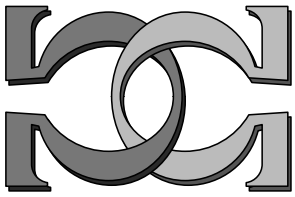
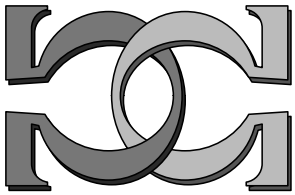
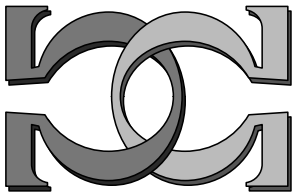
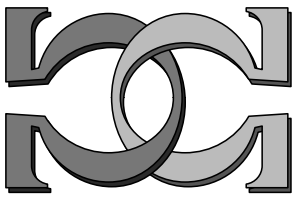


CDMTCS
Research
Report
Series

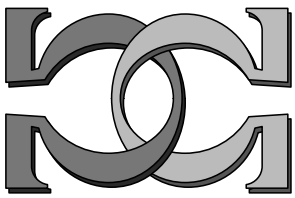




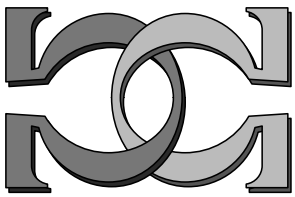
Understanding the Quantum Computational Speed-up via De-quantisation



A. A. Abbott and C. S. Calude
University of Auckland



CDMTCS-381
April 2010



Centre for Discrete Mathematics and
Theoretical Computer Science

Under consideration for publication in Math. Struct. in Comp. Science

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
Email: aabb009@aucklanduni.ac.nz, cristian@cs.auckland.ac.nz

Received 5 October 2010

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) and 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 and limits of the different methods are discussed, and the importance of utilising a range of techniques is emphasised. We further discuss some features of quantum algorithms which current de-quantisation methods do not cover and highlight several important open questions in the area.

[†] Revised and extended version of the paper A. A. Abbott, C. S. Calude. Understanding the quantum computational speed-up via de-quantisation, in S. B. Cooper, E. Kashefi, P. Panangaden (eds.). *Developments in Computational Models (DCM 2010)* EPTCS 26, 2010, pp. 1–12.

[‡] A. A. Abbott was supported in part by a UoA Summer 2010 Fellowship.
[§] C. S. Calude was supported in part by a UoA FRDF Grant 2010.

1. Introduction

Since Feynman (1982) first introduced the concept of a quantum computer 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 faster than 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 (Ekert and Jozsa 1998). In this paper we review the ability to *de-quantise* a quantum algorithm to obtain a classical algorithm which has the same complexity as 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 (Deutsch and Jozsa 1992) 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. for all $x_1, x_2 \in \{0,1\}^n$ we have $f(x_1) = f(x_2)$) or balanced (i.e. $f(x) = 0$ for exactly half of the possible inputs $x \in \{0,1\}^n$). Such a Boolean 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. The obvious classical algorithm would require $2^{n-1} + 1$ black-box calls, while the quantum solution requires only one.

The special case of $n = 1$ was first considered by Deutsch (1985) and is called the Deutsch problem; this was de-quantised by Calude (2007).[†]

It is important to note that unlike Deutsch's problem, where exactly half the valid functions are constant and half are balanced, 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 $f : \{0,1\}^n \to \{0,1\}$ is constant tends towards zero very quickly (recall that in Deutsch-Jozsa problem, f is guaranteed to be valid). Furthermore, the probability that a 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 goes to infinity. This is clearly not an ideal problem to work with; however even in this case we can gain useful information via de-quantisation.

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

2.2. *Quantum solution for $n = 2$*

We are only presenting in detail the $n = 2$ case. In this case the quantum black-box, which is the natural unitary generalisation of the classical one, takes as input three qubits and is represented by the following unitary operator U_f:

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

where $x \in \{0,1\}^2$. The sixteen possible Boolean functions are listed in Table 2.2; two of these are constant, another six are balanced and the remaining eight are not valid.

