A Lower Bound for Quantum Phase Estimation

Arvid J. Bessen*
Columbia University
Department of Computer Science
(Dated: January 26, 2005)

We obtain a query lower bound for quantum algorithms solving the phase estimation problem. Our analysis generalizes existing lower bound approaches to the case where the oracle Q is given by controlled powers Q^p of Q, as it is for example in Shor's order finding algorithm. In this setting we will prove a $\Omega(\log 1/\epsilon)$ lower bound for the number of applications of $Q^{p_1}, Q^{p_2}, \ldots$. This bound is tight due to a matching upper bound. We obtain the lower bound using a new technique based on frequency analysis.

PACS numbers: 03.67.Lx
Keywords: Quantum computing, complexity theory, lower bounds

I. INTRODUCTION

We study lower bounds for the phase estimation problem. In this problem we are given a unitary transformation Q as a black-box and we know that $|q\rangle$ is an eigenvector of Q, i.e.

$$Q\,|q\rangle = e^{2\pi i\varphi}\,|q\rangle\,, \quad \varphi \in [0,1). \tag{1}$$

We want to determine the phase φ up to precision ϵ.

The quantum phase estimation algorithm approximates φ given $|q\rangle$ and is the main building block in Shor's factoring algorithm, the counting algorithm, and the eigenvalue estimation algorithm [1–7].

The main element of this algorithm are controlled powers of Q, which we define as follows. Let Q be a t qubit unitary transformation and $|\psi\rangle$ an arbitrary t qubit state. For $l = 1, \ldots, c$, and $p \in \mathbb{N}$ we define the $c+t$ qubit transformation

$$W_l^p(Q)\,|x_1 \ldots x_c\rangle\,|\psi\rangle = \begin{cases} |x_1 \ldots x_c\rangle\,|\psi\rangle & x_l = 0 \\ |x_1 \ldots x_c\rangle\,Q^p\,|\psi\rangle & x_l = 1 \end{cases}. \tag{2}$$

We call $W_l^p(Q)$ a (controlled) *power query*. If the transformation Q is clear from the context, we will just write $W_l^p = W_l^p(Q)$.

This notation allows us to write the phase estimation algorithm in a compact form, see figure 1. The algorithm returns an approximation $\widetilde{\varphi}$ of the phase φ of $|q\rangle$.

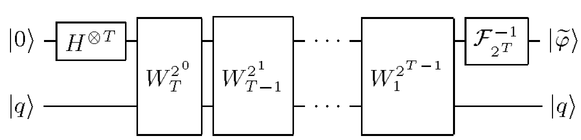

FIG. 1: The quantum phase estimation algorithm in power query notation. H is the Hadamard gate, W_l^p a power query as in equation (2), and $\mathcal{F}_{2^T}^{-1}$ is the inverse quantum Fourier transform on T qubits.

It is well known that $T = \mathcal{O}(\log \epsilon^{-1})$ power queries suffice to approximate φ up to ϵ. In this paper we study whether it is possible to improve on the performance of the phase estimation procedure, i.e., we ask what is the minimal number of applications of W_l^p to estimate φ up to ϵ.

Theorem 1. *Any quantum algorithm estimating the phase φ of an eigenvector $|q\rangle$ of matrices Q up to precision ϵ, with Q from the class*

$$\mathcal{Q}_{|q\rangle,t} = \big\{Q : Q \textit{ is a unitary } t \textit{ qubit transform}, \; |q\rangle \textit{ is an eigenvector of } Q\big\}. \tag{3}$$

has to use $\Omega(\log \frac{1}{\epsilon})$ power queries.

We prove Theorem 1 in section IV.

The query cost of the phase estimation algorithm may be given by counting each application of $W_l^p(Q)$ as p applications of Q, i.e. the query cost of this algorithm is

$$1 + 2 + 4 + \ldots + 2^{T-1} = 2^T - 1.$$

For certain problems, like order-finding, it is possible to exploit some knowledge about Q. Here $Q\,|y\rangle = |xy \mod N\rangle$ for a certain fixed x, and therefore

$$Q^{2^j}\,|y\rangle = \left|x^{2^j} y \mod N\right\rangle = \left|\left(x^{2^{j-1}}\right)^2 y \mod N\right\rangle$$

is easy to compute by repeated squaring and modular multiplication, see e.g. [2]. In this case we can use power queries $W_l^{2^k}$ with essentially the same cost as an application of Q. Thus we can execute the phase estimation algorithm with query cost T and have exponential speedup for the query cost: from $2^T - 1$ to T. Let us stress that this speedup only applies if the cost for computing Q^{2^j} is similar to that for computing Q.

II. PRIOR WORK

Quantum query complexity has been important in quantum computing since Grover's search algorithm,

*bessen@cs.columbia.edu

which is provably superior to classical algorithms [8, 9] in the number of queries. The first lower bound result was given in [10], which used an adversary argument.

Our lower bound approach is based on the ideas of the "polynomial approach" of Beals et. al., [11–14]. Other approaches include the quantum adversary argument and its generalizations [15–17].

