The Power of Various Real-Valued Quantum Queries

Arvid J. Bessen*

March 17, 2005

Universität Kaiserslautern
Fachbereich Informatik
Postfach 3049
D-67663 Kaiserslautern

Abstract

The computation of combinatorial and numerical problems on quantum computers is often much faster than on a classical computer in numbers of queries. A query is a procedure by which the quantum computer gains information about the specific problem.

Different query definitions were given and our aim is to review them and to show that these definitions are not equivalent. To achieve this result we will study the simulation and approximation of one query type by another. While approximation is "easy" in one direction, we will show that it is "hard" in the other direction by a lower bound for the numbers of queries needed in the simulation. The main tool in this lower bound proof is a relationship between quantum algorithms and trigonometric polynomials that we will establish.

1 Introduction to Quantum Queries

Since Grover's discovery of the quantum search algorithm [5], the notion of *query complexity* has played an important role in quantum computation (for a thorough introduction to quantum computation see Nielsen, Chuang, [8]). Grover studied the problem to find an index $j \in \{0, 1, \ldots, N-1\}$ so that for a function

$$f : \{0, \ldots, N-1\} \to \{0, 1\}$$

$f(j) = 1$ holds. He constructed a quantum algorithm that needs $\mathcal{O}(\sqrt{N})$ evaluations of f, if exactly one index j with $f(j) = 1$ exists, while an algorithm on a classical computer would need $\Theta(N)$ evaluations. His quantum evaluation of f was given by the transformation

$$|j\rangle \mapsto \begin{cases} |j\rangle & \text{if } f(j) = 0 \\ -|j\rangle & \text{if } f(j) = 1 \end{cases}$$

*bessen@cs.columbia.edu

This query can easily be seen to be equivalent to the query

$$|j\rangle\,|b\rangle \mapsto |j\rangle\,|b \oplus f(j)\rangle = |j\rangle\,|b + f(j) \mod 2\rangle \tag{1}$$

which was used by Beals et al. [2] and Nayak and Wu [7]. For this query they proved important lower bounds for many problems that involve Boolean queries.

All these queries refer to the following model of computation. Let Q_f denote a query transformation for a fixed function f, let U_k denote arbitrary unitary transformations not depending on f, and let $|\psi\rangle$ be a starting state. Consider the quantum algorithm

$$U_n Q_f U_{n-1} \dots U_1 Q_f U_0\,|\psi\rangle\,. \tag{2}$$

It returns a resulting state $|\chi_f\rangle$ after measurement with probability p_{χ_f}. We identify this state $|\chi_f\rangle$ with its index χ_f and map it to the solution space by a computable mapping φ not depending on f on a classical computer.

We briefly recall some definitions from information-based complexity (see the introductions and surveys Traub, Werschulz [13], and Traub, Wasilkowski, Woźniakowski [12]). These were transferred to quantum computers by Heinrich, [6], whose approach we follow. Let the correct solution to every problem f, f from the problem class F, be given by a mapping $S: F \to G$. If the algorithm returns a $\varphi(\chi_f) \in G$ for every input $f \in F$ with probability p_{χ_f}, so that

$$\sum_{\chi_f : ||S(f) - \varphi(\chi_f)|| < \epsilon} p_{\chi_f} \geq \frac{3}{4},$$

it is said to solve the problem for the problem class F. The best precision ϵ that can be achieved by a quantum algorithm, which uses only n queries, is called the *n-th minimal quantum query error* $\mathrm{e}^{\mathrm{q}}_{\mathrm{n}}(S,F)$. Conversely the *quantum query complexity* $\mathrm{comp}^{\mathrm{q}}_{\epsilon}(S,F)$ is the minimal number of queries that have to be used in a quantum algorithm to get the desired result with precision ϵ.

With this formal framework we are able to deal with numerical problems, if we define what the query Q_f is in this case. Since numerical queries have more than just two possible outcomes we have to extend our notion of a query. We will follow the formal approach of Heinrich to discuss the different queries. Suppose we want to query a function $f: D \to K$. To ease our discussion let us restrict to $K \subseteq [0,1]$. We have to choose a mapping $\tau: \{0, 1, \dots, 2^n - 1\} \to D$, decoding the input, and a mapping β encoding the output.

There are two different approaches to encode a value in $[0,1]$ in a quantum computer. The first approach was established by Abrams and Williams [1], and Novak [10], who proposed the following query

$$\begin{aligned} Q_f^{\text{phase}}\,|j\rangle\,|0\rangle &= \sqrt{1-\beta(f(\tau(j)))}\,|j\rangle\,|0\rangle + \sqrt{\beta(f(\tau(j)))}\,|j\rangle\,|1\rangle \\ Q_f^{\text{phase}}\,|j\rangle\,|1\rangle &= -\sqrt{\beta(f(\tau(j)))}\,|j\rangle\,|0\rangle + \sqrt{1-\beta(f(\tau(j)))}\,|j\rangle\,|1\rangle \end{aligned} \tag{3}$$

This query continuously changes between the two states $|0\rangle$ and $|1\rangle$. We will refer to this query as the *phase query* since it can be viewed as a (relative) phase rotation in the space spanned by $|0\rangle$, $|1\rangle$. In [1] the mapping β was chosen as

$$\begin{aligned} \beta : [0,1] &\to [0,1] \\ x &\mapsto x^2 \end{aligned}$$

while in [10] $\beta = \mathrm{id}$.

