Quantum Information and Computation, Vol. 12, No. 9&10 (2012) 0864–0875

QUANTUM PHASE ESTIMATION WITH ARBITRARY CONSTANT-PRECISION PHASE SHIFT OPERATORS

HAMED AHMADI
Department of Mathematics, University of Central Florida, 4000 Central Florida Boulevard Orlando, FL 32816, USA.[a]

CHEN-FU CHIANG
Département de Physique, Université de Sherbrooke 2500, boul. de l'Université Sherbrooke, Québec, Canada J1K 2R1S.[b]

Received January 12, 2011
Revised May 23, 2012

While Quantum phase estimation (QPE) is at the core of many quantum algorithms known to date, its physical implementation (algorithms based on quantum Fourier transform (QFT)) is highly constrained by the requirement of high-precision controlled phase shift operators, which remain difficult to realize. In this paper, we introduce an alternative approach to approximately implement QPE with arbitrary constant-precision controlled phase shift operators.

The new quantum algorithm bridges the gap between QPE algorithms based on QFT and Kitaev's original approach. For approximating the eigenphase precise to the nth bit, Kitaev's original approach does not require any controlled phase shift operator. In contrast, QPE algorithms based on QFT or approximate QFT require controlled phase shift operators with precision of at least Pi/2n. The new approach fills the gap and requires only arbitrary constant-precision controlled phase shift operators. From a physical implementation viewpoint, the new algorithm outperforms Kitaev's approach.

Keywords: Phase estimation, Fourier transform, Eigenvalue, Hadamard test, Finite precision
Communicated by: R Jozsa & M Mosca

1 Introduction

Quantum Phase Estimation (QPE) plays a core role in many quantum algorithms [1, 2, 3, 4, 5]. Some interesting algebraic and theoretic problems can be addressed by QPE, such as prime factorization [2], discrete-log finding [3], and order finding.

Problem 1 [Phase Estimation] *Let U be a unitary matrix with eigenvalue $e^{2\pi i\varphi}$ and corresponding eigenvector $|u\rangle$. Assume only a single copy of $|u\rangle$ is available, the goal is to find $\widetilde{\varphi}$ such that*

$$\Pr(|\widetilde{\varphi}-\varphi|<\frac{1}{2^n})>1-c, \tag{1}$$

where c is a constant less than $\frac{1}{2}$.

In this paper we investigate a more general approach for the QPE algorithm. This approach completes the transition from Kitaev's original approach that requires no controlled

[a]Email: hahmadi@cs.ucf.edu
[b]Email: Chen-Fu.Chiang@USherbrooke.ca

phase shift operators, to QPE with approximate quantum Fourier transform (AQFT). The standard QPE algorithm utilizes the complete version of the inverse QFT. The disadvantage of the standard phase estimation algorithm is the high degree of phase shift operators required. Since implementing exponentially small phase shift operators is costly or physically not feasible, we need an alternative way to use lower precision operators. This was the motivation for AQFT being introduced — for lowering the cost of implementation while preserving high success probability.

In AQFT the number of required phase shift operators drops significantly with the cost of lower success probability. Such compromise demands repeating the process extra times to achieve the final result. The QPE algorithm has a success probability of at least $\frac{8}{\pi^2}$ [6]. Phase estimation using AQFT instead, with phase shift operators up to degree m where $m > \log_2(n) + 2$, has success probability at least $\frac{4}{\pi^2} - \frac{1}{4n}$ [7, 8].

On the other hand, Kitaev's original approach requires only the first phase shift operator (as a single qubit gate not controlled). Comparing the existing methods, there is a gap between Kitaev's original approach and QPE with AQFT in terms of the degree of phase shift operators needed. In this paper our goal is to fill this gap and introduce a more general phase estimation algorithm such that it is possible to realize a phase estimation algorithm with any degree of phase shift operators in hand. In physical implementation of the phase estimation algorithm, the depth of the circuit should be small to avoid decoherence. Also, higher degree phase shift operators are costly to implement and in many cases it is not physically feasible.

