THE AMPLIFIED QUANTUM FOURIER TRANSFORM (AMPLIFIED-QFT)

DAVID J. CORNWELL

Abstract. In this paper, we show how to use Grover's algorithm to amplify and enhance the period finding capability of the quantum Fourier Transform (QFT).

In particular, we create a quantum algorithm, called the A**mplified-QFT algorithm**, which solves the following problem:
The Local Period Finding Problem: Let $\mathcal{L} = \{0, 1, ..., N-1\}$ be a set of N labels, and let A be a subset of M labels of period P, i.e., a subset of the form

$$A = \{j : j = s + rP, r = 0, 1, 2, \ldots, M-1\} \ ,$$

where $P \leq \sqrt{N}$ and $M << N$ and M is assumed known. Given a binary oracle $f : \mathcal{L} \longrightarrow \{0, 1\}$ which is 1 on A and 0 elsewhere (i.e., which is the characteristic function of A), find the period P.

The Amplified-QFT algorithm which solves this problem consists of three steps. **Step 1:** Apply Grover's algorithm without measurement to amplify the amplitudes of the M labels of the set A. **Step 2:** Apply the QFT to the resulting state. **Step 3:** Measurement.

We compare the probabilities of success of three algorithms that can be used to recover the period P: (1) Amplified-QFT (2) QFT and (3) QHS algorithms. Let the set $S_{ALG} = \{y : |\frac{y}{N} - \frac{d}{P}| \leq \frac{1}{2P^2}, (d, P) = 1\}$ be the set of "successful" y's. That is S_{ALG} consists of those y's which can be measured after applying one of the three algorithms denoted by ALG and from which the period P can be recovered by the method of continued fractions. We show that

$$\frac{N}{4M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QFT})} \geq \frac{N}{4M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2$$

and

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QHS})} \geq \frac{N}{2M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2$$

This shows that the Amplified-QFT is approximately $\frac{N}{4M}$ times more successful than the QFT and is $\frac{N}{2M}$ times more successful than the QHS. In addition it also shows that the QFT is 2 times more successful than the QHS in this problem. However, the success of the Amplified-QFT algorithm comes with a penalty of an increased work factor of $O(\sqrt{\frac{N}{M}})$. We also show how to recover the offset s and to test whether the pair of values (s, P) is correct.

Acknowledgement 1. *I would like to thank my advisor, Professor Samuel J. Lomonaco of the CSEE Department of the University of Maryland Baltimore County (UMBC) for his encouragement, analysis, feedback and direction in the writing of this paper.*

Date: September 30th, 2010.

2000 *Mathematics Subject Classification.* Primary 05C38, 15A15; Secondary 05A15, 15A18.

Key words and phrases. Quantum Fourier Transform, Amplitude Amplification, Oracle, Period Finding, Shor Algorithm, Grover Algorithm.

Contents

1. **Introduction**

We investigate the Amplified Quantum Fourier Transform (Amplified-QFT) algorithm which solves the following problem with a run time complexity of
$O(\sqrt{N/M}\log(N) + \log(N))$:

The Local Period Finding Problem: Let $\mathcal{L} = \{0, 1, ..., N-1\}$ be a set of N labels, and let A be a subset of M labels of period P, i.e., a subset of the form

$$A = \{j : j = s + rP, r = 0, 1, 2, \ldots, M-1\} \ ,$$

where $P \leq \sqrt{N}$ and $M << N$ and M is assumed known Given a binary oracle $f : \mathcal{L} \longrightarrow \{0, 1\}$ which is 1 on A and 0 elsewhere (i.e., which is the characteristic function of A), find the period P. The problem is to determine the period P.

The Amplified-QFT begins by first applying Grover's algorithm (without the last measurement step) to the state $|0>$. This procedure, known as amplitude amplification, uniformly increases the magnitude of the amplitude of the M labels in the set A while uniformly decreasing the magnitude of the amplitude of the remaining $N - M$ labels. The second step applies the quantum Fourier transform (QFT). The third and final step measures the resulting state in order to produce a y from which the period P can be recovered by the method of continued fractions.

In addition we compare the Amplified-QFT algorithm and with the generic QFT when applied to the Oracle. We also compare the Amplified-QFT to the Quantum Hidden Subgroup (QHS) algorithm when applied to the Oracle. In the tables below, we summarize our results, comparing the probability of measuring a y in the final state arrived at after applying one of the three algorithms- Amplified-QFT, QFT and QHS, where $\sin\theta = \sqrt{M/N}$ and $k = \lfloor \frac{\pi}{4\theta} \rfloor$:

Case 1 (Amplified-QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{lll} \cos^2 2k\theta & \text{if} & y = 0 \\ tan^2\theta \sin^2 2k\theta & \text{if} & Py = 0 \bmod N, y \neq 0 \\ \frac{1}{M^2} tan^2\theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py \neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\ 0 & \text{if} & Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise} \end{array} \right\}$$

Case 2 (QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{lll} \left(1 - \frac{2M}{N}\right)^2 & \text{if} & y = 0 \\ 4\frac{M^2}{N^2} & \text{if} & Py = 0 \bmod N, y \neq 0 \\ \frac{4}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py \neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\ 0 & \text{if} & Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise} \end{array} \right\}$$

Let y be fixed such that either

1. $Py = 0 \bmod N, y \neq 0$ or
2. $Py \neq 0 \bmod N$and $MPy \neq 0 \bmod N$

and define $\Pr Ratio(y) = \Pr(y)_{Amplified-QFT} / \Pr(y)_{QFT}$ then we have the following

$$\frac{N}{4M}\left(\frac{N}{N-M}\right) \geq \Pr Ratio(y) \geq \frac{N}{4M}\left(\frac{N}{N-M}\right)\left(1 - \frac{2M}{N}\right)^2$$
$$\Longrightarrow \Pr Ratio(y) \approx \frac{N}{4M}$$

Case 3 (QHS):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{lll} 1 - \frac{2M(N-M)}{N^2} & \text{if} & y = 0 \\ \frac{2M^2}{N^2} & \text{if} & Py = 0 \bmod N, y \neq 0 \\ \frac{2}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py \neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\ 0 & \text{if} & Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise} \end{array} \right\}$$

