Quantum State Restoration and Single-Copy Tomography for Ground States of Hamiltonians

Edward Farhi, David Gosset, Avinatan Hassidim, and Andrew Lutomirski
Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

Daniel Nagaj
Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia

Peter Shor
Department of Mathematics, Center for Theoretical Physics and CSAIL, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

(Received 8 February 2010; published 4 November 2010)

Given a single copy of an unknown quantum state, the no-cloning theorem limits the amount of information that can be extracted from it. Given a gapped Hamiltonian, in most situations it is impractical to compute properties of its ground state, even though in principle all the information about the ground state is encoded in the Hamiltonian. We show in this Letter that if you know the Hamiltonian of a system and have a single copy of its ground state, you can use a quantum computer to efficiently compute its local properties. Specifically, in this scenario, we give efficient algorithms that copy small subsystems of the state and estimate the full statistics of any local measurement.

DOI: 10.1103/PhysRevLett.105.190503 PACS numbers: 03.67.Lx, 03.67.Dd

Introduction.—One of the fundamental problems of statistical mechanics and condensed matter is to characterize ground states of Hamiltonians. If we know the Hamiltonian of a system, we can in principal learn anything we want about the ground state by exact diagonalization. But exact diagonalization is too slow to use for all but the smallest systems, and it is widely believed to be hard to find properties of ground states of generic Hamiltonians on large systems.

On the other hand, if we are somehow given many independent copies of the ground state of some system, we can learn properties of that state using standard tomography algorithms. These algorithms do not take advantage of the fact that the Hamiltonian is known.

In this Letter, we present tomography algorithms that take advantage of our knowledge of the Hamiltonian H of the system and only require a single copy of the ground state. The core of our approach is a method of copying small subsystems of the ground state $|\psi\rangle$ of a Hamiltonian without damaging the original state. Our procedure does not violate the no-cloning theorem (which only applies to completely unknown states) because our state $|\psi\rangle$ is known to be the ground state of H.

To motivate our algorithm, consider a classical problem. Suppose that there is some unknown n-bit string $z = z_A z_B$, where z_A is the first $n - k$ bits of z and z_B is the last k bits. Suppose further that there is a function

$$f(x) = \begin{cases} 1 & \text{if } x = z, \\ 0 & \text{otherwise} \end{cases}$$

on n-bit strings that tests whether they are equal to z. If we are given z_A and the ability to evaluate f, we can find z by randomly guessing: we pick a random k-bit string x_B and evaluate $f(z_A x_B)$, repeating until we get $f = 1$. This finds z in expected time 2^k.

Our main algorithm, quantum state restoration, is a straightforward quantum generalization of this classical algorithm, which surprisingly works even on entangled states. If $|\psi\rangle$ lives in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, our algorithm takes as input the part of $|\psi\rangle$ that lives in subsystem A and uses phase estimation on H to produce as output the state $|\psi\rangle$ in expected time $O(\text{poly}(\dim \mathcal{H}_B))$. It works by randomly guessing the part of $|\psi\rangle$ that lives in subsystem B and measuring if the resulting state is the ground state of $\mathcal{H}$. On a successful iteration (i.e., if we find that we are in the ground state), then we have recovered $|\psi\rangle$. On a failed iteration, there is minimal damage to the part of the state in subsystem A and we can try again.

This can be used to copy small subsystems of $|\psi\rangle$: if $|\psi\rangle$ has the reduced density matrix ρ_B on a small subsystem B, we can set aside subsystem B and then use state restoration to extend subsystem A to the full state $|\psi\rangle$. We are left with $|\psi\rangle$ and a mixed state ρ_B. If we use this to obtain multiple copies of ρ_B, we can perform tomography on subsystem B. We call this application single-copy tomography. We also give a reduction from estimating the statistics of a general POVM (positive operator value measurement) to single-copy tomography with running time polynomial in the number of POVM operators. The reduction is applicable even if the POVM includes noncommuting operators.

Quantum state restoration applies more generally than just to ground states: even if $|\psi\rangle$ is not known to be the ground state of any particular Hamiltonian, we can use our algorithms if we can efficiently measure $|\psi\rangle\langle\psi|$ by some other means.

