The Deutsch-Jozsa Problem: De-quantisation and Entanglement

Alastair A. Abbott

Department of Computer Science, University of Auckland,
38 Princes St, Auckland 1010, New Zealand
aabb009@aucklanduni.ac.nz

July 17, 2017

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 one in exactly one black-box call. It has been found that in some cases the algorithm can be de-quantised into an equivalent classical, deterministic solution. We explore the ability to extend this de-quantisation to further cases, and examine with more detail when de-quantisation is possible, both with respect to the Deutsch-Jozsa problem, as well as in more general black-box algorithms.

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 result [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 Preliminaries

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

1

manner. A *classical algorithm* is one which is computed by a (probabilistic) Turing Machine or equivalent computational model, while a *quantum algorithm* is one which is computed by a uniformly generated sequence of circuits $G = G_{T(n)} \ldots G_1$, where each gate G_i is either a unitary gate (chosen from a fixed set), or a measurement gate [1].

Most quantum algorithms have a trivial classical counterpart via the simulation of their matrix-mechanical formulation. As long as one is careful,[1] equivalent classical algorithms can be readily obtained by these means [10]. However, the dimension of Hilbert space (and thus the representation of the state) 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, leaving such simulations inefficient. In this paper we examine the existence of more efficient classical counterparts to quantum algorithms that are not exponential in time or space compared to the quantum algorithm. Some previous work in this has been done by Jozsa and Linden, who looked at conditions for simulating the matrix formulation of an algorithm efficiently [13]. We will look at the same issue from a slightly different angle with respect to the Deutsch-Jozsa problem, as well as in a more general black-box situation.

Throughout this paper 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:

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

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 [3, 14]. 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 black-box structure alone allows insight into the nature of the black-box [9, p. 554].

In the current literature it is usually implicitly assumed that solving a problem with a classical black-box is equivalent to 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 two-dimensional Hilbert space ($\mathcal{H}_2$). This difference in some sense appears to add extra complexity and power to the quantum black-box, and it is not clear that solutions can easily be compared without taking this into account. Some questions relating to this issue are developed more fully in [1], and ongoing joint work with the University of York involves studying this in a

---

[1] If incomputable coefficients were used in the algorithm this simulation would clearly run into trouble, although it is not clear if such situations will arise in quantum computation. Alternatively, it has been shown quantum value indefiniteness allows quantum sources to generate incomputable sequences of bits [5]; quantum computers can be used as such a source and trying to simulate this behaviour will clearly fail on a classical computer.

physical Nuclear Magnetic Resonance implementation to gain further insight. In this paper we will adopt the standard stance and work with the natural generalisation of the classical black-box.

2 Deutsch's Problem

The original problem proposed by Deutsch [8] is formulated as follows: consider a Boolean function $f : \{0,1\} \rightarrow \{0,1\}$, and suppose we are given a black-box (oracle) to compute 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 [6] which solves Deutsch's problem with probability one 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. Since the classical black-box is not reversible it is embedded in the unitary quantum black-box described by the unitary operator U_f, an f-controlled-NOT (f-cNOT) gate, such that

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

In order to see how the quantum solution works, note that

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

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 $H^{\otimes 2}$, we get:

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

Next, operating on the state with U_f:

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

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

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

3

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

This quantum solution is correct with probability one using only one call to the quantum black-box represented by U_f. An important note is that this computation involves no entanglement, and the auxiliary qubit remains unchanged by U_f leaving the two qubits separable.[2] The power of this quantum solution seems to come only from parallelism and interference, not entanglement.

2.2 Classical Solutions

While the quantum algorithm makes use of quantum parallelism and interference, these qualities (unlike entanglement) are not inherently quantum mechanical; their physical presence in the computation may be of quantum mechanical origin, but the mathematical effect and ability to be present in classical systems is due to the two-dimensionality of qubits compared to the one-dimensionality of classical bits. Hence, the same computational advantage should be achievable in a classical two-dimensional computational system.

The first method, presented in [4], uses complex numbers as classical two-dimensional bits. The set $\{1, i\}$ acts as a computational basis in the same way that $\{|0\rangle, |1\rangle\}$ does for quantum calculations, and its elements can similarly be assigned the meanings of '0' and '1'. Since an arbitrary complex number may be written as $z = a + bi$ with $a, b \in \mathbb{R}$, a complex number z is a natural superposition of the basis elements in the same way that a qubit is.

