Volume 112, Number 6, November-December 2007
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **112**, 307-311 (2007)]

A Quantum Algorithm Detecting Concentrated Maps

Volume 112 Number 6 November-December 2007

Isabel Beichl

National Institute of Standards and Technology,
Gaithersburg, MD 20899

Stephen S. Bullock

Institute for Defense Analyses,
Center for Computing Sciences,
Bowie, MD 20715

and

Daegene Song

Korea Institute for Advanced Study,
Seoul 130-722, Korea

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 $0 \le \theta \le \pi/2$, we say $f(x)$ is θ – *concentrated* if and only if $e^{2\pi i f(x)/N} \subset e^{i[\psi_0 - \theta, \psi_0 + \theta]}$ for some given ψ_0 and any $0 \le x \le N-1$. We present 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 random (classical) evaluation of the function testing for dispersed values (on average). Maximal outperformance occurs at $\theta = \frac{1}{2}\sin^{-1} {}^1/_\pi \approx 0.1620$ rad.

Key words: concentrated maps; Deutsch-Jozsa algorithm; Deutsch's algorithm; one-to-one mappings; quantum computation; quantum oracle; roots of unity.

Accepted: November 25, 2007

Available online: http://www.nist.gov/jres

1. Introduction

In recent years, much progress has been made in the study of quantum computation [1,2]. The first algorithm arguing for computational speed-up due to quantum mechanics was discovered in 1985 [3]. Deutsch considered a mapping with two inputs and two outputs. An oracle, which one might think of as a classical black-box, evaluates functions of a bit by inputting $b \in \{0, 1\}$ and outputting $f(b) \in \{0, 1\}$. Two calls to such an oracle are required to learn whether f is one-to-one. The calls compute $f(0)$ and $f(1)$, and then the one-to-one property holds when the values are distinct. Since quantum mechanics is linear, a quantum function evaluator (quantum oracle) must act on superpositions of states.

$$U_f(\alpha|0,0\rangle + \beta|1,0\rangle) = \alpha|0, f(0)\rangle + \beta|1, f(1)\rangle \quad (1)$$

A single call to this quantum oracle allows one to determine whether $f(0)$ and $f(1)$ are distinct [2, pg.36]. Several years later, Deutsch and Jozsa generalized the algorithm to allow for multiple inputs and two outputs [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 [5] distinguish between functions which are constant or else map onto an evenly spaced subset of the unit circle $\{|z| = 1\}$.

We present a variant of such algorithms. Specifically, suppose that we have a function $f : \{0, 1, 2, ..., N-1\}$

$\to \{0, 1, ..., N-1\}$, where $N = 2^n$ for n some (integer) number of qubits, so that the n-qubit state space $\mathcal{H}_1^{\otimes n}$ is N dimensional [2]. Let $\omega = e^{2\pi i/N}$ be the (2^n)th root of unity, and choose $\psi_0 \in [0, 2\pi)$. We say such an $f(x)$ is $\theta-$*concentrated* about ψ_0 if and only if

$$\omega^{f(x)} \in \exp(i[\psi_0 - \theta, \psi_0 + \theta]),\ \forall 0 \le x \le N-1 \qquad (2)$$

We say $f(x)$ is θ-concentrated if and only if there exists a ψ_0 so that (2) 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 briefly review quantum data spaces [2,6]. The state of a string of quantum bits is encoded as a vector 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 $\mathcal{H}_1 = \text{span}_{\mathbf{C}}\{|0\rangle, |1\rangle\}$, where this basis is Hermitian orthonormal. The n-qubit state space is then the $N = 2^n$ tensor (Kronecker) product

$$\begin{aligned}\mathcal{H}_n = \text{span}_{\mathbf{C}}\{&|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle : \\ &b_j \in \mathbf{F}_2 = \{0,1\}, 1 \le j \le n\}\end{aligned} \qquad (3)$$

The abbreviation $|b_1 b_2 ... b_n\rangle$ for $|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$ is typical, and the Hermitian inner product is that induced by the tensor structure. At times, we further abbreviate the bit-string $b_1 b_2 ... b_n$ 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 $\mathcal{H}_{2n} = \mathcal{H}_n \otimes \mathcal{H}_n$.

