

ARTICLE OPEN

Hamiltonian simulation with optimal sample complexity

Shelby Kimmel¹, Cedric Yen-Yu Lin¹, Guang Hao Low², Maris Ozols³ and Theodore J. Yoder²

We investigate the sample complexity of Hamiltonian simulation: how many copies of an unknown quantum state are required to simulate a Hamiltonian encoded by the density matrix of that state? We show that the procedure proposed by Lloyd, Mohseni, and Reberntrost [*Nat. Phys.*, 10(9):631–633, 2014] is optimal for this task. We further extend their method to the case of multiple input states, showing how to simulate any Hermitian polynomial of the states provided. As applications, we derive optimal algorithms for commutator simulation and orthogonality testing, and we give a protocol for creating a coherent superposition of pure states, when given sample access to those states. We also show that this sample-based Hamiltonian simulation can be used as the basis of a universal model of quantum computation that requires only partial swap operations and simple single-qubit states.

npj Quantum Information (2017)3:13; doi:10.1038/s41534-017-0013-7

INTRODUCTION

Much work has been done on the *time* and *query* complexity of Hamiltonian simulation when given a classical description or black box description of the Hamiltonian. Lloyd provided the first formal results on simulation, considering Hamiltonians that consist of sums of non-commuting terms.¹ Other lines of research have focused on simulating sparse Hamiltonians, with a long sequence of work recently culminating in an optimal algorithm² (see ref. 3 for a more complete history of work in this field).

In this work, we approach the problem of Hamiltonian simulation from a slightly different perspective. Rather than given a classical description or black-box access to a Hamiltonian H , we consider the problem of simulating H when given many copies of a quantum state ρ that encodes the Hamiltonian to be simulated. In particular, we assume that

$$\rho = \frac{H + c\mathbb{1}}{\text{Tr}(H + c\mathbb{1})} \quad (1)$$

for some constant $c \in \mathbb{R}$ such that $H + c\mathbb{1}$ is positive semidefinite and nonzero. In that case, ρ itself is positive semidefinite and $\text{Tr}\rho = 1$, so ρ is a valid density matrix. Note that the Hamiltonian dynamics of H and ρ are equivalent up to an overall phase and time scaling. Moreover, since the Hamiltonian H in Eq. (1) can be arbitrary, any unitary can in fact be expressed as $e^{-i\rho t}$ for an appropriately chosen state ρ and time t .

This modified version of the original Hamiltonian simulation problem is what we call *sample-based* Hamiltonian simulation: given one copy of an unknown state σ and n copies of an unknown state ρ , implement the following map:

$$\sigma \otimes \underbrace{\rho \otimes \rho \cdots \otimes \rho}_n \mapsto e^{-i\rho t} \sigma e^{i\rho t} \quad (2)$$

where t is the desired evolution time. We also allow for some error in the final state—we denote by δ the *trace distance*⁴ between the state that is output by the protocol and the ideal state $e^{-i\rho t} \sigma e^{i\rho t}$. This problem was first considered in ref. 5, where the authors give

a simple protocol, which we call the *LMR protocol* (LMR comes from the author's initials: Lloyd, Mohseni, and Reberntrost), for approximately implementing the unitary $e^{-i\rho t}$ using many copies of ρ . Their protocol is based on a *partial swap* operation that can also be considered as a finite-dimensional analog of a beam-splitter.⁶ An interesting feature of the LMR protocol is that it is agnostic with regard to ρ . In the spirit of^{7, 8} this suggests interpreting ρ as a “quantum software state”.

The main motivation for sample-based Hamiltonian simulation in ref. 5 is to perform principal component analysis of ρ . They do this by performing phase estimation on the unitary $e^{-i\rho}$. (We note in Supplementary Information Section C that a slightly more careful analysis gives a polynomial improvement in sample complexity over the complexity given in ref. 5 for performing phase estimation, which is a subroutine for principal component analysis). The LMR protocol has applications to many problems in machine learning, e.g., refs 5, 9–11.

In this paper, we ask the following question: given t and δ , what is the minimum n (number of copies of ρ) necessary to implement the unitary $e^{-i\rho t}$ on an unknown state σ to trace distance at most δ ? We call this the *sample complexity* of Hamiltonian simulation.

While the LMR protocol acts with each copy of ρ sequentially, perhaps one could achieve better performance by acting with a global operation?¹² For example, recent near-optimal tomographic protocols have relied on performing global operations (like the Schur transform) on many copies of the unknown state.^{13, 14} Along those lines, perhaps one could do better than LMR by applying tomographic protocols to get an estimate $\hat{\rho}$ of ρ from the n copies of ρ , and then evolve according to $e^{-i\hat{\rho} t}$.

On the contrary, however, we show that LMR performs asymptotically *better* than any tomographic strategy (‘LMR protocol vs. state tomography’), and performs sample-based Hamiltonian simulation with asymptotic optimality in both t and δ simultaneously (‘LMR protocol is optimal’). We additionally show LMR is optimal in δ when restricting to pure states, and provide a sample-optimal algorithm for a variant of Grover’s search. In

¹Joint Center for Quantum Information and Computer Science (QulCS), University of Maryland, College Park, MD 20742, USA; ²Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA and ³Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, UK
Correspondence: Shelby Kimmel (shelbyk@umd.edu)

Received: 9 September 2016 Revised: 25 January 2017 Accepted: 18 February 2017

Published online: 30 March 2017

'Generalized LMR for simulation of Hermitian polynomials', we discuss the sample complexity of more complex Hamiltonians that depend on multiple states. For example, we show how to simulate the Hamiltonians given by any Hermitian polynomial (i.e. any element of the Jordan–Lie algebra¹⁵) generated by states ρ_1, \dots, ρ_K to which we are given sample access. As applications of this result, we show how to simulate the commutator $i[\rho_1, \rho_2]$ and anticommutator $\{\rho_1, \rho_2\}$ of two states ρ_1 and ρ_2 , and how to simulate any real linear combination of states ρ_1, \dots, ρ_K when given access to many copies of those states. We prove the optimality of the commutator, anticommutator, and linear combinations protocols. In 'Applications of commutator simulation', we give applications of commutator simulation to orthogonality testing and quantum state addition. In 'Universality of LMR', we show how to use sample-based Hamiltonian simulation to implement a universal model of quantum computation using only partial swaps and a stream of input qubits initialized in $|0\rangle$ and $|+\rangle$.

In 'Discussion', we discuss the results and suggest open problems. Finally, in 'Methods' we give proofs for two of the main results in the paper: the lower bound on the LMR protocol, and the protocol for simulating Hamiltonians given by Hermitian polynomials of the input states.

Notation

We use \mathcal{H} to denote a finite-dimensional Hilbert space, and $D(\mathcal{H})$ to represent the set of positive semi-definite operators with trace 1 on \mathcal{H} (i.e. the set of valid quantum states).

