A Quantum Algorithm Detecting Concentrated Maps

April 23, 2004

Isabel Beichl, Stephen Bullock, and Daegene Song

Mathematical and Computational Sciences Division,
National Institute of Standards and Technology, Gaithersburg, MD 20899-8910
Correspondence: Stephen.Bullock@nist.gov

Abstract

We consider an arbitrary mapping $f : \{0, ..., N-1\} \rightarrow \{0, ..., N-1\}$ for $N = 2^n$, n some number of quantum bits. Using N calls to a classical oracle evaluating $f(x)$ and an N-bit memory, it is possible to determine whether $f(x)$ is one-to-one. For some radian angle $0 \leq \theta \leq \pi/2$, we say $f(x)$ is *θ-concentrated* iff $\mathrm{e}^{2\pi i f(x)/N} \subset \mathrm{e}^{i[\psi_0 - \theta, \psi_0 + \theta]}$ for some given ψ_0 and any $0 \leq x \leq N-1$. This manuscript presents a quantum algorithm that distinguishes a θ-concentrated $f(x)$ from a one-to-one $f(x)$ in $O(1)$ calls to a quantum oracle function U_f with high probability. For $0 < \theta < 0.3301$rad, the quantum algorithm outperforms the obvious classical algorithm on average, with maximal outperformance at $\theta = \frac{1}{2} \sin^{-1} \frac{1}{\pi} \approx 0.1620$rad. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant $f(x)$.

1 Introduction and Context

In recent years, much progress has been made in the study of quantum computation [4, 6]. In 1985, David Deutsch illustrated the early implication of computational speed-up of quantum algorithms [2]. Deutsch considers a mapping with two inputs and two outputs. Using quantum superposition, he shows that a single call to a quantum oracle allows one to determine whether such a function is one-to-one, in comparison to two classical evaluations of the function. Several years later, Deutsch and Jozsa generalized the algorithm to allow for multiple inputs and two outputs[3] [6, §1.4.4]. Specifically, they describe a multi-argument function as balanced if its image holds two elements and the preimage of each is the same size. Deutsch and Jozsa's algorithm then distinguishes between a constant and balanced function using a single quantum oracle call. Further generalizations [1] distinguish between functions which are constant and map onto the set of ℓ^{th}-roots of unity, $2 \leq \ell < N$.

This note presents a variant of such algorithms. Specifically, suppose that given is a function $f : \{0, 1, 2, \ldots, N-1\} \to \{0, 1, \ldots, N-1\}$, where $N = 2^n$ is a power of two. This is convenient as $N = 2^n$ is the dimension of the data-state space of n-quantum bits [6]. Let $\omega = \mathrm{e}^{2\pi/N}$ be the $(2^n)^{\text{th}}$ root of unity, and choose $\psi_0 \in [0, 2\pi)$. We say such an $f(x)$ is *θ-concentrated* about ψ_0 if and only if

$$\omega^{f(x)} \in \exp(i[\psi_0 - \theta, \psi_0 + \theta]), \quad \forall\ 0 \leq x \leq N-1 \tag{1}$$

We say $f(x)$ is θ-concentrated iff there exists a ψ_0 so that Equation 1 holds. Using $N-1$ bits and N evaluations of the function (classical oracle calls,) we may determine with certainty whether $f(x)$ is one-to-one. Suppose instead one has a quantum oracle U_f encoding an $f(x)$ which is known to be either constant or concentrated. We here present an algorithm which uses $O(1)$ calls to U_f to distinguish between these cases, with arbitrarily high probability.

