On the computational complexity of curing non-stoquastic Hamiltonians

Milad Marvian\textsuperscript{1,2,3}, Daniel A. Lidar\textsuperscript{2,3,4,5} & Itay Hen\textsuperscript{3,4,6}

Quantum many-body systems whose Hamiltonians are non-stoquastic, i.e., have positive off-diagonal matrix elements in a given basis, are known to pose severe limitations on the efficiency of Quantum Monte Carlo algorithms designed to simulate them, due to the infamous sign problem. We study the computational complexity associated with ‘curing’ non-stoquastic Hamiltonians, i.e., transforming them into sign-problem-free ones. We prove that if such transformations are limited to single-qubit Clifford group elements or general single-qubit orthogonal matrices, finding the curing transformation is NP-complete. We discuss the implications of this result.
he “negative sign problem”, or simply the “sign problem”\(^1\), is a central unresolved challenge in quantum many-body simulations, preventing physicists, chemists, and material scientists alike from being able to efficiently simulate many of the most profound macroscopic quantum physical phenomena of nature, in areas as diverse as high-temperature superconductivity and material design through neutron stars to lattice quantum chromodynamics. More specifically, the sign problem slows down quantum Monte Carlo (QMC) algorithms\(^2,3\), which are in many cases the only practical method available for studying large quantum many-body systems, to the point where they become practically useless. QMC algorithms evaluate thermal averages of physical observables by the (importance-) sampling of quantum configuration space via the decomposition of the partition function into a sum of easily computable terms, or weights, which are in turn interpreted as probabilities in a Markovian process. Whenever this decomposition contains negative terms, QMC methods tend to converge exponentially slowly. Most dishearteningly, it is typically the systems with the richest quantum—mechanical behavior that exhibit the most severe sign problem.

In defining the scope under which QMC methods are sign-problem free, the concept of “stoquasticity”, first introduced by Bravyi et al.\(^4\), has recently become central. The most widely used definition of a local stoquastic Hamiltonian is

**Definition 1** A local Hamiltonian, \(H = \sum_{\alpha=1}^{M} H_{\alpha} \) is called stoquastic with respect to a basis \(B \), if all the local terms \(H_{\alpha} \) have only non-positive off-diagonal matrix elements in the basis \(B \).

In the basis \(B \), the partition function decomposition of stoquastic Hamiltonians leads to a sum of strictly nonnegative weights and such Hamiltonians hence do not suffer from the sign problem. For example, in the path-integral formulation of QMC with respect to a basis \(B = \{ b \} \), the partition function \(Z \) is proportional to a \(b \)-fold product of sums over complete sets of basis states, \( \{ | b_{1} \rangle, \ldots, | b_{b} \rangle \} \), which are weighted by the size of the imaginary-time slice \( \Delta \tau = \beta \) and the matrix elements of \( e^{-\beta H} \). Namely, \( Z = \prod_{i=1}^{b} \sum_{b_i} \langle b_i | e^{-\beta \hat{H}} | b_{i+1} \rangle \), where \( L \) is the number of slices and periodic boundary conditions are assumed. For a Hamiltonian \( H \) that is stoquastic in the basis \( B \), all the matrix elements of \( e^{-\beta \hat{H}} \) are nonnegative for any \( \Delta \tau \), leading to nonnegative weights for each time slice. On the other hand, non-stoquastic Hamiltonians, whose local terms have positive off-diagonal entries, induce negative weights and generally lead to the sign problem\(^1,6\) unless certain symmetries are present.

The concept of stoquasticity is also important from a computational-complexity-theory viewpoint. For example, the complexity class StoqMA associated with the problem of deciding whether the ground-state energy of stoquastic local Hamiltonians is above or below certain values, is expected to be strictly contained in the complexity class QMA, that poses the same decision problem for general local Hamiltonians\(^5\). In addition, StoqMA appears as an essential part of the complexity classification of two-local qubit Hamiltonian problems\(^7\).

However, stoquasticity does not imply efficient (i.e., polynomial-time) equilibration. For example, finding the ground-state energy of a classical Ising model—which is trivially stoquastic—is already NP-hard\(^8\). Conversely, non-stoquasticity does not imply inefficiency: there exist numerous cases where an apparent sign problem (i.e., non-stoquasticity) is the result of a naive basis choice that can be transformed away, resulting in efficient equilibration\(^7,9\). Here, we focus on the latter, i.e., whether non-stoquasticity can be “cured”.

To this end, we first propose an alternative definition of stoquasticity that is based on the computational complexity associated with transforming non-stoquastic Hamiltonians into stoquastic ones. Then, we proceed by proving that finding such a transformation for general local Hamiltonians, even if restricted to the single-qubit Clifford group or the single-qubit orthogonal group, is computationally hard. Along the way, we provide several results of independent interest, in particular an algorithm to efficiently group local Hamiltonian terms, and an algorithm to efficiently decide the curing problem using Pauli operators. We conclude by discussing some implications of our results, employing planted solution ideas, and also some potential cryptographic applications.

**Results**

**Computationally stoquastic Hamiltonians.** To motivate our alternative definition, we first note that any Hamiltonian can trivially be presented as stoquastic via diagonalization. However, the complexity of finding the diagonalizing basis generally grows exponentially with the size of the system (as noted in ref.\(^6\)) and the new basis will generally be highly nonlocal and hence not efficiently representable. We also note that it is straightforward to construct examples where apparent non-stoquasticity may be transformed away. For example, consider the \(n \)-spin Hamiltonian \( H_{XZ} = \sum_{j} J_{ij} X_{i} X_{j} - \sum_{j} J_{ij} Z_{i} Z_{j} \), with nonnegative \( J_{ij} \), \( i \neq j \), and \( Z_{i} \). This Hamiltonian is non-stoquastic, but can easily be converted into a stoquastic form. Denoting the Hadamard gate (which swaps \( X \) and \( Z \) by \( W \)), consider the transformed Hamiltonian \( H_{XZ} = W^\dagger \sum_{j} J_{ij} X_{i} X_{j} + \sum_{j} J_{ij} Z_{j} \), which is stoquastic. The sign problem of the original Hamiltonian, \( H_{XZ} \), can thus be efficiently cured by a unit-depth circuit of single-qubit rotations. Moreover, thermal averages are invariant under unitary transformations; namely, defining \( (A)_{H} = Tr(e^{-\beta \hat{H}}A) / Tr(e^{-\beta \hat{H}}) \), it is straightforward to check that \( (A)_{H} = (UAU^\dagger)_{H_{U}} \). Therefore, if QMC is run on the transformed, stoquastic Hamiltonian, it is no longer slowed down by the sign problem. Finally, note that Definition 1 implies that a local Hamiltonian, \( H = \sum_{\alpha=1}^{M} H_{\alpha} \), is stoquastic if all terms \( H_{\alpha} \) are stoquastic. However, there always remains some arbitrariness in the manner in which the total Hamiltonian is decomposed into the various terms. Consider, e.g., \( H = -2X_{1} + X_{1}Z_{2} \). The second term separately is non-stoquastic, whereas the sum is stoquastic. This suggests that the grouping of terms matters (see the Methods section, “Grouping terms without changing the basis”).