Another approach to extend the Boolean query was chosen by Heinrich, [6]. He encoded the values in $[0,1]$ via β to $\{0, 1, \ldots, 2^m - 1\}$ and defined:

$$Q_f^{\mathrm{bit}} \left|j\right\rangle \left|x\right\rangle = \left|j\right\rangle \left|x \oplus \beta(f(\tau(j)))\right\rangle = \left|j\right\rangle \left|x + \beta(f(\tau(j))) \mod 2^m\right\rangle \tag{4}$$

For the rest of this paper we will refer to this query definition as the *bit query*.

Consider the problem to compute the mean. Let $F := \{f : \{0, \ldots, N-1\} \to [0,1]\}$. The solution operator $S_N : F \to [0,1]$ for this problem is

$$S_N(f) := \frac{1}{N} \sum_{j=0}^{N-1} f(j).$$

Brassard et al. [3], Novak [10], and Heinrich [6] showed that for this problem

$$\mathrm{comp}_\epsilon^{\mathrm{q}}(S_N, F) = \Theta(\frac{1}{\epsilon})$$

with *phase queries* as well as with *bit queries*, where in both cases the upper bounds were shown by the amplitude estimation algorithm.

Does this equivalence hold for all problems?

2 Bit queries can simulate phase queries

Suppose we are able to construct a unitary transformation that realizes a phase query by the use of bit queries. If we additionally show that the required number of bit queries is a small constant, no algorithm that uses phase queries could be (asymptotically) faster than an algorithm with bit queries.

Definition 1. *If it is possible to find unitary transformations U_i not depending on f with either*

$$Q_f^{(1)} = U_{n_q} Q_f^{(2)} U_{n_q - 1} \ldots U_1 Q_f^{(2)} U_0 \quad \textit{(simulation)} \tag{5}$$

or

$$\left\| Q_f^{(1)} - U_{n_q} Q_f^{(2)} U_{n_q - 1} \ldots U_1 Q_f^{(2)} U_0 \right\| \leq \delta \quad \textit{(approximation)} \tag{6}$$

for all $f \in F$, we say that the query $Q_f^{(1)}$ is simulated or approximated up to δ by $Q_f^{(2)}$ using n_q queries $Q_f^{(2)}$.

What does this definition of approximation say about the probability to measure the correct state? As it is shown e.g. in [8], box 4.1, suppose the probability that on input $\left|\psi\right\rangle$, the state $\left|\varphi\right\rangle$ is measured with probability p_U, if U is applied, and with p_V, if V is applied. Then

$$|p_U - p_V| \leq 2\|U - V\|. \tag{7}$$

Proposition 2. *Two applications of Q_f^{bit} suffice to approximate Q_f^{phase} by Q_f^{bit}. The precision of the approximation only depends on the encodings β^{phase}, β^{bit}, and the number of bits in the bit query Q_f^{bit}.*

Fix the encodings $\beta^{\text{bit}} : [0,1] \to \{0,\dots,2^m-1\}$, and $\beta^{\text{phase}} : [0,1] \to [0,1]$. Define $\beta_-^{\text{bit}} : \{0,\dots,2^m-1\} \to [0,1]$ as a mapping that satisfies $\beta^{\text{bit}} \circ \beta_-^{\text{bit}} = \text{id}$.

Let the starting state $|\psi\rangle$ be

$$|\psi\rangle = \sum_j \alpha_j |j\rangle |0\rangle + \sum_j \beta_j |j\rangle |1\rangle \in H_n \otimes H_1.$$

We just state the algorithm for the basis states $|j\rangle |0\rangle$, and $|j\rangle |1\rangle$, the extension to arbitrary states $|\psi\rangle$ follows from linearity.

