# A Lower Bound for the Sturm-Liouville Eigenvalue Problem on a Quantum Computer

Arvid J. Bessen*
Department of Computer Science, Columbia University

December 14, 2005

**Abstract**

We study the complexity of approximating the smallest eigenvalue of a univariate Sturm-Liouville problem on a quantum computer. This general problem includes the special case of solving a one-dimensional Schrödinger equation with a given potential for the ground state energy.

The Sturm-Liouville problem depends on a function $q$, which, in the case of the Schrödinger equation, can be identified with the potential function $V$. Recently Papageorgiou and Woźniakowski proved that quantum computers achieve an exponential reduction in the number of queries over the number needed in the classical worst-case and randomized settings for smooth functions $q$. Their method uses the (discretized) unitary propagator and arbitrary powers of it as a query ("power queries"). They showed that the Sturm-Liouville equation can be solved with $\mathcal{O}(\log(1/\varepsilon))$ power queries, while the number of queries in the worst-case and randomized settings on a classical computer is polynomial in $1/\varepsilon$. This proves that a quantum computer with power queries achieves an exponential reduction in the number of queries compared to a classical computer.

In this paper we show that the number of queries in Papageorgiou's and Woźniakowski's algorithm is asymptotically optimal. In particular we prove a matching lower bound of $\Omega(\log(1/\varepsilon))$ power queries, therefore showing that $\Theta(\log(1/\varepsilon))$ power queries are sufficient and

*bessen@cs.columbia.edu

necessary. Our proof is based on a frequency analysis technique, which examines the probability distribution of the final state of a quantum algorithm and the dependence of its Fourier transform on the input.

# 1 Introduction

This paper deals with the solution of the Sturm-Liouville problem on a quantum computer. Quantum computers have shown great promise in solving problems as diverse as the discrete problems of searching and factoring [4, 15] and the continuous problems including integration, path integration, and approximation [13, 5, 16, 6, 7]. The main motivation for quantum computing is its potential to solve these important problems efficiently. Shor's algorithm achieves an exponential speedup over any known classical algorithm for factoring, but until the classical complexity of factoring is proven, the exponential speedup remains a conjecture. The quantum algorithms for integration provide provable exponential speedups over classical *worst-case* algorithms, but only polynomial speedups over classical *randomized* algorithms.

Recently Papageorgiou and Woźniakowski introduced a quantum algorithm for the Sturm-Liouville problem [14] which uses the quantum phase estimation algorithm. They showed that quantum algorithms with power queries[1] achieve a provable exponential reduction in the number of power queries over the number of queries needed in the classical worst-case or randomized setting. Naturally query complexity results neglect the cost of actually implementing the queries. At the end of this paper we will discuss this problem for power queries, but it is currently not clear under which conditions power queries are sufficiently inexpensive to implement for the Sturm-Liouville problem.

In this paper we will prove *lower bounds* on the number of power queries for quantum algorithms that solve the Sturm-Liouville problem. This can be used to show the optimality of the algorithm proposed in [14]. To prove lower bounds for algorithms with power queries the previously known quantum lower bound techniques, such as the "polynomial method" of Beals et. al [1, 11] do not suffice. Our lower bound method builds on the "trigonometric polynomial method" [2], which is an extension of the above-mentioned polynomial method and was modified to be used with power queries in [3] to prove

[1]We will define power queries rigorously in Definition 1. Informally they are just an arbitrary (integer) power of a specific unitary matrix.

lower bounds for the phase estimation algorithm. Our method uses frequency analysis instead of a maximum degree argument, which is not applicable in the case of arbitrary powers.

## 2 The Sturm-Liouville eigenvalue problem

Papageorgiou and Woźniakowski study in [14] a simplified version of the univariate Sturm-Liouville problem. Consider the eigenvalue problem for the differential equation

$$\begin{aligned} -u''(x) + q(x)u(x) &= \lambda u(x) \\ u(0) = u(1) &= 0 \end{aligned} \tag{1}$$

for a given nonnegative function $q$ belonging to the class $\mathbf{Q}$ defined as

$$\mathbf{Q} = \left\{ q : [0,1] \to [0,1] \ : \ q \in C^2([0,1]) \text{ and } \max_{i=0,1,2} \max_{x \in [0,1]} |q^{(i)}(x)| \leq 1 \right\}. \tag{2}$$

We are looking for the smallest eigenvalue $\lambda$ such that there exists a non-zero function $u_\lambda$ that satisfies (1). What is the minimal number of queries of $q$ that permits the determination of the smallest eigenvalue $\lambda$ in this equation with error $\varepsilon$ and probability $3/4$ on a classical or quantum computer?

The one-dimensional time-independent Schrödinger equation

$$-\frac{\hbar^2}{2m}\frac{\mathrm{d}^2}{\mathrm{d}x^2}\Psi(x) + V(x)\Psi(x) = E\Psi(x) \tag{3}$$

of a particle in a box, see [10], is an instance of (1). We are given a potential $V$ and are looking for the eigenfunctions $\Psi$ of this equation and their corresponding energies $E$. In particular, we are interested in the ground-state and its energy, i.e., for a given potential $V$, we want to determine the eigenfunction $\Psi_0$ and its energy $E_0$, such that all other eigenfunctions $\Psi_n$ have higher energies $E_n \geq E_0$. Since quantum systems obey equation (3), it seems plausible that quantum computers could potentially solve the eigenvalue problem faster than a classical computer.

In the next section we define a quantum algorithm with power queries. We especially have to tackle the question concerning the form of the input (i.e., the function $q$ in the Sturm-Liouville problem) enters the quantum algorithm.

# 3 Quantum algorithms for the Sturm-Liouville problem

Let us denote the differential operator associated with the Sturm-Liouville problem for a certain $q \in \mathbf{Q}$ as $\mathbb{L}_q : C^2([0,\,1]) \to C^0([0,\,1])$, defined by

$$\mathbb{L}_q u(x) = -\frac{\mathrm{d}^2}{\mathrm{d}x^2} u(x) + q(x)u(x).$$

We discretize $\mathbb{L}_q$ by approximating the second derivative at the points $\frac{1}{n+1}$, $\frac{2}{n+1}$, ..., $\frac{n}{n+1}$ and obtain an $n \times n$ matrix $M_q$:

$$M_q = (n+1)^2 \begin{bmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 2 \end{bmatrix} + \begin{bmatrix} q(\frac{1}{n+1}) & & & & \\ & q(\frac{2}{n+1}) & & & \\ & & \ddots & & \\ & & & q(\frac{n-1}{n+1}) & \\ & & & & q(\frac{n}{n+1}) \end{bmatrix}. \quad (4)$$

The eigenvalues of $\mathbb{L}_q$ and $M_q$ are closely related. Let us denote the smallest eigenvalue of $\mathbb{L}_q$ by $\lambda(q)$ and let us write $\lambda_1(M_q)$ for the smallest eigenvalue of $M_q$. Then (see e.g. [9])

$$\lambda(q) - \lambda_1(M_q) = \mathcal{O}(n^{-2}). \quad (5)$$

The input $q \in \mathbf{Q}$ enters the quantum computer in the form of a unitary black-box transformation called a quantum query. For the Sturm-Liouville problem we define this query to be the unitary operator $\exp(\frac{i}{2}M_q)$. One can show that the smallest eigenvalue $\lambda(q)$ of the Sturm-Liouville equation satisfies $\pi^2 \leq \lambda(q) \leq \pi^2 + 1$. To avoid ambiguity we use proper scaling, i.e., instead of $\exp(iM_q)$ we use $\exp(\frac{i}{2}M_q)$, which defines a unique phase $\varphi \in [0,\,1)$ by $2\pi i\varphi = \frac{i}{2}\lambda(q)$.

We now define an associated quantum *power query* for $\exp(\frac{i}{2}M_q)$.