The above considerations motivate a reexamination of the concept of stoquasticity from a complexity-theory perspective, which can have important consequences for QMC simulations. (A related approach was discussed in ref.\(^12\).) For example, given a \(k\)-local non-stoquastic Hamiltonian \( H = \sum_{\alpha} H_{\alpha} \) (where each summand is a \( k \)-local term, i.e., a tensor product of at most \( k \) non-identity single-qubit Pauli operators), similarly to ref.\(^13\), we may ask whether there exists a constant-depth quantum circuit \( U \) such that \( H = U H_{U} \) can be written as a \( k \)-local stoquastic Hamiltonian \( H = \sum_{\alpha} H_{\alpha} \) and if so, what the complexity associated with finding it is. It is the answer to the latter question that determines whether the Hamiltonian in question should be considered computationally stoquastic, i.e., whether it is feasible (in a complexity theoretic sense) to find a “curing” transformation \( U \), which would then allow QMC to compute thermal averages with \( H \) by replacing it with \( H' \). More formally, we propose the following definition:

**Definition 2** A unitary transformation \( U \) “cures” a non-stoquastic Hamiltonian \( H \) (i.e., removes its sign problem) represented in a given basis if \( H' = U H U^\dagger \) is stoquastic, i.e., its off-diagonal elements in the given basis are all non-positive. A
family of local Hamiltonians \( \{ H \} \) represented in a given basis is efficiently curable (or, equivalently, computationally stoquastic) if there exists a polynomial-time classical algorithm such that for any member of the family \( H \), the algorithm can find a unitary \( U \) and a Hamiltonian \( H' \) with the property that \( H = U H U^\dagger \) is local and stoquastic in the given basis.

As an example, the Hamiltonian \( H_{\text{CZ}} \) considered above is efficiently curable. General local Hamiltonians are unlikely to be efficiently curable as this would imply the implausible result that QMA = StoqMA\(^{12}\).

Note that given some class of basis transformations, our definition distinguishes between the ability to cure a Hamiltonian efficiently or in principle. For example, deciding whether a Pauli group element \( U = \bigotimes_{i=1}^n u_i \), where \( u_i \) belongs to the single-qubit Pauli group \( \mathcal{P}_1 = \{ I, X, Y, Z \times \{ \pm 1, \pm i \} \} \), can cure each term \( \{ H_a \} \) of a \( k \)-local Hamiltonian \( H = \sum_a H_a \), which can be solved in polynomial time (see the Methods section, “Curing using Pauli operators”). However, the Hamiltonian \( H = X_i Z_k \) cannot be made stoquastic in principle using a Pauli group element, as conjugating it with Pauli operators results in \( \pm X_i Z_k \), both of which are non-stoquastic (see ref. \(^{13}\) for the results on an intrinsic sign problem for local Hamiltonians). Therefore, the fact that general local Hamiltonians are not considered to be computationally stoquastic does not imply that curing is computationally hard for a given class of transformations.

The last example illustrates that, while the curing problem can be efficiently decided for the Pauli group, this group can cure a very limited family of Hamiltonians. This motivates us to consider the curing problem beyond the Pauli group. Our main result is a proof that even for particularly simple local transformations such as the single-qubit Clifford group and real-valued rotations, the problem of deciding whether a family of local Hamiltonians is curable cannot be solved efficiently, in the sense that it is equivalent to solving 3SAT and is hence NP-complete.

We assume that a \( k \)-local Hamiltonian \( H = \sum_a H_a \) is described by specifying each of the local terms \( H_a \) and the goal is to find a unitary \( U \) that cures each of these local terms. In general, a unitary \( U \) that cures the total Hamiltonian \( H \) may not necessarily cure all \( H_a \) separately. However, for all of the constructions in this paper, we prove that a unitary \( U \) cures \( H \) if and only if it cures all \( H_a \) separately. The decomposition \( \{ H_a \} \) is merely used to guarantee that verification is efficient and the problem is contained in NP.

### Complexity of curing for the single-qubit Clifford group

To study the computational complexity associated with finding a curing transformation \( U \), we shall consider for simplicity single-qubit units, \( U = \bigotimes_{i=1}^n u_i \), and only real-valued Hamiltonian matrices. As we shall show, even subject to these simplifying restrictions, the problem of finding a curing transformation \( U \) is computationally hard when \( U \) is not in the Pauli group.

We begin by considering the computational complexity of finding local rotations from a discrete and restricted set of rotations. Specifically, we consider the single-qubit Clifford group \( \mathcal{C}_1 \) (with group action defined as conjugation by one of its elements), defined as \( \mathcal{C}_1 = \{ U U^\dagger U \in \mathcal{P}_1 \} \), i.e., the normalizer of \( \mathcal{P}_1 \). It is well known that \( \mathcal{C}_1 \) is generated by \( W \) and the phase gate \( P = \text{diag}(1, i) \). \(^{14}\)

**Theorem 1** Let \( U = \bigotimes_{i=1}^n u_i \), where \( u_i \) belongs to the single-qubit Clifford group. Deciding whether there exists a curing unitary \( U \) for 3-local Hamiltonians is NP-complete.

We prove this theorem by reducing the problem to the canonical NP-complete problem known as 3SAT (3-satisfiability)\(^{15}\), beginning with the following lemma:

| \( x_i \) | \( x_j \) | \( x_k \) | \( W(x) H_{jk}^{(111)} W^\dagger(x) \) | \( (x_i \lor x_j \lor x_k) \) |
|---|---|---|---|---|
| 0 | 0 | 0 | Stoquastic | 1 |
| 0 | 0 | 1 | Stoquastic | 1 |
| 0 | 1 | 0 | Stoquastic | 1 |
| 1 | 0 | 0 | Stoquastic | 1 |
| 1 | 1 | 0 | Stoquastic | 1 |
| 1 | 0 | 1 | Non-stoquastic | 0 |

The Hamiltonian \( W(x) H_{jk}^{(111)} W^\dagger(x) \) is stoquastic (True) for any choice of the variables \( x \), except \( (x_i, x_j, x_k) = (0, 1, 1) \), which makes it non-stoquastic (False). This is precisely the truth table for the 3SAT clause \( x_i \lor x_j \lor x_k \).

**Lemma 1** Let \( u_i \in \{ I, W \} \), where \( I \) is the identity operation and \( W \) is the Hadamard gate. Deciding whether there exists a curing unitary \( U = \bigotimes_{i=1}^n u_i \) for 3-local Hamiltonians is NP-complete.