	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

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 $f'(x) = f(x) \oplus 1$ and define $\left|\pm\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle \pm \left|1\right\rangle)$, we see that

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

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.

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 $\left|00\right\rangle \left|1\right\rangle$, and then operate on it with $H^{\otimes 3}$ to get:

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

After applying the f-controlled-NOT gate U_f we have

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

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 $(-1)^{f(00)}(-1)^{f(11)} = (-1)^{f(01)}(-1)^{f(10)}$, which is equivalent to requiring that $f(00) \oplus f(11) = f(01) \oplus f(10)$. From Table 2.2 it is clear this condition must hold for all balanced or constant functions f for $n = 2$, and thus no entanglement is present in this case.

We can now rewrite Equation 2 in a separable form as follows:

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

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

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

If we measure 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 result is correct with probability one.

2.3. *De-quantising the quantum solution*

The problem can be de-quantised by using complex numbers as two-dimensional classical bits (Calude 2007; Abbott 2009a) because the quantum solution contains no entanglement. The set $\{1, i = \sqrt{-1}\}$ acts as a computational basis in the same way that $\{\left|0\right\rangle, \left|1\right\rangle\}$ does for quantum computation,[‡] and a complex number $z = a + bi$ is a natural superposition of the basis in the same way that a qubit is.

We are now given a classical black-box that computes the function f; this is an *embedding* of the original classical black-box into one operating on complex numbers, just as the quantum black-box is an embedding into one operating in Hilbert-space on qubits. Similarly to U_f, the black-box operates on two complex numbers, $C_f : \mathbb{C}^2 \to \mathbb{C}^2$. Let z_1, z_2 be complex numbers,

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

It is important here to point out a couple of subtle issues about the black-box embedding. The embedding of the black-box for f into C_f seems to create a more powerful black-box; indeed C_f operates on a richer domain, and it is not immediately clear that we have not changed the original problem by allowing this embedding. This issue of the complexity of the black-box has been long overlooked and will be discussed in Section 8.

To simulate a Hadamard gate we multiply each of the complex numbers that the black-box outputs by their respective inputs. If we let $z_1 = z_2 = 1 + i$, multiplying by the input to project onto the computational basis, we get:

[‡] While we are not labelling the basis bits '0' and '1', they represent the classical bits 0 and 1 in the same way that $\left|0\right\rangle$ and $\left|1\right\rangle$ do.

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

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.

It is possible to classically reproduce the ability of the quantum solution to solve the problem with only one black-box call because the quantum solution is *separable*, i. If the quantum state was not separable then 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—this is the case for $n > 2$ in the Deutsch-Jozsa problem where a de-quantisation would need to be based around different techniques (Abbott 2009b). Interestingly, this de-quantisation is equivalent to the 'physical de-quantisation' using classical photon polarisations described by Arvind (2001).

2.4. *Implementing the de-quantised solution*

It is only natural to ask the question: can the de-quantised solution and black-box embedding be translated into an efficient physical implementation? Our interest goes more towards understanding the complexity/difficulty of the implementation of the classical embedding of the original black-box than the engineering aspects. There are different possible approaches, but we will discuss only one, the solution based on Nuclear Magnetic Resonance (NMR) spectroscopy (see Levitt (2008) for more information about NMR).

Solution-state NMR has been extensively studied 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 (Vandersypen *et al.* 2001).

A new approach proposed in Rosello-Merino *et al.* (2010) 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 (Abbott *et al.* a). In the experiments performed, uncoupled proton spins are used as the classical bits, and the projection of the spin-vectors onto the xy-plane determines the state of the two-dimensional classical bit. In this way the de-quantised solution is implemented alongside the quantum solution in the same medium; the cost of each implementation is seen to be the same but the extra freedom in the classical treatment allows us to determine the exact nature of f.

