Generation of eigenstates using the phase-estimation algorithm

B. C. Travaglione* and G. J. Milburn
Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Queensland, Australia
(Received 19 June 2000; published 5 February 2001)

The phase estimation algorithm is so named because it allows an estimation of the *eigenvalues* associated with an operator. However, it has been proposed that the algorithm can also be used to generate *eigenstates.* Here we extend this proposal for small quantum systems, identifying the conditions under which the phase-estimation algorithm can successfully generate eigenstates. We then propose an implementation scheme based on an ion trap quantum computer. This scheme allows us to illustrate two simple examples, one in which the algorithm effectively generates eigenstates, and one in which it does not.

DOI: 10.1103/PhysRevA.63.032301 PACS number(s): 03.67.Lx, 32.80.Pj

I. INTRODUCTION

Since the inception of quantum computation [1], people in the field have endeavored to find tasks which a quantum computer could perform more efficiently than a classical computer [2–5]. For a detailed introduction to the field of quantum computation and information, see Ref. [6]. The algorithm which has by far generated the most interest is Shor's factoring algorithm [4], as it enables the cracking of the Rivest, Shamir, and Adleman (RSA) encryption system [7]. Kitaev [8] generalized Shor's algorithm, showing how a quantum computer can generate an eigenvalue of an arbitrary unitary operator (in the limit of a large number of qubits, and not necessarily efficiently). Due to experimental difficulties, a large-scale quantum computer (if possible) will not be attainable for a number of years. However, small-scale quantum computers are already available [9]. In this paper, we show how a version of the phase-estimation algorithm can be implemented on a particular ''small-scale'' quantum computer: the ion trap quantum computer.

Given some unitary operator U and an approximate eigenstate, the goal of the phase estimation algorithm [8,10] is to obtain an eigenvalue of U and leave the quantum system in the corresponding eigenstate [11,12]. To accomplish this task, we shall need two quantum systems which can be coupled together. One we shall call the index system, and the other the target system. The index system is initially prepared in the state $|0\rangle$. After performing the algorithm, the index system will store an eigenvalue of the target system operator, U.

Traditionally both target and index systems have been qubit registers. In this paper the index system will remain a register of qubits; however, we shall allow the target system to be an arbitrary N-dimensional quantum system, where N may be equal to infinity. For a more generalized discussion of combining continuous and discrete quantum computation, see Ref. [13].

In Sec. II we briefly review the phase-estimation algorithm, and then derive analytical results which will allow us to characterize the algorithm's performance when using only a small number of qubits. In Sec. III we derive the Hamiltonians necessary to investigate the number and displacement operators in an ion trap, and contrast the algorithm's effectiveness with respect to the two different operators.

II. PHASE-ESTIMATION ALGORITHM

In what follows, we shall assume that our index system is a register of m qubits. First, we need to be able to perform the operation $\Lambda(U)$ on our coupled system. $\Lambda(U)$ is completely described by defining its action on the standard basis states of the index system, coupled to an arbitrary target system state,

$$\Lambda(U)|j\rangle_I|\psi\rangle_T = \mathbb{I}_I \otimes U^j{}_T|j\rangle_I|\psi\rangle_T = |j\rangle U^j|\psi\rangle, \quad \forall j \in \mathbb{Z}_M, \tag{1}$$

where $\mathbb{Z}_M=\{0,1,2,...,M-1\}$ and $M=2^m$. As in the last line of Eq. (1), we shall continue to omit the subscript notation when it is clear whether a ket or operator is referring to the target or index system. We begin the algorithm by initializing our quantum computer into the state

$$|\Psi_0\rangle = |0\rangle|\psi\rangle. \tag{2}$$

Performing a $\pi/2$ rotation of each qubit in the index register results in the state

$$|\Psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle|\psi\rangle, \tag{3}$$

We now perform $\Lambda(U)$ on this state, giving

$$|\Psi_2\rangle = \Lambda(U)|\Psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle U^j|\psi\rangle. \tag{4}$$