To prove Lemma 1, we first introduce a mapping between 3SAT and 3-local Hamiltonians. Our goal is to find an assignment of \( n \) binary variables \( x_i \in \{ 0, 1 \} \) such that the unitary \( W(x) \equiv \bigotimes_{i=1}^n W_{x_i} \) where \( x \equiv (x_1, \ldots, x_n) \) rotates an input Hamiltonian to a stoquastic Hamiltonian. We use the following 3-local Hamiltonian as our building block:

\[
H_{jk}^{(111)} = Z_i Z_j Z_k - 3(Z_i + Z_j + Z_k) - (Z_i Z_j + Z_i Z_k + Z_j Z_k),
\]

where \( i, j, \) and \( k \) are three different qubit indices. It is straightforward to check that

\[
W(x) H_{jk}^{(111)} W^\dagger(x) = W_j^x \otimes W_j^y \otimes W_k^z (H_{jk}^{(111)}) W_j^x \otimes W_j^y \otimes W_k^z
\]

is stoquastic (“True”) for any combination of the binary variables \( (x_i, x_j, x_k) \) except for \( (1, 1, 1) \), which makes \( (2) \) non-stoquastic ("False").

This is precisely the truth table for the 3SAT clause \( (x_i \lor x_j \lor x_k) \), where \( \lor \) denotes the logical disjunction and the bar denotes negation (see Table 1). We can define the other seven possible 3SAT clauses by conjugating \( H_{jk}^{(111)} \) with Hadamard or identity gates:

\[
H_{jk}^{(a\beta\gamma)} = W_i^a \otimes W_j^\beta \otimes W_k^\gamma H_{jk}^{(111)} W_i^a \otimes W_j^\beta \otimes W_k^\gamma
\]

The Hamiltonian \( W(x) H_{jk}^{(a\beta\gamma)} W^\dagger(x) \) is non-stoquastic (corresponds to a clause that evaluates to False) only when \( (x_i, x_j, x_k) = (\alpha, \beta, \gamma) \), and is stoquastic (True) for any other choice of the variables \( x \). We have thus established a bijection between 3-local Hamiltonians \( H_{jk}^{(a\beta\gamma)} \), with \((\alpha, \beta, \gamma) \in \{0, 1\}^3\), and the eight possible 3SAT clauses on three variables \( (x_i, x_j, x_k) \in \{0, 1\}^3\). We denote these clauses, which evaluate to False if \( (x_i, x_j, x_k) = (\alpha, \beta, \gamma) \), by \( C_{jk}^{(a\beta\gamma)} \).

The final step of the construction is to add together such “3SAT-clause Hamiltonians” to form

\[
H_{\text{3SAT}} = \sum_C H_{jk}^{(a\beta\gamma)}
\]

where \( C \) is the set of all \( M \) clauses in the given 3SAT instance \( \land C_{jk}^{(a\beta\gamma)} \). Having established a bijection between 3SAT clauses and 3SAT-clause Hamiltonians, the final step is to show that finding \( x \)
such that

\[ H' = W(x)H_{\text{SAT}}W(x) \] (5)

is stoquastic for every \( H_{\text{SAT}} \), is equivalent to solving the NP-complete problem of finding satisfying assignments \( x \) for the corresponding 3SAT instances. To prove the equivalence, we show (i) that satisfying a 3SAT instance implies that the corresponding \( H_{\text{SAT}} \) is cured, and (ii) that if \( H_{\text{SAT}} \) is cured, this implies that the corresponding 3SAT instance is satisfied.

(i) Note that any assignment \( x \) that satisfies the given 3SAT instance also satisfies each individual clause. It follows from the bijection we have established that such an assignment cures each corresponding 3SAT-clause Hamiltonian individually. The stoquasticity of \( H' \) then follows by noting that the tensor product of a stoquastic Hamiltonian with the identity matrix is still stoquastic and the sum of stoquastic Hamiltonians is stoquastic.

(ii) To simplify the argument, we assume that each clause has exactly three variables. This version of 3SAT, sometimes called EXACT-3SAT, remains NP-hard\(^7\). We prove that an unsatisfied 3SAT instance implies that the corresponding \( H_{\text{SAT}} \) is not cured. It suffices to focus on a particular clause \( C_{\alpha \beta \gamma} \). The choice of variables that makes this clause False rotates the corresponding 3SAT-clause Hamiltonian to one that contains a non-stoquastic \( +XX_X \) term, which generates positive off-diagonal elements in specific locations in the matrix representation of \( H_{\text{SAT}} \). In what follows, we show that no other 3SAT-clause Hamiltonian in \( H_{\text{SAT}} \) contains a \( \pm XX_X \) term and therefore these positive off-diagonal elements cannot be canceled out or made negative regardless of the choice of the other variables in the assignment. To see this, we first note that a 3SAT-clause Hamiltonian that does not contain \( x_0, x_2 \), and \( x_3 \) cannot generate a \( \pm XX_X \) term. Second, a choice of assignment for \( x_0, x_2 \), and \( x_3 \) that does not satisfy \( C_{\alpha \beta \gamma} \) would satisfy any other 3SAT-clause on these three variables. A satisfied 3SAT clause also does not generate an \( XX_X \) term. Therefore, the rotated Hamiltonian is guaranteed to be non-stoquastic.

This establishes that the problem is NP-Hard. Checking whether a given \( U \) cures all the local terms \( \{ H_m \} \) is efficient and therefore the problem is NP-complete.

To complete the proof of Theorem 1, let us consider the modified Hamiltonian

\[ \hat{H}_{\text{SAT}} = H_{\text{SAT}} + cH_0, \quad H_0 = -\sum_{i=1}^{n} (X_i + Z_i), \] (6)

where \( H_0 \) is manifestly stoquastic and \( c \) is any number larger than the maximum number of clauses that any variable appears in. As there are \( M \) clauses, we simply choose \( c = O(1)M \), which is still a polynomial in the number of variables. (Note that even a restricted variant of 3SAT with each variable restricted to appear at most in a constant number of clauses is still NP-Complete\(^8\) and therefore we can take \( c \) to be a constant.) The goal is to find a unitary \( U = \otimes_{i=1}^{n} u_i \) with \( u_i \in C_i \) that cures \( H_{\text{SAT}} \). Note first that any choice of \( U = \otimes_{i=1}^{n} W_i \) that cures \( H_{\text{SAT}} \) also cures \( \hat{H}_{\text{SAT}} \). Second, note that choosing any \( u_i \) that keeps \( H_0 \) stoquastic is equivalent to choosing one of the elements of \( C_i \equiv \{ I, X, W, XW \} \subset C_i \) (e.g., the phase gate, which is an element of \( C_i \), maps \( X \) to \( Y \) so it is excluded, as is \( WX \), which maps \( Z \) to \( -X \)). Therefore, by choosing \( c \) to be large enough, any choice of \( u_i \in C_i \) would transform \( \hat{H}_{\text{SAT}} \) into a non-stoquastic Hamiltonian. It follows that if \( u_i \in C_i \) and is to cure \( \hat{H}_{\text{SAT}} \) then in fact it must be an element of \( C_i \).