- Starting state is $|j\rangle |0\rangle$ or $|j\rangle |1\rangle$.
- Append $|0\rangle |0\rangle \in H_n \otimes H_m$:

$$|j\rangle |0\rangle |0\rangle |0\rangle \quad \text{or} \quad |j\rangle |1\rangle |0\rangle |0\rangle$$

- Copy (by addition modulo 2^n) the first register to the third register:

$$|j\rangle |0\rangle |j\rangle |0\rangle \quad \text{or} \quad |j\rangle |1\rangle |j\rangle |0\rangle$$

- Apply Q_f^{bit} to the third and fourth register:

$$|j\rangle |0\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle \quad \text{or} \quad |j\rangle |1\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle \tag{8}$$

- Define a mapping U by

$$\begin{aligned} U |j\rangle |0\rangle |j\rangle |x\rangle =& \sqrt{1-\beta^{\text{phase}}(\beta_-^{\text{bit}}(x))}\, |j\rangle |0\rangle |j\rangle |x\rangle \\ &+ \sqrt{\beta^{\text{phase}}(\beta_-^{\text{bit}}(x))}\, |j\rangle |1\rangle |j\rangle |x\rangle \\ U |j\rangle |1\rangle |j\rangle |x\rangle =& -\sqrt{\beta^{\text{phase}}(\beta_-^{\text{bit}}(x))}\, |j\rangle |0\rangle |j\rangle |x\rangle \\ &+ \sqrt{1-\beta^{\text{phase}}(\beta_-^{\text{bit}}(x))}\, |j\rangle |1\rangle |j\rangle |x\rangle \end{aligned} \tag{9}$$

  for every $j \in \{0,\dots,2^n-1\}$ and $x \in \{0,\dots,2^m-1\}$. Note that U does not depend on f. Apply U to the state (8), resulting in:

$$\begin{aligned} &\sqrt{1-\beta^{\text{phase}}(\beta_-^{\text{bit}}(\beta^{\text{bit}}(f(\tau(j)))))}\, |j\rangle |0\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle \\ &\quad + \sqrt{\beta^{\text{phase}}(\beta_-^{\text{bit}}(\beta^{\text{bit}}(f(\tau(j)))))}\, |j\rangle |1\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle \end{aligned} \tag{10}$$

  or

$$\begin{aligned} &-\sqrt{\beta^{\text{phase}}(\beta_-^{\text{bit}}(\beta^{\text{bit}}(f(\tau(j)))))}\, |j\rangle |0\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle \\ &\quad + \sqrt{1-\beta^{\text{phase}}(\beta_-^{\text{bit}}(\beta^{\text{bit}}(f(\tau(j)))))}\, |j\rangle |1\rangle |j\rangle \left|\beta^{\text{bit}}(f(\tau(j)))\right\rangle . \end{aligned} \tag{11}$$

- Uncompute Q_f^{bit} by mapping

$$|j\rangle |b\rangle |k\rangle |x\rangle \mapsto |j\rangle |b\rangle |k\rangle |(-x) \mod 2^m\rangle$$

  and applying Q_f^{bit}. Now map

$$|j\rangle |b\rangle |k\rangle |x\rangle \mapsto |j\rangle |b\rangle |(-k) \mod 2^n\rangle |x\rangle$$

  and again apply the copy operation. We can discard the additional quantum registers now, since they are in the state $|0\rangle |0\rangle$ again.

A close look at the states in (10), and (11) reveals that we have successfully simulated the mapping

$$Q^{\text{phase}}_{\beta^{\text{bit}}_{-} \circ \beta^{\text{bit}} \circ f}.$$

Since in general $\beta^{\text{bit}}_{-} \circ \beta^{\text{bit}} \neq \text{id}$, our approximation introduced an error in the simulation. This error is bounded by

$$\begin{aligned} \sup_{x \in D} |\beta^{\text{bit}}_{-}(\beta^{\text{bit}}(f(x))) - f(x)| &\leq \sup_{y \in [0,1]} |\beta^{\text{bit}}_{-}(\beta^{\text{bit}}(y)) - y| \\ &\leq \sup\{|x - y| \mid \beta^{\text{bit}}(x) = \beta^{\text{bit}}(y)\}. \end{aligned} \tag{12}$$

For the most obvious choice for β^{bit}

$$\begin{aligned} \beta^{\text{bit}} : [0,1) &\to \{0, \ldots, 2^m - 1\} \\ x &\mapsto \lfloor x \cdot 2^m \rfloor \end{aligned} \tag{13}$$

a good β^{bit}_{-} is

$$\begin{aligned} \beta^{\text{bit}}_{-} : \{0, \ldots, 2^m - 1\} &\to [0,1] \\ x &\mapsto x \cdot 2^{-m} + 2^{-m-1} \end{aligned} \tag{14}$$

for which the error from (12) is less than 2^{-m-1}.

As an example consider $\beta^{\text{phase}} = \text{id}$. After some calculation we get

$$||Q^{\text{phase}}_{f} - Q^{\text{phase}}_{\beta^{\text{bit}}_{-} \circ \beta^{\text{bit}} \circ f}|| \leq 2^{-m/2}.$$

3 Phase queries cannot efficiently approximate bit queries

Let us consider the (simple) evaluation problem

$$\begin{aligned} S : F &\to [0,1] \\ f &\mapsto Sf := f(0) \end{aligned} \tag{15}$$

with $F = \{f : \{0\} \to [0,1]\}$. It is obvious that this problem can be solved on a “classical” computer by just one evaluation of f, i.e. $\text{comp}_\epsilon(S, F) = 1$. The precision ϵ only depends on the accuracy of the query - the function call returning $f(0)$.