Just as in the quantum case, we need to embed the original classical black-box computing f in one which operates on complex numbers. This black-box can be represented by an operator C_f, a direct analogue of U_f (although the requirement of unitarity is no longer necessary). The effect of C_f (cf. Equation 1) 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 ($C_f(x) = \pm \overline{x}$). In order to project our complex numbers back on to the computational basis, we multiply the black-box output by the input. Note that this is not a physical operation but an abstract mathematical one; in the quantum case we are forced to work in a physical computational embedding, but classically this is not the case.

If $z = 1 + i$ (an equal superposition of basis states),

$$\frac{1}{2} z \times C_f(z) = \begin{cases} \frac{\pm 1}{2} z^2 = \pm i & \text{if } f \text{ is constant,} \\ \frac{\pm 1}{2} z\overline{z} = \pm 1 & \text{if } f \text{ is balanced.} \end{cases}$$

---

[2] In this paper we take the terms 'separable', 'product-state' and 'unentangled' to have the same meaning since we deal only with pure states. As such, we do attempt to generalise the results to mixed-state computations; see [13] for a discussion of the difficulties in extending general de-quantisation results to mixed-states.

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, and in fact the sign of the output allows us to identify *which* balanced or constant function f is. This is something the quantum algorithm provably cannot do [15].

This process of finding a classical solution with the same complexity as the quantum solution for a problem informally corresponds to what we call de-quantisation. Formally, the requirements for a classical algorithm to be a de-quantisation are different depending on the type of problem being solved. Let $\mathcal{A}$ be quantum algorithm with complexity measure $f(n)$ and output probability distribution $\mathcal{P}$. A probabilistic Turing machine M, such that for every computable $\gamma > 0$ there effectively exists a probability distribution $\mathcal{P}'$ with $|\mathcal{P} - \mathcal{P}'| < \gamma$, and M sampling from $\mathcal{P}'$ has complexity measure $g(n, \gamma)$, is a potential de-quantisation of $\mathcal{A}$ [1]. For M to be a de-quantisation, g must satisfy certain requirements depending on the type of problem. For example, in a standard (non black-box) algorithm, $f(n) = T(n)$, the size of the circuit for $\mathcal{A}$, and M is a de-quantisation if $g(n, \gamma) = \text{poly}(T(n), \log(1/\gamma))$. In the Deutsch-Jozsa algorithm $f(n) = 1$ is the number of black-box calls, and M is a de-quantisation if $g(n, \gamma) = f(n)$, i.e. the classical solution must also use only one black-box call. For an overview and comparison of various de-quantisation techniques we refer the reader to [1], but we focus on entanglement based techniques in this paper.

The de-quantisation we have presented is only one possible method, and places emphasis on mathematical correspondence with the quantum solution. A different solution is presented by Arvind in [2] which draws physical similarities that are more visible than in the above solution. Arvind uses the polarisation of a photon (treated classically) as the computational basis $\{x\text{-pol}, y\text{-pol}\}$, and any polarisation in the xy-plane is physically valid. It is noted that all transformations in the group SU(2) can be realised by two quarter-wave plates and a single half-wave plate orientated suitably, and Deutsch's problem is solved using such transformations. Written in matrix form the solution is mathematically identical to the quantum one. This corresponds to the following physical process: preparing a photon with y-polarisation, rotating its polarisation anti-clockwise in the xy-plane by $45°$, applying the optical black-box and applying the anti-clockwise rotation once more before measuring the y-polarisation of the photon.

The correspondence here relies not on embedding classical bits in a different, classical two-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 (regardless of whether or not photons are actually quantum mechanical objects—they do not need to be treated as such).

3 The Deutsch-Jozsa Problem

This problem was extended by Deutsch and Jozsa [9] to functions on n-bit strings. The standard formulation of the Deutsch-Jozsa problem is 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 $x \in \{0,1\}^n$). Such a function f is called *valid*. The Deutsch-Jozsa problem is to determine if f is constant or balanced in as few black-box calls as possible. 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 is constant tends towards zero very quickly (recall f is guaranteed to be valid). Furthermore, the probability that any randomly chosen function of the 2^N possible functions is valid is:

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

which also tends to zero as n increases. This is clearly 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 $n = 1$:

$$U_f \ket{x} \ket{y} = \ket{x} \ket{y \oplus f(x)},$$

where $x \in \{0,1\}^2$. For $n = 2$ there are sixteen possible Boolean functions. Two of these are constant, another six are balanced and the remaining eight are not valid. All these possible functions are listed in Table 1.

