The Deutsch-Jozsa Problem: De-quantization and entanglement

Alastair A. Abbott

Department of Computer Science
University of Auckland, New Zealand

May 31, 2009

Abstract

The Deustch-Jozsa problem is one of the most basic ways to demonstrate the power of quantum computation. Consider a boolean function $f : \{0,1\}^n \to \{0,1\}$ and suppose we have a black box to compute f. The Deutsch-Jozsa problem is to determine if f is constant [i.e. $f(x) = \text{const}, \forall x \in \{0,1\}^n$] or if f is balanced [i.e. $f(x) = 0$ for exactly half the possible input strings $x \in \{0,1\}^n$] using as few calls to the black box computing f as is possible, assuming f is guaranteed to be constant or balanced. Classically it appears that this requires at least $2^{n-1}+1$ black box calls in the worst case, but the well known quantum solution solves the problem with probability 1 in exactly one black box call. However, it has been found that in some cases equivalent classical, deterministic solutions also exist. We attempt to clarify the power of the quantum solution in order to gain better insight into where the power of quantum computation comes from, as well as the ability to determine when classical, deterministic counterparts can be found.

1 Introduction

Deutsch's problem and the more general Deutsch-Jozsa problem were some of the first problems tackled in the field of quantum computing. They are simple, but are sufficiently non-trivial to be of interest. The generally accepted quantum solutions contain aspects of quantum parallelism, interference and entanglement, which are commonly cited as the main tools which give quantum computing its power. In this paper, we build on a previous paper [4] that shows Deutsch's original problem is solvable classically. We extend this note to the general Deutsch-Jozsa problem in an attempt to explore what is fundamentally important to quantum computation.

1.1 Definitions

In order to be able to talk about the differences between classical and quantum algorithms, we need define them in a way which captures their differences in a constructive manner. We will call an algorithm a *classical algorithm* if it can be computed on a Turing machine and a *quantum algorithm* if it can be computed by a sequence of unitary operators, $U = U_L U_{L-1} \ldots U_1$. Many quantum algorithms have a trivial classical counterpart: all the operations in the matrix mechanics formulation of quantum mechanics can be easily computed by classical means . As long as one is careful (i.e. quantum features such as randomness are not fundamentally important to the algorithm) equivalent classical algorithms can be obtained by these means [9]. However, the dimension of Hilbert space grows exponentially with the number of qubits used in a quantum algorithm, so a classical counterpart obtained by the trivial means takes space and time that is exponentially larger than the quantum algorithm does, assuming we measure space in fundamental basis elements (i.e. 0,1,$|0\rangle$,$|1\rangle$ take equal space to within a constant factor). In this paper we examine the existence of classical counterparts to quantum algorithms that are not exponential in time or space compared to the quantum algorithm.

Throughout this paper we will use the standard orthogonal basis kets $|0\rangle$ and $|1\rangle$. We will use the shorthand notion $|+\rangle$ and $|-\rangle$ to represent the symmetric and antisymmetric equal superpositions of the basis states, so that the Hadamard gate H has the following effect [3]:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \text{ and}$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

1.2 Oracle Quantum Computations and Embeddings

The main subject of this paper, the Deutsch-Jozsa problem (and also Deutsch's problem) is a form of an oracle computational problem [2, 12]. This means that the input is given to us as a black box and the goal is to determine something about this black box. It is important that this information can only be obtained by asking the oracle allowable questions. It must not be the case that examination of the structure alone of the black box allows insight into the nature of the black box [8, p. 554].

In the current literature it is usually implicitly assumed that solving a problem with a classical black box is of the same difficulty as solving it with a quantum, or alternative kind of black box. In general, a standard classical black box can operate on classical bits only (0 or 1), while a quantum black box can operate on any state in 2 dimensional Hilbert space ($\mathscr{H}_2$). This difference in some sense appears to add extra complexity to a quantum black box. It is not clear that solving a problem given a quantum black box is the same as solving a problem given a classical black box. However, this is an issue to be explored in the future. In this paper we will assume the

normal situation that we are given a certain type of black box and asked to find information about what the black box represents.

2 Deutsch's Problem

The original problem proposed by Deutsch [7] is4 formulated as follows. Consider a boolean function $f : \{0,1\} \to \{0,1\}$, and suppose we are given a black box (oracle) to solve f. Deutsch's problem is to determine if f is constant [i.e. $f(0) = f(1)$] or balanced [i.e. $f(0) \neq f(1)$] in as few as possible calls to the black box computing f.