To describe U_f, we breifly review quantum data spaces; cf. [6, 5]. The state of a string of quantum bits is encoded as a vector (ket) in a complex Hilbert space, say $|\psi\rangle \in \mathcal{H}$. For qubit-states, the usual convention is that the one-qubit state space is $\mathcal{H}_1 = \mathrm{span}_{\mathbb{C}}\{|0\rangle, |1\rangle\}$ carrying the usual Hermitian inner product. The n-qubit state space is then the $N = 2^n$ tensor (Kronecker) product

$$\mathcal{H}_n = \mathrm{span}_{\mathbb{C}}\{|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle\ ;\ b_j \in \mathbb{F}_2 = \{0, 1\}, 1 \leq j \leq n\} \tag{2}$$

The abbreviation $|b_1 b_2 \ldots b_n\rangle$ for $|b_1\rangle \otimes |b_2\rangle \otimes \cdots |b_n\rangle$ is typical, and the Hermitian inner product is that induced by the tensor structure. At times, we further abbreviate the bit-string $b_1 b_2 \ldots b_n$ within the ket by the associated integer, i.e. the binary expansion. Explicit description of the oracle also makes it simpler to take $2n$ to be our number of quantum bits. We then refer to a *first register* and a *second register*, according to the tensor decomposition $\mathcal{H}_{2n} = \mathcal{H}_n \otimes \mathcal{H}_n$. For the remainder, by a local state we mean not a full tensor $|\psi\rangle = \otimes_{j=1}^{2n} |\psi_j\rangle$, $|\psi_j\rangle \in \mathcal{H}_1$ but rather a data state which is local to each register: $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, $|\psi_j\rangle \in \mathcal{H}_n$, $j = 1, 2$.

Given this, the conventions for the quantum oracle box are as following. The oracle U_f effects a unitary transformation of $\mathcal{H}_{2n}$ which linearly extends

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle \tag{3}$$

where $y \oplus f(x)$ denotes $y + f(x) \bmod N$ and the tensor symbols have been supressed. Our quantum algorithm then requires $O(1)$ calls to U_f and $O(n^2)$ two-qubit gates otherwise to distinguish with probability arbitrarily close to one between the cases

- $f(x)$ is one-to-one.
- $f(x)$ is θ-concentrated.

Hence the quantum algorithm in this sense outperforms a classical device using $O(N)$ classical oracle calls to determine whether $f(x)$ is one-to-one with certainty. However, consider instead a probabilistic classical computer, capable of evaluating $f(x)$ on a given random x, $0 \leq x \leq N-1$. With a single oracle call, such a classical probabilistic computer is likely to detect $f(x)$ is not θ-concentrated with probability $1 - \frac{2\theta}{2\pi}$. Hence $f(x)$ is one-to-one, by hypothesis. Making use of a single quantum oracle call, our quantum algorithm identifies any one-to-one function with certainty, and it correctly identifies a θ-concentrated $f(x)$ with probability $\cos^2\theta$. Taking $f(x)$ one-to-one or θ-concentrated, each with probability $\frac{1}{2}$, further demonstrates that the quantum algorithm outperforms the classical probabilistic algorithm on average for $0 < \theta < 0.3301\mathrm{rad}$, with maximal quantum outperformance at $\theta = \frac{1}{2}\sin^{-1}\frac{1}{\pi} \approx 0.1620\mathrm{rad}$.

2 Algorithms Determining $f(x)$ is 1-1

A Classical Deterministic Algorithm

This section applies to any $f : \{0, 1, \cdots, N-1\} \to \{0, 1, \cdots, N-1\}$, whether $N = 2^n$ or not. In the sequel, choosing $N = 2^n$ makes possible small quantum Fourier transform circuits, i.e. efficient quantum implementations of the Fourier transform of $\mathbb{Z}/N\mathbb{Z}$.

To determine whether $f(x)$ is one-to-one, proceed as follows. We suppose a classical oracle capable of evaluating $f(x)$ and a memory block of size N bits.

```
Initialize each memory bit to 0
for(j=0; j<=N-1; ++j)
{   Use oracle to compute $f(j)$
    if[ (bit # $f(j)$) == 1 ]
    {   report **not 1-1**
        end }
    Assign 1 to bit $f(j)$ }
report **1-1**
```

Moreover, note that there *can not* exist any oracle-based algorithm which determines whether $f(x)$ is one-to-one while only using $N-1$ or fewer calls to the classical oracle which evaluates $f(x)$.