Let y be fixed such that either
1. $Py = 0 \bmod N, y \neq 0$ or
2. $Py \neq 0 \bmod N$and $MPy \neq 0 \bmod N$

and define $\Pr Ratio(y) = \Pr(y)_{Amplified-QFT} / \Pr(y)_{QHS}$ then we have the following

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \Pr Ratio(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$
$$\Longrightarrow \Pr Ratio(y) \approx \frac{N}{2M}$$

Let $S_{ALG} = \{y : |\frac{y}{N} - \frac{d}{P}| \leq \frac{1}{2P^2}, (d,P) = 1\}$ be the set of "successful" y's. That is S_{ALG} consists of those y's which can be measured after applying one of the three algorithms denoted by ALG and from which the period P can be recovered by the method of continued fractions. Note that the set S_{ALG} is the same for each algorithm. However the probability of this set varies with each algorithm. We can see from the following that given $y1$ and $y2$, whose probability ratios satisfy the same inequality, we can add their probabilities to get a new ratio that satisfies the same inequality. In this way we can add probabilities over a set on the numerator and denominator and maintain the inequality:

$$A > \frac{P(y1)}{Q(y1)} > B \; and \; A > \frac{P(y2)}{Q(y2)} > B$$
$$\Longrightarrow A > \frac{P(y1) + P2(y2)}{Q(y1) + Q(y2)} > B$$

We see from the cases given above that

$$\frac{N}{4M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QFT})} \geq \frac{N}{4M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$

where the difference between the upper bound and lower bound is exactly 1 and that

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QHS})} \geq \frac{N}{2M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$

where the difference between the upper bound and lower bound is exactly 2.

This shows that the Amplified-QFT is approximately$\frac{N}{4M}$ times more successful than the QFT and $\frac{N}{2M}$ times more successful than the QHS when $M << N$. In addition it also shows that the QFT is 2 times more successful than the QHS in this problem. However, the success of the Amplified-QFT algorithms comes at an increase in work factor of $O(\sqrt{\frac{N}{M}})$. We note that in the case that P is a prime number that $(d,P) = 1$ is met trivially. However when P is composite the algorithms may need to be rerun several times until $(d,P) = 1$ is satisfied.

Towards the end of the paper we show how to test whether a putative value of P, given s is known, can be tested to see if it is the correct value. We also investigate the case where s is unknown but is from a small known set of values such that the values of s can be exhausted over on a classical computer. We also show how s can be recovered by using a quantum algorithm using amplitude amplification followed by a measurement.

2. The Three Step Amplified-QFT algorithm

Problem: We are given a binary valued Oracle $f(x)$ on N labels $\{0, 1, ..., N-1\}$, where $N = 2^n$, which takes the value 1 on a periodic subset $A = \{j : j = s+rP, r = 0, 1..., M-1\}$ of M labels, where s is a non-negative integer called the offset. We wish to determine the period P with the smallest number of queries of the Oracle.

The Amplified-QFT algorithm is defined by the following three step procedure.

Step 1: Apply all of Grover's algorithm in its entirety except for the last measurement step to the starting state $|0>$. The resulting state is given by $|\psi_k>$ (ref[4], ref[7],ref[1]) where $k = \left\lfloor \frac{\pi}{4\sin^{-1}(\sqrt{M/N})} \right\rfloor$:

$$|\psi_k >= a_k \sum_{z\in A} |z > +b_k \sum_{z\notin A} |z >$$

where

$$a_k = \frac{1}{\sqrt{M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin\theta = \sqrt{M/N}, \cos\theta = \sqrt{1-M/N}$$

Now we have , ref[7],

$k = \lfloor \frac{\pi}{4\theta} \rfloor \implies \frac{\pi}{4\theta} - 1 \le k \le \frac{\pi}{4\theta} \implies \frac{\pi}{2} - \theta \le (2k+1)\theta \le \frac{\pi}{2} + \theta$

$\implies \sin\theta = \cos(\frac{\pi}{2} - \theta) \ge \cos(2k+1)\theta \ge \cos(\frac{\pi}{2} + \theta) = -\sin\theta$

Notice that the total probability of the N-M labels that are not in A is

$$(N-M)(\frac{1}{\sqrt{N-M}} \cos(2k+1)\theta)^2 = \cos^2(2k+1)\theta$$

$$\implies \cos^2(2k+1)\theta \le \sin^2\theta = \sin^2(\sin^{-1}(\sqrt{\frac{M}{N}}))$$

$$\implies \cos^2(2k+1)\theta \le \frac{M}{N}$$

whereas the total probability of the M labels in A is

$$M(\frac{1}{\sqrt{M}} \sin(2k+1)\theta)^2 = \sin^2(2k+1)\theta = 1 - \cos^2(2k+1)\theta$$

$$\implies \sin^2(2k+1)\theta \ge 1 - \frac{M}{N}$$

.

Step 2: The QFT performs the following action

$$|z >\to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i z y/N} |y >$$

After the application of the QFT to the state $|\psi_k>$, letting $\omega = e^{-2\pi i/N}$, we have

$$|\phi_k >= \frac{a_k}{\sqrt{N}} \sum_{z\in A} \sum_{y=0}^{N-1} \omega^{zy} |y > + \frac{b_k}{\sqrt{N}} \sum_{z\notin A} \sum_{y=0}^{N-1} \omega^{zy} |y >$$

After interchanging the order of summation, we have

$$|\phi_k >= \sum_{y=0}^{N-1} \left[\frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \right] |y >$$

.

Step 3: Measure with respect to the standard basis to yield a integer $y \in \{0, 1, ..., N-1\}$ from which we can determine the period P using the continued fraction method.