2.1 Quantum Solution

A standard quantum solution for Deutsch's problem is briefly presented, as all further analysis will stem from this. This is based on the formulation given in [5] which solves Deutsch's problem with probability 1 using only one call to the quantum black box computing f. A traditional classical algorithm would require two calls to a classical black box in order to determine if f is constant or balanced. The quantum black box extends the classical black box to operate on superpositions of basis states. The quantum black box can be described by the unitary operator U_f representing an f-controlled-NOT (f-cNOT) gate such that

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

Noting that

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

we see that U_f is its own inverse and $U_f U_f = 1$. Hence U_f is unitary and our quantum black box is valid. In order to see how the quantum solution works, it is beneficial to observe the following:

$$\begin{aligned} U_f |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= |x\rangle \frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

From this observation we can formulate the quantum solution.
Taking the initial state $|0\rangle |1\rangle$ and operating on it with a 2-qubit Hadamard gate $H^{\otimes 2}$:

$$H^{\otimes 2} |0\rangle |1\rangle = H |0\rangle H |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |-\rangle .$$

Next, operating on the state with U_f:

$$\begin{aligned} \frac{1}{\sqrt{2}} U_f (|0\rangle + |1\rangle) |-\rangle &= \frac{1}{\sqrt{2}} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) |-\rangle \\ &= \frac{(-1)^{f(0)}}{\sqrt{2}} \left(|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle \right) |-\rangle \end{aligned}$$

and applying $H^{\otimes 2}$ one more time we get

$$H^{\otimes 2}\frac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle\right)|-\rangle=(-1)^{f(0)}|f(0)\oplus f(1)\rangle|1\rangle\,.$$

Measuring the first qubit we obtain 0 with probability 1 if f is constant and 1 with probability 1 if f is balanced.

This quantum solution is correct with probability 1 using only one call to the quantum black box represented by U_f. An important note is that this computation involves no entanglement. This can be seen by noting that the second qubit acts as an auxiliary bit and remains unchanged by U_f, and as a result the two qubits remain separable throughout the algorithm. This is evident in the presentation of the algorithm and as a result this quantum computation gains its power only from quantum parallelism and interference.

2.2 Classical Solutions

As noted, the quantum solution contains no entanglement. It uses the quantum properties of superposition and interference in order to achieve the desired result. However, these qualities (unlike entanglement) are not inherently quantum mechanical, but are rather due to the two dimensionality of qubits compared to the one dimensionality of classical bits. Hence, a classical two-dimensional system possesses these qualities, and should thus be able to achieve the same result as the quantum algorithm.

The first method, presented in [4], embeds classical bits in complex numbers. The set $\{1,i\}$ with $i=\sqrt{-1}$ acts as a computational basis in the same way that $\{|0\rangle,|1\rangle\}$ does for quantum calculations. It is worth noting that while we are not labeling the basis bits '0' and '1', they represent the classical bits 0 and 1 in the same way that $|0\rangle$ and $|1\rangle$ do.

A general complex number may be written as $z=a+bi$, so a general complex number z is a natural superposition of the basis in the same way that a general qubit is. We are now given a classical black box that computes our function f. This black box can be represented by a function C_f, a direct analogue of U_f (although the requirement of unitarity is no longer necessary). The effect of C_f (by direct correspondence with U_f, although the normalization factors and auxiliary bit are no longer necessary) is

$$C_f(a+bi)=(-1)^{f(0)}\left(a+(-1)^{f(0)\oplus f(1)}bi\right).$$

If f is constant, C_f is the identity operation to within a factor of -1 ($C_f(x)=\pm x$). If f is balanced, C_f is the conjugation operation ($C_f(x)=\pm\bar{x}$). The black box represented by C_f rotates the input in the complex plane depending on the nature of f, which is in direct analogy of the quantum black box U_f operating on input $|x\rangle$ in $\mathscr{H}_2$. In order to measure the output, we need a way to project our complex numbers back on to the computational basis. This is easily done

by multiplying by the input so the output is either purely imaginary or purely real (i.e. on the computational basis).

If $z = 1 + i$ (an equal superposition of basis states), $\frac{1}{2}zC_f(z) = \frac{\pm 1}{2}z^2 = \pm i$ if f is constant or $\frac{1}{2}zC_f(z) = \frac{\pm 1}{2}z\bar{z} = \pm 1$ if f is balanced. In this manner, if the output is imaginary then f is constant, if it is real then f is balanced. Importantly, this is a deterministic result.

