QMA-complete problems

Adam D. Bookatz*

December 12, 2012

Abstract

In this paper we give an overview of the quantum computational complexity class QMA and a description of known QMA-complete problems to date [1]. Such problems are believed to be difficult to solve, even with a quantum computer, but have the property that if a purported solution to the problem is given, a quantum computer would easily be able to verify whether it is correct. An attempt has been made to make this paper as self-contained as possible so that it can be accessible to computer scientists, physicists, mathematicians, and quantum chemists. Problems of interest to all of these professions can be found here.

1 Introduction

1.1 Background

The class QMA is the natural extension of the classical class NP to the quantum computing world. NP is an extremely important class in classical complexity theory, containing (by definition) those problems that have a short proof (or witness) that can be efficiently checked to verify that a valid solution to the problem exists. The class NP is of great importance because many interesting and important problems have this property – they may be difficult to solve, but given a solution, it is easy to verify that the solution is correct.

The probabilistic extension of NP is the class MA, standing for "Merlin-Arthur". Unlike in NP where witnesses must be verifiable with certainty, in MA valid witnesses need only be accepted with probability greater than 2/3 (and invalid witnesses rejected with probability greater than 2/3). MA can be thought of as the class of languages L for which a computationally-unbounded but untrustworthy prover, Merlin, can convince (with high probability) a verifier, Arthur (who is limited to polynomial-time computation), that a particular instance x is in L. Furthermore, when the instance x is not in L, the probability of Merlin successfully cheating must be low.

Because quantum computers are probabilistic by nature (as the outcome of a quantum measurement can generally be predicted only probabilistically), the *natural* quantum analogue of NP is actually the quantum analogue of MA, whence the quantum class QMA – Quantum-Merlin-Arthur[2]. QMA, then, is the class of languages for which small *quantum* witness states exist that enable one to prove, with high probability, whether a given string belongs to the language by whether the witness state causes an efficient *quantum verifier circuit* to output 1. It was first studied by Kitaev[20] and Knill[21]. A more precise definition will be given later.

The history of QMA takes its lead from the history of NP. In complexity theory, one of the most important results about NP was the first proof that it contains complete problems. A problem is NP-hard if, given the ability to solve it, one can also efficiently (that is, with only polynomial overhead) solve *any* other NP problem; in other words, a problem is NP-hard if any NP problem can be *reduced* to it. If, in addition to being NP-hard, a problem is itself in NP, it is called an NP-complete problem, and can be considered among the hardest of all the problems in NP. Two simple examples of NP-complete

*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA; bookatz@mit.edu

[1] The reader is invited to share more proven QMA-complete problems with the author.

[2] Initially QMA was referred to as BQNP [20]; the name QMA was coined in [32].

problems are BOOLEAN SATISFIABILITY (SAT) and CIRCUIT SATISFIABILITY (CSAT). The problem CSAT is to determine, given a boolean circuit, whether there exists an input that will be evaluated by the circuit as true. The problem SAT is to determine, given a set of clauses containing Boolean variables, whether there is an assignment of those variables that will satisfy all of the clauses. If the clauses are restricted to containing at most k literals each, the problem is called k-SAT. One may also consider the problem MAX-SAT, which is to determine, given a set of clauses (of Boolean variables) and an integer m, whether at least m clauses can be simultaneously satisfied.

The fact that a complete problem exists for NP is actually trivial, as the problem of deciding whether there exists a (small) input that will be accepted (in polynomial time) by a given Turing machine is trivially NP-complete; rather, the importance of NP-completeness is due to the existence of interesting NP-complete problems. The famous Cook-Levin theorem, which pioneered the study of NP-completeness, states that SAT is NP-complete. Its proof first shows that the above trivial NP-complete problem can be reduced to CSAT, and then shows that CSAT can be reduced to SAT.

The quantum analogue of CSAT is the QUANTUM CIRCUIT SATISFIABILITY problem (QCSAT), which is trivially QMA-complete (since QMA is defined in terms of quantum circuits). But QMA was found to have other, natural complete problems too. The most important of these, the k-LOCAL HAMILTONIAN problem [20], was defined by Kitaev [20] inspired by Feynman's ideas on Hamiltonian quantum computing [11]. This problem is a quantum analogue of MAX-SAT, in which Boolean variables are replaced by qubits and clauses are replaced by local Hamiltonians (which may be viewed as local constraints on the qubits); it is defined formally below in H-1. Just as the Cook-Levin theorem opened the study of NP-completeness by showing that CSAT (which was shown to be NP-complete) can be reduced to SAT, so too the study of QMA-completeness began by showing that QCSAT can be reduced to 5-LOCAL HAMILTONIAN.

However, unlike NP, for which thousands of complete problems are known, there are currently relatively few known QMA-complete problems. In this paper we will survey many, if not all, of them. This paper divides the QMA-complete problems into three main groups and one subgroup:

- Quantum circuit/channel property verification (V)
- Hamiltonian ground state estimation (H)
  - Quantum k-SAT (S)
- Density matrix consistency (C)

The letters in parentheses are used as labels to identify the group.

1.2 Formal definition of QMA

We now give a formal definition of QMA.

Definition 1.1. *QMA is the set of all languages $L \subset \{0,1\}^*$ for which there exists a (uniform family of) quantum polynomial-time verifier circuit V such that for every $x \in \{0,1\}^*$,*

if $x \in L$ then there exists a witness state $|\psi_x\rangle$ such that $V\big(x, |\psi_x\rangle\big)$ accepts with probability $\geqslant 2/3$

if $x \notin L$ then for every purported witness state $|\psi\rangle$, $V\big(x, |\psi\rangle\big)$ accepts with probability $\leqslant 1/3$.

Although the definition above used the numbers $2/3$ and $1/3$ (as is standard), we can generally define the class $\mathrm{QMA}(a,b)$: Given functions $a, b : \mathbb{N} \to (0,1)$ with $a(n) - b(n) \geqslant 1/\mathrm{poly}(n)$, a language is in $\mathrm{QMA}(a,b)$ if $2/3$ and $1/3$ in the definition above are replaced by a and b, respectively. It is important to note that doing this does not change the class: $\mathrm{QMA}(2/3, 1/3) = \mathrm{QMA}(1-\epsilon, \epsilon)$ provided that $\epsilon \geqslant 2^{-\mathrm{poly}(n)}$. Moreover, in going from $\mathrm{QMA}(2/3,1/3)$ to $\mathrm{QMA}(1-\epsilon,\epsilon)$, the amplification procedure can be carried out in such a way that the same witness is used, i.e. Merlin need only ever send a single copy of the witness state. [24]

When $a = 0$, i.e. when the witness must be verifiable with no error, the class is called QMA_1; thus $\mathrm{QMA}_1 = \mathrm{QMA}(1, 1/3) = \mathrm{QMA}(1, \epsilon)$. For the classical complexity class MA it is known that $\mathrm{MA} = \mathrm{MA}_1$, but it is still an open question whether $\mathrm{QMA}{=}\mathrm{QMA}_1$. Several QMA_1-complete problems are presented in this paper.

Furthermore, it should be noted that QMA actually consists of promise problems, meaning that when considering whether Merlin can truthfully convince Arthur or trick Arthur, we restrict our consideration to a subset of possible instances – we may assume that we are promised that our instance of consideration falls in this subset. With the above remarks, we can write the definition of QMA in a style matching that of the problem definitions provided in this paper.

Definition 1.2 (QMA). *A promise problem $L = L_{yes} \cup L_{no} \subset \{0,1\}^*$ is in QMA if there exists a quantum polynomial-time verifier circuit V such that for every $x \in \{0,1\}^*$,*

(yes case) *if $x \in L_{yes}$ then $\exists \text{poly}(|x|)$-qubit state $|\psi_x\rangle$ such that* $\Pr\left[V\left(x, |\psi\rangle_x\right) \text{ accepts}\right] \geqslant b$

(no case) *if $x \in L_{no}$ then $\forall \text{poly}(|x|)$-qubit states $|\psi\rangle$,* $\Pr\left[V\left(x, |\psi\rangle\right) \text{ accepts}\right] \leqslant a$

promised that one of these is the case (i.e. either x is in L_{yes} or L_{no}),
where $b - a \geqslant 1/\text{poly}(|x|)$ and $0 < \epsilon < a < b < 1 - \epsilon$, with $\epsilon \geqslant 2^{-\text{poly}(n)}$. If, instead, the above is true with $b = 1$, then L is in the class QMA_1.

