Query Lower Bounds for Phase Estimation on a Quantum Computer

Arvid J. Bessen
Columbia University

Department of Computer Science
Columbia University
1214 Amsterdam Ave, MC 0401
New York NY, 10027
email: bessen@cs.columbia.edu
http://www.cs.columbia.edu/~bessen

Abstract

We will obtain a lower bound for the estimation of the phase φ of the eigenvalue of an eigenvector $|q\rangle$ of a unitary matrix Q:

$$Q\,|q\rangle = e^{2\pi i\varphi}\,|q\rangle\,.$$

Our analysis generalizes existing lower bounds to the case where Q is given by controlled powers Q^p of Q, as it is for example in Shor's order finding algorithm [5].

In this most general setting where we are given controlled arbitrary powers Q^{p_1}, Q^{p_2}, … of Q, we will prove a $\Omega(\log\varepsilon^{-1})$ lower bound. This bound is derived by a variation of the polynomial approach, see [1], where we use trigonometric polynomials, see [2]. The bounds are not derived from the degree of the polynomial, though, but from a frequency analysis argument.

1 The Phase Estimation Problem

Goal: determine φ up to ε

We are given a unitary transformation Q as a black-box. We are guaranteed that $|q\rangle$ is an eigenvector of Q, i.e. $Q\,|q\rangle = e^{2\pi i\varphi}\,|q\rangle$. Our problem is to determine φ up to precision ε.

Phase estimation algorithm: compute Q, Q^2, Q^3, …

The phase estimation algorithm computes φ when given $|q\rangle$ and is the main building block of Shor's factoring algorithm, see [4], [5]. The algorithm requires the computation of all the powers Q, Q^2, Q^3, …, Q^{2^t-1} of Q.

Exponential savings through repeated squaring

Under certain circumstances, though, it is possible to use some knowledge about Q to use controlled Q^2, Q^{2^2}, Q^{2^3}, …, $Q^{2^{t-1}}$ queries. In this case we can obtain all powers of Q up to 2^t-1 with only t applications of Q^{2^j}.

Power Queries W_l^p

Let Q be a t qubit unitary transformation. Define the controlled *power query* $W_l^p(Q)(=W_l^p)$ acting on $c+t$ qubits as

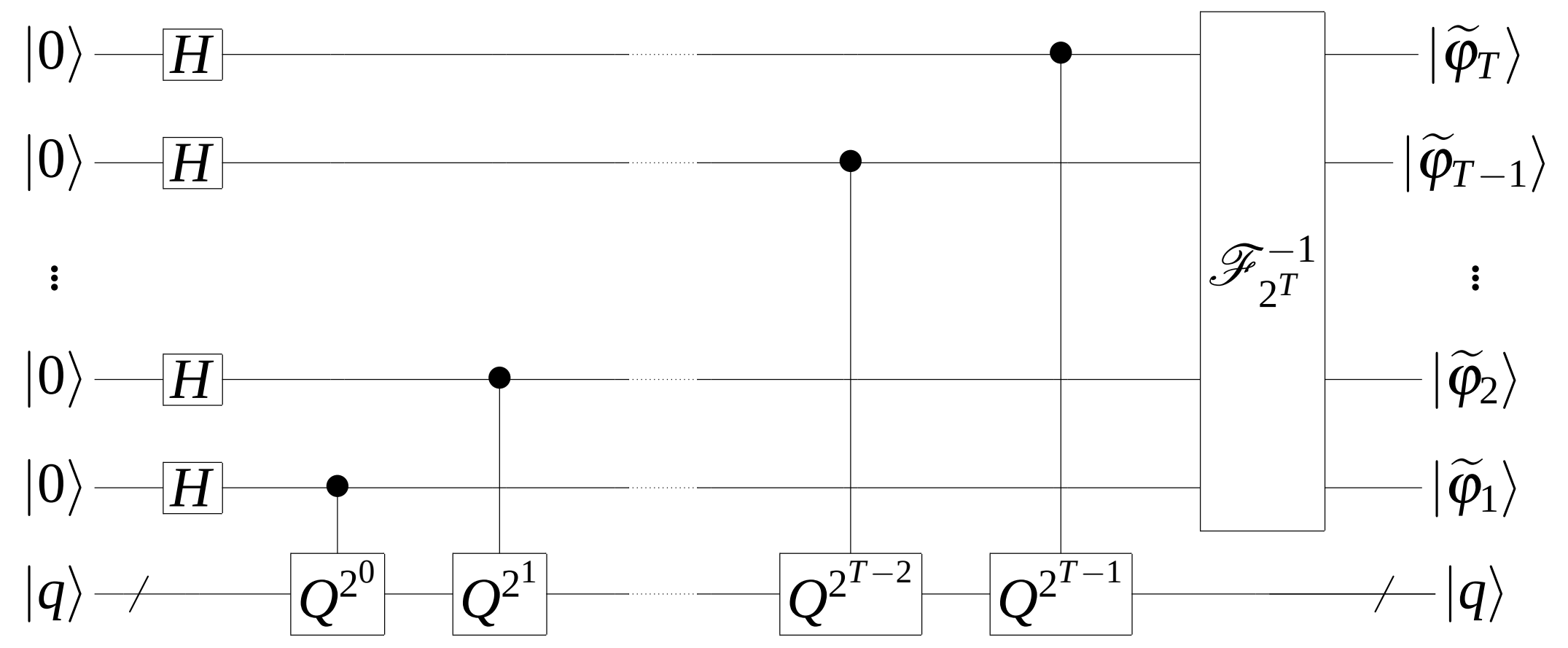
$$W_l^p(Q)\,|x_1\rangle\ldots|x_c\rangle\,|\psi\rangle = \begin{cases} |x_1\rangle\ldots|x_c\rangle\,|\psi\rangle & \text{for } x_l = 0 \\ |x_1\rangle\ldots|x_c\rangle\,Q^p\,|\psi\rangle & \text{for } x_l = 1 \end{cases}.$$