The *trace distance* between $\rho, \sigma \in D(\mathcal{H})$ is given by $\frac{1}{2} \|\rho - \sigma\|_1$, where $\|A\|_1 := \text{Tr}(\sqrt{AA^\dagger})$. The trace distance between ρ and σ gives the maximum difference in probability of any measurement on the two states.⁴ For two quantum channels \mathcal{E}_1 and \mathcal{E}_2 that act on $D(\mathcal{H})$, their *trace norm distance* is defined as

$$\frac{1}{2} \|\mathcal{E}_1 - \mathcal{E}_2\|_{\text{tr}} := \frac{1}{2} \max_{\rho \in D(\mathcal{H})} \|\mathcal{E}_1(\rho) - \mathcal{E}_2(\rho)\|_1 \quad (3)$$

The *diamond norm distance* is defined as

$$\frac{1}{2} \|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond} := \frac{1}{2} \max_{k, \rho \in D(\mathcal{H} \otimes \mathcal{H}_k)} \|(\mathcal{E}_1 \otimes \mathcal{I})(\rho) - (\mathcal{E}_2 \otimes \mathcal{I})(\rho)\|_1 \quad (4)$$

where \mathcal{I} is the identity channel on a k -dimensional space \mathcal{H}_k . Note $\|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond} \geq \|\mathcal{E}_1 - \mathcal{E}_2\|_{\text{tr}}$.

We use $\mathbb{1}_A$ to mean the identity matrix acting on subsystem A , but if clear from context, we will drop the subscript. We use $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ and denote single-qubit Pauli operators as X, Y , and Z .

RESULTS

LMR protocol vs. state tomography

Lloyd, Mohseni, and Rebentrost⁵ gave a simple method for approximating the transformation in Eq. (2). The number of copies of ρ required by their procedure is not only independent of σ and ρ , but is independent of the dimension and rank of ρ . We state their result in a slightly more general form, where σ has two registers and $e^{-i\rho t}$ is applied only to one of them.

Theorem 1 (ref. 5). *Let $\rho \in D(\mathcal{H}_A)$ and $\sigma \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ be two unknown quantum states and $t \in \mathbb{R}$ (can be either positive or negative). Then there exists a quantum algorithm that transforms $\sigma_{AB} \otimes \rho_{A_1} \otimes \dots \otimes \rho_{A_n}$ into $\tilde{\sigma}_{AB}$ such that*

$$\frac{1}{2} \|(e^{-i\rho_A t} \otimes \mathbb{1}_B) \sigma_{AB} (e^{i\rho_A t} \otimes \mathbb{1}_B) - \tilde{\sigma}_{AB}\|_1 \leq \delta, \quad (5)$$

as long as the number of copies of ρ is $n = O(t^2/\delta)$. In other words, this quantum algorithm implements the unitary $e^{-i\rho t}$ up to error δ in the diamond norm, using $O(t^2/\delta)$ copies of ρ .

We will give a sketch of the proof because many of our more general simulation techniques build on their ideas; for the full proof see Supplementary Information Section A. For simplicity we assume ρ and σ have the same dimension. Using a Taylor series expansion, the target state is

$$e^{-i\rho t} \sigma e^{i\rho t} = \sigma - i[\rho, \sigma]t - \frac{1}{2!}[\rho, [\rho, \sigma]]t^2 + \dots \quad (6)$$

We note that for very small evolution times Δ , we have the following direct calculation:

$$\begin{aligned} \text{Tr}_2[e^{-iS\Delta}(\sigma \otimes \rho)e^{iS\Delta}] &= \sigma - i[\rho, \sigma]\Delta + O(\Delta^2) \\ &= e^{-i\rho\Delta}\sigma e^{i\rho\Delta} + O(\Delta^2), \end{aligned} \quad (7)$$

where by Tr_i we mean taking the partial trace of the i th subsystem, and S is the swap operator between the two registers. If we take $\Delta = \delta/t$ and repeat this procedure $O(t^2/\delta)$ times, we end up implementing the operator $e^{-i\rho t}$ up to error $O(\Delta^2 \cdot t^2/\delta) = O(\delta)$.

Thus the LMR protocol uses $O(t^2/\delta)$ copies of ρ to implement the unitary $e^{-i\rho t}$ up to error δ in trace norm. (While not noted explicitly in ref. 5, the LMR protocol can be implemented efficiently, i.e. using $O(\log D \cdot t^2/\delta)$ single-qubit and Fredkin (controlled-swap) gates, where $D = \dim(\mathcal{H}_A)$, by applying the linear combination of unitaries algorithm (see, e.g., ref. 3 or ref. 16, Theorem 2.4). For more information, see Supplementary Information Section A). To obtain the result for the diamond norm, simply replace σ by σ_{AB} and perform the partial swap operation $e^{-iS\Delta}$ only between the A registers of σ_{AB} and ρ_A , and then discard the last register that was originally holding ρ_A .

Additionally, the LMR protocol can be modified to implement the controlled- $e^{-i\rho t}$ operation, which will be important if one wants to implement phase estimation on $e^{-i\rho t}$. A method for implementing controlled- $e^{-i\rho t}$ is stated without proof in ref. 5; we prove this method works and provide an additional approach in the Supplementary Information Section A.1.

An alternative method to LMR for sample-based Hamiltonian simulation would be to perform tomography on the copies of ρ to get an estimate $\hat{\rho}$ of ρ , and then implement $e^{-i\hat{\rho}t}$. In Supplementary Information Section B, we show that the number of samples needed if using this strategy is

$$n = \Omega\left(\frac{Cdr(t - \delta)^2 + t^2}{\delta^2 \log(dt/r\delta)} + \frac{t^2}{\delta^2}\right), \quad (9)$$

where d is the dimension of ρ , r is the rank of ρ , and t and δ are as in Theorem 1.

Comparing with Theorem 1, since LMR does not have any dependence on d or r , we immediately see that for large d or r , LMR does significantly better. Furthermore, even fixing d and r , we see that LMR provides a square-root improvement in sample complexity over tomography in terms of δ .

LMR protocol is optimal

To prove the LMR protocol is in fact asymptotically optimal, we first give a lower bound on the sample complexity of distinguishing two specific states. Next, we assume we have a protocol that simulates $e^{-i\rho t}$ to trace norm (which is a weaker assumption than using diamond norm) δ using $f(t, \delta)$ samples of ρ for some function f . Then we show that using such a protocol one can distinguish these two states. However, if $f = o(t^2/\delta)$, we would violate our lower bound on state discrimination.

