Optimal Quantum Measurements of Expectation Values of Observables

Emanuel Knill

Mathematical and Computational Sciences Division, National Institute of Standards and Technology, Boulder CO 80305

Gerardo Ortiz

Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545 and Department of Physics, Indiana University, Bloomington, IN 47405

Rolando D. Somma

Physics Division, Los Alamos National Laboratory, Los Alamos, NM 87545

(Dated: January 25, 2022)

Experimental characterizations of a quantum system involve the measurement of expectation values of observables for a preparable state $|j\rangle$ of the quantum system. Such expectation values can be measured by repeatedly preparing $|j\rangle$ and coupling the system to an apparatus. For this method, the precision of the measured value scales as $1/N$ for $N$ repetitions of the experiment. For the problem of estimating the parameter in an evolution $e^{-iHt}$, it is possible to achieve precision $1/N$ (the quantum metrology limit, see [1]) provided that sufficient information about $H$ and its spectrum is available. We consider the more general problem of estimating expectations of operators $A$ with minimal prior knowledge of $A$. We give explicit algorithms that approach precision $1/N$ given a bound on the eigenvalues of $A$ or on their tail distribution. These algorithms are particularly useful for simulating quantum systems on quantum computers because they enable efficient measurement of observables and correlation functions. Our algorithms are based on a method for efficiently measuring the complex overlap of $|j\rangle$ and $U|j\rangle$, where $U$ is an implementable unitary operator. We explicitly consider the issue of confidence levels in measuring observables and overlaps and show that, as expected, confidence levels can be improved exponentially with linear overhead. We further show that the algorithms given here can typically be parallelized with minimal increase in resource usage.

PACS numbers: 03.67.-a, 03.67.Mn, 03.65.Ud, 05.30-d

I. INTRODUCTION

Uncertainty relations such as Heisenberg’s set fundamental physical limits on the achievable precision when we extract information from a physical system. The goal of quantum metrology
is to measure properties of states of quantum systems as precisely as possible given available resources. Typically, these properties are determined by experiments that involve repeated preparation of a quantum system in a state followed by a measurement. The property is derived from the measurement outcomes. Because the repetitions are statistically independent, the precision with which the property is obtained scales as \( \frac{1}{\sqrt{N}} \), where \( N \) is the number of preparations performed. This is known as the standard quantum limit or the shot-noise limit, and it is associated with a purely classical statistical analysis of errors. It has been shown that in many cases of interest, the precision can be improved to \( \frac{1}{N} \) by using the same resources but with initial states entangled over multiple instances of the quantum system, or by preserving quantum coherence from one experiment to the next. It is known that it is usually not possible to attain a precision that scales better than \( \frac{1}{\sqrt{N}} \). (See [2] for a review of quantum-enhanced measurements.) A setting where this limit can be achieved is the parameter estimation problem, where the property is given by the parameter in an evolution \( e^{-iHt} \) for a known Hamiltonian \( H \) [1], which captures some common measurement problems. The standard method for determining requires the ability to apply \( e^{-iHt} \) and to prepare and measure an eigenstate of \( H \) with known eigenvalue. If it is not possible to prepare such an eigenstate or if we wish to determine expectations with respect to arbitrary states, this method fails. Here we are interested in the more general and physically important expectation estimation problem, where the property to be determined is an expectation \( \langle A \rangle \) of an observable (Hermitian operator) or unitary \( A \), for a possibly mixed state \( \rho \). Both \( A \) and \( \rho \) are assumed to be experimentally sufficiently controllable, but other than a bound on the eigenvalues of \( A \) or their tail distribution, no other properties of \( A \) or \( \rho \) need to be known. In particular, we need not be able to prepare eigenstates of \( A \) or know the spectrum of \( A \). The parameter estimation problem is a special instance of the expectation estimation problem. Parameter estimation reduces to the problem of determining \( \langle A \rangle = \text{tr}(\rho A) \) for \( \rho \) an eigenstate of \( H \) with non-zero eigenvalue. We show that for solving the expectation estimation problem, precision scalings of \( \frac{1}{N} \) for arbitrarily small \( \frac{1}{N} > 0 \) can be achieved with sequential algorithms, and the algorithms can be parallelized with minimal additional resources.

Our motivation for this work is the setting of quantum physics simulations on quantum computers. This is one of the most promising applications of quantum computing [3] and enables a potentially exponential speedup for the correlation function evaluation problem [4, 5, 6]. The measurement of these correlation functions reduces to the measurement of the expectation of an operator for one or more states. Because the measurement takes place within a scalable quantum computer, the operators and states are manipulatable via arbitrarily low-error quantum gates. The quantum computational methods that have been described for the determination of these expectations have order \( \frac{1}{N} \) precision. An example is the one-ancilla algorithm for measuring \( \text{tr}(U\rho U^\dagger) = \text{tr}(U \rho U^\dagger) \) for unitary \( U \) described in [5, 7, 8], which applies \( U \) conditional on an ancilla \( a \) prepared in a superposition state (Fig. 1). Improving the precision without special knowledge of the operator or state requires more sophisticated algorithms.

Here we give quantum algorithms based on phase and amplitude estimation [2, 10] to improve the resource requirements to achieve a given precision. We begin by giving an “overlap estimation” algorithm (OEA) for determining the amplitude and phase of \( \text{tr}(U \rho U^\dagger) \) for \( U \) unitary. We assume that quantum procedures for preparing from a standard initial state and for applying \( U \) are known and that it is possible to reverse these procedures. We determine the number of times \( N \) that these procedures are used to achieve a goal precision \( p \) and show that \( N \) is of order \( 1/p \). To determine \( \text{tr}(A \rho) \) for observables \( A \) not expressible as a small sum of unitary operators, we assume that it is possible to evolve under \( A \). This means that we can apply \( e^{-iA \tau} \) for positive times \( \tau \). The OEA can be used to obtain \( \text{tr}(A \rho) = \text{tr}(e^{-iA \tau} \rho) \) for small \( \tau \). The problem of how to measure
tr 𝜃 requires determining tr (e^{iHt}) with precision better than 𝑝, and choosing 𝑡 small enough that the error in the approximation does not dominate. We solve this problem by means of an “expectation estimation” algorithm (EEA) with minimal additional knowledge on the eigenvalue distribution of 𝐴. For this situation, the relevant resources are not only the number of uses of e^{iHt} and of the state preparation algorithm, but also the total time 𝑇 of evolution under 𝐴. We show that to achieve a goal precision 𝑝, 𝑁 and 𝑇 are of order 1 = (2^N) and 1 = 𝑝, respectively, with > 0 arbitrarily small. The term in the resource bound is due partly to the tail distribution of the eigenvalues of 𝐴 with respect to ρ. When it is known that 𝜃 is an eigenstate of 𝐴, so the distribution is a delta function, = 0. This applies to the parameter estimation problem. In the case where 𝐴 is unbounded, is still arbitrarily small if the tail distribution is exponentially decaying. But if only small moments of 𝐴 can be bounded, in which case the best bound on the tail distribution decays polynomially, becomes finite.

It is important to properly define the meaning of the term “precision”. Here, when we say that we are measuring tr (A) with precision 𝑝, we mean that the probability that the measured value 𝑎_{m,ea} is within 𝑝 of tr (A) is bounded below by a constant 𝐶 > 0. In other words, the “confidence level” that 𝑎_{m,ea} tr (A) 𝑎_{m,ea} + 𝑝 is at least 𝐶. Thus 𝑎_{m,ea} defines “confidence bounds” of the measurement for confidence level 𝐶. One interpretation of confidence levels is that if the measurement is independently repeated, the fraction of times the measured value is within the confidence bound is at least the confidence level. For measurement values 𝑎_{m,ea} that have an (approximately) gaussian distribution, it is conventional to use 𝐶 = 0.68 to identify the precision 𝑝 with the standard deviation. In this case, the confidence level that the measurement outcome is within 𝑥𝑝 can be bounded by erf(𝑥 = 𝑝), where erf(𝑦) is the error function, erf(𝑥 = 𝑝) = 1 e^{-𝑦^2}. This bound is often too optimistic, which is one reason to specify confidence levels explicitly. This becomes particularly important in our use of the “phase estimation” algorithm (PEA), whose standard version [9] has confidence levels that converge slowly toward 1 with 𝑥. Because of these issues, our algorithms are stated so that they solve the problem of determining tr (A) with precision 𝑝 and confidence level 𝐶, where 𝑝 and 𝐶 are specified at the beginning. This requires that the resource usage be parameterized by both 𝑝 and 𝐶 and we show that the resource usage grows by a factor of order \( j \log (1 - c) \) to achieve high confidence level 𝐶.
An important problem in measuring properties of quantum systems is how well the measurement can be parallelized with few additional resources. The goal of parallelizing is to minimize the time for the measurement by using more parallel resources. Ideally, the time for the measurement is independent of the problem. Typically we are satisfied if the time grows at most logarithmically. It is well known that for the parameter estimation problem, one can readily parallelize the measurement by exploiting entanglement in state preparation [11]. That this is still possible for the OEA and EEA given here is not obvious. In fact, we show that there are cases where parallelization either involves a loss of precision or requires additional resources. However, the entanglement method for parallelizing measurements works for expectation estimation and for overlap estimation when `j (U) j is not close to 1.

