

# The Deutsch–Jozsa problem: de-quantisation and entanglement

Alastair A. Abbott

Published online: 24 August 2011  
© Springer Science+Business Media B.V. 2011

**Abstract** The Deutsch–Jozsa problem is one of the most basic ways to demonstrate the power of quantum computation. Consider a Boolean function  $f: \{0, 1\}^n \rightarrow \{0, 1\}$  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 cases.

**Keywords** Quantum computing · Deutsch–Jozsa problem · De-quantisation · Classical simulation

## 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 (Calude 2007) 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,  $U = U_L U_{L-1} \dots U_1$ . 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 (Ekert and Jozsa 1998). 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.  $|0\rangle, |1\rangle$  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. 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 (Jozsa and Linden 2003). 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 situation.

---

A. A. Abbott (✉)  
Department of Computer Science, University of Auckland,  
Auckland, New Zealand  
e-mail: aabb009@aucklanduni.ac.nz

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 (Biham et al. 2004):

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

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

## 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 (Berthiaume and Brassard 1994; Kitaev et al. 2002). 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 (Deutsch and Jozsa 1992, 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 two-dimensional Hilbert space ( $\mathcal{H}_2$ ). 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 (1985) 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 Cleve et al. (1998) 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. 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:

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

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  $U_f$ :

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

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 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. 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

While the quantum algorithm makes use of quantum parallelism and interference, 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 be able to achieve the same result as the quantum algorithm.

The first method, presented in Calude (2007), embeds classical bits in complex numbers. The set  $\{1, i\}$  (where  $i = \sqrt{-1}$ ) 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.

An arbitrary complex number may be written as  $z = a + bi$  with  $a, b \in \mathbb{R}$ , so a complex number  $z$  is a natural superposition of the basis elements in the same way that a qubit is. We are now given a classical black-box which operates on complex numbers and computes our function  $f$ . 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  $C_f$  (in direct correspondence with  $U_f$ , although the normalisation 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  $\mathcal{H}_2$ . 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),

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

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 (Mermin 2007).

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 (2001) 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-quantisation*. This term was first used by Calude (2007), but the methods used by Arvind (2001), Hannachi et al.(2007) for example would also classify as de-quantisations.

Arvind uses the (classical) polarisation of a photon 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. 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 with  $y$ -polarisation, rotating its polarisation anti-clockwise in the  $xy$ -plane by  $45^\circ$ , 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.

## 3 The Deutsch–Jozsa problem

This problem was extended by Deutsch and Jozsa (1992) to functions on  $n$ -bit strings. The standard formulation of the Deutsch–Jozsa problem is as follows: let  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ , 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  $n = 1$ :

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

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.

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

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

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

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

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

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

From the well known rule (see Jorrand and Mhalla 2003) 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 Eq. 1) that is used in this algorithm. The situation is further simplified by noting that the mapping  $(-1)^{f(a)}(-1)^{f(b)} \leftrightarrow f(a) \oplus f(b)$  is a bijection. In this case, the separability condition reduces to  $f(00) \oplus f(11) = f(01) \oplus f(10)$ . By looking back at Table 1 it is clear this condition must hold for all balanced or constant functions  $f$  for  $n = 2$ .

We can now rewrite Eq. 2 as follows:

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

Indeed,

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

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

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

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

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

By measuring both the first and second qubits we can determine the nature of  $f$ : 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,  $C_f : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ , 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,

$$\begin{aligned} C_f \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} &= C_f \begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \end{pmatrix} \\ &= (-1)^{f(00)} \begin{pmatrix} a_1 + (-1)^{f(00) \oplus f(10)} b_1 i \\ a_2 + (-1)^{f(10) \oplus f(11)} b_2 i \end{pmatrix}. \end{aligned} \quad (4)$$

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:

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

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

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

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

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-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. 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.

<sup>1</sup> 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 Collins et al. 1998) 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.