This is only one method of solving the problem as well as the quantum algorithm does through classical, deterministic methods. The above method places emphasis on mathematical correspondence with the quantum solution. A different solution is presented by Arvind in [1] which draws physical similarities which are more visible than in the above solution. Such a method of taking a quantum algorithm and finding a classic counterpart which works just as efficiently is called a *de-quantization*. This term was first used by Calude [4], but the methods used by [1, 10] for example would also classify as de-quantizations.

Arvind uses the (classical) polarization of a photon as the computational basis (x-pol, y-pol), and any polarization in the x-y plane is physically valid. It is noted that all transformations in the group SU(2) can be realized by two quarter-wave plates and a single half-wave plates orientated suitably. Clearly the transformations required to solve Deutsch's problem are included in this, so the problem can be solved classically with one photon using wave plates. Written in matrix form the solution is mathematically identical to the quantum one. This corresponds to the following physical process: Preparing a photon in the y-polarization, rotating anti-clockwise in the x-y plane by 45°, applying the black box, and applying the anti-clockwise rotation once more before measuring the y-polarization of the photon.

The correspondence here relies not on embedding classical bits in a different, classical 2-dimensional basis but on directly implementing the transformations used in the quantum solution through classical means. In other words, the quantum algorithm does not take advantage of non-classical effects, so the same result can be obtained through purely classical optics.

3 The Deutsch-Jozsa Problem

This problem was extended by Deutsch and Jozsa [8] to functions on n-bit strings. In this case, the problem is formulated as follows. Let $f : \{0,1\}^n \to \{0,1\}$, and suppose we are given a black box computing f with the guarantee that f is either constant [i.e. $\forall x \in \{0,1\}^n : f(x) = a, a \in \{0,1\}$] or balanced [i.e. $f(x) = 0$ for exactly half of the possible inputs $x \in \{0,1\}^n$]. The Deutsch-Jozsa problem is to determine if f is constant or f is balanced. An important note is that unlike in Deutsch's problem, where there are exactly two balanced and two constant functions f, the distribution of constant and balanced functions is asymmetrical in the Deutsch-Jozsa problem. In general, there are $N = 2^n$ possible input strings, each with two possible outputs (0 or 1). Hence, for any given n there are 2^N possible functions f. Of these, exactly two are constant and $\binom{N}{N/2}$ are balanced. Evidently the probability that our f (promised to be balanced

or constant) is constant tends towards zero very quickly. Furthermore, the probability that any randomly chosen function of the 2^N possible functions is either balanced or constant (i.e. f is valid) is given by

$$\frac{\binom{N}{N/2}+2}{2^N}$$

which also tends to zero as n increases. This is evidently not an ideal problem to work with, however this does not mean that we cannot gain useful information from studying it.

4 Adaptation for $n = 2$

In this section we will provide a formulation of the solution for the Deutsch-Jozsa problem with $n = 2$ which makes the separability of the states clearly evident and draws obvious parallelism with the $n = 1$ solution presented in the previous section.

4.1 Quantum Solution

For $n = 2$ the quantum black box we are given takes as input three qubits and is represented by the following unitary operator U_f, just as it was for $n = 1$:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle, \text{ where } x \in \{0,1\}^2.$$

For $n = 2$ there are 16 possible boolean functions. Two of these are constant and another six are balanced. All these possible functions are listed in Table 1.

$f(x)$	Constant		Balanced						Other							
$f(00) =$	0	1	0	1	1	0	1	1	1	0	1	0	1	0	0	1
$f(01) =$	0	1	0	1	0	1	0	0	1	0	1	0	0	1	1	0
$f(10) =$	0	1	1	0	1	1	0	0	1	0	0	1	1	0	1	0
$f(11) =$	0	1	1	0	0	0	1	1	0	1	1	0	1	0	1	0

Table 1: All possible Boolean functions $f : \{0,1\}^2 \to \{0,1\}$

Evidently, half of these functions are simply the negation of another. If we let $f'(x) = f(x) \oplus 1$, we have:

$$\begin{aligned} U_{f'} |x\rangle |-\rangle &= (-1)^{f'(x)} |x\rangle |-\rangle \\ &= -\left((-1)^{f(x)} |x\rangle |-\rangle\right) \\ &= -U_f |x\rangle |-\rangle . \end{aligned}$$

In this case the result obtains a global phase factor of -1. Since global phase factors have no physical significance to measurement (a result is obtained with probability proportional to the amplitude squared), the outputs of U_f and $U_{f'}$ are indistinguishable.

