

Understanding the Quantum Computational Speed-up via De-quantisation

Alastair A. Abbott and Cristian S. Calude

Department of Computer Science
University of Auckland
Private Bag 92019, Auckland, New Zealand
www.cs.auckland.ac.nz/~{aabb009,cristian}

While it seems possible that quantum computers may allow for algorithms offering a computational speed-up over classical algorithms for some problems, the issue is poorly understood. We explore this computational speed-up by investigating the ability to de-quantise quantum algorithms into classical simulations of the algorithms which are as efficient in both time and space as the original quantum algorithms.

The process of de-quantisation helps formulate conditions to determine if a quantum algorithm provides a real speed-up over classical algorithms. These conditions can be used to develop new quantum algorithms more effectively (by avoiding features that could allow the algorithm to be efficiently classically simulated), as well as providing the potential to create new classical algorithms (by using features which have proved valuable for quantum algorithms).

Results on many different methods of de-quantisations are presented, as well as a general formal definition of de-quantisation. De-quantisations employing higher-dimensional classical bits, as well as those using matrix-simulations, put emphasis on entanglement in quantum algorithms; a key result is that any algorithm in which the entanglement is bounded is de-quantisable. These methods are contrasted with the stabiliser formalism de-quantisations due to the Gottesman-Knill Theorem, as well as those which take advantage of the topology of the circuit for a quantum algorithm.

The benefits of the different methods are contrasted, and the importance of a range of techniques is emphasised. We further discuss some features of quantum algorithms which current de-quantisation methods do not cover.

1 Introduction

Since Feynman first introduced the concept of a quantum computer [13] and noted the apparent exponential cost to simulate general quantum systems with classical computers there has been much interest in the power of quantum computation, in particular the possibility of using quantum physics to develop algorithms which are more efficient than classical ones. Many quantum algorithms (e.g. Deutsch's algorithm) have been claimed to be superior to any classical one solving the same problem, only to be discovered later that this was not the case. In order to construct good quantum algorithms it is important to know what features are necessary for a quantum algorithm to be better than a classical one. Many quantum algorithms have a trivial classical counterpart: with care, all the operations in the matrix mechanical formulation of quantum mechanics can be computed by classical means [12]. In this paper we review the ability to *de-quantise* a quantum algorithm to obtain a classical algorithm which is not exponentially slower in time (or larger in space) compared to the quantum algorithm, and explore when such a de-quantisation is possible.

2 A Preliminary Example

2.1 The Deutsch-Jozsa Problem

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. for all $x \in \{0, 1\}^n$ and some $a \in \{0, 1\} : f(x) = a$) 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. A typical classical algorithm would require 2^{n-1} black-box calls, while the quantum solution requires only one.

The special case of $n = 1$ was first considered by [11] and is called the Deutsch problem; this was de-quantised by Calude [10].¹

It is important to note that unlike 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 . In this finite class, exactly two functions are constant and $\binom{N}{N/2}$ are balanced. Evidently the probability that a valid function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is constant tends towards zero very quickly (recall that in Deutsch-Jozsa problem, f is guaranteed to be valid). Furthermore, the probability that any randomly chosen function of the 2^N possible functions is valid is $(\binom{N}{N/2} + 2) \cdot 2^{-N}$, which again tends to zero as n increases. This is clearly not an ideal problem to work with, however even in this case we can gain, via de-quantisation, useful information.

2.1.1 Quantum Solution

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 $x \in \{0, 1\}^2$. 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	1	0	1	0	1	0	0	1
$f(01) =$	0	1	0	1	1	0	0	1	1	0	1	0	1	0
$f(10) =$	0	1	1	0	1	0	1	0	1	0	0	1	1	0
$f(11) =$	0	1	1	0	0	1	0	1	0	1	1	0	1	0

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

Evidently, half of these functions are simply the negation of another. If we let $f'(x) = f(x) \oplus 1$ and define $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, we have:

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

¹Apparently, in this article the term 'de-quantisation' was used for the first time.

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.

We will present a revised form of the standard quantum solution in which we emphasise separability of the output state. We initially prepare our system in the state $|00\rangle|1\rangle$, and then operate on it with $H^{\otimes 3}$ to get:

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

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

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

From the well known rule (see e.g [17]) for the separability of 2-qubit 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. 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 holds for all balanced or constant functions f for $n = 2$.