Quantum state restoration.—Quantum state restoration takes as input a description of a Hamiltonian H and a large subsystem of the ground state $|\psi\rangle$ (this subsystem could be, for example, the first $n-k$ qubits of the n qubit state $|\psi\rangle$) and outputs the full state $|\psi\rangle$. In this section we first describe how to use the Hamiltonian to measure the operator $P = |\psi\rangle\langle\psi|$ and then we describe the algorithm for quantum state restoration (which uses this measurement as a subroutine).

Using H to measure the projector $|\psi\rangle\langle\psi|$.—Using the description of the Hamiltonian H, we can measure the operator $P = |\psi\rangle\langle\psi|$ on any state $|\phi\rangle$. We do this by using two extra quantum registers: one has enough digits to store the eigenvalues of H, and the other is a single qubit. We set both registers to zero, giving

$$|\phi\rangle|0\rangle|0\rangle.$$

We then use phase estimation to compute the energy:

$$\sum \alpha_i |\xi_i\rangle|E_i\rangle|0\rangle,$$

where the α_i are the (unknown) coefficients of $|\phi\rangle$ in the energy eigenbasis, $|\xi_i\rangle$ are eigenstates in increasing order of energy. For each i, E_i is the energy of $|\xi_i\rangle$. (This means that $|E_i\rangle$ is a quantum state that contains a *number* it is not an energy eigenstate of H.) We now apply a NOT operator to the third register, conditioned on the second register being greater than E_0. This gives

$$\alpha_0|\xi_0\rangle|E_0\rangle|0\rangle + \sum_{i>0}\alpha_i|\xi_i\rangle|E_i\rangle|1\rangle.$$

We now uncompute the phase estimation (that is, we apply the inverse operation), giving

$$\alpha_0|\xi_0\rangle|0\rangle|0\rangle + \sum_{i>0}\alpha_i|\xi_i\rangle|0\rangle|1\rangle.$$

The second register is now unentangled with the rest of the system, so we can discard it, and measure the third register. Noting that $|\xi_0\rangle = |\psi\rangle$ and $\sum_{i>0}\alpha_i|\psi_i\rangle = P^\perp|\phi\rangle$, we see that this procedure effectively measures the operator P. Using standard phase estimation, we will have a nonnegligible probability of error, but we can use standard techniques [1,2] to make the error exponentially small.

Algorithm for quantum state restoration.—The idea behind quantum state restoration is that any state $|\psi\rangle$ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ (where d is the dimension of $\mathcal{H}_B$) can be Schmidt decomposed as

$$|\psi\rangle = \sum_{i=1}^{\chi}\sqrt{p_i}\,|u_i\rangle|v_i\rangle$$

where χ is the Schmidt rank of $|\psi\rangle$ with respect to this decomposition. Note that $\chi \le d$. The initial mixture $\rho_A = \mathrm{Tr}_B|\psi\rangle\langle\psi|$ has all of its support on the Schmidt basis span$\{|u_i\rangle\}$. Starting from ρ_A, we can construct the state $\rho_A \otimes \frac{I}{d}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$. We now measure the projector P. If we obtain the outcome 1, then we are left with the state $|\psi\rangle$ If not, we discard (i.e., trace out) $\mathcal{H}_B$, leaving a state on $\mathcal{H}_A$ that *still* has all of its support on the Schmidt basis. We then try again until we obtain the outcome 1.

We now explicitly define the quantum state restoration algorithm.

(1) Start with the mixture

$$\rho_A = \mathrm{Tr}_B|\psi\rangle\langle\psi|.$$

as well as an extra register in the Hilbert space $\mathcal{H}_B$.

(2) Set the extra register to the fully mixed state (for example, by replacing it with a random state or by applying a random unitary). The state of the system is now

$$\rho_A \otimes \frac{\mathbb{I}}{d}.$$

(3) Measure the projector $P = |\psi\rangle\langle\psi|$. If the outcome is $+1$ then you are done: the state of the system is $|\psi\rangle$. If not, return to step 2.