If we initially prepare our system in the state $|00\rangle|1\rangle$, operating on this state with $H^{\otimes 3}$ gives

$$H^{\otimes 3}|00\rangle|1\rangle = \frac{1}{2}\sum_{x\in\{0,1\}^2}|x\rangle|-\rangle = |{+}{+}\rangle|-\rangle\,. \tag{1}$$

In the general case, after applying the f-cNOT gate U_f we have

$$\begin{aligned} U_f \sum_{x\in\{0,1\}^2} c_x|x\rangle|-\rangle &= \sum_{x\in\{0,1\}^2}(-1)^{f(x)}c_x|x\rangle|-\rangle \\ &= \Big[(-1)^{f(00)}c_{00}|00\rangle + (-1)^{f(01)}c_{01}|01\rangle + (-1)^{f(10)}c_{10}|10\rangle \\ &\qquad +(-1)^{f(11)}c_{11}|11\rangle\Big]|-\rangle\,. \end{aligned} \tag{2}$$

From the well known rule (see [11]) about 2-qubit separable states, we know that this state is separable if and only if $(-1)^{f(00)}(-1)^{f(11)}c_{00}c_{11} = (-1)^{f(01)}(-1)^{f(10)}c_{01}c_{10}$. While there are various initial superpositions of 2-qubit states which satisfy this condition, we only need to consider the equal superposition (shown in Equation (1)) that is used in this algorithm. In this case, the separability condition is $f(00)\oplus f(11) = f(01)\oplus f(10)$. By looking back at Table 1 it is obvious this condition must hold for all balanced or constant functions f for $n = 2$.

We can now rewrite Equation (2) as follows:

$$U_f|{+}{+}\rangle|-\rangle = \frac{\pm 1}{2}\left(|0\rangle + (-1)^{f(00)\oplus f(10)}|1\rangle\right)\left(|0\rangle + (-1)^{f(10)\oplus f(11)}|1\rangle\right)|-\rangle\,. \tag{3}$$

Indeed,

$$\begin{aligned} &(-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle \\ &= (-1)^{f(00)}|00\rangle + (-1)^{f(00)\oplus f(10)\oplus f(11))}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle \\ &= (-1)^{f(00)}\left(|00\rangle + (-1)^{f(10)\oplus f(11)}|01\rangle + (-1)^{f(00)\oplus f(10)}|10\rangle + (-1)^{f(00)\oplus f(11)}|11\rangle\right) \\ &= \pm\left(|0\rangle + (-1)^{f(00)\oplus f(10)}|1\rangle\right)\left(|0\rangle + (-1)^{f(10)\oplus f(11)}|1\rangle\right), \end{aligned}$$

as desired. By applying a final 3-qubit Hadamard gate to project this state onto the computational basis we obtain

$$\begin{aligned} \tfrac{\pm 1}{2}H^{\otimes 3}\left(|0\rangle + (-1)^{f(00)\oplus f(10)}|1\rangle\right)\left(|0\rangle + (-1)^{f(10)\oplus f(11)}|1\rangle\right)|-\rangle &= \pm|f(00)\oplus f(10)\rangle \\ &\quad\otimes|f(10)\oplus f(11)\rangle|1\rangle\,. \end{aligned}$$

By measuring both the first and second qubits we can determine the nature of f with probability 1. If both qubits are measured as 0, then f is constant, otherwise f is balanced.

4.2 Classical Solutions

Because the quantum solution contains no entanglement, the problem can be de-quantized in a similar way to the $n = 1$ case, but this time using two complex numbers as input. However, in order to retain enough information to solve the problem, the de-quantized black box must also output 2 complex numbers (C_f is a transformation rather than a function). We will define C_f by analogy to U_f just as we did for the $n = 1$ case. Let z_1, z_2 be complex numbers,

$$C_f\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = C_f\begin{pmatrix} a_1 + ib_1 \\ a_2 + ib_2 \end{pmatrix} = (-1)^{f(00)}\begin{pmatrix} a_1 + (-1)^{f(00)\oplus f(10)} ib_1 \\ a_2 + (-1)^{f(10)\oplus f(11)} ib_2 \end{pmatrix}. \tag{4}$$

It is important to note that, just as in the quantum case where the output of the black box was two qubits that can be independently measured, the output of C_f is two complex numbers that can be independently manipulated, rather than the complex number resulting from their product. This is fairly intuitive because the ability to measure specific bits (of any kind) is fundamental to computation. Note however, that in a quantum system it is impossible to measure entangled qubits independently of each other.