Theorem 2 *Let $f(t, \delta)$ be the number of copies of ρ required to implement the unitary $e^{-i\rho t}$ up to error δ in trace norm. Then as long as $\delta \leq 1/6$ and $\delta/t \leq 1/(6\pi)$, it holds that $f(t, \delta) = \Theta(t^2/\delta)$.*

The proof of Theorem 2 can be found in 'Discussion'. The proof uses mixed states, so it could be possible that simulating

$\exp(-i|\psi\rangle\langle\psi|t)$ for a pure state $|\psi\rangle$ could be done more efficiently. This relates to a practically relevant question, namely, the fact that the LMR protocol and certain pure states as resources create a universal model for quantum computation (see ‘Universality of LMR’). However, we can show that LMR is also optimal for pure states in the δ error parameter. We cannot expect to prove a meaningful lower bound on the t dependence in pure state LMR. The reason is that, given any state ρ and promised that $\exp(-i\rho t)$ is periodic with period T (i.e. $\exp(-i\rho t_1) = \exp(-i\rho t_2)$ for any $t_2 = t_1 + kT$ for integer k and real number T), we can always simulate the Hamiltonian ρ for an equivalent time $t' \in [0, T)$ instead. Therefore asymptotic scaling in terms of large t is meaningless. For pure states, we immediately know the period, namely 2π .

To prove that the LMR protocol is optimal for pure states, we employ variants of Grover’s search. While Grover’s search¹⁷ is a well-known quantum mechanical task, it is not often stated in its form as a decision problem, and very rarely¹⁸ as a metrological decision problem, where the inputs are unitaries and the output depends on a property that those unitaries either possess or do not possess. This guise is useful for our purposes, however, because the LMR protocol allows us to turn metrology problems on states into metrology problems on quantum operations.

In the metrological view, Grover’s search, or perhaps more precisely amplitude amplification,¹⁹ is the following problem of parameter estimation. Let \mathcal{T} be a subspace of \mathbb{C}^{2^q} . We call \mathcal{T} the *target subspace*. Let $\mathcal{U}_{\mathcal{T}}$ be a unitary acting on $q + 1$ qubits such that

$$\mathcal{U}_{\mathcal{T}}|\phi\rangle|0\rangle = \begin{cases} |\phi\rangle|1\rangle, & \text{if } |\phi\rangle \in \mathcal{T}, \\ |\phi\rangle|0\rangle, & \text{if } |\phi\rangle \perp \mathcal{T}. \end{cases} \quad (10)$$

In this problem, and in the following variations, we will assume access to $\mathcal{U}_{\mathcal{T}}$ and $\mathcal{U}_{\mathcal{T}}^\dagger$ are free. For a q -qubit unitary V , define

$$\lambda := |(\mathbb{1} \otimes \langle 1|) \mathcal{U}_{\mathcal{T}}(V|0\rangle^{\otimes q} \otimes |0\rangle)|^2. \quad (11)$$

Then in Grover’s search, the task is to decide whether $\lambda \geq w$ (for $w > 0$) or $\lambda = 0$, while using V and V^\dagger as few times as possible. In other words, if we call $|s\rangle := V|0\rangle^{\otimes q}$ the start state, we would like to determine whether the start state has substantial probability mass in the target subspace or none, promised one is the case. If we solve this problem using Grover’s search and count the number of uses of V and V^\dagger required to succeed with probability $1 - \varepsilon$, we get the standard complexity $\Theta(\log(1/\varepsilon)/\sqrt{w})$.^{20, 21}

One simple modification of metrological Grover’s search is to replace the circuit description of V with copies of the start state $|s\rangle$ instead. The problem is now to determine whether $\lambda := |(\mathbb{1} \otimes \langle 1|) \mathcal{U}_{\mathcal{T}}|s\rangle \otimes |0\rangle|^2$ is at least $w > 0$ or equal to zero, promised one is the case, given copies of $|s\rangle$ and unlimited access to $\mathcal{U}_{\mathcal{T}}$ and $\mathcal{U}_{\mathcal{T}}^\dagger$. We call this *sample-based Grover’s search*.

A second variant of metrological Grover’s search is to replace both V and $\mathcal{U}_{\mathcal{T}}$ with quantum states. In this form, the problem becomes: given copies of q -qubit states $|s\rangle$ and $|t\rangle$, determine whether $\lambda = |\langle s|t\rangle|^2$ is at least $w > 0$ or equal to zero, promised one is the case. We call this variant *orthogonality testing*. We address optimal orthogonality testing in ‘Applications of commutator simulation’.

In Supplementary Information Section D.2, we first prove that for sample-based Grover’s search, we lose the square-root advantage of the regular Grover’s search:

Lemma 3 *Sample-based Grover’s search with success probability $1 - \varepsilon$ uses $\Theta(\log(1/\varepsilon)/w)$ copies of $|s\rangle$.*

Using this result, we prove:

Theorem 4 *The number of copies of an unknown pure state ρ required for any algorithm to simulate $e^{-i\rho t}$ to trace norm δ is $\Omega(1/\delta)$.*

The main idea of the proof, which can be found in Supplementary Information Section D.2, is that the reflections V and V^\dagger needed for Grover’s algorithm can be implemented by sample-based Hamiltonian simulation using many copies of the state $|s\rangle$. This gives us a way to reduce sample-based Grover’s search to sample-based Hamiltonian simulation. Then we apply the lower bound of Lemma 3.

Generalized LMR for simulation of Hermitian polynomials

We show sample-based Hamiltonian simulation of Eq. (2) can be further generalized. Instead of evolution of σ by a single state ρ , the target Hamiltonian H could be encoded by some combination of multiple states $\rho_1, \rho_2, \dots, \rho_K$. For example, we might want to implement the map

$$\sigma \otimes \bigotimes_{j=1}^K \rho_j^{\otimes n_j} \mapsto e^{-if(\rho_1, \rho_2, \dots, \rho_K)t} \sigma e^{if(\rho_1, \rho_2, \dots, \rho_K)t}, \quad (12)$$

where $H = f(\rho_1, \rho_2, \dots, \rho_K)$ is some Hermitian polynomial function of the input states. In fact, we prove it is possible to simulate arbitrary Hermitian multinomial functions:

Theorem 5 *Let $\rho_1, \dots, \rho_K \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be unknown quantum states, and let*

$$H = \sum_{r \in R} c_r H_r, \quad H_r = \frac{1}{2} (e^{i\phi_r} \rho_{r_1} \rho_{r_2} \cdots \rho_{r_{|r|}} + e^{-i\phi_r} \rho_{r_{|r|}} \rho_{r_{|r|-1}} \cdots \rho_{r_1}) \quad (13)$$

be a Hermitian polynomial in ρ_1, \dots, ρ_K , where R is a finite set of strings over the alphabet $\{1, 2, \dots, K\}$. Using n samples from the states $\{\rho_1, \dots, \rho_K\}$, a quantum algorithm can transform σ_{AB} into $\tilde{\sigma}_{AB}$ such that

$$\frac{1}{2} \| (e^{-iHt} \otimes \mathbb{1}_B) \sigma_{AB} (e^{iHt} \otimes \mathbb{1}_B) - \tilde{\sigma}_{AB} \|_1 \leq O(\delta), \quad (14)$$

if $n = O(Lc^2t^2/\delta)$ where $c := \sum_{r \in R} |c_r|$ and $L := \max_{r \in R} |r|$ is the multinomial degree of H . Moreover, on average, the number of copies of ρ_j consumed is $n_j = O(K_j c^2 t^2 / \delta)$ where $K_j = \sum_{r \in R} \mathbb{1}_{\{j \in r\}} |c_r| / c$, and $\mathbb{1}_{\{j \in r\}} = \mathbb{1}_{\{s: r_s = j\}}$.