A Probabilistic Algorithm

Since the quantum algorithm will only decide between the one-to-one and θ-concentrated cases with probability very close to one, we also consider competitive probabilistic classical algorithms. For simplicity, suppose now $f(x)$ is either one-to-one or θ-concentrated about 0, i.e. $\psi_0 = 0$ in Equation 1. Given a random number generator, the following algorithm is immediate:

```
Choose a random $0 \le x \le N-1$
Evaluate $f(x)$
if[$\omega^{f(x)} \notin \exp(i[-\theta, \theta])$]
    report $f(x)$ **is 1-1**
else
    report $f(x)$ **is likely concentrated**
```

The probabilistic algorithm fails if and only if $f(x)$ is one-to-one and yet $\omega^{f(x)} \in \exp(i[-\theta, \theta])$, roughly with probability $1 - \frac{\theta}{\pi}$ for n large.

Quantum Algorithm

Henceforth, suppose $N = 2^n$, a quantum data space $\mathcal{H}_{2n}$, and a quantum oracle U_f per Equation 3. We now specify the quantum algorithm. Continue to view $\mathcal{H}_{2n} \cong \mathcal{H}_n \otimes \mathcal{H}_n$.

References to the first register refer to the first tensor factor while references to the second register refer to the second. The adjective local refers to the tensor decomposition into n-qubit registers.

To distinguish a concentrated from a one-to-one $f(x)$:

1. Prepare the first register as $|0\rangle^{\otimes n}$ and the second as $|1\rangle^{\otimes n}$. Thus the original data state is $|\Phi\rangle = |\Phi_1\rangle \otimes |\Phi_2\rangle = |0\rangle^{\otimes n}|1\rangle^{\otimes n}$.

2. Let $\omega = \mathrm{e}^{2\pi i/N}$, for $N = 2^n$. As is well-known, there is a quantum circuit, polynomial in size in n, which implements the quantum Fourier transform map: $\mathcal{F} : \mathcal{H}_n \to \mathcal{H}_n$ linearly extending $|y\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{yz} |z\rangle$. Apply $\mathcal{F}$ to the second register, for $|\Phi\rangle_2 = \mathcal{F}|N-1\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{-z} |z\rangle$.

3. Recall the one-qubit Hadamard gate given by $H = \frac{1}{\sqrt{2}} \sum_{j,k=0}^{1} (-1)^{jk} |j\rangle\langle k|$. Then apply $H^{\otimes n}$ to the first register, with the result that

$$|\Phi_1\rangle = (H|0\rangle)^{\otimes n} = \Big[\, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \,\Big]^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{4}$$

Thus the first register now holds an equal superposition of all states. As preparation for the next step, we also note the full data state:

$$|\Phi_1\rangle \otimes |\Phi_2\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle|y\rangle \tag{5}$$

4. We next apply the quantum oracle U_f. The possibly nonlocal result is

$$|\Phi_1, \Phi_2\rangle = U_f \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle|y\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle|y \oplus f(x)\rangle \tag{6}$$

Note that a single call to U_f implicitly uses every value of $f(x)$ for a state in full superposition, such as $|\Phi_1\rangle$.

5. In fact, *the above data state is local.* For fix any $x = x_0$, and label $z = y - f(x_0)$. Then $\sum_{y=0}^{N-1} \omega^{-y} |y \oplus f(x_0)\rangle = \sum_{z=0}^{N-1} \omega^{z+f(x_0)} |z\rangle$. As this is true for all x_0, we have

$$|\Phi_1, \Phi_2\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \omega^{-z+f(x)} |x\rangle|z\rangle = \Big(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{f(x)} |x\rangle \Big) \otimes \Big(\frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{-z} |z\rangle \Big) \tag{7}$$

The next step is to disregard the known data $|\Phi_2\rangle$ in the second register.