We can now rewrite Equation 2 as follows:

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

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

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

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. This is correct with probability-one.

2.1.2 De-quantising the Quantum Solution

Because the quantum solution contains no entanglement, the problem can be de-quantised by embedding classical bits in complex numbers [10, 2]. The set $\{1, i = \sqrt{-1}\}$ acts as a computational basis in the same way that $\{|0\rangle, |1\rangle\}$ does for quantum computation.² A complex number may be written as $z = a + bi$, so z is a natural superposition of the basis in the same way that a qubit is.

²While we are not labelling 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.

We are now given a classical black-box that computes the function f . Similarly to U_f , the black-box operates on two complex numbers, $C_f : \mathbb{C}^2 \rightarrow \mathbb{C}^2$. Let z_1, z_2 be complex numbers,

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

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. Note, however, that in a quantum system it is impossible to measure entangled qubits independently of each other.

To simulate a Hadamard gate we multiply each of the complex numbers that the black-box outputs by their respective inputs. If we let $z_1 = z_2 = 1 + i$, we obtain the following:

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

By measuring both 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, 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. Interestingly, this de-quantisation is equivalent [3] to the ‘physical de-quantisation’ using classical photon polarisations described by Arvind in [7].

2.1.3 Implementing the De-quantised Solution

It is only natural to ask the question: how efficiently can we physically implement the de-quantised solution presented in Section 2.1.2? There are different possible approaches, but we will discuss only one.

Nuclear magnetic resonance (NMR) spectroscopy [20] exploits the spin dynamics of nuclear spin systems; it involves placing a sample in a strong external magnetic field and hence a splitting of the nuclear spin energy levels (Zeeman splitting). The corresponding resonance frequencies (Larmor frequencies) are typically of the order of hundreds of MHz. NMR spectroscopy is a rich source of information as spectra reflect interactions of nuclear spins with their electronic environment as well as interactions (couplings) between nuclear spins themselves.

In particular, solution-state NMR has been extensively examined as a possible implementation platform for quantum computations. This approach relies on couplings between spins within molecules and the manipulation of such finite-sized spin systems with appropriate pulse sequences. For example, Shor's algorithm has been successfully implemented in a 7-qubit NMR quantum computer [28].

A new approach proposed in [24] uses NMR as a classical computing substrate, where interactions between spins play no role and where the dynamics of these isolated spins can be fully described by a classical vector model. The technical difficulties of instability and decoherence present in quantum computation with NMR are less of an issue in this classical approach as their major source (internuclear couplings) is absent. Three different implementations have been demonstrated to simulate logic gates and other more complicated classical circuits. By making suitable choices of input and output parameters from the parameter space describing the NMR experiment, one can achieve different types of classical computations. The available parallelism, stability and ease in implementing two-dimensional classical bits (e.g. based on the three-dimensional vector model, or using two different spin species) makes NMR a well-suited substrate for implementations of de-quantised solutions of quantum algorithms. Work in progress of the groups in York (UK) and Auckland (NZ) involves NMR implementations of the de-quantised algorithms for the Deutsch-Josza problem described in Section 2.1.

3 Benefits

The above example allows us to enumerate a few 'immediate' benefits of de-quantisation as well as some long-term possible benefits:

- an example of a problem previously thought to be classically impossible to solve, was solved by 'de-quantising' a quantum solution;
- the solution is not uniform, so not ideal. It seems hard to analyse the complexity (asymptotically) of the de-quantised solution;
- the de-quantised solution is stronger than the original quantum one: it is deterministic and it can distinguish between functions not only classes (balanced/constant);
- via de-quantisation, a new classical computational technique was proposed;
- the lack of entanglement³ 'allowed' this type of de-quantisation;
- de-quantisation is not only theoretical: it can lead to efficient implementations.

De-quantisation can be one technique (among others) used to gain a better understanding of complexity in quantum computation, which can help to:

- understand the power and need for quantum computation;
- more clearly see where quantum speed ups potentially come from;
- develop new quantum algorithms.

4 De-quantisation

Until now we have used the term 'de-quantisation' in an intuitive sense, so it is time to propose a more formal definition.