As corollaries of Theorem 5, we have the following simulation results for linear combinations of states (Corollary 6) and for the commutator and anticommutator of two states (Corollary 7):

Corollary 6 *Let $\rho_1, \dots, \rho_K \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be unknown quantum states, and let $c_1, \dots, c_K \in \mathbb{R}$. Using n samples from the states $\{\rho_1, \dots, \rho_K\}$, a quantum algorithm can transform σ_{AB} into $\tilde{\sigma}_{AB}$ such that*

$$\frac{1}{2} \| (e^{-iHt} \otimes \mathbb{1}_B) \sigma_{AB} (e^{iHt} \otimes \mathbb{1}_B) - \tilde{\sigma}_{AB} \|_1 \leq O(\delta), \quad H = \sum_{j=1}^K c_j \rho_j, \quad (15)$$

if $n = O(c^2 t^2 / \delta)$ where $c := \sum_{j=1}^K |c_j|$. Moreover, on average, the number of copies of ρ_j consumed is $n_j = O(|c_j| c t^2 / \delta)$.

Corollary 7 *Let $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be unknown quantum states, and $\phi \in [0, 2\pi)$. Using n samples each of ρ_1 and ρ_2 , a quantum algorithm can transform σ_{AB} into $\tilde{\sigma}_{AB}$ such that*

$$\frac{1}{2} \| (e^{-iHt} \otimes \mathbb{1}_B) \sigma_{AB} (e^{iHt} \otimes \mathbb{1}_B) - \tilde{\sigma}_{AB} \|_\diamond \leq O(\delta), \quad (16)$$

$$H = \frac{1}{2} (e^{i\phi} \rho_1 \rho_2 + e^{-i\phi} \rho_2 \rho_1),$$

if $n = O(t^2 / \delta)$

Note from Eq. (16) that

$$H = \frac{1}{2} \cos(\phi) \{\rho_1, \rho_2\} + \frac{1}{2} \sin(\phi) i[\rho_1, \rho_2], \quad (17)$$

so by choosing $\phi = 0$, we recover the anticommutator Hamiltonian $\{\rho_1, \rho_2\}/2$, and choosing $\phi = \pi/2$ we recover the commutator Hamiltonian $i[\rho_1, \rho_2]/2$.

Furthermore, Corollary 6 and Corollary 7 are both optimal:

Theorem 8 Let $\{c_1, \dots, c_K\}$ be a set of K real numbers. Then there exist ρ_1, \dots, ρ_K such that to simulate $H = \sum_{j=1}^K c_j \rho_j$ for time t and to error δ in trace norm requires $\Omega(c^2 t^2 / \delta)$ copies of states in $\{\rho_1, \dots, \rho_K\}$, where $c := \sum_j |c_j|$, as long as δ and $\delta/(ct)$ are smaller than some constants.

Theorem 9 To simulate $H = i[\rho_1, \rho_2]$ for time t and to trace norm error δ requires $\Omega(t^2/\delta)$ copies each of the states ρ_1 and ρ_2 , as long as δ and δ/t are smaller than some constants.

While Theorem 9 only applies to commutators, it is easy to see that the simulation from Corollary 7 of the anticommutator $\{\rho_1, \rho_2\}$ has optimal scaling in t and δ , because in the qubit case, we can always choose $\rho_2 = \mathbb{1}/2$ so that $\{\rho_1, \rho_2\} = \rho_1$ and we can apply the lower bound from Theorem 2. The proofs for results in this section can be found in Supplementary Information Section D.3.

Applications of commutator simulation

We now describe how one can use commutator simulation to perform tasks such as orthogonality testing and coherent addition of two pure states.

We first give a protocol for coherent state addition: given many copies of unknown pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, the task is to obtain a state of the form

$$a|\psi_1\rangle + b|\psi_2\rangle \quad (18)$$

for some $a, b \in \mathbb{R}$. Note that the target state is sensitive to the global phases of the two input states—in particular, the relative phase between $|\psi_1\rangle$ and $|\psi_2\rangle$ —which have no physical meaning. To make the task well-defined, we instead demand the target state to be of the form

$$a|\psi_1\rangle + b \frac{\langle \psi_2 | \psi_1 \rangle}{\langle \psi_2 | \psi_1 \rangle} |\psi_2\rangle \quad (19)$$

for some $a, b \in \mathbb{R}$, which is unique (up to a global phase) even when the global phases of the two input states have not been specified. Note that we can always recover Eq. (18) from Eq. (19) by fixing the global phases of the two input states appropriately (i.e. such that $\langle \psi_2 | \psi_1 \rangle > 0$).

Theorem 10 Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be unknown pure states of the same dimension. Promised that the angle between the two states is $\Delta := \arccos |\langle \psi_1 | \psi_2 \rangle|$ and $\Delta \notin \{0, \pi/2\}$, it is possible to create the state

$$|\psi(\chi)\rangle := \frac{1}{\sin \Delta} (\sin(\Delta - \chi) |\psi_1\rangle + e^{i\phi} \sin \chi |\psi_2\rangle) \quad (20)$$

to trace distance δ using $O(\frac{\chi^2}{\delta \sin^2 2\Delta})$ copies of $|\psi_1\rangle$ and $|\psi_2\rangle$, where $e^{i\phi} := \langle \psi_2 | \psi_1 \rangle / |\langle \psi_2 | \psi_1 \rangle|$ is an unimportant phase factor that can be ignored by appropriately adjusting the global phases of the two states.

A similar protocol has been independently discovered in ref. 22, Theorem 2, and recently implemented experimentally.²³ While our protocol involves only the two input states $|\psi_1\rangle$ and $|\psi_2\rangle$, the protocol of ref. 22 requires an additional reference state $|\chi\rangle$. Another difference between the two results is that we consume several copies of the input states to obtain an approximation of the target state, while²³ consume only a single copy but rely on a probabilistic postselection.