In this paper, we assume only one copy of the eigenvector $|u\rangle$ is available. This implies a restriction on the use of controlled-U gates that all controlled-U gates should be applied on one register. Thus, the entire process is a single circuit that can not be divided into parallel processes. Due to results by Griffiths and Niu, who introduced semi classical quantum Fourier transform [9], quantum circuits implementing different approaches discussed in this paper would require the same number of qubits.

The structure of this paper is organized as follows. In Sec. 2 we give a brief overview on existing approaches, such as Kitaev's original algorithm and standard phase estimation algorithm based on QFT and AQFT. In Sec. 3 we introduce our new approach and discuss the requirements to achieve the same performance output (success probability) as the methods above. Finally, we make our conclusion and compare with other methods.

2 Quantum phase estimation algorithms

2.1 Kitaev's original approach

Kitaev's original approach is one of the first quantum algorithms for estimating the phase of a unitary matrix [10]. Let U be a unitary matrix with eigenvalue $e^{2\pi i\varphi}$ and corresponding eigenvector $|u\rangle$ such that

$$U|u\rangle = e^{2\pi i\varphi}|u\rangle . \tag{2}$$

In this approach, a series of Hadamard tests are performed. In each test the phase $2^{k-1}\varphi$ $(1 \leq k \leq n)$ will be computed up to precision $1/16$. Assume an n-bit approximation is desired. Starting from $k = n$, in each step the kth bit position is determined consistently from the results of previous steps.

For the kth bit position, we perform the Hadamard test depicted in Figure 1, where the gate $K = I_2$. Denote $\varphi_k = 2^{k-1}\varphi$, the probability of the post measurement state is

$$\Pr(0|k) = \frac{1+\cos(2\pi\varphi_k)}{2}, \quad \Pr(1|k) = \frac{1-\cos(2\pi\varphi_k)}{2}. \tag{3}$$

In order to recover φ_k, we obtain more precise estimates with higher probabilities by iterating the process. But, this does not allow us to distinguish between φ_k and $-\varphi_k$. This can be solved by the same Hadamard test in Figure 1, but instead we use the gate

$$K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{4}$$

The probabilities of the post-measurement states based on the modified Hadamard test become

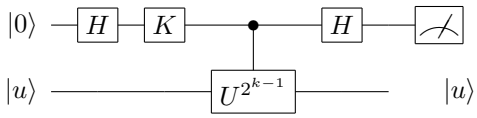

Fig. 1. Hadamard test with extra phase shift operator.

$$\Pr(0|k) = \frac{1-\sin(2\pi\varphi_k)}{2}, \quad \Pr(1|k) = \frac{1+\sin(2\pi\varphi_k)}{2}. \tag{5}$$

Hence, we have enough information to recover φ_k from the estimates of the probabilities.

In Kitaev's original approach, after performing the Hadamard tests, some classical post processing is also necessary. Suppose $\varphi = 0.x_1x_2\ldots x_n$ is an exact n-bit. If we are able to determine the values of φ, $2\varphi, \ldots, 2^{n-1}\varphi$ with some constant-precision (1/16 to be exact), then we can determine φ with precision $1/2^n$ efficiently [11, 10].

Starting with φ_n we increase the precision of the estimated fraction as we proceed toward φ_1. The approximated values of φ_k $(k = n, \ldots, 1)$ will allow us to make the right choices.

For $k = 1, \ldots, n$ the value of φ_k is replaced by β_k, where β_k is the closest number chosen from the set $\{\frac{0}{8}, \frac{1}{8}, \frac{2}{8}, \frac{3}{8}, \frac{4}{8}, \frac{5}{8}, \frac{6}{8}, \frac{7}{8}\}$ such that

$$|\varphi_k - \beta_k|_{\text{mod } 1} < \frac{1}{8}. \tag{6}$$

The result follows by a simple iteration. Let $\beta_n = \overline{0.x_nx_{n+1}x_{n+2}}$ and proceed by the following iteration:

$$x_k = \begin{cases} 0 & \text{if} \quad |\overline{0.0x_{k+1}x_{k+2}} - \beta_k|_{\text{mod } 1} < 1/4 \\ 1 & \text{if} \quad |\overline{0.1x_{k+1}x_{k+2}} - \beta_k|_{\text{mod } 1} < 1/4 \end{cases} \tag{7}$$

for $k = n-1, \ldots, 1$. By using simple induction, the result satisfies the following inequality:

$$|\overline{0.x_1x_2\ldots x_{n+2}} - \varphi|_{\text{mod } 1} < 2^{-(n+2)}. \tag{8}$$