³Just one type of many features which leads to de-quantisation;

In the most general sense, a quantum circuit C_n for a computation operating on an n -qubit input can be considered a sequence of gates $G = G_{T(n)} \dots G_1$, where each gate is either a unitary gate chosen from a fixed, finite set of gates \mathcal{G} , or a measurement gate. We can define a quantum algorithm in a similarly general sense. A quantum algorithm \mathcal{A} is an infinite, uniformly generated, sequence of quantum circuits (C_0, C_1, \dots) . We say the algorithm runs in time $T(n)$ if C_n contains $T(n)$ gates.

Many well known algorithms fall into the class BQP, which where $T(n) = \text{poly}(n)$ and $C_n = M_{T(n)} U_{T(n)-1} \dots U_1$, where the $U_i \in \mathcal{G}$ are unitary and $M_{T(n)}$ is a measurement gate [16]. In other words, measurement is the last step of the algorithm. However, the definition of a quantum computation is more general than this, and any de-quantisation should be equally able to handle intermediate measurements and any other reasonable requirements.

A classical algorithm is a program for a probabilistic Turing machine or any other computationally equivalent model of classical computation. The random access program machine is a particularly useful variation which operates with an infinite set of distinguishable, numbered, but unbounded registers each of which can contain an integer. Such a program has the capability for indirect addressing (i.e. the contents of a register can be used as an address to specify another register), thus allowing for optimisations based on memory indices [8].

A quantum algorithm (C_0, C_1, \dots) running in time $T(n)$, with output probability distribution \mathcal{P} , given by a classical Turing machine that computes C_n in time $\text{poly}(n)$ can be *de-quantised* if there is a probabilistic universal Turing machine U such that for every computable real $\gamma > 0$ there (effectively) exists a probability distribution \mathcal{P}' with $|\mathcal{P}' - \mathcal{P}| < \gamma$ such that U sampling from \mathcal{P}' runs in time $\text{poly}(T(n), \log(1/\gamma))$.

5 De-quantisation Techniques

5.1 Entanglement Based Methods

One of the simplest approaches of de-quantisation arises from simulating the matrix-mechanical formalism of the state evolution. While the quantum mechanical state vector for n qubits contains, in general, 2^n components, under certain conditions it is possible to find compact representations for the state vector which are polynomial in n , and this can lead to de-quantisations.

The simplest such case is, as in the Deutsch-Jozsa example of Section 2.1, when the state vector remains separable throughout the computation. In these situations, the mathematics of the quantum algorithm can be directly simulated in an efficient manner, because both the state vector and any transformations scale polynomially in the number of qubits n , and thus also in classical resources. This type of de-quantisation is simple to understand and implement classically, as mentioned for the Deutsch-Jozsa problem, but is too restrictive since most quantum algorithms make use of entanglement.

However, the conditions requiring separability can be loosened. Jozsa and Linden [19] and Vidal [29] studied the situation where entanglement is bounded throughout the computation, and the primary result is Theorem 1. It was also noted [29] that these results are applicable to the simulation of continuous time quantum dynamics in some many-body systems.

Theorem 1 (Jozsa and Linden, [19], Vidal [29]). *Suppose \mathcal{A} is a polynomial time quantum algorithm with the property that at each step in the computation on an input of n -qubits, no more than p_n qubits are entangled. If p_n is $O(\log n)$, i.e. the entanglement grows no faster than logarithmically in the input size, then the quantum computation is de-quantisable.*

This is an important result for de-quantisations, but it is not directly applicable to algorithms such as those which solve the Deutsch-Jozsa or Simon's [26] problems, where the algorithm must make use of a

black-box. Since this ‘quantum oracle’ is not usually in \mathcal{G} or efficiently decomposable into gates from \mathcal{G} , we further require that the entanglement of the quantum state is bounded both before and after the application of the black-box [3]—this allows the equivalent classical black-box to be represented in an efficient form, preserving the ability to de-quantise.

Theorem 2 (Abbott, [3]). *Suppose \mathcal{A} is a black-box algorithm which makes use of a black-box U_f . If \mathcal{A} satisfies the conditions for Theorem 1 with the gate set $\mathcal{G}' = \mathcal{G} \cup U_f$, then it is de-quantisable.*

These results require good quantum algorithms to necessarily utilise unbounded entanglement if they are to have any benefit over classical algorithms, and while this was already suspected by many, the ability to utilise these results to de-quantise known algorithms can lead to surprising classical results. Another example of such an instance is with the quantum Fourier transform (QFT). While it often creates unbounded entanglement, for certain classes of input states this is not the case and the computation remains separable [4]. It is conceivable that in various problems there may be natural constraints which enforce such conditions and allow a simple de-quantisation.