3. **Analysis of the Amplified-QFT Algorithm**

We calculate the $\Pr(y)$ for the following cases:

a) $y = 0$
b) $Py = 0 \bmod N$ and $y \neq 0$
c) $Py \neq 0 \bmod N$

The amplitude $Amp(y)$ of $|y>$ is given by

$$\begin{aligned}
Amp(y) &= \frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \sum_{r=0}^{M-1} \omega^{(s+rP)y} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy}
\end{aligned}$$

3.1. **Amplified-QFT Analysis: y=0.** We have

$$\begin{aligned}
Amp(y) &= \frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \\
&= \frac{1}{\sqrt{N}} (M a_k + (N-M) b_k) \\
&= \frac{1}{\sqrt{N}} \left[\frac{M}{\sqrt{M}} \sin(2k+1)\theta + \frac{N-M}{\sqrt{N-M}} \cos(2k+1)\theta \right] \\
&= \sqrt{\frac{M}{N}} \sin(2k+1)\theta + \sqrt{1 - \frac{M}{N}} \cos(2k+1)\theta \\
&= \sin\theta \sin(2k+1)\theta + \cos\theta \cos(2k+1)\theta \\
&= \cos(2k\theta)
\end{aligned}$$

We have

$$\Pr(y = 0) = \cos^2(2k\theta)$$

3.2. **Amplified-QFT Analysis: $Py = 0 \bmod N, y \neq 0$.** Using the fact that

$$\sum_{z=0}^{N-1} \omega^{zy} = \frac{1-\omega^{Ny}}{1-\omega^{y}} = 0, w^y \neq 1$$

we have

$$\begin{aligned}
Amp(y) &= \frac{(a_k-b_k)}{\sqrt{N}}\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} + \frac{b_k}{\sqrt{N}}\sum_{z=0}^{N-1}\omega^{zy}\\
&= \frac{(a_k-b_k)}{\sqrt{N}}\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy}\\
&= \frac{(a_k-b_k)}{\sqrt{N}}\omega^{sy}M\\
&= \frac{Mw^{sy}}{\sqrt{NM}}\sin(2k+1)\theta - \frac{Mw^{sy}}{\sqrt{N(N-M)}}\cos(2k+1)\theta\\
&= \omega^{sy}\sqrt{\frac{M}{N}}(\sin(2k+1)\theta - \sqrt{\frac{M/N}{1-M/N}}\cos(2k+1)\theta)\\
&= \omega^{sy}\sqrt{\frac{M}{N}}(\sin(2k+1)\theta - \frac{\sin\theta}{\cos\theta}\cos(2k+1)\theta)\\
&= \omega^{sy}\tan\theta\sin 2k\theta
\end{aligned}$$

We have

$$\Pr(y) = tan^2\theta\sin^2 2k\theta$$

Using $k = \lfloor \frac{\pi}{4\theta} \rfloor \implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - 2\theta \leq 2k\theta \leq \frac{\pi}{2} \implies \sin(\frac{\pi}{2} - 2\theta) \leq \sin 2k\theta \leq 1$ we have

$$\begin{aligned}
\frac{\sin^2\theta}{\cos^2\theta} &\geq \Pr(y) = \tan^2\theta\sin^2 2k\theta \geq \tan^2\theta\sin^2(\frac{\pi}{2}-2\theta)\\
&\implies \frac{M}{N}\frac{1}{1-\frac{M}{N}} \geq \Pr(y) \geq \tan^2\theta\sin^2(\frac{\pi}{2}-2\theta)\\
&\implies \frac{M}{N}(\frac{N}{N-M}) \geq \Pr(y) \geq \frac{\sin^2\theta}{\cos^2\theta}\cos^2 2\theta\\
&\implies \frac{M}{N}(\frac{N}{N-M}) \geq \Pr(y) \geq \frac{\sin^2\theta}{\cos^2\theta}(2\cos^2\theta - 1)^2\\
&\implies \frac{M}{N}(\frac{N}{N-M}) \geq \Pr(y) \geq \frac{M}{N}(\frac{N}{N-M})(1-\frac{2M}{N})^2
\end{aligned}$$

3.3. **Amplified-QFT Analysis:** $Py \neq 0 \bmod N$**.** Making use of the previous results we have

$$\begin{aligned}
Amp(y) &= \frac{(a_k - b_k)}{\sqrt{N}}\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} + \frac{b_k}{\sqrt{N}}\sum_{z=0}^{N-1}\omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}}\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}}\omega^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right] \\
&= \frac{1}{M}\frac{(a_k - b_k)}{\sqrt{N}}\omega^{sy}M\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right] \\
&= \frac{1}{M}\omega^{sy}\tan\theta\sin 2k\theta\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]
\end{aligned}$$

Making use of the following identity

$$|1 - e^{i\theta}|^2 = 4\sin^2(\theta/2)$$

we have

$$\left|\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right|^2 = \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

and so

$$\Pr(y) = \frac{1}{M^2}tan^2\theta\sin^2 2k\theta\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

Using the previous result $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2\theta\sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$ and letting $R = \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$ we have

$$\frac{1}{M^2}\frac{M}{N}(\frac{N}{N-M})R \geq \Pr(y) \geq \frac{1}{M^2}\frac{M}{N}(\frac{N}{N-M})(1-\frac{2M}{N})^2 R \text{ and so}$$
$$\frac{1}{NM}(\frac{N}{N-M})R \geq \Pr(y) \geq \frac{1}{NM}(\frac{N}{N-M})(1-\frac{2M}{N})^2 R$$

We notice that if in addition $MPy = 0 \bmod N$ then $\Pr(y) = 0$.

3.4. **Amplified-QFT Summary.** The probability $\Pr(y)$ is given exactly by

$$\left\{\begin{array}{lll}
\cos^2 2k\theta & \text{if} & y = 0 \\
tan^2\theta\sin^2 2k\theta & \text{if} & Py = 0 \bmod N, y \neq 0 \\
\frac{1}{M^2}tan^2\theta\sin^2 2k\theta\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py \neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\
0 & \text{if} & Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise}
\end{array}\right\}$$

4. **Applying the QFT to the Oracle.**

In this section we just apply the QFT to the binary Oracle f, which is 1 on A and 0 elsewhere.

