Complexity and Decidability in Unconventional Computational Models

— case for support —

Jacob Biamonte, Ed Blakey, Bob Coecke and Joël Ouaknine

January 18, 2008

Part 1: Research Track Record

Bob Coecke (PI)

Bob Coecke[1] is University Lecturer in Quantum Computer Science at Oxford University Computing Laboratory, and a Governing Body Fellow of Wolfson College; he currently enjoys an EPSRC Advanced Research Fellowship in ICT, entitled *The Structure of Quantum Information and its Ramifications for IT*. He also coordinates the EC FET Open STREP Foundational Structures for Quantum Information and Computation (QICS), worth 1.625 M EUR, which has structures and high-level methods for unconventional quantum computational models as its main focus, and involves leading European Quantum Informatics and CS groups [1]. This proposal was ranked second out of the 487 proposals that were submitted for this FET Open call within FP6.

Coecke has approximately 70 refereed publications. He was awarded the *2004 Biennial Prize for Meritorious Research in the Field of Quantum Structures*. In the past five years, he has given approximately 60 invited talks. A joint paper with Abramsky [2] in 2004 was the first paper on quantum computing ever to have been accepted for the prestigious IEEE conference on Logic in Computer Science.

His research expertise includes the development of mathematical formalisms and the use of logic in computation and physics, quantitative and qualitative theories of information [24, 25], and, in particular, high-level methods for quantum informatics [1, 2]. He also organized several events on mathematical formalisms and high-level methods for quantum computing, was recently invited to co-organize a special session on Quantum Algorithms and Complexity at the *2008 Computability in Europe* conference, and is currently the PC chair of the *Third International Workshop on Development of Computational Models*, a satellite of this year's ICALP conference.

Joël Ouaknine (co-PI)

Joël Ouaknine[2] is a University Lecturer in Computer Science at Oxford University. Ouaknine is the author of more than 40 peer-reviewed conference and journal papers, and in 2007 served on the programme committees of five conferences and workshops. He has research collaborators in several overseas universities, including ENS Cachan (which he visited as Invited Professor for a one-month period in 2006), Berkeley, CMU, the Technion, Uppsala, and ETH Zürich.

His main areas of expertise include dense-time, probabilistic and infinite-state systems, and, in particular, the decidability and complexity of various decision problems arising in these paradigms. He also has extensive experience in concurrent software verification. His PhD thesis was concerned with studying the relationship between dense-time and discrete-time modelling frameworks, and developing model-checking algorithms for real-time systems [42, 45].

Ouaknine's subsequent work in timed systems has been mostly theoretical in nature, obtaining decidability and complexity results for various problems such as language inclusion and model checking/satisfiability of dense-time temporal logics. In particular, he and his colleagues have recently shown that several Metric Temporal Logic model-checking problems are decidable [46, 47, 20], despite long-standing and widely cited claims to the contrary. Ouaknine has also obtained results concerning the trade-offs between precision assumptions in modelling real-time systems and the decidability of various verification problems for these [43, 44].

Other contributions involve decision procedures for probabilistic systems [39], as well as foundational work in the theory of labelled Markov processes [52].

We propose two research students—both exceptionally experienced at this stage, and adequately skilled to perform the proposed research.

Ed Blakey (RS1)

Ed Blakey[3] read for the degree of Bachelor of Arts in Mathematical Sciences at the University of Oxford, for which he received First Class Honours (and was placed first in his year for the Functional Programming and Algorithm Design course), and during which he was twice awarded a Styring Exhibition. He then read (again at Oxford) for the degree of Master of Science in Mathematics and the Foundations of Computer Science, being awarded a Distinction (one of only three Distinctions in his year). His dissertation for this degree was singled out in the Examiners' Report as being 'truly excellent (and completely original)'.

Blakey worked for four years at IBM as a software, hardware and firmware engineer. He is the sole inventor on a pending US patent [14], applied for by IBM on his behalf, for a factorizing machine that is a motivating example for the proposed work. Blakey has since returned to the University of Oxford, where he is reading for the degree

[1] `web.comlab.ox.ac.uk/oucl/work/bob.coecke/`

[2] `web.comlab.ox.ac.uk/oucl/work/joel.ouaknine/`

[3] `web.comlab.ox.ac.uk/oucl/work/ed.blakey/`

of Doctor of Philosophy in Computer Science, specializing in the complexity of non-standard models of computation. He has written two peer-reviewed conference papers on this subject; one [15] was presented at and appears in the proceedings of *Unconventional Computing 2007* (Bristol), the other [16] was presented at and will appear in the proceedings of the *Second International Workshop on Natural Computing* (Nagoya, Japan).