6. Apply a Fourier transform to the retained register for

$$|\Phi_1\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{xy+f(x)} |y\rangle = \Big(\frac{1}{N} \sum_{x=0}^{N-1} \omega^{f(x)} |0\rangle \Big) + \frac{1}{N} \sum_{y=1}^{N-1} \sum_{x=0}^{N-1} \omega^{xy+f(x)} |y\rangle \tag{8}$$

7. Measure the probability that $|\Phi_1\rangle$ is $|0\rangle$. Per the $|0\cdots 0\rangle$ coefficient of Equation 8,

$$\text{Prob}\Big(|\Phi_1\rangle == |00\ldots 0\rangle \Big) = \left| \frac{1}{N} \sum_{x=0}^{N-1} \omega^{f(x)} \right|^2 \tag{9}$$

We briefly comment on the quantum computational resources consumed. Besides the $2n$-qubits, $O(n)$ local computations and two n-qubit Fourier transforms are required. The latter require $O(n^2)$ gates [6].

This algorithm is capable of distinguishing a one-to-one $f(x)$ from a θ-concentrated $f(x)$ with high probability if $\theta < \frac{\pi}{2}$. For one will never observe $|\psi\rangle == |00\cdots 0\rangle$ if $f(x)$ is one-to-one, while we prove below this happens with probability $\cos^2\theta$ if $f(x)$ is θ-concentrated. Hence, to distinguish any one-to-one $f(x)$ from a θ-concentrated $f(x)$ using U_f with probability $1-\epsilon$, run at least T independent trials of the above for $\epsilon > \sin^{2T}\theta$. In terms of ϵ, as $\log\sin\theta < 0$ we demand $T > \frac{1}{2}\frac{\log\epsilon}{\log\sin\theta}$.

3 Proof of correctness

Correctness from the algorithm follows from the following proposition. To see this, recall the formula of Equation 9 for Prob($|\Phi_1\rangle == |00\ldots 0\rangle$).

Proposition: Let $f : \{0,1,\ldots,N-1\} \to \{0,1,\ldots,N-1\}$, $N = 2^n$ be θ-concentrated, and continue to denote $\omega = \mathrm{e}^{2\pi i/N}$. Then

$$(\ f(x) \text{ is one-to-one }) \Longrightarrow \Big(\ \sum_{x=0}^{N-1} \omega^{f(x)} = 0\ \Big) \tag{10}$$

Hence, the $|0\rangle$ coefficient of the output $|\Phi_1\rangle$ is 0 if $f(x)$ is one-to-one. On the other hand,

$$(\ f(x) \text{ is concentrated }) \Longrightarrow \Big(\ \Big| \sum_{x=0}^{N-1} \omega^{f(x)} \Big| \geq N\cos^2\theta\ \Big) \tag{11}$$

Proof: First, recall that as an N^{th} root of unity, $\omega = \mathrm{e}^{2\pi i/N}$ solves $z^N - 1 = 0$. Then

- $z^N - 1 = (z-1)(\ \sum_{j=0}^{N-1} z^j\ )$
- $\omega \neq 1$
- For $f(x)$ one-to-one, $\sum_{j=0}^{N-1}\omega^j = \sum_{j=0}^{N-1}\omega^{f(j)}$.

Thus Equation 10 follows.

Suppose on the other hand that $f(x)$ is concentrated. Then we must always have $\omega^{f(j)-i\psi_0} = a_j + ib_j$ for ψ_0 per Equation 1, and moreover $\cos\theta \leq a_j \leq 1$. It follows that $\left|\sum_{x=0}^{N-1}\omega^{f(x)}\right| = \sqrt{(\sum_{j=0}^{N-1} a_j)^2 + (\sum_{j=0}^{N-1} b_j)^2} \geq \sum_{j=0}^{N-1} a_j \geq N\cos\theta$. This concludes the proof of Equation 11. □

4 Average performance per oracle call

We finally compare the probabilistic classical algorithm with the quantum algorithm above, allowing each a single oracle call. For simplicity we suppose $\psi_0 = 0$ in Equation 1; this hypothesis favors the classical algorithm. Also for simplicity, we suppose $f(x)$ is equally likely to be either concentrated or one-to-one.