These approaches only cover problems concerning Boolean functions, so we have to extend them to numerical problems. This has been done through extensions of the polynomial method [18, 19] and has been applied widely to integration [20–22], path integration [23], approximation [24–26], and eigenvalue estimation [6, 7].

In this paper we apply the approach of [19] to the phase estimation problem. Instead of using a maximum degree argument, which is not applicable in the case of arbitrary powers, we will develop a new lower bound technique based on frequency analysis.

III. QUANTUM ALGORITHMS WITH POWER QUERIES FOR PHASE ESTIMATION

We would like to derive lower bounds for any quantum algorithm with power queries that estimates the phase of a matrix Q for a given eigenvector $|q\rangle$. In other words the set of allowed inputs for our problem is

$$\mathcal{Q}_{|q\rangle,t} = \{Q : Q \text{ is a unitary } t \text{ qubit transform}, \\ |q\rangle \text{ is an eigenvector of } Q\}.$$

We now give a framework that is general enough to allow us to analyze any algorithm with power queries $W_l^p(Q)$ that solves this problem. The most general algorithm will be of the following form:

$$\left|\psi^{(T)}(Q)\right\rangle = U_T W_{l_T}^{p_T}(Q) U_{T-1} \dots W_{l_1}^{p_1}(Q) U_0 \left|\psi^{(0)}\right\rangle. \quad (4)$$

Here the $U_0, U_1, \dots, U_T$ are arbitrary but fixed $c+t$ qubit unitary transformations and $\left|\psi^{(0)}\right\rangle$ a fixed $c+t$ qubit state, for example $|0\rangle|q\rangle$. In our analysis we neglect the cost to implement the U_j or to prepare $\left|\psi^{(0)}\right\rangle$.

The varying parts of algorithm (4) are the $W_{l_j}^{p_j} = W_{l_j}^{p_j}(Q)$: power queries of Q for $p_j \in \mathbb{N}$, $l_j = 1, \dots, c$, and $c \in \mathbb{N}$ arbitrary. A measurement of the final state $\left|\psi^{(T)}(Q)\right\rangle$ in the standard basis yields a state $|k\rangle$, $k = 0, \dots, 2^{c+t} - 1$, with probability $p_{k,Q}$, from which we get a solution $\widetilde{\varphi}(k) \in [0, 1)$. If for all $Q \in \mathcal{Q}_{|q\rangle,t}$ the probability to get an ϵ-estimate to the correct phase φ of Q

$$\sum_{k:||\varphi-\widetilde{\varphi}(k)||<\epsilon} p_{k,Q} \geq \frac{3}{4}, \quad (5)$$

then the algorithm (4) solves the phase estimation problem to within ϵ with probability $\frac{3}{4}$ in T power queries.

We are interested in the smallest number T such that a quantum power query algorithm of form (4) fulfills condition (5) for all $Q \in \mathcal{Q}_{|q\rangle,t}$.

IV. GENERAL CONTROLLED ARBITRARY POWER QUERIES

We consider arbitrary powers $p_1, \dots, p_T$. This requires us to introduce a new proof technique. To illustrate the idea consider the phase estimation algorithm, performed as in figure 1 with $c = T = 3$ control qubits.

$$(\mathcal{F}_{2^3}^{-1} \otimes I) W_1^4 W_2^2 W_3^1 (H^{\otimes 3} \otimes I) \big|0\big\rangle |q\rangle .$$

Let us trace through each of the steps in this algorithm (we neglect normalization factors).

1. $(|0\rangle + |1\rangle + |2\rangle + |3\rangle + \dots + |7\rangle)|q\rangle$
2. $(|0\rangle + e^{2\pi i\varphi}|1\rangle + |2\rangle + e^{2\pi i\varphi}|3\rangle + \dots + e^{2\pi i\varphi}|7\rangle)|q\rangle$
3. $(|0\rangle + e^{2\pi i\varphi}|1\rangle + e^{2\pi i 2\varphi}|2\rangle + \dots + e^{2\pi i 3\varphi}|7\rangle)|q\rangle$
   The possible multiplicities j of φ in the coefficients $e^{2\pi i j\varphi}$ are
   $$\mathcal{J}_2 = \{0, p_1, p_2, p_1 + p_2\} = \{0, 1, 2, 3\}.$$
4. $(|0\rangle + e^{2\pi i\varphi}|1\rangle + e^{2\pi i 2\varphi}|2\rangle + \dots + e^{2\pi i 7\varphi}|7\rangle)|q\rangle$
   The possible multiplicities after this step are
   $$\mathcal{J}_3 = \{j, j + p_3 : j \in \mathcal{J}_2\} = \{0, 1, \dots, 7\}.$$

The final step, the inverse Fourier transform, does not depend on φ. It also does not change the possible multiplicities of φ, but just creates linear combinations of them. Consider, e.g., the coefficient of the state $|2\rangle$:

$$\sum_{j=0}^{7} e^{-2\pi i 2j/8} e^{2\pi i j\varphi} |2\rangle|q\rangle = \sum_{j=0}^{7} e^{2\pi i j(\varphi - 1/4)} |2\rangle|q\rangle ,$$

which gives the probability $p_2(\varphi)$ of measuring $|2\rangle$:

$$p_2(\varphi) = \Big|\sum_{j=0}^{7} e^{2\pi i j(\varphi-1/4)}\Big|^2 = \sum_{j,l=0}^{7} e^{2\pi i(j-l)(\varphi-1/4)},$$

which is plotted in figure 2. Figure 2 shows that the probability that $|2\rangle$ is measured is high if φ is close to 0.25, which is the value represented by $|2\rangle$.