In Eq. 6, we do not have the exact value of φ_k. So, we have to estimate this value and use the estimate to find β_k. Let $\widetilde{\varphi_k}$ be the estimated value and

$$\epsilon = |\widetilde{\varphi_k} - \varphi_k|_{\text{mod } 1} \tag{9}$$

be the estimation error. Now we use the estimate to find the closest β_k. Since we know the exact binary representation of the estimate $\widetilde{\varphi_k}$, we can choose β_k such that

$$|\widetilde{\varphi_k} - \beta_k|_{\text{mod } 1} \leq \frac{1}{16}. \tag{10}$$

By the triangle inequality we have,

$$|\varphi_k - \beta_k|_{\text{mod } 1} \leq |\widetilde{\varphi_k} - \varphi_k|_{\text{mod } 1} + |\widetilde{\varphi_k} - \beta_k|_{\text{mod } 1} \leq \epsilon + \frac{1}{16}. \tag{11}$$

To satisfy Eq. 6, we need to have $\epsilon < 1/16$, which implies

$$|\widetilde{\varphi_k} - \varphi_k|_{\text{mod } 1} < \frac{1}{16}. \tag{12}$$

Therefore, it is required for the phase to be estimated with precision $1/16$ at each stage.

In the first Hadamard test (Eq. 3), in order to estimate $\Pr(1|k)$ an iteration of Hadamard tests should be applied to obtain the required precision of $1/16$ for φ_k. This is done by counting the number of states $|1\rangle$ in the post measurement state and dividing that number by the total number of iterations performed.

The Hadamard test outputs $|0\rangle$ or $|1\rangle$ with a fixed probability. We can model an iteration of Hadamard tests as Bernoulli trials with success probability (obtaining $|1\rangle$) being p_k. The best estimate for the probability of obtaining the post measurement state $|1\rangle$ with t samples is

$$\widetilde{p_k} = \frac{h}{t}, \tag{13}$$

where h is the number of ones in t trials. This can be proved by Maximum Likelihood Estimation (MLE) methods [12].

In order to find $\sin(2\pi\varphi_k)$ and $\cos(2\pi\varphi_k)$, we can use estimates of probabilities in Eq. 3 and EQ. 5. Let s_k be the estimate of $\sin(2\pi\varphi_k)$ and t_k the estimate of $\cos(2\pi\varphi_k)$. It is clear that if

$$|\widetilde{p_k} - p_k| < \epsilon_0, \tag{14}$$

then

$$|s_k - \sin(2\pi\varphi_k)| < 2\epsilon_0, \quad |t_k - \cos(2\pi\varphi_k)| < 2\epsilon_0. \tag{15}$$

Since the inverse tangent function is more robust to error than the inverse sine or cosine functions, we use

$$\widetilde{\varphi_k} = \frac{1}{2\pi} \arctan\left(\frac{s_k}{t_k}\right) \tag{16}$$

as the estimation of φ_k. By Eq. 12 we should have

$$\left|\varphi_k - \frac{1}{2\pi} \arctan\left(\frac{s_k}{t_k}\right)\right|_{\text{mod } 1} < \frac{1}{16}. \tag{17}$$

The inverse tangent function can not distinguish between the two values φ_k and $\varphi_k \pm 1/2$. However, because we find estimates of the sine and cosine functions as well, the correct value can be determined properly. It is easy to see, in order to estimate the phase φ_k with precision $1/16$, the probabilities in Eq. 3 and Eq. 5 should be estimated with error at most $\frac{1}{4}\sqrt{1 - \frac{1}{\sqrt{2}}}$

which is approximately 0.1353. In other words, it is necessary to find the estimate of $\Pr(1|k)$ such that

$$\left|\Pr(1|k) - \frac{h}{t}\right| < \frac{1}{4}\sqrt{1 - \frac{1}{\sqrt{2}}} \approx 0.1353. \tag{18}$$