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

$$U_{f'} |x\rangle |-\rangle = (-1)^{f'(x)} |x\rangle |-\rangle = -U_f |x\rangle |-\rangle \,.$$

In this case the result obtains a global phase factor of -1; this has no physical significance so 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

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

After applying the f-cNOT gate U_f we have

$$U_f \frac{1}{2} \sum_{x \in \{0,1\}^2} |x\rangle |-\rangle = \sum_{x \in \{0,1\}^2} \frac{(-1)^{f(x)}}{2} |x\rangle |-\rangle \,. \tag{3}$$

From the well known rule (see [12]) about 2-qubit separable states, we know that this state is separable if and only if $(-1)^{f(00)}(-1)^{f(11)} = (-1)^{f(01)}(-1)^{f(10)}$. By noting that the mapping $(-1)^{f(a)}(-1)^{f(b)} \leftrightarrow f(a) \oplus f(b)$ is a bijection, we see that the separability condition reduces to $f(00) \oplus f(11) = f(01) \oplus f(10)$. From Table 1 it is clear this condition must hold for all balanced or constant functions f for $n = 2$, and thus no entanglement is present in the $n = 2$ case.

We can now rewrite Equation 3 in a separable form as follows:

$$U_f |++\rangle |-\rangle = \frac{(-1)^{f(00)}}{2} \left(|0\rangle + (-1)^{f(00) \oplus f(10)} |1\rangle \right) \left(|0\rangle + (-1)^{f(10) \oplus f(11)} |1\rangle \right) |-\rangle \,. \tag{4}$$

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

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

By measuring both the first and second qubits we can determine the nature of f: 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-quantised in a similar way to the $n = 1$ case, but this time using two complex numbers as the input to the black-box. We extend the black-box to operate on two complex numbers, $C_f : \mathbb{C}^2 \to \mathbb{C}^2$, and define it by analogy to U_f just as we did for the $n = 1$ case. Let z_1, z_2 be complex numbers,

$$C_f \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = C_f \begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{pmatrix} = \begin{pmatrix} (-1)^{f(00)} \left[a_1 + (-1)^{f(00) \oplus f(10)} b_1 i \right] \\ a_2 + (-1)^{f(10) \oplus f(11)} b_2 i \end{pmatrix} \,. \tag{5}$$

If we let $z = z_1 = z_2 = 1 + i$, multiplying by z to project onto the computational basis as for the $n = 1$ case, we get:

$$\frac{z}{2} \times C_f \begin{pmatrix} z \\ z \end{pmatrix} = \frac{1}{2} \times \begin{cases} \begin{pmatrix} (-1)^{f(00)} z^2 \\ z^2 \end{pmatrix} = \begin{pmatrix} (-1)^{f(00)} i \\ i \end{pmatrix} & \text{if } f \text{ is constant,} \\[2em] \begin{pmatrix} (-1)^{f(00)} z\bar{z} \\ z^2 \end{pmatrix} = \begin{pmatrix} (-1)^{f(00)} \\ i \end{pmatrix} \\[1em] \begin{pmatrix} (-1)^{f(00)} z\bar{z} \\ z\bar{z} \end{pmatrix} = \begin{pmatrix} (-1)^{f(00)} \\ 1 \end{pmatrix} & \text{if } f \text{ is balanced.} \\[1em] \begin{pmatrix} (-1)^{f(00)} z^2 \\ z\bar{z} \end{pmatrix} = \begin{pmatrix} (-1)^{f(00)} i \\ 1 \end{pmatrix} \end{cases}$$

By checking 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. In fact, just as in the $n = 1$ case, the ability to determine if the output numbers are negative or positive allows us to determine the value of $f(00)$ and thus which Boolean function f is.

It is because of the separability of the quantum solution that it is possible to reproduce the ability to solve the problem with only one black-box call. If the quantum state was not separable there would be no embedding of the original black-box into one operating on two complex-bits which would allow us to determine the nature of f with only one black-box call.