The figure indicates that the width of this probability peak depends on the frequencies present in the probability function: higher frequencies allow sharper peaks. The goal of this paper is to prove that every halving of the width of the probability peak requires one additional step of the algorithm.

The proof consists of three steps. The first is to quantify the influence of each additional application of W_l^p on the frequencies present in the probability function (Theorem 2). Now consider a probability function as in figure 2. It must have a high peak $\geq 3/4$ with small width ϵ and should be close to zero everywhere else. We will show that such a function requires a large range of frequencies to be present (lemma 3). Finally we

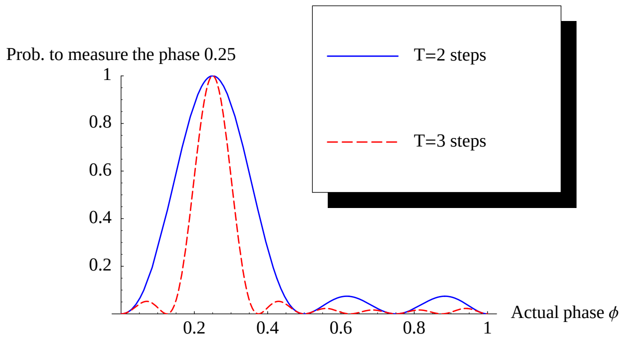

FIG. 2: (Color online) The probability of measuring the state $|2\rangle$ depending on φ for the algorithm depicted in figure 1 with $T = 2$ and $T = 3$.

will show an upper bound on the number of frequencies that a power query algorithm can generate with T power queries, which proves Theorem 1.

In Theorem 2 consider a general Q, which acts on t qubits and therefore has 2^t eigenvectors $|\psi_s\rangle$ with eigenvalues $e^{2\pi i\varphi_s}$. We assume that the eigenvectors $|\psi_s\rangle$ are fixed, but that the eigenvalues change. We will prove that after T steps only coefficients like

$$\alpha e^{2\pi i(j_1\varphi_1+\ldots+j_{2^t}\varphi_{2^t})}$$

will occur. Here $(j_1, \ldots, j_{2^t})$ is from the set $\mathcal{J}_T$ defined by the recursion

$$\mathcal{J}_{T+1} := \{(j_1, ..., j_{2^t}), (j_1 + p_{T+1}, ..., j_{2^t}), ..., \\ (j_1, ..., j_{2^t} + p_{T+1}) \,:\, (j_1, ..., j_{2^t}) \in \mathcal{J}_T\} \quad (6)$$

and $\mathcal{J}_0 = \{(0, \ldots, 0)\}$.

Theorem 2. *Let Q be a unitary operation with eigenvectors $|\psi_s\rangle$ and corresponding eigenvalues $e^{2\pi i\varphi_s}$, $s = 1, \ldots, 2^t$. Let the $|\psi_s\rangle$ be fixed and vary the phases $\varphi_s \in [0, 1)$. Any quantum algorithm with power queries $W_l^p = W_l^p(Q)$, fixed unitary transformations U_j and starting state $\left|\psi^{(0)}\right\rangle$, can be written as*

$$U_T W_{l_T}^{p_T} ...U_1 W_{l_1}^{p_1} U_0 \left|\psi^{(0)}\right\rangle = \sum_k S_k^{(T)}(\varphi_1, ..., \varphi_{2^t})\,|k\rangle \quad (7)$$

for all $\varphi_s \in [0, 1)$, where the $S_k^{(T)}(\varphi_1, \ldots, \varphi_{2^t})$ are trigonometric polynomials of the following form:

$$S_k^{(T)}(\varphi_1, \ldots, \varphi_{2^t}) \\ = \sum_{(j_1,\ldots,j_{2^t})\in\mathcal{J}_T} \alpha_{k,(j_1,\ldots,j_{2^t})}^{(T)} e^{2\pi i(j_1\varphi_1+\ldots+j_{2^t}\varphi_{2^t})}, \quad (8)$$

with $\alpha_{k,(j_1,\ldots,j_{2^t})}^{(T)} \in \mathbb{C}$ and $\mathcal{J}_T$ defined by (6).