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;
— a better understanding of the quantum solution was obtained by analysing the role of the 'embedding' of the original black-box into the quantum one;
— 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 entanglement[§] '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.

[§] Just 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 is a sequence of gates $G = G_{T(n)} \dots G_1$, where each gate is either a unitary gate chosen from a fixed, finite, universal set of gates $\mathcal{G}$, a unitary black-box from a finite set $\mathcal{B}_n$ given as input to the algorithm, 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 *time-complexity* of $\mathcal{A}$ is $T(n)$ if C_n contains $T(n)$ gates. For black-box algorithms where the set $\mathcal{B}_n$ is non-empty we define the *black-box-complexity* of $\mathcal{A}$, $B(n)$, as the number of gates G_i in C_n which are from $\mathcal{B}_n$.

Many well known algorithms fall into the class BQP, where $T(n) = \text{poly}(n)$ and $C_n = M_{T(n)} U_{T(n)-1} \dots U_1$, the $U_i \in \mathcal{G}$ are unitary and $M_{T(n)}$ is a measurement gate (Gruska 1999). In other words, measurement is the last step of the algorithm in which the output probability distribution is sampled. 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 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 (Boolos and Jeffrey 2007).

Formally, the requirements for a classical algorithm to be a de-quantisation are different depending on the type of problem being solved—specifically the complexity measure we are interested in preserving.

Let $\mathcal{A}$ be a quantum algorithm with output probability distribution $\mathcal{P}$. If the last gate in the quantum circuit C_n is not a measurement gate the output probability distribution is not well defined, so we must consider the distribution resulting from a *counterfactual measurement* at the end of the algorithm. A probabilistic[¶] Turing machine M, such that for every computable $\gamma > 0$ there effectively exists a probability distribution $\mathcal{P}'$ with distance from $\mathcal{P}$ smaller than γ, $\Delta(\mathcal{P}, \mathcal{P}') < \gamma$, which M samples from, is a potential de-quantisation for $\mathcal{A}$.

For a standard (non black-box) algorithm $\mathcal{A}$ with time-complexity $T(n)$, M is a de-quantisation if the (classical) time-complexity of M is $g(n, \gamma) = \text{poly}(T(n), \log(1/\gamma))$. For black-box algorithms we instead consider black-box complexity. The black-box-complexity of the quantum algorithm $\mathcal{A}_{DJ}$ solving the Deutsch-Jozsa problem is $B(n) = 1$. The classical algorithm M_{DJ} is a de-quantisation of $\mathcal{A}_{DJ}$ if it has black-box complexity $g(n, \gamma) = B(n) = 1$, i.e the classical solution must also use only one black-box call. In the more general black-box setting, M is a de-quantisation of a quantum algorithm $\mathcal{A}$ with black-box-complexity $B(n)$ if M has black-box complexity $g(n, \gamma) = \text{poly}(B(n))$.

Often the type of de-quantisation referred to will be clear from context, such as in the

[¶] Here it is necessary that M is probabilistic; this does not affect generality as probabilistic Turing machines have the same computational power as deterministic Turing machines.

Deutsch-Jozsa example presented in Section 2 (although the de-quantisation presented is not uniform; it only applies for the $n = 2$ case). Most de-quantisations are focused around time-complexity as this corresponds to efficient simulation of standard quantum algorithms.

The total variation distance between $\mathcal{P}$ and $\mathcal{P}'$ defined by $\Delta(\mathcal{P}, \mathcal{P}') = \max_A |\mathcal{P}(A) - \mathcal{P}'(A)|$ seems a reasonable measure of distance between probability spaces. However, it is an *open problem whether different distance measures differentiate strengths of de-quantisation* (see the discussion in Section 6) .

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, 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 (2003) and Vidal (2003) studied the situation where entanglement is bounded throughout the computation, and the primary result is Theorem 1. Vidal (2003) further noted that these results are applicable to the simulation of continuous time quantum dynamics in some many-body systems.