5.2 Circuit Topology Methods

The study of de-quantising the QFT has led to another class of de-quantisations which, rather than focusing on the mathematical form of the operators and states, exploits various properties of the structure of the quantum circuit for the algorithm. One of the simplest such results is that of Arahonov, Landau and Makowsky [6]. They show that a slightly modified version of the QFT circuit can be expressed in a form with logarithmic bubblewidth, a visual measure closely related to treewidth.⁴ This leads to a polynomial time classical simulation computing the QFT.

In a similar fashion, both Markov and Shi [21] and Jozsa [18] have explored de-quantisation of circuits by working with tensor networks and treewidth. A tensor network for a circuit associates a tensor with every operator or end of wire in the quantum circuit, and distinct indices are used for different wire segments in the circuit. The network is simulated by contracting tensors together, and results focus around the ability to do so efficiently. While the input state must be separable in order to be simulated, this formalism has the notable advantage that it will work even if entanglement is present in the algorithm. The main result [21] is Theorem 3.

Theorem 3 (Markov and Shi, [21]). *Quantum circuits with T gates and treewidth d can be simulated in time polynomial in T and exponential in d by the method of tensor contraction for product state inputs. Hence, polynomial size circuits with logarithmic treewidth are de-quantisable for product state inputs.*

Jozsa further extended [18] the set of de-quantisable circuits to those which could be arranged so that for every qubit i , there are only logarithmically many 2-qubit gates applied to qubits j and k with $j \leq i \leq k$.

These results, along with a few others [30, 27], provide the basis of the circuit topological de-quantisations. By dealing with circuits they are able to make use of the extensive graph theoretic literature relating to properties such as the treewidth. These results have been applied to the QFT [32], complementing the de-quantisation using entanglement based techniques. These results have the advantage that they can simulate the circuit on arbitrary product state inputs, but unlike the bounded entanglement simulations can only sample from the probability distributions; in many cases this is reasonable, but it makes understanding the role of the QFT as a ‘quantum subroutine’ in other algorithms more difficult [32].

⁴The bubblewidth and treewidth differ by no more than poly-logarithmic factors. See [6] for further details.

It is further worth noting that the structural methods generally produce more complicated de-quantised algorithms. This is evident in the comparison of the different types of QFT de-quantisations [4], and is a result of being overly faithful to the quantum construction which must conform to the restrictions of avoiding measurement and locality. Another example of this is the de-quantisation result of Browne [9], who realised that Niu and Griffiths' semiclassical QFT [15] can be easily turned into a completely classical de-quantised algorithm with no loss in efficiency. This method is different from the other structural approaches as rather than primarily focusing on the internal structure, it is more a result of the ability to measure or 'sample' a qubit once all transformations involving it are completed, and using this to condition the next qubit's transformations.

5.3 Operator Methods

At the other end of the spectrum from the de-quantisation techniques which follow the evolution of the state vector, are the methods which follow the evolution of the operators acting on the state—very much as is the case in the Heisenberg representation in quantum mechanics, as opposed to the Schrödinger representation in which the states evolve. This approach led to the well known Gottesman-Knill Theorem [14, 1], which provides a de-quantisation result for algorithms using only the controlled-NOT, Hadamard and Phase gates, which are generators for the Clifford group.

Theorem 4 (Gottesman-Knill, [14]). *Any quantum computation which uses only gates from the Clifford group (possibly conditioned on classical bits) and measurements on the computational basis, can be de-quantised.*

While the Clifford gates are not universal, this result is in some sense surprising because it allows de-quantisation of algorithms which contain unbounded entanglement. This result is a complement to Theorem 1, as it indicates that a good quantum algorithm must not permit a compact description of the state *or* the operators. This counters the notion that it is entanglement which provides the quantum computational advantage. The Gottesman-Knill Theorem has further been extended by Van den Nest [22] by reducing them to a simplified normal form and showing that all circuits consisting of Toffoli and diagonal gates only, followed by a basis measurement, are de-quantisable.