Except for a glossary at the end, which provides the definitions of several basic reoccurring mathematical terms that appear in this work, the remainder of this paper is devoted to listing known QMA-complete problems, along with their description and sometimes a brief discussion. When a problem is given matrices, vectors, or constants as inputs, it is assumed that they are given to precision of $\text{poly}(n)$ bits. When a problem is given a unitary or quantum circuit, U_x, it is assumed that the problem is actually given a classical description x of the corresponding quantum circuit, which consists of $\text{poly}(|x|)$ elementary gates. Likewise, quantum channels are specified by efficient classical descriptions.

This paper has attempted to be as self-contained as possible, but for a more complete description and motivation of a problem, the reader is invited to consult the references provided. An attempt has been made to include as many currently known QMA-complete and QMA_1-complete problems as possible, but it is, of course, unlikely that this goal has been accomplished in full. The reader is invited to share other proven QMA-complete problems with the author for their inclusion in future versions of this work. Note that this paper has restricted itself to QMA-complete and QMA_1-complete problems; it does not include other QMA-inspired classes, such as QMA(2) (when there are multiple unentangled Merlins) or QCMA (when the witness is classical).

2 Quantum circuit/channel property verification

V-1 **QUANTUM CIRCUIT-SAT (QCSAT)**

Problem: Given a quantum circuit V on n witness qubits and $m = \text{poly}(n)$ ancilla qubits, determine whether:

(yes case) $\exists$ n-qubit state $|\psi\rangle$ such that $V(|\psi\rangle|0\ldots0\rangle)$ accepts with probability $\geqslant b$, i.e. outputs a state with $|1\rangle$ on the first qubit with amplitude-squared $\geqslant b$

(no case) $\forall$ n-qubit state $|\psi\rangle$, $V(|\psi\rangle|0\ldots0\rangle$ accepts with probability $\leqslant a$,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$ and $|0\ldots0\rangle$ is the all-zero m-qubit ancilla state.

This problem is QMA-complete immediately from the definition of QMA.

V-2 **NON-IDENTITY CHECK**

Problem: Given unitary U implemented by a quantum circuit on n qubits, determine whether U is *not* close to a trivial unitary (the identity times a phase), i.e.,
determine whether:

(yes case) $\forall \phi \in [0, 2\pi), \left\|U - e^{i\phi}\,\mathbb{1}\right\| \geqslant b$

(no case) $\exists \phi \in [0, 2\pi)$ such that $\left\|U - e^{i\phi}\,\mathbb{1}\right\| \leqslant a$,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$.

Theorem: QMA-complete [proven by Janzing, Wocjan, and Beth [13]]
Theorem: QMA-complete even for small-depth quantum circuits [proven by Ji and Wu [14]]
Hardness reduction from: QCSAT (V-1)

V-3 **NON-EQUIVALENCE CHECK**

This problem, a generalisation of NON-IDENTITY CHECK, is to determine whether two quantum circuits (do not) define approximately the same unitary (up to phase) on some chosen invariant subspace. The subspace could, of course, be chosen to be the entire space, but in many cases one is interested in restricting their attention to a subspace, e.g. one defined by a quantum error-correcting code.

Problem: Given two unitaries, U_1 and U_2, implemented by a quantum circuit on n qubits, let $\mathcal{V}$ be a common invariant subspace of $(\mathbb{C}^2)^{\otimes n}$ specified by a quantum circuit V (that ascertains with certainty whether a given input is in $\mathcal{V}$ or not). The problem is to determine, given U_1, U_2, and V, whether the restrictions of U_1 and U_2 to $\mathcal{V}$ are not approximately equivalent, i.e.,
determine whether:

(yes case) $\exists\ |\psi\rangle \in \mathcal{V}$ such that $\forall \phi \in [0, 2\pi), \left\| (U_1 U_2^\dagger - e^{i\phi}\,\mathbb{1})\,|\psi\rangle \right\| \geqslant b$

(no case) $\exists\ \phi \in [0, 2\pi)$ such that $\forall |\psi\rangle \in \mathcal{V}, \left\| (U_1 U_2^\dagger - e^{i\phi}\,\mathbb{1})\,|\psi\rangle \right\| \leqslant a,$

promised one of these to be the case,
where $b - a \geqslant 1/\mathrm{poly}(n)$.

Theorem: QMA-complete [proven by Janzing, Wocjan, and Beth [13]]
Hardness reduction from: NON-IDENTITY CHECK (V-2)

V-4 **MIXED-STATE NON-IDENTITY CHECK**

In this problem, either the given circuit acts like some unitary U that is far from the identity, or else it acts like the identity. This is very similar to non-identity check, but allows for mixed-states. The diamond norm used here is defined in the glossary (appendix A).

Problem: Given a quantum circuit C on n-qubit density matrices,
determine whether:

(yes case) $\|C - \mathbb{1}\|_\diamond \geqslant 2 - \epsilon$ and there is an efficiently implementable unitary U and state $|\psi\rangle$ such that $\|C(|\psi\rangle\langle\psi|) - U\,|\psi\rangle\langle\psi|\,U^\dagger\|_{tr} \leqslant \epsilon$ and $\|U\,|\psi\rangle\langle\psi|\,U^\dagger - |\psi\rangle\langle\psi|\,\|_{tr} \geqslant 2 - \epsilon$

(no case) $\|C - \mathbb{1}\|_\diamond \leqslant \epsilon$,

promised one of these to be the case,
where $1 > \epsilon \geqslant 2^{-\mathrm{poly}(n)}$.

Theorem: QMA-complete [proven by Rosgen [29]]
Hardness reduction from: Quantum circuit testing (see appendixB) (X-1)

V-5 **NON-ISOMETRY TESTING**

Preliminary information:
This problem tests to see if a quantum channel is not almost a linear isometry (given a mixed-state quantum circuit description of the channel).

Definition 2.1 (isometry)**.** *A linear isometry is a linear map $U : \mathcal{H}_1 \to \mathcal{H}_2$ that preserves inner products, i.e. $U^\dagger U = \mathbb{1}_{\mathcal{H}_1}$.*

Note that this is more general than a unitary operator, as $\mathcal{H}_1$ and $\mathcal{H}_2$ may be different sizes and U need not be surjective. Practically speaking, isometries are the operations involving unitaries that have access to fixed ancillae (say, ancillae starting in the $|0\rangle$ state). This problem asks how far from an isometry the input is, so it requires a notion of approximate isometries. A characterising property of isometries is that they map pure states to pure states, even in the presence of a reference system; therefore, the notion of an approximate isometry is defined in terms of how mixed the output of a channel is in the presence of a reference system.

Definition 2.2 (ϵ-isometry)**.** *A quantum channel Φ that is a linear transformation from $\mathcal{H}_1$ to $\mathcal{H}_2$ is an ϵ-isometry if $\forall |\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_1$, we have $\|(\Phi \otimes \mathbb{1}_{\mathcal{H}_1})(|\psi\rangle\langle\psi|)\| \geqslant 1 - \epsilon$. i.e. it maps pure*

states (in a combined input and reference system) to almost-pure states. The norm appearing in this definition is the operator norm[3].

Problem: Given a quantum channel Φ that takes density matrices of $\mathcal{H}_1$ to density matrices of $\mathcal{H}_2$, determine whether:

(yes case) Φ is not an ϵ-isometry, i.e. $\exists|\psi\rangle$ such that $\|(\Phi\otimes\mathbb{1}_{\mathcal{H}_1})(|\psi\rangle\langle\psi|)\|\leqslant\epsilon$

(no case) Φ is an ϵ-isometry, i.e. $\forall|\psi\rangle$, $\|(\Phi\otimes\mathbb{1}_{\mathcal{H}_1})(|\psi\rangle\langle\psi|)\|\geqslant 1-\epsilon$,

promised one of these to be the case,
where $\frac{1}{2}>\epsilon\geqslant 2^{-\text{poly}}$.

Theorem: QMA-complete when $0<\epsilon<1/19$ [proven by Rosgen [28, 29]]
Hardness reduction from: QCSAT (V-1)

V-6 DETECTING INSECURE QUANTUM ENCRYPTION

In this problem, we wish to determine whether the given purported encryption channel E is insecure on a large subspace (for any key), or is close to being perfectly secure. The diamond norm used here is defined in the glossary (appendix A).