**Definition 1.** *Let $\mathbb{L}_q$ be the differential operator for a Sturm-Liouville problem and $M_q$ its discretization at $n$ points as in (4) for $q \in \mathbf{Q}$. We define the power query $W_l^p(\exp(\frac{i}{2}M_q))$ as*

$$W_l^p(\exp(\tfrac{i}{2}M_q)) \left|x_1\right\rangle \ldots \left|x_c\right\rangle \left|\psi\right\rangle = \begin{cases} \left|x_1\right\rangle \ldots \left|x_c\right\rangle \exp(\frac{i}{2}pM_q) \left|\psi\right\rangle & \text{for } x_l = 1 \\ \left|x_1\right\rangle \ldots \left|x_c\right\rangle \left|\psi\right\rangle & \text{otherwise} \end{cases}$$

*for all $x_1, \ldots, x_c \in \{0, 1\}$ and arbitrary normalized vectors $\left|\psi\right\rangle \in \mathbb{C}^n$ and extend this definition to all quantum states by linearity.*

Suppose that the $|\psi_s\rangle$, $s = 1, \ldots, n$, are the eigenvectors of $M_q$ and that $M_q |\psi_s\rangle = \lambda_s |\psi_s\rangle$. Then for $|\psi\rangle = \sum_{s=1}^{n} \alpha_s |\psi_s\rangle$ and $|x\rangle = |x_1\rangle \ldots |x_c\rangle$ with $x_l = 1$

$$W_l^p(\exp(\tfrac{i}{2}M_q))\,|x\rangle\,|\psi\rangle = |x\rangle \exp(\tfrac{i}{2}pM_q)\,|\psi\rangle = \sum_{s=1}^{n} \alpha_s\,|x\rangle\, e^{\frac{i}{2}p\lambda_s}\,|\psi_s\rangle\,.$$

Quantum algorithms are products of unitary transformations. Every quantum algorithm that approximates $\lambda(q)$ can be divided into stages that use powers of $\exp(\frac{i}{2}M_q)$ and therefore depend on $q$, and stages that are independent of $q$. Let us define a quantum algorithm with power queries.

**Definition 2.** *For a Sturm-Liouville problem given by the input $q \in \mathbf{Q}$ with the solution $\lambda(q)$, we define a quantum algorithm*

$$\mathcal{A} = (\left|\psi^{(0)}\right\rangle; U_0, \ldots, U_T; l_1, p_1, \ldots, l_T, p_T; \widetilde{\lambda})$$

*with $T$ power queries that solves this problem as follows. Let $U_0$, $U_1$, …, $U_T$ be arbitrary but fixed unitary transformations and $\left|\psi^{(0)}\right\rangle$ a fixed initial state. Let $W_{l_j}^{p_j}(\exp(\frac{i}{2}M_q))$ be a power query as in Definition 1. A measurement of the state*

$$\left|\psi^{(T)}(\exp(\tfrac{i}{2}M_q))\right\rangle = U_T W_{l_T}^{p_T}(\exp(\tfrac{i}{2}M_q)) \ldots U_1 W_{l_1}^{p_1}(\exp(\tfrac{i}{2}M_q)) U_0 \left|\psi^{(0)}\right\rangle$$

*in the standard basis yields a state $|k\rangle$ with probability $p_k(q)$. For each $k$ compute an approximation $\widetilde{\lambda}(k) \in \mathbb{R}$ to the eigenvalue of interest $\lambda(q)$ on a classical computer. For every $q \in \mathbf{Q}$ the probability that an $\varepsilon$-approximation $\widetilde{\lambda}(k)$ of $\lambda(q)$ is computed is given by*

$$\sum_{k:|\lambda(q)-\widetilde{\lambda}(k)|<\varepsilon} p_k(q). \tag{6}$$

*For any algorithm $\mathcal{A}$ with $T$ power queries we define*

$$e(\mathcal{A}, T) = \inf\left\{\varepsilon : \varepsilon \text{ chosen such that (6) is larger than } \tfrac{3}{4} \text{ for all } q \in \mathbf{Q}\right\}$$

*as the worst-case quantum error of $\mathcal{A}$.*

We measure in the standard basis for convenience only; a measurement in any other basis is easily achieved by modifying the operator $U_T$ accordingly.

A model like this was introduced in [1] for discrete inputs $q$. It was extended to continuous functions by Heinrich in [5]. Our model is an extension of this model to incorporate power queries.

# 4 Upper bounds

To estimate $\lambda(q)$ on a quantum computer with power queries Papageorgiou and Woźniakowski used the quantum phase estimation algorithm, see e.g. [12]. This algorithm takes a unitary transformation $Q$ with an eigenvector $|\xi\rangle$ as input, i.e., $Q|\xi\rangle = e^{2\pi i\varphi}|\xi\rangle$. Here $\varphi \in [0, 1)$ is called the "phase" of the eigenvalue corresponding to $|\xi\rangle$, and the phase estimation algorithm gives us an approximation $\widetilde{\varphi}$ to $\varphi$. This algorithm has the final state

$$\left|\psi^{(T)}(Q)\right\rangle = (\mathcal{F}_{2^T}^{-1} \otimes I) W_1^{2^{T-1}}(Q) W_2^{2^{T-2}}(Q) \dots W_T^{2^0}(Q) (H^{\otimes T} \otimes I) |0\rangle |\xi\rangle ,$$

and is depicted in Figure 1. Suppose $Q$ is a $r$ qubit transformation. A

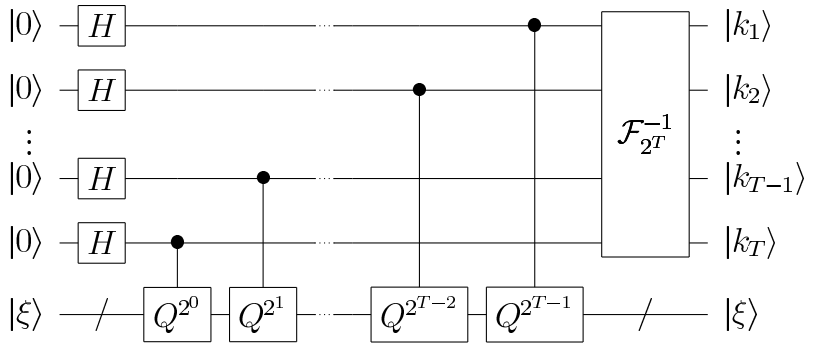


Figure 1: The quantum phase estimation algorithm. $\mathcal{F}_{2^T}^{-1}$ is the inverse quantum Fourier transform on $T$ qubits.

measurement of $\left|\psi^{(T)}(Q)\right\rangle$ returns a state

$$|k\rangle = |k_1\rangle \dots |k_T\rangle |k_{T+1}\rangle \dots |k_{T+r}\rangle .$$

The algorithm then uses $k$ to compute an approximation $\widetilde{\varphi}(k) = k_1 2^{-1} + k_2 2^{-2} + \dots + k_T 2^{-T}$ to $\varphi$ classically.

One can show, see e.g. [12], that with probability greater than $\frac{3}{4}$ the algorithm approximates $\varphi$ up to precision $\varepsilon$ with $\mathcal{O}(\log((1/\varepsilon)))$ power queries. Papageorgiou and Woźniakowski use this algorithm to approximate the smallest eigenvalue $\lambda(q)$ of the Sturm-Liouville operator $\mathbb{L}_q$ and use the operator $Q = \exp(\frac{i}{2} M_q)$ as a query. Since the phases of $\exp(\frac{i}{2} M_q)$ and $\exp(\frac{i}{2} \mathbb{L}_q)$ are related through equation (5), we have to discretize at $n = \mathcal{O}(\varepsilon^{-1/2})$ points.

The quantum phase estimation algorithm requires the knowledge of the eigenvector for which the phase is estimated. For the Sturm-Liouville problem we need the eigenvector $|z_1(M_q)\rangle$ of $M_q$ corresponding to the smallest eigenvalue $\lambda_1(M_q)$. We can compute $|z_1(M_q)\rangle$ through the method of Jaksch and Papageorgiou [8], which computes a superposition of eigenvectors $|z_j(M_q)\rangle$ of $M_q$, with a sufficiently large $|z_1(M_q)\rangle$ component. For details see [8, 14].

# 5 Lower Bounds

Our goal is to prove that the algorithm described in the previous section is optimal with respect to the number of power queries. We have to prove that every quantum algorithm $\mathcal{A}$ with $T$ power queries that returns a correct answer with precision $e(\mathcal{A}, T) \leq \varepsilon$ has to use $T = \Omega(\log(1/\varepsilon))$ power queries.

We will show that even for a much simplified version of the problem this lower bound still holds. Consider as input only constant functions $q(x) = q \in [0, 1]$. Obviously $q \in \mathbf{Q}$. It is easy to see that in this case the eigenfunctions which fulfill the boundary condition in (1) are

$$u_s(x) = \sin(s\pi x) \tag{7}$$

for $s \in \mathbb{N}$ and that they have eigenvalues $\lambda_s = s^2\pi^2 + q$, which means that the smallest eigenvalue $\lambda(q)$ is $\lambda(q) = \pi^2 + q$.