The phase estimation algorithm

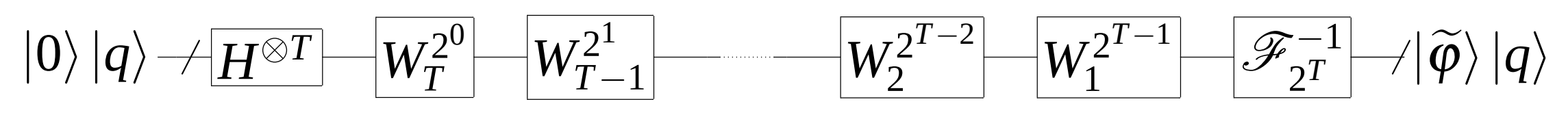
- **Input:** a transformation Q, which has a fixed eigenvector $|q\rangle$
- **Output:** an approximation $\widetilde{\varphi}$ of the *phase* φ of $|q\rangle$, i.e.

$$Q\,|q\rangle = e^{2\pi i\varphi}\,|q\rangle\,.$$

- **Algorithm:** compute



where $\mathscr{F}_{2^T}^{-1}$ is the inverse QFT on T qubits. In power query notation:



What is the minimal number of queries?

The phase estimation algorithm needs $T=\mathscr{O}(\log 1/\varepsilon)$ queries to $W_{l_1}^{2^0}, W_{l_2}^{2^1}, W_{l_3}^{2^2}, \ldots$ for an ε approximation to φ. Can we do better than that?

2 Quantum Query Algorithms

Quantum algorithm with power queries

A general framework for algorithms with power queries:

- **Input:** a *query* transformation Q (gives the algorithm information about the problem), with Q from the set of all possible inputs $\mathscr{Q}$.
- **Output:** a *solution* $S(Q)$ depending on Q (an ε approximation to $S(Q)$ with probability greater than $\frac{3}{4}$ is actually enough)
- **Algorithm:** Let U_0, U_1, …, U_T be fixed unitary transformations and $\left|\psi^{(0)}\right\rangle$ a fixed state. Let $W_{l_j}^{p_j}(Q)$ be the power query for all Q. An quantum algorithm is a sequence

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

Output of the algorithm

A measurement of the state $\left|\psi^{(T)}(Q)\right\rangle$ yields a state $|\chi\rangle$ with probability $p_{\chi,Q}$. If for every $Q\in\mathscr{Q}$

$$\sum_{\chi:\|S(Q)-\chi\|<\varepsilon} p_{\chi,Q} \geq \frac{3}{4},$$

the algorithm (1) is said to solve the problem for all inputs $Q\in\mathscr{Q}$.