Preliminary information:
A private channel is a quantum channel with a classical key such that the input state cannot be determined from the output state without the key. Formally, it is defined as follows.

Definition 2.3 (ϵ-private channel)**.** *Suppose E is a channel taking as input an integer $k\in\{1,\ldots,K\}$ and quantum state in space $\mathcal{H}_1$, and producing a quantum output in space $\mathcal{H}_2$, with $dim\mathcal{H}_1\leqslant dim\mathcal{H}_2$. Let E_k be the quantum channel where the integer input is fixed as k. Let Ω be the completely depolarizing channel that maps all density matrices to the maximally mixed state. E is an ϵ-private channel if $\|\frac{1}{K}\sum_k E_k-\Omega\|_\diamond\leqslant\epsilon$ (so if the key k is not known, the output of E gives almost no information about the input) and there is a polysize decryption channel D (operating on the same space as E) such that $\forall k,\|D_k\circ E_k-\mathbb{1}\|_\diamond\leqslant\epsilon$ (i.e. if k is known, the output can be reversed to obtain the input).*

Problem: Let $\delta\in(0,1]$. Given circuit E, which upon input k implements channel E_k acting from space $\mathcal{H}_1$ to $\mathcal{H}_2$ (with $\dim\mathcal{H}_1\leqslant\dim\mathcal{H}_2$),
determine whether:

(yes case) $\exists$ subspace S, with $\dim S\geqslant(\dim\mathcal{H}_1)^{1-\delta}$, such that for any k and any reference space $\mathcal{R}$, if ρ is a density matrix on $S\otimes\mathcal{R}$ then $\|(E_k\otimes\mathbb{1}_R)(\rho)-\rho\|_{tr}\leqslant\epsilon$

(no case) E is an ϵ-private channel,

promised one of these to be the case,
where $1>\epsilon\geqslant 2^{-\text{poly}}$.

Theorem: QMA-complete for $0<\epsilon<1/8$ [proven by Rosgen [29]]
Hardness reduction from: Quantum circuit testing (see appendixB) (X-1)

Notes: In this problem, channels are given as mixed-state circuits.

V-7 QUANTUM CLIQUE

This is the quantum analogue of the NP-complete problem LARGEST INDEPENDENT SET on a graph G, which asks for the size of the largest set of vertices in which no two vertices are adjacent. According to the analogy, the graph G becomes a channel, and two inputs are 'adjacent' if they can be confused after passing through the channel, i.e. if there is an output state that could have come from either of the two input states. In this quantum QMA-complete problem, the channel is a quantum entanglement-breaking channel Φ and the problem is to find the size of the largest

[3] definition provided in the glossary (appendix A)

set of input states that cannot be confused after passing through the channel, that is, to determine if there are k inputs $\rho_1, \ldots, \rho_k$ such that $\Phi(\rho_1), \ldots, \Phi(\rho_k)$ are (almost) orthogonal under the trace inner product. Regarding the name, note that the NP-complete problems LARGEST INDEPENDENT SET and LARGEST CLIQUE (which asks for the largest set of vertices, all of which are adjacent) are essentially the same: a set of vertices is an independent set on a graph G if and only if it is a clique on the complement of G.

Preliminary information:
Let S be the SWAP gate, so $S|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$. Note that $\mathrm{Tr}(\sigma_1\sigma_2) = \mathrm{Tr}(S\sigma_1 \otimes \sigma_2)$ for all density matrices σ_1 and σ_2, so the right hand side can be used to evaluate the trace inner product (and therefore determine orthogonality). For any density matrix ρ on k registers, let ρ^i denote the result of tracing out all but the ith register of ρ. Similarly, define $\rho^{i,j} = \mathrm{Tr}_{\{1,\ldots k\}\setminus\{i,j\}}(\rho)$.

Definition 2.4 (entanglement-breaking channel; q-c channel)**.** *A quantum channel Φ is entanglement-breaking if there are POVM (Hermitian, positive-semidefinite operators that sum to the identity) $\{M_i\}$ and states σ_i such that $\Phi(\chi) = \sum_i \mathrm{Tr}(M_i\chi)\sigma_i$. In this case it is a fact that $\Phi^{\otimes 2}(\rho^{1,2})$ is always a separable state. If the σ_i in the above definition can be chosen to be $\sigma_i = |i\rangle\langle i|$, where $|i\rangle$ are orthogonal states, then Φ is called a quantum classical channel (q-c channel).*

Problem: Given an integer k and a quantum entanglement-breaking channel Φ acting on n-qubit states,
determine whether:

(yes case) $\exists\ \rho_1 \otimes \cdots \otimes \rho_k$ such that $\sum_{i,j} \mathrm{Tr}(S\Phi(\rho_i) \otimes \Phi(\rho_j)) \leqslant a$

(no case) $\forall$ k-register state ρ, $\sum_{i,j} \mathrm{Tr}(S\Phi^{\otimes 2}(\rho^{i,j})) \geqslant b$,

promised one of these to be the case,
where b and a are inverse-polynomially separated.

There are two theorems associated with this problem.

(a) Theorem: QMA-complete [proven by Beigi and Shor [3]]

(b) Theorem: QMA_1-complete when $a = 0$ and Φ is further restricted to q-c channels [proven by Beigi and Shor [3]]

Hardness reduction from: k-local Hamiltonian (H-1)
Classical analogue: LARGEST INDEPENDENT SET is NP-complete.

V-8 QUANTUM NON-EXPANDER

A quantum expander is a superoperator that rapidly takes density matrices towards the maximally mixed state. The QUANTUM NON-EXPANDER problem is to check whether a given superoperator is *not* a good quantum expander. This problem uses the Frobenius norm[4].

Preliminary information:
A density matrix can always be written as $\rho = I + A$, where I is the maximally mixed state and A is traceless. A quantum expander is linear (and unital), so $\Phi(\rho) = I + \Phi(A)$, which differs from I by $\Phi(A)$. Thus a good quantum expander rapidly kills of traceless matrices. We have the following formal definition.

Definition 2.5 (quantum expander)**.** *Let Φ be a superoperator acting on n-qubit density matrices and obeying $\Phi(\rho) = \frac{1}{D}\sum_d U_d\rho U_d^\dagger$ where $\{U_d : d = 1, \ldots D\}$ is a collection of $D = \mathrm{poly}(n)$ efficiently-implementable unitary operators. Φ is a κ-contractive quantum expander if $\forall$ $2^n \times 2^n$ traceless matrix A, $\|\Phi(A)\|_F \leqslant \kappa\|A\|_F$.*

[4]definition provided in the glossary (appendix A)

Problem: Given a superoperator Φ that can be written in the form appearing in the above definition, determine whether:

(yes case) Φ is not a b-contractive quantum expander

(no case) Φ is an a-contractive quantum expander,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$.

Theorem: QMA-complete [proven by Bookatz, Jordan, Liu, and Wocjan [5]]
Hardness reduction from: QCSAT (V-1)

3 Hamiltonian ground-state energy estimation

H-1 **k-LOCAL HAMILTONIAN**

This is the problem of estimating the ground-state energy[5] of a Hamiltonian in which all interactions are k-local, that is, they only ever involve at most k qubits at a time. Formally, H is a k-local Hamiltonian if $H = \sum_i H_i$ where each H_i is a Hermitian operator acting (non-trivially) on at most k qubits. In addition to restricting the locality of a Hamiltonian in terms of the number of qubits on which it acts, one can also consider geometric restrictions on the Hamiltonian. Indeed, one can imagine a 2-local Hamiltonian in which interactions can only occur between neighbouring sites, e.g. $H = \sum_{i=1}^{n-1} H_{i,i+1}$ where each $H_{i,i+1}$ acts non-trivially only on particles i and $i+1$ arranged on a line. The results of these considerations will also be mentioned below. Note that all these problems use the operator norm[5].

Problem: Given a k-local Hamiltonian on n qubits, $H = \sum_{i=1}^{r} H_i$, where $r = \text{poly}(n)$ and each H_i acts non-trivially on at most k qubits and has bounded operator norm $\|H_i\| \leqslant \text{poly}(n)$, determine whether:

(yes case) H has an eigenvalue less than a

(no case) all of the eigenvalues of H are larger than b,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$.