II. OVERLAP ESTIMATION

Let $U$ be a unitary operator and a state of quantum system $S$. We assume that we can prepare and apply $U$ to any quantum system $S_0$ that is equivalent to $S$. Both the preparation procedure and $U$ must be reversible. In addition, we require that the quantum systems are sufficiently controllable and that $U$ can be applied conditionally (see below). We use labels to clarify which quantum system is involved. Thus, $(S_0)$ is the state of system $S_0$ and $U (S_0)$ is $U$ acting on system $S_0$. This allows us to prepare and apply $U$ in parallel on multiple quantum systems.

When we say that we can prepare, we mean that we can do this fully coherently. That is, we have access to a unitary operator $V (SE)$ that can be applied to a standard initial state $\rho_{SE}$ of $S$ and an ancillary system $E$ (environment) such that $(S) = \text{tr}_E (V (SE) \rho_{SE} \rho_j (V (SE))^*)$. The state $V (SE) \rho_{SE}$ is a so-called purification of $(S)$. For our purposes and without loss of generality, we can assume that is pure by merging systems $E$ and $S$ and letting unitaries act on the merged system. With this simplification we can write $\rho_{ij} = \rho_{ih} \rho_{j} \rho_{j}^* \rho_{j} \rho_{j}^* \rho_{j} = \rho_{ij}$ and use $S;S_0;\cdots$ to refer to equivalent merged systems. The goal of the OEA is now to estimate the overlap $\langle U \rangle j$ of $j$ with $U j$.

The OEA and EEA require that $S$ is sufficiently controllable. In particular, we require that it is possible to couple $S$ to ancilla qubits and to implement conditional selective sign changes of $\sigma_{ij}$.

Let $\rho_0 (S) = \rho(S) \rho_j \rho_j$, be the selective sign change of $\sigma_{ij}$, with $\rho_0 (S)$ the identity (or no-action) operator. If an ancilla (control) qubit is labeled $a$, an instance of the conditional selective sign change is defined by

$$\rho_{ij} = \rho_{ia} \rho_{ija} + \rho_{ija} \rho_{ija}$$

(1)

If $S$ consists of qubits and $\sigma_{ij}$ is the usual starting state with all qubits in logical state $\sigma_{ij}$, then this is essentially a many-controlled sign flip and has efficient implementations [12].

As mentioned above, for the OEA we require that $U$ can be applied conditionally. This means that the unitary operator

$$U (S_0) = \rho_{ja} \rho_{ija} + \rho_{ija} \rho_{ija}$$

(2)

is available for use. When $U$ is associated with an evolution simulated on a quantum computer, this is no problem since all quantum gates are readily “conditionalized” [12]. Nevertheless, we note that $U$ is not required if only the amplitude $\rho_{ija} \rho_{ija}$ of $h j j j$ is needed.

The “amplitude estimation” algorithm (AEA) [11] can almost immediately be applied to obtain $\rho_{ija} \rho_{ija}$. To accomplish our goals we need to adapt it for arbitrarily prepared states and use a version that avoids the complexities of the full quantum Fourier transform [13]. Before we describe and analyze the version of the AEA needed here, we show how the OEA uses it to estimate the
phase and amplitude of \( \mathcal{A}_a \). Let \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) be the estimate of \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) obtained by the AEA for goal precision \( p \). (We specify the meaning of the precision parameter below.)

**Overlap estimation algorithm:** Given are \( \mathcal{U}, j^i \) (in terms of a preparation unitary \( V : \mathcal{U} \rightarrow \mathcal{U} \) and the goal precision \( p \). An estimate of \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) is to be returned.

1. Obtain \( a = \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1; p=4) \), so that \( a \) is an estimate of \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1; p=4) \).

2. Obtain \( b_0 = \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1; p=16) \).

   Note that \( a \) and \( b_0 \) are obtained by geometrical reasoning, as shown in Fig. 2.

3. Obtain \( b_{<2} = \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1; p=16) \).

   Note that \( a \) and \( b_{<2} \) are obtained by geometrical reasoning, as shown in Fig. 2.

4. Estimate the phase of \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) by computing the argument of the complex number \( y \) defined by

\[
\Re(y) = (4b_0^2 a^2 - 1) = 2;
\Im(y) = (4b_{<2}^2 a^2 - 1) = 2;
\]

(3)

If \( a, b_0 \) and \( b_{<2} \) were the exact values of the amplitudes estimated by the three instances of the AEA, then we would have \( y = \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \). For example, the formula for \( \Re(y) \) may be obtained by geometrical reasoning, as shown in Fig. 2.

5. Estimate \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) as \( e^i a \). The reason for not using \( y \) directly is that if the overlap has amplitude near 1, then the error in the amplitude of \( y \) can be substantially larger than the error in \( a \). (This is because of the way we estimate \( y \) using a PEA; see below.)

We define \( \mathcal{O}_a(\mathcal{U};j^i_2;j^i_1; p) \) to be the value returned by the OEA. A flowchart for the algorithm is depicted in Fig. 3.

When \( a = \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) is close to 1, the absolute precision with which \( a \) is obtained is as much as quadratically better for the same resources. To avoid this nonuniformity of the precision to resource relationship, we define the precision of an overlap by means of a parameterization of \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) using the points \( (\kappa_1; x_2; x_3) \) on the upper hemisphere of the surface of a unit sphere in three dimensions. For this purpose, define \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) = x_3 + i x_2 \) for \( x_2^2 + x_3^2 + x_3^2 = 1 \) and \( x_3 \neq 0 \). Define the distance between \( (\kappa_1; x_2; x_3) \) and \( (\kappa_0; x_0^0; x_0^0) \) to be the angular distance along a great circle. The precision of the value \( \mathcal{O}_a(\mathcal{U};j^i_2;j^i_1) \) is determined by the distance between the liftings \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) and \( \mathcal{A}_a(\mathcal{U};j^i_2;j^i_1) \) (see Fig. 4). We define the precision of the value returned by the AEA similarly, by restricting the parametrization to the positive reals. The precision parameters with which the AEA is called in the OEA are chosen so that the returned overlap has precision \( p \) with respect to our parametrization (see Note [14]).

The AEA is based on a trick for converting amplitude into phase information, so that an efficient PEA can be applied. Let \( j^i_0 = j^i_1 \) and \( j^i_1 = U j^i_1 \). Let \( S_0 = I \) and \( S_1 = U^2 \) be the selective sign change of \( j^i_0 \) and \( j^i_1 \). The composition \( S = S_0 S_1 \) is a unitary operator that rotates \( j^i_0 \) toward \( j^i_1 \) in the two-dimensional subspace \( Q \) spanned by \( j^i_0 \) and \( j^i_1 \). The rotation is by a Bloch-sphere angle of \( \theta = 2 \arccos(\mathcal{A}_a(\mathcal{U};j^i_1;j^i_1)) \). Thus, the eigenvalues of \( S \) in \( Q \) are \( e^i \). The Bloch sphere picture of the states and the rotation are shown in Fig. 5. When \( j^i_0 j^i_1 = j^i_1 j^i_0 = I, S \) is the identity.
FIG. 2: Geometrical construction for computing $\text{Re}(\langle h | U | j \rangle)$ from $a = \langle h | U | j \rangle$ and $2b_0 = |j| + \langle h | U | j \rangle$. According to the law of cosines, $(2b_0)^2 = a^2 + 1 + 2a \cos(\theta)$, and we have $\text{Re}(\langle h | U | j \rangle) = a \cos(\theta) = (2b_0)^2 = a^2 + 1) = 2$.

FIG. 3: OEA flowchart. An estimate of the overlap $\langle h | U | j \rangle$ is obtained. The algorithm requires three state preparations and calls the AEA three times. The amplitude of the returned value shown in the flowchart may need to be adjusted according to the value of $a$ to optimize the precision. For details see the text.
FIG. 4: Visualization of the parameterization of the overlap in terms of points on the upper hemisphere of a unit sphere. The function $h$ is defined by $h(x_1; x_2; x_3) = x_1 + ix_2$. Note that for overlaps $\langle h^ji | h^j0i \rangle$ approaching 1 and small, $^0i$ approaches $^22=2$.

operator. The PEA for $S$ with initial state $j^0i$ determines the phase of one of these eigenvalues, where each of the signs has equal probability of being returned. The overlap $\langle h^ji | h^j0i \rangle$ is obtained from by the formula $\langle h^ji | h^j0i \rangle = \cos(\pi/2)$. The PEA requires use of the conditional $S$ operator, $^0S$. As defined, this needs to be decomposed into a product of $V^0V^0U^V^VU^V^V$. This works because if the controlling qubit is in state $j^0i$, all the $U$'s and $V$'s are canceled by matching $U$'s and $V$'s.

Let $PE(\bar{W}; j^0i; ^0p)$ be a phase returned by the PEA for unitary operator $\bar{W}$ and initial state $j^0i$ with precision goal $^0p$. The AEA may be summarized as follows.

Amplitude estimation algorithm: Given are $U$, $j^0i$ (in terms of a preparation unitary $V : j^0i \langle \bar{\gamma} | j^0i \rangle$) and the goal precision $^0p$. An estimate of $\langle h^ji | h^j0i \rangle$ is to be returned.