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

$$U_f\, |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle \qquad (4)$$

where $y \oplus f(x)$ denotes $y + f(x)$ mod N and the tensor symbols have been suppressed. 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, $0 \le x \le N-1$. 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 $0 < \theta < 0.3301$ rad, with maximal quantum outperformance at $\theta = \frac{1}{2}\sin^{-1}\frac{1}{\pi} \approx 0.1620$ rad.

2. A Solution with No Quantum Oracle

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 $\mathbf{Z}/N\mathbf{Z}$.

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
      return }
   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 $f(x)$.

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 (2). Given a random number generator, the following algorithm is immediate:

```
Choose a random 0 ≤ x ≤ N − 1
Evaluate f(x)
if [ω^f(x) ∉ exp(i[−θ, θ])]
    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.

3. A Quantum Variant of Deutsch-Jozsa

The following algorithm exploits a quantum oracle U_f per Eq. (4). It requires two quantum registers, each n bits long.

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 $\omega = e^{2\pi i/N}$, for $N = 2^n$. As is well-known [2], 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 $|y\rangle \mapsto \frac{1}{\sqrt{N}} \Sigma_{y=0}^{N-1} \omega^{yz}|z\rangle$. Apply $\mathcal{F}$ to the second register, for $|\Phi\rangle_2 = \mathcal{F}|N-1\rangle = \frac{1}{\sqrt{N}} \Sigma_{z=0}^{N-1} \omega^{-z}|z\rangle$.

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

$$|\Phi_1\rangle = (H|0\rangle)^{\otimes n} = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \quad (5)$$

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:

$$|\Phi_1\rangle \otimes |\Phi_2\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle |y\rangle \quad (6)$$

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

$$\begin{aligned} |\Phi_1\rangle \otimes |\Phi_2\rangle &= U_f \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle |y\rangle \\ &= \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{-y} |x\rangle |y \otimes f(x)\rangle \end{aligned} \quad (7)$$

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. We reindex a sum in the last equation as follows. For fixed $x = x_0$, label $z = y - f(x_0)$. Then $\Sigma_{y=0}^{N-1} \omega^{-y} |y \oplus f(x_0)\rangle = \Sigma_{z=0}^{N-1} \omega^{-z+f(x_0)} |z\rangle$. As this is true for all x_0, we have

$$\begin{aligned} |\Phi_1\rangle \otimes |\Phi_2\rangle &= \frac{1}{N} \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \omega^{-z+f(x)} |x\rangle |z\rangle \\ &= \left(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{f(x)} |x\rangle\right) \otimes \left(\frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{-z} |z\rangle\right) \end{aligned} \quad (8)$$

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

$$\begin{aligned} |\Phi_1\rangle &= \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega^{xy+f(x)} |y\rangle \\ &= \left(\frac{1}{N} \sum_{x=0}^{N-1} \omega^{f(x)}\right) |0\rangle + \frac{1}{N} \sum_{y=1}^{N-1} \sum_{x=0}^{N-1} \omega^{xy+f(x)} |y\rangle \end{aligned} \quad (9)$$

7. Measure the probability that $|\Phi_1\rangle$ is $|00 \ldots 0\rangle$. Recall that the probability of this classical outcome is its square of the amplitude (i.e., coefficient) of $|00 \ldots 0\rangle$ in the coherent superposition $|\Phi_1\rangle$. (9),

$$\text{Prob}(|\Phi_1\rangle = |00 \ldots 0\rangle) = \left| \frac{1}{N} \sum_{x=0}^{N-1} \omega^{f(x)} \right|^2 \quad (10)$$

8. Should the classical bits 00 ... 0 be observed, assert that f is concentrated. Else assert that f is one-to-one.

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 [1].