The analogue to applying a Hadamard gate to each qubit in order to project it onto the computational basis is to multiply each of the complex numbers that the black box outputs by their respective inputs (in similar fashion to that in the $n = 1$ case).

If we let $z_1 = z_2 = 1 + i$, we get the following:

$$\frac{(1+i)}{2} C_f\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{(-1)^{f(00)}}{2} \times \begin{cases} \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} i \\ i \end{pmatrix}, & \text{if } f \text{ is constant,} \\ \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1+i) \end{pmatrix} = \begin{pmatrix} 1 \\ i \end{pmatrix}, & \\ \begin{pmatrix} (1+i)(1+i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} i \\ 1 \end{pmatrix}, & \text{if } f \text{ is balanced.} \\ \begin{pmatrix} (1+i)(1-i) \\ (1+i)(1-i) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & \end{cases}$$

By measuring both of the resulting complex numbers, we can determine whether f is balanced or constant with certainty. If both complex numbers are imaginary then f is constant, otherwise it is balanced.

Because the quantum solution is separable, it is possible to write the output of the black box as a list of two complex numbers, and hence we can find a solution equivalent to the one obtained via a quantum computation. Writing the output in this form would not have been possible if the state was not separable, and finding a classical solution in this fashion would have required a list of complex numbers exponential in the number of input qubits.

As with the $n = 1$ case, an alternative classical approach can be presented using two photons. If a transformation on two qubits can be written as a transformation on each bit independently

(e.g. $H \otimes H$) then the transformation is trivially implemented classically. It only remains to the 2-bit transformation U_f can be implemented classically on 2-photons. Equation (3) shows that the quantum black box for $n = 2$, U_f can be written as a product of two 1-bit gates[1]:

$$U_f^{(1)} |+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{f(00)\oplus f(10)} |1\rangle \right),$$
$$U_f^{(2)} |+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{f(11)\oplus f(10)} |1\rangle \right).$$

Each of these are valid unitary operators, and the transformation describing the black box may be written $U_f = U_f^{(1)} \otimes U_f^{(2)}$. This means that the operation of f can be computed by applying a 1-bit operation (implemented as wave-plates) to each photon independently, and thus a classical solution for $n = 2$ is easily found in this fashion. The photons need not interact with each other at any point during the algorithm, not even inside the black box implementation.

This classical, optical method is equivalent to both the quantum solution and the previously described classical solution. The difference is in how it is represented, bringing emphasis on the fact that for $n = 2$ the quantum solution does not take advantage of uniquely quantum behaviour and is thus classical in nature. Further, it shows that the solution can be obtained without any interaction or sharing of information between qubits.

5 Work on n $\geq$ 3

We have already seen that for $n = 1$ and 2, the Deutsch-Jozsa problem can be de-quantized to give a classical algorithm that is just as efficient as the quantum algorithm. To examine what happens for larger n is a little more difficult.

For $n \geq 3$, it is no longer the case that the output of U_f is separable for all balanced or constant f. This can be easily seen by taking into account the results of [11]. We will briefly state their result and show how it is applicable.

In a system of n qubits, the general system state can be written as $|\psi_n\rangle = \sum_{i=0}^{N-1} c_i |i\rangle$, where $N = 2^n$ and c_i is the amplitude of the ith possible state of the system. Pair product invariance is defined as:

$|\psi_n\rangle$ is pair product invariant $\iff \forall k \in [1,n], \forall i \in [0, K-1] : c_i c_{K-i-1}$ is constant where $K = 2^k$.

Pair product invariance can also be reformulated recursively as follows. Let P_n be the set of all tuples $(c_i c_{K-i-1}, \alpha_k)$ such that $c_i c_{K-i-1}$ must equal a non-zero constant α_k for $|\psi_n\rangle$ to be pair

[1] So far we have been considering the case where U_f operates on n input qubits and one auxiliary qubit, $|-\rangle$. It has been shown (see [6]) that the auxiliary qubit is not necessary if we restrict ourselves to the subspace spanned by $|-\rangle$. However, we have presented the algorithm with the auxiliary qubit present because it is more intuitive to think of the input-dependent phase factor being an eigenvalue of the auxiliary qubit which is 'kicked back'. The de-quantized solutions however bear more resemblance to this reduced version of U_f operating only on n qubits.