This algorithm requires an expected number of iterations $\chi d \le d^2$.

In the simple case where all of the p_i are equal, then the initial state ρ_A is the fully mixed state over the span$\{|u_i\rangle\}$. In this case, if you measure 0 in step 3, the density matrix left in register A after tracing out register B is unchanged. The algorithm terminates with probability $\frac{1}{\chi d}$ on each iteration, finishing in an expected number of iterations χd. If the p_i are not all equal, then the algorithm can reach bad states where most of the weight is on low-weight elements of the Schmidt basis. When this happens, the chance of success on any given iteration drops (see Fig. 1 for an example), but the probability of reaching these bad states decreases with the corresponding p_i. Surprisingly, these effects exactly cancel, and the expected number of iterations required to restore the state is χd regardless of the values of the p_i.

To prove this, we define the map

$$F_0(\sigma) = \mathrm{Tr}_B\left[(1 - |\psi\rangle\langle\psi|)\left(\sigma \otimes \frac{\mathbb{I}}{d}\right)(1 - |\psi\rangle\langle\psi|)\right]$$

$F_0(\sigma)$ is the unnormalized density matrix obtained by applying steps 2 and 3 of the algorithm to the state σ, conditioned on the measurement outcome 0. We also define $T(\sigma)$ to be the expected number of measurements used in the algorithm if we start with the state σ. In the supplementary material [3] we show that $T(\sigma)$ is linear (To extend $T(\sigma)$ to all nonnegative operators σ, we define

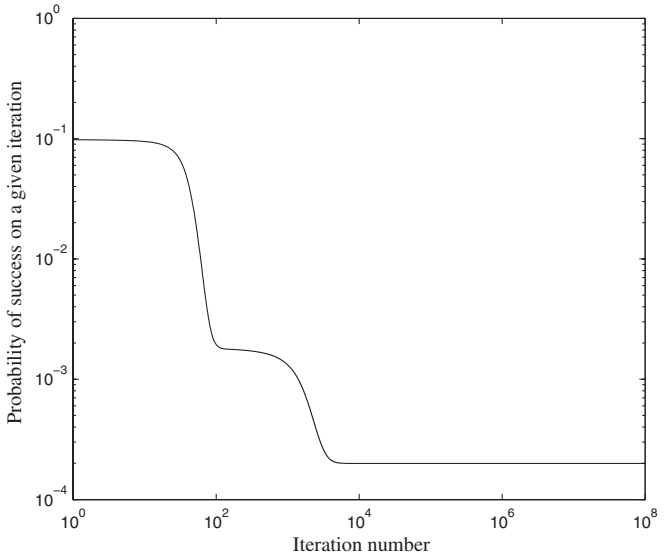

FIG. 1. Probability of restoring the state on a given iteration conditioned on all previous iterations failing. Conditioned on failing every time, the first two flat regions are metastable states and the third is stable. In this graph, $|\psi\rangle = \sqrt{1-10^{-2}-10^{-3}}|0\rangle_A|0\rangle_B + \sqrt{10^{-2}}|1\rangle_A|1\rangle_B + \sqrt{10^{-3}}|2\rangle_A|2\rangle_B$, $\dim\mathcal{H}_B = 10$, and the expected number of iterations required is 30.

$T(\sigma) = \mathrm{Tr}\sigma T(\sigma/\mathrm{Tr}\sigma))$. We are interested in the quantity $T(\rho_A)$, which we write as

$$T(\rho_A) = \sum_{i=1}^{\chi} p_i T(|u_i\rangle\langle u_i|). \tag{1}$$

We expand $T(|u_i\rangle\langle u_i|)$ by conditioning on the outcome of the first measurement

$$\begin{aligned} &T(|u_i\rangle\langle u_i|) \\ &\quad = 1 + T(F_0(|u_i\rangle\langle u_i|)) \\ &\quad = 1 + T\Big(|u_i\rangle\langle u_i| - 2\frac{p_i}{d}|u_i\rangle\langle u_i| + \frac{p_i}{d}\sum_{j=1}^{\chi} p_j|u_j\rangle\langle u_j|\Big) \\ &\quad = 1 + \Big(1 - 2\frac{p_i}{d}\Big)T(|u_i\rangle\langle u_i|) + \frac{p_i}{d}\sum_{j=1}^{\chi} p_j T(|u_j\rangle\langle u_j|). \end{aligned}$$