Theorem 1 (Jozsa and Linden, 2003; Vidal, 2003). Suppose $\mathcal{A}$ is an algorithm in BQP 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 with respect to time-complexity.

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 (1997) problems, where the algorithm must make use of a black-box. Since the quantum black-boxes (gates in $\mathcal{B}_n$) are not, in general, 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 (Abbott 2009b)—this allows the equivalent classical black-box to be represented in an efficient form, preserving the ability to de-quantise.

Theorem 2 (Abbott, 2010). Let $\mathcal{A}$ be a quantum black-box algorithm which queries

the black-box U_f, and suppose that U_f never entangles its input, i.e. both the input and output of U_f are separable. Then $\mathcal{A}$ can be de-quantised into a classical algorithm with the same number of black-box calls.

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 (Abbott 2010). 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 Arahanov, Landau and Makowsky (2007). 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.[‖] This leads to a polynomial time classical simulation computing the QFT.

In a similar fashion, both Markov and Shi (2008) and Jozsa (2006) 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 (Markov and Shi 2008) is Theorem 3.

Theorem 3 (Markov and Shi, 2008). 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 with respect to time-complexity for product state inputs.

Jozsa (2006) further extended 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 (Yoran and Short 2006; Valiant 2002), 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

[‖] The bubblewidth and treewidth differ by no more than poly-logarithmic factors. See (Aharonov *et al.* 2007) for further details.

as the treewidth. These results have been applied to the QFT (Yoran and Short 2007b), 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 (Yoran and Short 2007b).

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 (Abbott 2010), 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 (2007), who realised that Niu and Griffiths' (1996) semiclassical QFT 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 since it is more a result of the ability to measure or 'sample' a qubit once all transformations involving it are completed and use this to condition future qubit transformations, rather than primarily focusing on internal structure.

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—as is very much 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 (Gottesman 1999; Aaronson and Gottesman 2004), 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, 1999). 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 with respect to time-complexity.

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 (2009) 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 (Van den Nest 2010). 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 explicitly computed, only sampled. While this is sufficient for de-quantisation, the amount of work being done is somewhat different. In Van den Nest (2010) 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 (Yoran and Short 2007a)), 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 (Van den Nest 2010).

7. A limit of de-quantisation

Can every quantum algorithm can be de-quantised? The negative answer, briefly argued below, raises two *open questions: what are the classes of quantum algorithms which can (and, cannot) be de-quantised, and how large are these classes?*

A simple and fast quantum algorithm certified by value indefiniteness—the logical impossibility of the simultaneous, definite, deterministic pre-existence of all conceivable observables from quantum conditions alone (see Svozil 2010)—which produces (potentially an infinite sequence of) quantum random bits, goes beyond the Turing barrier, i.e. it cannot be simulated by any classical Turing machine (Calude and Svozil 2008; Calude *et al.* 2010b). In this context the impossibility of de-quantisation is very strong: it is not only a matter of complexity, it is a matter of incomputability (in fact, strong incomputability: no Turing machine can provably compute any bit of a sequence of quantum

random bits generated by a quantum algorithm certified by value indefiniteness (Abbott *et al.* b)). As a consequence, every quantum algorithm which uses in 'an essential way' a string of quantum random bits cannot be simulated by any classical Turing machine.

This result runs against the standard notion that classical and quantum computational models have equivalent power.[††] The difference between the two is subtle and appears when one considers infinite sequences. The issues around this are at the heart of the incomputability of quantum randomness, and will be treated in a future paper (Abbott *et al.* b).

8. '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 (Jozsa and Linden 2003). Extending these conditions to necessary conditions is the final, optimistic goal, as this would allow us to understand better 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, a stringent necessity.

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. Alternative classes of algorithms, such as those based on quantum random walks have been studied (Aharanov *et al.* 1993; Shenvi *et al.* 2003). Exploring de-quantisation in these different settings could lead to new results in this area.

9. Comparing complexities of quantum and classical algorithms: The case of black-box quantum algorithms

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: the first is deterministic, while the second is probabilistic.