Next, we note that conjugating a matrix by a tensor product of \( X \) or identity operators only shuffles the off-diagonal elements, but never changes their values (for a proof see the Methods section, “Conjugation by a product of \( X \) operators”). Therefore, for the purpose of curing a Hamiltonian, applying \( X \) is equivalent to applying \( I \) and applying \( WX \) is equivalent to applying \( W \). With this observation, the set of operators that can cure a Hamiltonian is effectively reduced from \( \{ I, W, WX, X \} \) to \( \{ I, W \} \). According to Lemma 1, deciding whether such a curing transformation exists is NP-complete.

Complexity of curing for the single-qubit orthogonal group.

Similarly, we can use Lemma 1 to show that the problem of curing the sign problem remains NP-complete when the set of allowed rotations is extended to the continuous group of single-qubit orthogonal matrices, i.e., transformations of the form \( Q = \otimes_{i=1}^{n} q_i \), where \( q_i q_i^\dagger = I \forall i \). Namely:

**Theorem 2** Deciding whether there exists a curing orthogonal transformation \( Q \) for 6-local Hamiltonians is NP-complete.

See the Methods section, “Proof of Theorem 2”, for the proof. In analogy to the proof of Theorem 1, the crucial step is to show that by promoting each \( Z, X, \) and \( W \) to a two-qubit operator, the continuous set of possible curing transformations reduces to the discrete set considered in Lemma 1.

Implications and applications.

An immediate and striking implication of Theorem 1 is that even under the promise that a non-stoquastic Hamiltonian can be cured by one-local Clifford unitaries (corresponding to trivial basis changes), the problem of actually finding this transformation is unlikely to have a polynomial-time solution.

An interesting implication of Theorem 2 is the possibility of constructing “secretly stoquastic” Hamiltonians. That is, one may generate stoquastic quantum many-body Hamiltonians \( H_{\text{stoq}} \) but present these in a “scrambled” non-stoquastic form \( H_{\text{stoq}} \Rightarrow UH_{\text{stoq}}U^\dagger \), where \( U \) is a tensor product of single-qubit orthogonal matrices (or in the general case a constant-depth quantum circuit). We conjecture that the latter Hamiltonians will be computationally hard to simulate using QMC by parties that have no access to the “descrambling” circuit \( U \). In other words, it is possible to generate efficiently simulable spin models that might be inefficient to simulate unless one has access.

![Fig. 1 A classical bit string connecting a stoquastic Hamiltonian to a seemingly non-stoquastic Hamiltonian. One may generate an \( n \)-qubit stoquastic Hamiltonian \( H_{\text{stoq}} \) and then transform it using a randomly chosen unitary (specified by a classical bit string) to bring it into a seemingly non-stoquastic form. Unlike the generated stoquastic Hamiltonian, the simulation of the seemingly non-stoquastic Hamiltonian can be computationally hard. Also, as discussed here, given a non-stoquastic Hamiltonian, finding the bit string that converts it into a stoquastic Hamiltonian can be computationally hard in general. Therefore, the classical bit string can serve as a secret key, without which certain properties of \( H_{\text{stoq}} \) cannot be efficiently simulated.](https://10.1038/s41467-019-09501-6)
to the “secret key” to make them stoquastic (see Fig. 1). This observation may potentially have cryptographic applications (see the Methods section, “Encryption based on secretly stoquastic Hamiltonians”).

Our work also has implications for the connection between the sign problem and the NP-hardness of a QMC simulation. A prevailing view of this issue associates the origin of the NP-hardness of a QMC simulation to the relation between a (“fermionic”) Hamiltonian that suffers from a sign problem and the corresponding (“bosonic”) Hamiltonian obtained by replacing every coupling coefficient by its absolute value. Consider the following example: \( H_X = \sum_{ij} J_{ij} X_i X_j \), with \( J_{ij} \) randomly chosen from the set \{0, ±1\} on a three-dimensional lattice, has a sign problem. Deciding whether its ground-state energy is below a given bound is NP-complete\(^6\). Deciding the same for its bosonic and sign-problem-free version \( H_X^b = \sum_{ij} |J_{ij}| X_i X_j \) is in BPP (classical polynomial time with bounded error) since this Hamiltonian is that of a simple ferromagnet. The conclusion drawn in ref. \(^6\) was that since the bosonic version is easy to simulate, the sign problem is the origin of the NP-hardness of a QMC simulation of this model (\( H_X \)).

The view we advocate here is that a solution to the sign problem is to find an efficiently computable curing transformation that removes it in such a way that the model has the same physics (in general the fermionic and bosonic versions of the same Hamiltonian do not), i.e., conserves thermal averages. In the above example, computing thermal averages via a QMC simulation of \( H_X \) is the same as for \( H_Z = \sum_{ij} H_{ij} Z_i Z_j \), which is stoquastic. Thus, the sign problem of \( H_Z \) is efficiently curable, after which (when it is presented as \( H_Z \)) deciding its ground-state energy remains NP-hard.

Discussion

We have proposed an alternative definition of stoquasticity (or absence of the sign problem) of quantum many-body Hamiltonians that is motivated by computational complexity considerations. We discussed the circumstances under which non-stoquastic Hamiltonians can in fact be made stoquastic by the application of single-qubit rotations and in turn potentially become efficiently simulable by QMC algorithms. We have demonstrated that finding the required rotations is computationally hard when they are restricted to the one-qubit Clifford group or one-qubit continuous orthogonal matrices.

These results raise multiple questions of interest. It is important to clarify the computational complexity of finding the curing transformation in the case of constant-depth circuits that also allow two-body rotations, whether discrete or continuous. Also, since our NP-completeness proof involved 3- and 6-local Hamiltonians, it is interesting to try to reduce it to 2-local building blocks. Another direction into which these results can be extended is to relax the constraints on the off-diagonal elements and require that they are smaller than some small \( \varepsilon > 0 \). This is relevant when some small positive off-diagonal elements can be ignored in a QMC simulation.

Finally, it is natural to reconsider our results from the perspective of quantum computing. Namely, for non-stoquastic Hamiltonians that are curable, do there exist quantum algorithms that cure the sign problem more efficiently than is possible classically? With the advent of quantum computers, specifically quantum annealers, it may be the case that these can be used as quantum simulators, and as such they will not be plagued by the sign problem. Will such physical implementations of quantum computers offer advantages over classical computing even for problems that are incurably non-stoquastic? We leave these as open questions to be addressed in future studies.