There are different ways we can guarantee an error bound with constant probability. The first method, used in [10], is based on the Chernoff bound. Let $X_1, \ldots, X_m$ be Bernoulli random variables, by Chernoff's bound we have

$$\Pr\left(\left|\frac{1}{m}\sum_{i=0}^{m} X_i - p_k\right| \geq \delta\right) \leq 2e^{-2\delta^2 m}, \tag{19}$$

where in our case the estimate is $\widetilde{p_k} = \frac{1}{m}\sum_{i=0}^{m} X_i$. Since we need an accuracy up to 0.1353, we get

$$\Pr\left(|\widetilde{p_k} - p_k| > 0.1353\right) < 2e^{-(0.0366)m}. \tag{20}$$

In order to obtain

$$\Pr\left(|\widetilde{p_k} - p_k| < 0.1353\right) > 1 - \frac{\varepsilon}{2}, \tag{21}$$

a minimum of m_1 trials is sufficient when

$$\begin{aligned} m_1 &\approx 28 \ln \frac{4}{\varepsilon} \\ &\approx 38 + 28 \ln \frac{1}{\varepsilon} \end{aligned} \tag{22}$$

This is the number of trials for each Hadamard test, as we have two Hadamard tests at each stage. Therefore, in order to have

$$\Pr\left(|\widetilde{\varphi_k} - \varphi_k| < \frac{1}{16}\right) > 1 - \varepsilon. \tag{23}$$

we require a minimum of

$$\begin{aligned} m &= 2m_1 \\ &\approx 55 \ln \frac{4}{\varepsilon} \\ &\approx 76 + 55 \ln \frac{1}{\varepsilon} \end{aligned} \tag{24}$$

many trials.

In the analysis above, we used the Chernoff bound, which is not a tight bound. If we want to obtain the result with a high probability, we need to apply a large number of Hadamard tests. In this case, we can use an alternative method to analyze the process by employing methods of statistics [13].

Iterations of Hadamard tests have a Binomial distribution which can be approximated by a normal distribution. This is a good approximation when p is close to $1/2$ or $mp > 10$ and $m(1-p) > 10$, where m is the number of iterations and p the success probability. In other words, if we see 10 successes and 10 fails in our process, we can use this approximation to obtain a better bound.

In Kitaev's algorithm each Hadamard test has to be repeated a sufficient number of times to achieve the required accuracy with high probability. Because only one copy of $|u\rangle$ is available, all controlled-U gates have to be applied to one register. Therefore, all the Hadamard tests have to be performed in sequence, instead of parallel, during one run of the circuit. A good example for this case is the order finding algorithm. We refer the reader to [14] for more details.

In Kitaev's approach, there are n different Hadamard tests that should be performed. Thus, if the probability of error in each Hadamard test is ε_0, by applying the union bound, the error probability of the entire process is $\varepsilon = n\varepsilon_0$. Therefore, in order to obtain

$$\Pr(|\varphi - \widetilde{\varphi}| < \frac{1}{2^n}) > 1 - \varepsilon, \tag{25}$$

for approximating each bit we need m trials where

$$m = 55 \ln \frac{4n}{\varepsilon}. \tag{26}$$

Since, all of these trials have to be done in one circuit, the circuit consists of mn Hadamard tests. Therefore the circuit involves mn controlled-U^{2^k} operations. As a result, if a constant success probability is desired, the depth of the circuit will be $O(n \log n)$.

2.2 Approach based on QFT

One of the standard methods to approximate the phase of a unitary matrix is QPE based on QFT. The structure of this method is depicted at Figure 2. The QPE algorithm requires two registers and contains two stages. If an n-bit approximation of the phase φ is desired, then the first register is prepared as a composition of n qubits initialized in the state $|0\rangle$. The second register is initially prepared in the state $|u\rangle$. The first stage prepares a uniform superposition over all possible states and then applies controlled-U^{2^k} operations. Consequently, the state will become

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i \varphi k} |k\rangle. \tag{27}$$

The second stage in the QPE algorithm is the $\mathrm{QFT}^\dagger$ operation.