Given the advantages of the two complementary (state and operator based) de-quantisations, it is natural to ask if there is some further relation between these methods. This is an area in need of more research, and understanding the relationships between de-quantisation techniques will help understand quantum computation better. *It is not unreasonable to consider next an interaction picture type de-quantisation, making the best use of compact descriptions of state and operators simultaneously.*

6 Levels of De-quantisation

It is interesting to note that certain de-quantisation techniques appear to be 'stronger' than others [23]. Since quantum computation is inherently probabilistic, the goal of the de-quantisation is primarily to classically sample from the same probability distribution. However, the sampling techniques such as the entanglement-based techniques and the Gottesman-Knill method are somewhat artificial. In these cases, the probability distribution is calculated, and then a sample is taken by classical probabilistic methods at the end of the computation. This is in contrast to tensor-network de-quantisations, in which the de-quantised algorithm is inherently probabilistic, and the probability distribution is never calculated, only sampled. While this is sufficient for de-quantisation, the amount of work being done is somewhat

different. In [23] it is shown that there exist circuits for which this ‘weaker’ sampling based form of de-quantisation is possible in polynomial time, but calculating the probability distribution is $\#P$ -complete and thus at least as hard as an NP-complete problem.

This result suggests we should focus our attention on sample-based de-quantisations, but this is perhaps a little premature. Even though they may be less general, the ‘strong’ de-quantisations have the advantage that they are trivial to compose together (unlike the ‘weak’ methods [31]), easier to implement classically, and if the de-quantised algorithm is one where the quantum solution is correct with probability-one, such as the Deutsch-Jozsa problem, the de-quantised algorithm can be made deterministic rather than probabilistic. Examining which type of de-quantisation is possible for an algorithm gives further insight into, and distinction between the power of different quantum algorithms. On the other side of the picture, this sample-based approach to de-quantisation shows much promise to be extended, and alternative probabilistic de-quantisations are being explored [23].

7 ‘Where to Next?’ Is the Resounding Question

As we have seen, a range of de-quantisation techniques with different advantages and disadvantages have been developed. These techniques give us necessary, but not sufficient, conditions which a quantum algorithm must have in order to pose a benefit over a classical algorithm. For example, we know that a good quantum algorithm must lack both a concise description of the state and the operators. However, there may exist many other properties which allow de-quantisation, and all such properties must be absent from a good quantum algorithm [19]. Extending these conditions to necessary conditions is the final, optimistic goal, as this would allow us to understand the relation between quantum and classical complexity classes.

However, since this has proven to be extremely difficult, searching for new, different properties which allow de-quantisation is a rewarding and realistic goal. Such properties are beneficial as they deepen our understanding of the power of quantum computation, and the more insight we have to this, the more effectively we can develop quantum algorithms.

In order to find new de-quantisation techniques, it is worth exploring other types of quantum algorithms. Current techniques have focused around the standard algorithms which primarily consist of Fourier transforms and interference. However, alternative classes of algorithms, such as those based on quantum random walks have been studied [5, 25]. Exploring de-quantisation in these different settings could lead to new results in this area.

Comparing the complexities of a quantum and a classical algorithm solving the same problem is not easy. For example, a polynomial-time classical algorithm is stronger than a polynomial-time quantum algorithm solving the same problem.

For ‘oracle-type’ problems, like the Deutsch-Jozsa problem, to compare complexities means to compare the classical and quantum black-boxes. Why? Let us recall that in the Deutsch-Jozsa problem the input is a classical black-box computing a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The quantum solution *embeds* the classical black-box into a (more powerful) quantum black-box, capable of computing with superposition states. Formally, we have changed the problem, as we do not operate with the given data, the classical black-box, but with a modified version of this black-box. The new black-box computes the function in a higher-dimension than the original classical one. Indeed, one could argue that we could create a classical black-box which takes as input a classical version of the ‘equal superposition’ (which is separable), and output the suitable solution to the problem. Intuitively this is cheating, as all of the complexity has been hidden within the black-box. However, it is not clear how to take into consideration

this black-box complexity, and at what point we are no longer solving the same problem.

The root of the proposed de-quantised solution lies in the fact that the embedding can be done as efficiently classically as it can be quantum-mechanically. To compare the complexities of the quantum and de-quantised solutions we ought to compare the costs/resources necessary for performing these ‘embeddings’. In order to understand the cost of the embedding, it seems necessary take into consideration its physical feasibility. Consider the following: by realising that the quantum black-box is a physical object, it must take, as input, a physical resource. If the black-box could be suitably isolated and embedded into the quantum computational system, since all physics is inherently quantum mechanical, the classical black-box could reasonably be transformed into a quantum one. It is not clear to see how the same can be done to embed the black-box in a de-quantised solution. For example, the embedding in the NMR implementation is somewhat artificial as we are able to ‘create’ the classical black-box. However, mathematically the quantum and de-quantised algorithms are identical and this apparent difference cannot be readily evaluated. So an important question is: how do we take into account the physical cost of the embedding in order to truly evaluate the complexity of the classical and de-quantised solutions?