Methods

Proof of Theorem 2. The proof builds on that of Theorem 1, but first we note that the clause Hamiltonians introduced in Eq. (2) can have curing solutions that are orthogonal rotations outside the Clifford group (see Fig. 2). To deal with this richer set of rotations—which is now a continuous group—we promote each \( Z, X \), and \( W \) in the clause Hamiltonians to a two-qubit operator: \( Z_i \rightarrow Z_i \equiv Z_{i1} Z_{i2} \), \( X_i \rightarrow X_i \equiv X_{i1} X_{i2} \), \( W_i^n \rightarrow W_i^n \equiv W_{i1}^n \otimes W_{i2}^n \). Thus Eq. (1) becomes

\[
R_i^{(111)} = Z_i Z_j Z_k - 3(Z_i + Z_j + Z_k) - (Z_i Z_j + Z_i Z_k + Z_j Z_k). \tag{7}
\]

Let \( \tilde{W}(x) \equiv \bigotimes_{i} W_i^x \). It is again straightforward to check that \( \tilde{W}(x) H_i^{(111)} \tilde{W}(x) \) is stoquastic for any combination of the binary variables \( (x_0, \ldots, x_{n-1}) \) except for \((1, 1, 1)\). Likewise, generalizing Eq. (3), we define

\[
R_i^{(\alpha\beta\gamma)} = \tilde{W}_i^\alpha \otimes \tilde{W}_i^\beta \otimes \tilde{W}_i^\gamma \cdot R_i^{(111)} \cdot \tilde{W}_i^\alpha \otimes \tilde{W}_i^\beta \otimes \tilde{W}_i^\gamma, \tag{8}
\]

\( H_i^{(\alpha\beta\gamma)} \) is a clause Hamiltonian corresponding to a clause in the 3SAT instance. Similarly, \( \tilde{W}(x) H_i^{(\alpha\beta\gamma)} \tilde{W}(x) \) is stoquastic for any combination of the binary variables \( (x_0, \ldots, x_{n-1}) \) except for \((\alpha, \beta, \gamma)\). Generalizing Eq. (4) we define

\[
\mathcal{H}_{3SAT} = \sum_{C} \mathcal{H}_{i}^{(\alpha\beta\gamma)}, \tag{9}
\]

where \( C \) denotes the corresponding set of clauses in a 3SAT instance, constructed just as in the proof of Lemma 1. This, again, establishes a bijection between 3SAT clauses and “3SAT-clause Hamiltonians”, now of the form \( \mathcal{H}_{3SAT} \).

In lieu of Eq. (4), we consider the 6-local Hamiltonian \( \mathcal{H}_{6SAT} \)

\[
\mathcal{H}_{6SAT} = \mathcal{H}_{3SAT} + c H_6, \quad H_6 = \sum_{i} (Z_i^2 + X_i), \tag{10}
\]

where \( c = O(1) \). Just as in the proof of Theorem (1), we prove that (i) any satisfying assignment of a 3SAT instance provides a curing \( Q \) for the corresponding Hamiltonian \( \mathcal{H}_{6SAT} \), and (ii) any \( Q \) that cures \( \mathcal{H}_{6SAT} \) provides a satisfying assignment for the corresponding 3SAT instance. Because of the relation between a single-qubit orthogonal matrix and a single-qubit rotation, it suffices to prove the hardness only for pure rotations (see the next subsection for the relation between a
Fig. 3  Reducing the continuous region of solutions to a discrete set. The set of possible orthogonal transformations that can cure $H_{\text{SAT}}$ (introduced in Eq. (10)) reduces to a discrete set. We assign the value of each binary variable satisfying a 3SAT instance depending on the value of the curing transformation. We set $x_i = 0$ if the curing transformation has $(\theta_{x_i = 0}, \theta_{x_i = 1}) \in \{(0, 0), (\pi/2, \pi/2)\}$, while we assign $x_i = 1$ if the curing transformation has $(\theta_{x_i = 1}, \theta_{x_i = 0}) \in \{(-\pi/2, \pi/2), (\pi/2, -\pi/2)\}$

single-qubit real-orthogonal matrix and a single-qubit rotation); we let $R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$ denote a rotation by angle $\theta$.

(i) Let $P(x)$ denote the product of $2n$ single-qubit rotations such that if $x_i = 0$ then qubits $2i - 1$ and $2i$ are unchanged, or if $x_i = 1$ then they are both rotated by $R(\theta)$:

$$P(x) = \otimes_{i=1}^{n} R(\theta) \otimes R(\pi/4),$$

where $x$ is a $n$-bit string ($x_0, \ldots, x_n$). Let us now show that if the 3SAT instance has a satisfying assignment $x^*$ then $P(x^*) H_{\text{SAT}} P(x^*)$ is stoquastic. Note that $R(\pi/4) = XW$, and as we discussed in the article (under “Complexity of curing for the single-qubit Clifford group”) it is equivalent to $W$ for curing. To prove the claim, note that $x^*$ necessarily satisfies each individual clause of the 3SAT instance, and therefore makes the corresponding clause Hamiltonian stoquastic, i.e., $P(x^*) H_{\text{SAT}} P(x^*)$ is stoquastic $\forall \theta \in (0, \pi)$. Also, $P(x) H_{\text{SAT}} P(x)$ is clearly stoquastic for any $x$, where $H_0 = -\sum_{i=1}^{n} X_0 + X_1$ [Eq. (10)]. The stoquasticity of $P(x) H_{\text{SAT}} P(x)$, then follows immediately.

(ii) We need to prove that any rotation that cures $H_{\text{SAT}}$ provides a satisfying assignment for the corresponding 3SAT instance. We do this in two steps:

(a) Below “A useful lemma”, we prove that for any $H_{\text{SAT}}$, any curing rotation $R = \otimes_{i=1}^{n} R(\theta)$ has to satisfy the condition that $(\theta_{x_i = 1}, \theta_{x_i = 0}) \in \{(\pi/2, \pi/2), (0, \pi/2)\}$ $\forall i$. This is the crucial step, since it reduces the problem from a continuum of angles to a discrete set. If $(\theta_{x_i = 1}, \theta_{x_i = 0}) \in \{(\pi/2, \pi/2), (0, \pi/2)\}$, we assign $x_i = 0$, while if $(\theta_{x_i = 1}, \theta_{x_i = 0}) \in \{(-\pi/2, \pi/2), (\pi/2, -\pi/2)\}$, we assign $x_i = 1$, since rotations with the angles in each pair have the same effect.

(b) If $R$ cures $H_{\text{SAT}}$, $x = [x_0, \ldots, x_n]$ satisfies the corresponding 3SAT instance. See Fig. 3 for the discrete set of solutions and the corresponding assignments.

To see this, we first note that if $R$ cures $H_{\text{SAT}}$, it must cure all the clauses separately: Using step (a), we know that any such solution must be one of the four possible cases. Therefore, if $R$ were to cure $H_{\text{SAT}}$ but does not cure one of the 3SAT-clause Hamiltonians, it would result in a $\chi X \chi X \chi$ term in the corresponding clause. Since no other 3SAT-clause Hamiltonian in $H_{\text{SAT}}$ contains an identical $X_0 X_1 X_2$ term, these positive off-diagonal elements cannot be canceled out or made negative, regardless of the choice of the other variables in the assignment. Therefore, if $R$ cures $H_{\text{SAT}}$, it also necessarily separately cures all the terms in $H_{\text{SAT}}$. By construction, if $R$ cures a term $H_{\text{SAT}}^{(\psi)}$, the string $x$ satisfies the corresponding 3SAT clause $C(\psi)$. Thus $x$ satisfies all the clauses in the corresponding 3SAT instance. The decision problem for the existence of $R$ (and hence $Q$) is therefore NP-hard. Given a unitary $U$ and a set of local terms $\{H_j\}$, verifying whether $U$ cures all of the terms is clearly efficient and therefore this problem is NP-complete.