## 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 Jorrand and Mhalla (2003). 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 (Jorrand and Mhalla 2003). 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  $\forall k \in \{1, \dots, n\}, \forall i \in \{0, \dots, K-1\} : \alpha_{i \oplus 2^{k-1}} = \alpha_i \alpha_{K-i-1} = c_k$ , 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  $k \in \{1, \dots, n\}$ . To do so we define  $P_l$  as:  $P_l = \{(i, k) \mid k \in \{2, \dots, l\}, i \in \{0, \dots, 2^{k-1} - 1\}\}$ . (5)

Recursively, this becomes:

$$P_l = P_{l-1} \cup \{(i, l) \mid i \in \{0, \dots, 2^{l-1} - 1\}\}$$

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 (5), 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 to a single term, and is hence unnecessary. The definition of  $P_l$  in (5) ensures that the quantifier  $\forall (a, k), (b, k) \in P_n$  runs for  $k \in \{2, \dots, n\}$ ,  $a, b \in \{0, \dots, 2^{k-1} - 1\}$ . 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.

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

**Theorem 2** (Theorem 1 in Jorrand and Mhalla (2003)) If  $\forall i \in \{0, \dots, N-1\} : \alpha_i \neq 0$ , 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  $\alpha_i$  are equal and the conditions are trivially satisfied. The output of the quantum black-box for constant  $f$  can be separated as:

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

### 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

$$\begin{aligned} (f(0), f(1), f(2), f(3), f(4), f(5), f(6), f(7)) \\ = (0, 0, 0, 1, 1, 1, 1, 0), \end{aligned}$$

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 definition 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.

The action of  $f_{n+1}$  on the remaining  $N = 2^n$  input strings is determined by Theorem 1. This requires that  $\alpha_{N-1} \alpha_N = \alpha_{N-2} \alpha_{N+1} = \dots = \alpha_0 \alpha_{2N-1}$ . Since  $\alpha_{N-1}$  is already determined,  $\alpha_N$  can take on two possible values. However, once this value is chosen, all  $\alpha_i$  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,

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

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 that the number of possible functions  $f_n$  which are either balanced or constant is

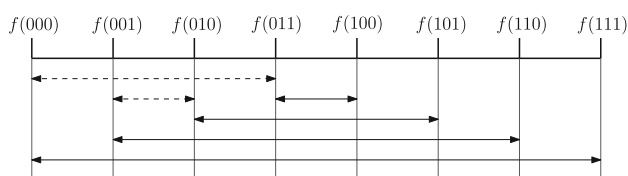
$$b_n = \binom{N}{N/2} + 2 = \binom{2^n}{2^{n-1}} + 2.$$

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  $n$ .

The result of this observation 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. This means that the method of de-quantisation used for  $n = 1, 2$  will not scale directly 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 (2003) that using the stabiliser description of quantum computation it is possible to find an efficient classical simulation of a quantum algorithm containing unbounded entanglement.



**Fig. 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

## 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 which solves the problem without requiring exponential 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 (2003), who examined the ability to efficiently simulate standard quantum algorithms by simulating the matrix mechanical formulation of these algorithms. This formalism is a little more abstract than the de-quantisation method used in this paper, but is an effective method of showing general results. 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 3.

**Theorem 3** *Let  $\mathcal{A}$  be a quantum algorithm with the property that after every unitary gate application the state  $|\psi\rangle$  is  $p$ -blocked, with  $p$  independent of 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.<sup>2</sup> 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. It can also be easier to apply and produces simpler results than blind simulation of the matrix mechanics. Our method 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

<sup>2</sup> 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.

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 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 4** *Let  $U_f$  be the unitary operator the black-box represents, and assume that for the set of input states used by the quantum algorithm  $\mathcal{A}$  we wish to de-quantise, both the input and output  $U_f$  are separable. Then the black-box can be de-quantised into an efficient classical solution.*

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

$$U_f|\psi_1\rangle|\psi_2\rangle\cdots|\psi_n\rangle = |\phi_1\rangle|\phi_2\rangle\cdots|\phi_n\rangle.$$

Since  $U_f$  is unitary, there must exist a unitary inverse  $U_f^\dagger$ , which has the effect

$$U_f^\dagger|\phi_1\rangle|\phi_2\rangle\cdots|\phi_n\rangle = |\psi_1\rangle|\psi_2\rangle\cdots|\psi_n\rangle.$$