On a quantum computer that uses bit queries to evaluate f also

$$\text{comp}^{\text{q,bit}}_\epsilon(S, F) = 1, \tag{16}$$

at least, if we choose β^{bit} as in (13) and if the number of qubits m is chosen so that $2^m > \frac{1}{\epsilon}$.

If we are only allowed to use phase queries however, we can prove a lower bound theorem.

Theorem 3. *Consider the evaluation problem (15). For any quantum algorithm that is only allowed to access f by phase queries,*

$$\text{comp}^{q,phase}_\epsilon(S, F) = \Omega(\frac{1}{\epsilon}), \tag{17}$$

if the encoding β^{phase} is chosen as $\beta^{phase} = \text{id}$.

To prove this theorem we will need lemma 6 and lemma 8, thus we will postpone the proof. But theorem 3 allows us to easily prove the following corollary:

Corollary 4. *The approximation of an m-bit query Q_f^{bit} to $\delta \leq \frac{1}{8}$ by a phase query Q_f^{phase} requires $\Omega(2^m)$ phase queries Q_f^{phase} when $\beta^{phase} = \mathrm{id}$.*

Proof. Suppose we could approximate an m-bit query by $n_q = n_q(m)$ phase queries and for all $c > 0$, $m_0 \in \mathbb{N}$ there exists an $m \geq m_0$ with

$$n_q(m) < c2^m.$$

Fix such an m. Approximation means

$$\left\| Q_f^{\mathrm{bit}} - U_{n_q} Q_f^{\mathrm{phase}} U_{n_q-1} \dots U_1 Q_f^{\mathrm{phase}} U_0 \right\| \leq \delta.$$

We know that just one m-bit query is sufficient to solve the evaluation problem to accuracy $\epsilon := 2^{-m+1}$ and certainty, so we could use the following algorithm:

$$\widetilde{U}_1 U_{n_q} Q_f^{\mathrm{phase}} U_{n_q-1} \dots U_1 Q_f^{\mathrm{phase}} U_0 \widetilde{U}_0 \left|\psi\right\rangle,$$

where

$$\widetilde{U}_1 Q_f^{\mathrm{bit}} \widetilde{U}_0 \left|\psi\right\rangle$$

is the algorithm that uses just one bit query.

The probability that the output of this algorithm with an approximated query is incorrect would be less or equal than 2δ, see (7). Thus we could solve the evaluation problem with

$$\mathrm{comp}_\epsilon^{\mathrm{q}}(S, F) \leq n_q < c2^m = 2c\frac{1}{\epsilon},$$

which is a contradiction to theorem 3. □

With the result from section 2 that any phase query can be approximated by 2 bit queries we can conclude that bit queries are more powerful than phase queries.

To prove theorem 3 let us introduce multivariate trigonometric polynomials (for an introduction see e.g. [9]).

Definition 5. *A mapping $T : \mathbb{R}^n \to \mathbb{C}$ is called an **n-variate trigonometric polynomial**, if it is of the form*

$$T(\theta_0, \dots, \theta_{n-1}) = \sum_{j \in J} c_j e^{i(n_{j,0}\theta_0 + \dots + n_{j,n-1}\theta_{n-1})}$$

with $c_j \in \mathbb{C}$, $n_{j,k} \in \mathbb{Z}$, and $|J| < \infty$. We additionally define

$$\deg T(\theta_0, \dots, \theta_{n-1}) := \max_{j \in J} \left(|n_{j,0}| + \dots + |n_{j,n-1}| \right)$$

*as the **degree** of $T(\theta_0, \dots, \theta_{n-1})$.*

This definition allows us to define for every quantum algorithm, which depends on a phase query Q_f^{phase}, a corresponding multivariate polynomial. The idea that allows this is that every phase query as in (3) can also be written as

$$\begin{aligned} Q_f^{\text{phase}} |j\rangle |0\rangle &= \cos\theta_j |j\rangle |0\rangle + \sin\theta_j |j\rangle |1\rangle \\ Q_f^{\text{phase}} |j\rangle |1\rangle &= -\sin\theta_j |j\rangle |0\rangle + \cos\theta_j |j\rangle |1\rangle , \end{aligned} \tag{18}$$

if θ_j is chosen so that

$$\theta_j = \arcsin\sqrt{\beta^{\text{phase}}(f(\tau(j)))}. \tag{19}$$

Now we can prove the following lemma, which closely follows the proof idea in Beals et al., [2].

Lemma 6. *For every quantum algorithm A making n_q queries Q_f^{phase} there are trigonometric polynomials $T_k(\theta_0, \ldots, \theta_{n-1})$, $\deg T_k(\theta_0, \ldots, \theta_{n-1}) \leq n_q$, so that*

$$\begin{aligned} A|\psi\rangle &= U_{n_q} Q_f^{phase} U_{n_q-1} \ldots U_1 Q_f^{phase} U_0 |\psi\rangle \\ &= \sum_k T_k(\theta_0, \ldots, \theta_{n-1}) |k\rangle \end{aligned}$$

holds with θ_j defined as in (19).