For 'oracle-type' problems, like the Deutsch-Jozsa problem, to compare complexities means not only to compare the number of calls of the black-box, but also the complexities of the enlarged black-boxes, classical and quantum. Why? Let us recall that

[††] This seems to date back as early as Feynman (1982).

in the Deutsch-Jozsa problem the input is a classical black-box computing a function $f : \{0,1\}^n \to \{0,1\}$. 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. Bluntly, the quantum solution does not solve the original (classical) problem; if we accept that the quantum algorithm 'solves' the original problem, then we have to accept the legitimacy of the search for classical, equivalent embeddings.

There must be some minimum requirements on the embedding of the original black-box. If there were not, 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. The embedded black-box must still compute the original function f when operating on basis-states, otherwise it is computing a different function. However, since the embedded black-box can operate on much more than the basis states, it is not clear how to take this into account when considering the complexity of the embedded black-box, and at which point we are no longer solving the original problem but adding more power to the black-box so that it solves the original problem as a 'sub-case'. Also, the information encoded in the input given to the embedded black-box should be exactly the same as the information given in the input of the original black-box.

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 to 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 (as discussed in Section 2.4) is somewhat artificial as we are able to 'create' the classical black-box; it does not correspond to an actual physical 'embedding', and hence the de-quantised embedding can be equally well performed. However, mathematically the quantum and de-quantised algorithms are identical and this apparent difference cannot be readily evaluated. So an important question is: *how de we take into account the physical cost of the embedding in order to truly evaluate the complexity of the classical and de-quantised solutions?*

By isolating the external observer from the observed system in (Calude *et al.* 2010a) a de-quantisation of Deutsch's quantum algorithm in terms of finite automata was proposed. In this framework one shows that depending on the computational power of the external observer, de-quantisation is not possible, or, when de-quantisation is possible,

the de-quantised algorithm distinguishes only between constant and balanced classes of functions, or it can distinguish between all four functions.

10. 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 take into account the complexity of both the black-box embedding and the observer when analysing black-box algorithms.*

Acknowledgement

We thank Matthias Bechmann, Sonny Datt and Angelika Sebald for comments that improved this paper.

References

Aaronson, S. and Gottesman, D. (2004) Improved simulation of stabilizer circuits. *Phys. Rev. A* **70** (5) 052328.

Abbott, A. A. (2009a) De-quantisation in Quantum Computation. Honours Thesis, University of Auckland.

Abbott, A. A. (2009b) The Deutsch-Jozsa problem: De-quantisation and entanglement. *Workshop on Physics and Computation 2009, Azores, Portugal. arXiv:0910.1990v2.*

Abbott, A. A. (2010) The Deutsch-Jozsa problem: De-quantisation and entanglement. *Natural Computing* to appear.

Abbott, A. A., Bechmann, M., Calude, C. S., and Sebald, A. Unpublished work on NMR implementations of the de-quantised solution to the Deutsch-Jozsa problem, in preparation.

Abbott, A. A., Calude, C. S., and Svozil, K. Unpublished work on the incomputability of quantum randomness, in preparation.

Aharanov, Y., Davidovich, L., and Zagury, N. (1993) Quantum random walks. *Phys. Rev. A* **48** (2) 1687–1690.

Aharonov, D., Landau, Z., and Makowsky, J. (2007) The quantum FFT can be classically simulated. *arXiv:quant-ph/0611156v2.*

Arvind (2001) Quantum entanglement and quantum computational algorithms. *Pramana - J. Phys.* **56** (2 & 3) 357–365.

Boolos, G. and Jeffrey, R. (2007) *Computability and Logic*, Cambridge University Press.

Browne, D. E. (2007) Efficient classical simulation of the quantum Fourier transform. *New J. Phys.* **9** (5) 146.

Calude, C. S. (2007) De-quantizing the solution of Deutsch's problem. *Int. J. Quantum Inf.* **5** (3) 409–415.