Similarly for the discretization $M_q$ of $\mathbb{L}_q$ with constant $q \in [0, 1]$ the eigenvectors are

$$|u_s\rangle = \sqrt{\tfrac{2}{n+1}} \sum_{x=1}^{n} \sin\left(\tfrac{s\pi x}{n+1}\right) |x\rangle \tag{8}$$

with eigenvalues $4(n+1)^2 \sin^2\left(\frac{s\pi}{2(n+1)}\right) + q$.

We want to investigate how different power queries lead to different outputs and turn to the techniques in [3]. For the following theorem we abbreviate $\vec{j} = (j_1, \ldots, j_n)$, $\vec{\varphi} = (\varphi_1, \ldots, \varphi_n)$, and use the following "dot product" notation:

$$\vec{j} \cdot \vec{\varphi} = j_1\varphi_1 + \ldots + j_n\varphi_n.$$

**Theorem 3.** *For a given orthonormal set of vectors $\{|\psi_s\rangle : s = 1, 2, \ldots, n\}$ consider all unitary matrices $Q$ for which the $|\psi_s\rangle$ are eigenvectors. Denote the eigenvalues corresponding to $|\psi_s\rangle$ by $e^{2\pi i\varphi_s}$, $\varphi_s \in [0, 1)$, $s = 1, 2, \ldots, n$.*

*Any quantum algorithm with power queries $W_l^p(Q)$, see Definition 2, that uses $c \in \mathbb{N}$ control qubits, can be written as*

$$\left|\psi^{(T)}(Q)\right\rangle = U_T W_{l_T}^{p_T}(Q) U_{T-1} \dots U_1 W_{l_1}^{p_1}(Q) U_0 \left|\psi^{(0)}\right\rangle = \sum_{k=0}^{n2^c-1} S_k^{(T)}(\vec{\varphi}) \left|k\right\rangle, \tag{9}$$

*where $S_k^{(T)}(\vec{\varphi})$ are trigonometric polynomials of the following form:*

$$S_k^{(T)}(\vec{\varphi}) = \sum_{\vec{j} \in \mathcal{J}_T} \alpha_{k,\vec{j}}^{(T)} e^{2\pi i \vec{j} \cdot \vec{\varphi}}, \tag{10}$$

*with $\mathcal{J}_T$ defined as $\mathcal{J}_0 = \{(0, \dots, 0)\}$ and*

$$\mathcal{J}_{T+1} = \big\{(j_1, \dots, j_n), (j_1 + p_{T+1}, \dots, j_n), \dots, (j_1, \dots, j_n + p_{T+1}) : (j_1, \dots, j_n) \in \mathcal{J}_T\big\}, \tag{11}$$

*and the coefficients $\alpha_{k,\vec{j}}^{(T)} \in \mathbb{C}$ do not depend on $\vec{\varphi}$ and are normalized:*

$$\sum_k \sum_{\vec{j} \in \mathcal{J}_T} |\alpha_{k,\vec{j}}^{(T)}|^2 = 1. \tag{12}$$

The proof of Theorem 3 can be found in the appendix. It is very similar to a proof in [3], but additionally proves equation (12).

In the Sturm-Liouville problem we are interested in the smallest eigenvalue $\lambda(q)$ of $\mathbb{L}_q$. Suppose we choose the constant functions $q(x) = q \in [0, 1)$ as input. The eigenfunctions $u_s$ of $\mathbb{L}_q$ and the eigenvectors $|u_s\rangle$ of $M_q$ are then independent of $q$, see (7), (8). Therefore we can apply Theorem 3 and write the final state $\left|\psi^{(T)}(q)\right\rangle = \left|\psi^{(T)}(\exp(\frac{i}{2}M_q))\right\rangle$ of any algorithm with $T$ power queries as

$$\left|\psi^{(T)}(q)\right\rangle = \sum_k S_k^{(T)}(\vec{\varphi}) \left|k\right\rangle = \sum_k \sum_{\vec{j} \in \mathcal{J}_T} \alpha_{k,\vec{j}}^{(T)} e^{2\pi i \vec{j} \cdot \vec{\varphi}} \left|k\right\rangle,$$

see equations (9) and (10), with $\vec{\varphi}$ depending on $q$. The eigenvalues of $M_q$ are $4(n+1)^2 \sin^2\left(\frac{s\pi}{2(n+1)}\right) + q$. This implies that the eigenvalues of $\exp(\frac{i}{2}M_q)$ are

$$e^{2\pi i \varphi_s} = e^{\frac{i}{2}\left(4(n+1)^2 \sin^2\left(\frac{s\pi}{2(n+1)}\right) + q\right)}.$$

Therefore we can split $e^{2\pi i\vec{j}\cdot\vec{\varphi}}$ as follows:

$$\begin{aligned} e^{2\pi i\vec{j}\cdot\vec{\varphi}} =& e^{\frac{i}{2}\left(j_1\left(4(n+1)^2\sin^2\left(\frac{\pi}{2(n+1)}\right)+q\right)+\ldots+j_n\left(4(n+1)^2\sin^2\left(\frac{n\pi}{2(n+1)}\right)+q\right)\right)} \\ =& e^{\frac{i}{2}\left(j_1 4(n+1)^2\sin^2\left(\frac{\pi}{2(n+1)}\right)+\ldots+j_n 4(n+1)^2\sin^2\left(\frac{n\pi}{2(n+1)}\right)\right)} e^{\frac{i}{2}(j_1+\ldots+j_n)q} \\ =:& \zeta_{(j_1,\ldots,j_n)} e^{\frac{i}{2}(j_1+\ldots+j_n)q}, \end{aligned}$$

which greatly simplifies $\left|\psi^{(T)}(q)\right\rangle$ as

$$\begin{aligned} \left|\psi^{(T)}(q)\right\rangle =& \sum_k \sum_{(j_1,\ldots,j_n)\in\mathcal{J}_T} \alpha^{(T)}_{k,(j_1,\ldots,j_n)} \zeta_{(j_1,\ldots,j_n)} e^{\frac{i}{2}(j_1+\ldots+j_n)q} \left|k\right\rangle \\ =:& \sum_k \sum_{m\in\mathcal{M}_T} \eta^{(T)}_{k,m} e^{\frac{i}{2}mq} \left|k\right\rangle \end{aligned} \tag{13}$$

with

$$\mathcal{M}_T = \{j_1+\ldots+j_n \,:\, (j_1,\ldots,j_n)\in\mathcal{J}_T\} \tag{14}$$

and the coefficients $\eta^{(T)}_{k,m}$ defined by

$$\eta^{(T)}_{k,m} = \sum_{\substack{(j_1,\ldots,j_n)\in\mathcal{J}_T \\ j_1+\ldots+j_n=m}} \alpha^{(T)}_{k,(j_1,\ldots,j_n)} \zeta_{(j_1,\ldots,j_n)}.$$

These coefficients $\eta^{(T)}_{k,m}$ are bounded in the following way:

$$\begin{aligned} \sum_k \sum_{m\in\mathcal{M}_T} |\eta^{(T)}_{k,m}|^2 \leq& \sum_k \sum_{m\in\mathcal{M}_T} \sum_{\substack{(j_1,\ldots,j_n)\in\mathcal{J}_T \\ j_1+\ldots+j_n=m}} |\alpha^{(T)}_{k,(j_1,\ldots,j_n)} \zeta_{(j_1,\ldots,j_n)}|^2 \\ =& \sum_k \sum_{\vec{j}\in\mathcal{J}_T} |\alpha^{(T)}_{k,\vec{j}}|^2 = 1, \end{aligned} \tag{15}$$

where we used $|\zeta_{(j_1,\ldots,j_n)}| = 1$ and equation (12).