The final steps in the algorithm are to perform the unitary quantum Fourier transform [14] on the index register, and measure this register [18]. However, before applying this transform we shall rewrite Eq. (4). First we replace $|\psi\rangle$ by its representation as a sum of eigenvectors of U,

$$|\psi\rangle = \sum_k c_k|\phi_k\rangle, \tag{5}$$

*Electronic address: btrav@physics.uq.edu.au; URL: www.physics.uq.edu.au/people/btrav/

where k sums over the dimensionality of the target system. Hence the state $|\Psi_2\rangle$ can be written as

$$|\Psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle U^j \sum_k c_k |\phi_k\rangle. \tag{6}$$

We shall write the eigenvalue associated with $|\phi_k\rangle$ as $e^{i\phi_k}$. Noting that U^j applied to each eigenvector $|\phi_k\rangle$ is simply $e^{ij\phi_k}|\phi_k\rangle$, and changing the order of the summations, we obtain

$$|\Psi_2\rangle = \sum_k c_k \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle e^{ij\phi_k} |\phi_k\rangle. \tag{7}$$

Finally, for clarity, we exchange the order of the systems, and replace ϕ_k with $2\pi\omega_k/M$, where $\omega_k \in [0,M)$:

$$|\Psi_2\rangle = \sum_k c_k |\phi_k\rangle \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{2\pi i j\omega_k/M} |j\rangle. \tag{8}$$

It is now not hard to show that taking the quantum Fourier transform of the index register results in the state

$$|\Psi_3\rangle = \sum_k c_k |\phi_k\rangle \sum_{j=0}^{M-1} f(\omega_k, j)|j\rangle, \tag{9}$$

where

$$f(\omega_k, j) = \begin{cases} \dfrac{1}{M} \dfrac{\sin(\pi\omega_k)}{\sin\left(\pi \dfrac{\omega_k - j}{M}\right)} \exp\left(\pi i \left[\omega_k - \dfrac{\omega_k j}{M}\right]\right), & \omega_k \neq j \\ 1, \quad \omega_k = j. \end{cases} \tag{10}$$

As we will see shortly, it is helpful to note that

$$|f(\omega_k, j)| \geqslant |\mathrm{sinc}(\omega_k - j)|, \tag{11}$$

for all $\omega_k \in [0,M)$ and $j \in \mathbb{Z}_M$. A plot of $|f(\omega_k, j)|$ is shown in Fig. 1, where $M=16$ and j has been set to 5.

Finally, measuring the index register will, with a high probability, yield an approximate eigenvector. To understand this, let us begin by looking at the most simplified case. Suppose for a moment, that we have $\omega_k \in \mathbb{Z}_M$ for all k; then

$$f(\omega_k, j) = \delta_{\omega_k - j}. \tag{12}$$

Thus Eq. (9) simplifies to

$$\sum_k c_k |\phi_k\rangle |\omega_k\rangle. \tag{13}$$

If we add the assumption that no two values of k give the same ω_k (i.e., we have no degeneracy [19]) then upon measuring the index register, we will obtain $|\omega_k\rangle$, and hence $e^{i\phi_k}$, with probability $|c_k|^2$, and leave the target system in the eigenstate $|\phi_k\rangle$.

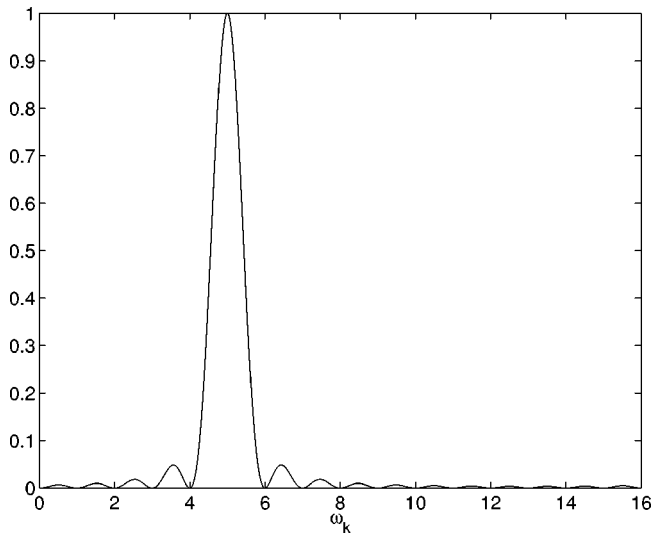

FIG. 1. A plot of $|f|$ as a function of ω_k, with $M=16$ and $j=5$.