1. Let $= PE(\bar{S}; j^0i; 2^0p)$ with $S = S_0S_1 = \bar{V}P_0\bar{V}V^VU^V P_0V^VU^V$.

2. Estimate $\langle h^ji | h^j0i \rangle \cos(\pi/2)j$

The precision parameter for the PEA has the conventional interpretation (modulo 2). Because $\alpha \cos(\langle h^ji | h^j0i \rangle)$ is the angle along the semicircle in the parametrization of the overlap defined above, the precision $2^0p$ of the value returned by the PEA translates directly to the desired precision in the value to be returned by the AEA.

The PEA [3] for a unitary operator $\bar{W}$ and initial state $j^0i$ returns an estimate of the phase ("eigenphase") of an eigenvalue $e^i$ of $\bar{W}$, where the probability of is given by the probability amplitude of $j^0i$ in the $e^i$-eigenspace of $\bar{W}$. In the limit of perfect precision, it acts as a von Neumann measurement of $\bar{W}$ on state $j^0i$ in the sense that the final state is projected onto the $e^i$-eigenspace of $\bar{W}$. For finite precision, the eigenspaces may be decohered and the projection...
is incomplete, unless there are no other eigenvalues within the precision bound. The error in the projection is related to the confidence level with which the precision bound holds.

The original PEA is based on the binary quantum Fourier transform \cite{13}. It determines an eigenphase with precision $\frac{1}{2^n}$ with $2^n$ uses of the conditional $\mathbf{W}$ operator to obtain a phase kickback to ancilla qubits. The original PEA begins by preparing $n$ qubits labeled $1 \cdots n$ in state $|+\rangle \cdots |+\rangle_n$ and system $S$ in state $|0\rangle_S$. Next, for each $m = 1 \cdots n$, $\mathbf{W}$ is applied from qubit $m$ to system $S$ $2^n - 1$ times. The binary quantum Fourier transform is applied to the $n$ qubits, and the qubits are measured in the logical basis $|0\rangle_S; |1\rangle_S$. The measurement outcomes give the first $n$ digits of the binary representation of $(2 - x) = 2^j$, where $j < 1=2$ with probability at least 0.405 \cite{9}.

The PEA as outlined in the previous paragraph makes suboptimal use of quantum resources. We prefer a one-qubit version of the algorithm based on the measured quantum Fourier transform \cite{15} that has been experimentally implemented on an ion trap quantum computer \cite{16}. An advantage of this approach is that it does not require understanding the quantum Fourier transform and is readily related to more conventional approaches for measuring phases. To understand how the algorithm given below works, note that the eigenstates of $\mathbf{W}$ are invariant under $\mathbf{W}$. The only interaction with $S$ is via uses of $\mathbf{W}$. Therefore, without loss of generality, we can assume that $S$ is initially projected to an $e^i$-eigenstate of $\mathbf{W}$ with $0 < 2$. The bits of an approximation of $= (2 - x)$ are determined one by one, starting with the least significant one that we wish to learn. Given $n$, let $\{b_1 \cdots b_n \} = [\prod_{i=1}^{n} b_i = 2^i \text{ (with } b_i = 0, 1) \}$ be a best $n$-digit binary approximation to $= (2 - x)$, where the notation $[x]_b$ is used to convert a sequence of binary digits $x$ to the number that it represents. Write $\mathbf{W} = ( = (2 - x) \text{ )} \{x \cdots b_n \} 2^n$.

**Phase estimation algorithm:** Given are $\mathbf{W}$, $|\psi\rangle$ (as a state of a quantum system) and the goal precision $p$. An estimate of an eigenphase of $\mathbf{W}$ is to be returned, where the probability of is given by the population of $|0\rangle$ in the corresponding eigenspace.

0. Let $n$ be the smallest natural number such that $2^n \ \ \ 1=p$.
FIG. 6: Step 2 of the PEA to estimate bit \( k \) of the eigenphase, where \( k = 3 \). The phase \( \hat{\phi}_k \) is computed according to previously obtained information about the eigenphase. By applying it before the measurement, the probability of obtaining the optimal value for bit \( k \) is maximized. The measurement is denoted by the triangle pointing left with \( + = \) inside and is a measurement in the \( \hat{\mathbf{1}}_j \) basis. The outlined part of the network will be parallelized in Sect. V.

1.a. Prepare \( |+\rangle_a \) in an ancilla qubit \( a \) and apply \( W^{(aS)} \) \( 2^n - 1 \) times. With the auxiliary assumption that \( |\hat{\mathbf{1}}_j\rangle \) is an \( e^{i\hat{\phi}} \)-eigenstate of \( W \), the effect is a phase kickback, changing \( |+\rangle_a \) to \( (|\mathbf{1}_j\rangle + e^{i2\hat{\phi}_k} |\mathbf{1}_1\rangle = \frac{P}{2}. \)

1.b. Measure \( a \) in the \( \hat{\mathbf{1}}_j \) basis, so that measurement outcome \( 0 (1) \) is associated with detecting \( |+\rangle \) \( |\hat{\mathbf{1}}_j\rangle \). Let \( b_0^0 \) be the measurement outcome. With the auxiliary assumption, the probability that \( b_0^0 = b_0 \) is \( \cos (\hat{\phi} = 2\hat{\phi}_k). \)

2 Do the following for each \( k = (n - 1); \ldots; 1; \):

2.a Prepare \( |+\rangle_a \) in an ancilla qubit \( a \) and apply \( W^{(aS)} \) \( 2^{k-1} \) times. With the auxiliary assumption, this changes \( |+\rangle_a \) to \( (|\mathbf{1}_j\rangle + e^{i2\hat{\phi}_k} |\mathbf{1}_1\rangle = \frac{P}{2}. \)

2.b Compensate the phase of \( |\mathbf{1}_1\rangle \) by changing it by \( e^{i2\hat{\phi}_k} \). With the auxiliary assumption, this changes the state of the ancilla to \( (|\mathbf{1}_j\rangle + e^{i2\hat{\phi}_k} |\mathbf{1}_1\rangle = \frac{P}{2}. \)

2.c Measure \( a \) in the \( \hat{\mathbf{1}}_j \) basis to obtain \( b_0^k \). With the auxiliary assumption and if \( b_0^k = b_0 \) for \( l > k \), the probability that \( b_0^k = b_0 \) is \( \cos (\hat{\phi} = 2^{k+1})^2. \)

3 Estimate as \( 2^k b_0^k \).

A step of the algorithm is depicted in Fig. 6.

The probability \( P(\cdot) \) that the value returned by the PEA is \( 2^k b_0^k \) is the product of the probabilities \( \cos (\hat{\phi} = 2) \) for \( l = 1; \ldots; n \) and is bounded below by \( \sin (\hat{\phi} = 2) \). This bound can be obtained by taking the limit \( n \to 1 \) in \( P(\cdot) \). The worst case is given for \( j = 1; 2 \), leading to the bound \( P(\cdot) \approx 2^{-0.405} \). Since the goal precision is \( 2^{-n} \), it is acceptable for the algorithm to obtain the next best binary approximation to \( 2^{-n} \). For this, the value obtained for \( b_0^k \) may
not be the one with maximum probability, but the subsequent bits $l_k^j$ are always the best possible given $b_k^j$. Taking this into account, the probability that the phase returned is within $2^{-n}$ is given by $P(\cdot^0) + P(\cdot^1) = 2^{-2} = 0.25$ (see Note [17]).

The key step of the one-qubit phase estimation procedure is to modify the phase kickback by the previously obtained phase estimate. This differentiates it from an adaptive phase measurement $P_E(x)$ or pulse time. In [1], which approximates what is done in practice for the efficient determination of an unknown frequency or pulse time. This is the phase estimation method given in [18] and mentioned in [1], which approximates what is done in practice for the efficient determination of an unknown frequency or pulse time.

The resources required by the PEA, AEA and OEA can be summarized as follows.

$P_E(\omega; j \oplus \mathbf{p})$: This requires $N = 2^{d \log_2 (1-\mathbf{p})}$ uses of $\omega$. $\oplus \mathbf{p}$ is prepared once. Here, $d \mathbf{p}$ denotes the least integer in $x$.

$A_E(U; j \oplus \mathbf{p})$: This calls $P_E$ once. It requires $N = V P_0 V^Y U V P_0 V^Y U^Y$ and one use of $V$ to prepare the initial state. We count this as being equivalent to $4N$ ($\mathbf{p}$) + 1 state preparations and $2N$ ($\mathbf{p}$) applications of $U$.

$O_E(U; j \oplus \mathbf{p})$: This contains three calls to the AEA with higher precision. The total resource count is $8N$ ($\mathbf{p}=8$) + $4N$ ($\mathbf{p}=2$) + 3 state preparations and $4N$ ($\mathbf{p}=8$) + $2N$ ($\mathbf{p}=2$) uses of $U$.

Since $N = \mathbf{p}$ is of order $1=\mathbf{p}$, each of these algorithms uses resources of order $1=\mathbf{p}$.