Proof. The proof is by induction over the number of queries n_q.

$\underline{n_q = 0:}$ we have not made any queries Q_f^{phase} therefore the state can be written as

$$U_0 |\psi\rangle = \sum_k \alpha_k |k\rangle$$

with constants α_k.

$\underline{n_q \mapsto n_q + 1:}$ suppose

$$U_{n_q} Q_f^{\text{phase}} U_{n_q-1} \ldots U_1 Q_f^{\text{phase}} U_0 |\psi\rangle = \sum_k T_k(\theta_0, \ldots, \theta_{n-1}) |k\rangle .$$

with $\deg T_k(\theta_0, \ldots, \theta_{n-1}) \leq n_q$. We can split this state into

$$\begin{aligned} \sum_k T_k(\theta_0, \ldots, \theta_{n-1}) |k\rangle = &\sum_{i,j,l} T_{ij0l}(\theta_0, \ldots, \theta_{n-1}) |i\rangle |j\rangle |0\rangle |l\rangle \\ &+ \sum_{i,j,l} T_{ij1l}(\theta_0, \ldots, \theta_{n-1}) |i\rangle |j\rangle |1\rangle |l\rangle . \end{aligned} \tag{20}$$

Let $\Theta = (\theta_0, \ldots, \theta_{n-1})$. After applying Q_f^{phase} to state (20), the result can be written as

$$\begin{aligned}
& \sum_{i,j,l} |i\rangle \left(\cos\theta_j T_{ij0l}(\Theta)\,|j\rangle\,|0\rangle + \sin\theta_j T_{ij0l}(\Theta)\,|j\rangle\,|1\rangle\right)|l\rangle \\
+ & \sum_{i,j,l} |i\rangle \left(-\sin\theta_j T_{ij1l}(\Theta)\,|j\rangle\,|0\rangle + \cos\theta_j T_{ij1l}(\Theta)\,|j\rangle\,|1\rangle\right)|l\rangle \\
= & \sum_{i,j,l} \left(\cos\theta_j T_{ij0l}(\Theta) - \sin\theta_j T_{ij1l}(\Theta)\right)|i\rangle\,|j\rangle\,|0\rangle\,|l\rangle \\
+ & \sum_{i,j,l} \left(\sin\theta_j T_{ij0l}(\Theta) + \cos\theta_j T_{ij1l}(\Theta)\right)|i\rangle\,|j\rangle\,|1\rangle\,|l\rangle\,.
\end{aligned}$$

The terms

$$\cos\theta_j T_{ij0l}(\theta_0,\ldots,\theta_{n-1}) - \sin\theta_j T_{ij1l}(\theta_0,\ldots,\theta_{n-1})$$

and

$$\sin\theta_j T_{ij0l}(\theta_0,\ldots,\theta_{n-1}) + \cos\theta_j T_{ij1l}(\theta_0,\ldots,\theta_{n-1})$$

again are multivariate trigonometric polynomials and of degree at most n_q+1.

Finally the mapping U_{n_q+1} is independent of f, thus not dependent on Θ, and just maps to a new linear combination of trigonometric polynomials, which again has degree at most n_q+1. □

For (univariate) trigonometric polynomials we cite (see e.g. [4], [11])

Theorem 7 (Bernstein's Inequality). *Let $t(\theta)$ be a trigonometric polynomial. Then*

$$\max_{-\pi\le\theta\le\pi} |t'(\theta)| \le \deg t(\theta) \max_{-\pi\le\theta\le\pi} |t(\theta)|.$$

The trigonometric polynomials $T_k(\theta_0,\ldots,\theta_{n-1})$ we found in lemma 6 were related to f via equation (19):

$$\theta_j = \arcsin\sqrt{\beta^{\text{phase}}(f(\tau(j)))}.$$

What is the bound of Bernstein's inequality in dependence on $\arcsin\sqrt{\cdot}$?

Lemma 8. *If there exist an $x\in[0,1]$, and a Δ with $x+\Delta\in[0,1]$ so that for the trigonometric polynomial $t(\theta)$*

$$t(\arcsin\sqrt{x}) \ge \frac{3}{4} \quad \textit{and} \quad t(\arcsin\sqrt{x+\Delta}) \le \frac{1}{4}$$

and $t(\theta)\in[0,1]$ for all $\theta\in\mathbb{R}$, then

$$\deg t(\theta) \ge c\left(\sqrt{\frac{1}{|\Delta|}} + \frac{\sqrt{m(1-m)}}{|\Delta|}\right), \tag{21}$$

with $m\in\{x, x+\Delta\}$ so that $|m-\frac{1}{2}|$ is maximal and a constant c.