Removing the assumption of zero degeneracy, measuring the index register still allows us to obtain some eigenvalue $e^{2\pi ij/M}$; however, the target system is now left in the state

$$\frac{1}{\sqrt{\mathcal{N}}} \sum_{k'} c_{k'} |\phi_{k'}\rangle, \tag{14}$$

where $k' = \{k : \omega_k = j\}$, and $\mathcal{N} = \Sigma_{k'} |c_{k'}|^2$ is a normalization constant.

Finally, we shall remove the assumption that the ω_k must be elements of $\mathbb{Z}_M$. The probability $P(j)$, of measuring the index register in some basis state $|j\rangle$ is

$$P(j) = \sum_k |\langle \phi_k | \langle j | \Psi_3 \rangle|^2 = \sum_k |c_k f(\omega_k, j)|^2. \tag{15}$$

Having measured the index register to be in some state $|j\rangle$, the target system is left in the state

$$|\psi_j'\rangle = \sum_k c_k' |\phi_k\rangle, \quad c_k' = \frac{c_k f(\omega_k, j)}{\sqrt{\mathcal{N}}}, \tag{16}$$

where $\mathcal{N} = \Sigma_k |c_k f(\omega_k, j)|^2$.

In order to gain some useful information from Eqs. (15) and (16), let us assume that our initial target system state $|\psi\rangle$ is an approximate eigenstate of $|\phi_q\rangle$ for some q such that

$$|c_q|^2 \equiv |\langle \phi_q | \psi \rangle|^2 = p. \tag{17}$$

Remembering that ω_q will be some real number between 0 and M, we define $\lfloor \omega_q \rfloor$ to be the nearest m-bit integer less than ω_q, and $\lceil \omega_q \rceil$ to be the nearest m-bit integer greater than

ω_q, where modulo M has been assumed. The probability of measuring the index register in either the state $|\lfloor \omega_q \rfloor\rangle$ or $|\lceil \omega_q \rceil\rangle$ is

$$\begin{aligned} P(\lfloor \omega_q \rfloor \text{ or } \lceil \omega_q \rceil) &= \sum_k |c_k f(\omega_k, \lfloor \omega_q \rceil)|^2 \\ &\quad + \sum_k |c_k f(\omega_k, \lceil \omega_q \rceil)|^2 \\ &\geqslant |c_q f(\omega_q, \lfloor \omega_q \rceil)|^2 + |c_q f(\omega_q, \lceil \omega_q \rceil)|^2 \\ &\geqslant |c_q|^2 2\,\mathrm{sinc}^2(0.5) > 0.8p. \end{aligned} \tag{18}$$

Hence, with a probability greater than $0.8p$, we will obtain an approximate eigenvalue associated with $|\phi_q\rangle$, which differs in phase from the actual eigenvalue by less than $2\pi/2^m$. Thus, if p is reasonably large, we have a high probability of finding the best estimate of the eigenvalue. However, as we shall see, large p does not imply that we will improve on the approximate eigenstate.