To shorten our proofs we will use the following shorthand notations. We say that a trigonometric polynomial $S_k^{(T)}(\varphi_1, \ldots, \varphi_{2^t})$ is of powers $\mathcal{J}_T$, indicated by the $^{(T)}$ superscript, if it can be written as a sum over $\mathcal{J}_T$ as in (8). Furthermore we abbreviate the vectors $\vec{j} = (j_1, \ldots, j_{2^t})$, $\vec{\varphi} = (\varphi_1, \ldots, \varphi_{2^t})$, and define the following notation:

$$\vec{j}\cdot\vec{\varphi} = j_1\varphi_1 + \ldots + j_{2^t}\varphi_{2^t}.$$

Proof of Theorem 2: To simplify the proof we choose a different basis instead of the standard basis. We divide the quantum state into a control part $|m\rangle$ and an eigenvector part $|\psi_s\rangle$ and show that we can write

$$U_T W_{l_T}^{p_T} ...W_{l_1}^{p_1} U_0 \left|\psi^{(0)}\right\rangle = \sum_{m=0}^{2^c-1}\sum_{s=1}^{2^t} \widehat{S}_{m,s}^{(T)}(\vec{\varphi})\,|m, \psi_s\rangle\,, \quad (9)$$

for trigonometric polynomials of powers $\mathcal{J}_T$,

$$\widehat{S}_{m,s}^{(T)}(\vec{\varphi}) = \sum_{\vec{j}\in\mathcal{J}_T} \widehat{\alpha}_{m,s,\vec{j}}^{(T)} e^{2\pi i\vec{j}\cdot\vec{\varphi}}. \quad (10)$$

The proof is by induction on the number of queries T. For $T = 0$ we have no dependence on $\vec{\varphi}$ and $\widehat{S}_{m,s}^{(0)}(\vec{\varphi})$ is just a constant since Q was not applied:

$$\begin{aligned} U_0 \left|\psi^{(0)}\right\rangle &= \sum_{m=0}^{2^c-1}\sum_{s=1}^{2^t} \left\langle m, \psi_s \middle| U_0 \middle| \psi^{(0)}\right\rangle |m, \psi_s\rangle \\ &=: \sum_{m=0}^{2^c-1}\sum_{s=1}^{2^t} \widehat{\alpha}_{m,s,(0,\ldots,0)}^{(0)}\,|m, \psi_s\rangle \\ &= \sum_{m=0}^{2^c-1}\sum_{s=1}^{2^t}\sum_{\vec{j}\in\mathcal{J}_0} \widehat{\alpha}_{m,s,\vec{j}}^{(0)} e^{2\pi i\vec{j}\cdot\vec{\varphi}}\,|m, \psi_s\rangle\,. \end{aligned}$$

Let now T be arbitrary and let equations (9) and (10) hold. If we apply $W_{l_{T+1}}^{p_{T+1}}$ to (9), only those states $|m, \psi_s\rangle$ are affected for which the l_{T+1}-th control bit is set, i.e. $m_{l_{T+1}} = 1$. For these states we get

$$W_{l_{T+1}}^{p_{T+1}}\,|m, \psi_s\rangle = |m\rangle\, Q^{p_{T+1}}\,|\psi_s\rangle \;=|m\rangle\, e^{2\pi i p_{T+1}\varphi_s}\,|\psi_s\rangle$$

and therefore the coefficient of $|m, \psi_s\rangle$ changes to

$$\begin{aligned} \widehat{S}_{m,s}^{(T)}(\vec{\varphi})e^{2\pi i p_{T+1}\varphi_s} &= \sum_{\vec{j}\in\mathcal{J}_T} \widehat{\alpha}_{m,s,\vec{j}}^{(T)} e^{2\pi i\vec{j}\cdot\vec{\varphi}} e^{2\pi i p_{T+1}\varphi_s} \\ &= \sum_{\vec{j}\in\mathcal{J}_T} \widehat{\alpha}_{m,s,\vec{j}}^{(T)} e^{2\pi i(j_1\varphi_1+\ldots+(j_s+p_{T+1})\varphi_s+\ldots j_{2^t}\varphi_{2^t})}. \end{aligned}$$

But this is a trigonometric polynomial of powers $\mathcal{J}_{T+1}$ (recall eqn. (6)), and we can write it as

$$\widetilde{S}_{m,s}^{(T+1)}(\vec{\varphi}) = \sum_{\vec{j}\in\mathcal{J}_{T+1}} \widetilde{\alpha}_{m,s,\vec{j}}^{(T+1)} e^{2\pi i\vec{j}\cdot\vec{\varphi}}$$

if we define the coefficients $\widetilde{\alpha}^{(T+1)}_{m,s,\vec{j}}$ properly:

$$\widetilde{\alpha}^{(T+1)}_{m,s,(j_1,\ldots,j_s,\ldots,j_{2^t})} = \widehat{\alpha}^{(T)}_{m,s,(j_1,\ldots,j_s-p_{T+1},\ldots,j_{2^t})}$$

for $p_{T+1} \leq j_s$ and 0 otherwise.