Proof. Applying the mean value theorem yields a $\xi \in [x, x+\Delta]$ or $\xi \in [x+\Delta, x]$ with

$$|t(\arcsin\sqrt{x}) - t(\arcsin\sqrt{x+\Delta})| = \left|\arcsin\sqrt{x} - \arcsin\sqrt{x+\Delta}\right| |t'(\xi)|$$

and thus

$$|t'(\xi)| \geq \frac{1}{2}\left|\arcsin\sqrt{x} - \arcsin\sqrt{x+\Delta}\right|^{-1}.$$

Now bound the degree of $t(\theta)$ by Bernstein's inequality (lemma 7) and use that $t(\theta) \in [0,1]$:

$$\frac{1}{2}\left|\arcsin\sqrt{x+\Delta} - \arcsin\sqrt{x}\right|^{-1} \leq \deg t(\theta) \max_{-\pi\leq\theta\leq\pi} |t(\theta)| \leq \deg t(\theta). \tag{22}$$

For the first bound we use that for all $\varphi, \psi \in [0, \pi/2]$

$$\frac{2}{\pi}|\varphi - \psi| \leq \sqrt{2|\sin^2\varphi - \sin^2\psi|}, \tag{23}$$

and therefore from (22) and (23)

$$\deg t(\theta) \geq c\sqrt{\frac{1}{|\sin^2\arcsin\sqrt{x+\Delta} - \sin^2\arcsin\sqrt{x}|}} = c\sqrt{\frac{1}{|\Delta|}}.$$

The second bound is proven by another application of the mean-value theorem. There exists a $\xi \in [x, x+\Delta]$ or $\xi \in [x+\Delta, x]$ with

$$\deg t(\theta) \geq \frac{1}{2}\left|(\arcsin\sqrt{\xi})'(x+\Delta-x)\right|^{-1}$$

Note that for $\xi \in [x, x+\Delta]$ or $\xi \in [x+\Delta, x]$

$$(\arcsin\sqrt{\xi})' = \frac{1}{2\sqrt{\xi(1-\xi)}}$$

is maximized by $\xi = m$, with $m \in \{x, x+\Delta\}$ so that $|m - \frac{1}{2}|$ is maximal. Thus

$$\deg t(\theta) \geq c\frac{\sqrt{m(1-m)}}{|\Delta|}.$$

□

Note that the bound (21) closely resembles the bound of Nayak and Wu, [7]. With the help of lemma 8 we are able to prove theorem 3.

Proof of theorem 3. Let n_q be the number of queries of an algorithm for the evaluation problem. By lemma 6 trigonometric polynomials $T_k(\theta)$ exist with

$$U_{n_q} Q_f^{\text{phase}} \ldots U_0 |\psi\rangle = \sum_k T_k(\theta) |k\rangle, \tag{24}$$

for $\theta = \arcsin\sqrt{\beta^{\text{phase}}(f(\tau(j)))}$, see (19), and $\deg T_k(\theta) \leq n_q$.

The state (24) is measured and φ maps the result of the measurement to an element of our solution set $[0,1]$. Let B be the set of all states so that

$$B := \{k \mid |\varphi(k) - 1/2| < \epsilon\}. \tag{25}$$

The probability to measure a state $|k\rangle$ is given by $|T_k(\theta)|^2$. Let

$$T_k(\theta) = \sum_l \alpha_{k,l} e^{in_{k,l}\theta}.$$

Then

$$\sum_{k\in B} |T_k(\theta)|^2 = \sum_{k\in B} \left(\sum_l \alpha_{k,l} e^{in_{k,l}\theta}\right)\left(\sum_l \overline{\alpha_{k,l}} e^{-in_{k,l}\theta}\right) =: T(\theta),$$

which is a trigonometric polynomial again, $\deg T(\theta) \leq 2n_q$, and $T(\theta) \in [0,1]$.

Choose the input $f_1, f_2 \in F$ with $f_1(0) = \frac{1}{2}$, $f_2(0) = \frac{1}{2} - 2\epsilon$, $0 < \epsilon < \frac{1}{4}$. If the algorithm is correct,

$$T(\arcsin\sqrt{\beta^{\text{phase}}(f_1(0))}) \geq \frac{3}{4} \quad \text{and} \quad T(\arcsin\sqrt{\beta^{\text{phase}}(f_2(0))}) \leq \frac{1}{4}$$

(all query inputs are mapped to 0 by τ).

Our lemma 8 tells us a bound for the degree of $T(\theta)$:

$$2n_q \geq \deg T(\theta) \geq c\left(\sqrt{\frac{1}{|\Delta|}} + \frac{\sqrt{m(1-m)}}{|\Delta|}\right),$$

where

$$\Delta = \beta^{\text{phase}}(f_1(0)) - \beta^{\text{phase}}(f_2(0)). \tag{26}$$

and $m \in \{\beta^{\text{phase}}(f_1(0)), \beta^{\text{phase}}(f_2(0))\}$ so that $|m - \frac{1}{2}|$ is maximal.