We begin with the following state

$$|\xi >= \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}|z> \otimes \frac{1}{\sqrt{2}}(|0> - |1>)$$

and apply the unitary transform for f, U_f , to this state which performs the following action:

$$U_f|z>|c>=|z>|c\oplus f(z)>$$

to get the state $|\psi>$

$$\begin{aligned}
|\psi >&= U_f\frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}|z> \frac{1}{\sqrt{2}}(|0> - |1>)\\
&= \frac{1}{\sqrt{N}}\left[(-1)\sum_{z\in A}|z> + \sum_{z\notin A}|z>\right]\frac{1}{\sqrt{2}}(|0> - |1>)\\
&= \frac{1}{\sqrt{N}}\left[(-2)\sum_{z\in A}|z> + \sum_{z=0}^{N-1}|z>\right]\frac{1}{\sqrt{2}}(|0> - |1>)
\end{aligned}$$

Next we apply the QFT to try to find the period P, dropping $\frac{1}{\sqrt{2}}(|0> - |1>)$. The QFT applies the following action:

$$|z>\to \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\omega^{zy}|y>$$

to get

$$|\phi >= \sum_{y=0}^{N-1}\left[\frac{(-2)}{N}\sum_{z\in A}\omega^{zy} + \frac{1}{N}\sum_{z=0}^{N-1}\omega^{zy}\right]|y>$$

4.1. **QFT Analysis:** $y = 0$. We have

$$\begin{aligned}
Amp(y) &= \frac{(-2)}{N}\sum_{z\in A}\omega^{zy} + \frac{1}{N}\sum_{z=0}^{N-1}\omega^{zy}\\
&= \frac{(-2)M}{N} + \frac{N}{N}\\
&= 1 - \frac{2M}{N}
\end{aligned}$$

Therefore, in the QFT case, we have $\Pr(y = 0)$ is very close to 1 and is given by

$$\Pr(y=0) = 1 - \frac{4M}{N} + 4\frac{M^2}{N^2} = \left(1 - \frac{2M}{N}\right)^2$$

whereas in the Amplified-QFT case we have $\Pr(y=0)$ is given by

$$\Pr(y=0) = \cos^2 2k\theta$$

4.2. **QFT Analysis:** $Py = 0 \bmod N, y \neq 0$**.** Using the fact that

$$\sum_{z=0}^{N-1} \omega^{zy} = \frac{1-\omega^{Ny}}{1-\omega^{y}} = 0$$

we have

$$\begin{aligned} Amp(y) = & \ \frac{-2}{N}\sum_{z\in A}\omega^{zy} + \frac{1}{N}\sum_{z=0}^{N-1}\omega^{zy} \\ &= \frac{-2}{N}\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} \\ &= \frac{-2M}{N}\omega^{sy} \end{aligned}$$

Therefore in the QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = 4\frac{M^2}{N^2}$$

whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = tan^2\theta \sin^2 2k\theta$$

We can determine how the increase in amplitude varies with the number of iterations k of the Grover step in the Amplified-QFT by examining the ratio of the amplitudes of the Amplified-QFT case and QFT case. This ratio is given exactly by

$$\begin{aligned} AmpRatio(y) &= \frac{\frac{(a_k-b_k)}{\sqrt{N}}\omega^{sy}M}{\frac{-2M}{N}\omega^{sy}} \\ &= \frac{(a_k-b_k)}{-2}\sqrt{N} \\ &= \frac{1}{-2}\left[\sqrt{\frac{N}{M}}\sin(2k+1)\theta - \sqrt{\frac{N}{N-M}}\cos(2k+1)\theta\right] \\ &= \frac{N}{-2M}\tan\theta\sin 2k\theta \end{aligned}$$

Using $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2\theta\sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$, we have the following inequality for the $\Pr Ratio(y)$, the increase in the probability due to amplification:

$$\begin{aligned} \frac{N}{4M}(\frac{N}{N-M}) \geq \Pr Ratio(y) \geq \frac{N}{4M}(\frac{N}{N-M})(1-\frac{2M}{N})^2 \\ \implies \Pr Ratio(y) \approx \frac{N}{4M} \end{aligned}$$

4.3. **QFT Analysis:** $Py \neq 0 \bmod N$**.** We have

$$\begin{aligned}
Amp(y) = &\ \frac{-2}{N}\sum_{z\in A}\omega^{zy} + \frac{1}{N}\sum_{z=0}^{N-1}\omega^{zy} \\
= &\ \frac{-2}{N}w^{sy}\sum_{r=0}^{M-1}\omega^{rPy} \\
= &\ \frac{-2}{N}w^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right] \\
= &\ \frac{-2}{N}w^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]
\end{aligned}$$

Once again, making use of the following identity

$$|1-e^{i\theta}|^2 = 4\sin^2(\theta/2)$$

in the QFT case, we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{4}{N^2}\left[\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}\right]$$

whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{1}{M^2}tan^2\theta\sin^2 2k\theta\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

We notice that if in addition $MPy = 0 \bmod N$ then $\Pr(y) = 0$.
The ratio of the amplitudes of the Amplified-QFT case and QFT case is given exactly by

$$\begin{aligned}
AmpRatio(y) = &\ \frac{\frac{(a_k-b_k)}{\sqrt{N}}\omega^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]}{\frac{-2}{N}w^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]} \\
= &\ \frac{(a_k-b_k)}{-2}\sqrt{N} \\
= &\ \frac{1}{-2}\left[\sqrt{\frac{N}{M}}\sin(2k+1)\theta - \sqrt{\frac{N}{N-M}}\cos(2k+1)\theta\right] \\
= &\ \frac{N}{-2M}\tan\theta\sin 2k\theta
\end{aligned}$$

We note that this ratio is the same as in that given in the previous section and is independent of y. The variables in this ratio do not depend in anyway on the QFT.