Relation between an orthogonal matrix and a rotation. The condition $q_i q_i^T = I$ forces each real-orthogonal matrix $q_i$ to be either a reflection or a rotation of the form

$$q_i = \begin{bmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{bmatrix},$$

with $a_i = +1$ (a reflection) or $a_i = -1$ (a rotation). The operators $X$, $Z$, and Hadamard, are included in the family with $a_i = 1$; and $I$ is $XZ$ are in the family with $a_i = -1$. Note that $\forall H, \forall \theta \in [0, \pi]$ $q_i(q_j H q_i^T q_j^T) = q_i(q_j + \pi) H q_j^T q_j^T$. Therefore, the angles that cure a Hamiltonian are periodic with a period of $\pi$.

Hence, it suffices to consider the curing solutions only in one period: $\theta_i \in \left(\frac{-\pi}{2}, \frac{\pi}{2}\right)$.

Next, observe that a reflection by angle $\theta_i$ can be written as

$$\begin{bmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{bmatrix} = X, \quad \begin{bmatrix} \cos \theta_i \sin \theta_i & -\sin \theta_i \cos \theta_i \\ \sin \theta_i \cos \theta_i & \cos \theta_i \sin \theta_i \end{bmatrix} = XR(\pi/2),$$

As discussed below (under “Conjugation by a product of X operators”), if $XR(\pi/2)$ is a curing operator so is $R(\pi/2)$. Therefore, any curing $Q = \otimes_{i=1}^{n} q_i$ provides a curing $R = \otimes_{i=1}^{n} R(\theta_i)$. Hence, the NP-completeness of the decision problem for $R$ implies the NP-hardness of the decision problem for $Q$, which is the statement of Theorem 2.

A useful lemma. Here, we prove that any curing rotation $R = \otimes_{i=1}^{n} R(\theta_i)$ for any $H_{\text{SAT}}$, as introduced in Eq. (10), must satisfy the condition that $(\theta_{x_i = 1}, \theta_{x_i = 0}) \in \{(\pi/2, \pi/2), (0, \pi/2)\}$ $\forall i$. In what follows, we show this for $i = 1$ (local rotations on the first two qubits), but the proof trivially works for any choice of $i$.

Our strategy is to expand any locally rotated $H_{\text{SAT}}$ on the first two qubits and then find necessary conditions that any curing rotations on these two qubits must satisfy. With this motivation, we introduce the following lemma:

**Lemma 2** Let $\theta_1, \theta_2 \in \left(\frac{-\pi}{2}, \frac{\pi}{2}\right)$. Consider the 2-qubit Hamiltonian

$$H' = Z_1 \otimes Z_2 \otimes M_1 + X_1 \otimes X_2 \otimes M_2 + I_1 \otimes I_2 \otimes M_1,$$

where $M_1$, $M_2$, and $M_3$ are Hamiltonians on $n-2$ qubits satisfying the following two conditions:

1. The absolute value of at least one element of $M_i$ is different from the absolute value of the corresponding element in $M_{i+1}$.
2. Both $M_i$ and $M_{i+1}$ have at least one negative element.

Then the only rotation $R(\theta_1) \otimes R(\theta_2)$ that can cure $H'$ has angles given by the following four points:

$$\{\theta_1, \theta_2\} \in \left\{\left(\frac{\pi}{4}, \frac{\pi}{4}\right), \left(0, \frac{\pi}{4}\right), \left(-\frac{\pi}{4}, \frac{\pi}{4}\right)\right\}.$$

To relate this lemma to our construction, note that any locally rotated $H_{\text{SAT}}$ is in the form of $H'$. To be more precise, we will choose $H' = R' \hat{H}_{\text{SAT}} R'^T$, where $R' = \otimes_{i=1}^{n} R(\theta_i)$.

We proceed by first proving the lemma. Then we show that both of the conditions introduced in the lemma are satisfied for our construction.

Proof: It is straightforward to check that

$$R(\theta) XR(\theta) = \cos 2\theta X - \sin 2\theta Z,$$

$$R(\theta) ZR(\theta) = \sin 2\theta X + \cos 2\theta Z.$$
off-diagonal elements for any nonzero matrix $B$ (a similar observation holds for $Z_iX_i \otimes C$). Second, we note that there are no common off-diagonal elements between $X_iX_j \otimes A, X_iY_j \otimes B,$ and $Z_iX_j \otimes C$. Third, there is no common off-diagonal elements between these three matrices and $Z_iZ_j \otimes D$ and $I_1I_2 \otimes E$. Therefore, these terms cannot make the $zB$ in $X_iZ_j \otimes B$ non-positive.

Thus, for $H'$ to become stoquastic it is necessary to have $B = 0$:

$$\sin 2\theta_1 \cos 2\theta_1 M_1 - \cos 2\theta_1 \sin 2\theta_1 M_1 = 0.$$  \hspace{1cm} (20)

Similar reasoning for $Z_iX_j \otimes C$ yields

$$\cos 2\theta_1 \sin 2\theta_1 M_1 - \sin 2\theta_1 \cos 2\theta_1 M_1 = 0.$$  \hspace{1cm} (21)

If the absolute value of at least one element of $M_1$ is different from the absolute value of the corresponding element in $M_\ell$ (i.e., Condition 1 is satisfied), comparing the corresponding expressions from Eqs. (20) and (21), we can conclude that

$$\sin 2\theta_1 \cos 2\theta_1 = \cos 2\theta_1 \sin 2\theta_1 = 0.$$

Equation (22) gives rise to two possible cases: (i) $\sin 2\theta_1 = \sin 2\theta_0 = 0$, or (ii) $\cos 2\theta_1 = \cos 2\theta_0 = 0$. For $\theta_i < \left( -\frac{\pi}{2}, \frac{\pi}{2} \right)$, these are the eight possible solutions:

$$\left(\theta_1, \theta_2\right) \in \left\{ \left(0, 0\right), \left(0, \frac{\pi}{2}\right), \left(0, -\frac{\pi}{2}\right), \left(\frac{\pi}{2}, \frac{\pi}{2}\right) \right\}.$$  \hspace{1cm} (23)

Now, we observe that Condition 2 generates additional constraints on the allowed values of $\theta_1$ and $\theta_2$. To see this, we consider the $X_iX_j \otimes A$ term in Eq. (19) in the two possible cases. For case (i), if $\sin 2\theta_1 = \sin 2\theta_0 = 0$ and hence $\cos 2\theta_1 = \cos 2\theta_0 = 1$, this term becomes $X_iX_j \cos 2\theta_0 \cos 2\theta_1$, if $M_1$ has any negative element, then the two combinations such that $\cos 2\theta_0 \cos 2\theta_1 = \cos 2\theta_1 = 1 \pm \cos 2\theta_0$ are the only rotations that can keep $H'$ stoquastic and make the term $M_1$ non-negative, if $M_1$ has any negative element, then the only rotations that can keep $H'$ stoquastic satisfy $\sin 2\theta_0 = -1$ or $\sin 2\theta_0 = 1$. Similarly, for case (ii), when $\cos 2\theta_0 = 0$, if $M_1$ has any negative element, the only rotations that can keep $H'$ stoquastic satisfy $\sin 2\theta_0 = -1$ or $\sin 2\theta_0 = 1$.

