The amplified quantum Fourier transform: solving the local period problem

David J. Cornwell

Abstract This paper creates and analyzes a new quantum algorithm called the Amplified Quantum Fourier Transform (QFT) for solving the following problem:

The Local Period Problem: Let $L = \{0, 1 \ldots N - 1\}$ 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

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

where $P \leq \sqrt{N}$ and $M \ll N$, and where $M$ is assumed known. Given an oracle $f : L \rightarrow \{0, 1\}$ which is 1 on $A$ and 0 elsewhere, find the local period $P$ and the offset $s$.

The first part of this paper defines the Amplified QFT algorithm. The second part of the paper summarizes the main results and compares the new algorithm against the QFT and QHS algorithms when solving the local period problem. It is shown that the new algorithm is, on average, quadratically faster than both the QFT and QHS algorithms.

Keywords Quantum algorithms · Quantum Fourier transform · Amplification · Shor algorithm · Grover algorithm · Oracle · Period finding

Mathematics Subject Classification (2000) Primary: 05C38 · 15A15; Secondary: 05A15 · 15A18

D. J. Cornwell (✉)
Department of Mathematics, University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD, USA
e-mail: dave.cornwell@yahoo.com
1 Introduction

This paper creates and analyzes a new quantum algorithm called the Amplified Quantum Fourier Transform (Amplified-QFT) for solving the following problem:

The Local Period Problem: Let \( L = \{0, 1 \ldots N - 1\} \) 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 \( A = \{j : j = s + rP, r = 0, 1 \ldots M - 1\} \) where \( P \leq \sqrt{N} \) and \( M \ll N \), and where \( M \) is assumed known. Given an oracle \( f : L \rightarrow \{0, 1\} \) which is 1 on \( A \) and 0 elsewhere, find the local period \( P \). A separate algorithm finds the offset \( s \).

The first part of this paper defines the Amplified-QFT algorithm. The second part of the paper summarizes the main results and compares the Amplified-QFT algorithm against the QFT and Quantum Hidden Subgroup (QHS) algorithms when solving the local period problem. It is shown that the Amplified-QFT algorithm is, on average, quadratically faster than both the QFT and QHS algorithms. The third part of the paper provides the detailed proofs of the main results, describes the method of recovering \( P \) from an observation \( y \) and describes the algorithm for finding the offset \( s \).

2 Background-amplitude amplification

In Ref. [1] Lov Grover specified a quantum search algorithm that searched for a single marked element \( x0 \) in an \( N \) long list \( L \). An oracle \( f : L \rightarrow \{0, 1\} \) is used to mark the element such that \( f(x0) = 1 \) and \( f \) is 0 elsewhere. Grover’s quantum algorithm finds the element with a work factor of \( O(\sqrt{N}) \) whereas on a classical computer this would take \( O(N) \), thereby obtaining a quadratic speedup. Grover’s algorithm can be summarized as follows:

(a) Initialize the state to be the uniform superposition state \( |\psi\rangle = H|0\rangle \) where \( H \) is the Hadamard transform.
(b) Reflect the current state about the plane orthogonal to the state \( |x0\rangle \) by using the operator \( (I - 2|x0\rangle \langle x0|) \).
(c) Reflect the new state back around \( |\psi\rangle \) by using the operator \( (2|\psi\rangle \langle \psi| - I) \). This operator is a reflection about the average of the amplitudes of the new state.
(d) Repeat steps (b) and (c) \( O(\sqrt{N}) \) times until most of the probability is on \( |x0\rangle \).
(e) Measure the resulting state to obtain \( x0 \).

Also in Ref. [1], Grover suggested this algorithm could be extended to the case of searching for an element in a subset \( A \) of \( M \) marked elements in an \( N \) long list \( L \). Once again an oracle \( f : L \rightarrow \{0, 1\} \) is used to mark the elements of the subset \( A \). Grover’s algorithm solves this problem with a work factor of \( O(\sqrt{N/M}) \). The elements of the set \( A \) are sometimes referred to as “good” and the elements not in \( A \) are called “bad”. Grover’s algorithm for this problem can be summarized as follows:

(a) Initialize the state to be the uniform superposition state \( |\psi\rangle = H|0\rangle \) where \( H \) is the Hadamard transform.
(b) Reflect the current state about the plane orthogonal to the state \( |xgood\rangle \) by using the operator \( (I - 2|xgood\rangle \langle xgood|) \), where \( xgood \) is the normalized sum of the