Theorem: QMA-complete for $k \geqslant 2$ [proven by Kempe, Kitaev, and Regev [19]]
Hardness reduction from: QCSAT (V-1)

Additionally, it has been proved that it is:

(a) Theorem: QMA-complete when $k = O(\log n)$ (still provided $k \geqslant 2$) [proven by Kitaev [20]]

(b) Theorem: QMA-complete even when $k = 3$ with constant norms, i.e. $\|H_i\| = O(1)$ [proven by Nagaj [26]]

(c) Theorem: QMA-complete even when 2-local on a line of 11-dimensional qudits, i.e. when the qudits are arranged on a line and only nearest-neighbour interactions are present [proven by Nagaj[6] [25]]

(d) Theorem: QMA-complete even when 2-local on a 2-D lattice [proven by Oliveira and Terhal [27]]

(e) Theorem: QMA-complete even for interacting bosons under two-body interactions [proven by Wei, Mosca, and Nayak [33]]

[5] see the glossary (appendix A) for a very brief definition of these terms
[6] Based on initial work by Aharonov, Gottesman, Irani, and Kempe[1] who claimed this for 12-dimensional qudits

(f) Theorem: QMA-complete even for interacting fermions under two-body interactions [proven by Whitfield, Love, and Aspuru-Guzik [34]]

(g) Theorem: QMA-complete even when restricted to real 2-local Hamiltonians [proven by Biamonte and Love [4]]

(h) Theorem: QMA-complete even for stochastic[7]Hamiltonians (i.e. symmetric Markov matrices) when $k \geqslant 3$ [proven by Jordan, Gosset, and Love [15]]

Notes: For $k = 1$, the 1-LOCAL HAMILTONIAN is in P [19].
Many other simple modifications of k-LOCAL HAMILTONIAN are also QMA-complete. For example, QMA-completeness is not changed when restricting to dense k-local Hamiltonians, i.e. for a negative-semidefinite Hamiltonian when the ground energy is (in absolute value) $\Omega(n^k)$.[8]

Classical analogue: MAX-k-SAT is NP-complete for $k \geqslant 2$.
This problem may easily be rephrased in terms of satisfying constraints imposed by the H_i terms. The yes case corresponds to the existence of a state that violates, in expectation value, only fewer than a weighted-constraints; the no case, to all states violating, in expectation value, at least b weighted-constraints. This problem can therefore be viewed as estimating the largest number of simultaneously satisfiable constraints, whence the analogy to MAX-SAT.

H-2 **EXCITED k-LOCAL HAMILTONIAN**

We have seen that estimating the ground-state energy of a Hamiltonian is QMA-complete. The current problem shows that estimating the low-lying excited energies of a Hamiltonian is QMA-complete; specifically, estimating the c^{th} energy eigenvalue of a k-local Hamiltonian is QMA-complete when $c = O(1)$.

Problem: Given an integer $c \geqslant 1$ and a k-local Hamiltonian H on n qubits,
determine whether:
(yes case) the c^{th} eigenvalue of H is $\leqslant a$
(no case) the c^{th} eigenvalue of H is $\geqslant b$,
promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$.

Theorem: QMA-complete for $c = O(1)$ and $k \geqslant 3$ [proven by Jordan, Gosset, and Love [15]]
Hardness reduction from: 2-LOCAL HAMILTONIAN (H-1)

H-3 **HIGHEST ENERGY OF A k-LOCAL STOQUASTIC HAMILTONIAN**

Problem H-1h states that finding the lowest eigenvalue of a stochastic[9] Hamiltonian is QMA-complete. Since if H is a stochastic Hamiltonian then $-H$ is stoquastic[9], we also have QMA-completeness for the problem of estimating the largest energy of a stoquastic Hamiltonian.

Problem: Given a k-local stoquastic Hamiltonian H on n qubits,
determine whether:
(yes case) H has an eigenvalue greater than b
(no case) all of the eigenvalues of H are less than a,
promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$.

[7]definition provided in the glossary (appendix A)
[8][12] actually defined their problem for finding the highest energy of a positive-semidefinite Hamiltonian. Their interest lay in finding approximation algorithms for this problem.
[9]definition provided in the glossary (appendix A)

Theorem: QMA-complete for $k \geqslant 3$ [proven by Jordan, Gosset, and Love [15]]
Hardness reduction from: k-LOCAL STOCHASTIC HAMILTONIAN (H-1h) which itself is from (H-5a)

Notes: k-LOCAL STOQUASTIC HAMILTONIAN, i.e. finding the lowest energy rather than the highest energy, is in AM. [7]

H-4 **SEPARABLE k-LOCAL HAMILTONIAN**

This problem is the k-LOCAL HAMILTONIAN problem with the extra restriction that the quantum state of interest be a separable state, i.e. the question is whether there is a *separable* state with energy less than a (or greater than b). The state may still be entangled – the separability need only be with respect to a given partition of the space into two sets.

Problem: Given the same input as described in the k-LOCAL HAMILTONIAN problem, as well as a partition of the qubits to disjoint sets $\mathcal{A}$ and $\mathcal{B}$,
determine whether:
(yes case) $\exists\, |\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$, with $|\psi\rangle_A \in \mathcal{A}$ and $|\psi\rangle_B \in \mathcal{B}$, such that $\langle\psi|H|\psi\rangle \leqslant a$
(no case) $\forall\, |\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$, with $|\psi\rangle_A \in \mathcal{A}$ and $|\psi\rangle_B \in \mathcal{B}$, $\langle\psi|H|\psi\rangle \geqslant b$,
promised one of these to be the case,
where $b - a \geqslant 1/\mathrm{poly}(n)$.

Theorem: QMA-complete [proven by Chailloux and Sattath [9]]
Hardness reduction from: k-LOCAL HAMILTONIAN (H-1)

Notes: Interestingly, although the QMA-hardness proof follows immediately from k-LOCAL HAMILTONIAN, the "in QMA" proof is non-trivial and relies on the LOCAL CONSISTENCY PROBLEM (C-1).

H-5 **PHYSICALLY RELEVANT HAMILTONIANS**

2-LOCAL HAMILTONIAN is also QMA-complete when the Hamiltonian is restricted to various physically-relevant forms. These Hamiltonians may serve as good models for phenomena found in nature, or may be relatively easy to physically implement.

We will not explain all of the relevant physics and quantum chemistry here. However, we use the following notations:

The Pauli matrices X, Y, and Z are denoted as

$$\sigma^x = X, \qquad \sigma^y = Y, \qquad \sigma^z = Z, \qquad \boldsymbol{\sigma} = (\sigma^x, \sigma^y, \sigma^z).$$

When particles are on a lattice, $\langle i, j\rangle$ denotes nearest neighbours on the lattice. An electron on a lattice is located at some lattice site i and can be either spin-up ($\uparrow$) or spin-down ($\downarrow$). The operators $a^\dagger_{i,s}$ and $a_{i,s}$ are the fermionic raising and lowering operators, respectively; they create and annihilate an electron of spin $s \in \{\uparrow, \downarrow\}$ at site i, respectively. The operator corresponding to the number of electrons of spin s at site i is $n_{i,s} = a^\dagger_{i,s} a_{i,s}$.

Note that proving the QMA-completeness of physical Hamiltonians is important towards the goal of implementing adiabatic quantum computation: any QMA-complete Hamiltonian can be used to realise universal adiabatic quantum computation [4].

(a) The 2-local Hamiltonian

$$H_{ZZXX} = \sum_i h_i \sigma^z_i + \sum_i d_i \sigma^x_i + \sum_{i,j} J_{ij} \sigma^z_i \sigma^z_j + \sum_{i,j} K_{ij} \sigma^x_i \sigma^x_j$$

where coefficients d_i, h_i, K_{ij}, J_{ij} are real numbers. This represents a 2-local Ising model with 1-local transverse field and a tunable 2-local transverse $\sigma^x\sigma^x$ coupling. The $\sigma^x\sigma^x$ is realisable, e.g., using capacitive coupling of flux qubits or with polar molecules.[4].
Theorem: QMA-complete [proven by Biamonte and Love [4]]
Hardness reduction from: 2-LOCAL REAL HAMILTONIAN (H-1g)

Classical analogue: When when $K_{ij} = d_i = 0$ we obtain the famous Ising (spin glass) model with a magnetic field, which is NP-complete on a planar graph [2].