Finally we define $\widetilde{S}^{(T+1)}_{m,s}(\vec{\varphi}) := \widehat{S}^{(T)}_{m,s}(\vec{\varphi})$ for the states for which the control bit is not set ($m_{l_{t+1}} = 0$) and we can write

$$W^{p_{T+1}}_{l_{T+1}} U_T \ldots W^{p_1}_{l_1} U_0 \left|\psi^{(0)}\right\rangle = \sum_{m=0}^{2^c-1} \sum_{s=1}^{2^t} \widetilde{S}^{(T+1)}_{m,s}(\vec{\varphi}) \left|m, \psi_s\right\rangle .$$

Now we use that the transformation U_{T+1} and the eigenvectors $|\psi_s\rangle$ are fixed for all algorithms we consider and define $u^{(T+1)}_{m,s;n,t} = \langle m, \psi_s| U_{T+1} |n, \psi_t\rangle$. Then

$$\begin{aligned} U_{T+1} \sum_{n,t} \widetilde{S}^{(T+1)}_{n,t}(\vec{\varphi}) \left|n, \psi_t\right\rangle \\ = \sum_{m,s,n,t} \widetilde{S}^{(T+1)}_{n,t}(\vec{\varphi}) u^{(T+1)}_{m,s;n,t} \left|m, \psi_s\right\rangle , \end{aligned} \tag{11}$$

which gives the following coefficient for $|m, \psi_s\rangle$:

$$\begin{aligned} &\sum_{n,t} \sum_{\vec{j} \in \mathcal{J}_{T+1}} \widetilde{\alpha}^{(T+1)}_{n,t,\vec{j}} e^{2\pi i \vec{j}\cdot\vec{\varphi}} u^{(T+1)}_{m,s;n,t} \\ &= \sum_{\vec{j} \in \mathcal{J}_{T+1}} \left[\sum_{n,t} u^{(T+1)}_{m,s;n,t} \widetilde{\alpha}^{(T+1)}_{n,t,\vec{j}} \right] e^{2\pi i \vec{j}\cdot\vec{\varphi}} \\ &=: \sum_{\vec{j} \in \mathcal{J}_{T+1}} \widehat{\alpha}^{(T+1)}_{m,s,\vec{j}} e^{2\pi i \vec{j}\cdot\vec{\varphi}} =: \widehat{S}^{(T+1)}_{m,s}(\vec{\varphi}). \end{aligned} \tag{12}$$

This completes the induction and establishes equations (9) and (10).

Using the same argumentation as in equations (11) and (12) we can finally rewrite the state in equation (9) in the standard basis $|k\rangle \in \{|0\rangle, |1\rangle, \ldots, |2^{c+t}-1\rangle\}$ through

$$\alpha^{(T+1)}_{k,\vec{j}} = \sum_{m,s} \langle k|m, \psi_s\rangle \, \widehat{\alpha}^{(T+1)}_{m,s,\vec{j}}$$

and $S^{(T)}_k(\vec{\varphi})$ is of the same powers as $\widehat{S}^{(T)}_{m,s}(\vec{\varphi})$, which is of powers $\mathcal{J}_T$. This proves equation (7) and (8). □

We now focus on the specific problem of phase estimation. The next lemma provides us with a necessary condition on the powers $p_1, p_2, \ldots$ such that a quantum algorithm with power queries can solve the phase estimation problem with precision ϵ.

Lemma 3. *Any quantum algorithm estimating the phase φ of an eigenvector $|q\rangle$ of matrices Q from the class*

$$\mathcal{Q}_{|q\rangle,t} = \big\{ Q : Q \text{ is a unitary } t \text{ qubit transform}, \\ |q\rangle \text{ is an eigenvector of } Q \big\}.$$

up to precision ϵ has to use power queries $W^{p_1}_{j_1}$, $W^{p_2}_{j_2}$, …, $W^{p_T}_{j_T}$ such that the set

$$\mathcal{M}_T = \Big\{ l - l' \,\big|\, l, l' = \sum_{k\in K} p_k \,\Big|\, K \subseteq \{1, \ldots, T\} \Big\} \tag{13}$$

has more than $|\mathcal{M}_T| \geq \frac{1}{2\epsilon}$ elements.

Note that this is both a condition on $p_1, \ldots, p_T$ as well as on T: by cleverly choosing the powers $p_1, \ldots, p_T$ we can get away with a smaller T, e.g. for $p_j = 2^{j-1}$ we get

$$\mathcal{M}_T = \left\{ -2^T + 1, -2^T + 2, \ldots, 2^T - 1 \right\},$$

while for the choice $p_j = 1$ we only get

$$\mathcal{M}_T = \{-T, -T+1, \ldots, T-1, T\}.$$

Proof of lemma 3: For simplicity assume that

$$2\epsilon = \frac{1}{N} \text{ for some } N \in \mathbb{N}. \tag{14}$$

We will analyze the behavior of all possible algorithms for the phase estimation problem on a special subset of $\mathcal{Q}_{|q\rangle,t}$. Fix some arbitrary vectors $|\psi_2\rangle, \ldots, |\psi_{2^t}\rangle$ such that $|q\rangle, |\psi_2\rangle, \ldots, |\psi_{2^t}\rangle$ form an orthonormal basis and consider the following input:

$$Q_r := e^{2\pi i 2r\epsilon} \left|q\right\rangle \left\langle q\right| + \sum_{s=2}^{2^t} e^{2\pi i \varphi_s} \left|\psi_s\right\rangle \left\langle \psi_s\right| . \tag{15}$$

The phase φ we are interested in is $\varphi = 2r\epsilon$ for input Q_r.