How likely are the assertions of the last step to be correct? Observing $|\Phi_1\rangle = |00 \cdots 0\rangle$ has probability of zero if $f(x)$ is one-to-one, since $\Sigma_{j=0}^{N-1} \omega^j = 0$; we prove below that this observation has probability at least $\cos^2\theta$ 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 $1 - \varepsilon$, run at least T independent trials of the above for $\varepsilon > \sin^{2T}\theta$. In terms of ε, as $\log \sin \theta < 0$ we demand $T > \frac{1}{2} \frac{\log \varepsilon}{\log \sin \theta}$.

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

$$(f(x) \text{ is one-to-one}) \Rightarrow \left(\sum_{x=0}^{N-1} \omega^{f(x)} = 0 \right) \quad (11)$$

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

$$(f(x) \text{ is concentrated}) \Rightarrow \left(\left| \sum_{x=0}^{N-1} \omega^{f(x)} \right| \geq N\cos\theta \right) \quad (12)$$

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

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

Thus Eq. (11) follows.

Suppose on the other hand that $f(x)$ is concentrated. Then $\omega^{f(j)-i\psi_0} = a_j + ib_j$ for ψ_0 per Eq. (2), and moreover $\cos\theta \leq a_j \leq 1$.

$$\left| \sum_{x=0}^{N-1} \omega^{f(x)} \right| = \sqrt{(\sum_{j=0}^{N-1} a_j)^2 + (\sum_{j=0}^{N-1} b_j)^2} \geq \sum_{j=0}^{N-1} a_j \geq N\cos\theta \quad (13)$$

This concludes the proof of Eq. (12). □

4. Comparison of Quantum to Classical

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 (2); 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 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 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

$$\begin{aligned} \text{Prob}(G_c) &= \text{Prob}(G_C|O)\text{Prob}(O) + \text{Prob}(G_C|C)\text{Prob}(C) \\ &\approx (1 - \frac{\theta}{\pi})(1/2) + (1)(1/2) \\ &= 1 - \frac{\theta}{2\pi} \end{aligned} \quad (14)$$

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 $1 - (\frac{\theta}{2\pi})^l$ 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 is correct with probability of at least $\cos^2\theta$. Thus

$$\begin{aligned} \text{Prob}(G_Q) &= \text{Prob}(G_Q|O)\text{Prob}(O) + \text{Prob}(G_Q|C)\text{Prob}(C) \\ &\geq (1)(1/2) + (\cos^2\theta)(1/2) \end{aligned} \quad (15)$$

Thus the appropriate comparison of the probabilistic and quantum algorithms might be quantified by the difference $\text{Prob}(G_Q)$–$\text{Prob}(G_C)$, i.e., the quantum approach is preferable for those θ with $\cos^2\theta \geq 1 - \frac{\theta}{\pi}$, i.e., $\sin^2\theta \geq \frac{\theta}{\pi}$. The maximum difference occurs at $\theta = \frac{1}{2}\sin^{-1}\frac{1}{\pi} \approx 0.1620$ rad, while applying Newton's method to $\sin^2\theta - \frac{\theta}{\pi}$ shows that the quantum approach is preferable given $0 < \theta < 0.3301$ rad. The right boundary of the interval is approximate.

Acknowledgment

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

5. References

[1] A. Ekert and R. Jozsa, Quantum Computation and Shor's Factoring Algorithm, Rev. Mod. Phys. **68**, 733-753 (1996).
[2] M.A. Nielsen and I. Chuang, Quantum Information and Quantum Computation, Cambridge University Press (2000).
[3] D. Deutsch, Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, Proc. Royal Soc. Lond. A **400**, 97-117 (1985).
[4] D. Deutsch and R. Jozsa, Rapid Solution of Problems by Quantum Computation, Proc. Royal Soc. Lond. A **439**, 553-558 (1992).
[5] D. P. Chi, J. Kim, and S. Lee, Initialization Free Generalized Deutsch-Jozsa, J. Phys. A - Math. Gen. **34**, 5251-5258 (2001).
[6] S. Gudder, Quantum Computation, Amer. Math. Monthly **110**, 181-201 (2003).

About the authors: *Isabel Beichl is a mathematician in the Information Technology Laboratory of the National Institute of Standards and Technology. Stephen S. Bullock is a staff researcher at the Institute for Defense Analyses Center for Computing Sciences. Formerly, he was an NRC Postdoctoral Fellow at the National Institute of Standards and Technology.*

Daegene Song is a research fellow at the Korea Institute for Advanced Study and was formerly an NRC postdoctoral fellow at the National Institute of Standards and Technology. The National Institute of Standards and Technology is an agency of the U.S. Department of Commerce.