(b) The 2-local Hamiltonian

$$H_{ZX} = \sum_i h_i \sigma_i^z + \sum_i d_i \sigma_i^x + \sum_{i<j} J_{ij} \sigma_i^z \sigma_j^x + \sum_{i<j} K_{ij} \sigma_i^x \sigma_j^z$$

where coefficients d_i, h_i, K_{ij}, J_{ij} are real numbers. The $\sigma^x \sigma^z$ is realisable using flux qubits [4].
Theorem: QMA-complete [proven by Biamonte and Love [4]]
Hardness reduction from: 2-LOCAL REAL HAMILTONIAN (H-1g)

(c) The 2D Heisenberg Hamiltonian with local magnetic fields
The 2D Heisenberg Hamiltonian is a model for spins on a 2-dimensional lattice in a magnetic system, and is often used to study phase transitions. It takes the form

$$H_{\text{Heis}} = J \sum_{\langle i,j \rangle} \boldsymbol{\sigma_i} \cdot \boldsymbol{\sigma_j} - \sum_i \boldsymbol{\sigma_i} \cdot \boldsymbol{B}_i.$$

Here, sums over i range over all sites i in the lattice, and $\langle i, j \rangle$ range over nearest-neighbouring sites. The local magnetic field at site i is denoted by $\boldsymbol{B_i}$, and the coupling-constant J is a real constant. Hamiltonians restricted to this form are QMA-complete both for $J > 0$ and for $J < 0$.
Theorem: QMA-complete [proven by Schuch and Verstraete [30]]
Hardness reduction from: 2-local 2D-lattice Hamiltonian (H-1d)

(d) The 2D Hubbard Hamiltonian with local magnetic fields
The 2D Hubbard model describes a system of fermions on a 2-dimensional lattice and is therefore used to model electrons in solid-state systems. It takes the form

$$H_{\text{Hubb}} = -t \sum_{\langle i,j \rangle, s} a_{i,s}^\dagger a_{j,s} + U \sum_i n_{i,\uparrow} n_{i,\downarrow} - \sum_i \bar{\boldsymbol{\sigma}}_{\boldsymbol{i}} \cdot \boldsymbol{B}_i \ .$$

Here, sums over i range over all sites i in the lattice, $\langle i, j \rangle$ range over nearest-neighbouring sites, and s range over spins $\{\uparrow, \downarrow\}$. In this model, $\bar{\boldsymbol{\sigma}}_{\boldsymbol{i}}$ is the Pauli matrices vector converted into orbital pair operators: $\bar{\boldsymbol{\sigma}}_{\boldsymbol{i}} = \{\bar{\sigma}_i^x, \bar{\sigma}_i^y, \bar{\sigma}_i^z\}$ with $\bar{\sigma}_i^\alpha = \sum_{s,s'} \sigma_{ss'}^\alpha a_{i,s}^\dagger a_{i,s'}$ where $\sigma_{ss'}^\alpha$ denotes the (s, s') element of Pauli matrix σ^α. The local magnetic field at site i is denoted by $\boldsymbol{B_i}$, and t and U are positive numbers representing the electron-electron Coulomb repulsion and electron tunneling rate, respectively.
Theorem: QMA-complete [proven by Schuch and Verstraete [30]]
Hardness reduction from: Heisenberg Hamiltonian (H-5c)

H-6 **TRANSLATIONALLY INVARIANT k-LOCAL HAMILTONIAN**

There has been some interest in studying the k-LOCAL HAMILTONIAN (H-1) problem with the added restriction that the Hamiltonian be *translationally invariant*, i.e. that the Hamiltonian be identical at each particle (qudit[10]) in the system. Such systems are generally in a one-dimensional geometry with periodic boundary conditions. Some problems additionally employ geometric locality (which we refer to here as being on a line), such as constraining interactions to be between nearest-neighbouring particles, or between nearby (but not necessarily nearest-neighbouring) particles; some problems do not, however, have such geometric locality constraints. Current results are listed here. These results are all built on Ref.[1]. Finally, note that there may be complications in discussing QMA-completeness, since if a Hamiltonian is local and translationally invariant, the only input that scales is the number of qudits, n; it may need to be assumed that n is given to the problem in unary to avoid these complications, but we will not discuss this here.

[10] definition provided in the glossary (appendix A)

The k-LOCAL HAMILTONIAN problem is:

(a) Theorem: QMA-complete even with a translationally invariant 3-local Hamiltonian with 22-state qudits, but where the interactions are not necessarily geometrically local. [proven by Vollbrecht and Cirac [31]]

(b) Theorem: QMA-complete even for translationally invariant 2-local Hamiltonians on poly(n)-state qudits [proven by Kay [16]]

(c) Theorem: QMA-complete even for translationally invariant $O(\log n)$-local Hamiltonians on 7-state qudits, where the interactions are geometrically local (albeit not restricted to nearest-neighbours) [proven by Kay [16]]

(d) Theorem: QMA-complete even for 2-local Hamiltonians on a line of 49-state qudits where all strictly-2-local Hamiltonian terms are translationally invariant, although the 1-local terms can still be position-dependent [proven by Kay [17]]

Notes: Although not discussed here, similar results exist for rotationally invariant Hamiltonians [18].

H-7 **UNIVERSAL FUNCTIONAL OF DFT**

Preliminary information:

In quantum chemistry, *density functional theory* (DFT) is a method for approximating the ground-state energy of an electron system (see [30] and the references therein). The Hamiltonian for a system of N electrons is $H = T^e + V^{ee} + V^e$ where the kinetic energy, electron-electron Coulomb potential, and local potential are given respectively by

$$\begin{aligned} T^e &= -\frac{1}{2}\sum_{i=1}^{N} \nabla_i^2 \\ V^{ee} &= \sum_{1 \leqslant i < j \leqslant N} \frac{\gamma}{|\boldsymbol{r}_i - \boldsymbol{r}_j|} \\ V^e &= \sum_{i=1}^{N} V(\boldsymbol{x}_i) \end{aligned}$$

where $\gamma > 0$, $\boldsymbol{r}_i$ is the position of the ith electron, and $\boldsymbol{x}_i = (\boldsymbol{r}_i, s_i)$ is the position ($\boldsymbol{r}_i$) of the ith electron together with its spin (s_i).

The ground-state energy of a system of N electrons can be found by minimizing the energy over all N-electron densities $\rho^{(N)}(\boldsymbol{x})$, but it can also be given by minimizing over all single-electron probability distributions $n(\boldsymbol{x})$ as

$$E_0 = \min_n \Big(\mathrm{Tr}[V^e n(\boldsymbol{x})] + F[n(\boldsymbol{x})] \Big)$$

where the *universal functional of DFT* is

$$F[n(\boldsymbol{x})] = \min_{\rho^{(N)} \to n} \mathrm{Tr}\Big[(T^e + V^{ee}) \rho^{(N)}(\boldsymbol{x}) \Big] .$$

In the universal functional, the minimization is over all N-electron densities $\rho^{(N)}(\boldsymbol{x})$ that give rise to the reduced-density $n(\boldsymbol{x})$; therefore $F[n]$ gives the lowest energy of $T^e + V^{ee}$ consistent with n. The difficult part of DFT is approximating $F[n(\boldsymbol{x})]$, which is independent of the external potential V^e and is therefore universal for all systems.

Problem: Given an integer N, representing the number of electrons, and a one-electron probability density $n(\boldsymbol{x})$,
determine whether:

(yes case) $F[n(\boldsymbol{x})] \geqslant b$

(no case) $F[n(\boldsymbol{x})] \leqslant a$,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(N)$ and the strength of the Hamiltonian is bounded by $\text{poly}(N)$.

Theorem: QMA-complete [proven by Schuch and Verstraete [30, 34]]
Hardness reduction from: Hubbard model (H-5d)

3.1 Quantum k-SAT and its variations

Quantum k-SAT is really just the k-local Hamiltonian problem restricted to projection operators. Nonetheless, it is included here as a subsection of its own due to its high level of interest and study. Note that occasionally people speak of the problem MAX-quantum-k-SAT; this is just another name for the k-local Hamiltonian problem (H-1), and is therefore QMA-complete for $k \geqslant 2$. The problem Quantum k-SAT, however, is different.