We chose $\beta^{\text{phase}} = \text{id}$, so

$$2n_q \geq c\left(\sqrt{\frac{1}{2\epsilon}} + \frac{\sqrt{(\frac{1}{2} - 2\epsilon)(1 - \frac{1}{2} + 2\epsilon)}}{2\epsilon}\right) = c\left(\sqrt{\frac{1}{2\epsilon}} + \frac{\sqrt{\frac{1}{4} - 4\epsilon^2}}{2\epsilon}\right).$$

There exists a constant c' so that for ϵ small enough

$$n_q \geq c'\frac{1}{\epsilon}$$

holds, therefore

$$\text{comp}_\epsilon^{\text{q,phase}}(S,F) = \Omega(\frac{1}{\epsilon}).$$

□

4 Another proof for the hardness of evaluation with phase queries

An anonymous referee suggested a shorter proof for theorem 3. The proof is based on the observation that for two inputs f_1 and f_2 which are chosen as in the proof of theorem 3, $f_1, f_2 \in F = \{f : \{0\} \to [0,1]\}$,

$$f_1(0) = \frac{1}{2} \quad \text{and} \quad f_2(0) = \frac{1}{2} - 2\epsilon,$$

the difference of $Q_{f_1}^{\text{phase}}$ and $Q_{f_2}^{\text{phase}}$ is bounded in the operator norm by

$$\begin{aligned} ||Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}}|| &= \sup_{|x\rangle, |||x\rangle||=1} ||(Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}}) |x\rangle || \\ &= \sup ||(Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}})(a_{00} |0\rangle |0\rangle + a_{01} |0\rangle |1\rangle || \end{aligned}$$

with $a_{00}, a_{01} \in \mathbb{C}$ and $|a_{00}|^2 + |a_{01}|^2 = 1$, since $Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}} = 0$ for all other inputs.

Each of the terms can be bounded in the following way (here for $a_{00} |0\rangle |0\rangle$):

$$\begin{aligned} & ||(Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}}) a_{00} |0\rangle |0\rangle || \\ &= |a_{00}| \left\| \sqrt{1/2} |0\rangle |0\rangle + \sqrt{1/2} |0\rangle |1\rangle - \sqrt{1/2 + 2\epsilon} |0\rangle |0\rangle - \sqrt{1/2 - 2\epsilon} |0\rangle |1\rangle \right\| \\ &= \frac{|a_{00}|}{\sqrt{2}} \left\| (1 - \sqrt{1+4\epsilon}) |0\rangle + (1 - \sqrt{1-4\epsilon}) |1\rangle \right\| \\ &= \frac{|a_{00}|}{\sqrt{2}} \sqrt{1 - 2\sqrt{1+4\epsilon} + 1 + 4\epsilon + 1 - 2\sqrt{1-4\epsilon} + 1 - 4\epsilon} \\ &= |a_{00}| \sqrt{2 - \sqrt{1+4\epsilon} - \sqrt{1-4\epsilon}}. \end{aligned}$$

If we develop $\sqrt{1+4x}$ into a Taylor series we get

$$\sqrt{1+4x} = 1 + 2x - 2x^2 \pm \mathcal{O}(|x|^3)$$

and thus

$$\begin{aligned} & ||(Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}}) a_{00} |0\rangle |0\rangle || \\ &\leq |a_{00}| \sqrt{2 - 2 + 4\epsilon^2 \mp \mathcal{O}(|\epsilon|^3)} \\ &= |a_{00}| \, \epsilon \, \sqrt{4 \mp \mathcal{O}(|\epsilon|)} \\ &\in |a_{00}| \mathcal{O}(\epsilon). \end{aligned}$$

The bounds for the term $a_{01} |0\rangle |1\rangle$ are analogous.

Therefore we can conclude that

$$||Q_{f_1}^{\text{phase}} - Q_{f_2}^{\text{phase}}|| \in \mathcal{O}(\epsilon).$$

Now we turn to our quantum algorithm, which is of the form described in equation (2):

$$U_n Q_f^{\text{phase}} U_{n-1} \dots U_1 Q_f^{\text{phase}} U_0 |\psi\rangle .$$

We would like to bound the difference between the algorithm on input f_1 and on f_2:

$$\left\| U_n Q_{f_1}^{\text{phase}} U_{n-1} \dots U_1 Q_{f_1}^{\text{phase}} U_0 |\psi\rangle - U_n Q_{f_2}^{\text{phase}} U_{n-1} \dots U_1 Q_{f_2}^{\text{phase}} U_0 |\psi\rangle \right\| . \quad (27)$$