As in the previous section, we have the following inequality for the $\Pr Ratio(y)$, the increase in the probability due to amplification when $k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2\theta\sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\frac{N}{4M}(\frac{N}{N-M}) \geq \Pr Ratio(y) \geq \frac{N}{4M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$
$$\Longrightarrow \Pr Ratio(y) \approx \frac{N}{4M}$$

4.4. **QFT Summary.** The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{lll} \left(1-\frac{2M}{N}\right)^2 & \text{if} & y=0 \\ 4\frac{M^2}{N^2} & \text{if} & Py = 0 \bmod N, y \neq 0 \\ \frac{4}{N^2}\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py \neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\ 0 & \text{if} & Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise} \end{array} \right\}$$

5. Applying the QHS to the Oracle

The Quantum Hidden Subgroup algorithm (QHS) algorithm is a two register algorithm as follows (see ref[13] for details). We begin with $|0>|0>$ where the first register is n qubits and the second register is 1 qubit and apply the Hadamard transform to the first register to get a uniform superposition state, followed by the unitary transformation for the Oracle f to get:

$$|\psi>= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x>|f(x)>$$

Next we apply the QFT to the first register to get

$$\begin{aligned} |\psi> &= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\omega^{xy}|y>|f(x)> \\ &= \sum_{y=0}^{N-1}\frac{1}{N}\sum_{x=0}^{N-1}\omega^{xy}|y>|f(x)> \\ &= \sum_{y=0}^{N-1}\frac{1}{N}|y>\sum_{x=0}^{N-1}\omega^{xy}|f(x)> \\ &= \sum_{y=0}^{N-1}\frac{|||\Gamma(y)>||}{N}|y>\frac{|\Gamma(y)>}{|||\Gamma(y)>||} \end{aligned}$$

where

$$\begin{aligned} |\Gamma(y)> &= \sum_{x=0}^{N-1}\omega^{xy}|f(x)> \\ &= \sum_{x\in A}\omega^{xy}|1> + \sum_{x\notin A}\omega^{xy}|0> \end{aligned}$$

and where

$$|||\Gamma(y)>||^2 = \left|\sum_{x\in A}\omega^{xy}\right|^2 + \left|\sum_{x\notin A}\omega^{xy}\right|^2$$

Next we make a measurement to get y and find that the probability of this measurement is

$$\begin{aligned}\Pr(y) &= \frac{|||\Gamma(y)>||^2}{N^2} \\ &= \frac{1}{N^2}\left|\sum_{x\in A}\omega^{xy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2\end{aligned}$$

The state that we end up in is of the form

$$|\phi>=|y>\frac{|\Gamma(y)>}{|||\Gamma(y)>||}$$

So now we are interested in the probability of measuring y in the usual cases in order to recover the period P.

5.1. **QHS Analysis:** $y = 0$**.** We have

$$\begin{aligned}\Pr(y) &= \frac{1}{N^2}\left|\sum_{x\in A}\omega^{xy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2 \\ &= \frac{M^2}{N^2} + \frac{(N-M)^2}{N^2} = \frac{M^2+N^2-2NM+M^2}{N^2} \\ &= 1 - \frac{2M(N-M)}{N^2}\end{aligned}$$

whereas in the Amplified-QFT case we have $\Pr(y = 0)$ is given by

$$\Pr(y=0) = \cos^2 2k\theta$$

5.2. **QHS Analysis:** $Py = 0 \bmod N, y \neq 0$**.** We have

$$\begin{aligned}\Pr(y) &= \frac{1}{N^2}\left|\sum_{x\in A}\omega^{xy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2 \\ &= \frac{1}{N^2}\left|\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2 \\ &= \frac{1}{N^2}\left|\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy}\right|^2 + \frac{1}{N^2}\left|-\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} + \frac{1}{N}\sum_{x=0}^{N-1}\omega^{xy}\right|^2 \\ &= \frac{2M^2}{N^2}\end{aligned}$$

where we have used the fact that

$$\sum_{x=0}^{N-1}\omega^{xy} = 0$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = tan^2\theta \sin^2 2k\theta$$

By comparing the results of the QHS and the Amplified-QFT algorithms we have the following inequality for the $\Pr Ratio(y) = \Pr(y)_{Amplified-QFT} / \Pr(y)_{QHS}$, the increase in the probability due to amplification when $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2\theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \Pr Ratio(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$
$$\Longrightarrow \Pr Ratio(y) \approx \frac{N}{2M}$$

5.3. **QHS Analysis:** $Py \neq 0 \bmod N$**.** We have

$$\begin{aligned}
\Pr(y) &= \frac{1}{N^2}\left|\sum_{x\in A}\omega^{xy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2 \\
&= \frac{1}{N^2}\left|\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy}\right|^2 + \frac{1}{N^2}\left|\sum_{x\notin A}\omega^{xy}\right|^2 \\
&= \frac{1}{N^2}\left|\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy}\right|^2 + \frac{1}{N^2}\left|-\omega^{sy}\sum_{r=0}^{M-1}\omega^{rPy} + \frac{1}{N}\sum_{x=0}^{N-1}\omega^{xy}\right|^2 \\
&= \frac{1}{N^2}\left|\omega^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]\right|^2 + \frac{1}{N^2}\left|-\omega^{sy}\left[\frac{1-\omega^{MPy}}{1-\omega^{Py}}\right]\right|^2 \\
&= \frac{2}{N^2}\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}
\end{aligned}$$

where we have used the fact that

$$\sum_{x=0}^{N-1}\omega^{xy} = 0$$

and that

$$|1-e^{i\theta}|^2 = 4\sin^2(\theta/2)$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{1}{M^2} tan^2\theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

We notice that if in addition $MPy = 0 \bmod N$ then $\Pr(y) = 0$.