**Lemma 4.** *Let $\mathcal{A}$ be a $T$ power query quantum algorithm for the Sturm-Liouville problem with powers $p_1,\ldots,p_T$ and $c\in\mathbb{N}$ control bits as defined in Definition 2. Let $\mathcal{B}$ be a partition of the set of all basis vectors, i.e.*

$$\bigcup_{B\in\mathcal{B}} B = \{|k\rangle \,:\, k=0,1,\ldots,n2^c-1\} \text{ and } B\cap C=\emptyset \text{ for } B,C\in\mathcal{B},\ B\neq C.$$

*If the input $q \in \mathbf{Q}$ is a constant function $q(x) = q \in [0,\, 1)$, the probability of measuring a state $|k\rangle$ from $B \in \mathcal{B}$ is a trigonometric polynomial*

$$p_B(q) = \sum_{l \in \mathcal{L}_T} \beta_{B,l}^{(T)} e^{\frac{i}{2} l q}, \tag{16}$$

*with coefficients $\beta_{B,l}^{(T)} \in \mathbb{C}$ that are bounded by*

$$\sum_{B \in \mathcal{B}} |\beta_{B,l}^{(T)}| \leq 1$$

*for all possible partitions $\mathcal{B}$, and the set $\mathcal{L}_T$ is given by $\mathcal{L}_0 = \{0\}$ and*

$$\mathcal{L}_{T+1} = \bigcup_{l \in \mathcal{L}_T} \{l,\, l + p_{T+1},\, l - p_{T+1}\}\,. \tag{17}$$

Lemma 4 is proven in the appendix. Note that $|\mathcal{L}_T| \leq 3^T$. This bound is sharp, since for the choice of $p_i = 3^{i-1}$ we have $\mathcal{L}_0 = \{0\}$, $\mathcal{L}_1 = \{-1, 0, 1\}$, $\mathcal{L}_2 = \{-4, -3, -2, \ldots, 3, 4\}$ and in general

$$\mathcal{L}_T = \left\{-3^T - 3^{T-1} - \ldots - 1, \ldots, 3^T + 3^{T-1} + \ldots + 1\right\}.$$

## 5.1 Fourier Analysis of Power Query Algorithms

With Theorem 3 and Lemma 4 we have the tools needed to provide a lower bound for the Sturm-Liouville problem. We are now able to apply our frequency analysis technique to this problem.

**Theorem 5.** *Any quantum algorithm $\mathcal{A}$ with $T$ power queries which estimates the smallest eigenvalue $\lambda(q)$ in the Sturm-Liouville eigenvalue problem for all inputs $q(x) = q \in [0,\, 1)$ with precision $e(\mathcal{A}, T) \leq \varepsilon$ and probability greater than $3/4$ has to use $T = \Omega(\log(1/\varepsilon))$ power queries.*

Notice that a lower bound on the "easy" subset of constant functions $q(x) = q$ implies that the same lower bound holds for any set of inputs that includes the constant functions, hence it also holds for the class $\mathbf{Q}$.

*Proof.* After $T$ power queries we measure the final state and receive a state $|k\rangle$ with probability $p_k(q)$. From the integer $k$ we classically compute a

solution $\widetilde{\lambda}(k)$. A successful algorithm has to return an $\varepsilon$-approximation for every $q \in [0,\, 1)$ with probability

$$\sum_{k:\left|\lambda(q)-\widetilde{\lambda}(k)\right|\leq\varepsilon} p_k(q) \geq \frac{3}{4},$$

see Definition 2. Define

$$A_{q,\varepsilon} := \{k : |\lambda(q) - \widetilde{\lambda}(k)| \leq \varepsilon\}$$

as the set of states that are mapped to $\varepsilon$-correct answers for input $q$. Choose $N \in \mathbb{N}$ such that $\frac{1}{N}$ is slightly bigger than $2\varepsilon$, i.e., $\frac{1}{N+1} \leq 2\varepsilon < \frac{1}{N}$ and define the points $x_r := (r + 1/2)/N$ for $r = 0, 1, \ldots, N-1$. For the inputs $q = x_r$ we can visualize the quantum algorithm $\mathcal{A}$ as in Figure 2. Notice that the sets $A_{x_r,\varepsilon}$ are mutually disjoint for $r = 0, \ldots, N-1$, because $x_r$ and $x_{r+1}$ are chosen such that

$$|\lambda(x_r) - \lambda(x_{r+1})| = \left|16\sin^2\left(\tfrac{\pi}{4}\right) + \tfrac{r+\frac{1}{2}}{N} - 16\sin^2\left(\tfrac{\pi}{4}\right) - \tfrac{r+1+\frac{1}{2}}{N}\right| = \frac{1}{N} > 2\varepsilon.$$

Therefore there can be no state $|k\rangle$ that is mapped to an output $\widetilde{\lambda}(k)$, which is an $\varepsilon$-approximation to $\lambda(x_r)$ and $\lambda(x_{r+1})$ at the same time. Let

$$p_{r,\varepsilon}(q) = \sum_{k\in A_{x_r,\varepsilon}} p_k(q) \tag{18}$$

be the probability of measuring an $\varepsilon$-approximation to $\lambda(x_r)$. Since the sets $A_{x_r,\varepsilon}$ partition the set of all outputs, Lemma 4 allows us to write

$$p_{r,\varepsilon}(q) = p_{A_{x_r,\varepsilon}}(q) = \sum_{l\in\mathcal{L}_T} \beta^{(T)}_{r,\varepsilon,l} e^{\frac{i}{2}lq}.$$

We apply the $N$-point inverse discrete Fourier Transform to $p_{r,\varepsilon}(q)$, which

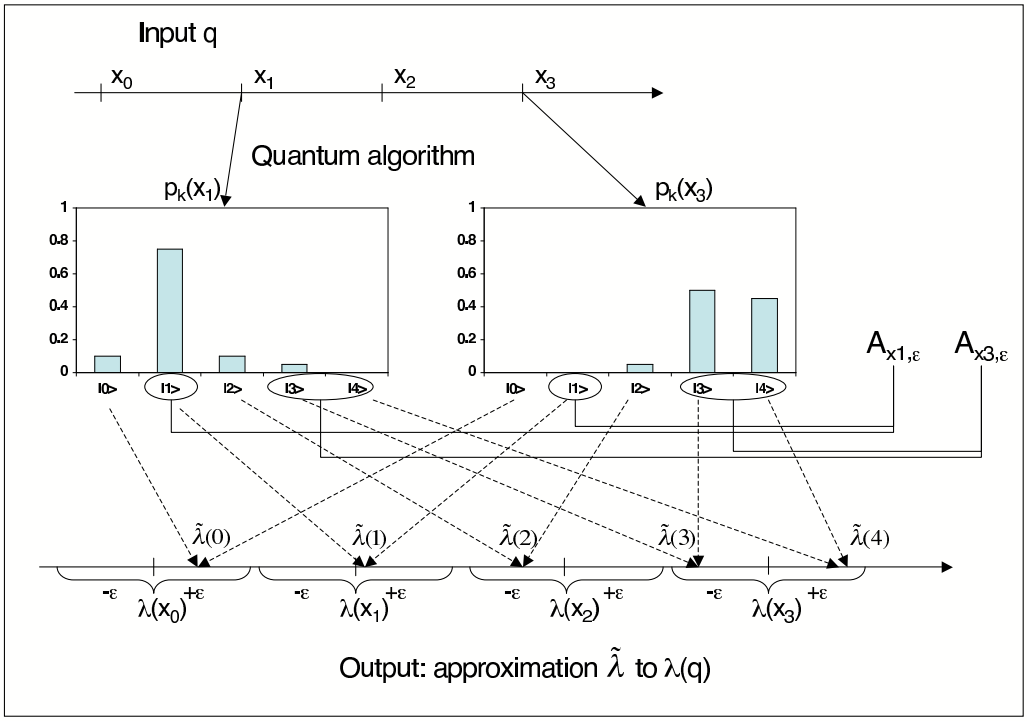


Figure 2: A quantum algorithm for the Sturm-Liouville problem with inputs $q = x_r$, $r = 0, \ldots, N-1$, will result in a probability distribution $p_k(q)$ on the states $|k\rangle$ that are measured. Each state $|k\rangle$ is mapped to an answer $\widetilde{\lambda}(k)$. We write $A_{x_r,\epsilon}$ for the set of all states $|k\rangle$ that are mapped to $\varepsilon$-approximations of $\lambda(x_r)$.