Using (1), this can be transformed into

$$2p_i T(|u_i\rangle\langle u_i|) - p_i T(\rho_A) = d.$$

Summing both sides over $i = 1, \ldots, \chi$ using $\sum p_i = 1$ and (1) again, we obtain

$$T(\rho_A) = \chi d,$$

which is the desired result. More efficient algorithms and a complete analysis can be found in the supplementary material [4].

Single-copy tomography and estimation of measurement statistics.—Quantum state restoration can be used to perform tomography on a single copy the ground state of a gapped Hamiltonian. We can perform several different types of tomography, and we give algorithms for some types that are faster than quantum state restoration.

In the simplest case, we have a gapped Hamiltonian H and a single copy of its (unknown) ground state $|\psi\rangle$. As before, we can use H to measure the projector $P = |\psi\rangle\langle\psi|$ and we would like to estimate properties of the density matrix $\rho_B = \mathrm{Tr}_A|\psi\rangle\langle\psi|$ for a subsystem B. We can do this by using quantum state restoration to prepare many unentangled states, each with (independent) density matrices ρ_B. We can then use any standard state tomography algorithm on these states. Alternatively, we can use the techniques below to estimate an informationally complete POVM on subsystem B.

We want to estimate the probabilities $q_i = \mathrm{Tr}[|i\rangle_{BB} \times \langle i||\psi\rangle\langle\psi|]$ of obtaining the outcome i if one were to measure subsystem B of $|\psi\rangle$ in the orthonormal basis $\{|i\rangle_B\}$. The simplest way to estimate these statistics is to repeat the measurement many times, running quantum state restoration after each measurement, and to estimate q_i as $\frac{m_i}{N}$ where m_i is the number of appearances of outcome i in N trials. In the supplementary material [3], we present two algorithms that estimate the values $\{q_i\}$ more efficiently by applying ideas from the QMA (quantum Merlin Arthur) amplification schemes presented by Marriott and Watrous [5] and Nagaj *et al.* [6]. Fixing a precision $\delta > 0$ and an error probability $\epsilon > 0$, the algorithm produces estimates q_i^{est} such that $|q_i^{\mathrm{est}} - q_i| < \delta$ for all i with probability at least $1 - \epsilon$ in expected time $O(\frac{d}{\delta}\log(\frac{d}{\epsilon}))$ (measured in number of uses of P).

We can use any of these algorithms to estimate the statistics of a general measurement on a single copy of a ground state $|\phi\rangle$. This is because a general POVM measurement can be reduced to a measurement of a subsystem in an orthogonal basis, as we now review. We work in a two register Hilbert space: register A can hold $|\phi\rangle$ and register B is a d-dimensional ancilla. Given an efficiently implementable POVM $\{E_i\}$ where $i \in \{1, \ldots, d\}$, we can implement a unitary operator U such that

$$U(|\phi\rangle_A|1\rangle_B) = \sum_{i=1}^{d}(\sqrt{E_i}|\phi\rangle_A)|i\rangle_B$$

for any state $|\phi\rangle$. The probability of measurement outcome i when the POVM is measured on $|\phi\rangle$ is equal to

$$\langle\phi|E_i|\phi\rangle = \mathrm{Tr}[\rho_B|i\rangle_{BB}\langle i|]$$

where $\rho_B = \mathrm{Tr}_A[U|\phi\rangle_A|1\rangle_{BB}\langle 1|_A\langle\phi|U^\dagger]$. If we define

$$|\psi\rangle = U|\phi\rangle_A|1\rangle_B \qquad P' = |\psi\rangle\langle\psi| = UPU^\dagger$$

then $\rho_B = \mathrm{Tr}_A|\psi\rangle\langle\psi|$, $|\psi\rangle$ can be efficiently prepared (starting from $|\phi\rangle$) and P' can be efficiently measured. We can now estimate the measurement statistics of subsystem B of $|\psi\rangle$ using the projector P' in the computational

basis, yielding the probabilities $\langle\phi|E_i|\phi\rangle = \mathrm{Tr}[|i\rangle\langle i|\rho'_B]$. After estimating the probabilities, we uncompute U to recover the initial state $|\phi\rangle$.