Suppose we measure the index register in the state $|[\omega_q]\rangle$, where $[\omega_q]$ denotes the closest m-bit integer to ω_q. (N.B. This will occur with probability greater than $0.4p$, as $|f(\omega_q, [\omega_q])|^2 > 0.4$.) The key question that we wish to address in this paper is: has our initial approximate eigenstate improved? Letting $p' \equiv |c_q'|^2$, we are effectively asking what bounds can be placed on p'? For an arbitrary U it is obvious that the upper bound of $p'=1$ can be obtained by setting $|\psi\rangle = |\phi_q\rangle$. We now investigate the lower bound by dividing the eigenstates into three disjoint sets:

$$\begin{aligned} \mathcal{Q} &= \{q\}, \\ \mathcal{G} &= \{g : g \neq q, |\omega_g - [\omega_q]| \leqslant 1\}, \\ \mathcal{H} &= \{h : |\omega_h - [\omega_q]| > 1\}. \end{aligned} \tag{19}$$

We now have

$$p' = \frac{p|f(\omega_q, [\omega_q])|^2}{\mathcal{N}}, \tag{20}$$

with

$$\begin{aligned} \mathcal{N} &= p|f(\omega_q, [\omega_q])|^2 + \sum_{g \in \mathcal{G}} |c_g|^2 |f(\omega_g, [\omega_q])|^2 \\ &\quad + \sum_{h \in \mathcal{H}} |c_h|^2 |f(\omega_h, [\omega_q])|^2. \end{aligned} \tag{21}$$

Using Eqs. (10) and (19), it is not hard to show that

$$\begin{aligned} 0.4 &< |f(\omega_q, [\omega_q])|^2 \leqslant 1, \\ 0 &\leqslant |f(\omega_g, [\omega_q])|^2 \leqslant 1, \\ 0 &\leqslant |f(\omega_h, [\omega_q])|^2 \leqslant \lambda, \end{aligned} \tag{22}$$

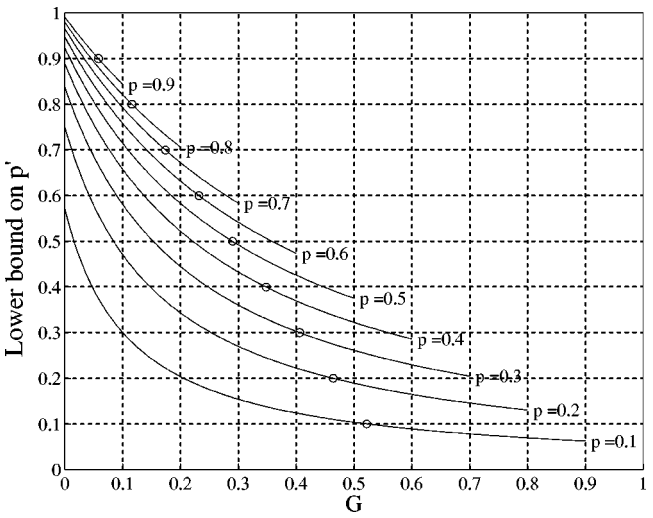

FIG. 2. The lower bound on p' as a function of G for $|f(\omega_q, [\omega_q])|^2 = 0.6$ and various values of p. The circles indicate the points at which the minimum of p' equals p.

where $\lambda = |f(1.5,0)|^2$. As m increases, λ tends to $(2/3\pi)^2 \approx 0.045$. However, for our analysis it is sufficient to note that $0.045 < \lambda < 0.05$ for $m > 3$. Equation (22) leads to the lower bound

$$p' \geqslant \frac{p|f(\omega_q, [\omega_q])|^2}{p|f(\omega_q, [\omega_q])|^2 + (1-\lambda)G + \lambda(1-p)} \tag{23}$$

where $G = \Sigma_g |c_g|^2$. Figure 2 contains a plot of this lower bound as a function of G for $|f(\omega_q, [\omega_q])|^2 = 0.6$ and various values of p. The circles indicate the points at which the minimum of p' equals p. Thus we see that by endeavoring to make G as small as possible, we increase the amplitude of $|\phi_q\rangle$. For a given U and $|\psi\rangle$, G can be made arbitrarily small by increasing m. However, we are interested in the performance of the algorithm for small values of m. We shall now look at G's dependence on U and $|\psi\rangle$ by attempting to create eigenvectors for both the number and displacement operator in a ion trap.