Jacob Biamonte (RS2)

Jacob Biamonte works on the crossover between theory, design and experimental practices in non-standard models of computing. While earning his BS degree in Physics and Electrical Engineering, he spent two summers abroad at the Korean Advanced Institute of Science and Technology, in Daejeon, South Korea, where he helped write software to optimize pulse sequences for NMR quantum computers, the results of which appeared in [37]. He also extended methods used to test classical switching circuits to test quantum and reversible circuits [10, 11].

Biamonte co-authored one paper on quantum complexity theory, which has been cited three times before being published [12]. He has been involved in the experimental implementation and design of superconducting electronic qubits [30], the results of which work were published in the leading physics journal Physical Review Letters. He was a staff physicist at D-Wave Systems Inc. During his time there, the company filed on his behalf one patent, which related to his discovery of simple quantum lattice spin models that have ground-state energy problems complete for the complexity class **QMA**. Such lattices are of key interest in the physics-inspired adiabatic model of quantum computation. He also worked as a research assistant in the Aspuru-Guzik group at Harvard University, where he contributed to the development of gate-model quantum algorithms to simulate Chemical Hamiltonians. He is listed as second author on a paper that will appear in the *Proceedings of the National Academy of Sciences*. He left Harvard to read for a DPhil at Oxford University.

He has been a reviewer for several journals and will be a reviewer for the Special Session on Quantum Computing at the 2008 IEEE Congress on Evolutionary Computation.

Host organization

Oxford University has a deep history in the theory of non-standard models of computation. From David Deutch's development of the quantum analogue of the Church-Turing Thesis [26] to the very first experimental implementation of a quantum algorithm [33], Oxford University has remained a leader in the development of quantum computation. While, initially, the activity was mainly within the physics department, the Materials Department now also has a strong Quantum Information Processing group led by Andrew Briggs, and the Computing Laboratory (OUCL) has a strong Quantum Computer Science group led by Samson Abramsky FRS and Bob Coecke. OUCL also has a substantial bio-computing group led by Peter Jeavons. Recently, OUCL has become strong in algorithms, complexity and decidability, and there is a strong databases group led by Georg Gottlob. OUCL also pioneered Computer Science Semantics, having had Christopher Strachey, Dana Scott and Sir Tony Hoare amongst its ranks. It remains today among the world leaders of the field; the Theory and Verification Group led by Christopher Strachey and Professor Abramsky FRS includes Bill Roscoe, Luke Ong, Tom Melham, James Worrell, EPSRC ARF Andrzej Murawski and many others.

Proposed and existing collaborations

The EC FET Open STREP *Foundational Structures for Quantum Information and Computation*, which PI Coecke coordinates, involves several leading European quantum informatics groups, including some that count the pioneers of the field amongst their members: the Bristol group headed by Jozsa (quantum algorithms and protocols), the Innsbruck group headed by Briegel (measurement-based quantum computing), the York group headed by Braunstein (continuous variable quantum systems) and the Braunschweig group headed by Werner (Quantum Cellular Automata). The Quantum Computer Science group at Oxford University Computing Laboratory also has an ongoing workshop series (QUOXIC) with the Imperial College quantum optics group and the University College Quantum Information group, both in London, which include Browne, Eisert and Rudolph (measurement-based quantum computing). All of these will provide an ideal context for the quantum informatics component of the proposed research.

We also intend to collaborate with Harvard University's Quantum Chemistry group, lead by Professor Alan Aspuru-Guzik, who has contributed to the theory of using quantum algorithms to simulate natural physical systems [6]. Apart from its work on quantum algorithm design, the group has also proposed and implemented several classical algorithms to simulate chemical systems, and has released the well known software package, 'Zori', a general-purpose quantum Monte Carlo simulator.[4] In collaboration, with RS2 Biamonte, the group is currently developing several new methods to utilize quantum algorithms to simulate chemical reaction dynamics. The Aspuru-Guzik group comprises three postdoctoral researchers and five PhD students, and owns one supercomputer, which is housed on site at Harvard.

UK context

The UK Computing Research Committee (UKCRC), in its recent *Grand Challenges Exercise* [32], proposed as its Seventh Grand Challenge *Journeys in non-classical computation*. Several events have taken place in the UK, including the International Workshop, *The Grand Challenge in Non-Classical Computation*, jointly hosted by Microsoft Research and the University of York, and the 2007 Conference on Unconventional Computing in Bristol. Currently, there is also an EPSRC network on Semantics for Quantum Computing (QNET), of which Oxford University Computing Laboratory is a partner site. More generally, the UK is a world leader in quantum computing.