product invariant, i.e.

$$P_n = \{(c_i c_{K-i-1}, \alpha_k), \forall k \in [1,n], \forall i \in [0,K-1]\}.$$

Recursively, this can be written by breaking up the iteration over all $k \in [1,n]$. We find that

$$\begin{aligned} &P_n = P_{n-1} \cup \{(c_i c_{2^n-i-1}, \alpha_n), \forall i \in [0, 2^{n-1}-1]\}, \text{ with the base case} \\ &P_2 = \{(c_{00}c_{11}, \alpha_2), (c_{01}c_{10}, \alpha_2)\}. \end{aligned}$$

The main theorem of relevance to us (Theorem 1 in [11]) is: *Provided all $c_i \neq 0$, a state $|\psi_n\rangle$ is fully separable if and only if it is pair product invariant.* In order to determine if our state $|\psi_n\rangle$ is separable we only need to check to see if all elements of P_n evaluate to the corresponding α_k.

Note that any constant function (for all n) is pair product invariant as all c_i are equal and the conditions are trivially satisfied. The output of the quantum black box for constant f can be separated as

$$\begin{aligned} \frac{1}{2^{n/2}} U_f \sum_{x\in\{0,1\}^n} |x\rangle |-\rangle &= \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle \\ &= \frac{\pm 1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle |-\rangle \\ &= \pm |+\rangle^{\otimes n} |-\rangle . \end{aligned}$$

For $n = 3$ we are able to find balanced functions that are not pair product invariant and thus entangled.

If we choose f such that $(f(000), f(001), f(010), f(011), f(100), f(101), f(110), f(111)) = (0,0,0,1,1,1,1,0)$, this f is obviously balanced. For this choice of f, $f(000) \oplus f(011) \neq f(001) \oplus f(010)$. Since the amplitudes of a state $|x\rangle$ are on a 1-1 mapping with $f(x)$, this shows that $c_{000}c_{011} \neq c_{001}c_{010}$ and hence the output of U_f in the standard quantum algorithm is not pair product invariant and is thus entangled.

The recursive definition of pair product invariance allows us to determine exactly how many separable states exist for any given n. For a function f_{n+1} acting on $n+1$ bits to be separable, we know that all pairs in P_{n+1} evaluate to some constant. Since $P_n \subset P_{n+1}$, all pairs in P_n must also evaluate to a constant. But the set of n bit functions f_n for which each element in P_n is constant is exactly the set of separable functions f_n. Hence we see that all separable functions f_{n+1} satisfy $f_{n+1}(0 \cdot x_n) = f_n(x_n), \forall x_n \in \{0,1\}^n$, where $0 \cdot x_n$ denotes the concatenation of x_n onto 0. This determines the action of f_{n+1} on half of the possible input strings, and we must determine the possible actions on the other half.

Because our $c_i = (-1)^{f(i)}$, the requirement for all pairs in P_{n+1} to be equal means the parity of all pairs must be the same, i.e.

$$c_i c_{K-i-1} = c_j c_{K-j-1} \iff f(i) \oplus f(K-i-1) = f(j) \oplus f(K-j-1).$$

The action of f_{n+1} on the remaining $N = 2^n$ inputs is determined the pair product invariance condition. This requires that $c_{N-1}c_N = c_{N-2}c_{N+1} = \cdots = c_0c_{2N-1}$. Since c_{N-1} is already determined, c_N can take on two possible values. However, once it takes on this value, all c_i for $i > N$ are uniquely determined. If we let a_n be the number of separable functions f_n, then f_{n+1} can have a_n possible configurations for acting of $f_{n+1}(0 \cdot x_n)$, and for each of these configurations, there are two configurations for the remaining N input strings. Hence,

$$a_{n+1} = 2a_n.$$

This is a simple linear recursion with the known initial condition $a_1 = 4$. This gives us an explicit result for the number of boolean functions f_n such that $U_{f_n}|x\rangle|-\rangle$ is separable:

$$a_n = 2^{n+1}.$$

We see that the number of separable states increases exponentially with the number of qubits being used. We also know the number of possible functions f_n which are either balanced or constant is

$$b_n = \binom{N}{N/2} + 2 = \binom{2^n}{2^n - 1} + 2.$$

The fraction of possible boolean functions which can be separated is

$$\frac{a_n}{b_n} = 2^{n+1} / \left(\binom{2^n}{2^{n-1}} + 2 \right).$$

This tends towards zero extremely quickly even for small n.