This combines ideas from [1], [6], and [3].

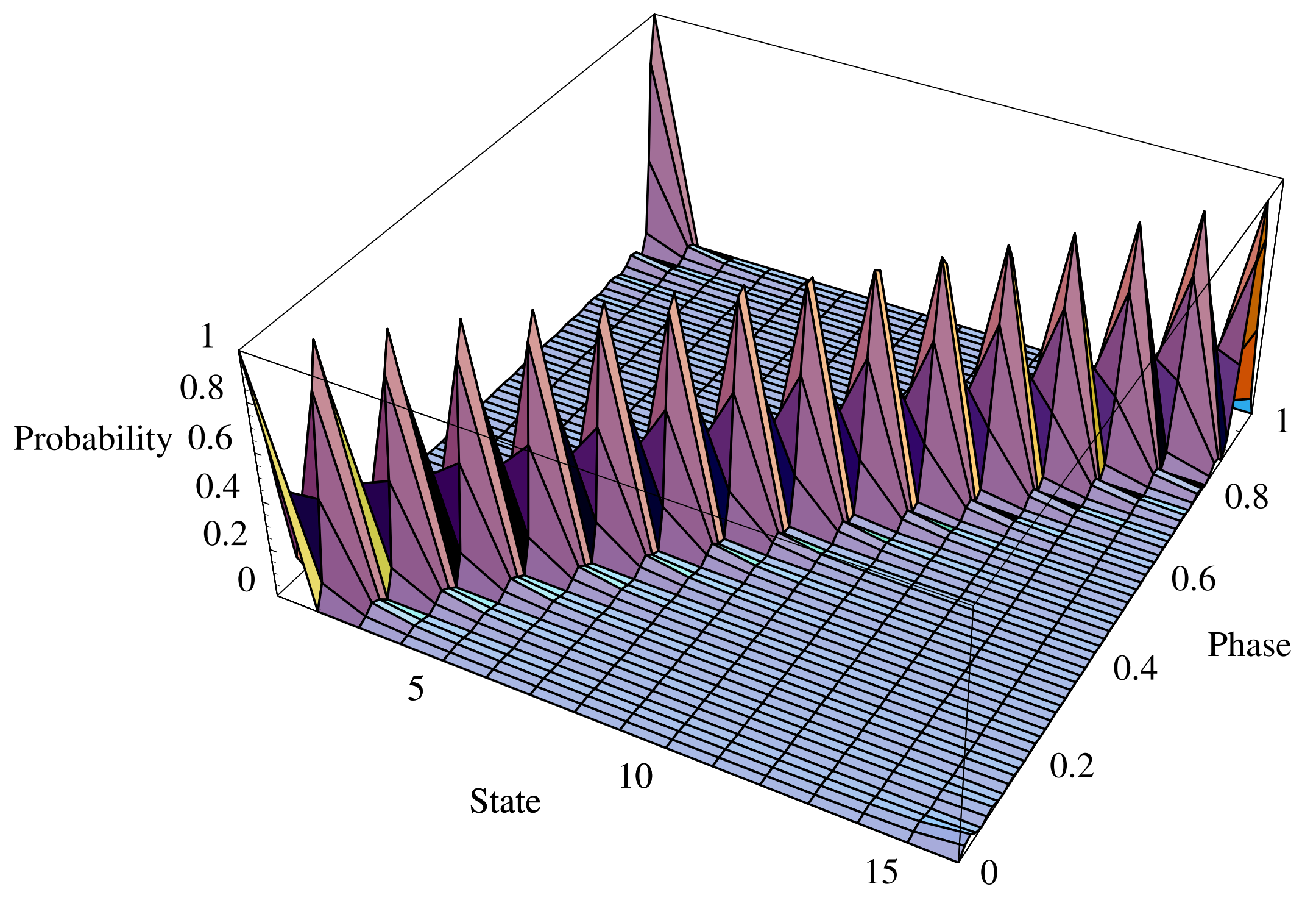


Figure 1: The probability distribution of the Phase Estimation Algorithm for each state, depending on the phase φ

In our analysis we will focus on the dependence of the probability for one state with varying φ.