The proof of Theorem 10 (which can be found in Supplementary Information Section F) is based on commutator simulation and effectively implements a rotation in the two-dimensional subspace spanned by $|\psi_1\rangle$ and $|\psi_2\rangle$. Indeed, note from Eq. (20) that $|\psi(0)\rangle = |\psi_1\rangle$ and $|\psi(\Delta)\rangle = e^{i\phi} |\psi_2\rangle$, while intermediate values of χ produce states that interpolate between these two. (If one does not care about the relative phase $e^{i\phi}$, one can always exchange the two states and replace χ by $\Delta - \chi$, which would improve the complexity by a constant factor when $\chi > \Delta/2$). As a consequence, the target state in Eq. (19) has real coefficients a and b . One can also achieve complex coefficients using a more sophisticated Hamiltonian that includes terms proportional to $|\psi_1\rangle\langle\psi_1|$ and $|\psi_2\rangle\langle\psi_2|$, but we do not consider this case here for the sake of simplicity.

Our protocol requires a very large number of samples when the states $|\psi_1\rangle$ and $|\psi_2\rangle$ have either very small or very large overlap (i.e. in cases when $\sin^2 2\Delta$ is very small). This is because we use commutator simulation to effectively implement a rotation in the two-dimensional subspace spanned by $|\psi_1\rangle$ and $|\psi_2\rangle$, and in the special cases when $|\psi_1\rangle \perp |\psi_2\rangle$ or $|\psi_1\rangle = e^{i\phi} |\psi_2\rangle$ the commutator vanishes and hence our protocol fails (in the second case the task is trivial though).

Interestingly, by choosing $\chi = \Delta/2$ in Eq. (20) it is possible to coherently add two states, i.e. create a state proportional to $|\psi_1\rangle + |\psi_2\rangle$ (we are ignoring the relative phase between the two states). However, to determine Δ one needs to estimate the inner product between the two states, which can be done by running phase estimation on the commutator.

We note that the commutator of orthogonal states is zero, while the commutator of non-orthogonal states is non-zero (as long as the states are not identical). Using this fact, and by performing phase estimation on the unitary generated by the commutator of two pure states, we can create a test for orthogonality (for proof, see Supplementary Information Section F).

Theorem 11 Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be unknown pure states of the same dimension. Promised that either $|\langle \psi_1 | \psi_2 \rangle| = 0$ or $|\langle \psi_1 | \psi_2 \rangle| \geq w$, deciding which with probability $1 - \epsilon$ uses $\Theta(\log(1/\epsilon)/w)$ copies of $|\psi_1\rangle$ and $|\psi_2\rangle$.

Universality of LMR

In many solid-state implementations of quantum computers, such as quantum dots,²⁴ donor pairs,²⁵ and electron spins,²⁶ the Heisenberg exchange is the natural coupling interaction between qubits. More specifically, the Heisenberg interaction between qubits i and j is given by

$$H_{ij} := X^i \otimes X^j + Y^i \otimes Y^j + Z^i \otimes Z^j, \quad (21)$$

where X^i , Y^i , and Z^i are the Pauli matrices acting on qubit i . Up to an overall scaling, this is the same as the swap interaction S used in the LMR protocol, see Eq. (7). In the solid state systems mentioned above, the Heisenberg interaction typically can be turned on and off for pairs of qubits for any desired length of time, and the operations induced by these interactions are usually fast and reliable.

While it is beneficial to create computing models that take advantage of the Heisenberg exchange interaction, this interaction is not universal for spin-1/2 systems.²⁷ Several schemes have overcome this limitation by using encoded logical qubits and decoherence-free subsystems.^{28, 29}

In this section, we use the LMR protocol to design a universal model for quantum computation that does not use encoded qubits, but which requires only the Heisenberg interaction, as well as the ability to prepare the states $|0\rangle$ and $|+\rangle$ on a single qubit. Our scheme thus requires $n+1$ physical qubits to perform computations on n qubits, in contrast to encoded schemes, of



Fig. 1 Connectivity graph for qubits in our model. Each circle represents a qubit. Qubits connected by a solid line can have the Heisenberg interaction applied between them. The qubit q_* can be prepared in the state $|0\rangle$ or $|+\rangle$

which the simplest require 2 or 3 times the number of physical qubits.^{28, 29} Furthermore, there has been much research in the field of quantum dots on how to quickly and reliably prepare a fixed qubit state, e.g., in refs 30–33. These schemes could be applied to produce the single-qubit states $|0\rangle$ and $|+\rangle$ needed for our protocol.

We consider a connectivity graph of the qubits as in Fig. 1 (different connectivity graphs lead to different scalings depending on which costs you would like to optimize). We assume exchange interactions can be applied between connected qubits in the form of unitaries $\exp(-itH_{ij})$ for arbitrary t . The qubit q_* is where the states $|0\rangle$ and $|+\rangle$ are prepared.

Recall that arbitrary single-qubit gates combined with any entangling two-qubit gate is sufficient for universal quantum computation.³⁴ Since we do not have encoded qubits, the exchange interaction itself immediately gives us an entangling gate. Now for universal quantum computation we need to show how to perform arbitrary single-qubit gates.

Let $X_\phi := \exp[-i\theta X]$ and let $Z_\theta := \exp[-i\theta Z]$ for Pauli's X and Z . Then any single-qubit rotation can be written as $X_\phi Z_\theta X_\xi$ for some angles ϕ , θ , and ξ .⁴ Therefore, it is sufficient to show how to perform X and Z rotations.

If qubit i needs to have a single-qubit gate performed on it, using the Heisenberg interaction, we use swap gates to move that qubit to position 0 of Fig. 1. We now show how to perform Z_ϕ and X_θ on the qubit in position 0. Using LMR, given n copies of the state $|0\rangle$ input at qubit q_* , using only partial swap operations on qubits q_0 and q_* , (i.e. applying the Heisenberg interaction between qubits q_0 and q_*) we can apply the unitary

$$\exp(-i2\phi|0\rangle\langle 0|) = Z_\phi \quad (22)$$

(up to a global phase) to accuracy $O(n^{-1})$. Likewise, using the LMR protocol, given n copies of the state $|+\rangle$, using only partial swap interactions between qubits q_0 and q_* , we can apply the unitary

$$\exp(-i2\theta|+\rangle\langle +|) = X_\theta \quad (23)$$

(up to a global phase) to accuracy $O(n^{-1})$.