8 Conclusion

We have reviewed the ability to *de-quantise* a quantum algorithm to obtain a classical algorithm which is not exponentially slower in time compared to the quantum algorithm. The main ideas involved in de-quantisation have been illustrated with the Deutsch-Jozsa problem: from re-visiting the quantum solution to the construction of the de-quantised algorithm, the identification of the ‘ingredient’ allowing de-quantisation, a physical implementation of the de-quantised algorithm, to benefits and open questions. A formal definition of de-quantisation was proposed and the main techniques for de-quantisation have been briefly reviewed. Finally, the discussion of open problems has ended with the main unsolved problem related to the de-quantisation of the Deutsch-Jozsa problem: how to compare the classical and quantum black-boxes.

Acknowledgement

We thank Matthias Bechmann, Sonny Datt and Angelika Sebald for comments that improved this paper. This work was in part supported by UoA Summer 2010 Fellowship (Abbott) and UoA FRDF Grant 2010 (Calude).

References

- [1] S. Aaronson & D. Gottesman (2004): *Improved Simulation of Stabilizer Circuits*. *Physical Review A* 70(5), p. 052328. Available at <http://dx.doi.org/10.1103/PhysRevA.70.052328>.
- [2] A. A. Abbott (2009). *De-quantisation in Quantum Computation*. Honours Thesis, University of Auckland.
- [3] A. A. Abbott (2009): *The Deutsch-Jozsa Problem: De-quantisation and Entanglement*. Submitted to *Natural Computing*, presented at the *Workshop on Physics and Computation 2009, Azores, Portugal*. [arXiv:0910.1990v2](http://arxiv.org/abs/0910.1990) Available at <http://arxiv.org/abs/0910.1990>.
- [4] A. A. Abbott (2010): *De-quantisation of the Quantum Fourier Transform*. Accepted to the conference *Physics and Computation 2010, the Nile, Egypt, August 2010*.
- [5] Y. Aharonov, L. Davidovich & N. Zagury (1993): *Quantum Random Walks*. *Physical Review A* 48(2), pp. 1687–1690. Available at <http://dx.doi.org/10.1103/PhysRevA.48.1687>.