III. AN ION-TRAP IMPLEMENTATION

We first derive the Hamiltonian for $\Lambda(U)$, where U is the evolution operator associated with the number operator, and investigate the phase-estimation algorithm's performance for various initial states. We then derive the Hamiltonian for the more complicated case of U being the displacement operator. For both of these examples the index register will be two electronic levels of m ions in a linear ion trap, and the target system will be the center-of-mass (CM) vibrational mode of the ions.

A. Number operator

Consider the standard Hamiltonian of the one-dimensional harmonic oscillator,

$$H = \hbar\omega(a^\dagger a + \tfrac{1}{2}). \tag{24}$$

where $a^\dagger$ and a are the creation and annihilation operators. Ignoring the overall phase contribution of the zero-energy state, the unitary operator we will first be analyzing is

$$U(t)=e^{-i\omega a^\dagger a t}. \tag{25}$$

In this case, $\Lambda(U)$ is given by

$$\Lambda(U)=\exp\left(\frac{-it}{\hbar}\sum_{j=0}^{m-1}H_j\right), \tag{26}$$

where

$$H_j=\hbar a^\dagger a 2^j\omega(\sigma_z^{(j)}+\tfrac{1}{2}). \tag{27}$$

The inversion operator for each ion is defined by $\sigma_z^{(j)}=(|0\rangle\langle 0|-|1\rangle\langle 1|)/2$. This Hamiltonian can be obtained for interaction times greater than the period of the CM vibrational mode by applying a set of far-detuned standing wave pulses to the ion [15].

We begin our analysis by initializing the CM mode in some phonon number state $|n\rangle$ [16], and setting $\omega t=2\pi(1-1/M)$. It is important to note that we are assuming that all the higher vibrational modes are in the vacuum state. Assuming no errors, applying the phase-estimation algorithm results in the index register being measured in the state $|n \bmod M\rangle$ and the target system being left unchanged. If we now let ωt be some arbitrary value, applying the algorithm will leave the target system unchanged, and the index system will be measured in the state $|j\rangle$ with probability

$$P(j)=\left|f\left(\frac{-\omega t n M}{2\pi},j\right)\right|^2. \tag{28}$$

Let us consider the more interesting situation where the target system is initialized in some coherent state $|\alpha\rangle$. We can utilize the phase-estimation algorithm to transform the state of the target system into an approximation to a Fock state.

For example, suppose we use four index qubits, $\omega t=1$, and choose to approximate the Fock state $|n=9\rangle$ by using the coherent state $|\alpha=3\rangle$. In this example we perhaps might think that $|\alpha=3\rangle$ is not a good approximate state because $p\approx 0.13$; however, the fact that $G<0.035$ indicates that the algorithm should work well. Applying the algorithm and measuring the index register in state $|9\rangle$, we obtain $p'\approx 0.93$. The initial and final target states for this scenario are shown in Fig. 3.

Having shown that the phase-estimation algorithm can be used to generate Fock states from coherent states, we now attempt to generate eigenstates of the displacement operator.