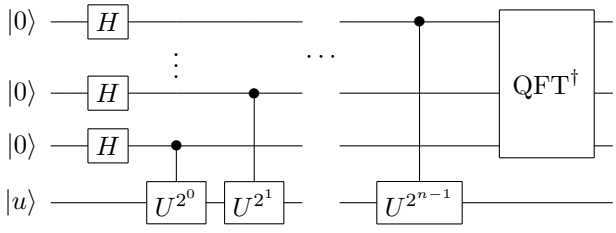

Fig. 2. Standard Quantum Phase Estimation.

There are different ways to interpret the inverse Fourier transform. In the QPE algorithm, the post-measurement state of each qubit in the first register represents a bit in the final approximated binary fraction of the phase. Therefore, we can consider computing each bit

as a step. The inverse Fourier transform can be interpreted such that at each step (starting from the least significant bit), using the information from previous steps, it transforms the state

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^k \varphi}|1\rangle) \tag{28}$$

to get closer to one of the states

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.0}|1\rangle) &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &\text{or} \\ \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.1}|1\rangle) &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{29}$$

Assume we are at step k in the first stage. By applying controlled-U^{2^k} operators due to phase kick back, we obtain the state

$$\frac{|0\rangle + e^{2\pi i 0.x_{k+1}x_{k+2}\ldots x_n}|1\rangle}{\sqrt{2}}. \tag{30}$$

Shown in Figure 3, each step (dashed-line box) uses the result of previous steps, where phase shift operators are defined as

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{31}$$

for $2 \leq k \leq n$.

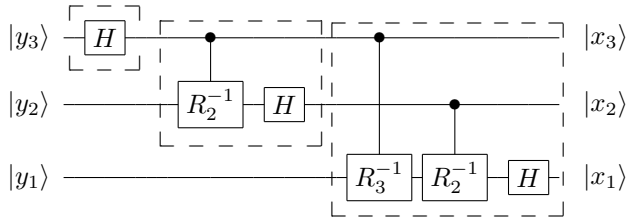

Fig. 3. 3-qubit inverse QFT where $1 \leq i \leq 3$, $|y_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_i\ldots x_3)}|1\rangle)$.

By using the previously determined bits $x_{k+2}, \ldots, x_n$ and the action of corresponding controlled phase shift operators (as depicted in Figure 3) the state in Eq. 30 becomes

$$\frac{|0\rangle + e^{2\pi i 0.x_{k+1}0\ldots 0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + (-1)^{x_{k+1}}|1\rangle}{\sqrt{2}}. \tag{32}$$

Thus, by applying a Hadamard gate to the state above we obtain $|x_{k+1}\rangle$. Therefore, we can consider the inverse Fourier transform as a series of Hadamard tests.

If φ has an exact n-bit binary representation the success probability at each step is 1. While, in the case that φ cannot be exactly expressed in n-bit binary fraction, the success probability P of the post-measurement state, at step k, is

$$P = \cos^2(\pi\theta) \quad \text{for} \quad |\theta| < \frac{1}{2^{k+1}} \tag{33}$$

Detailed analysis obtaining similar probabilities are given in Sec. 3.

Therefore, the success probability increases as we proceed. The following theorem gives us the success probability of the QFT algorithm.

Theorem 1 ([6]) *If* $\frac{x}{2^n} \leq \varphi \leq \frac{x+1}{2^n}$*, then the phase estimation algorithm returns one of* x *or* $x+1$ *with probability at least* $\frac{8}{\pi^2}$*.*

2.3 Approach based on AQFT

AQFT was first introduced by Barenco, et al [7]. It has the advantage in algorithms that involve periodicity estimation. Its structure is similar to regular QFT but differs by eliminating higher precision phase shift operators. The circuit of AQFT is shown in Figure 4. At the RHS of the circuit, for $n - m < i \leq n$

$$|y_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_i \ldots x_n)}\,|1\rangle) \tag{34}$$

and for $1 < i \leq n - m$,

$$|y_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_i \ldots x_{i+m-1})}\,|1\rangle). \tag{35}$$