By comparing the results of the QHS and the Amplified-QFT algorithms we have the following inequality for the $\Pr Ratio(y) = \Pr(y)_{Amplified-QFT} / \Pr(y)_{QHS}$, the increase in the probability due to amplification when $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2\theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \Pr Ratio(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1-\frac{2M}{N})^2$$
$$\Longrightarrow \Pr Ratio(y) \approx \frac{N}{2M}$$

5.4. **QHS Summary.** The $\Pr(y)$ in the QHS case is:

$$\left\{ \begin{array}{lll} 1-\frac{2M(N-M)}{N^2} & \text{if} & y=0 \\ \frac{2M^2}{N^2} & \text{if} & Py=0 \bmod N, y\neq 0 \\ \frac{2}{N^2}\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if} & Py\neq 0 \bmod N \text{and } MPy \neq 0 \bmod N \\ 0 & \text{if} & Py\neq 0 \bmod N \text{ and } MPy = 0 \bmod N \text{ otherwise} \end{array} \right\}$$

6. Recovering the Period P from an Observation y

As in Shor's algorithm, we use the continued fraction expansion of y/N to find the period P,where y is a measured value such that y/N is close to d/P and $(d,P)=1$. See ref[2] and ref[3]for details which we provide below.

Let$\{a\}_N$ be the residue of $a \bmod N$ of smallest magnitude such that $-N/2 < \{a\}_N < N/2$. Let $S_N = \{0,1,...,N-1\}$, $S_P = \{d \in S_N : 0 \leq d < P\}$ and $Y = \{y \in S_N : |Py| \leq P/2\}$. Then the map $Y \to S_P$ given by $y \to d = d(y) = round(Py/N)$ with inverse $y = y(d) = round(Nd/P)$ is a bijection and $\{Py\}_N = Py - Nd(y)$. In addition the following two sets are in 1-1 correspondence $\{y/N : y \in Y\}$ and $\{d/P : 0 \leq d < P\}$.

We make use of the following theorem from the theory of continued fractions ref[5] (Theorem 184 p.153):

Theorem 1. *Let x be a real number and let a and b be integers with $b > 0$. If $|x - \frac{a}{b}| \leq \frac{1}{2b^2}$ then the rational a/b is a convergent of the continued fraction expansion of x.*

Corollary 1. *If $P^2 \leq N$ and $|\{Py\}_N| \leq \frac{P}{2}$ then $d(y)/P$ is a convergent of the continued fraction expansion of y/N.*

Proof. Since $\{Py\}_N = Py - Nd(y)$ we have
$|Py - Nd(y)| \leq \frac{P}{2}$ or
$|\frac{y}{N} - \frac{d(y)}{P}| \leq \frac{1}{2N} \leq \frac{1}{2P^2}$
and we can apply Theorem 1 so that d/P is a convergent of the continued fraction expansion of y/N. □

Since we know y and N we can find the continued fraction expansion of y/N. However we also need that $(d,P)=1$ in order that d/P is a convergent and enabling us to read off P directly. The probability that $(d,P)=1$ is $\varphi(P)/P$ where $\varphi(P)$ is Euler's totient function. If P is prime we get $(d,P)=1$ trivially.

By making use of the following Theorem it can be shown that $\frac{\varphi(P)}{P} \geq \frac{e^{-\gamma}-\epsilon(P)}{\ln 2}\frac{1}{\ln\ln N}$, where $\epsilon(P)$ is a monotone decreasing sequence converging to zero.

Theorem 2. $\liminf \frac{\varphi(N)}{N/\ln\ln N} = e^{-\gamma}$

where $\gamma = 0.57721566$ is Euler's constant and where $e^{-\gamma} = 0.5614594836$.

This may cause us to repeat the experiment $\Omega(\frac{1}{\ln \ln N})$ times in order to get $(d, P) = 1$.

We note that we needed to add a condition on the period P that $P^2 \leq N$ or $P \leq \sqrt{N}$ in order for the proof of the corollary to work.

6.1. **Testing if $P_1 = P$ when s is known or is 0.** We can easily test if $s = 0$ by checking to see if $f(0) = 1$.

Now given a putative value of the period P_1 and a known offset or shift s, how can we test whether $P_1 = P$?

Assuming we have access to the Oracle to test individual values, we can confirm $f(s) = 1$ since s is known. We will show that if $f(s+P_1) = 1$ and $f(s+(M-1)P_1) = 1$ then $P_1 = P$.

Case 1: If $P_1 > P$ then $s + (M-1)P_1 > s + (M-1)P$. But $s + (M-1)P$ is the largest index x such that $f(x) = 1$. Therefore if $P_1 > P$ we must have $f(s + (M-1)P_1) = 0$.

Case 2: If $0 < P_1 < P$ then $s < s + P_1 < s + P$ but between s and P there are no other values x such that $f(x) = 1$.Therefore if $0 < P_1 < P$ we must have $f(s + P_1) = 0$.

Therefore if $f(s) = 1, f(s + P_1) = 1$ and $f(s + (M-1)P_1) = 1$ we must have $P_1 = P$.

6.2. **Testing if $(s_1, P_1) = (s, P)$ when s is from a small known set and $s \neq 0$.** If we assume s is unknown and $s \neq 0$ but is from a small known set of possible values such that we can exhaust over this set on a classical computer and we are given a putative value of the period P_1, how can we test whether a pair of values (s_1, P_1) is the correct pair (s, P) ?

We need only test whether $f(s_1) = 1$, $f(s_1 + P_1) = 1$ and $f(s_1 + (M-1)P_1) = 1$ where M is assumed known.

Case 1: If $s_1 < s$ then $f(s_1) = 0$ since s is the smallest index x with $f(x) = 1$.

Case 2: If $s_1 > s$ and $f(s_1) = 1$ then $s_1 = s + rP$ with $r > 0$. If $f(s_1 + P_1) = 1$ then $s_1 + P_1 = s + tP = s_1 + (t-r)P$ with $t > r > 0$. Hence $P_1 = (t-r)P > 0$. If $f(s_1+(M-1)P_1) = 1$ then $s_1+(M-1)P_1 = s+rP+(M-1)(t-r)P > s+(M-1)P$ which is the largest index x with $f(x) = 1$. Therefore $f(s_1 + (M-1)P_1) = 0$.

Hence if $f(s_1) = 1$, $f(s_1 + P_1) = 1$ and $f(s_1 + (M-1)P_1) = 1$ we must have $s_1 = s$ and then by following the case when s is known we must also have $P_1 = P$.