we evaluate at the points $x_n$, and get the following value at $k = 0, 1, \ldots, N-1$:

$$\begin{aligned} DFT_N[p_{r,\varepsilon}](k) &= \sum_{n=0}^{N-1} p_{r,\varepsilon}(x_n) e^{-2\pi i k n/N} \\ &= \sum_{n=0}^{N-1} \sum_{l \in \mathcal{L}_T} \beta_{r,\varepsilon,l}^{(T)} e^{\frac{i}{2} l(n+1/2)/N} e^{-2\pi i k n/N} \\ &= \sum_{l \in \mathcal{L}_T} \beta_{r,\varepsilon,l}^{(T)} e^{\frac{i}{2} l/(2N)} \sum_{n=0}^{N-1} e^{2\pi i (\frac{l}{4\pi} - k) n/N} \\ &= \sum_{l \in \mathcal{L}_T} \beta_{r,\varepsilon,l}^{(T)} e^{\frac{i}{2} l/(2N)} \left\{ \begin{array}{ll} \frac{e^{2\pi i (\frac{l}{4\pi} - k)} - 1}{e^{2\pi i (\frac{l}{4\pi} - k)/N} - 1}, & \frac{l}{4\pi} \not\equiv k \pmod{N} \\ N, & \frac{l}{4\pi} \equiv k \pmod{N} \end{array} \right\} \end{aligned} \tag{19}$$

where $\frac{l}{4\pi} \equiv k \pmod N$ indicates that there exists an integer $z$ such that $\frac{l}{4\pi} = k + zN$. For every $l$ define $l_{/4\pi(N)} \in [0,\, N)$ as

$$l_{/4\pi(N)} := \min\left\{ l/(4\pi) - zN \,:\, z = 0, 1, 2, ...,\ \text{and}\ l/(4\pi) - zN \geq 0 \right\}.$$

Then $\exp(2\pi i \frac{l}{4\pi}/N) = \exp(2\pi i l_{/4\pi(N)}/N)$. To take the absolute value of equation (19), we use $\left|e^{i2\theta} - 1\right| = 2\left|\sin(\theta)\right|$ and get

$$\left|DFT_N[p_{r,\varepsilon}](k)\right| \;\leq\; \sum_{l \in \mathcal{L}_T} \left|\beta^{(T)}_{r,\varepsilon,l}\right| \left\{ \begin{array}{ll} \frac{\left|\sin(\pi(l_{/4\pi(N)} - k))\right|}{\left|\sin(\pi(l_{/4\pi(N)} - k)/N)\right|} & , l_{/4\pi(N)} \neq k \\ N & , l_{/4\pi(N)} = k \end{array} \right\} \quad (20)$$

We can bound the Fourier transform (19) by separating the correct answers, i.e., the $\varepsilon$-approximations to $x_r$, from the rest: if the input $q = x_r$ then the algorithm has to return an answer $\widetilde{\lambda}$ that is $\varepsilon$-close to the correct answer $\lambda(x_r)$ with probability greater or equal $3/4$. This probability is given by $p_{r,\varepsilon}(q)$, i.e., we demand that $p_{r,\varepsilon}(x_r) \geq 3/4$. Then:

$$\begin{aligned} \Big| \sum_{n=0}^{N-1} p_{r,\varepsilon}(x_n) e^{-2\pi i k n/N} \Big| \geq & \Big| p_{r,\varepsilon}(x_r) \Big| - \sum_{\substack{n=0 \\ n \neq r}}^{N-1} \Big| p_{r,\varepsilon}(x_n) \Big| \\ \geq & \frac{3}{4} - \sum_{\substack{n=0 \\ n \neq r}}^{N-1} p_{r,\varepsilon}(x_n), \end{aligned} \quad (21)$$

Consider the second term in (21), $\sum_{\substack{n=0 \\ n \neq r}}^{N-1} p_{r,\varepsilon}(x_n)$. Recall that $p_{r,\varepsilon}(q)$ is the probability that the algorithm measures a state $|k\rangle$ that is mapped to an answer $\widetilde{\lambda}(k)$ that is an $\varepsilon$-approximation to $\lambda(x_r)$, i.e., $|k\rangle \in A_{x_r,\varepsilon}$, see (18). This probability $p_{r,\varepsilon}(q)$ depends on the actual input $q$. For input $q = x_n \neq x_r$ a state $|k\rangle \in A_{x_r,\varepsilon}$ will *not* yield an $\varepsilon$-correct answer: we chose the $x_n$, $n = 0, \ldots, N-1$, such that $|\lambda(x_n) - \lambda(x_r)| > 2\varepsilon$ for $n \neq r$, and thus there cannot be an $\varepsilon$ close answer for both $x_r$ and $x_n$. The sum $\sum_{\substack{n=0 \\ n \neq r}}^{N-1} p_{r,\varepsilon}(x_n)$ now tells us how often the algorithm chooses a state from $A_{r,\varepsilon}$.

If we knew that none of the wrong answers is preferred by our algorithm, say e.g. $\sum_{\substack{n=0 \\ n \neq r}}^{N-1} p_{r,\varepsilon}(x_n) < \frac{1}{2}$, equation (21) would read

$$\Big| \sum_{n=0}^{N-1} p_{r,\varepsilon}(x_n) e^{-\frac{2\pi i k n}{N}} \Big| \geq \frac{3}{4} - \sum_{\substack{n=0 \\ n \neq r}}^{N-1} p_{r,\varepsilon}(x_n) > \frac{1}{4}. \quad (22)$$

We will show that this property has to be true for some $r = 0, \ldots, N-1$, indexing the set of states $A_{x_r,\varepsilon}$ that represents numbers $\varepsilon$-close to $x_r$. Let $R^<$ be the set of all $r$ for which $\sum_{\substack{n=0 \\ n\neq r}}^{N-1} p_{r,\varepsilon}(x_n) < \frac{1}{2}$ holds and $R^{\geq}$ the set for which it does not. We estimate the number of elements of $R^<$ by splitting

$$N = \sum_{n=0}^{N-1} 1 \geq \sum_{n=0}^{N-1}\sum_{r=0}^{N-1} p_{r,\varepsilon}(x_n) = \sum_{r=0}^{N-1} p_{r,\varepsilon}(x_r) + \sum_{r=0}^{N-1}\sum_{\substack{n=0 \\ n\neq r}}^{N-1} p_{r,\varepsilon}(x_n)$$

into the following parts:

$$\begin{aligned} N &\geq \sum_{r=0}^{N-1} p_{r,\varepsilon}(x_r) + \sum_{r\in R^<}\sum_{\substack{n=0 \\ n\neq r}}^{N-1} p_{r,\varepsilon}(x_n) + \sum_{r\in R^{\geq}}\sum_{\substack{n=0 \\ n\neq r}}^{N-1} p_{r,\varepsilon}(x_n) \\ &\geq N\frac{3}{4} \qquad\qquad + |R^<| \cdot 0 \qquad\qquad + \left|R^{\geq}\right| \frac{1}{2} \end{aligned}$$

and therefore we can conclude that $\left|R^{\geq}\right| \leq \frac{1}{2}N$ and thus $|R^<| \geq \frac{1}{2}N$. Now $|R^<| > 0$ implies that we can actually choose an element $r \in R^<$. Fix such an $r$ and we can combine equations (20) and (22) to

$$1/4 < \sum_{l\in\mathcal{L}_T} \left|\beta^{(T)}_{r,\varepsilon,l}\right| \left\{ \begin{array}{ll} \frac{\left|\sin(\pi(l_{/4\pi(N)}-k))\right|}{\left|\sin(\pi(l_{/4\pi(N)}-k)/N)\right|} & , l_{/4\pi(N)} \neq k \\ N & , l_{/4\pi(N)} = k \end{array} \right\}. \tag{23}$$

We will now fix the parameter $k = 0, 1, \ldots, N-1$ in inequality (23) in such a way that the terms in the sum on the right-hand-side of the inequality are as small as possible. This will imply that the sum must be over a large number of elements, i.e., that $|\mathcal{L}_T|$ is large. Since $|\mathcal{L}_T| \leq 3^T$ this will help us to ultimately prove that $T = \Omega(\log N)$ if we could show that $|\mathcal{L}_T| = \Omega(N)$. More specifically we will show that $|\mathcal{L}_T|^2 \geq \frac{1}{10}N$ which proves $T = \Omega(\log N)$.

We prove $|\mathcal{L}_T|^2 \geq \frac{1}{10}N$ by contradiction. Assume $|\mathcal{L}_T|^2 < \frac{1}{10}N$. This assumption allows us to find a $k$ such that the right-hand-side of inequality (23) is smaller than the left-hand-side, which will lead to our desired contradiction.