3 Lower Bounds

Trigonometric polynomial approach

We can use trigonometric polynomials to describe the output of a quantum query algorithm (1) for the phase estimation problem.

Proposition 1. *A quantum algorithm of form (1) for the phase estimation problem can be written as*

$$\left|\psi^{(T)}\right\rangle = \sum_{j\in J_\varphi} \alpha_{k,j}^{(T)} e^{2\pi i j\varphi}\,|k\rangle\,.$$

with $\alpha_{k,j}^{(T)}\in\mathbb{C}$. The set J_φ is given by

$$J_\varphi = \Big\{ \sum_{k\in K} p_k, \Big| K\subseteq\{1,\ldots,T\} \Big\}. \qquad (2)$$

The set J_φ is the set of all possible sums of the p_i:

$$J_\varphi = \{0, p_1,\ldots,p_T, p_1+p_2,\ldots,p_1+p_T,\ldots,p_1+\ldots+p_T\}\,.$$

and it has at most 2^T elements.

Analysis of the probability dependence on φ

Let us consider an arbitrary algorithm of the form (1). We can show that for every outcome m, $p_m(\varphi)$ is a trigonometric polynomial

$$p_m(\varphi) = \sum_{l\in L_\varphi} \eta_{m,l} e^{2\pi i l\varphi},$$

where L_φ is given by $L_\varphi = \left\{ j-j' \,|\, j,j'\in J_\varphi \right\}$.

Proposition 2. *L_φ cannot have more than 2^{2T} elements. I.e.,* ***with T queries we can only get 2^{2T} frequencies.***