Applications of quantum state restoration and single-copy tomography.—Quantum computers offer potentially exponential speedups in simulating quantum mechanics, but some problems are still hard. For example, preparing ground states of many-body systems generically takes exponential time in the number of particles. Nonetheless, for sufficiently small systems with large enough energy gaps, algorithms such as [7] may run quickly enough to prepare a single copy of the ground state. Single-copy tomography allows us to make multiple tomographic measurements (even of noncommuting operators) after preparing only a single copy of the ground state. This gives a speedup over traditional tomography.

In addition, single-copy tomography could be useful to characterize the ground state during adiabatic evolution. This information could be used in real time to guide the choice of path for an adiabatic algorithm.

In the introduction, we mentioned that quantum state restoration also works on states that are not ground states but are instead verified by some quantum algorithm. One example of this type of state is quantum money [8–12]. Quantum money is meant to be the quantum analog of the everyday money we hold in our pocket, except that it should be secure against forgery by a counterfeiter with limited computational resources. One type of quantum money scheme works as follows. The mint generates bills (a bill is a quantum state $|\psi_p\rangle$ paired with a classical serial number p), and publishes a verification algorithm which, taking as input the serial number p of a quantum money state $|\psi_p\rangle$, implements the measurement of $|\psi_p\rangle\langle\psi_p|$. Using this verification algorithm, anyone (for example a merchant) can check that a bill is authentic. In this scenario, a would-be forger with one quantum bill can use quantum state restoration to efficiently learn properties of the quantum money state $|\psi_p\rangle$. Quantum money protocols must therefore be secure against this type of attack.

This work was supported in part by funds provided by the U.S. Department of Energy under cooperative research agreement No. DE-FG02-94ER40818, the W. M. Keck Foundation Center for Extreme Quantum Information Theory, the U.S. Army Research Laboratory's Army Research Office through Grant No. W911NF-09-1-0438, the National Science Foundation through Grant No. CCF-0829421, the NDSEG, the Natural Sciences and Engineering Research Council of Canada, Microsoft Research, European Project OP CE QUTE ITMS NFP 26240120009, and the Slovak Research and Development Agency under Contract No. APVV LPP-0430-09.

[1] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, arXiv:quant-ph/0005055.
[2] V. Bužek, R. Derka, and S. Massar, Phys. Rev. Lett. **82**, 2207 (1999).
[3] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, D. Nagaj, and P. Shor, arXiv:0912.3823.
[4] See supplementary material at http://link.aps.org/supplemental/10.1103/PhysRevLett.105.190503 for detailed proofs and runtime analysis.
[5] Chris Marriott and John Watrous, Comput. Complex. **14**, 122 (2005).
[6] Daniel Nagaj, Pawel Wocjan, and Yong Zhang, Quantum Inf. Comput. **9**, 1053 (2009).
[7] David Poulin and Pawel Wocjan. Phys. Rev. Lett. **102**, 130503 (2009).
[8] S. Aaronson, in *Computational Complexity, Proceedings of the Annual IEEE Conference* (IEEE Computer Society, Washington, DC, 2009), pp. 229–242.
[9] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology–Proceedings of Crypto* (Plenum Press, New York, 1983), Vol. 82, p. 267275.
[10] M. Mosca and D. Stebila, in *Error-Correcting Codes, Finite Geometries, and Cryptography*, Contemporary Mathematics Vol. 523 (American Mathematical Society, Providence, 2010), p. 35.
[11] Stephen Wiesner, SIGACT News **15**, 78 (1983).
[12] Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jon Kelner, Andrew Lutomirski, and Peter Shor, arXiv:0912.3825