Since the difference between the phases of the matrices Q_r is 2ϵ and we require ϵ correctness, a measurement will yield states $|k\rangle$ from the *distinct* sets B_r:

$$B_r = \left\{ k : \|2r\epsilon - \widetilde{k}\| < \epsilon \right\}. \tag{16}$$

Depending on the number of qubits we use in our quantum algorithm, the sets B_r can contain one or more states.

By Theorem 2 we know that we can write the coefficient of a state $|k\rangle \in B_r$ after T queries as

$$\begin{aligned} &S^{(T)}_k(\varphi, \varphi_2, \ldots, \varphi_{2^t}) \\ &\quad = \sum_{(j_1,\ldots,j_{2^t}) \in \mathcal{J}_T} \alpha^{(T)}_{k,(j_1,\ldots,j_{2^t})} e^{2\pi i (j_1\varphi + j_2\varphi_2 + \ldots + j_{2^t}\varphi_{2^t})}. \end{aligned}$$

In this proof we are only interested in the behavior for the Q_r. Therefore we can drop the dependence on $\varphi_2, \ldots, \varphi_{2^t}$ and let

$$S^{(T)}_k(\varphi) := S^{(T)}_k(\varphi, \varphi_2, \ldots, \varphi_{2^t}) = \sum_{l \in \mathcal{L}_T} \beta^{(T)}_{k,l} e^{2\pi i l \varphi},$$

where $\mathcal{L}_0 = \{0\}$ and

$$\begin{aligned} \mathcal{L}_T &= \{ j_1 \,:\, (j_1, \ldots, j_{2^t}) \in \mathcal{J}_T \} \\ &= \{ j_1, j_1 + p_T \,:\, (j_1, \ldots, j_{2^t}) \in \mathcal{J}_{T-1} \} \\ &= \{ \sum_{k\in K} p_k \,\big|\, K \subseteq \{1, \ldots, T\} \} \end{aligned}$$

and the coefficients (note that l is fixed on the right side)

$$\beta_{k,l}^{(T)} = \sum_{(l,j_2,\ldots,j_{2^t})\in\mathcal{J}_T} \alpha_{k,(l,j_2,\ldots,j_{2^t})}^{(T)} e^{2\pi i(j_2\varphi_2+\ldots+j_{2^t}\varphi_{2^t})}$$

The probability $p_{B_r}(\varphi)$ of measuring a state from the set B_r defined in (16) of all ϵ approximations to $\varphi = 2r\epsilon$ is now given by:

$$\begin{aligned} p_{B_r}(\varphi) :=& \sum_{k\in B_r} \left|S_k^{(T)}(\varphi)\right|^2 \\ =& \sum_{k\in B_r}\sum_{l\in\mathcal{L}_T}\sum_{l'\in\mathcal{L}_T} \beta_{k,l}^{(T)}\overline{\beta_{k,l'}^{(T)}} e^{2\pi i(l-l')\varphi} \\ =:& \sum_{l\in\mathcal{L}_T}\sum_{l'\in\mathcal{L}_T} \gamma_{r,l,l'}^{(T)} e^{2\pi i(l-l')\varphi} \\ =:& \sum_{m\in\mathcal{M}_T} \eta_{r,m}^{(T)} e^{2\pi i m\varphi} \end{aligned} \tag{17}$$

with the set $\mathcal{M}_T$ given by

$$\mathcal{M}_T = \{l - l' \,|\, l, l' \in \mathcal{L}_T\}$$

and the coefficient

$$\eta_{r,m}^{(T)} = \sum_{\substack{l,l'\in\mathcal{L}_T\\ l-l'=m}} \gamma_{r,l,l'}^{(T)} = \sum_{\substack{l,l'\in\mathcal{L}_T\\ l-l'=m}}\sum_{k\in B_r} \overline{\beta}_{k,l}^{(T)}\beta_{k,l'}^{(T)}.$$

For illustration recall figure 2, which shows exactly one of these probability functions $p_{B_r}(\varphi)$ and also their highly oscillatory behavior. In the case of the phase estimation algorithm, $B_r = \{|r\rangle\}$ and the figure shows $p_{B_2}(\varphi)$.