As with the $n = 1$ case, an alternative classical approach can be presented using two photons. If a transformation on two qubits can be separated into a transformation on each qubit independently then the transformation is trivially implemented classically. As Arvind noted [2], the 2-qubit transformations U_f can be written in such a way since they are separable: from Equation 4 it is clear U_f can be written as a product of the two 1-qubit gates[3]

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

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

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

---

[3]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 [7]) that the auxiliary qubit is not necessary if we restrict ourselves to the subspace spanned by $|-\rangle$. 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-quantised solutions, however, bear more resemblance to this reduced version of U_f operating only on n qubits.

computed by applying a 1-qubit operation (implemented as wave-plates) to each photon independently, and thus a classical solution for $n = 2$ is easily found. 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 (although the latter is abstract and mathematical, while the former are physical). 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   Separability in the Deutsch-Jozsa problem

Before we consider de-quantisation of the Deutsch-Jozsa problem for $n \geq 3$, we will first examine the separability of the states used in the quantum solution more carefully, as determining if a state is separable is a key step in determining if an easy de-quantisation is possible. Conditions to determine if a n-qubit state is separable are presented in [12]. We will review these results, before reformulating them in a recursive manner which will allow us to apply these results much more easily to the Deutsch-Jozsa problem.

In order to determine if an arbitrary n-qubit state is separable, we must first introduce the concept of pair product invariance [12]. A state $|\psi_n\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ with $N = 2^n$ is *pair product invariant* if and only if $\forall k \in \{1, \ldots, n\}, \forall i \in \{0, \ldots, K-1\} : \alpha_i \alpha_{K-i-1} = c_k$, where each c_k is a constant and $K = 2^k$.

Pair product invariance can also be reformulated recursively. We let P_n be the set of all pairs (i, k) such that for any two elements $(a, k), (b, k) \in P_n$ we have $\alpha_a \alpha_{K-a-1} = \alpha_b \alpha_{K-b-1} = c_k$ if and only if $|\psi\rangle$ is pair product invariant. We can recursively write this by breaking up the iteration over all $k \in \{1, \ldots, n\}$. To do so we define P_l as:

$$P_l = \{(i, k) \mid k \in \{2, \ldots, l\}, i \in \{0, \ldots, 2^{k-1} - 1\}\}. \tag{6}$$

Recursively, this becomes:

$$P_l = P_{l-1} \cup \{(i, l) \mid i \in \{0, \ldots, 2^{l-1} - 1\}\}, \text{ with the base case}$$
$$P_2 = \{(0, 2), (1, 2)\}.$$

Theorem 1. *An n-qubit state $|\psi_n\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ is pair product invariant if and only if P_n, as defined by (6), satisfies the following condition: $\forall (a, k), (b, k) \in P_n : \alpha_a \alpha_{K-a-1} = \alpha_b \alpha_{K-b-1} = c_k$ where $K = 2^k$ and c_k is constant.*

Proof. Firstly, note that the base case, P_2, simply amounts to the well-known condition that $\alpha_{00} \alpha_{11} = \alpha_{01} \alpha_{10}$. We can modify the definition of pair product invariance by changing i to range from 0 to $2^{k-1} - 1$ instead of $K - 1$ since $\alpha_i \alpha_{K-i-1} = \alpha_{K-i-1} \alpha_i$, thus avoiding double counting. The $k = 1$ case can also be removed since it now reduces

9

to a single term, and is hence unnecessary. The definition of P_l in (6) ensures that the quantifier $\forall (a,k),(b,k) \in P_n$ runs for $k \in \{2,\ldots,n\}$, $a,b \in \{0,\ldots,2^{k-1}-1\}$. It is then clear to see that the required condition is satisfied by P_n if and only if $|\psi\rangle$ is pair product invariant. $\qquad \square \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

The main theorem of relevance to us regarding pair product invariance is Theorem 2 below.

Theorem 2 (Theorem 1 in [12]). *If $\forall i \in \{0,\ldots,N-1\} : \alpha_i \neq 0$, a state $|\psi_n\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ is fully separable if and only if it is pair product invariant.*

Hence, in order to determine if a state $|\psi_n\rangle$ is separable we can simply apply Theorems 1 and 2. The recursive formulation of pair product invariance will prove more useful to develop general results on separability.

Note that any constant function produces a pair product invariant state, as all α_i are equal and the conditions are trivially satisfied. The output of the quantum black-box for constant f can be separated as:

$$\frac{1}{2^{n/2}} U_f \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle$$

$$= \frac{(-1)^{f(00)}}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle$$

$$= (-1)^{f(00)} |+\rangle^{\otimes n} |-\rangle.$$

5.1 The case of $n \geq 3$

For $n = 3$ we are able to find balanced functions which do not produce pair product invariant states, and thus, by Theorem 2, these states are entangled.