### III. CONFIDENCE BOUNDS

The PEA as described in the previous section obtains an estimate $\hat{E}$ of an eigenphase $\phi$ such that the prior probability that $\hat{E} < 2^{-n+1}$ is at least $0.25$, regardless of the value of $n$. (The comparison of $\hat{E}$ to $\phi$ is modulo $2^1$, so that $\hat{E} < 2^{-n+1}$ is angular distance between $e^{i \hat{E}}$ and $e^{i \phi}$.) Thus, after having obtained $\hat{E}$, we say that $\hat{E} < 2^{-n+1}$ with confidence level $0.25$ or $P[\hat{E} < 2^{-n+1}] = 0.25$. The error bound of $2^{-n+1}$ must not be confused with a standard deviation. Suppose that we use a single sample from a gaussian distribution with standard deviation to infer the mean. We would expect that the confidence level increases as $1 - e^{(-\cdot)^2}$ for an error bound of $\sigma$. (The notation $\sim$ means a quantity asymptotically bounded below by something proportional to $x$, that is, there exists a constant $C > 0$ such that the quantity is eventually bounded below by $C x$.) In general, it is desirable to have confidence levels that increase at least exponentially as a function of distance or as a function of additional resources used. Unfortunately, for a single instance of the PEA, we cannot do better than have confidence level $1 - (1 = \mathbf{p})$ for $\hat{E} < 2^{-n+1}$ [5]. (Here, $\mathbf{p}$ denotes a quantity that is of order $x$, that is a quantity that is eventually bounded above by $C x$ for some constant $C$. The meaning of “eventually” depends on context. Here it means “for sufficiently small $x$”. If the asymptotics of the argument require that it go to infinity, it means “for sufficiently large $x$”.) The method suggested in [5] for increasing the confidence level is to use the PEA with a higher goal precision of $\mathbf{p}=2^1$. However this improves the confidence level on $\hat{E} < 2^{-n+1}$ to only $1 - (1 = (2^1))$ and requires a $2^1$ resource overhead, which is not an efficient improvement in confidence level.

A reasonable goal is to attain confidence level $c = 1 - (c)$ that $\hat{E} < 2^{-n+1}$ with a resource overhead of a factor of $\mathbf{p}$ ($\mathbf{p}$). This modifies the resource counts from the previous
Modified Phase estimation algorithm: Given are \( W \), a goal precision \( p \), and a goal confidence level \( c \). An eigenphase of \( W \) is to be returned, where the probability of is given by the population of \( j \cdot \frac{\pi}{3} \) in the corresponding eigenspace. The final state of \( S \) consists of states with eigenphases in the range \( p \) with prior probability at least \( c \).
0. Let \( n \) be the smallest natural number such that \( 2^n \leq 1 = p \). Let \( r \) be the smallest natural number such that \( x(n; r) < (1 - \epsilon) \).

1. Obtain \( \theta_{\text{est}}^0 \) with the two sets of \( r \) measurements described above. Let \( a_n = 1 \) if \( \theta_{\text{est}}^0 \) is closer to \( \epsilon \) than 0 and \( a_n = 0 \) otherwise.

2. Do the following for each \( k = (n \ 1); \ldots; 1 \), in this order:
   
   2.a Obtain an estimate of the \( k \)'th bit \( a_k \) of a binary approximation to \( \theta = (2 \ ) \) by \( r \) repetitions of the measurement of the \( k \)'th bit of \( \theta_{\text{est}}^0 \) as an argument. Because the OEA has three independent calls to the AEA, it needs to make these calls with confidence level arguments of \( 1 \ (1 - c) = 3 \) to ensure that the final confidence level is \( c \). The resource requirements of all three algorithms are \( O (\log(1 - c) j = p) \), where this applies to both the uses of \( \theta \) and of the state preparation operator \( V \) in the case of the AEA and OEA.

3. Return 2 \([a_1 ; : : ; a_n ]\).

We define \( PE(0; j 0; j) \) to be the value returned by the modified PEA.

The resources required grow by a factor of less than \( 2r \), where \( r = O (\log (1 - c) j) \). The constant hidden by the order notation may be determined from the expression for \( r \) in step 0 and is not very large. To modify the AEA to attain confidence level \( c \), it suffices to change the call to \( PE \) by including \( c \) as an argument. Because the OEA has three independent calls to the AEA, it needs to make these calls with confidence level arguments of \( 1 \ (1 - c) = 3 \) to ensure that the final confidence level is \( c \). The resource requirements of all three algorithms are \( O (\log (1 - c) j = p) \), where this applies to both the uses of \( \theta \) and of the state preparation operator \( V \) in the case of the AEA and OEA.

**IV. EXPECTATION ESTIMATION**

Let \( A \) be an observable and assume that it is possible to evolve under \( A \) for any amount of time. This means that we can implement the unitary operator \( e^{iA} \) for any \( t \). The traditional idealized procedure for measuring \( \lambda = \text{tr}(A) \) is to adjoin a system consisting of a quantum particle in one dimension with momentum observable \( \varphi \) and apply the coupled evolution \( e^{iA} \varphi \) to the initial state \( \psi \) where \( \psi \) is the position “eigenstate” with eigenvalue 0. Measuring the position of the particle yields a sample from the distribution of eigenvalues of \( A \) \([5, 20] \).

This procedure requires unbounded energy, both for preparing \( \psi \) and to implement the coupled evolution. Performing this measurement \( N \) times yields an estimate of \( \lambda \) with precision of order \( \sqrt{\lambda} = \frac{2}{N} \), where the variance is \( \text{var}(\lambda) = \lambda \text{tr}(A) )^2 \). It is desirable to improve the precision and to properly account for the resources required to implement the coupling.

We focus on measurement methods that can be implemented in a quantum information processor. In order to accomplish this, some prior knowledge of the distribution of eigenvalues of \( A \) with respect to \( \lambda \) is required. Suppose we have an upper bound \( b \) on \( \text{tr}(A) \) and a bound on the tail distribution \( F(\ ) \text{tr}(A \ hAJ > ) \), where \( [A \ hAJ > \) denotes the projection operator onto eigenspaces of \( A \) with eigenvalues satisfying \( j \ hAJ > \). That is, \( F(\ ) \ 

\( j \ hAJ > \) with \( p = \text{tr}(j \ hAJ ) \). Without loss of generality, \( F \) is non-increasing in \( \lambda \). An estimate on the tail distribution is needed to guarantee the confidence bounds on \( \text{tr}(A) \) derived from measurements by finite means. Here are some examples: If the maximum eigenvalue of \( A \) is \( m_{\text{ax}} \), we can set \( b = m_{\text{ax}} \) and use \( F(\ ) = 1 \) if \( < m_{\text{ax}} \) and \( F(\ ) = 0 \), otherwise. Suppose that we have an upper bound \( v \) on the variance \( \text{var}(\lambda) \). If we know that the distribution of eigenvalues of \( A \) is gaussian, we can estimate \( F(\ ) \) by means of the error function for gaussian distributions. With no such prior knowledge, the best estimate is \( F(\ ) = m \ln (1; v = 1) \). (Observe
that $v^{2/p} \propto t^{p/p}$.) Such “polynomial” tails result in significant overheads for measuring $\mathfrak{H}$. “Good” tails should drop off at least exponentially for large $t$ (“exponential tails”).

We give an EEA based on overlap estimation. The relevant resources for the EEA are the number $M$ of times a unitary operator of the form $e^{iA t}$ is used, the total time $T$ that we evolve under $A$, and the number $N$ of preparations of $A$. The total time $T$ is the sum of the absolute values of exponents $t$ in uses of $e^{iA t}$. For applying the OEA, it is necessary to be able to evolve under $A$ as well as $\mathfrak{H}$. If the evolution is implemented by means of quantum networks, this poses no difficulty. However, if the evolution uses physical Hamiltonians, this is a nontrivial requirement. The complexity of realizing $e^{iA t}$ may depend on $t$ and the precision required. Since this is strongly dependent on $A$ and the methods used for evolving under $A$, we do not take this into consideration and assume that the error in the implementation of $e^{iA t}$ is sufficiently small compared to the goal precision. In most cases of interest this is justified by results such as those in [21], which show that for a large class of operators $A$, $e^{iA t}$ can be implemented with resources of order $t^{2+0} = O(1)$, where $0$ is the error of the implementation and $0$ is arbitrarily small.

For exponential tails $F$, our algorithm achieves $M; N = O(L=\text{to the }\text{th}^2)$ and $T = O(L=\text{to the }\text{th}^2)$ for arbitrarily small $L$. The order notation hides constants and an initialization cost that depends on $b$ and $F$. The strategy of the algorithm is to measure tr$(e^{iA t})$ for various $t$. In the limit of small $t$, $tr(e^{iA t}) = 1 + O(t^2) \exp(A) + O(t^2)$, so that $\mathfrak{H}$ can be determined to $O(t^2)$ from the imaginary part of $tr(e^{iA t})$. The first problem is to make an initial determination of $\mathfrak{H}$ to within a deviation of $A$ as determined by $F$. This is an issue when $b$ is large compared to the deviation. To solve the first problem, we can use phase estimation. We also give a more efficient method based on amplitude estimation. The second problem is to avoid excessive resources to achieve the desired precision while making $t$ small. To solve this problem requires choosing $t$ carefully and taking advantage of higher-order approximations of $\mathfrak{H}$ by linear combinations of tr$(e^{iA t})$ for different times $t$.