To apply an arbitrary single-qubit rotation to accuracy ϵ , we need $O(\epsilon^{-1})$ resource states $|0\rangle$ and $|+\rangle$ (this construction is reminiscent of ideas in ref. 35). Suppose that over the course of an algorithm, one must apply M single-qubit gates and M' CNOT gates. A CNOT gate requires a constant number of single-qubit gates as well as a constant number of partial swap gates.³⁴ Then to bound the error over the course of the algorithm, we require accuracy of $O((M+M')^{-1})$ for each single-qubit gate. Therefore, we require $O((M+M')^2)$ resource states $|0\rangle$ and $|+\rangle$ in total. Additionally, using the connectivity graph of Fig. 1, to move qubits into proximity with one another to perform any single-qubit or two-qubit gate requires $O(N)$ swap operations operations, where N is the number of qubits. Thus the total number of operations scales as $O(N(M+M')^2)$.

The states $|0\rangle$ and $|+\rangle$ need not be prepared perfectly for our protocol to work. For example, given depolarized versions of these states, we would need to increase the number of rounds in the LMR protocol by a constant factor. In fact, two arbitrary states (other than $|0\rangle$ and $|+\rangle$) could be used, as long as they are well characterized and not diagonal in the same basis.

Our model produces a polynomial (in particular squared) blow-up in the number of operations, which still allows for universal quantum computation. However, it would be impossible to obtain a speed-up for problems such as Grover's search. We hope it is a useful model for systems where the Heisenberg exchange is a

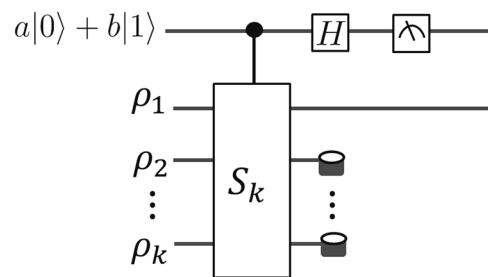


Fig. 2 The gadget to create $\rho^{(r)}$. Here S_k is the permutation of k registers given in Eq. (32), and the waste bins indicate the partial trace. The H -gate is a single-qubit Hadamard gate and measurement is in the Z -basis. In ref. 41 they use the same circuit, but use the measurement outcomes to perform spectrum estimation

natural operation. It may even be useful in non-solid state systems such as cold, trapped atoms, where it was shown that partial swaps could be implemented using Rydberg interactions or through coupling to a cavity.³⁶

DISCUSSION

We have shown that the LMR protocol is optimal for the problem of simulating unknown Hamiltonians encoded as quantum states. Moreover, the protocol and its generalizations also turn out to be optimal for a variety of other tasks, such as discriminating between pure states and Hamiltonian evolution under the commutators of unknown states. We hope that this study will motivate the discovery of other possible applications of this versatile protocol.

We have not shown the optimality of our protocol for simulating the evolution by the multinomials in Eq. (12). It would be interesting to investigate whether it is optimal, or whether better algorithms can be found.

Another interesting aspect is the role of ancilla qubits in our protocol. While the original LMR protocol for Hamiltonian simulation is based on partial swaps and hence does not require ancilla qubits, the use of ancillas seems to be essential in our more general simulation protocol (see Fig. 2 in 'Methods'). We wonder whether the use of ancillas is necessary in our protocol or, for example, whether it can instead be implemented using the continuous permutations introduced in ref. 12. These continuous permutations generalize the partial swap operation and do not require ancillas.

Another possible direction is to investigate distributed versions of our protocols in the context of multiparty communication. Reference 37 considers a protocol for simulating distributed unitaries over multiple remote parties using shared entanglement and a limited amount of quantum communication, and the techniques they use are reminiscent of those of the LMR protocol. It would be interesting to investigate the connections of ref. 37 with the protocols in our work.

Finally, the LMR protocol can be seen as allowing the encoding of the operation $e^{-i\rho t}$ into multiple copies of a quantum state ρ . As discussed in 'LMR protocol vs. state tomography', having access to $O(t^2/\delta)$ copies of ρ allows a user to perform the operation $e^{-i\rho t}$, but may be insufficient for the user to determine what ρ is through tomography. It is an intriguing question whether other quantum operations could be encoded into states in this way, so that a user could perform the quantum operation but learn little else about

what operation is being performed. This could be seen as a form of quantum copy-protection.³⁸ See ref. 39 for some progress in this direction, and ref. 40 for negative results when the encoding is required to be a circuit and not a state.

METHODS

In this section, we give proofs for two of the main results in the paper: Theorem 2 (optimality of the LMR protocol), and Theorem 5 (the protocol for simulating arbitrary Hermitian polynomials of the input states). Many of the other proofs in this paper are similar, and can be found in the [Supplementary Information](#).

Proof of Theorem 2 The upper bound holds by the LMR protocol, Theorem 1, so we will only prove the lower bound. The fact that the trace norm lower bounds the diamond norm makes a tight lower bound in terms of the trace norm a stronger result than if we had used the diamond norm. Let

$$\rho(x) := x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1| = \frac{1}{2}1 + \left(x - \frac{1}{2}\right)Z. \quad (24)$$

Then, given many copies of an unknown state ρ , suppose we want to distinguish between the cases $\rho_1 := \rho(1/2)$ and $\rho_2 := \rho(\frac{1}{2} + \epsilon)$, with $0 < \epsilon \leq 1/2$, promised ρ is one of the two. One way of doing this is to consider the single-qubit unitary operator $\mathcal{U}(\rho, t) := \exp(-ipt)$. Then for $t_\epsilon := \pi/(2\epsilon)$ the operators $\mathcal{U}(\rho_i, t_\epsilon)$ become orthogonal, namely,

$$\mathcal{U}(\rho_1, t_\epsilon) \propto \mathbb{1}, \quad \mathcal{U}(\rho_2, t_\epsilon) \propto Z, \quad (25)$$

where \propto indicates that we have hidden an unimportant phase factor. Consequently, applying $\mathcal{U}(\rho, t)$ to $|+\rangle$ and measuring in the X -basis will distinguish ρ_1 from ρ_2 with certainty. Thus, we can distinguish between $\rho = \rho_1$ or $\rho = \rho_2$ with probability at least $2/3$ using no more than $f(t_\epsilon, 1/3)$ copies of ρ by implementing a map that differs from $\mathcal{U}(\rho, t_\epsilon)$ by trace norm $1/3$. However, Lemma D1 in the [Supplementary Information](#) tells us that C_η/ϵ^2 samples of ρ are required if $\epsilon < \eta \leq 1/2$. Therefore

$$f(t_\epsilon, 1/3) \geq C_\eta/\epsilon^2 = Ct_\epsilon^2, \quad t_\epsilon \geq \pi, \quad (26)$$