We apply the Discrete Inverse Fourier Transform to $p_{B_r}(\varphi)$ (evaluated at the points $\varphi = n/N$ for $n = 0, \ldots, N-1$) and get for the k-th coefficient

$$\begin{aligned} &\sum_{n=0}^{N-1} p_{B_r}(n/N) e^{-2\pi i k n/N} \\ =&\sum_{n=0}^{N-1}\sum_{m\in\mathcal{M}_T} \eta_{r,m}^{(T)} e^{2\pi i(m-k)n/N} \\ =&N \sum_{\substack{m\in\mathcal{M}_T\\ m\equiv k \mod N}} \eta_{r,m}^{(T)}, \end{aligned} \tag{18}$$

since for $m \not\equiv k \mod N$

$$\sum_{n=0}^{N-1} e^{2\pi i(m-k)n/N} = \frac{1-e^{2\pi i(m-k)N/N}}{1-e^{2\pi i(m-k)1/N}} = 0. \tag{19}$$

We can bound (18) by separating the part where a state from B_r is correctly returned from $p_{B_r}(\varphi)$,

$$\begin{aligned} &\Big|\sum_{n=0}^{N-1} p_{B_r}(\frac{n}{N}) e^{-\frac{2\pi i k n}{N}}\Big| \\ \geq&\Big|p_{B_r}(\frac{r}{N})e^{-\frac{2\pi i k r}{N}}\Big| - \Big|\sum_{\substack{n=0\\ n\neq r}}^{N-1} p_{B_r}(\frac{n}{N})e^{-\frac{2\pi i k n}{N}}\Big| \\ \geq&\frac{3}{4} - \sum_{\substack{n=0\\ n\neq r}}^{N-1} p_{B_r}(\frac{n}{N}), \end{aligned} \tag{20}$$

since the probability $p_{B_r}(\varphi)$ has to obey $p_{B_r}(r/N) \geq \frac{3}{4}$ (recall the definitions of p_{B_r} and Q_r). If we knew that for the second term in (20)

$$\sum_{\substack{n=0\\ n\neq r}}^{N-1} p_{B_r}(n/N) < \frac{3}{4} \tag{21}$$

we could establish that

$$\left|\sum_{n=0}^{N-1} p_{B_r}(n/N) e^{-\frac{2\pi i k n}{N}}\right| = \left|N \sum_{\substack{m\in\mathcal{M}_T\\ m\equiv k \mod N}} \eta_{r,m}^{(T)}\right| > 0.$$

We will show that this property, while not necessarily always true, will be true for at least most of the $p_{B_r}(\varphi)$.

There are N different possible outcome sets $B_0, \ldots, B_{N-1}$. We know that for any $\varphi = n/N$ all mutually exclusive probabilities of measuring a state from B_r for $r = 0, \ldots, N-1$ have to add up to at most 1:

$$\sum_{r=0}^{N-1} p_{B_r}(n/N) \leq 1 \text{ for } n = 0, \ldots, N-1,$$

Let $R^< \subseteq \{0, \ldots, N-1\}$ be the set of all r for which (21) holds and $R^\geq$ the set for which it does not. $|R^<|$ has to be greater than 1 since we can split

$$N = \sum_{n=0}^{N-1} 1 \geq \sum_{n=0}^{N-1}\sum_{r=0}^{N-1} p_{B_r}(\frac{n}{N})$$

into the following parts:

$$\begin{aligned} &\sum_{r=0}^{N-1} p_{B_r}(\frac{r}{N}) + \sum_{r\in R^<}\sum_{\substack{n=0\\ n\neq r}}^{N-1} p_{B_r}(\frac{n}{N}) + \sum_{r\in R^\geq}\sum_{\substack{n=0\\ n\neq r}}^{N-1} p_{B_r}(\frac{n}{N}) \\ &\geq \frac{3}{4}N + 0\left|R^<\right| + \frac{3}{4}\left|R^\geq\right| = \frac{3}{4}N + \frac{3}{4}\left|R^\geq\right| \end{aligned}$$

and therefore $\left|R^\geq\right| \leq \frac{1}{3}N$ or $|R^<| \geq \frac{2}{3}N$.

Thus there is an $r \in R^<$ for which eqn. (21) holds and

$$0 < \left|N \sum_{\substack{m\in\mathcal{M}_T\\ m\equiv k \mod N}} \eta_{r,m}^{(T)}\right| \leq N \sum_{\substack{m\in\mathcal{M}_T\\ m\equiv k \mod N}} \left|\eta_{r,m}^{(T)}\right| \tag{22}$$

for all $k = 0, \ldots, N-1$.

This means at least N of the $\eta_{r,m}^{(T)}$ have to be nonzero and thus $p_{B_r}(\varphi)$ from eqn. (17) must have at least N nonzero terms. In other words

$$|\mathcal{M}_T| \geq N = \frac{1}{2\epsilon}, \tag{23}$$

where we used the definition of N in (14). □

Lemma 3 now allows us to give a lower bound for the phase estimation problem. The numbers of queries T that is needed by any quantum algorithm is $\Omega(\log \frac{1}{\epsilon})$.