S-1 **QUANTUM k-SAT**

Quantum k-SAT is the quantum analogue of the classical problem k-SAT. It is actually simply the k-local Hamiltonian problem restricted to the case of k-local projector Hamiltonians[11]. In classical k-SAT, the objective is to determine whether there exists a bit string (so each character in the string can be either 0 or 1) that satisfies (all of) a set of boolean clauses, each of which only involves at most k bits of the string. In the quantum analogue, rather than boolean clauses we have projection operators. A quantum k-SAT instance has a solution if there is a quantum state that passes (i.e., is a 0-eigenvalue of) each projection operator.

We provide two equivalent definitions of this problem here. The first emphasises quantum k-SAT as a special case of k-local Hamiltonian, and the second emphasises the similarity to classical k-SAT.

Problem: Given k-local projection operators $\{\Pi_1, \ldots, \Pi_m\}$ on n qubits, where $m = \text{poly}(n)$, and letting $H = \sum_{i=1}^{m} \Pi_i$,
determine whether:

(yes case) H has an eigenvalue of precisely 0

(no case) all of the eigenvalues of H are larger than b,

promised one of these to be the case,
where $b \geqslant 1/\text{poly}(n)$.

Equivalently, we can define the problem as follows.

Problem: Given polynomially many k-local projection operators $\{\Pi_i\}$,
determine whether:

(yes case) $\exists\ |\psi\rangle$ such that $\Pi_i|\psi\rangle = 0\ \forall i$

(no case) $\forall\ |\psi\rangle, \sum_i \langle\psi|\Pi_i|\psi\rangle \geqslant \epsilon$ (i.e. the expected number of 'clause violations' is $\geqslant \epsilon$),

promised one of these to be the case,
where $\epsilon \geqslant 1/\text{poly}(n)$.

Theorem: QMA_1-complete for $k \geqslant 4$ [proven by Bravyi [6]]
Hardness reduction from: QCSAT (V-1)

Notes: Quantum k-SAT is in P for $k = 2$. The case of $k = 3$ is still an open problem, but is known to be NP-hard.

Quantum k-SAT is still QMA_1-complete if instead of demanding that Π_i be projectors, we demand they be positive-semidefinite operators with zero ground-state energies and constant norms [26].

[11] definition provided in the glossary (appendix A)

Classical analogue: k-SAT is NP-complete for $k \geqslant 3$.

S-2 **QUANTUM $(d_1, d_2, \ldots, d_k)$-SAT**

Quantum $(d_1, d_2, \ldots, d_k)$-SAT is a quantum k-SAT problem but in which the ith qubit is replaced by a d_i-dimensional qudit, i.e. instead of the ith register containing a qubit (i.e. a 2-dimensional state), it contains a d_i-dimensional (qudit) state. For purposes of notation, we assume that $d_1 \geqslant d_2 \geqslant \ldots \geqslant d_k$.

For $k \geqslant 4$, this class is trivial: since quantum 4-SAT is QMA_1-complete for qubits, it is certainly QMA_1-complete for qudits. The cases of $k = 2$ or 3 are not fully understood; however, the following results are known.

(a) QUANTUM (5,3)-SAT, i.e. with a cinquit and a qutrit
Theorem: QMA_1-complete for $k = 2$ with $d_1 \geqslant 5$, $d_2 \geqslant 3$ [proven by Eldar and Regev [10]]

(b) QUANTUM (3,2,2)-SAT, i.e. with a qutrit and two qubits
Theorem: QMA_1-complete for $k = 3$ with $d_1 \geqslant 3$, and $d_2, d_3 \geqslant 2$ [proven by Nagaj and Mozes [26]]

(c) QUANTUM (11,11)-SAT ON A (ONE-DIMENSIONAL) LINE
Theorem: QMA_1-complete [proven by Nagaj [25]]

Notes: QUANTUM (2,2)-SAT, i.e. QUANTUM 2-SAT, is in P.
QUANTUM (d_1, d_2)-SAT when $d_1 < 5$ or $d_2 = 2$ are open questions. They are known to be NP-hard (except for $d_1 = d_2 = 2$ which is in P).[10]
QUANTUM (2,2,2)-SAT, i.e. QUANTUM 3-SAT, is in an open question.

Classical analogue: even though classical 2-SAT is in P, classical (3,2)-SAT, where one of the binary variables is replaced by a ternary variable, is NP-complete[10].

S-3 **STOCHASTIC k-SAT**

This problem is like QUANTUM k-SAT, except that instead of projection operators it uses stochastic, Hermitian, positive-semidefinite, operators (see glossary, appendix A, for definitions).

Problem: Given set of k-local stochastic, Hermitian, positive-semidefinite, operators $\{H_1, \ldots, H_m\}$ on n-qubits with norms bounded by $\mathrm{poly}(n)$,
determine whether:
(yes case) the lowest eigenvalue of $H = \sum_i H_i$ is 0
(no case) all eigenvalues of H are $\geqslant b$,
promised one of these to be the case,
where $b \geqslant 1/\mathrm{poly}(n)$.

Theorem: QMA_1-complete for $k = 6$ [proven by Jordan, Gosset, and Love [15]]
Hardness reduction from: QUANTUM 4-SAT (S-1)

Notes: STOQUASTIC QUANTUM k-SAT, where the word 'stochastic' is replaced by 'stoquastic' above, is in MA and is MA-complete for $k \geqslant 6$. [8] Note that STOCHASTIC k-SAT makes no mention of projection operators, and therefore isn't really a quantum k-SAT problem. In STOQUASTIC QUANTUM k-SAT, its MA-complete cousin, however, the operators can be converted to equivalent operators that are projectors, whence the relation to QUANTUM k-SAT. No connection to projectors is known in the stochastic case.

4 Density matrix consistency

C-1 **k-LOCAL DENSITY MATRIX CONSISTENCY**

Given a set of density matrices on subsystems of a constant number of qubits, this problem is to determine whether there is a global density matrix on the entire space that is consistent with the subsystem density matrices.

Problem: Consider a system of n qubits. Given $m = \text{poly}(n)$ k-local density matrices $\rho_1, \ldots, \rho_m$, so that each ρ_i acts only on a subset $C_i \subseteq \{1, \ldots n\}$ of qubits with $|C_i| \leqslant k$,
determine whether:

(yes case) $\exists$ n-qubit density matrix σ such that $\forall i$, if $\tilde{\sigma}_i = \text{Tr}_{\{1,\ldots,n\}\setminus C_i}(\sigma)$, then $\|\rho_i - \tilde{\sigma}_i\|_{tr} = 0$

(no case) $\forall$ n-qubit density matrix σ, $\exists i$ such that if $\tilde{\sigma}_i = \text{Tr}_{\{1,\ldots,n\}\setminus C_i}(\sigma)$, then $\|\rho_i - \tilde{\sigma}_i\|_{tr} \geqslant b$,

promised one of these to be the case,
where $b \geqslant 1/\text{poly}(n)$.

Theorem: QMA-complete even for $k = 2$ [proven by Liu [22]]
Hardness reduction from: k-LOCAL HAMILTONIAN (H-1). [Turing reduction]
Classical analogue: CONSISTENCY OF MARGINAL DISTRIBUTIONS is NP-hard.

C-2 **N-REPRESENTABILITY**

This is the same problem as 2-LOCAL DENSITY MATRIX CONSISTENCY (C-1), but specialised to fermions (particles whose quantum state must be antisymmetric under interchange of particles).

Problem: Given a system of N fermions and d possible modes, with $N \leqslant d \leqslant \text{poly}(N)$, and a $\frac{d(d-1)}{2} \times \frac{d(d-1)}{2}$ 2-fermion density matrix ρ,
determine whether:

(yes case) $\exists$ $\binom{d}{N} \times \binom{d}{N}$ N-fermion density matrix σ such that $\text{Tr}_{\{3,\ldots,N\}}(\sigma) = \rho$

(no case) $\forall$ N-fermion density matrices σ, $\|\rho - \text{Tr}_{\{3,\ldots,N\}}(\sigma)\|_{tr} \geqslant b$,

promised one of these to be the case,
where $b \geqslant 1/\text{poly}(N)$.