To bound the systematic error in the approximation of $\mathfrak{H}$ by $\mathfrak{H}$, note that $\mathfrak{H}$ is a sum of the complex form of $\mathfrak{H}$. This bound suffices for achieving $L=2$ in the bounds on $M$ and $N$. Reducing requires a better approximation, which we can derive from the Taylor series of the principal branch of $\log(x + 1)$. For $|x| < 1$,

$$j \log(x + 1) = (1 + x^k, j) = k + 1 = (k + 1 + 1)(\log(j + x)^{K+1}) k = 1$$

To apply these series to the problem of approximating $\mathfrak{H}$, we compute

$$C_1 e^{iB x} = \sum_{k=1}^{\infty} (1 + x) e^{iB x} = \sum_{k=1}^{\infty} (1 + x) e^{iB x}$$

for real constants $C_1$ satisfying $C_1 j = 2^k$. In particular, if $B$ is an operator satisfying $B < x=t$, we can estimate

$$\sum_{k=1}^{\infty} (1 + x) e^{iB x} = \sum_{k=1}^{\infty} (1 + x) e^{iB x}$$

Define $G_e(x) = F(x) + \sum_{k=1}^{\infty} F(x) ds$. Then $G_e(x)$ is an upper bound on the contribution to the mean from eigenvalues of $A$ that differ from the mean by more than $0$. That is, $G_e(x)$
We assume that a non-increasing bound $G(\cdot)$ is known and that $G(\cdot)$ is non-increasing. Because $F(\cdot) = G(\cdot)$, we can use $G$ to bound both $G(\cdot)$ and $F$. For $x > 0$, define $G^{-1}(x) = \inf \exists (\cdot) \gg x$. The behavior of $G^{-1}$ as $x$ goes to 0 determines the resource requirements for the EEA. If $A$ is a bounded operator with bound $\max$, then we can use $G^{-1}(x) = \max$ independent of $x > 0$. If $F$ is exponentially decaying, then so is $G$, and $G^{-1}(x) = O(j\log(\chi))$. For polynomial tails with $F(\cdot) = O(1=2^x)$, we have $G(\cdot) = O(1=1^x)$ and $G^{-1}(x) = O(1=x^{1/4})$.

The EEA has two stages. The first is an initialization procedure to determine $\rho A |i$ with an initial precision that is of the order of a bound on the deviation of $A$ from its mean, where the deviation is determined from $F$ and $G$. This initialization procedure involves phase estimation to sample from the eigenvalue distribution of $A$. Its purpose is to remove offsets in the case where the expectation of $A$ may be very large compared to the width of the distribution of eigenvalues as bounded by $F$ and $G$. The second stage zooms in on $\text{tr}(\rho A |i)$ by use of the overlap estimation procedure. As before, we can assume without loss of generality that $\rho = j\rho_j$. We first give a version of the EEA that achieves $M; N = O(1=p^{3=2})$ and then refine the algorithm to achieve better asymptotic efficiency.

**Expectation estimation algorithm:** Given are $A$, $j\rho_j (\text{in terms of a preparation unitary } V:$ $\rho_i \rho_j j\rho_j)$, a goal precision $p$ and the desired confidence level $c$. The returned value is within $p$ of $\rho A |i = \text{tr}(\rho A |ih j)$ with probability at least $c$.

**Stage I.**

1. Choose such that $F(\cdot) < 1=4$ and $p$ should be chosen as small as possible. Let $t_i = (4j \rho_i + \cdot)$. Let $x$ be the minimum natural number such that $2e^{-x} = 4-2^x$. Let $c_d$ according to the identity $r(1-c_d) = (1-c_d) = 4$.

2. Obtain $\rho_i \rho_j j\rho_j$ from $x$ instances of the PEA, $k = PE(\epsilon i \rho_i ; j \rho_j ; t_i ; t_l = 2;c_d)$, where 2 is subtracted for any return values between and 2 to ensure that $k <$.

3. Let $m$ be the median of $\rho_i \rho_j j\rho_j$. We show below that the probability that $j = t_i + \rho A |i > j\rho_j$ is bounded by $2e^{-x} + x(1-c_d) = 2$.

4. Let $a_0 = m - t_i$. We expect $a_0$ to be within of $\rho A |i$ with confidence level $1 (1-c_d) = 2$.

**Stage II.** If $p = \cdot$, return $a_0$ and skip this stage.

1. Choose $m$ and $t$ so that they satisfy

$$
\begin{align*}
(A) & \quad \frac{3}{m} = 6, \\
(B) & \quad G(\cdot) = \frac{m}{m} = 4; \\
(C) & \quad \frac{m}{m} = 1; \\
(D) & \quad \frac{t}{m} = \cdot.
\end{align*}
$$

The constraints and how they can be satisfied are explained below. The parameter $t$ should be chosen as large as possible to minimize resource requirements.

1. Obtain $x = OE(\epsilon i \rho_j a_0 ; t = 2); j \rho_j$; $(t = 2)p = 4; 1 (1-c_d) = 2$.

2. Return $\rho A |i = (t = 2) + a_0$. 

\[ \text{tr}(\rho A h A |i j\rho j j\rho j >) = \frac{p}{j} h A |i j\rho j j\rho j . \]
Consider stage I of the algorithm. The probability that \( j_m = t_i + h A \lambda j \geq 0 \) may be bounded as follows. The choice of \( t_i \) ensures that eigenvalues of \( A t_i \) within \( t_i \) of the mean are between \( -4 \) and do not get “aliased” by \( e^{\lambda t_i} \) in the calls to the PEA. With probability at least \( 1 - x(1 - c^2) \), each \( k \) returned by these calls is within \( t_i = 2 \) of an eigenvalue of \( A t_i \) sampled according to the probability distribution induced by \( j \). Assume that the event described in the previous sentence occurred. The probability that \( j_m = t_i + h A \lambda j \geq 0 \) is upper bounded by the probability that at least \( dx = 2e \) of the \( x \) samples fall outside the range \([ h A t_i, t_i; h A t_i + t_i \] \). The choice of \( t_i \) with respect to \( F \) implies that Hoeffding’s bound can be applied to bound this probability by \( 2e^{-x^2} \) Thus, we can bound the overall prior probability \( P \) that \( j_m = t_i + h A \lambda j \geq 0 \) by \( P < 2e^{-x^2 + x(l - c^2)} \). Constraints (B) and (C) of Eq. (8) together with \( 1^{\lambda t_i} \) not being zero and is bounded by \( 3 A_{\text{max}} = 6(t_i = 2) \) is \( P = 4 \) (constraint (A) of Eq. (8)). The second and third come from eigenvalues of \( A_{\text{max}} = 2 \) outside \([ h A t_i, t_i; h A t_i + t_i \] \) which is why we need constraint (D) of Eq. (8). The first arises from eigenvalues of \( A_{\text{max}} = 2 \) in \([ m_{\text{max}}, m_{\text{max}} \] \) due to \( 3 A_{\text{max}} = 6(t_i = 2) \) is \( P = 4 \) (constraint (A) of Eq. (8)). Consider stage II of the algorithm. The error \( j \) of \( \Delta = t_i \) is within a factor of 2 of \( 2x \). Constraints (B) and (C) of Eq. (8) imply that the contribution to \( h A \lambda j \) of eigenvalues differing from the mean by more than \( m_{\text{max}} = 2(t_i = 2) \) is at most \( m_{\text{max}} = 8 \). However the same eigenvalues still contribute to the measurement, each contributing at most 1 to \( x \). Constraint (B) of Eq. (8) together with the inequality \( F(\cdot) \) of Eq. (8) imply that \( F(\cdot) \) has probability at most \( 2 \) so this contribution has probability at most \( 2 \) and therefore adds at most another \( P = 4 \) (after dividing by \( t_i = 2 \)) to the approximation error. Thus, the combination of the approximation and precision error is less than \( p \), as desired. Clearly these estimates are suboptimal, tighter choices of \( m_{\text{max}} \) and \( t_i \) could be made. However, this does not affect the asymptotics of the resource requirements.

To find good solutions \( m_{\text{max}} = 2 \) and \( t_i \) subject to the constraints given in Eq. (8), we can rewrite the constraints as follows:

\[
\begin{align*}
(A') & \quad G \quad (m_{\text{max}} = 8) \quad m_{\text{max}} = t_i \quad (p = 8) = (m_{\text{max}} = 6); \\
(B') & \quad m_{\text{max}} = t_i; \quad m_{\text{max}} = t_i.
\end{align*}
\]
To satisfy these constraints, we first find $m_{\text{ax}} = 1$ as large as possible so that

$$G^{1} (m_{\text{ax}} p=8) (p=8) = (\frac{2}{m_{\text{ax}}} = 6);$$

and then set $t = m_{\text{ax}} = G^{1} (m_{\text{ax}} p=8)$. Consider the three examples of bounded, exponential and polynomial tails. For the case of bounded tails, constraint (A’’) of Eq. (10) can be solved by setting $m_{\text{ax}}$ according to $m_{\text{ax}} = (p=8) = (\frac{2}{m_{\text{ax}}} = 6)$, so that $m_{\text{ax}} = (3p=(4 m_{\text{ax}}))^{1+2}$. The parameter $t$ is given by $m_{\text{ax}} = m_{\text{ax}} = (3p=(4 m_{\text{ax}})^{1+2} = (p^{1+2})$. For the case of exponential tails, we can use $G^{1} (\alpha) = O ((j \log (\alpha))^{j^{1+2}})$ and $t = (p^{1+2} = j \log (p))^{j^{1+2}}$ (see Note [22]). For polynomial tails with $G^{1} (\alpha) = O (\alpha^{1+2})$, we get $m_{\text{ax}} = (p^{2+} = (1+2))$ and $t = (p^{5+6} + 2j = (1+2)^j)$ (see Note [23]).