From (6) we see that each qubit undergoes the transformation  $|\psi_i\rangle \rightarrow |\phi_i\rangle$ , but we must show this transformation is unitary. Let us write  $U_f = U_f^{(1)} \otimes U_f^{(2)} \otimes \cdots \otimes U_f^{(n)}$ , where each  $U_f^{(i)}$  acts on the  $i$ th qubit to implement this single-qubit transformation. Since the tensor product is distributive with respect to adjoints, we can write  $U_f^\dagger = (U_f^{(1)})^\dagger \otimes (U_f^{(2)})^\dagger \otimes \cdots \otimes (U_f^{(n)})^\dagger$ . Hence, we see that  $U_f^{(i)}|\psi_i\rangle = |\phi_i\rangle$  and  $(U_f^{(i)})^\dagger|\phi_i\rangle = |\psi_i\rangle$ . Thus the single qubit transformation is indeed unitary and we can write  $U_f$  as the product of single-qubit unitary transformation above. It is then clear to see that de-quantisation of the black box is possible. Evidently, the optical method we previously employed can trivially be used since each  $U_f^{(i)} \in \text{SU}(2)$  and the black-box is then constructed out of wave

plates. We only need to prepare the  $n$  photons in the correct state, operate on them with the black-box and continue the rest of the algorithm with the transformed photons. Equivalently, a method using two-dimensional classical bits such as complex numbers could easily be used.  $\square$

This shows that, as expected, a quantum black-box algorithm can be de-quantised easily into an equivalent classical algorithm if no entanglement is present. This black-box de-quantisation could be extended to allow bounded entanglement as in Theorem 3, although the photon method would no longer be sufficient since we would have unitary transformations not in  $\text{SU}(2)$ . However, higher-dimensional classical bits could easily be used. We will not explore this explicitly further, but this result on black-box simulation along with the result on standard algorithm de-quantisation allow for a powerful tool to assess quantum computations. 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 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 method of de-quantisation presented in Calude (2007) to the  $n = 2$  case, and by showing separability of the quantum algorithm for  $n = 2$  have obtained a similar de-quantised 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 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. We have assumed that we are given a black-box, as is usual in oracle computations. However, comparing algorithms which use different types of black-boxes should take into account the difference in complexity in these black-boxes. 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.

**Acknowledgment** The author would like to thank Prof. Cristian Calude for motivating this research and many subsequent discussions about de-quantisation.

## References

- Arvind (2001) Quantum entanglement and quantum computational algorithms. *Pramana J Phys* 56(2–3):357–365
- Berthiaume A, Brassard G (1994) Oracle quantum computing. *J Mod Opt* 41(12):2521–2535
- Biham E, Brassard G, Kenigsberg D, Mor T (2004) Quantum computing without entanglement. *Theoret Comput Sci* 320: 15–33
- Calude CS (2007) De-quantizing the solution of Deutsch’s problem. *Int J Quantum Inf* 5(3):409–415
- Cleve R, Ekert A, Macchiavello C, Mosca M (1997) Quantum algorithms revisited.. *Proc R Soc Lond A* 1998(454):339–354
- Collins D, Kim KW, Holton WC (1998) Deutsch–Jozsa algorithm as a test of quantum computation. *Phys Rev A* 58(3):R1633–R1636
- Deutsch D (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc R Soc Lond A* 400: 97–117
- Deutsch D, Jozsa R (1992) Rapid solution of problems by quantum computation. *Proc R Soc Lond A* 439:553–558
- Ekert A, Jozsa R (1998) Quantum algorithms: entanglement enhanced information processing. *Philos Trans R Soc A* 356(1743): 1769–1782
- Hannachi MS, Dong F, Hatakeyama Y, Hirota K (2007) On the use of fuzzy logic for inherently parallel computations. In: 3rd International Symposium on Computational Intelligence and Intelligent Informatics
- Jorrand P, Mhalla M (2003) Separability of pure  $n$ -qubit states: two characterizations. *Int J Found Computer Sci* 14(5):797–814
- Jozsa R, Linden N (2003) On the role of entanglement in quantum-computational speed-up. *Proc Math Phys Eng Sci* 459(2036): 2011–2032
- Kitaev AY, Shen AH, Vyalii MN (2002) Classical and quantum computation. American Mathematical Society, Boston
- Mermin ND (2007) Quantum computer science. Cambridge University Press, Cambridge

Copyright of Natural Computing is the property of Springer Science & Business Media B.V. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.