Therefore if one or more of the values $f(s_1)$, $f(s_1 + P_1)$, $f(s_1 + (M-1)P_1)$ is zero, either s_1 or P_1 is wrong. For a given P_1 we must exhaust over all possible values of s before we can be sure that $P_1 \neq P$. For in the case that $P_1 \neq P$, we will have for every possible s_1 that at least one of the values $f(s_1)$, $f(s_1 + P_1)$, $f(s_1 + (M-1)P_1)$ is zero. In such a case we must try another putative P_1.

6.3. **Finding $s \neq 0$ using a Quantum Computer.** We can assume $s \neq 0$ as the case $s = 0$ is trivial and was considered above. Let $s = \alpha + \beta P$ where $\alpha = s \bmod P$ so that $0 \leq \alpha \leq P - 1$ and $0 \leq \alpha + \beta P + (M-1)P \leq N - 1$.

We assume we are given the correct value of P. If P is wrong, it will be detected in the algorithm.

Step 1:

We create an initial superposition on N values

$$|\psi_1>=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x>$$

and apply the Oracle f and put this into the amplitude. We then apply Grover without measurement to amplify the amplitudes and we have the following state

$$|\psi_1>=a_k\sum_{\times\in A}|x>+b_k\sum_{x\notin A}|x>$$

where

$$a_k=\frac{1}{\sqrt{M}}\sin(2k+1)\theta, b_k=\frac{1}{\sqrt{N-M}}\cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin\theta=\sqrt{M/N}, \cos\theta=\sqrt{1-M/N}$$

Next we measure the register and with probability exceeding $1-M/N$ we will measure a value $x_1\in A$ where $x_1=s+r_1P$ with $0\leq r_1\leq M-1$. Note that the total probability of the set A is given by

$$\Pr(x\in A)=M(\frac{1}{\sqrt{M}}\sin(2k+1)\theta)^2=\sin^2(2k+1)\theta=1-\cos^2(2k+1)\theta$$

$$\Longrightarrow \Pr(x\in A)=\sin^2(2k+1)\theta\geq 1-\frac{M}{N}$$

Now using our measured value $x_1=s+r_1P$ with $0\leq r_1\leq M-1$ we check that $f(x_1)=1$ and $f(x_1-P)=1$. If $f(x_1-P)=0$ then either the value of P we are using is wrong or we have $r_1=0$ and $x_1=s$. If we test $f(s)=1$, $f(s+P)=1$ and $f(s+(M-1)P)=1$ then we have the correct P and s otherwise P is wrong. So assuming $f(x_1-P)=1$ we must have either the correct P or a multiple of P. We can use the procedure in Step 2 or Step 2' to find s. The method in Step 2 uses the Exact Quantum Counting algorithm to find s (See ref[11] for details). The method in Step 2' uses a method of decreasing sequence of measurements to find s.

Step 2 (using the Exact Quantum Counting algorithm):

Let T be such that $T\geq M$ is the smallest power of 2 greater than M. We form a superposition

$$|\varphi_1>=\frac{1}{\sqrt{T}}\sum_{x=0}^{T-1}|x>|0>$$

and apply the function $g(x)=Max(0,x_1-(x+1)P)$ where $x_1=s+r_1P$ is our measured value, with $0\leq r_1\leq M-1$and put the values of $g(x)$ into the second register to get

$$|\varphi_2>=\frac{1}{\sqrt{T}}\sum_{x=0}^{T-1}|x>|g(x)>$$

Notice that as x increases from 0, $g(x)$ is a decreasing sequence $s + rP$ with $r = (r_1 - x - 1)$. When $g(x)$ dips below 0 we set $g(x) = 0$ to ensure $g(x) \geq 0$. Now we apply f to $g(x)$ and put the results into the amplitude to get

$$|\varphi_3 >= \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} (-1)^{f(g(x))} |x > |g(x) >$$

Notice that $f(g(x)) = 1$ when $s \leq g(x) < s + r_1 P$ and is 0 elsewhere. We apply the exact quantum counting algorithm which determines how many values $f(g(x)) = 1$.Let this total be R. If P is correct we expect $R = r_1$ and we can determine $s = x_1 - RP = s + r_1 P - RP$. We can then test if we have the correct pair of values s, P by testing whether $f(s) = 1$, $f(s + P) = 1$ and $f(s + (M - 1)P) = 1$. If this test fails then P must be an incorrect value and we must repeat the period finding algorithm.

We use Theorem 8.3.4 of ref[11]: The Exact Quantum Counting algorithm requires an expected number of applications of U_f in $O(\sqrt{(R+1)(T-R+1)}$ and outputs the correct value R with probability at least $2/3$.

Step 2' (decreasing sequence of measurements method):

Let T be such that $T \geq M$ is the smallest power of 2 greater than M. We form a superposition

$$|\varphi_1 >= \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x > |0 >$$

and apply the function $g(x) = Max(0, x_1 - (x + 1)P)$ where $x_1 = s + r_1 P$ with $0 \leq r_1 \leq M - 1$and put these values into the second register to get

$$|\varphi_2 >= \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x > |g(x) >$$

Notice that as x increases from 0, $g(x)$ is a decreasing sequence $s + rP$ with $r = (r_1 - x - 1)$. When $g(x)$ dips below 0 we set $g(x) = 0$ to ensure $g(x) \geq 0$. Now we apply f to $g(x)$ and put the results into the third register and then into the amplitude.

$$|\varphi_3 >= \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} (-1)^{f(g(x))} |x > |g(x) >$$

Notice that $f(g(x)) = 1$ when $s \leq g(x) < s + r_1 P$ and is 0 elsewhere.

We then run Grover without measurement to amplify the amplitudes and measure the second register containing $g(x)$.