Thus, $f(x)$ is either either one-to-one (event O) or θ-concentrated (event C) with probability $\frac{1}{2}$. Suppose the classical probabilistic algorithm makes one oracle call and then guesses $f(x)$ is concentrated if $\omega^{f(x)}$ lies within the sector $\exp(i[-\theta, \theta])$ and one-to-one else. If $f(x)$ is θ-concentrated, then the classical algorithm always makes a correct guess (event G_C.) In the one-to-one case, the probability of a correct guess is approximately $1 - \frac{\theta}{\pi}$. So

$$\begin{aligned} \mathrm{Prob}(G_C) &= \mathrm{Prob}(G_C|O)\mathrm{Prob}(O) + \mathrm{Prob}(G_C|C)\mathrm{Prob}(C) \\ &\approx (1 - \tfrac{\theta}{\pi})(1/2) + (1)(1/2) \\ &= 1 - \tfrac{\theta}{2\pi} \end{aligned} \tag{12}$$

If multiple oracle calls are allowed, it will help to recall x from previous trials and force the oracle to evaluate new values. However, as $N = 2^n$ is expected to be large, this is a minor consideration, and $1 - (\frac{\theta}{2\pi})^\ell$ is approximately the probability of making a correct guess after ℓ-trials.

In contrast, consider the quantum algorithm. It guesses $f(x)$ is concentrated if $|00\cdots 0\rangle$ is observed and guesses one-to-one else. Thus, in contrast to the classical algorithm, the quantum algorithm never fails if $f(x)$ is one-to-one. If $f(x)$ is concentrated, then the quantum guess if correct (event G_Q) with probability at least $\cos^2\theta$. Thus

$$\begin{aligned} \mathrm{Prob}(G_Q) &= \mathrm{Prob}(G_Q|O)\mathrm{Prob}(O) + \mathrm{Prob}(G_Q|C)\mathrm{Prob}(C) \\ &\geq (1)(1/2) + (\cos^2\theta)(1/2) \end{aligned} \tag{13}$$

Thus the appropriate comparison of the probabilistic and quantum algorithms is given by $\mathrm{Prob}(G_Q) \geq^? \mathrm{Prob}(G_C)$, i.e. for which θ do we have $\cos^2\theta \geq 1 - \frac{\theta}{\pi}$? Hence as asserted the maximum outperformance $\mathrm{Prob}(G_Q) - \mathrm{Prob}(G_C)$ occurs at $\theta = \frac{1}{2}\sin^{-1}\frac{1}{\pi} \approx 0.1620$rad, with outperformance of the quantum algorithm whenever $0 < \theta < 0.3301$rad.

Acknowledgements We are grateful to Francis Sullivan and Michael Robinson for very helpful discussions.

References

[1] D.P. Chi, J. Kim, and S. Lee, Initialization-free generalized Deutsch-Jozsa algorithm, J. of Phys. A - Math. and General **34** (2001) 5251-5258.

[2] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. R. Soc. Lond. A **400** (1985) 97-117.

[3] D. Deutsch and R. Jozsa, Rapid solutions of problems by quantum computation, Proc. R. Soc. Lond. A **439** (1992) 553-558.

[4] A. Ekert and R. Jozsa, Quantum computation and Shor's factoring algorithm, Mod. Rev. Phys. **68** (1996) 733-753.

[5] S. Gudder, Quantum Computation, this MONTHLY **110** (2003) 181-201.

[6] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2000.