- [6] D. Aharonov, Z. Landau & J. Makowsky (2007): *The Quantum FFT can be Classically Simulated*. arXiv:quant-ph/0611156v2 Available at <http://arxiv.org/abs/quant-ph/0611156>.
- [7] Arvind (2001): *Quantum Entanglement and Quantum Computational Algorithms*. *Pramana - Journal of Physics* 56(2 & 3), pp. 357–365.
- [8] G. Boolos & R. Jeffrey (2007): *Computability and Logic*. Cambridge: Cambridge University Press.
- [9] D. E. Browne (2007): *Efficient Classical Simulation of the Quantum Fourier Transform*. *New Journal of Physics* 9(5), p. 146. Available at <http://dx.doi.org/10.1088/1367-2630/9/5/146>.
- [10] C. S. Calude (2007): *De-Quantizing the Solution of Deutsch's Problem*. *International Journal of Quantum Information* 5(3), pp. 409–415. Available at <http://dx.doi.org/10.1142/S021974990700292X>.
- [11] D. Deutsch (1985): *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*. *Proceedings of the Royal Society of London Series A* 400, pp. 97–117. Available at <http://www.jstor.org/stable/2397601>.
- [12] A. Ekert & R. Jozsa (1998): *Quantum Algorithms: Entanglement Enhanced Information Processing*. *Philosophical Transactions of the Royal Society A* 356(1743), pp. 1769–1782. Available at <http://dx.doi.org/10.1098/rsta.1998.0248>.
- [13] R. P. Feynman (1982): *Simulating Physics with Computers*. *International Journal of Theoretical Physics* 21(6/7), pp. 467–488. Available at <http://dx.doi.org/10.1007/BF02650179>.
- [14] D. Gottesman (1999): *The Heisenberg Representation of Quantum Computers*. In: S. P. Corney, R. Delbourgo & P. D. Jarvis, editors: *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pp. 32–43.
- [15] R. Griffiths & C. Niu (1996): *Semiclassical Fourier Transform for Quantum Computation*. *Physical Review Letters* 76(17), pp. 3228–3231. Available at <http://dx.doi.org/10.1103/PhysRevLett.76.3228>.
- [16] J. Gruska (1999): *Quantum Computing*. McGraw Hill.
- [17] P. Jorrand & M. Mhalla (2003): *Separability of Pure n -qubit States: Two Characterizations*. *International Journal of Foundations of Computer Science* 14(5), pp. 797–814. Available at <http://dx.doi.org/10.1142/S0129054103002035>.
- [18] R. Jozsa (2006): *On the Simulation of Quantum Circuits*. arXiv:quant-ph/0603163 Available at <http://arxiv.org/abs/quant-ph/0603163>.
- [19] R. Jozsa & N. Linden (2003): *On the Role of Entanglement in Quantum-computational Speed-up*. *Proceedings of the Royal Society of London Series A* 459(2036), pp. 2011–2032. Available at <http://www.jstor.org/stable/3560059>.
- [20] M. H. Levitt (2008): *Spin Dynamics: Basics of Nuclear Magnetic Resonance*. John Wiley & Sons, 2nd edition.
- [21] I. L. Markov & Y. Shi (2008): *Simulating Quantum Computation by Contracting Tensor Networks*. *SIAM Journal on Computing* 38(3), pp. 963–981. Available at <http://dx.doi.org/10.1137/050644756>.
- [22] M. Van den Nest (2009): *Classical Simulation of Quantum Computation, the Gottesman-Knill Theorem, and Slightly Beyond*. arXiv:0811.0898v2 Available at <http://arxiv.org/abs/0811.0898>.
- [23] M. Van den Nest (2010): *Simulating Quantum Computers With Probabilistic Methods*. arXiv:0911.1624v2 Available at <http://arxiv.org/abs/0911.1624>.
- [24] M. Rosello-Merino, M. Bechmann, A. Sebald & S. Stepney (2010): *Classical Computing in Nuclear Magnetic Resonance*. *Int. J. Unconventional Computing* 6(3–4), p. in press.
- [25] N. Shenvi, J. Kempe & K. B. Whaley (2003): *Quantum Random-walk Search Algorithm*. *Physical Review A* 67(5), p. 052307. Available at <http://dx.doi.org/10.1103/PhysRevA.67.052307>.
- [26] D. R. Simon (1997): *On the Power of Quantum Computation*. *SIAM Journal on Computing* 26(5), pp. 1474–1483. Available at <http://dx.doi.org/10.1137/S0097539796298637>.

- [27] L. G. Valiant (2002): *Quantum Circuits that can be Simulated Classically in Polynomial Time*. *SIAM Journal on Computing* 31(4), pp. 1229–1254. Available at <http://dx.doi.org/10.1137/S0097539700377025>.
- [28] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood & I. L. Chuang (2001): *Experimental Realization of Shor's Quantum Factoring Algorithm using Nuclear Magnetic Resonance*. *Nature* 414(6866), pp. 883–887. Available at <http://dx.doi.org/10.1038/414883a>.
- [29] G. Vidal (2003): *Efficient Classical Simulation of Slightly Entangled Quantum Computations*. *Physical Review Letters* 91(14), p. 147902. Available at <http://dx.doi.org/10.1103/PhysRevLett.91.147902>.
- [30] N. Yoran & A. J. Short (2006): *Classical Simulation of Limited-width Cluster-state Quantum Computation*. *Physical Review Letters* 96(17), p. 170503. Available at <http://dx.doi.org/10.1103/PhysRevLett.91.147902>.
- [31] N. Yoran & A. J. Short (2007): *Classical Simulability and the Significance of Modular Exponentiation in Shor's Algorithm*. *Physical Review A* 76(6), p. 060302. Available at <http://dx.doi.org/10.1103/PhysRevA.76.060302>.
- [32] N. Yoran & A. J. Short (2007): *Efficient Classical Simulation of the Approximate Quantum Fourier Transform*. *Physical Review A* 76(4), p. 042321. Available at <http://dx.doi.org/10.1103/PhysRevA.76.042321>.