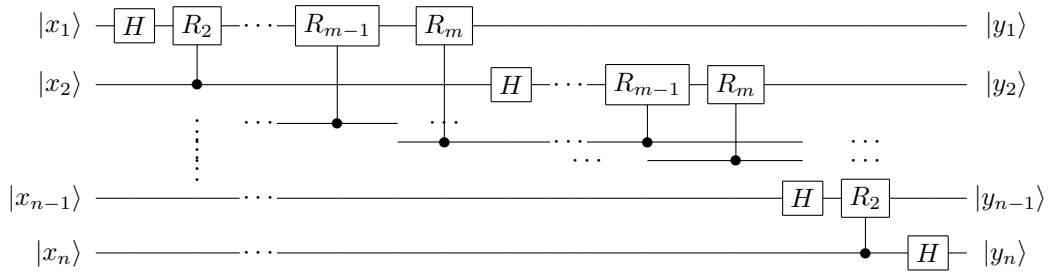

Fig. 4. Quantum circuit for AQFT.

Let $0.x_1x_2 \ldots x_n$ be the binary representation of eigenphase φ. For estimating each x_p, where $1 \leq p \leq n$, AQFT_m requires at most m phase shift operations. Here m is defined as the degree of the AQFT_m.

Therefore, phase shift operations in AQFT_m requires precision up to $e^{2\pi i/2^m}$. The probability P of gaining an accurate output using AQFT_m, when $m \geq \log_2 n + 2$, is at least [7]

$$P \geq \frac{8}{\pi^2}(\sin^2(\frac{\pi}{4}\frac{m}{n})). \tag{36}$$

The accuracy of AQFT_m approaches the lower bound for the accuracy of the full QFT, which is $\frac{8}{\pi^2}$. A better lower bound is also achieved by Cheung in [8]

$$P \geq \frac{4}{\pi^2} - \frac{1}{4n}. \tag{37}$$

Moreover, this indicates the logarithmic-depth AQFT provides an alternative approach to replace the regular QFT in many quantum algorithms. The total number of the phase shift

operator invocations in AQFT_m is $O(n \log_2 n)$, instead of $O(n^2)$ in the QFT. The phase shift operator precision requirement is only up to $e^{2\pi i/4n}$, instead of $e^{2\pi i/2^n}$.

By using the AQFT instead of the QFT we trade off smaller success probability with smaller degrees of phase shift operators and a shorter circuit.

3 New approach with constant degree phase shift operators

In this section we introduce our new approach for QPE. Our approach draws a trade-off between the highest degree of phase shift operators being used and the depth of the circuit. As a result, when smaller degrees of phase shift operators are used, the depth of the circuit increases and vice versa.

As pointed out in Sec. 2.2, by using information of previous qubits, the full-fledged inverse QFT transforms the phase such that the phase of the corresponding qubit gets closer to one of the states $|+\rangle$ or $|-\rangle$. For our approach, we first consider the case where only the controlled phase shifts operators R_2 and R_3 are used (Eq. 31). In this case, we only use the information of the two previous qubits (see Figure 5). In such a setting, we show that it is possible to perform the QPE algorithm with arbitrary success probability.

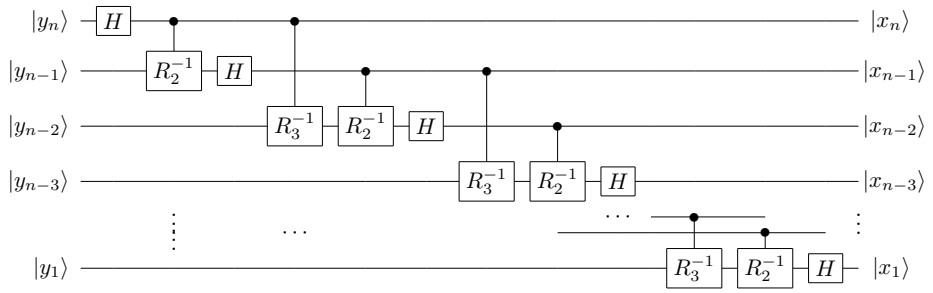

Fig. 5. QPE with only two controlled phase shift operations.