[4] `http://www.zori-code.com`

Part 2: Programme & Context

1 Background

While today's computing has been an amazing success story, there is a growing realization that it covers only a small region within the landscape of the computational potential offered to us by nature. Indeed, the UK Computing Research Committee (UKCRC), in its recent Grand Challenges Exercise [32], has put *Journeys in non-classical computation* forward as one of the key milestones for advance in knowledge and technology. However, once we enter the domain of unconventional computational paradigms, we find ourselves in largely unexplored territory where the well established methods and standards of Turing computing may become inapplicable or insufficient. A paradigmatic example that nicely illustrates this fact concerns the particularly difficult task of factorizing a natural number.

Factorization is not known to be $\mathbf{NP}$-complete, though the required time of the best known factorizing algorithm grows *exponentially* with the number of digits of the number we wish to factorize. This apparent difficulty in factorizing is the reason for its cryptographic importance, imbuing, as it does, the RSA system with security, for example. It is this important use of factorization that has fuelled (not least financially) the enormous expansion of the field of quantum computing. For Shor's quantum factorizing algorithm, the required time grows only *polynomially* with the number of digits; hence, its implementation on a sufficiently large quantum computer, which has yet to be built, would render many currently used encryption schemes gravely unsafe.

We present below an analogue factorization system [13]—due to proposed RS1 Blakey, who is the sole inventor on IBM's corresponding pending US patent [14]—with the surprising property of having *constant* time and space complexities. This may at first cause shock or disbelief; the catch, for of course there is one, is that the *precision* with which the system must be initialized and measured increases as an *exponential* function of the size of the number being factorized. This renders the constant time and space complexities totally irrelevant. Indeed, the true complexity of this analogue computer arises neither from its run-time nor from its required space, nor indeed from any other such Turing-machine-inspired complexity measure, but from its *required precision*. We now describe the system.

First, note that the task of finding factors of a given natural number n is equivalent to finding integer solutions x and y to the equation $y = \frac{n}{x}$. Note further that the curve $y = \frac{n}{x}$ is a hyperbola, and in particular a conic section. We can therefore restate the problem of factorization in terms of finding the coordinates of points of intersection of the two-dimensional integer grid and a cone; this geometric formulation is exploited in the method's physical implementation, which is now outlined.

A source of electromagnetic (hereafter 'e.m.') waves and a configuration of mirrors are used to create an interference pattern that models the integer grid. The use of such waves is motivated by (a) the regularity of wavefronts and consequent regular spacing of the grid, and (b) the ease with which different values of n can be factorized (by altering the e.m. radiation's wavelength). A second source radiating e.m. waves through this lattice onto a circular sensor models the cone (the source is the apex, and the circle of the sensor a cross-section, of the cone).

Integer points in the grid have, by construction, maximum amplitude wave activity from the first source, which, by examining radiation arriving at the sensor (and in particular looking for maximally dark spots) can be detected. The coordinates of these dark points are converted using simple geometry into coordinates of the corresponding integer points on the cone's surface; these latter coordinates relate (via a simple change of scale) directly to factors of n. Hence, this method—of which more details are in [13]—offers much-improved calculation times when compared with existing, algorithmic solutions, largely because it uses a direct, physical implementation of the problem in preference to contrived conversion of the problem into an instance of the standard model of computation.

That the system enjoys both time and space complexities that are constant in the size of the input value serves not to highlight the power of the method but to expose that:

- *traditional complexity theory seems not to address all relevant resources.*

As n increases, the system does in fact require more resource (though neither specifically time nor space) to function correctly; namely, the *precision* with which n must be input (by setting the wavelength of the grid source and the height of the cone) and its factors read (by measuring the positions of dark spots on the sensor) increases with n—this places a technological limit on the magnitude of numbers that we may factorize using this method (and renders the RSA system unscathed). This suggests that, for some analogue computers, traditional, 'algorithmic' complexity theory—which is defined with Turing machines or equivalent in mind—is inadequate, failing, notably, to capture the true complexity of physical computers of which input and output are prone to error.

Similar and complementary arguments have also been put forward by Andrew C. Yao in [56].