Theorem: QMA-complete [proven by Liu, Christandl, and Verstraete [23]]
Hardness reduction from: 2-LOCAL HAMILTONIAN (H-1) [Turing reduction]

C-3 **BOSONIC N-REPRESENTABILITY**

This is the same problem as 2-LOCAL DENSITY MATRIX CONSISTENCY (C-1), but specialised to bosons (particles whose quantum state must be symmetric under interchange of particles).

Problem: Given a system of N bosons and d possible modes, with $d \geqslant cN$ (for some constant $c > 0$), and a $\frac{d(d+1)}{2} \times \frac{d(d+1)}{2}$ 2-boson density matrix ρ,
determine whether:

(yes case) $\exists$ $\binom{N+d-1}{N} \times \binom{N+d-1}{N}$ N-boson density matrix σ such that $\text{Tr}_{\{3,\ldots,N\}}(\sigma) = \rho$

(no case) $\forall$ N-boson density matrices σ, $\|\rho - \text{Tr}_{\{3,\ldots,N\}}(\sigma)\|_{tr} \geqslant b$,

promised one of these to be the case,
where $b \geqslant 1/\text{poly}(N)$.

Theorem: QMA-complete [proven by Wei, Mosca, and Nayak [33]]
Hardness reduction from: 2-local Hamiltonian (H-1) [Turing reduction]

A Glossary

The definitions given here are not necessarily the most general or precise possible, but they suffice for the needs of this paper.

i^{th} energy of a Hamiltonian H – the i^{th} eigenvalue of H.

ground-state energy of a Hamiltonian H – the smallest eigenvalue of H.

Hamiltonian – the generator of time-evolution in a quantum system. Its eigenvalues correspond to the allowable energies of the system. It also dictates what interactions are present in a system. As a matrix, it is Hermitian.

Hermitian matrix – a square matrix H that is equal to its own conjugate-transpose, i.e. $H^\dagger = H$.

norms of matrices – Several different matrix norms appear in this paper. Given a matrix A with elements a_{ij}, the

- **operator norm** of A is $\|A\| = \max\{\|A|\psi\rangle\|_2 : \||\psi\rangle\|_2 = 1\}$. For a square matrix, it is also known as the spectral norm; it is the largest singular value of A, and if A is normal, then it is the largest absolute value of the eigenvalues of A.
- **Frobenius norm** of A is $\|A\|_F = \sqrt{\mathrm{Tr}[A^\dagger A]} = \sqrt{\sum_{i,j} |a_{ij}|^2}$.
- **trace norm** of A is $\|A\|_{tr} = \mathrm{Tr}\left[\sqrt{A^\dagger A}\right]$, which when A is normal is the sum of the absolute value of its eigenvalues. It is often written $\|A\|_{tr} = \mathrm{Tr}|A|$ where $|A|$ denotes $\sqrt{A^\dagger A}$.

norms of quantum superoperators – Occasionally norms of superoperators are required in this paper.

- **diamond norm** of a superoperator Φ that acts on density matrices that act on a Hilbert space $\mathcal{H}$ is $\|\Phi\|_\diamond = \sup_X \|(\Phi \otimes \mathbb{1})(X)\|_{tr} / \|X\|_{tr}$ where the supremum is taken over all linear operators $X : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$.

positive-semidefinite matrix – a Hermitian matrix whose eigenvalues are all non-negative.

k-local projector on n qubits – a Hermitian matrix of the form $\Pi = \mathbb{1}^{\otimes(n-k)} \otimes \sum_i |\psi\rangle\langle\psi|_i$ where the $|\psi\rangle_i$ are orthonormal k-qubit states. It satisfies $\Pi^2 = \Pi$.

stochastic matrix – a square matrix of non-negative real numbers such that each row sums to 1. If additionally each column sums to 1, it is called a doubly stochastic matrix.

stoquastic Hamiltonian – a Hamiltonian in which the off-diagonal matrix elements are non-positive real numbers in the standard basis.

qudit – generalization of a qubit: for some d, a d-state quantum-mechanical system, or mathematically, a unit-normalized vector in $(\mathbb{C}^d)$ (but where global phase is irrelevant). When $d = 2$ it is called a qubit, when $d = 3$ it is called a qutrit. When $d = 5$ it may be called a cinquit[10], but to avoid headaches, I advise against trying to name the $d = 4$ version.

B QMA-hard theorems

This appendix contains a theorem that allows one to prove that several quantum circuit verification problems are QMA-hard. Note that it doesn't prove QMA-completeness, only QMA-hardness, so it is relegated to the appendix.

X-1 **QUANTUM CIRCUIT TESTING**

This problem involves testing the behaviour of a quantum circuit. Given input circuit C, one wishes to determine whether it acts like a circuit from uniform circuit family $\mathscr{C}_0$ on a large input space, or like a circuit from uniform circuit family $\mathscr{C}_1$ for all inputs, promised that the two families are significantly different.

Problem: Let $\delta \in (0,1]$ and let $\mathscr{C}_0$ and $\mathscr{C}_1$ be two uniform families of quantum circuits. Given input quantum circuit C acting on n-qubit input space $\mathcal{H}$, let $C_0 \in \mathscr{C}_0$ and $C_1 \in \mathscr{C}_1$ act on the same input space $\mathcal{H}$. The problem is,
determine whether:

(yes case) $\exists$ subspace S, with $\dim S \geqslant (\dim \mathcal{H})^{1-\delta}$, such that for any reference space $\mathcal{R}$, if ρ is a density matrix on $S \otimes \mathcal{R}$ then $\|(C \otimes \mathbb{1}_{\mathcal{R}})(\rho) - (C_0 \otimes \mathbb{1}_{\mathcal{R}})(\rho)\|_{tr} \leqslant \epsilon$

(no case) for any reference space $\mathcal{R}$, if ρ is a density matrix on the full space $\mathcal{H} \otimes \mathcal{R}$ then $\|(C \otimes \mathbb{1}_{\mathcal{R}})(\rho) - (C_1 \otimes \mathbb{1}_{\mathcal{R}})(\rho)\|_{tr} \leqslant \epsilon$,

promised one of these to be the case,
where $1 > \epsilon \geqslant 2^{-\mathrm{poly}(n)}$. Note that the promise actually imposes a condition on the allowable $\mathscr{C}_0$ and $\mathscr{C}_1$, forcing them to be significantly different.

Theorem: QMA-hard for constant δ [proven by Rosgen [29]]
Hardness reduction from: QCSAT (V-1)

Notes: leads to: MIXED-STATE NON-IDENTITY CHECK (V-4), NON-ISOMETRY TESTING (V-5), DETECTING INSECURE QUANTUM ENCRYPTION(V-6)

C Diagram of QMA-complete problems

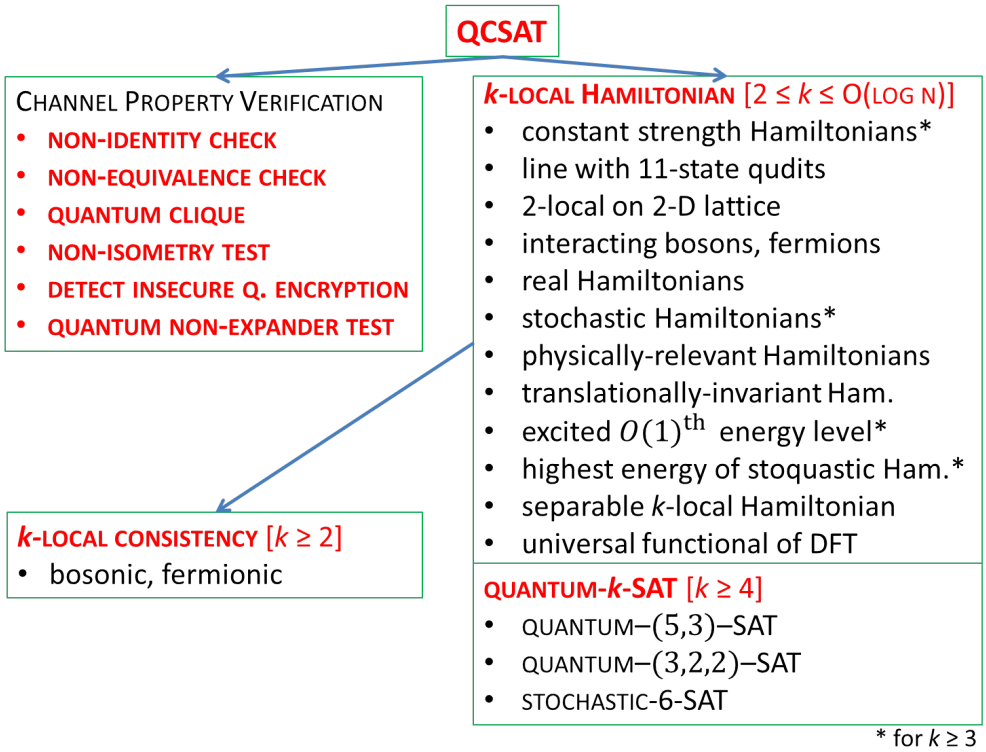

Figure 1: Schematic showing the QMA-complete problems listed in this paper, according to their categories. Lines show hardness reductions.