If we project $\mathcal{L}_T$ into the interval $[0,\ N)$ through $l \mapsto l_{/4\pi(N)}$ we will get a set $\left\{l_{/4\pi(N)} : l \in \mathcal{L}_T\right\}$. Order this set as $0 \leq t_1 \leq t_2 \leq \ldots \leq t_{|\mathcal{L}_T|} < N$. This defines "gaps" between these numbers, i.e., intervals $G = (t_j,\ t_{j+1})$ for $j = 1, \ldots, |\mathcal{L}_T|$ if we define $t_{|\mathcal{L}_T|+1} = t_1 + N$ (we "wrap around"). Define the

width $w(G)$ of such a gap $G$ as the distance between its endpoints. Thus $w((t_j,\, t_{j+1})) = t_{j+1} - t_j$.

Let $G_m$ be the gap with the maximal width $w(G_m)$ in the distribution. Its width must be $w(G_m) \geq N/\left|\mathcal{L}_T\right|$, since

$$N = \sum_G w(G) \leq \sum_G \max_G w(G) = \left|\mathcal{L}_T\right| \max_G w(G).$$

Additionally $w(G_m) > 10$, since we assumed $\left|\mathcal{L}_T\right|^2 < \frac{1}{10}N$ and therefore $\frac{N}{\left|\mathcal{L}_T\right|} > 10\left|\mathcal{L}_T\right| \geq 10$. Thus there are at least ten integers $k \in \{0, 1, \ldots, N-1\}$ that fall into this largest gap $G_m$, i.e $k \in G_m$. One of these $k$ has maximum distance to *both* boundaries $t_j$ and $t_{j+1}$ of $G_m$: it is the $k$ that is closest to the middle $m = \frac{t_{j+1}+t_j}{2}$ of $G_m = (t_j,\, t_{j+1})$. This integer $k$ fulfills $|k-m| \leq \frac{1}{2}$ and

$$\begin{aligned}\min\{k - t_j, t_{j+1} - k\} &= \min\{m - t_j + k - m, m - k + t_{j+1} - m\} \\ &\geq \frac{w(G_m)}{2} - \frac{1}{2} \geq \frac{N}{2\left|\mathcal{L}_T\right|} - \frac{1}{2}.\end{aligned}$$

Fix this $k \in (t_j,\, t_{j+1})$. Now $|\sin(x)| \geq 2/\pi\,|x|$ for $-\pi/2 \leq x \leq \pi/2$ and therefore

$$\begin{aligned}\min_{l\in\mathcal{L}_T}\left|\sin\frac{\pi(l_{/4\pi(N)} - k)}{N}\right| &\geq \min_{l\in\mathcal{L}_T}\frac{2}{N}\left|l_{/4\pi(N)} - k\right| = \frac{2}{N}\min\{k - t_j, t_{j+1} - k\} \\ &\geq \frac{1}{\left|\mathcal{L}_T\right|} - \frac{1}{N}.\end{aligned}$$

Then we can use this to estimate (23):

$$1/4 < \sum_{l\in\mathcal{L}_T}\left|\beta^{(T)}_{r,\varepsilon,l}\right|\frac{\left|\sin(\pi(l_{/4\pi(N)} - k))\right|}{\left|\sin(\pi(l_{/4\pi(N)} - k)/N)\right|} \leq \sum_{l\in\mathcal{L}_T}\left|\beta^{(T)}_{r,\varepsilon,l}\right|\frac{1}{1/\left|\mathcal{L}_T\right| - 1/N}$$

We sum the last inequality over all $r \in R^<$ for which it is valid, and get:

$$\sum_{r\in R^<}\frac{1}{4} \leq \frac{1}{1/\left|\mathcal{L}_T\right| - 1/N}\sum_{r\in R^<}\sum_{l\in\mathcal{L}_T}\left|\beta^{(T)}_{r,\varepsilon,l}\right| \tag{24}$$

Since the number of elements in $R^<$ is bounded by $|R^<| \geq \frac{1}{2}N$, the left-hand-side of (24) is bounded by $\frac{1}{8}N \leq |R^<|\,\frac{1}{4}$. The right-hand-side of inequality (24) can be bounded through Lemma 4:

$$\sum_{r\in R^<}\sum_{l\in\mathcal{L}_T}\left|\beta^{(T)}_{r,\varepsilon,l}\right| \leq \left|\mathcal{L}_T\right|.$$

If we put both sides together again and recall that we assumed $|\mathcal{L}_T|^2 < \frac{1}{10}N$ we get

$$\frac{1}{8}N \leq \frac{|\mathcal{L}_T|}{1/|\mathcal{L}_T| - 1/N} = \frac{|\mathcal{L}_T|^2}{1 - |\mathcal{L}_T|/N} < \frac{\frac{1}{10}N}{1 - \frac{1}{10|\mathcal{L}_T|}} \leq \frac{\frac{1}{10}N}{1 - \frac{1}{10}} = \frac{1}{9}N,$$

which is a contradiction.

Therefore $|\mathcal{L}_T|^2 \geq \frac{1}{10}N$ must hold. This, together with $|\mathcal{L}_T| \leq 3^T$, leads us to $N \leq 10 \cdot 9^T$. Take the logarithm and we get $T = \Omega(\log N)$. We chose $N$ such that $\frac{1}{N+1} \leq 2\varepsilon < \frac{1}{N}$ which finally proves that the number of power queries $T$ for any algorithm $\mathcal{A}$ with error $e(\mathcal{A}, T) \leq \varepsilon$ has to be of the order $T = \Omega(\log(1/\varepsilon))$. □

# 6 Discussion

In this paper we have proven lower bounds for the number of quantum power queries for the Sturm-Liouville problem and settled an open problem in [14].

How does this number of $T = \Theta(\log(1/\varepsilon))$ power queries relate to the cost of quantum algorithms? Here we understand "cost" as an abstraction on the number of elementary quantum gates or the duration for which a Hamiltonian has to be applied to a quantum system. Suppose the function $q$ is from a class $\mathbf{Q}' \subseteq \mathbf{Q}$ where each power query $W_l^p(\exp(\frac{i}{2}M_q))$ can be implemented with $\mathrm{cost}(W_l^p(\exp(\frac{i}{2}M_q))) = \mathrm{cost}(\mathbf{Q}', p)$.

If we implement $W_l^p(\exp(\frac{i}{2}M_q))$ naively as

$$W_l^p(\exp(\tfrac{i}{2}M_q)) = \left(W_l^1(\exp(\tfrac{i}{2}M_q))\right)^p,$$

then $\mathrm{cost}(\mathbf{Q}', p) = p \cdot \mathrm{cost}(\mathbf{Q}')$ and the cost of the Sturm-Liouville algorithm with $T = \Theta(\log(1/\varepsilon))$ power queries grows as

$$\sum_{j=0}^{T-1} \mathrm{cost}(\mathbf{Q}', 2^j) = \sum_{j=0}^{T-1} 2^j \cdot \mathrm{cost}(\mathbf{Q}') = (2^T - 1) \cdot \mathrm{cost}(\mathbf{Q}') = \Theta(1/\varepsilon) \cdot \mathrm{cost}(\mathbf{Q}').$$

This is polynomial in $1/\varepsilon$ just like the Sturm-Liouville algorithm with bit queries discussed in [14]. To take advantage of the proposed power query algorithm it is therefore necessary to realize power queries $W_l^p(\exp(\frac{i}{2}M_q))$ on a quantum computer in such a way that $\mathrm{cost}(\mathbf{Q}', p) = o(p) \cdot \mathrm{cost}(\mathbf{Q}')$

The implementation of power queries with cost that is not linear in the power $p$ of the query is still not settled and requires more work. It would be of interest to identify subclasses $\mathbf{Q}' \subseteq \mathbf{Q}$ for which we are able to prove $\mathrm{cost}(\mathbf{Q}', p) = o(p) \cdot \mathrm{cost}(\mathbf{Q}')$.

Another open question is whether it is possible to extend the methods we used for upper and lower bounds for the Sturm-Liouville problem in one dimension to the Sturm-Liouville problem in higher dimensions. Most important for this problem is probably the extension of the results in [8] on good enough approximations of the eigenvector with the smallest eigenvalue to higher dimensional Sturm-Liouville problems.