If we choose f such that

$$(f(0),f(1),f(2),f(3),f(4),f(5),f(6),f(7)) = (0,0,0,1,1,1,1,0),$$

then this f is obviously balanced. For this choice of f, $f(000) \oplus f(011) \neq f(001) \oplus f(010)$. This implies that $\alpha_{000}\alpha_{011} \neq \alpha_{001}\alpha_{010}$ and hence the output of U_f in the standard quantum algorithm is not pair product invariant and is thus entangled.

The recursive formulation of pair product invariance allows us to determine exactly how many separable states exist for any given n. Theorem 1, along with the fact that $P_n \subset P_{n+1}$, means that for a function f_{n+1} to produce a separable state, the first n qubits of the resulting state must be pair product invariant. Hence we see that all functions f_{n+1} which produce separable states are based on another such function f_n, and hence satisfy $f_{n+1}(0 \circ x_n) = f_n(x_n), \forall x_n \in \{0,1\}^n$, where $0 \circ x_n$ 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. Figure 1 shows this nature of pair product invariance.
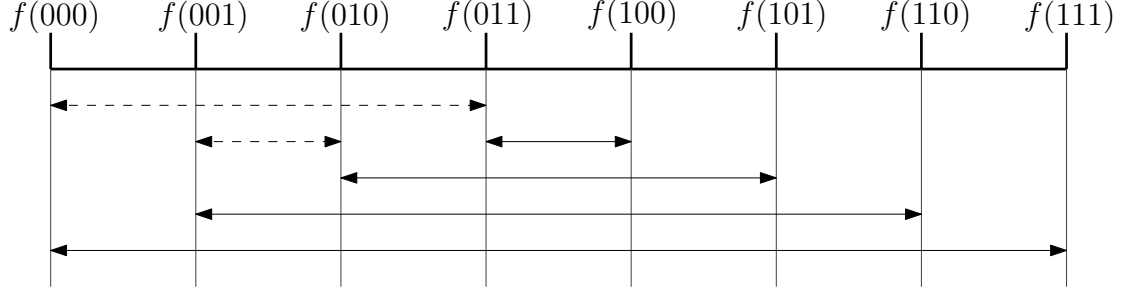
Figure 1: A diagram showing the recursive nature of pair product invariance. All pairs of states linked by the same type of arrow must have the same parity under addition modulo 2.

The action of f_{n+1} on the remaining $N = 2^n$ input strings is determined by Theorem 1. This requires that $\alpha_{N-1}\alpha_N = \alpha_{N-2}\alpha_{N+1} = \cdots = \alpha_0\alpha_{2N-1}$. Since α_{N-1} is already determined, α_N can take on two possible values. However, once this value is chosen, all α_i for $i > N$ are uniquely determined by the Theorem 1. If we let a_n be the number of functions f_n which produce separable states, then f_{n+1} can have a_n possible configurations for acting on $f_{n+1}(0 \circ x_n)$, and for each of these configurations, there are two configurations for the remaining N input strings, hence $a_{n+1} = 2a_n$. Using the fact that $a_1 = 4$ we get 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 that 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. Further, we can verify that for all $n \geq 3$ there exist valid functions f such that the output of the black-box is *maximally* entangled, i.e. all n qubits are entangled together.

Proposition 3. *For all $n \geq 3$ there exists a valid $f : \{0,1\}^n \to \{0,1\}$ such that the first n qubits of $U_f |+\rangle^{\otimes n} |-\rangle = |\psi\rangle |-\rangle$ are all entangled.*

Proof. Firstly we note that if any qubit is separable from the rest, a specific sub-structure is present in the state-vector. Without loss of generality assume the ith qubit, $|\psi_i\rangle$, is separable from the rest, and let $|\psi'\rangle = |\psi_1\rangle \cdots |\psi_{i-1}\rangle |\psi_{i+1}\rangle \cdots |\psi_n\rangle$ be the state of the other