References

[1] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe, *The power of quantum systems on a line*, Communications in Mathematical Physics 287(1), pp.41-65, 2009; http://dx.doi.org/10.1007/s00220-008-0710-3

[2] F. Barahona, *On the computational complexity of Ising spin glass models*, J. Phys. A: Math and Gen., 15(10), 3241, 1982; http://dx.doi.org/10.1088/0305-4470/15/10/028

[3] S. Beigi and P. W. Shor, *On the complexity of computing zero-error and Holevo capacity of quantum channels*, 2007; http://arxiv.org/abs/0709.2090

[4] J. D. Biamonte and P. J. Love, *Realizable Hamiltonians for universal adiabatic quantum computers*, Phys.Rev.A, 78(1), 012352, 2008, http://link.aps.org/doi/10.1103/PhysRevA.78.012352

[5] A. Bookatz, S. Jordan, Y.-K. Liu, and P. Wocjan, *Testing quantum expanders is co-QMA-complete*, 2012; http://arxiv.org/abs/1210.0787

[6] S. Bravyi, *Efficient algorithm for a quantum analogue of 2-SAT*, 2006; http://arxiv.org/abs/quant-ph/0602108.

[7] S. Bravyi, D. DiVincenzo, R. Oliveira, and B. M. Terhal, *The complexity of stoquastic local Hamiltonian problems*, Quant. Inf. Comp. 8(5), pp. 0361-0385, 2008; http://arxiv.org/abs/quant-ph/0606140

[8] S. Bravyi and B. Terhal, *Complexity of stoquastic frustration-free Hamiltonians*, SIAM J. Comput. 39(4), p. 1462, 2009; http://dx.doi.org/10.1137/08072689X

[9] A. Chailloux and O. Sattath, *The complexity of the separable Hamiltonian problem*, 2012 IEEE 27th Annual Conference on Computational Complexity, pp.32-41, 2012; http://dx.doi.org/10.1109/CCC.2012.42

[10] L. Eldar and O. Regev, *Quantum SAT for a qutrit-cinquit pair is QMA_1-complete*, Proceedings of the 35th International Colloquium on Automata,Languages and Programming, pp. 881-892, 2008; http://dx.doi.org/10.1007/978-3-540-70575-8_72

[11] R. P. Feynman, *Quantum mechanical computers*, Found. Phys., 16, pp. 507-531, 1986; originally published in Optics News (February 1985), pp. 11-20; http://dx.doi.org/10.1007/BF01886518

[12] S. Gharibian and J. Kempe, *Approximation algorithms for QMA-complete problems*, SIAM J. Comput., 41(4), pp. 1028-1050, 2012; http://epubs.siam.org/doi/pdf/10.1137/110842272

[13] D. Janzing, P. Wocjan, and T. Beth, *Non-identity check is QMA-complete*, International Journal of Quantum Information, 3(3), pp. 463–473, 2005; http://www.worldscientific.com/doi/abs/10.1142/S0219749905001067

[14] Z. Ji and X. Wu, *Non-identity check remains QMA-complete for short circuits*, Proc. Asian Conference on Quantum Information Science, 2009; http://arxiv.org/abs/0906.5416

[15] S. P. Jordan, D. G. Gosset, and P. J. Love, *Quantum-Merlin-Arthurcomplete problems for stoquastic Hamiltonians and Markov matrices*, Phys. Rev. A 81(3), 032331, 2010; http://link.aps.org/doi/10.1103/PhysRevA.81.032331

[16] A. Kay, *Quantum-Merlin-Arthur-complete translationally invariant Hamiltonian problem and the complexity of finding ground-state energies in physical systems*, Phys. Rev. A, 76(3), 030307, 2007; http://link.aps.org/doi/10.1103/PhysRevA.76.030307

[17] A. Kay, *The computational power of symmetric Hamiltonians*, Phys. Rev. A, 78(1), 012346, 2008; http://link.aps.org/doi/10.1103/PhysRevA.78.012346

[18] A. Kay, *Role of rotational invariance in the properties of Hamiltonians*, Phys. Rev. A, 80(4), 040301, 2009; http://link.aps.org/doi/10.1103/PhysRevA.80.040301

[19] J. Kempe, A. Kitaev, and O. Regev, *The complexity of the local Hamiltonian problem*, SIAM J. Comput., 35(5), pp. 1070-1097, 2006; http://epubs.siam.org/doi/pdf/10.1137/S0097539704445226

[20] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and quantum computation*, Graduate Studies in Mathematics, Vol. 47 (AMS, Providence, RI), 2002.

[21] E. Knill, *Quantum randomness and nondeterminism*, 1996; http://arxiv.org/abs/quant-ph/9610012

[22] Y.-K. Liu, *Consistency of local density matrices is QMA-complete*, Proc. 10th International Workshop on Randomization and Computation, RANDOM 2006, Lecture Notes in Computer Science 4110, pp. 438-449, 2006; http://dx.doi.org/10.1007/11830924_40

[23] Y.-K. Liu, M. Christandl, and F. Verstraete, *Quantum computational complexity of the N-representability problem: QMA complete*, Phys. Rev. Lett. 98, 110503, 2007; http://link.aps.org/doi/10.1103/PhysRevLett.98.110503

[24] C. Marriott and J. Watrous, *Quantum Arthur-Merlin games*, Computational Complexity, 14(2), 122152, 2005; http://dx.doi.org/10.1007/s00037-005-0194-x

[25] D. Nagaj, *Local Hamiltonians in quantum computation*, Ph.D. Thesis, MIT, 2008; http://arxiv.org/abs/0808.2117

[26] D. Nagaj and S. Mozes, *A new construction for a QMA-complete 3-local Hamiltonian*, J. Math. Phys. 48, 072104, 2007, http://dx.doi.org/10.1063/1.2748377

[27] R. Oliveira and B. Terhal, *The complexity of quantum spin systems on a two-dimensional square lattice*. Quant. Inf. Comp. 8(10), 09000924, 2008; http://arxiv.org/abs/quant-ph/0504050

[28] B. Rosgen, *Testing non-isometry is QMA-complete*, Theory of Quantum Computation, Communication, and Cryptography, pp63-76, 2011; http://dx.doi.org/10.1007/978-3-642-18073-6_6

[29] B. Rosgen, *Testing quantum circuits and detecting insecure encryption*, 2011; http://arxiv.org/abs/1108.1052

[30] N. Schuch and F. Verstraete, *Computational complexity of interacting electrons and fundamental limitations of density functional theory*, Nature Physics, 5, pp. 732–735, 2009; http://arxiv.org/pdf/0712.0483

[31] K. G. H. Vollbrecht and J. I. Cirac, *Quantum Simulators, Continuous-Time Automata, and Translationally Invariant Systems*, Phys. Rev. Lett. 100(1), 010501, 2008; http://link.aps.org/doi/10.1103/PhysRevLett.100.010501

[32] J. Watrous, *Succinct quantum proof for properties of finite groups*, Proc. 41st Foundations on Computer Science, pp. 537–546, 2000; http://dx.doi.org/10.1109/SFCS.2000.892141

[33] T.-C. Wei, M. Mosca, and A. Nayak, *Interacting Boson problems can be QMA hard*, Phys. Rev. Lett., 104, 040501, 2010; http://link.aps.org/doi/10.1103/PhysRevLett.104.040501

[34] J. D. Whitfield, P. J. Love, and A. Aspuru-Guzik, *Computational complexity in electronic structure*, 2012; http://arxiv.org/abs/1208.3334