The result of this observation is that even if we are promised f is balanced or constant, we can no longer be sure the output of the black box is separable, and for $n \geq 3$ the probability that it is separable tends to zero very quickly. This means that the method of de-quantization used for $n = 1, 2$ will not scale directly to higher n and in general yields very little information about a function. Intuitively it would look like separability is a requirement for de-quantization to be possible. Looking at this from the view of computation with classical photons, there is no physical, classical equivalent of entangled photons as this is a purely quantum-mechanical effect. However, in general it is very hard to show that no de-quantization exists for a quantum algorithm which does not introduce exponential increase in space or time. In most cases, as earlier mentioned, a trivial method of de-quantization is possible, but to show no better de-quantization exists is very hard.

6 General de-quantization

While de-quantization appears to be very hard in the Deutsch-Jozsa problem for $n \geq 3$, one can investigate the ability to de-quantize algorithms not involving entanglement. So far de-quantization in this kind of fashion has only been explored for Deutsch's problem. The main

task in trying to de-quantize a quantum algorithm is to de-quantize the black box. Using the methods previously looked at in this paper, this step would initially require showing that both the input and output of the black box is separable. We will assume both the input and output of the black box U_f is separable, and look at what can be said about the ability to de-quantize the algorithm.

The simplest case is that U_f itself can be expressed in terms of n 1-qubit gates. If it is possible to do this we can write

$$U_f = U_f^{(1)} U_f^{(2)} \cdots U_f^{(n)}$$

where $U_f^{(i)}$ acts on the ith qubit only. This is easy to compute classically using the classical photon method used earlier. Since each $U_f^{(i)} \in \mathrm{SU}(2)$, they can be implemented using wave-plates. Further, the photons do not interact and are independent of each other throughout the computation. Hence, we can prepare the n photons as required, operate on each one with the appropriate wave-plate arrangements before measuring the polarization of each photon. Because U_f can be separated in this way, the de-quantized algorithm clearly implements the same transformation and hence yields the same result as the quantum algorithm, but with a classical deterministic result.

The next case to consider is the case that U_f cannot be written in terms of 1-qubit gates, but still does not entangle the input. We know that any unitary gate can be separated into a sequence of 1-qubit gates and cNOT gates (see [12]), and since we have already shown all 1-qubit gates are de-quantizable we need only examine thoroughly the cNOT gate. We note that any de-quantization of a cNOT gate is more complicated than that of any 1-qubit gate. The cNOT gate clearly involves some kind of interaction between the two input qubits. The classical photon de-quantization would appear to fall apart here, because it relied on the photons being treated independently. However, this does not mean that de-quantization is not possible. In general, when an n-qubit gate is decomposed into 1-qubit gates and cNOT gates, we cannot assume the input of the cNOT gates is not entangled, even if the input and output of U_f as a whole is separable. This is because the intermediate steps in the circuit could entangle and then unentangle. For de-quantization to be easy, we want the qubits to remain unentangled throughout the whole computation.

The cNOT gate is defined as

$$C\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|y \oplus x\right\rangle.$$

We can derive an expression for the requirement that the output of the cNOT gate is separable.

$$\begin{aligned} C(a\left|0\right\rangle + b\left|1\right\rangle)(c\left|0\right\rangle + d\left|1\right\rangle) &= C(ac\left|00\right\rangle + ad\left|01\right\rangle + bc\left|10\right\rangle + bd\left|11\right\rangle) \\ &= ac\left|00\right\rangle + ad\left|01\right\rangle + bd\left|10\right\rangle + bc\left|11\right\rangle. \end{aligned}$$

For this to be separable, we require that

$$\begin{aligned} abc^2 &= abd^2 \\ \Rightarrow c &= \pm d, \end{aligned}$$

subject to the normalization constraint $|c|^2 + |d|^2 = 1$, which tells us that $|y\rangle = |\pm\rangle$ if $c = \frac{1}{\sqrt{2}}$, or $|y\rangle = -|\pm\rangle$ if $c = \frac{-1}{\sqrt{2}}$. If this condition holds true at every cNOT gate in the decomposition of U_f onto the basis of unitary gates, then de-quantization is possible. More precisely, if we have $c = \pm d$,

$$\begin{aligned} C|x\rangle|y\rangle &= C(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\ &= \pm(a|0\rangle + b|1\rangle)(d|0\rangle + c|1\rangle) \\ &= \pm|x\rangle(d|0\rangle + c|1\rangle). \end{aligned}$$