$n-1$ qubits. Since all the amplitudes in $|\psi\rangle$ are $\pm 2^{-n/2}$, we know $|\psi_i\rangle = |\pm\rangle = (1, \pm 1)$—we use the state-vector notation with normalisation implicit. Let us write the state vector of $|\psi'\rangle$ in blocks of size 2^{n-i} as $|\psi'\rangle = (\mathbf{x}_1, \ldots, \mathbf{x}_{2^{i-1}})$. Because of the symmetry in the state vector due to the tensor-product we have $|\psi\rangle = (\mathbf{x}_1, \pm\mathbf{x}_1, \ldots, \mathbf{x}_{2^{i-1}}, \pm\mathbf{x}_{2^{i-1}})$ where all the signs ± 1 are identical. The function defined by

$$f(a) = \begin{cases} 0 & \text{for } a = 0, 1, \ldots, 2^{n-1} - 2, 2^n - 2, \\ 1 & \text{elsewhere,} \end{cases}$$

is clearly valid, but the corresponding state $|\psi\rangle$ for this f is

$$|\psi\rangle = (\underbrace{1, \ldots, 1, 1}_{2^{n-1}-1 \text{ times}}, -1, \underbrace{-1, \ldots, -1}_{2^{n-1}-2 \text{ times}}, 1, -1),$$

which can easily be verified to not have the required sub-structure, and is thus maximally entangled. $\qquad\square\qquad\qquad\qquad\qquad\square$

The result of these observations is that even if we are promised f is valid, 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. Since any de-quantisation would have to handle maximally entangled outputs of the black-box, this method of de-quantisation used for $n = 1, 2$ will not scale easily to higher n, and in general yields very little information about the nature of a function. Looking at this from the view of computation with classical photons, there is no classical physical equivalent of entangled photons, as this is a purely quantum mechanical effect. However, in general it is very hard to show that no de-quantisation 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-quantisation is possible, but to show no better de-quantisation exists is very hard. As an example, Jozsa and Linden showed [13] that using the stabiliser description of quantum computation [11] it is possible to find an efficient classical simulation of a quantum algorithm containing unbounded entanglement.

6   General de-quantisation

While de-quantisation appears to be very hard in the Deutsch-Jozsa problem for $n \geq 3$, we can investigate the general ability to de-quantise black-box algorithms. The main task in trying to de-quantise such an algorithm is to de-quantise the black-box. Indeed, efficiently simulating a black-box algorithm requires finding a classical black-box embedding which doesn't use an exponentially increasing amount of time or space. Using the methods looked at in this paper, this step would initially require showing that both the input and output of the black-box are separable.

Firstly, we will summarise some important results due to Jozsa and Linden [13], who examined the ability to efficiently simulate standard quantum algorithms by simulating

the matrix mechanical formulation of these algorithms. We call a qubit register $|\psi\rangle$ p-blocked if at every step of the computation no subset of more than p qubits are entangled. Their main result is Theorem 4.

Theorem 4. *Let $\mathcal{A}$ be a quantum algorithm with the properties that only the final gate is a measurement gate, and after every unitary gate application the state $|\psi\rangle$ is p-blocked, with p independent of the input size n. Then the algorithm $\mathcal{A}$ can be de-quantised using the matrix formulation.*

The proof relies on breaking up the $2^n \times 2^n$ matrices describing the gates with which the circuits in $\mathcal{A}$ are composed of into matrices operating on no more than $2p$ qubits at once.[4] Each matrix corresponding to a gate is replaced by a single matrix no larger than $2^{2p} \times 2^{2p}$. Since p is constant, the cost of directly simulating the quantum algorithm by matrix multiplication can be reduced to a linear overhead, exponential in p rather than n.

This fixed-parameter tractability approach is mathematically equivalent to our approach, although our approach has the advantage that it retains more similarity to the quantum algorithms. Our method can also be easier to apply and produces simpler results than blind simulation of the matrix mechanics, and also more easily extends to the setting of black-box computation. The approach used by Jozsa and Linden does not directly apply to black-box computation where the nature of the black-box is unknown. It could readily be adapted by having the black-box perform a set of matrix multiplications, but such an approach is less natural. We will explore applying our de-quantisation method to arbitrary separable black-box computations since it is easier to examine and work with. Note that it is also not surprising that de-quantisation does not easily extend in the Deutsch-Jozsa problem since we have shown the entanglement grows exponentially.