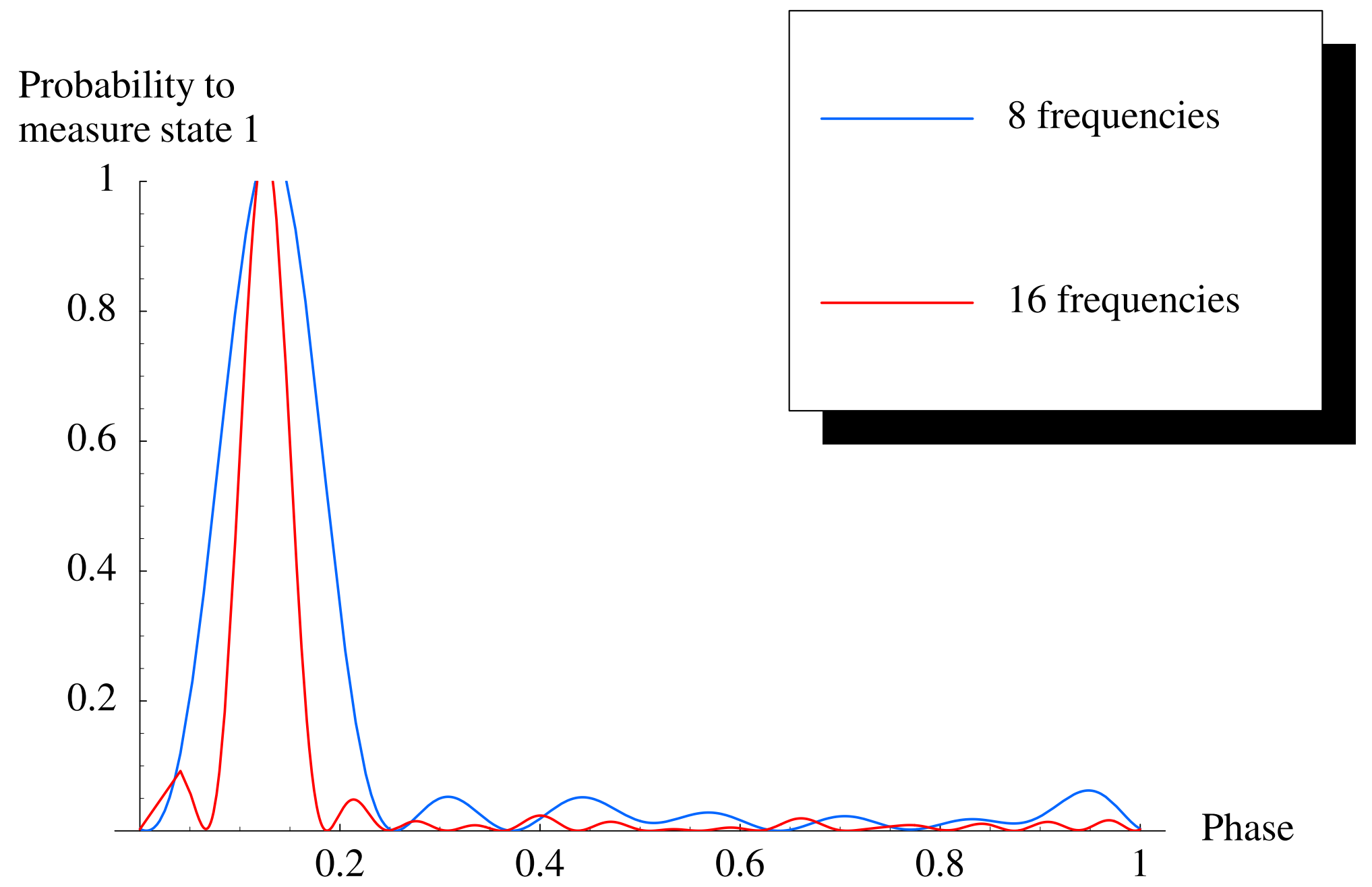


Figure 2: The probabilities for $|1\rangle$ in a perturbed phase estimation algorithm, depending on φ

The sharper the spike in theprobability distribution, the more frequencies must be present

Proposition 3. ***To get a sharp probability peak of width ε, all frequencies up to order $1/\varepsilon$ have to be present.***