The first stage of our algorithm is similar to the first stage of QPE based on QFT. Assume the phase is $\varphi = 0.x_1x_2x_3\ldots$ with an infinite binary representation. At step k, the phase after the action of the controlled gate U^{2^k} is $2^k\varphi = 0.x_{k+1}x_{k+2}\ldots$ and the corresponding state is

$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^k \varphi}\,|1\rangle). \tag{38}$$

By applying controlled phase shift operators R_2 (controlled by the $(k-1)$th qubit) and R_3 (controlled by the $(k-2)$th qubit) to the state above, we obtain

$$\left|\widetilde{\psi_k}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \widetilde{\varphi}}\,|1\rangle), \tag{39}$$

where

$$\widetilde{\varphi} = 0.x_{k+1}00x_{k+4}\ldots. \tag{40}$$

It is easy to see that

$$|\widetilde{\varphi} - 0.x_{k+1}| < \frac{1}{8}. \tag{41}$$

Hence, we can express

$$\widetilde{\varphi} = 0.x_{k+1} + \theta \tag{42}$$

where $|\theta| < \frac{1}{8}$. Therefore, the state $\left|\widetilde{\psi_k}\right\rangle$ can be rewritten as

$$\left|\widetilde{\psi_k}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(0.x_{k+1}+\theta)}\,|1\rangle). \tag{43}$$

In order to approximate the phase φ at this stage (kth step), we need to find the value of x_{k+1} by measuring the kth qubit. In this regard, we first apply a Hadamard gate before the measurement to the state $\left|\widetilde{\psi_k}\right\rangle$. The post-measurement state will determine the value of x_{k+1} correctly with high probability. The post measurement probabilities of achieving $|0\rangle$ or $|1\rangle$ in the case where $x_{k+1} = 0$ is

$$\begin{aligned} \Pr(0|k) &= \cos^2(\pi\theta) \\ \Pr(1|k) &= \sin^2(\pi\theta). \end{aligned} \tag{44}$$

Therefore,

$$\begin{aligned} \Pr(0|k) &\geq \cos^2(\frac{\pi}{8}) \approx 0.85 \\ \Pr(1|k) &\leq \sin^2(\frac{\pi}{8}) \approx 0.15 \end{aligned} \tag{45}$$

In the case where $x_{k+1} = 1$, the success probability is similar.

By iterating this process a sufficient number of times and then letting the majority decide, we can achieve any desired accuracy. The analysis is similar to Sec. 2.1. In this case, all we require is to find the majority. Therefore, by a simple application of the Chernoff's bound

$$\Pr\left(\frac{1}{m}\sum_{i=0}^{m} X_i \leq \frac{1}{2}\right) \leq e^{-2m(p-\frac{1}{2})^2}, \tag{46}$$

where in this case $p = \cos^2(\pi/8)$. It is easy to see that if a success probability of $1-\varepsilon$ is required, then we need at least

$$m = 4\ln(\frac{1}{\varepsilon}) \tag{47}$$

many trials for approximating each bit.

By comparing Eq. 26 and Eq. 47 (Table 1), we see that while preserving the success probability, our new algorithm differs by a constant and scales about 14 times better than Kitaev's original approach in terms of the number of Hadamard tests required (Figure 6). In physical implementations this is very important, especially in the case where only one copy of the eigenvector $|u\rangle$ is available and all Hadamard tests should be performed during one run of the circuit.

In the algorithm introduced above, only phase shift operators R_2 and R_3 are used. When higher phase shift operators are used in our algorithm, the success probability of each Hadamard test will increase. As a result, fewer trials are required in order to achieve similar success probabilities. As pointed out in Sec. 2.3, the QPE based on AQFT requires phase shift operators of degree at least $2+\log n$. With this precision of phase shift operators in hand, the