The resource requirements for stage II of the EEA can be estimated as $M = O ((j \log (1+c) \geq p))$, uses of an exponential of the form $e^{i A}$, $N = O ((j \log (1+c) \geq p)$ state preparations, and a total time of $T = O ((j \log (1+c) \geq p)$, in terms of the parameter $t$ computed in step 0 (of stage II). The dependence on $\alpha$ is now up in the value of $t$. With $t$ as computed in the previous paragraph, for bounded $A$, $M$ and $N$ are $O ((j \log (1+c) \geq p^{3+2})$. For exponential tails, $M$ and $N$ are $O ((j \log (1+c) \geq (p=j \log (p))^{3+2})$. For polynomial tails, they are $O ((j \log (1+c) \geq (p^{1+2}))$, where $(p)$ is a polynomial satisfying $(p) = 1 + 1 + 2$ for $l = 1 + 1 + 5$ for $l = 0$.

To reduce the resource requirements of stage II of the EEA, we use overlap estimation at multiple values of $t$ and Eq. (6). Here is the modified stage. We assume that $K = 2$.

Stage II’.

0. Choose $m_{\text{ax}}$ and $t$ so that they satisfy

$$A^{1} \quad (m_{\text{ax}} p=8) \quad (p=8) = (\frac{2}{m_{\text{ax}}} = 6);$$

and then set $t = m_{\text{ax}} = G^{1} (m_{\text{ax}} p=8)$. Consider the three examples of bounded, exponential and polynomial tails. For the case of bounded tails, constraint (A’’) of Eq. (10) can be solved by setting $m_{\text{ax}}$ according to $m_{\text{ax}} = (p=8) = (\frac{2}{m_{\text{ax}}} = 6)$, so that $m_{\text{ax}} = (3p=(4 m_{\text{ax}}))^{1+2}$. The parameter $t$ is given by $m_{\text{ax}} = m_{\text{ax}} = (3p=(4 m_{\text{ax}})^{1+2} = (p^{1+2})$. For the case of exponential tails, we can use $G^{1} (\alpha) = O ((j \log (\alpha))^{j^{1+2}})$ and $t = (p^{1+2} = j \log (p))^{j^{1+2}}$ (see Note [22]). For polynomial tails with $G^{1} (\alpha) = O (\alpha^{1+2})$, we get $m_{\text{ax}} = (p^{2+} = (1+2))$ and $t = (p^{5+6} + 2j = (1+2)^j)$ (see Note [23]).

The resource requirements for stage II of the EEA can be estimated as $M = O ((j \log (1+c) \geq p))$, uses of an exponential of the form $e^{i A}$, $N = O ((j \log (1+c) \geq p)$ state preparations, and a total time of $T = O ((j \log (1+c) \geq p)$, in terms of the parameter $t$ computed in step 0 (of stage II). The dependence on $\alpha$ is now up in the value of $t$. With $t$ as computed in the previous paragraph, for bounded $A$, $M$ and $N$ are $O ((j \log (1+c) \geq p^{3+2})$. For exponential tails, $M$ and $N$ are $O ((j \log (1+c) \geq (p=j \log (p))^{3+2})$. For polynomial tails, they are $O ((j \log (1+c) \geq (p^{1+2}))$, where $(p)$ is a polynomial satisfying $(p) = 1 + 1 + 2$ for $l = 1 + 1 + 5$ for $l = 0$.

To reduce the resource requirements of stage II of the EEA, we use overlap estimation at multiple values of $t$ and Eq. (6). Here is the modified stage. We assume that $K = 2$.

Stage II’.

0. Choose $m_{\text{ax}}$ and $t$ so that they satisfy

$$A^{1} \quad (m_{\text{ax}} p=8) \quad (p=8) = (\frac{2}{m_{\text{ax}}} = 6);$$

and then set $t = m_{\text{ax}} = G^{1} (m_{\text{ax}} p=8)$. Consider the three examples of bounded, exponential and polynomial tails. For the case of bounded tails, constraint (A’’) of Eq. (10) can be solved by setting $m_{\text{ax}}$ according to $m_{\text{ax}} = (p=8) = (\frac{2}{m_{\text{ax}}} = 6)$, so that $m_{\text{ax}} = (3p=(4 m_{\text{ax}}))^{1+2}$. The parameter $t$ is given by $m_{\text{ax}} = m_{\text{ax}} = (3p=(4 m_{\text{ax}})^{1+2} = (p^{1+2})$. For the case of exponential tails, we can use $G^{1} (\alpha) = O ((j \log (\alpha))^{j^{1+2}})$ and $t = (p^{1+2} = j \log (p))^{j^{1+2}}$ (see Note [22]). For polynomial tails with $G^{1} (\alpha) = O (\alpha^{1+2})$, we get $m_{\text{ax}} = (p^{2+} = (1+2))$ and $t = (p^{5+6} + 2j = (1+2)^j)$ (see Note [23]).

The parameter $t$ should be chosen as large as possible to minimize resource requirements.

1. For $l = 1; \ldots; K$, obtain $y_{l} = O (e^{i A} a_{l}) (l=2); j = 1$; $(t=2)p = (4K 2^{K}) (l = 1, c) = (2K))$. Let $y_{0} = 1$.

2. Return $\text{Im} (\sum_{l=0}^{K} C_{l} y_{l}) = (t=2) + a_{0}$.

The precisions and the confidence levels in the calls to the OEA have been adjusted so that the final answer has the correct precision and confidence level. The explanation for this is similar to that for the original stage II (see Note [24]).

The earlier method for finding $m_{\text{ax}}$ and $t$ is readily adapted to the constraints in stage II’. Constraint A’’ of Eq. (10) now reads as

$$A^{1} \quad (m_{\text{ax}} p=8) \quad (p=8) = (\frac{2}{m_{\text{ax}}} = 6);$$

and we can set $t = m_{\text{ax}} = G^{1} (m_{\text{ax}} p=8)$. To simplify the right hand side of Eq. (12), we add the inequality $m_{\text{ax}} = (1=K + 1)$, and use the inequality $1=4 \quad (2=3) (1=K + 1) K^{1+1}$ (for $K = 2$) to replace the right hand side by $(p=32) (K + 1) = m_{\text{ax}}$. Thus for bounded tails, $m_{\text{ax}} = (\infty (1=K ; p^{1+K}))$ and $t = (\infty (1=K ; p^{1+K}))$, where we give the asymptotic dependence on $K$ explicitly but suppress parameters not depending
on \( K \) or \( p \) (see Note [25]). For exponential tails, \( m_{ax} = (m \in (1=K; (p=j \log \phi) j^{1-K})) \) and \( t = (m \in (1=K (j \log \phi) j + K)) ; p^{1-K} = (j \log \phi) j^{1-K} (j \log \phi (p) j + K))) \) (see Note [26]). For polynomial tails with exponent \( t \), \( m_{ax} = (m \in (1=K ; p^{2^K j^{1-K}} (1+K))) \) and \( t = (m \in (1=K \phi^{(1+K)}) ; M ; N = \phi^{1-(1+K)} + 1) \)) (see Note [27]).

With the expressions from the previous paragraph, we can estimate the resources requirements of stage II'. In terms of \( t, M \) and \( N \) are \( (K - 2^K j \log (1 + c) j \log p - p) \), and \( T = (K - 2^K j \log (1 + c) j \log p) \), where the powers of \( K \) account for the \( K \) calls to the OEA, the coefficient in the denominator of the precision, and in the factor of 1 in the evolution time. For bounded tails, we obtain \( M ; N = (j \log ((1 + c)) \phi^{3K + \frac{1}{2} + l o g K}) \), where we have loosely increased the power of \( K \) by 1 to account for the upper bound of \( (1=K) \) on \( t \). For exponential tails, \( M ; N = (j \log ((1 + c) = K)) \phi^{4K + \frac{1}{2} + l o g K} \) (with appropriate increases in the power of \( K \)), and for polynomial tails, \( M ; N = (j \log ((1 + c) = K)) \phi^{4K + \frac{1}{2} + l o g K} \) (with conservative increases in the power of \( K \) and the exponent of 2), where \( (K \) approaches \( 1 + l = (1 + t) \) for large \( K \). Note that for \( t = 0 \), this approaches the “classical” resource bound as a function of precision.

The final task of this section is to modify stage I so that the dependence of the resource requirements on \( b \) is logarithmic rather than linear in \( b \). The basic idea is to use logarithmic search to reduce the uncertainty in \( hA \) to \( \delta \). Define \( q \) by \( b = q \).

Stage I'.