using the definition of t_ϵ , and where $C := 4C_\eta/\pi^2$ is some positive constant. Eq. (26) holds whenever $t_\epsilon \geq \pi$ since $\epsilon \leq 1/2$ and so $t_\epsilon = \frac{\pi}{2} \cdot \frac{1}{\epsilon} \geq \pi$. Now suppose instead we have arbitrary δ and t satisfying $\delta \leq 1/6$ and $t/\delta \geq 6\pi$, as assumed in the theorem statement. We note the following inequality for any $t \in \mathbb{R}$ and any integer $m \geq 0$:

$$mf(t, \delta) \geq f(mt, m\delta), \quad (27)$$

which holds because one way of simulating $\exp(-ipmt)$ up to error $m\delta$ is to run m times a simulation of $\exp(-ipt)$ up to error δ . Taking $m = \lceil 1/(6\delta) \rceil$, we have

$$f(t, \delta) \geq f(mt, m\delta)/m \quad (28)$$

$$\geq C(mt)^2/m = Cmt^2 \quad (29)$$

$$= \Omega(t^2/\delta), \quad (30)$$

where Eq. (29) holds because $m\delta \leq 1/6 + \delta \leq 1/3$ and $mt \geq t/(6\delta) \geq \pi$, so Eq. (26) applies.

We now give a proof of Theorem 5. One key tool in the proof will be the following lemma, which lets us simulate a Hamiltonian given by the difference of two subnormalized states:

Lemma 12 Let $\rho' \in \mathcal{D}(\mathbb{C}^2 \otimes \mathcal{H}_A)$ be a quantum state of the form $\rho' = |0\rangle\langle 0| \otimes \rho_+ + |1\rangle\langle 1| \otimes \rho_-$, where ρ_+, ρ_- are unknown subnormalized states with $\text{Tr } \rho_+ + \text{Tr } \rho_- = 1$. Using n samples of ρ' , a quantum algorithm can transform σ_{AB} into $\tilde{\sigma}_{AB}$ such that

$$\frac{1}{2} \|(e^{-iHt} \otimes \mathbb{1}_B) \sigma_{AB} (e^{iHt} \otimes \mathbb{1}_B) - \tilde{\sigma}_{AB}\|_1 \leq O(\delta), \quad H = \rho_+ - \rho_-, \quad (31)$$

if $n = O(t^2/\delta)$.

The idea is to use the first qubit of ρ' as a control that determines whether one applies a positive or negative time evolution of partial swap between the second register of ρ' and the target state. The rest of the

proof (found in [Supplementary Information Section E.2](#)) proceeds as in the proof sketch of the standard LMR protocol.

Proof of Theorem 5 We first consider a term H_r with $r = (1, 2, \dots, k)$, for some k such that $2 \leq k \leq K$. (More general r will follow easily from this special case.) Let S_k be the cyclic permutation of k copies of \mathcal{H}_A that acts as follows: $S_k |j_1 j_2 \dots j_k\rangle = |j_k j_1 \dots j_{k-1}\rangle$. In other words,

$$S_k := \sum_{j_1, j_2, \dots, j_k=1}^{\dim \mathcal{H}_A} |j_k\rangle\langle j_1| \otimes |j_1\rangle\langle j_2| \otimes |j_2\rangle\langle j_3| \otimes \dots \otimes |j_{k-1}\rangle\langle j_k|. \quad (32)$$

Consider the circuit in Fig. 2. The output is of the form $\rho^{(r)} = |0\rangle\langle 0| \otimes \rho_+^{(r)} + |1\rangle\langle 1| \otimes \rho_-^{(r)}$, where

$$\begin{aligned} \rho_+^{(r)} &:= \frac{1}{2} (|a|^2 \rho_1 + |b|^2 \rho_k + ab^* \rho_1 \rho_2 \dots \rho_k + a^* b \rho_k \rho_{k-1} \dots \rho_1), \\ \rho_-^{(r)} &:= \frac{1}{2} (|a|^2 \rho_1 + |b|^2 \rho_k - ab^* \rho_1 \rho_2 \dots \rho_k - a^* b \rho_k \rho_{k-1} \dots \rho_1). \end{aligned} \quad (33)$$

When we chose $ab^* = e^{i\phi_r}/2$, we find

$$\rho_+^{(r)} - \rho_-^{(r)} = \frac{1}{2} e^{i\phi_r} \rho_1 \rho_2 \dots \rho_k + \frac{1}{2} e^{-i\phi_r} \rho_k \rho_{k-1} \dots \rho_1 = H_r. \quad (34)$$

To deal with arbitrary r with $|r|=k$, simply supply the appropriate input states ρ_j in Fig. 2. Now without loss of generality, we can assume $c_r \geq 0$ for all r , since the sign can be absorbed into the phase ϕ_r . Therefore by sampling from $r \in R$ with probability c_r/c and creating $\rho^{(r)}$, we obtain the state

$$\rho' = \frac{1}{c} \left(\sum_{r \in R} c_r \rho^{(r)} \right) = \frac{1}{c} \left(|0\rangle\langle 0| \otimes \left(\sum_{r \in R} c_r \rho_+^{(r)} \right) + |1\rangle\langle 1| \otimes \left(\sum_{r \in R} c_r \rho_-^{(r)} \right) \right). \quad (35)$$

By Lemma 12, we can therefore simulate the Hamiltonian

$$H = \sum_{r \in R} c_r (\rho_+^{(r)} - \rho_-^{(r)}) = \sum_{r \in R} c_r H_r \quad (36)$$

for the desired time and precision using $O(c^2 t^2/\delta)$ copies of ρ' . Since each copy of ρ' requires a sample of a state $\rho^{(r)}$, and each of these states requires at most $L = \max_{r \in R} |r|$ copies of states in $\{\rho_1, \dots, \rho_K\}$, we obtain the stated total sample complexity. To calculate the average number of uses of the state ρ_j , we note that ρ_j is used $v_j(r)$ times to create the state $\rho^{(r)}$, and to create the state ρ' , the state $\rho^{(r)}$ is chosen with probability $|c_r|/c$. Thus ρ_j is used on average $k_j = \sum_{r \in R} v_j(r) |c_r|/c$ times to create a single ρ' . Then since $O(c^2 t^2/\delta)$ copies of ρ' are used in the simulation, we obtain the stated complexity.

ACKNOWLEDGEMENTS

We thank Andrew Childs for suggesting the proof idea of Theorem 4, Aram Harrow, Stephen Jordan, Seth Lloyd, Iman Marvian, Ronald de Wolf, Michael Gullans, and Henry Yuen for useful discussions, and Michał Oszmaniec for pointing out the ref. 22. Part of this work was done while M.O. was visiting the University of Maryland and MIT, so he thanks both institutions for their hospitality. S.K. and C.Y.L. are funded by the Department of Defense. G.H.L. is funded by the NSF CCR and the ARO quantum computing projects. M.O. acknowledges Leverhulme Trust Early Career Fellowship (ECF-2015-256) and European Union project QALGO (Grant Agreement No. 600700) for financial support. T.J.Y. thanks the DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a. The authors are grateful to the University of Maryland Libraries' Open Access Publishing Fund and the Massachusetts Institute of Technology Open Access Publishing Fund for partial funding for open access.