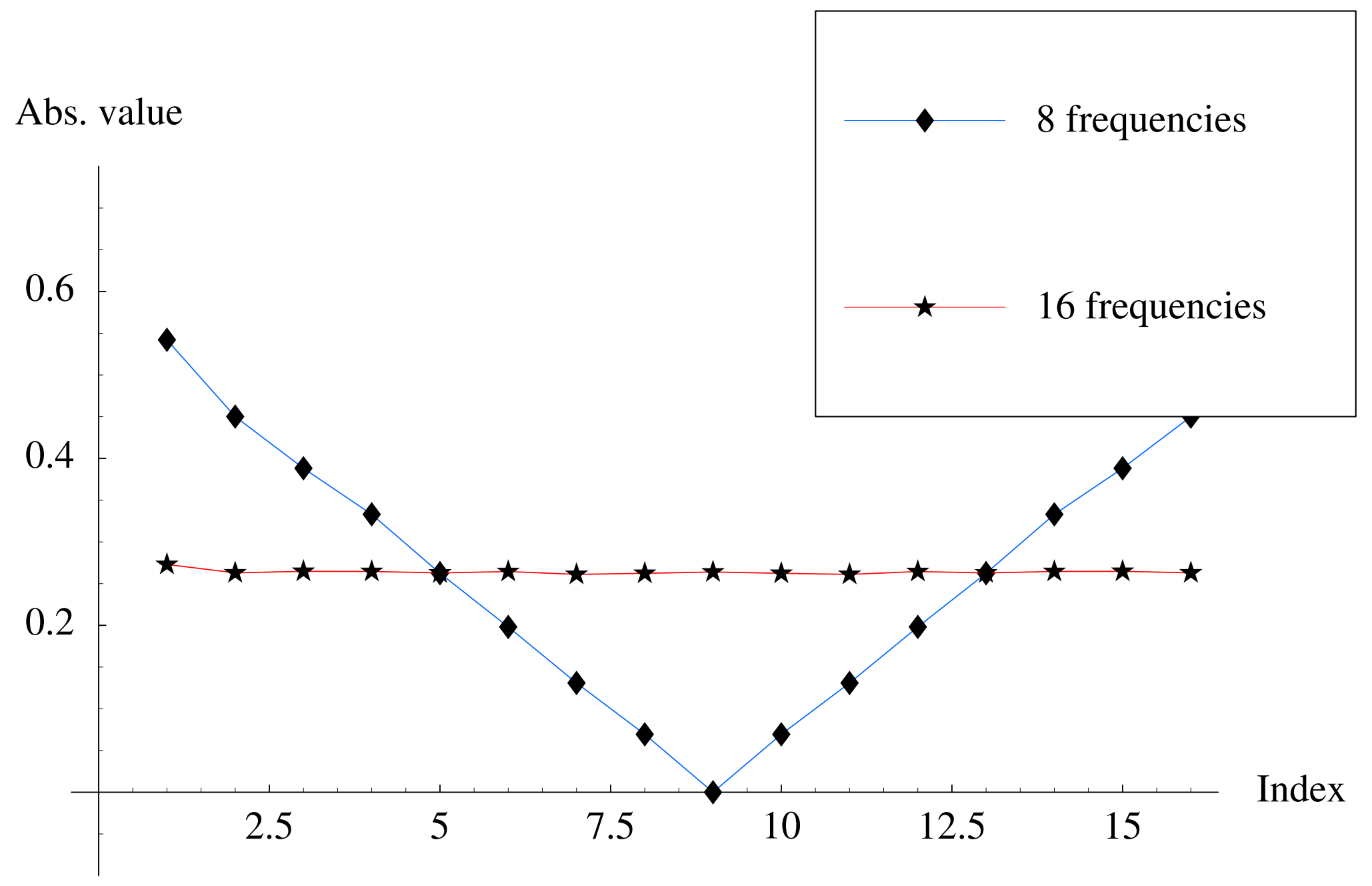


Figure 3: The Discrete Fourier Transform of the probability function for $|1\rangle$, sampled at 16 points

Proof sketch: A Discrete Fourier Transform of $p_m(\varphi)$ at $N=\frac{1}{2\varepsilon}$ points yields

$$DFT_N[p_m(\varphi)](k) = \sqrt{N} \sum_{\substack{l\in L_\varphi \\ l\equiv k \mod N}} \eta_{m,l}.$$

We know that if the state m is "correct" for a certain phase $\varphi_m = m/N$, the success probability has to be high: $p_m(m/N)\geq\frac{3}{4}$.

We can therefore bound

$$|DFT_N[p_m(\varphi)](k)| \geq \left| p_m(\frac{m}{N}) e^{2\pi imk/N} \right| - \left| \sum_{\substack{n=0\\n\neq m}}^{N-1} p_m(\frac{n}{N}) e^{2\pi ink/N} \right| > 0.$$

Since this holds for all $k=0,\ldots,N-1$, at least N of the coefficients $\eta_{m,l}$ must be non-zero. In other words: the probability function must have more than N present frequencies. □

Theorem 4. *Every quantum algorithm that computes an ε approximation to the phase estimation problem has to use at least $\Omega(\log\frac{1}{\varepsilon})$ power queries.*

Proof. Combining proposition 2 and 3 we get $2^{2T}\geq c\frac{1}{\varepsilon}$ and therefore

$$T \geq c'\log\frac{1}{\varepsilon}.$$

□

4 Conclusion

The use of controlled queries in the phase estimation algorithm yielded exponential speed-up compared to standard quantum queries. In this paper we could show that the proposed repeated squaring pattern is optimal in the number of power queries, i.e., it uses the powers in the optimal way.

Interesting future research includes the application of these techniques to the problems of eigenvalue estimation and order-finding to find query lower bounds for these problems.

5 Acknowledgments

The author would like to thank J. Traub and H. Woźniakowski for insightful discussions. This research was supported in part by the National Science Foundation (NSF) and by the Defense Advanced Research Agency (DARPA) and Air Force Research Laboratory under agreement F30602-01-2-0523.

References

[1] 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. quant-ph/9802049.

[2] Arvid J. Bessen. The power of various real-values quantum queries. *Journal of Complexity*, 2004. to be published, quant-ph/0308140.

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

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

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

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