Calude, C. S., Cavaliere, M., and Mardare, R. (2010a) An observer-based de-quantisation of Deutsch's algorithm. *Int. J. Found. Comput. Sci.* to appear.

Calude, C. S., Dinneen, M. J., Dumitrescu, M., and Svozil, K. (2010b) Experimental evidence of quantum randomness incomputability. *Phys. Rev. A* **82** (022102).

Calude, C. S. and Svozil, K. (2008) Quantum randomness and value indefiniteness. *Adv. Sci. Lett.* **1** (165–168).

Deutsch, D. (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. A* **400** 97–117.

Deutsch, D. and Jozsa, R. (1992) Rapid solution of problems by quantum computation. *Proc. R. Soc. A* **439** 553–558.

Ekert, A. and Jozsa, R. (1998) Quantum algorithms: Entanglement enhanced information processing. *Phil. Trans. R. Soc. A* **356** (1743) 1769–1782.

Feynman, R. P. (1982) Simulating physics with computers. *Int. J. Theor. Phys.* **21** (6/7) 467–488.

Gottesman, D. (1999) The Heisenberg representation of quantum computers. In Corney, S. P., Delbourgo, R., and Jarvis, P. D., editors, *Group 22: Proc. XXII Int. Colloquium on Group Theor. Methods in Phys.* pages 32–43.

Griffiths, R. and Niu, C. (1996) Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.* **76** (17) 3228–3231.

Gruska, J. (1999) *Quantum Computing*, McGraw Hill.

Guerra, H., editor (2010) *De-quantisation of the Quantum Fourier Transform*, CAMIT, University of Azores.

Jorrand, P. and Mhalla, M. (2003) Separability of pure n-qubit states: Two characterizations. *Int. J. Found. Comput. Sci.* **14** (5) 797–814.

Jozsa, R. (2006) On the simulation of quantum circuits. *arXiv:quant-ph/0603163.*

Jozsa, R. and Linden, N. (2003) On the role of entanglement in quantum-computational speed-up. *Proc. R. Soc. A* **459** (2036) 2011–2032.

Levitt, M. H. (2008) *Spin Dynamics: Basics of Nuclear Magnetic Resonance*, John Wiley & Sons, 2nd edition.

Markov, I. L. and Shi, Y. (2008) Simulating quantum computation by contracting tensor networks. *SIAM J. Comput.* **38** (3) 963–981.

Rosello-Merino, M., Bechmann, M., Sebald, A., and Stepney, S. (2010) Classical computing in nuclear magnetic resonance. *Int. J. Unconventional Computing* **6** (3–4):in press.

Shenvi, N., Kempe, J., and Whaley, K. B. (2003) Quantum random-walk search algorithm. *Phys. Rev. A* **67** (5) 052307.

Simon, D. R. (1997) On the power of quantum computation. *SIAM J. Comput.* **26** (5) 1474–1483.

Svozil, K. (2010) Quantum value indefiniteness. *arXiv:1001.1436v1.*

Valiant, L. G. (2002) Quantum circuits that can be simualted classically in polynomial time. *SIAM J. Comput.* **31** (4) 1229–1254.

Van den Nest, M. (2009) Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond. *arXiv:0811.0898v2*.

Van den Nest, M. (2010) Simulating quantum computers with probabilistic methods. *arXiv:0911.1624v2*.

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L. (2001) Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414** (6866) 883–887.

Vidal, G. (2003) Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.* **91** (14) 147902.

Yoran, N. and Short, A. J. (2006) Classical simulation of limited-width cluster-state quantum computation. *Phys. Rev. Lett.* **96** (17) 170503.

Yoran, N. and Short, A. J. (2007a) Classical simulability and the significance of modular exponentiation in Shor's algorithm. *Phys. Rev. A* **76** (6) 060302.

Yoran, N. and Short, A. J. (2007b) Efficient classical simulation of the approximate quantum Fourier transform. *Phys. Rev. A* **76** (4) 042321.