AUTHOR CONTRIBUTIONS

All authors contributed equally.

COMPETING INTERESTS

The authors declare no competing financial interest.

REFERENCES

- Lloyd, S. Universal quantum simulators. *Science* **273**, 1073–1078 (1996).
- Low, G.H. & Chuang, I.L. Optimal Hamiltonian simulation by quantum signal processing. *Physical Review Letters* **108**, 010501 (2017).

3. Berry, D. W., Childs, A. M. & Kothari, R. Hamiltonian simulation with nearly optimal dependence on all parameters. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, 792–809 (IEEE, 2015).
4. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2010). <https://books.google.com/books?id=s4DEy7o-a0C>.
5. Lloyd, S., Mohseni, M. & Rebentrost, P. Quantum principal component analysis. *Nat. Phys.* **10**, 631–633 (2014).
6. Audenaert, K., Datta, N. & Ozols, M. Entropy power inequalities for qudits. *J. Math. Phys.* **57**, 052202 (2016).
7. Preskill, J. Plug-in quantum software. *Nature* **402**, 357–358 (1999).
8. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390–393 (1999).
9. Wang, G. Quantum algorithms for curve fitting. arXiv preprint arXiv:1402.0660 (2014).
10. Rebentrost, P., Mohseni, M. & Lloyd, S. Quantum support vector machine for big data classification. *Phys. Rev. Lett.* **113**, 130503 (2014).
11. Cong, I. & Duan, L. Quantum discriminant analysis for dimensionality reduction and classification. *New J. Phys.* **18**, 073011 (2016).
12. Ozols, M. How to combine three quantum states. arXiv preprint arXiv:1508.0086. (2015)
13. Haah, J., Harrow, A. W., Ji, Z., Wu, X. & Yu, N. Sample-optimal tomography of quantum states. *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, 913–925 (ACM, 2016).
14. O'Donnell, R. & Wright, J. Efficient quantum tomography. *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, 899–912 (ACM, 2016).
15. Emch, G. G. *Mathematical and Conceptual Foundations of 20th-Century Physics*. North-Holland Mathematics Studies (Elsevier Science, 1984). <https://books.google.com/books?id=eYQHjkaEroCpg=PA306>.
16. Kothari, R. *Efficient algorithms in quantum query complexity*. Ph.D. thesis, University of Waterloo (2014). <http://hdl.handle.net/10012/8625>.
17. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219 (ACM, 1996).
18. Demkowicz-Dobrzański, R. & Markiewicz, M. Quantum computation speedup limits from quantum metrological precision bounds. *Phys. Rev. A* **91**, 062322 (2015).
19. Brassard, G., Høyer, P., Mosca, M. & Tapp, A. Quantum amplitude amplification and estimation. *Contemp. Math.* **305**, 53–74 (2002).
20. Boyer, M., Brassard, G., Høyer, P. & Tapp, A. Tight bounds on quantum searching. *Fortschritte der Physik* **46**, 493–505 (1998).
21. Buhrman, H., Cleve, R., de Wolf, R. & Zalka, C. Bounds for small-error and zero-error quantum algorithms. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, 358–368 (IEEE, 1999).
22. Oszmaniec, M., Grudka, A., Horodecki, M. & Wójcik, A. Creating a superposition of unknown quantum states. *Phys. Rev. Lett.* **116**, 110403 (2016).
23. Li, K. et al. Experimentally superposing two pure states with partial prior knowledge. arXiv preprint arXiv:1608.04349 (2016)
24. Loss, D. & DiVincenzo, D. P. Quantum computation with quantum dots. *Phys. Rev. A* **57**, 120–126 (1998).
25. Kane, B. E. A silicon-based nuclear spin quantum computer. *Nature* **393**, 133–137 (1998).
26. Vrijen, R. et al. Electron-spin-resonance transistors for quantum computing in silicon-germanium heterostructures. *Phys. Rev. A* **62**, 012306 (2000).
27. Barenco, A. et al. Elementary gates for quantum computation. *Phys. Rev. A* **52**, 3457–3467 (1995).
28. DiVincenzo, D. P., Bacon, D., Kempe, J., Burkard, G. & Whaley, K. B. Universal quantum computation with the exchange interaction. *Nature* **408**, 339–342 (2000).
29. Levy, J. Universal quantum computation with spin-1/2 pairs and Heisenberg exchange. *Phys. Rev. Lett.* **89**, 147902 (2002).
30. Costache, M. V. & Valenzuela, S. O. Experimental spin ratchet. *Science* **330**, 1645–1648 (2010).
31. Folk, J. A., Potok, R. M., Marcus, C. M. & Umansky, V. A gate-controlled bidirectional spin filter using quantum coherence. *Science* **299**, 679–682 (2003).
32. Hanson, R. et al. Semiconductor few-electron quantum dot operated as a bipolar spin filter. *Phys. Rev. B* **70**, 241304 (2004).
33. Recher, P., Sukhorukov, E. V. & Loss, D. Quantum dot as spin filter and spin memory. *Phys. Rev. Lett.* **85**, 1962–1965 (2000).
34. Bremner, M. J. et al. Practical scheme for quantum computation with any two-qubit entangling gate. *Phys. Rev. Lett.* **89**, 247902 (2002).
35. Marvian, I. & Mann, R. B. Building all time evolutions with rotationally invariant Hamiltonians. *Phys. Rev. A* **78**, 022304 (2008).
36. Pichler, H., Zhu, G., Seif, A., Zoller, P. & Hafezi, M. A measurement protocol for the entanglement spectrum of cold atoms. Preprint at arXiv:1605.08624 (2016).
37. Harrow, A. W. & Leung, D. W. A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities. *IEEE Trans. Inform. Theory* **57**, 5504–5508 (2011).
38. Aaronson, S. Quantum copy-protection and quantum money. In *Computational Complexity (CCC), 2009 IEEE 24th Annual Conference on*, 229–242 (IEEE, 2009).
39. Marvian, I. & Lloyd, S. Universal quantum emulator. arXiv preprint arXiv:1606.02734 (2016).
40. Alagic, G. & Fefferman, B. On quantum obfuscation. arXiv preprint arXiv:1602.01771 (2016).
41. Ekert, A. K. et al. Direct estimations of linear and nonlinear functionals of a quantum state. *Phys. Rev. Lett.* **88**, 217901 (2002).



This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>

© The Author(s) 2017

Supplementary Information accompanies the paper on the *npj Quantum Information* website (doi:10.1038/s41534-017-0013-7).