To summarize, if both conditions hold, the solutions are necessarily one of these four points:

$$\sin 2\theta_0 = 0, \cos 2\theta_0 = 1, \sin 2\theta_1 = 0, \cos 2\theta_1 = 1 \implies \left(\theta_1, \theta_2\right) = \left(0, 0\right).$$  \hspace{1cm} (24)

$$\sin 2\theta_0 = 0, \cos 2\theta_0 = -1, \sin 2\theta_1 = 0, \cos 2\theta_1 = -1 \implies \left(\theta_1, \theta_2\right) = \left(0, \frac{\pi}{2}\right).$$  \hspace{1cm} (25)

$$\sin 2\theta_0 = 1, \cos 2\theta_0 = 0, \sin 2\theta_1 = 1, \cos 2\theta_1 = 0 \implies \left(\theta_1, \theta_2\right) = \left(\frac{\pi}{4}, \frac{\pi}{4}\right).$$  \hspace{1cm} (26)

$$\sin 2\theta_0 = -1, \cos 2\theta_0 = 0, \sin 2\theta_1 = -1, \cos 2\theta_1 = 0 \implies \left(\theta_1, \theta_2\right) = \left(\frac{3\pi}{4}, \frac{3\pi}{4}\right).$$  \hspace{1cm} (27)

Having proved the lemma, we now proceed with identifying the properties of $M_1$ and $M_\ell$ for our construction. As mentioned earlier, we choose $H' = R R_{\text{SAT}} R^T$, where $R_{\text{SAT}} = \sum_{\ell = 1}^n R_\ell^{(\ell)}$. $M_\ell$ can be written as $H'_\ell = -L_\ell$, where $L_\ell$ denotes the terms in $M_\ell$ coming from $H_{\text{SAT}}$. Similarly, $M_1 = H_1 - L_1$, where $H_1$ denotes the terms in $M_1$ coming from $H_{\text{SAT}}$. The term $Z_i \otimes H_1$ (recall that $Z_i \equiv Z_i \otimes X_i$, and $X_i \equiv X_i \otimes X_i$) is composed of rotated $3$SAT-clause Hamiltonians that share $x_i$ in their corresponding $3$SAT clauses. Therefore, we have

$$H_1 = R R_{\text{SAT}} R^T = \sum_{\ell = 1}^n W_\ell \otimes W_\ell (Z_i X_i + 3 - Z_i X_i) W_\ell \otimes W_\ell R^T.$$  \hspace{1cm} (28)

It is straightforward to check that each of the rotated $3$SAT-clause Hamiltonians has only non-positive diagonal elements. Namely, using Eq. (17), it is straightforward to check that the max norm, defined as $\|A\|_{\text{max}} = \max_{|x|} |A_x|$, of any rotated Pauli operator is at most 1, and therefore the same is true for any tensor product of rotated Pauli operators. In each $3$SAT-clause Hamiltonian, there are three or less off-diagonal terms. Therefore, the off-diagonal elements that are larger than 3. There is a 3-term for each clause, guaranteeing that all the diagonal terms remain non-positive.

As $H_1$ is a sum of these matrices with all non-positive diagonal elements, we conclude that all the diagonal elements of $H_1$ are non-positive. $H_1$ is similar to $H_0$, but with a sum over $C_{\text{SAT}}^{(\ell)}$. Using similar arguments, we conclude that all the diagonal elements of $H_\ell$ are non-positive.

Therefore, all the diagonal elements of $M_1 = H_1 - L_1$ and $M_\ell = H_\ell - 2L$ are negative, and we conclude that Condition 2 is satisfied for our construction.

Now, we show that the first condition also holds. Using the cyclic property of the trace and noting that all the terms in $H_\ell$ except the 3-are traces, we have

$$\text{Tr}(H_\ell) = 3M_k \quad k \leq \ell$$

where $M_k \equiv \sum_{i=1}^n M_i$. Therefore, we have $\text{Tr}(H_\ell) = 3M_k$, where $k \leq \ell$. Using similar arguments, we conclude that $\text{Tr}(H_1) = 3M_k$, where $k \leq \ell$. The same holds for $H_\ell$.

Conjugation by a product of $X$ operators. Here, we show that conjugating a Hamiltonian by a product of $X$ operators or identity operators only shuffles the off-diagonal elements without changing their values.
Lemma 3 Let $U_X = X^n \otimes \cdots \otimes X^n$, where $a_i \in \{0, 1\}$. The set of off-diagonal elements of a general $2^n \times 2^n$ matrix $B$, $\text{OFF}(B) = \{|B|_{i,j} \in \{0, 1\}^n, i \neq j\}$, is equal to the set of off-diagonal elements of $U_X B U_X$ for all possible $|a_i|$. Proof. Let $a = (a_1, \ldots, a_n)$. Similarly, let $i$ and $j$ represent $n$-bit strings. The elements of the matrix $U_X B U_X$ are

$$
|U_X B U_X|_{ij} = (|U_X|_{i1} \otimes |U_X|_{j1}) \otimes \cdots \otimes (|U_X|_{in} \otimes |U_X|_{jn}) = (|i| \otimes |a|) (|j| \otimes |a|) = (|i| \otimes |a|) + (|j| \otimes |a|)
$$

where $\otimes$ denotes the XOR operation. Clearly for any fixed $a$, we have $|i| \otimes |a| \Leftrightarrow |j| \otimes |a|$ and therefore

$$
\text{OFF}(U_X B U_X) = \{|B|_{i,j} \in \{0, 1\}^n, i \neq j\} = \{|B|_{i,j} \in \{0, 1\}^n, i \otimes |a| \Leftrightarrow |a| \otimes a\}
$$

A similar argument proves that $U_X$ shuffles the diagonal elements: $\text{DIA}(U_X B U_X) = \text{DIA}(B)$

Therefore, conjugating a Hamiltonian by $U_X$ does not change the set of inequalities one needs to solve to make a Hamiltonian stoquastic. As a consequence, whenever we want to pick $U$, as a solution, we can instead choose $X^n$.