B. Displacement operator

The displacement operator applied to the CM vibrational mode is defined as

$$D(\alpha)=\exp(\alpha a^\dagger-\alpha^* a). \tag{29}$$

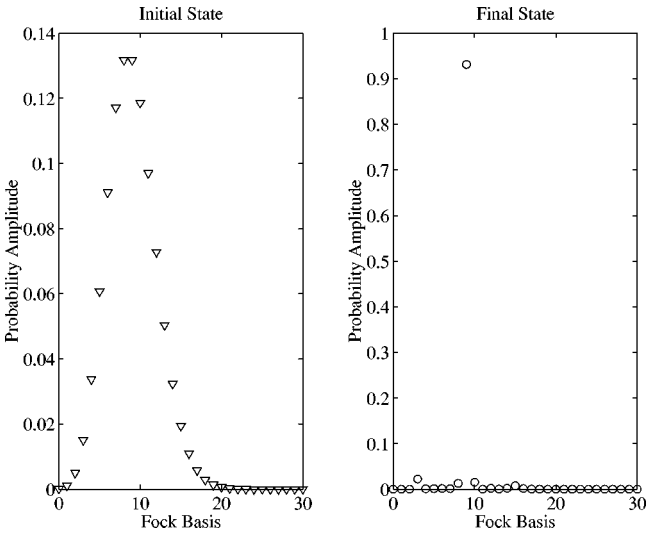

FIG. 3. Fock state distributions for the target system initially in a coherent state with $\alpha=3$, and the state of the system after applying the phase-estimation algorithm and measuring the four index qubits.

Thus the operator we wish to apply is

$$\Lambda(D)=\exp\left(\frac{-it}{\hbar}\sum_{j=0}^{m-1}H_j\right), \tag{30}$$

where H_j are now defined as

$$H_j=i\hbar(\alpha a^\dagger-\alpha^* a)2^j(\sigma_z^{(j)}+\tfrac{1}{2}). \tag{31}$$

It was already shown [17] that conditional displacement operations such as the Hamiltonian in Eq. (31) can be performed in an ion trap.

It is not hard to show that

$$D(de^{i[\phi+(\pi/2)]})|\alpha,\varepsilon\rangle\approx e^{i2d|\alpha|e^{-r}}|\alpha,\varepsilon\rangle \tag{32}$$

for large values of the squeezing parameter r, and where $\alpha=|\alpha|e^{i\phi}$, $\varepsilon=re^{2i\phi}$, and

$$|\alpha,\varepsilon\rangle\equiv S(\varepsilon)D(\alpha)|0\rangle \tag{33}$$

is a squeezed coherent state. Thus the squeezed coherent states $|\alpha,\varepsilon\rangle$ form approximate eigenvectors of the displacement operator $D(de^{i[\phi+(\pi/2)]})$.

Without loss of generality we can set $\phi=0$ in which case the eigenstates of the displacement operator are simply the position eigenstates. It is then not hard to show that for small fixed m, $G\approx 1-p$, which leads to $p'\approx p$. Thus applying the phase-estimation algorithm to squeezed displaced states does not produce improved eigenstates of the displacement operator.

IV. CONCLUSION

We have shown that the phase-estimation algorithm can be used to generate eigenstates of the number operator, even when we severely limit the size of the index system. It would be interesting to see if an analogous implementation could be performed using cavity QED, allowing generation of photon number states with only small numbers of trapped atoms. We have also shown that the algorithm's performance depends on the relation between the approximate eigenstate and the spectrum of the operator. We can gauge the algorithm's performance by calculating a parameter G.

ACKNOWLEDGMENTS

B.C.T. acknowledges support from the University of Queensland Traveling Scholarship, and thanks S. Lloyd, S. Schneider, M. Nielson, and D. F. V. James for helpful discussions.

[1] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[2] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).
[3] D. R. Simon, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 116.
[4] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.
[5] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[7] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[8] A. Y. Kitaev, e-print quant-ph/9511026.
[9] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe, Nature (London) **404**, 256 (2000).
[10] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998).
[11] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999).
[12] C. Zalka, Proc. R. Soc. London, Ser. A **454**, 313 (1996).
[13] S. Lloyd, e-print quant-ph/0008101.
[14] D. Coppersmith (unpublished).
[15] C. D'Helon and G. J. Milburn, Phys. Rev. A **54**, 5141 (1996).
[16] D. M. Meekhof, C. Monroe, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **76**, 1796 (1996).
[17] C. Monroe, D. M. Meekhof, B. E. King, and D. J. Wineland, Science **272**, 1131 (1996).
[18] By combining the QFT and measurement steps we remove the need to perform any two-qubit operations. The two-qubit controlled rotation operations can be replaced with measurement and conditional single-qubit rotations. However, for clarity we keep the description of these two steps separate.
[19] Please note that this unrealistic situation is not even possible if our target system has a dimension greater than 2^m.