0. Chose minimal so that \( G (x) = 6 \) and \( F (x) \leq 18 \). Set the initial estimate of \( hA \) to \( a = 0 \) and the initial precision to \( p_a = b = q \).

1. Repeat the following until \( p_a \):

1.a. Set \( t = 1 = (p_a + \phi) \) and obtain \( x = \phi (e \phi \ A (x)) ; j i = 18; j (1 + c) = \phi (e (2 \log \phi (q) e)). \)

1.b. Update \( a \) and \( p_a \) according to the assignments \( a = a + \phi \) and \( p_a = p_a + \phi 6 + (5=18) \) (5=18).

We claim that at the end of this stage, we have determined \( hA \) to within \( 1 + c = 2 \), so that we can continue with the second stage, as before. To verify the claim, it is necessary to confirm that at the end of step 1.b., the updated estimate \( a \) of \( hA \) has precision \( p_a \). The error in \( a \) can be bounded as we have done for stage II. Let \( a_0 \) be the estimate of \( A \) used in the call to the OEA. There is an error of less than \( 1 = (1 = t) = (p_a + \phi) = 18 \) due to precision of \( x \) in the call to the OEA. The remaining error is due to the approximation of \( tr (\phi A a_0) t \phi \) by \( \phi A a_0 ) t \phi \). For eigenvalues of \( A \) within \( 1 = t = a \), this is bounded by \( j t + \phi \) \( (q = 1) j = 6 \), which translates into an approximation error of at most \( 1 = (t + \phi) = (p_a + \phi) = 6 \). Eigenvalues of \( A \) further from \( a \) than \( 1 = t = p_a + \phi \) are at least from \( hA \). This requires the inductive assumption that \( p_a = hA a_0 \). The contribution to the mean from such eigenvalues is bounded by \( = 6 \), and the bias resulting from their contribution to \( x \) is at most \( F (x) = p_a + \phi \) = 18. Adding up the errors gives the \( p_a \) computed in step 1.b. The confidence levels in the calls to the OEA are chosen so that the final confidence level is \( 1 = (t + \phi) = 2 \). To see this requires verifying that the number of calls of the OEA is at most \( 2 \log \phi (q) e \). It suffices to show that if \( p_a = 2 \), then \( 6 + (5=18) + p_a = 2 \). Rewrite the left hand side as \( (8=18) + (5=18) p_a = 2 \), which for \( p_a = 2 \) is less than \( (4=18) p_a + (5=18) p_a = p_a = 2 \).

Each call to the OEA in stage II' has constant precision, which implies that \( M \) and \( N \) are both \( O (\log q) \) for large \( q \) The total time \( T \) is \( O (l = 1) \).
FIG. 7: Parallelization of the PEA algorithm to estimate the bit $k = 3$ of the phase. This replaces the outlined parts of the network in Fig. 6. $E$ is an entangler such that $E$ $j\ i\ 0\ a = (j\ 0\ i\ a + j\ 1\ i\ a)\ 1\ 2$, and $E$ $j\ i\ 0\ a = 0\ i\ a$ $0\ j\ a = 1\ 2$. $E^{-1}$ is the decoding operation that maps $E^{-1} j\ i\ a = 0\ i\ a$ $j\ 0\ a$. The $k$’th bit is estimated from the measurement outcome of the first ancilla qubit in the logical basis.

V. PARALLELIZABILITY

To what extent are the algorithms given in the previous sections parallelizable? Consider the OEA. At its core is the PEA with a unitary operator $S$ that has two eigenvalues $e^\ i$ on the relevant state space. In the sequential implementation, one of the eigenvalues is eventually obtained with the desired precision. Which eigenvalue is returned cannot be predicted beforehand. The initial state is such that each one has equal probability. If it is possible to deterministically (or near-deterministically) prepare an eigenstate $j\ i$ with (say) eigenvalue $e^\ i$ using sufficiently few resources, then we can use the entanglement trick in [11] to parallelize the algorithm. Instead of applying $V$ sequentially $2^k$ many times to determine bit $k$ of the phase, we prepare the entangled state $(J:\ 0\ i\ a + J:\ 1\ i\ a)\ 2^k$ on $2^k$ ancilla qubits and $2^k$ copies of $j\ i$. We next apply $S$ between the $j$’th ancilla and the $j$’th copy of $j\ i$ and then make a measurement of $(J:\ 0\ i\ a + J:\ 1\ i\ a)\ 2^k$. On a quantum computer, the measurement requires decoding the superposition into a qubit, which can be done with $O(2^k)$ gates. The decoding procedure can be parallelized to reduce the time to $O(k)$ (see Note [28]). Using this trick reduces the time of the PEA to $O(\log(1/p))$ (the number of bits to be determined), counting only the sequential uses of $U$ and ignoring the complexity of preparing the initial states $j\ i$ and the decoding overhead in the measurement. The repetitions required for achieving the desired confidence level are trivially parallelizable and do not contribute to the time. It is possible to reduce the time from $O(\log(1/p))$ to $O(1)$ by avoiding the feed-forward phase correction used in the algorithm and reverting to the algorithm in [18] and mentioned in [1].

Based on the discussion in the previous paragraph, the main obstacle to parallelizing the OEA
is the preparation of $j\;i$. If $\theta = 2\arccos(jr/S)$ is not close to 0, $j\;i$ can be prepared near deterministically with relatively few resources as follows. Suppose we have a lower bound on $\theta$. With the original initial state, use sequential phase estimation with precision $\theta/2$ and confidence level 1 to determine whether we have projected onto the eigenstate $j\;i$ with eigenvalue $e^i$ or the one with $e^{-i}$. The occurrence of $p$ in the confidence level accounts for the total number of states that need to be prepared. The parameter $B$ is a constant that provides an additional adjustment to the confidence level. It must be chosen sufficiently large, and other confidence level parameters must be adjusted accordingly, to achieve the desired overall confidence level.

If we have projected onto $j\;i$, return the state. If not, either try again, or adapt the parallel PEA to use the inverse operator $S^y$ instead of $S$ for this instance of the initial state. The (sequential) resources required are of the order of $j\log((1-\cos\theta))\frac{\pi}{2}$, but all the needed states can be prepared in parallel. For $\alpha$, the time required by the parallel PEA is increased by a factor of $O(j\log((1-\cos\theta))\frac{\pi}{2})$. The parallel overlap estimation for a unitary operator $U$ based on these variations of phase estimation thus requires $O(j\log((1-\cos\theta))\frac{\pi}{2})$ time, provided $\theta$ is not too close to 1.

For $\theta$ not close to 1, the OEA is intrinsically not parallelizable without increasing the total resource cost by a factor of up to $O(\frac{\pi}{2})$. This is due to the results in [29], where it is shown that Grover’s algorithm cannot be parallelized without reducing the performance to that of classical search. For example, consider the problem of determining which unique state $j\;i$ of the states $j\;i \cdots j\;i$ has its sign flipped by a “black-box” unitary operator $V$. This can be done with $n$ many uses of the OEA by preparing the states $j\;i \cdots j\;i$ that are uniform superpositions of the $j\;i$ for which the number $i$ has 1 as its $b$'th bit. If $h_{b}j\;j\;i\;i = 1=2n^{-1}$, then the $b$'th bit of $k$ is 1. If $h_{b}j\;j\;i\;i = 0$, then it is 0. It suffices to use an unparametrized (Fig. [4]) precision of $1=2n^{-1}$ and confidence level sufficiently much bigger than 1 for $n$. Because $j\;i \cos(\frac{\pi}{2})j\;i = 0$ (3), the parameterized precision required is $O(1=2n^{-2})$. (\(x\)) is a quantity that is both $O(x)$ and $O(2n^{-2})$ sequential resources suffice, which is close to the optimum attained by Grover’s algorithm. However, the results of [29] imply that implementing quantum search with depth (sequential time) $d$ requires $O(2n^d)$ uses of $V$ for $d < 2n^{-2}$. This implies that to achieve a parameterized precision of $O(1=2n^{-2})$ for $1 \neq j\;j\;i\;i = 0 (1=2n)$ using time $O(2n^{-2}\;P)$ requires $O(2n^{-2}\;P)$ resources.

The EEA was described so that overlap estimation is used with small $\theta$, and therefore can not be immediately parallelized without loss of precision or larger resource requirements. However, for the version of overlap estimation needed for stages I’ and II’, it is only the imaginary part of the overlap that is needed, and the parameters are chosen so that the overlap’s phase is expected to be within 1 of 0 (because $m_{ax} = 1$). The actual precision required is absolute in the overlap, not the parameterization of the overlap in terms of the upper hemisphere in Fig. [4]. This implies that we can call the parallel overlap algorithm with an intentionally suppressed overlap. If the desired overlap is $h_{b}j\;j\;i\;i$, one way to suppress it is to replace $U$ by $U^{\frac{\pi}{2}}$ and the initial state by $|1\rangle = 2j\;\vec{x}$, $j\;\vec{y}$. The suppression ensures that the phases in the calls to the PEA are sufficiently distinguishable to allow the near deterministic preparation of the appropriate eigenstates discussed above. This adds at most a constant overhead to the EEA due to the additional precision required to account for the scaling associated with the overlap suppression.