# 7 Acknowledgments

The author would like to thank M. Kwas, A. Papageorgiou, J. Traub and H. Woźniakowski for inspiring discussions. Partial funding was provided by Columbia University through a Presidential Fellowship. This research was supported in part by the National Science Foundation and the Defense Advanced Research Projects Agency.

# A Proofs of Theorem 3 and Lemma 4

*Proof of Theorem 3.* We want to prove that for a unitary operation $Q$ with fixed eigenvectors $|\psi_s\rangle$ and varying eigenvalues $e^{2\pi i \varphi_s}$, $s = 1, \ldots, n$, every quantum algorithm with power queries $W_l^p(Q)$ as in Definition 2 can be written as

$$\left|\psi^{(T)}(Q)\right\rangle = U_T W_{l_T}^{p_T}(Q) U_{T-1} \ldots U_1 W_{l_1}^{p_1}(Q) U_0 \left|\psi^{(0)}\right\rangle = \sum_k S_k^{(T)}(\vec{\varphi}) \left|k\right\rangle .$$

In this equation the trigonometric polynomials $S_k^{(T)}(\vec{\varphi}) = \sum_{\vec{j} \in \mathcal{J}_T} \alpha_{k,\vec{j}}^{(T)} e^{2\pi i \vec{j} \cdot \vec{\varphi}}$ are of powers $\mathcal{J}_T$, with $\mathcal{J}_T$ recursively in Equation (11). We also claim that the coefficients $\alpha_{k,\vec{j}}^{(T)} \in \mathbb{C}$ fulfill $\sum_k \sum_{\vec{j} \in \mathcal{J}_T} |\alpha_{k,\vec{j}}^{(T)}|^2 = 1$.

The proof is by induction on the number of queries $T$. We will write the state of the algorithm after $T$ steps $\left|\psi^{(T)}(Q)\right\rangle$ in the basis $(\left|k\right\rangle \left|\psi_s\right\rangle)_{k,s}$, which is split into a control part $|k\rangle$ and an eigenvector part $|\psi_s\rangle$. We will not address the ancilla qubits in our proof, but they can easily be treated (after possibly reordering the qubits) as control bits that are never used.

At the start of the algorithm we can write

$$U_0 \left|\psi^{(0)}\right\rangle = \sum_{k,s} \alpha^{(0)}_{k,s,(0,\ldots,0)} \left|k\right\rangle \left|\psi_s\right\rangle ,$$

which contains only powers $e^{2\pi i\vec{j}\cdot\vec{\varphi}}$ from $\vec{j} \in \mathcal{J}_0 = \{(0,\ldots,0)\}$ and obviously

$$\sum_{k,s} \sum_{\vec{j}\in\mathcal{J}_0} |\alpha^{(0)}_{k,s,\vec{j}}|^2 = \sum_{k,s} |\alpha^{(0)}_{k,s,(0,\ldots,0)}|^2 = 1.$$

Let us now assume $\left|\psi^{(T)}(Q)\right\rangle$ can be written as

$$\left|\psi^{(T)}(Q)\right\rangle = \sum_{k,s} \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} \left|k\right\rangle \left|\psi_s\right\rangle ,$$

with coefficients $\alpha^{(T)}_{k,s,\vec{j}}$ fulfilling condition (12). If we apply $W^{p_{T+1}}_{l_{T+1}}(Q)$ to $\left|\psi^{(T)}(Q)\right\rangle$ we get ($k_{l_{T+1}}$ is the control bit, i.e., the $l_{T+1}$-th bit in the binary representation of $k$):

$$\begin{aligned} W^{p_{T+1}}_{l_{T+1}}(Q)\left|\psi^{(T)}(Q)\right\rangle = & \sum_{\substack{k,s \\ k_{l_{T+1}}=0}} \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} \left|k\right\rangle \left|\psi_s\right\rangle \\ & + \sum_{\substack{k,s \\ k_{l_{T+1}}=1}} \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} \left|k\right\rangle Q^{p_{T+1}} \left|\psi_s\right\rangle . \end{aligned}$$

We analyze the second term where the control bit is set and get the following sum over $\mathcal{J}_{T+1}$ (here $\vec{e_s}$ is the $s$-th unit vector $(0,\ldots,0,1,0,\ldots,0)$):

$$\begin{aligned} \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} \left|k\right\rangle Q^{p_{T+1}} \left|\psi_s\right\rangle &= \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} e^{2\pi i p_{T+1}\varphi_s} \left|k\right\rangle \left|\psi_s\right\rangle \\ &= \sum_{\vec{j}\in\mathcal{J}_T} \alpha^{(T)}_{k,s,\vec{j}} e^{2\pi i(\vec{j}+p_{T+1}\vec{e_s})\cdot\vec{\varphi}} \left|k\right\rangle \left|\psi_s\right\rangle \\ &=: \sum_{\vec{j}\in\mathcal{J}_{T+1}} \widetilde{\alpha}^{(T+1)}_{k,s,\vec{j}} e^{2\pi i\vec{j}\cdot\vec{\varphi}} \left|k\right\rangle \left|\psi_s\right\rangle \end{aligned}$$

where $\widetilde{\alpha}^{(T+1)}_{k,s,\vec{j}}$ is defined as

$$\widetilde{\alpha}^{(T+1)}_{k,s,\vec{j}} := \begin{cases} \alpha^{(T)}_{k,s,\vec{j}-p_{T+1}\vec{e_s}} & \text{for } k_{l_{T+1}} = 1 \text{ and } \vec{j} - p_{T+1}\vec{e_s} \in \mathcal{J}_T \\ \alpha^{(T)}_{k,s,\vec{j}} & \text{for } k_{l_{T+1}} = 0 \text{ and } \vec{j} \in \mathcal{J}_T \\ 0 & \text{otherwise} \end{cases}$$

Thus we can write

$$W_{l_{T+1}}^{p_{T+1}}(Q)\big|\psi^{(T)}(Q)\big\rangle = \sum_{k,s}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)} e^{2\pi i\vec{j}\cdot\vec{\varphi}}\,|k\rangle\,|\psi_s\rangle$$

and our normalization condition (12) holds for $\widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)}$,

$$\begin{aligned}\sum_{k,s}\sum_{\vec{j}\in\mathcal{J}_{T+1}} |\widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)}|^2 &= \sum_{\substack{k,s\\ k_{l_{T+1}}=0}}\sum_{\vec{j}\in\mathcal{J}_T} |\alpha_{k,s,\vec{j}}^{(T)}|^2 + \sum_{\substack{k,s\\ k_{l_{T+1}}=1}}\sum_{\vec{j}-p_{T+1}\vec{e_s}\in\mathcal{J}_T} |\alpha_{k,s,\vec{j}-p_{T+1}\vec{e_s}}^{(T)}|^2\\ &= \sum_{k,s}\sum_{\vec{j}\in\mathcal{J}_T} |\alpha_{k,s,\vec{j}}^{(T)}|^2 = 1.\end{aligned}$$

The next step is to apply $U_{T+1}$ to $W_{l_{T+1}}^{p_{T+1}}(Q)\big|\psi^{(T)}(Q)\big\rangle$. Define the coefficients $u_{l,t,k,s} = \langle l,t|\,U_{T+1}\,|k,s\rangle$. Then we can define $\alpha_{l,t,\vec{j}}^{(T+1)}$ such that

$$\begin{aligned}U_{T+1}W_{l_{T+1}}^{p_{T+1}}(Q)\big|\psi^{(T)}(Q)\big\rangle &= \sum_{k,s}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)} e^{2\pi i\vec{j}\cdot\vec{\varphi}} U_{T+1}\,|k\rangle\,|\psi_s\rangle\\ &= \sum_{l,t}\sum_{\vec{j}\in\mathcal{J}_{T+1}}\sum_{k,s} \widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)} u_{l,t,k,s} e^{2\pi i\vec{j}\cdot\vec{\varphi}}\,|l\rangle\,|\psi_t\rangle\\ &=: \sum_{l,t}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \alpha_{l,t,\vec{j}}^{(T+1)} e^{2\pi i\vec{j}\cdot\vec{\varphi}}\,|l\rangle\,|\psi_t\rangle\,.\end{aligned}$$