In this project we aim to address the following questions:

- *For a given model of computation, what are the relevant and required complexity measures to quantify the hardness of problems and the cost (with respect to various resources) of solution methods?*
- *How can the complexity of computing devices, possibly from differing computation models and possibly with respect to differing complexity measures, be meaningfully and consistently compared?*
- *Is there a general, abstract, compositional theory for adjoining additional resources affecting the complexity of performing certain tasks in various computational models?*

1.1 Some recent progress

There is a growing community actively working with a variety of unconventional computing models, with annual, dedicated, international conferences and other events, and an international journal [3]; this community is particularly well represented in the UK. The specific fields of DNA and quantum computing have enjoyed marked expansion over the last decade; quantum computing in particular has seen the emergence of unconventional quantum computational models (such as measurement-based quantum computing and adiabatic quantum computing), driven by the desire for adequate implementation. PI Coecke and RS2 Biamonte are actively involved in this area: Coecke currently coordinates an EC FP6 Strep on the development of new methods for these unconventional quantum computational models [1], and Biamonte was actively involved in the realization of NMR quantum computing devices at the Korean Advanced Institute of Science and adiabatic quantum computing devices Technology and D-Wave Systems inc. Proposed collaborators in the Aspuru-Guzik group at Harvard are active in quantum simulation algorithms.

These distinct computational models all have their own solution methods for given problems. To compare their respective efficiency in solving a particular problem—factorization, say—, we need a general, model-independent scheme for assigning measures of complexity; this scheme should be sufficiently flexible to account for a variety of resources that have an impact on this complexity. Steps in this direction were taken by proposed RS1 Blakey, first by defining the notion of *precision complexity* (for analogue and other physical, I/O-error-prone computers), and secondly by introducing the idea of *dominant resource*, both presented at UC'07 [15].

Similar issues exist in more abstract computational models such as real-time automata and probabilistic systems [43, 44] on which co-PI Ouaknine is an authority.

We take a closer look at some of these developments.

1.1.1 Precision complexity and dominant resource

For a physical computing system of which input and output are prone to error (since the manipulation and measurement by the user of physical parameters—which manipulation constitutes input to, and measurement output from, the system—are prone to error), we may question which magnitudes of error terms allow correct functioning of the system. It is, in this context, natural to view each error term as an axis, and to consider the space spanned by such. The volume (by which we mean whichever is appropriate of length, area, volume, hyper-volume, etc.) of the region in this space of which region each point corresponds to error term values that guarantee correct performance of the system is, we intuitively feel, a measure of the system's robustness against input/output imprecision; in [15], Blakey formally defined the system's *precision complexity*—which we view as a function of the size of the input to the system—to be one divided by this volume.

Having defined this complexity measure, which better captures the complexity of the analogue factorizing system above and many other physical computers than do the traditional measures (time, space, etc.), it is desired to introduce a framework in which meaningfully to compare systems' complexity according to this measure with other systems' (where these systems are possibly instances of different models of computation) complexity according to other measures. To this end, Blakey introduced (again in [15]) the notion of *dominant resource*, which formalizes, for a given system, which of time, space, precision, etc. is the relevant resource when categorizing the system's complexity; corresponding complexity classes are also defined in [15].

These notions of precision complexity and dominant resource can accommodate the analogue computation model whilst avoiding the problems, described above, encountered with traditional complexity theory—see examples in [15].

1.1.2 Timed automata

Real-time computing is the study of hardware and software systems that are subject to 'real-time constraints' i.e., operational deadlines from event to system response. Timed automata [4] represent one of the most prominent modelling formalisms for real-time systems. They are, essentially, finite-state machines equipped with real-valued clocks. Timed automata accept *timed words*, i.e., words in which each letter has a real-valued timestamp. Ouaknine obtained results on the trade-offs between *precision* assumptions in modelling real-time systems and the decidability of various verification problems for these [43, 44].

1.1.3 Quantum computing

As mentioned above, one of the reasons for the interest in quantum computing is Shor's factorization algorithm. In the conventional model of quantum computing—that is, the circuit model—, a quantum computation is expressed as the preparation of several quantum bits, followed by a sequence of applications to subsets of these quantum bits of unitary operations taken from a complete set, followed by a measurement of the system. Enumeration of the invocations of these unitary operations is the basis of an existing definition of complexity of quantum computing devices—pp.1̃91–194 of [40]. Recently, an alternative for this particular quantification for complexity of quantum computing was proposed by Nielsen et al. in [41]. They consider a unitary evolution, generated by some time-dependent Hamiltonian $H(t)$, and the hardness of the computation is expressed in terms of a cost function $F(H(t))$ of the Hamiltonian control.

In the *measurement-based quantum computational model* [50] due to Raussendorf, Browne and Briegel,[5] one starts with a large entangled state and the computation consists only of measurements of individual qubits, which, at least in principle, could be performed simultaneously. One may reasonably expect that the resources that affect the overall difficulty in effectively implementing such a computation may be radically different from those considered for the circuit model: counting the invocations of unitary operations no longer applies in a straightforward manner.