Acknowledgments

We thank Ryan Epstein and Scott Glancy for their help in reviewing and editing this manuscript. Contributions to this work by NIST, an agency of the US government, are not subject to copyright.
laws. This work was carried out under the auspices of the National Nuclear Security Administration of the U.S. Department of Energy at Los Alamos National Laboratory under Contract No. DE-AC52-06NA25396.

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 96, 010401/1 (2006).
[2] V. Giovannetti, S. Lloyd, and L. Maccone, Science 306, 1330 (2004).
[3] R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
[4] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A 61, 022301/1 (2000).
[5] G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A 64, 022319/1 (2001), quant-ph/0012334.
[6] R. Somma, G. Ortiz, E. Knill, and J. Gubernatis, Int. J. Quantum Inf. 1, 189 (2003), quant-ph/0304063.
[7] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A 65, 042323/1 (2002), quant-ph/0108146.
[8] C. Miquel, J. P. Paz, M. Saraceno, E. Knill, R. Laflamme, and C. Negrevergne, Nature 418, 59 (2002), quant-ph/0109072.
[9] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A 454, 339 (1998), quant-ph/9708016.
[10] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, in Quantum Computation and Quantum Information: A Millennium Volume, edited by J. S. J. Lomonaco (AMS Contemporary Mathematics Series, Am. Math. Soc. USA, 2000).
[11] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Phys. Rev. A 54, R4649 (1996).
[12] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A 52, 3457 (1995).
[13] P. W. Shor, SIAM J. Comput. 26, 1484 (1997).
[14] For the moment, we identify the precision with the maximum error. The correct formulation of precision in terms of confidences is given later. Because $\|j\|$ $\|j\|$ $\|i\|$ $\|i\|$ 1, the error in the value of $\bar{a}$ is at most $p=2$. Similarly, the errors in $4\lambda^2$ and $4\lambda^2-2$ are at most $p=2$. Here we used the fact that the parametrized precision returned by the AEA is also an upper bound on the precision of the (unparameterized) value returned. Thus $Re\{y\}$ and $Im\{y\}$ are both off by at most $p=2$. This error affects only the component of the returned value perpendicular to $h$ $\|j\|$ $\|j\|$ $\|i\|$ $\|i\|$ in the complex plane, to which it contributes at most $p=2$. When these errors are lifted back to the upper unit hemisphere, they are bounded by $p=2) + (p=2) = p=2$, taking into account that the precision in $a$ is actually with respect to the parameterization. Our choice of precisions in the calls to amplitude estimation can be improved.
[15] R. B. Griffiths and C.-S. Niu, Phys. Rev. Lett. 76, 3228 (1996).
[16] J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M. D. Barrett, R. B. Blakestad, W. M. Itano, J. D. Jost, C. Langer, T. Schaeetz, et al., Science 308, 997 (2005).
[17] Using $n$ as an explicit parameter, we have $P_0() = 1$, and $P_n() = P_{n-1}(=2) \cos(=2)$ The probability $P$ that the phase returned is within $2^n$ is the probability $P_n()$ of getting the best approximation, plus the the probability $1 \cos(=2) = \sin(=2) = \cos(=2)$ that the most significant bit is wrong times the probability $P_{n-1}(=2) = 2$ that all subsequent bits are best possible. Thus $P = P_n() + P_{n-1}(=2) \cos(=2) = P_n() + P_n(=2) \cos(=2)$ = 0.81.
[18] A. Y. Kitaev (1995), quant-ph/9511026.
The prior probability that all the

D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders (2005), quant-ph/0508139.

Let \( C \) be a constant so that \( G^{1}(x) = C x \log(x) \) for \( x \) small enough. Since we are considering the asymptotic behavior of resources for small \( p, x \) is small and the first inequality in constraint (A') of Eq. (10) may be assumed to be satisfied. To solve constraint (A'), maximize \( m_{ax} \) subject to

\[
\frac{1}{\log(m_{ax}p^{=}8)} j (p=8) = \left(\frac{1}{m_{ax}} \right) = 6.
\]

Rewrite this inequality as

\[
\frac{1}{\log(m_{ax}p^{=}8)} j (p=8) = \frac{2}{m_{ax}}.
\]

For \( p \) small enough (and since \( m_{ax} \geq 1 \), this is the same as)

\[
\frac{2}{m_{ax}} \log(p=8) + \frac{2}{m_{ax}} \log(p=8) = \frac{2}{m_{ax}} \log(p=8).
\]

We can impose the additional constraint that \( j \log(\frac{m_{ax}}{p}) \) to write the inequality in the form

\[
\frac{2}{m_{ax}} \log(p=8) = \frac{2}{m_{ax}} \log(p=8) \text{ for some constant } D = \frac{1}{2} \log(p=8) j^{1-2}. \]

For this solution, \( j \log(\frac{m_{ax}}{p}) \) is sufficiently small \( p \). Hence the additional constraint is asymptotically satisfied.

Let \( C \) be a constant so that \( G^{1}(x) = C x \log(x) \) for \( x \) small enough. As in

we are interested in the behavior for small \( p \). To solve constraint (A'), maximize \( m_{ax} \) subject to

\[
\frac{1}{\log(m_{ax}p^{=}8)} j (p=8) = \left(\frac{1}{m_{ax}} \right) = 6.
\]

Equivalently,

\[
\frac{1}{\log(m_{ax}p^{=}8)} j (p=8) = \frac{1}{m_{ax}} = \frac{1}{m_{ax}} \log(p=8) = \frac{1}{m_{ax}} \log(p=8) \text{ for some constant } D = \frac{1}{2} \log(p=8) j^{1-2}.
\]

Hence

\[
\frac{1}{m_{ax}} \log(p=8) = \frac{1}{m_{ax}} \log(p=8) \text{ for } \frac{1}{m_{ax}} \log(p=8) j^{1-2}.
\]

Thus we get \( t = \frac{1}{m_{ax}} \log(p=8) \).

The prior probability that all the \( y_{1} \) are within \( (t=2) p = (4K 2^{K}) \) of the true overlap in the calls to the OEA is at least \( (1 + K l C^{=0}) = (2K) \) = 0 (1 + C). Thus the confidence for stage II' matches that of stage II. Assuming that all the \( y_{1} \) have the stated precision, the difference

\[
\int_{x=0}^{x=0} c y_{1} \text{ is bounded by } B = \int_{x=0}^{x=0} c \log(p=8) = (4K 2^{K}).
\]

Since \( c \log(p=8) \) is bounded by \( \log(p=8) j^{1-2} \),

\[
\text{As before, the approximation error } j \text{ is } \frac{1}{m_{ax}} \log(p=8) = \frac{1}{m_{ax}} \log(p=8) \text{ for some constant } D = \frac{1}{2} \log(p=8) j^{1-2}.
\]

Each such eigenvalue still contributes to the values returned by the calls to the OEA, changing each \( y_{1} \) by at most \( F (m_{ax}=t) \) = \( (8K 2^{K}) \), which changes the returned value by at most \( p=4 \).

In this case, \( G^{1}(x) = \frac{1}{m_{ax}} \log(p=8) \) and can set \( t = \frac{1}{m_{ax}} \log(p=8) \).

Asymptotically, \( K + 1 \) is \( K \) in the expressions obtained.

Use \( G^{1}(x) = C j \log(p=8) j \) for sufficiently small \( x \). We therefore need \( C j \log(\frac{m_{ax}p^{=}8}{\log(8K 2^{K})}) j (p=32)(K + 1) = \frac{1}{m_{ax}} \log(p=8) \).

Because \( \log(8K 2^{K}) \) is \( K \), it is sufficient to satisfy \( (j \log(\frac{m_{ax}}{p}) j + j \log(p) j + 3K) \)^{K} = \( K = p^{=8}(j \log(p) j + 3K) \)^{K}.

Add the additional constraint \( j \log(\frac{m_{ax}}{p}) j \) \( j \log(p) j \) so that \( K = p^{=8}(j \log(p) j + 3K) \) suffices. We can therefore set \( m_{ax} = \frac{1}{K} \log(p=8) j + 3K) \)^{K} = \( (p=8)(j \log(p) j)^{1-K} \).

Thus we need \( m_{ax} = \frac{1}{K} \log(p=8) j + 3K) \)^{K}.

Here \( G^{1}(x) = C x \log(x) \) for sufficiently small \( x \), so we solve \( (m_{ax}=p^{=8}(8K 2^{K})) \) for sufficiently small \( p \), independent of \( K \). To obtain \( t \), note that \( G^{1}(x) = p^{=8}(8K 2^{K}) \) = \( O(j \log(p) j + K) \), where we used the order notation to absorb constants.
bound $t, G^1 (\frac{m_{ax}}{P}=8K^2 \sigma K) = O (2K^{1+\frac{1}{2}} \sigma K^{1+K}) 1=(l+\sigma K)$. Thus $t = O (2K^{1+\frac{1}{2}} \sigma K^{1+K}) 1=(l+\sigma K)$. 

[28] It suffices to assign the qubits to the leaves of a binary tree. The decoding proceeds recursively by applying CNOTs to pairs of leaves with a common parent, removing the target qubit, assigning the control qubit to the parent and removing the leaves from the tree. The qubit that ends up at the root of the tree is measured in the $j+i\sigma j$ basis.

[29] C. Zalka, Phys. Rev. A 60, 2746 (1999).