One-local rotations are not enough. Consider, e.g., the three Hamiltonians

$$
H_i = Z_{j} Z_{j+1} + X_{j} X_{j+1}, \quad (i,j) \in \{(1,2), (2,3), (3,1)\}.
$$

The sum of any pair of these Hamiltonians can be cured by single-qubit unitaries (e.g., $H_2 = H_1 + H_3$ can be cured by applying $U = Z_1$). In contrast, the frustrated Hamiltonian $H = H_1 + H_2 + H_3$ cannot be cured using any combination of single-qubit rotations. To see this, we first note that the partial trace of a stoquastic Hamiltonian is necessarily stoquastic. By partial trace over single qubits of $H$, we conclude that in order for $H$ to be stoquastic, all three $H_j$s must be stoquastic. To find all the solutions that convert each of these Hamiltonians into a stoquastic Hamiltonian, we expand $R_1(\theta_1) \otimes R_2(\theta_2) H R_1^\dagger(\theta_1) R_2^\dagger(\theta_2) \otimes R_3^\dagger(\theta_3)$ and note that it has $\sin 2(\theta_1 - \theta_2)$ and $\cos 2(\theta_1 - \theta_2)$ as off-diagonal elements. Demanding that the rotated Hamiltonians are all stoquastic (so that $\sin 2(\theta_1 - \theta_2) = 0$) forces $\cos 2(\theta_1 - \theta_2) = 1$ for $(i,j) \in \{(1,2), (2,3), (3,1)\}$. But this set of constraints does not have a feasible point. To see this note that

$$
\sin 2(\theta_1 - \theta_2) = \sin 2(\theta_1 - \theta_3) = \sin 2(\theta_2 - \theta_3) = -1 \times 1 = 0 \Leftrightarrow +1.
$$

Therefore, $H$ cannot be made stoquastic using $2 \times 2$ rotational matrices. Because of the relation between rotation and orthogonal matrices discussed above, we conclude that $H$ cannot be made stoquastic using $2 \times 2$ orthogonal matrices.

Encryption based on secretly stoquastic Hamiltonians. By generating 3SAT instances with planted solutions (see, e.g., refs. 39–42) and transforming these to non-stoquastic Hamiltonians via the mapping prescribed by Theorems 1 (or 2), one would be able to generate 3-local (or 6-local) Hamiltonians that are stoquastic, but are computationally hard to transform into a stoquastic form.

This construction may have cryptographic implications. For example, imagine planting a secret n-bit message in the (unique by design) ground state of a stoquastic Hamiltonian. Since the solution is planted, Alice automatically knows it. She checks that QMC can find the ground state in a prescribed amount of time $t(n)$, and if this is not the case, she generates a new, random, stoquastic Hamiltonian with the same planted solution and checks again, etc., until this condition is met. Alice and Bob pre-share the secret key, i.e., the curing transformation, and after they separate, Alice transmits only the $O(n^2)$ coefficients of the non-stoquastic Hamiltonians (transformed via the mapping prescribed by Theorem 1) for every new message she wishes to send to Bob. To discover Alice’s secret message, Bob runs QMC on the cured Hamiltonian. Since Alice verified that QMC can find the ground state in polynomial time, Bob will also find the ground state in polynomial time.

This scheme should be viewed as merely suggestive of a cryptographic protocol, since as it stands it contains several potential loopholes: (i) its security depends on the existence of effective two-or-more qubit curing transformations, as well as the absence of algorithms other than QMC that can efficiently find the ground state of the non-stoquastic Hamiltonians generated by Alice; (ii) the fact that Alice must start from Hamiltonians for which the ground state can be found in polynomial time may make the curing problem easy as well; (iii) this scheme transmits an $n$-bit message using $r n$ message bits, where $r$ is the number of bits required to specify the $n^2$ coefficients of the transmitted non-stoquastic Hamiltonian, so it is less efficient than a one-time pad. Additional research is needed to improve this into a scheme that overcomes these objections.

Data availability

Data sharing was not applicable to this article, as no datasets were generated or analyzed during the current study.

Received: 17 August 2018 Accepted: 14 March 2019
Published online: 05 April 2019

References

1. Loh, E. Y. et al. Sign problem in the numerical simulation of many-electron systems. Phys. Rev. B 41, 9307–9307 (1990).
2. Landau, D. & Binder, K. A Guide to Monte Carlo Simulations in Statistical Physics. (Cambridge University Press, New York, NY, USA, 2005).
3. Newman, M.E.J. and Barkema, G.T. Monte Carlo Methods in Statistical Physics. (Clarendon Press, New York, Oxford 1999).
4. Bravyi, S., DiVincenzo, D. P., Oliveira, R. I. & Terhal, B. M. The complexity of stoquastic local hamiltonian problems. Quant. Inf. Comp. 8, 0361 (2008).
5. Bravyi, S. & Terhal, B. Complexity of stoquastic frustration-free hamiltonians. SIAM J. Comput. 39, 1462–1485 (2009).
6. Troyer, M. & Wiese, U.-J. Computational complexity and fundamental limitations to fermionic quantum monte carlo simulations. Phys. Rev. Lett. 94, 170201 (2005).
7. Cubitt, T. & Montanaro, A. Complexity classification of local hamiltonian problems. SIAM J. Comput. 45, 268–316 (2016).
8. Barahona, F. On the computational complexity of Ising spin glass models. J. Phys. A: Math. Gen. 15, 3241 (1982).
9. Okunishi, K. & Harada, K. Symmetry-protected topological order and negative-sign problem for SO(n) bilinear-biquadratic chains. Phys. Rev. B 89, 134422 (2014).
10. Alet, F., Damié, K. & Pujari, S. Sign проблем-free monte carlo simulation of certain frustrated quantum magnets. Phys. Rev. Lett. 117, 197203 (2016).
11. Honerkamp, A. et al. Thermodynamic properties of highly frustrated quantum spin ladders: Influence of many-particle bound states. Phys. Rev. B 93, 054408 (2016).
12. Terhal, B. Adiabatic quantum computing conference, http://www.smapip.is.tohoku.ac.jp/aqc2017/program.html (2018).
13. Hastings, M. How quantum are non-negative wavefunctions? J. Math. Phys. 57, 012110 (2016).
14. Nielsen, M. A. & Chuang, I. L. Quantum computation and quantum information. (Cambridge University Press, 2000).
15. Karp, R. Reducibility among combinatorial problems. In Miller, R. E. & Thatcher, J. W. (eds.) Complexity of Computer Computations, The IBM Research Symposia Series, 85 (Plenum, New York, 1972).
16. Tovey, C. A. A simplified np-complete satisfiability problem. Discret. Appl. Math. 8, 85–89 (1984).
17. Hen, I. et al. Probing for quantum speedup in spin-glass problems with planted solutions. Phys. Rev. A 92, 042325 (2015).
18. Hamze, F. et al. From near to eternity: spin-glass planting, tiling puzzles, and constraint-satisfaction problems. Phys. Rev. E 97, 043303 (2018).

Acknowledgements

The research is based upon work (partially) supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via the U.S. Army Research Office contract W911NF-17-C-0050. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. We thank Ehsan Esmaymjezhadeh, Iman Marvian, Evgeny Mozgunov, Ben Reichardt, and Federico Spedalieri for useful discussions.

Author contributions

I.H. conceived of the project. M.M. devised most aspects of the technical proofs. I.H., D.A.L. and M.M. contributed equally to discussions and writing the paper.