Proof of Theorem 1: From lemma 3 we know that the set $\mathcal{M}_T$ has to have $|\mathcal{M}_T| \geq \frac{1}{2\epsilon}$ elements. We can easily derive an upper bound on $|\mathcal{M}_T|$. There are at most 2^T elements in the set

$$\mathcal{L}_T = \{ \sum_{k \in K} p_k \,|\, K \subseteq \{1, \ldots, T\} \}$$

and therefore we have $|\mathcal{M}_T| \leq |\mathcal{L}_T|^2 \leq (2^T)^2 = 2^{2T}$. Combining our estimates for $|\mathcal{M}_T|$ we get

$$2^{2T} \geq |\mathcal{M}_T| \geq \frac{1}{2\epsilon},$$

and the number of queries T must grow like

$$T \geq \frac{1}{2} \log_2 \frac{1}{2\epsilon} = \Omega(\log \frac{1}{\epsilon}).$$

□

V. CONCLUSIONS AND EXTENSIONS

In this paper we have obtained lower bounds for quantum algorithms that approximate the phase estimation problem through the new lower bound proof technique of frequency analysis. These lower bounds match the known upper bounds for phase estimation.

The frequency analysis method can be used to give lower bounds for the Sturm-Liouville eigenvalue problem [7]. The results also extend to other forms of quantum queries, e.g. the query

$$Q_f \, |x\rangle \, |y\rangle = |x\rangle \, |y \oplus f(x)\rangle = |x\rangle \, |y + f(x) \mod 2^m\rangle .$$

An application of the frequency analysis method to these problems will be the subject of future work.

Acknowledgments

The author would like to thank J. Traub, H. Woźniakowski, and A. Papageorgiou for inspiring discussions. Funding was provided by Columbia University through a Presidential Fellowship. This research was supported in part by the National Science Foundation and by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Material Command, USAF, under agreement number F30602-01-2-0523.

[1] P. W. Shor, in *Proc. of the 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134, quant-ph/9508027.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[3] G. Brassard, P. Høyer, and A. Tapp, in *25th International Colloqium, ICALP'98* (Springer Verlag, 1998), vol. 1443 of *Lecture Notes in Computer Science*, pp. 820–831, quant-ph/9805082.

[4] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, in *Quantum Computation and Quantum Information: A Millennium Volume* (AMS, 2002), vol. 305 of *Contemporary Mathematics*, quant-ph/0005055.

[5] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999), quant-ph/9807070.

[6] P. Jaksch and A. Papageorgiou, Phys. Rev. Lett. **91** (2003), quant-ph/0308016.

[7] A. Papageorgiou and H. Woźniakowski (2004), to be published.

[8] L. K. Grover, in *Proc. of the 28th Annual ACM Symposium on Theory of Computing* (1996), pp. 212–219, quant-ph/9605043.

[9] M. Boyer, P. Brassard, P. Høyer, and A. Tapp, Fortschritte der Physik **46**, 493 (1998), quant-ph/9605034.

[10] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. on Computing **26**, 1510 (1997), quant-ph/9701001.

[11] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, in *Proc. of the 39th IEEE Conference on Foundations of Computer Science* (1998), pp. 352–361, quant-ph/9802049.

[12] A. Nayak and F. Wu, in *Proc. of the 31th Annual ACM Symposium on Theory of Computing* (1999), pp. 384–393, quant-ph/9804066.

[13] S. Aaronson, in *Proc. of the 33rd annual ACM symposium on Theory of computing* (ACM Press, 2001), quant-ph/0111102.

[14] Y. Shi, in *Proc. of the 43rd Symposium on Foundations of Computer Science* (IEEE Computer Society, 2002), pp. 513–519, ISBN 0-7695-1822-2, quant-ph/0112086.

[15] A. Ambainis, in *Proc. of the 32nd annual ACM symposium on Theory of computing* (ACM Press, 2000), pp. 636–643, quant-ph/0002066.

[16] S. Laplante and F. Magniez, in *Proc. of the 19th IEEE Annual Conference on Computational Complexity* (2004), pp. 294–304, quant-ph/0311189.

[17] H. Barnum, M. Saks, and M. Szegedy, in *Proc. of the 18th IEEE Conference on Computational Complexity* (2003), pp. 179–193.

[18] S. Heinrich, Journal of Complexity **18**, 1 (2002), quant-ph/0105116.

[19] A. J. Bessen, Journal of Complexity **20**, 699 (2004), quant-ph/0308140.

[20] E. Novak, Journal of Complexity **17**, 2 (2001), quant-ph/0008124.

[21] S. Heinrich, Journal of Complexity **19**, 19 (2003), quant-ph/0112153.

[22] S. Heinrich, M. Kwas, and H. Wozniakowski, in *Monte Carlo and Quasi-Monte Carlo Methods 2002*, edited by H. Niederreiter (Springer Verlag, 2003), pp. 243–258, quant-ph/0311036.

[23] J. F. Traub and H. Wozniakowski, Quantum Information Processing **1**, 365 (2002), quant-ph/0109113.

[24] E. Novak, I. H. Sloan, and H. Woźniakowski, Found. Comput. Math. **4**, 121 (2004), quant-ph/0206023.

[25] S. Heinrich, Journal of Complexity **20**, 5 (2004), quant-ph/0305030.

[26] S. Heinrich, Journal of Complexity **20**, 27 (2004), quant-ph/0305031.