The simplest case to tackle for de-quantising an arbitrary black-box algorithm is the case that both the input and output of the black-box U_f can be expressed in a separable form. In this case we can show how a simple de-quantisation in the spirit presented previously can easily be obtained. A nice feature which makes de-quantisation of a black-box algorithm simple is that we do not have to worry about considering the separability of the decomposition of the gate, as it is supplied as an arbitrarily complex unitary gate, not necessarily decomposed into gates from a universal basis (indeed, we have no way of knowing how the black-box is devised). If we knew that the input and output of U_f were separable, but had to decompose it into smaller unitary gates, we could not guarantee separability throughout the decomposed circuit representing U_f. However, the unitarity of U_f, regardless of its dimension, will allow a simple de-quantisation.

Theorem 5. *Let U_f be the unitary operator representing the black-box such that U_f never entangles its input in the quantum algorithm $\mathcal{A}$, i.e. both the input and output of*

---

[4]The $2p$ comes about rather than p in the case where a 2-qubit gate may operate on qubits from two separate entangled blocks. This approach assumes the circuit is decomposed into 1-qubit and 2-qubit gates.

U_f are separable. Then $\mathcal{A}$ can be de-quantised into a classical algorithm with the same number of black-box calls.

Proof. We can write the action of U_f under these assumptions as

$$U_f \left|\psi_1\right\rangle \left|\psi_2\right\rangle \cdots \left|\psi_n\right\rangle = \left|\phi_1\right\rangle \left|\phi_2\right\rangle \cdots \left|\phi_n\right\rangle, \tag{7}$$

and hence we can write $U_f = U_f^{(1)} \otimes U_f^{(2)} \otimes \cdots \otimes U_f^{(n)}$, where each $U_f^{(i)}$ acts on the ith qubit only. Since the quantum amplitudes can, in general, be complex-valued, we give a general construction of the classical black-box C_f acting on complex-vectors rather than the complex-bits we used previously. This method amounts to simulating the matrix-mechanical formulation, much as in Theorem 4. Let

$$U_f^{(i)} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then define

$$C_f \begin{pmatrix} (\alpha_1, \beta_1) \\ \vdots \\ (\alpha_n, \beta_n) \end{pmatrix} = \begin{pmatrix} (a\alpha_1 + b\beta_1, c\alpha_1 + d\beta_1) \\ \vdots \\ (a\alpha_n + b\beta_n, c\alpha_n + d\beta_n) \end{pmatrix}.$$

A de-quantisation of $\mathcal{A}$ can then simulate the matrix evolution of the quantum algorithm, but replace queries to the quantum black-box by ones to the classical black-box represented by C_f operating on n two-component vectors. Thus the de-quantised algorithm will call the black-box exactly the same number of times as the quantum one. □ □

This shows that, as expected, a quantum black-box algorithm can be de-quantised easily into an equivalent classical algorithm if the black-box never entangles the input. Note that while the de-quantised algorithm might be inefficient with respect to time, the number of black-box calls is the same as for the quantum algorithm. This black-box de-quantisation could be extended to allow bounded entanglement as in Theorem 4. If entanglement is bounded throughout the whole algorithm, Theorem 4 will guarantee the de-quantisation is also efficient in time. These de-quantisation tools provide a useful technique of developing new classical algorithms from ones which are more naturally expressed in the quantum world. If unbounded entanglement is present, a successful de-quantisation will need to handle the problem using a different representation of the process.

7   Conclusion

We have examined the ability to de-quantise 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 de-quantisation presented in [4] to the $n = 2$ case by utilising separability of the quantum algorithm. 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 helps us 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 conditions for which, if satisfied, indicate a black-box algorithm can be de-quantised. These kind of conditions, if explored further, are a step towards better measures of the usefulness of quantum algorithms.

An area that still needs to be looked into much further is that of the black-box complexity. It is not clear the standard procedure of ignoring the differences in complexity between quantum and classical black-boxes is entirely valid. Without a proper method to compare different types of black-box algorithms it is hard to convincingly claim one is better than the other, because they might not be solving quite the same problem. We see this as an important issue to investigate further.

Acknowledgment

References

[1] A. A. Abbott and C. S. Calude. Understanding the quantum computational speed-up via de-quantisation. *EPTCS*, 26:1–12, 2010.

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

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

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

[5] C. S. Calude and K. Svozil. Quantum randomness and value indefiniteness. *Advanced Science Letters*, 1(165–168), 2008.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] D. Gottesman. The heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1999.

[12] 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.

[13] R. Jozsa and N. Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings: Mathematical, Physical and Engineering Sciences*, 459(2036):2011–2032, Jan 2003.

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

[15] N. D. Mermin. *Quantum Computer Science*. Cambridge University Press, 2007.