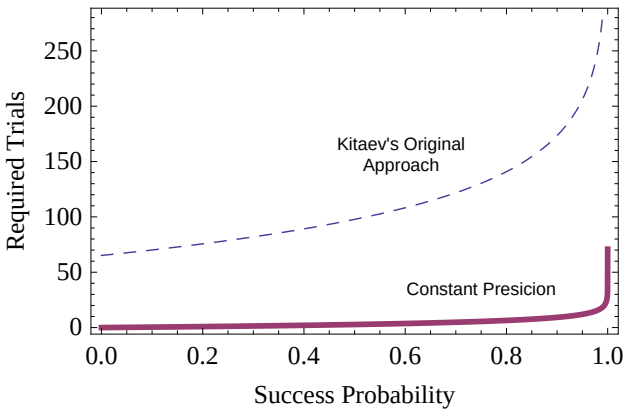

Fig. 6. Required trails for estimating each bit in Kitaev's original approach and our new approach.

success probability at each step would be high enough such that there is no need to iterate each step. In such scenario, one trial is sufficient to achieve an overall success probability of a constant.

Table 1. Required trials for estimating each bit by using Chernoff's bound.

Success Probability	**Kitaev's Original Approach**	**Constant Precision**
0.50000	114	3
0.68269	139	5
0.95450	245	13
0.99730	399	24
0.99993	599	39

Recall the phase estimation problem stated in the introduction. If a constant success probability greater than $\frac{1}{2}$ is required, the depth of the circuit for all the methods mentioned in this paper (except the QPE based on full fledged QFT, which is $O(n^2)$), would be $O(n \log n)$ (assuming the cost of implementing the controlled-U^{2^k} gates are all the same). This means the depth of the circuits differ only by a constant. However, the disadvantage of Kitaev's original approach to our new approach is the large number of Hadamard tests required for each bit in the approximated fraction.

Therefore, the new method introduced in this paper provides the flexibility of using any available degree of controlled phase shift operators while preserving the success probability and the length of the circuit up to a constant.

Acknowledgments

We would like to thank Pawel Wocjan for useful discussions and Stephen Fulwider for helpful comments. H. A. and C. C. gratefully acknowledge the support of NSF grants CCF-0726771 and CCF-0746600. C. C. also gratefully acknowledges the support of Lockheed Martin Corporation.

References

1. S. Hallgren (2007), *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*, J. ACM, 54, no. 1.
2. P. W. Shor (1994), *Algorithms for quantum computation: discrete logarithms and factoring*, in 35th Ann. IEEE Symp. Found. (Santa Fe, NM, 1994), pp. 124–134.
3. P. W. Shor (1997), *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comp., 26, no. 5, pp. 1484–1509.
4. M. Szegedy (2004), *Quantum speed-up of markov chain based algorithms*, in 45th Ann. IEEE Symp. Found., pp. 32 – 41.
5. P. Wocjan , C. Chiang, D. Nagaj and A. Abeyesinghe (2009), *Quantum algorithm for approximating partition functions*, Phys. Rev. A, 80, p. 022340.
6. P. Kaye, R. Laflamme and M. Mosca (2007), *An introduction to quantum computing*. Oxford: Oxford University Press.
7. A. Barenco, A. Ekert, K. Suominen and P. Törmä (1996), *Approximate quantum Fourier transform and decoherence*, Phys. Rev. A, 54, no. 1, pp. 139–146.
8. D. Cheung (2004), *Improved bounds for the approximate QFT*, Proceedings of the winter international symposium on Information and communication technologies, WISICT '04, pp. 1–6, Trinity College Dublin.
9. R. Griffiths and C. Niu (1996), *Semiclassical fourier transform for quantum computation*, Phys. Rev. Lett., 76, no. 17, pp. 3228–3231.
10. A. Kitaev, A. H. Shen and M. N. Vyalyi (2002), *Classical and quantum computation*, Providence, RI: American Mathematical Society.
11. A. Kitaev (1996), *Quantum measurements and the Abelian stabilizer problem*, technical report.
12. J. W. Harris and H. Stocker (1998), *Maximum likelihood method*, Handbook of Mathematics and Computational Science, p. 824, New York: Springer-Verlag.
13. D. Sivia and J. Skilling (2006), *Data analysis: a Bayesian tutorial*. Oxford science publications, Oxford University Press.
14. M. A. Nielsen and I. L. Chuang (2000), *Quantum computation and quantum information*. Cambridge: Cambridge University Press.