With probability close to 1 we will measure a new value $x_2 = s + r_2 P$ with $0 \leq r_2 < r_1$. We test the values $f(x_2) = 1$ and $f(x_2 - P) = 1$. If $f(x_2 - P) = 0$ then either the value of P we are using is wrong or we have $r_2 = 0$ and $x_2 = s$. If we test $f(s) = 1$, $f(s + P) = 1$ and $f(s + (M - 1)P) = 1$ then we have the correct P and s otherwise P is wrong. So assuming $f(x_2 - P) = 1$ we must have either the correct P or a multiple of P. We repeat this algorithm and go to Step 2' replacing the value x_1 in the function $g(x)$ with x_2 etc. As we repeat the algorithm we will measure a decreasing sequence of values $x_1, x_2 ...$ that converges to s. This procedure will eventually terminate with the correct pair of values P and s or we will determine that we have been using an incorrect value of P and we must repeat the quantum algorithm for finding putative P and repeat the process.

How many times do we expect to repeat Step 2'? When we make our first measurement we expect $r_1 = M/2$. For our second measurement we expect $r_2 = r_1/2$ etc. Therefore we expect to repeat this algorithm $O(\ln_2(M))$ times.

7. Replacing the QFT With a General Unitary Transform U

In general, if we had any Oracle f which is 1 on a set of labels A and 0 elsewhere and we replaced the QFT with any unitary transform U which performs the following

$$|z> \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \alpha(z,y)|y>$$

we can compute the $AmpRatio(y) = \frac{Amplitude(Amplified-U)}{Amplitude(U)}$ as follows.
As before, we have the following state after applying U_f:

$$|\psi> = \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in A} |z> + \sum_{z=0}^{N-1} |z> \right]$$

Next we apply the general unitary transform U to obtain the state

$$U|\psi> = \sum_{y=0}^{N-1} \left[\frac{(-2)}{N} \sum_{z \in A} \alpha(z,y) + \frac{1}{N} \sum_{z=0}^{N-1} \alpha(z,y) \right] |y>$$

In the Amplified-U case we apply Grover without measurement followed by U we obtain the state

$$|\phi_k> = \sum_{y=0}^{N-1} \left[\frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \alpha(z,y) + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \alpha(z,y) \right] |y>$$

If $\sum_{z=0}^{N-1} \alpha(z,y) = 0$ and $\sum_{z \in A} \alpha(z,y) \neq 0$ we get the same $AmpRatio(y)$ formula that we obtained when $U = QFT$

$$
\begin{aligned}
AmpRatio(y) &= \frac{\frac{(a_k-b_k)}{\sqrt{N}}\sum_{z\in A}\alpha(z,y)+\frac{b_k}{\sqrt{N}}\sum_{z=0}^{N-1}\alpha(z,y)}{\frac{(-2)}{N}\sum_{z\in A}\alpha(z,y)+\frac{1}{N}\sum_{z=0}^{N-1}\alpha(z,y)}\\
&= \frac{\frac{(a_k-b_k)}{\sqrt{N}}\sum_{z\in A}\alpha(z,y)}{\frac{(-2)}{N}\sum_{z\in A}\alpha(z,y)}\\
&= \frac{\frac{(a_k-b_k)}{\sqrt{N}}}{\frac{(-2)}{N}}\\
&= \frac{(a_k-b_k)}{-2}\sqrt{N}\\
&= \frac{1}{-2}\left[\sqrt{\frac{N}{M}}\sin(2k+1)\theta-\sqrt{\frac{N}{N-M}}\cos(2k+1)\theta\right]\\
&= \frac{N}{-2M}\tan\theta\sin 2k\theta
\end{aligned}
$$

This gives

$$
\Pr Ratio(y) = \frac{N^2}{4M^2}\tan^2\theta\sin^2 2k\theta
$$

As in the case when U=QFT, we have the following inequality for the $\Pr Ratio(y)$ for a general U, the increase in the probability due to amplification when $k=\lfloor\frac{\pi}{4\theta}\rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M})\geq\tan^2\theta\sin^2 2k\theta\geq\frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$
\begin{aligned}
\frac{N}{4M}(\frac{N}{N-M}) \geq \Pr Ratio(y) &\geq \frac{N}{4M}(\frac{N}{N-M})(1-\frac{2M}{N})^2\\
\Longrightarrow \Pr Ratio(y) &\approx \frac{N}{4M}
\end{aligned}
$$

References

[1] Nakahara and Ohmi, “Quantum Computing: From Linear Algebra to Physical Realizations”, CRC Press (2008).

[2] S. Lomonaco, “Shor’s Quantum Factoring Algorithm,” AMS PSAPM, vol. 58, (2002), 161-179.

[3] P. Shor, “Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM J. on Computing, 26(5) (1997) pp1484-1509 (quant-ph/9508027).

[4] L. Grover, “A fast quantum mechanical search algorithm for database search”, Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996), (1996) 212-219.

[5] Hardy and Wright “An Introduction to the Theory of Numbers”, Oxford Press Fifth Edition (1979).

[6] S. Lomonaco and L. Kauffman, “Quantum Hidden Subgroup Algorithms: A Mathematical Perspective,” AMS CONM, vol. 305, (2002), 139-202.

[7] S. Lomonaco, “Grover’s Quantum Search Algorithm,” AMS PSAPM, vol. 58, (2002), 181-192.

[8] S. Lomonaco and L. Kauffman, “Is Grover’s Algorithm a Quantum Hidden Subgroup Algorithm?,” Journal of Quantum Information Processing, Vol. 6, No. 6, (2007), 461-476.

[9] G. Brassard, P. Hoyer, M. Mosca and A. Tapp, ”Quantum Amplitude Amplification and Estimation”, AMS CONM, vol 305, (2002), 53-74.

[10] M. Nielsen and I. Chuang, ”Quantum Computation and Quantum Information”, Cambridge University Press (2000).

[11] P. Kaye, R. Laflamme and M. Mosca, ”An Introduction to Quantum Computing”, Oxford University Press (2007).

[12] N. Yanofsky and M. Mannucci, ”Quantum Computing For Computer Scientists”, Cambridge University Press (2008).

[13] S. Lomonaco, ”A Lecture on Shor’s Quantum Factoring Algorithm Version 1.1”,quant-ph/0010034v1 9 Oct 2000.

Current address: David J. Cornwell (PhD Student), Department of Mathematics, University of Maryland Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250

E-mail address: `David J. Cornwell: dave.cornwell@yahoo.com`