Grant No. 1721/17, and part of this work was done while Y.L. was affiliated with the Hebrew University of Jerusalem. Part of this work was done while A.B.G. was affiliated to CWI and QuSoft and part of it was done while A.B.G. was visiting the Simons Institute for the Theory of Computing A.B.G. is supported by ANR JCJC TCS-NISQ ANR-22-CE47-0004, and by the French National Research Agency award number ANR-22-PNCQ-0002.

[16] Notice that we can assume this without loss of generality, since if any $x \in S$ (which implies that x is good) is not connected to any other string, a random walk starting at it never finds a bad string since it stays stationary in a good string. In this case our statement is trivially true.

References

[1] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. "Classical and quantum computation". American Mathematical Soc. (2002).

[2] Julia Kempe and Oded Regev. "3-local hamiltonian is QMA-complete". Quantum Information and Computation **3**, 258–264 (2003).

[3] Julia Kempe, Alexei Kitaev, and Oded Regev. "The complexity of the local hamiltonian problem". SIAM Journal on Computing **35**, 1070–1097 (2006).

[4] Roberto Oliveira and Barbara M Terhal. "The complexity of quantum spin systems on a two-dimensional square lattice". Quantum Information & Computation **8**, 900–924 (2008).

[5] Dorit Aharonov, Daniel Gottesman, Sandy Irani, and Julia Kempe. "The power of quantum systems on a line". Communications in Mathematical Physics **287**, 41–65 (2009).

[6] Andrew M. Childs, David Gosset, and Zak Webb. "The bose-hubbard model is QMA-complete". In International Colloquium on Automata, Languages, and Programming. Pages 308–319. Springer (2014).

[7] Toby Cubitt and Ashley Montanaro. "Complexity classification of local hamiltonian problems". SIAM Journal on Computing **45**, 268–316 (2016).

[8] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Joshua Lapan, Andrew Lundgren, and Daniel Preda. "A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem". Science **292**, 472–475 (2001).

[9] Mark W Johnson, Mohammad HS Amin, Suzanne Gildert, Trevor Lanting, Firas Hamze, Neil Dickson, Richard Harris, Andrew J Berkley, Jan Johansson, Paul Bunyk, et al. "Quantum annealing with manufactured spins". Nature **473**, 194–198 (2011).

[10] Tameem Albash and Daniel A Lidar. "Adiabatic quantum computation". Reviews of Modern Physics **90**, 015002 (2018).

[11] Sergey Bravyi, David P. Divincenzo, Roberto Oliveira, and Barbara M. Terhal. "The complexity of stoquastic local hamiltonian problems". Quantum Info. Comput. **8**, 361–385 (2008).

[12] Sergey Bravyi, Arvid J Bessen, and Barbara M Terhal. "Merlin-arthur games and stoquastic complexity" (2006).

[13] Sergey Bravyi and Barbara Terhal. "Complexity of stoquastic frustration-free hamiltonians". SIAM Journal on Computing **39**, 1462–1485 (2010).

[14] Sergey Bravyi and Matthew Hastings. "On complexity of the quantum ising model". Communications in Mathematical Physics **349**, 1–45 (2017).

[15] Thomas J. Schaefer. "The complexity of satisfiability problems". In Proceedings of the 10th Annual ACM Symposium on Theory of Computing, STOC 78. (1978).

[16] László Babai. "Trading group theory for randomness". In Proceedings of the 17th Annual ACM Symposium on Theory of Computing. Pages 421–429. (1985).

[17] Ran Raz and Avishay Tal. "Oracle separation of BQP and PH". In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019. Pages 13–23. ACM (2019).

[18] Adam R Klivans and Dieter van Melkebeek. "Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses". SIAM Journal on Computing **31**, 1501–1526 (2002).

[19] Peter Bro Miltersen and N Variyam Vinodchandran. "Derandomizing arthur–merlin games using hitting sets". Computational Complexity **14**, 256–279 (2005).

[20] Martin Furer, Oded Goldreich, Yishay Mansour, Michael Sipser, and Stathis Zachos. "On completeness and soundness in interactive proof systems". Advances in Computing Research: A Research Annual, **5**, 429–442 (1989).

[21] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. "Achieving perfect completeness in classical-witness quantum merlin-arthur proof systems". Quantum Information & Computation **12**, 461–471 (2012).

[22] Dorit Aharonov and Alex Bredariol Grilo. "Stoquastic pcp vs. randomness". In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS). Pages 1000–1023. IEEE (2019).

[23] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. "Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?". Chic. J. Theor. Comput. Sci.**2009** (2009).

[24] Aram W Harrow and Ashley Montanaro. "Testing product states, quantum merlin-arthur games and tensor optimization". Journal of the ACM (JACM) **60**, 1–43 (2013).

[25] Shayan Oveis Gharan and Luca Trevisan. "Approximating the expansion profile and almost optimal local graph clustering". In 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012. Pages 187–196. (2012).

[26] David A. Levin, Yuval Peres, and Elizabeth L. Wilmer. "Markov chains and mixing times". American Mathematical Society. (2006).

[27] Michael A Nielsen and Isaac Chuang. "Quantum computation and quantum information" (2002).

[28] John Watrous. "Succinct quantum proofs for properties of finite groups". In Proceedings 41st Annual Symposium on Foundations of Computer Science. Pages 537–546. IEEE (2000).

[29] Joel Klassen and Barbara M Terhal. "Two-local qubit hamiltonians: when are they stoquastic?". Quantum **3**, 139 (2019).

[30] Dorit Aharonov and Alex B. Grilo. "Two combinatorial MA-complete problems". In 12th Innovations in Theoretical Computer Science Conference, ITCS 2021. Pages 36:1–36:20. (2021).