Hence we need only consider the possible cases for $|y\rangle$:

$$C|x\rangle|y\rangle \begin{cases} C|x\rangle|\pm\rangle = \pm|x\rangle|\pm\rangle, & \text{if } c = \frac{1}{\sqrt{2}}, \\ -C|x\rangle|\pm\rangle = \mp|x\rangle|\pm\rangle, & \text{if } c = \frac{-1}{\sqrt{2}}. \end{cases}$$

Importantly, we see that if the conditions are met for the cNOT gate to not entangle the input, it can be treated as a 1-qubit gate which introduces a factor of ± 1 depending on the makeup of the second input qubit. In this situation, the gate can be treated as a 1-qubit gate that we know can be implemented classically, and de-quantization is possible.

If the condition that $c = \pm d$ holds at every cNOT gate in the decomposition of U_f, then separability is maintained throughout the computation, and every gate, including the cNOT gates, can be represented as 1-qubit gates, thus de-quantization of the complete black box is possible. However, the ability to determine if this condition holds could be relatively hard in general, and this is an issue that remains to be explored further. If this condition does not hold, it does not necessarily tell us that de-quantization is not possible. There may be an alternative decomposition of U_f into a different set of basis gates for which separability is maintained. For de-quantization to be successful, we must only find one such suitable decomposition. Exploring this in order to get stronger conditions for the ability to de-quantize an algorithm is a subject of future research.

7 Conclusion

We have examined the ability to de-quantize the Deutsch-Jozsa problem for various values of n in order to gain a better understanding of quantum algorithms and the ability for them to give exponential improvements over classical algorithms. We have extended the method of de-quantization presented in [4] to the $n = 2$ case, and by showing separability of the quantum algorithm for $n = 2$ have obtained a similar de-quantized solution.

We have shown that for $n > 2$ there exist many balanced boolean functions f for which the output of U_f is entangled. The fraction of balanced functions which are separable has been shown to approach zero very rapidly. This tells us that if we were to pick a random boolean function which is constant or balanced, the probability of being able to learn information about the nature of the function through classical means in one black box call tends to zero.

The systematic method of tackling quantum algorithms and searching for classical counterparts

makes it easier to see where quantum algorithms get their power from. Trying to understand this is an extremely important step in the process of trying to devise new quantum algorithms. In order to make good quantum algorithms with ease, we need to have a much better understanding than we currently do about where their power comes from, and how to use this effectively. In our investigation we obtained some conditions which, if satisfied, indicate de-quantization is possible. These kind of conditions, if explored further are a step towards better measures of the usefulness of a quantum algorithm.
An area that still needs to be looked into much further is that of the black box complexity. We have assumed that we are given a black box, as is usual in oracle computations. However, comparing algorithms which use different oracles should take into account the difference in complexity in these oracles. This has been largely ignored to date, but needs to be given systematic treatment if we really wish to compare quantum oracle algorithms with classical ones.

References

[1] Arvind. Quantum entanglement and quantum computational algorithms. *Pramana - Journal of Physics*, 56(2 & 3):357–365, Jan 2001.

[2] A. Berthiaume and G. Brassard. Oracle quantum computing. *Journal of Modern Optics*, 41(12):2521–2535, Dec. 1994.

[3] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor. Quantum computing without entanglement. *Theoretical Computer Science*, 320:15–33, 2004.

[4] C. S. Calude. De-quantizing the solution of Deutsch's problem. *International Journal of Quantum Information*, 5(3):409–415, Jun 2007.

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London A*, 1998(454):339–354, Jan 1997.

[6] D. Collins, K. W. Kim, and W. C. Holton. Deutsch-Jozsa algorithm as a test of quantum computation. *Physical Review A*, 58(3):R1633–R1636, Sep 1998.

[7] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97–117, Jan 1985.

[8] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439:553–558, Jan 1992.

[9] A. Ekert and R. Jozsa. Quantum algorithms: Entanglement enhanced information processing. *Philosophical Transactions of the Royal Society A*, 356(1743):1769–1782, 1998.

[10] M. S. Hannachi, F. Dong, Y. Hatakeyama, and K. Hirota. On the use of fuzzy logic for inherently parallel computations. In *3rd International Symposium on Computational Intelligence and Intelligent Informatics*, 2007.

[11] P. Jorrand and M. Mhalla. Separability of pure n-qubit states: two characterizations. *International Journal of Foundations of Computer Science*, 14(5):797–814, 2003.

[12] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.