It remains to check that

$$\begin{aligned}\sum_{l,t}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \left|\alpha_{l,t,\vec{j}}^{(T+1)}\right|^2 &= \sum_{l,t}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \left[\sum_{k,s}\left(\widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)}\right)^*\left(u_{l,t,k,s}\right)^*\right]\left[\sum_{k',s'}\widetilde{\alpha}_{k',s',\vec{j}}^{(T+1)} u_{l,t,k',s'}\right]\\ &= \sum_{k,s,k',s'}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \left(\widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)}\right)^*\left[\sum_{l,t}\left(u_{l,t,k,s}\right)^* u_{l,t,k',s'}\right]\widetilde{\alpha}_{k',s',\vec{j}}^{(T+1)}\\ &= \sum_{k,s}\sum_{\vec{j}\in\mathcal{J}_{T+1}} \left|\widetilde{\alpha}_{k,s,\vec{j}}^{(T+1)}\right|^2 = 1.\end{aligned}$$

□

*Proof of Lemma 4.* Consider quantum queries $\exp(\frac{i}{2}M_q)$ for constant functions $q(x) = q \in [0,1)$ in the Sturm-Liouville problem. From equation (13)

we know that the final state of every $T$ power query algorithm can be written as

$$\left|\psi^{(T)}(q)\right\rangle = \sum_k \sum_{m\in\mathcal{M}_T} \eta_{k,m}^{(T)} e^{\frac{i}{2}mq} \left|k\right\rangle .$$

Let $\mathcal{B}$ be a partition of the set of all basis states $|k\rangle$. Thus the probability to measure a state from the set $B \in \mathcal{B}$ is

$$\begin{aligned} p_B(q) =& \sum_{k\in B} \left| \sum_{m\in\mathcal{M}_T} \eta_{k,m}^{(T)} e^{\frac{i}{2}mq} \right|^2 \\ =& \sum_{k\in B} \left[ \sum_{m_1\in\mathcal{M}_T} \left(\eta_{k,m_1}^{(T)}\right)^* e^{-\frac{i}{2}m_1 q} \right] \left[ \sum_{m_2\in\mathcal{M}_T} \eta_{k,m_2}^{(T)} e^{\frac{i}{2}m_2 q} \right] \\ =& \sum_{k\in B} \sum_{m_1,m_2\in\mathcal{M}_T} \left(\eta_{k,m_1}^{(T)}\right)^* \eta_{k,m_2}^{(T)} e^{\frac{i}{2}(m_2-m_1)q} \\ =:& \sum_{l\in\mathcal{L}_T} \beta_{B,l}^{(T)} e^{\frac{i}{2}lq}, \end{aligned}$$

where the set $\mathcal{L}_T$ is

$$\mathcal{L}_T = \{m_1 - m_2 \,:\, m_1, m_2 \in \mathcal{M}_T\} . \tag{25}$$

and with coefficients $\beta_{B,l}^{(T)}$ defined by

$$\beta_{B,l}^{(T)} := \sum_{k\in B} \sum_{\substack{m_1,m_2\in\mathcal{M}_T \\ m_2-m_1=l}} \left(\eta_{k,m_1}^{(T)}\right)^* \eta_{k,m_2}^{(T)}. \tag{26}$$

For any partition $\mathcal{B}$ we can now bound the $\beta_{B,l}^{(T)}$ as follows

$$\begin{aligned} \sum_{B\in\mathcal{B}} \left|\beta_{B,l}^{(T)}\right| =& \sum_{B\in\mathcal{B}} \left| \sum_{k\in B} \sum_{\substack{m_1,m_2\in\mathcal{M}_T \\ m_2-m_1=l}} \left(\eta_{k,m_1}^{(T)}\right)^* \eta_{k,m_2}^{(T)} \right| \\ \leq& \sum_k \sum_{\substack{m_1,m_2\in\mathcal{M}_T \\ m_2-m_1=l}} \left| \eta_{k,m_1}^{(T)} \eta_{k,m_2}^{(T)} \right| , \end{aligned}$$

where $\sum_k$ is the sum over all possible states $|k\rangle$. From (15) we now derive

by the Cauchy-Schwarz inequality

$$\sum_k \sum_{\substack{m_1,m_2\in\mathcal{M}_T \\ m_2-m_1=l}} \left|\eta_{k,m_1}^{(T)}\eta_{k,m_2}^{(T)}\right| = \sum_k \sum_{m:m,m+l\in\mathcal{M}_T} \left|\eta_{k,m}^{(T)}\eta_{k,m+l}^{(T)}\right|$$

$$\leq \sum_k \left(\sum_{m\in\mathcal{M}_T} \left|\eta_{k,m}^{(T)}\right|^2\right)^{1/2} \left(\sum_{m+l\in\mathcal{M}_T} \left|\eta_{k,m+l}^{(T)}\right|^2\right)^{1/2} \leq \sum_k \sum_{m\in\mathcal{M}_T} \left|\eta_{k,m}^{(T)}\right|^2 \leq 1.$$

It remains to show that the two definitions of $\mathcal{L}_T$ in equations (17) and (25) are identical. The proof is by induction. $T = 0$ is trivially true. We use the definitions (11), (14) of $\mathcal{J}_T$ and $\mathcal{M}_T$ to see that

$$\begin{aligned}
\mathcal{M}_{T+1} &= \left\{ j_1 + \ldots + j_n \,:\, \vec{j} \in \mathcal{J}_{T+1} \right\} \\
&= \left\{ j_1 + \ldots + j_n, j_1 + \ldots + j_n + p_{T+1} \,:\, \vec{j} \in \mathcal{J}_T \right\} \\
&= \{ m, m + p_{T+1} \,:\, m \in \mathcal{M}_T \} .
\end{aligned}$$

With this we can derive

$$\begin{aligned}
\mathcal{L}_{T+1} &= \{ m_1 - m_2 \,:\, m_1, m_2 \in \mathcal{M}_{T+1} \} \\
&= \big\{ m_1 - m_2, m_1 + p_{T+1} - m_2, m_1 - m_2 - p_{T+1}, \\
&\qquad m_1 + p_{T+1} - m_2 - p_{T+1} \,:\, m_1, m_2 \in \mathcal{M}_T \big\} \\
&= \{ l, l + p_{T+1}, l - p_{T+1} \,:\, l \in \mathcal{L}_T \} ,
\end{aligned}$$

which completes the proof. □

# References


[1] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proc. of the 39th IEEE Conference on Foundations of Computer Science*, pages 352–361, 1998. quant-ph/9802049.

[2] A. J. Bessen. The power of various real-values quantum queries. *Journal of Complexity*, 20(4):699–712, 2004. quant-ph/0308140.

[3] A. J. Bessen. A lower bound for phase estimation on a quantum computer. *Physical Review A*, 71(4):042313, 2005. quant-ph/0412008.

[4] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219, 1996. quant-ph/9605043.

[5] S. Heinrich. Quantum summation with an application to integration. *Journal of Complexity*, 18(1):1–50, 2002. quant-ph/0105116.

[6] S. Heinrich. Quantum approximation i. embeddings of finite dimensional lp spaces. *Journal of Complexity*, 20(1):5–26, 2004. quant-ph/0305030.

[7] S. Heinrich. Quantum approximation ii. sobolev embeddings. *Journal of Complexity*, 20(1):27–45, 2004. quant-ph/0305031.

[8] P. Jaksch and A. Papageorgiou. Eigenvector approximation leading to exponential speedup of quantum eigenvalue calculation. *Phys. Rev. Lett.*, 91(257902), 2003. quant-ph/0308016.

[9] H. B. Keller. *Numerical methods for two-point boundary-value problems*. Waltham, Mass., 1968.

[10] A. Messiah. *Quantum Mechanics*. Amsterdam, North-Holland Pub. Co.; New York, Interscience Publishers, 1961-62.

[11] A. Nayak and F. Wu. The quantum query complexity of approximating the median and related statistics. In *Proc. of the 31th Annual ACM Symposium on Theory of Computing*, pages 384–393, 1999. quant-ph/9804066.

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

[13] E. Novak. Quantum complexity of integration. *Journal of Complexity*, 17:2–16, 2001. quant-ph/0008124.

[14] A. Papageorgiou and H. Woźniakowski. Classical and quantum complexity of the sturm–liouville eigenvalue problem. *Quantum Information Processing*, 4(2):87–127, 2005. quant-ph/0502054.

[15] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. quant-ph/9508027.

[16] J. F. Traub and H. Wozniakowski. Path integration on a quantum computer. *Quantum Information Processing*, 1(5):365–388, 2002. quant-ph/0109113.