We will use the following inequality for unitary matrices A, B, C, and D:

$$\begin{aligned} & ||AB - CD|| = ||AB - CB + CB - CD|| \\ &\leq ||AB - CB|| + ||CB - CD|| \leq ||A - C|| \, ||B|| + ||C|| \, ||B - D|| \\ &= ||A - C|| + ||B - D|| \end{aligned} \quad (28)$$

(see e.g. Nielsen and Chuang [8]). Hence equation (27) is bounded by

$$n \left\| Q_{f_1}^{\mathrm{phase}} - Q_{f_2}^{\mathrm{phase}} \right\| .$$

Recall the definition of B, the set of all states representing $\frac{1}{2}$ from equation (25). Our algorithm for the evaluation problem must ensure that for f_1 the probability to measure a state from B is greater than $\frac{3}{4}$ and for f_2 less than $\frac{1}{4}$. Let p_{f_1} be the probability to measure a state from B on input f_1 and p_{f_2} be the probability on input f_2. We want to have

$$|p_{f_1} - p_{f_2}| \geq \frac{1}{2}. \tag{29}$$

We use the fact from equation (7) that for $A_{f_1} := U_n Q_{f_1}^{\mathrm{phase}} \dots U_0$ and $A_{f_2} := U_n Q_{f_2}^{\mathrm{phase}} \dots U_0$ and a measurement projection P

$$\begin{aligned}
&|p_{f_1} - p_{f_2}| = \left| \langle\psi| A_{f_1}^{\dagger} P A_{f_1} |\psi\rangle - \langle\psi| A_{f_2}^{\dagger} P A_{f_2} |\psi\rangle \right| \\
&= \left| \langle\psi| \left(A_{f_1}^{\dagger} P (A_{f_1} - A_{f_2}) + A_{f_1}^{\dagger} P A_{f_2} + (A_{f_1}^{\dagger} - A_{f_2}^{\dagger}) P A_{f_2} - A_{f_1}^{\dagger} P A_{f_2} \right) |\psi\rangle \right| \\
&\leq \left| \langle\psi| A_{f_1}^{\dagger} P (A_{f_1} - A_{f_2}) |\psi\rangle \right| + \left| \langle\psi| (A_{f_1}^{\dagger} - A_{f_2}^{\dagger}) P A_{f_2} |\psi\rangle \right| \\
&\leq \|P A_{f_1} |\psi\rangle\| \, \|(A_{f_1} - A_{f_2}) |\psi\rangle\| + \|(A_{f_1} - A_{f_2}) |\psi\rangle\| \, \|P A_{f_2} |\psi\rangle\| \\
&\leq 2 \|A_{f_1} - A_{f_2}\| ,
\end{aligned}$$

where we used the Cauchy-Schwarz inequality. This bound can be found, e.g., in Nielsen and Chuang [8].

We choose P as a projection on the subspace $\operatorname{span} B$ and get

$$\begin{aligned}
|p_{f_1} - p_{f_2}| &\leq 2 \|A_{f_1} - A_{f_2}\| \\
&\leq 2n \left\| Q_{f_1}^{\mathrm{phase}} - Q_{f_2}^{\mathrm{phase}} \right\| \\
&\in 2n \mathcal{O}(\epsilon)
\end{aligned} \tag{30}$$

Combining equations (29) and (30) now yields

$$n \in \Omega \left(\frac{1}{\epsilon} \right) .$$

5 Acknowledgments

This work was done as a master thesis under the supervision of Stefan Heinrich. I am very grateful for his guidance and the many helpful discussions we had on quantum computing and complexity theory. His valuable suggestions were greatly appreciated.

References

[1] D. S. Abrams and C. P. Williams. Fast quantum algorithms for numerical integrals and stochastic processes. Technical report, NASA Jet Propulsion Laboratory, 1999. http://arXiv.org/abs/quant-ph/9908083.

[2] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science (FOCS)*, pages 352–361, 1998. http://-arXiv.org/abs/quant-ph/9802049.

[3] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. http://arXiv.org/abs/quant-ph/0005055, 2000.

[4] E. W. Cheney. *Introduction to Approximation Theory.* McGraw-Hill Book Company, 1966.

[5] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219, 1996. http://arXiv.org/abs/quant-ph/9605043.

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

[7] A. Nayak and F. Wu. The quantum query complexity of approximating the median and related statistics. In *Proceedings of the 31th Annual ACM Symposium on Theory of Computing (STOC)*, pages 384–393, 1999. http://arXiv.org/abs/quant-ph/9804066.

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

[9] S. M. Nikol'skii. *Approximation of Functions of Several Variables and Imbedding Theorems.* Springer Verlag, 1975.

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

[11] T. J. Rivlin. *The Chebyshev Polynomials.* Wiley, 1974.

[12] J. F. Traub, G. W. Wasilkowski, and H. Woźniakowski. *Information-Based Complexity.* Academic Press, 1988.

[13] J. F. Traub and A.G. Werschulz. *Complexity and Information.* Cambridge University Press, 1998.