In the *adiabatic quantum computational model*, one uses ground-state properties of a quantum system [28]. This model works by evolving a system from the accessible ground state of an initial Hamiltonian H_i to the ground state of a final Hamiltonian H_f, which encodes a problem's solution. The evolution takes place over parameter $s \in [0,1]$ as $H(s) = (1-s)H_\mathrm{i} + sH_\mathrm{f}$, where s changes sufficiently slowly that transitions out of the ground state are suppressed [5]. Somewhat controversially, [34] and [35]

[5] See 'Proposed and existing collaborations' for our connection thereto.

offer a quantum adiabatic system that purports to solve the *Turing-undecidable* Hilbert's Tenth problem. The scientific community did not accept this result, though a formal and precise refutation was never given; we attribute this to the fact that the appropriate resources required for a complexity argument were not identified, and suggest that the notions of the current proposal can be used to formalize why the system of [34, 35] does not in fact violate the extended Church-Turing thesis.

Finally, issues of *precision* already affect the very foundations of quantum theory itself [23, 38].

1.1.4 Ground-state computing

In the late 1970s and early 1980s, a wide range of computer technologies and architectures was proposed. Of particular interest are Rapid Single Flux Quantum digital logic and the related Quantum Flux Parametron Supercomputers, which are digital/analogue hybrids. Such circuits are constructed from Josephson Junctions, which allow switching speeds many orders of magnitude greater than those thought to be possible with conventional, room-temperature electronics.

The Quantum Flux Parametron is a two-state system (a magnet), which is used to represent and process bits of information [31]. Flux Parametrons are coupled by programmable circulating current loops. Ferro- and anti-ferromagnetic coupling allow, along with controllability of the local magnetic fields, a lattice of Flux Parametrons to represent the controllable, or random-field, Ising model. In 1982, Barahona [8] showed that finding the ground state of the random-field Ising model is $\mathbf{NP}$-hard. Such observations fostered approaches to solving problems based on classical [36] and later quantum [22] annealing. The Flux Parametron is a type of analogue computer that can execute classical annealing programs.

It was not until the late 1990s that the idea of using the ground-state properties of a quantum system for computation found its expression in the adiabatic model of quantum computation [28]. It is interesting to note that the designers of the Quantum Flux Parametron consider quantum tunnelling of the 'bits' to be a bug, and that they invested design effort to ensure that Parametrons were operated in a regime that minimized the overlap in adjacent wave functions, and hence suppressed tunnelling. The reason for which they wished to suppress quantum tunnelling is that they felt it decreased *precision*.

1.2 Other related work

Existing work in the vein of this proposal includes:

a. presentation by Blum et al. ([17]) of a Turing-machine-like framework to accommodate real-number computations, rather than traditional, $\{0, 1\}$-based (without loss of generality) computations, though without focus on precision;

b. an investigation by Woods ([54, 55]) into an optical model of computation (and the complexity of instances thereof), though avoiding issues of precision by implicitly using the trade-off with space (here, number of pixels);

c. an exploration by Tucker, Costa and collaborators ([9]) of the power of the Turing machine when augmented by physical-computer oracles, with particular regard to the effect of precision on computability (this follows on from, and explicitly makes relevant to the current proposal, Tucker's previous work on analogue, kinematic computers);

d. a study by Bournez et al. ([19]) of computability with (though not complexity of instances of) a specific model of analogue computation;

e. a study by Vergis et al. ([53]) of analogue complexity, in which precision of measurement is seen as a factor constraining the set of problems that can be solved, rather than—as here—a dependent-variable property of problem instances and hence a resource type;

f. a comprehensive study of continuous variable quantum systems by Braunstein and collaborators [21]; and

g. a study of the role of precision in quantum simulation, which recently began in Kendon's group in Leeds.

We intend to study and make use of these related schemes whenever applicable. The differences (of which some are mentioned above) between these and the current proposal render the framework of computation and complexity presented here sufficiently novel to warrant study.

2 Program and methodology

There will be two main strands of research. The first will consist of the development of a general framework for complexity of unconventional computational devices. In the second strand, we wish to test these results within and apply this theory to a variety of contexts (i.e., specific computational models), in which the named researchers and proposed collaborators have profound expertise; these case studies should guide us towards a more general, abstract, compositional theory of resources affecting complexity in general computational models.

We stress that the intent of the project is not that it be of practical use by, for example, offering physical solution methods that improve upon the speed, efficiency or similar offered by existing—especially digital—computers. Rather, the work is to be a foundational study: the wider, more physical framework of computation is investigated as a context in which to generalize the closely related notions of resource and complexity. The ultimate aim, from this foundational viewpoint, is to shed light on whether complexity is inherent in *problems* as opposed to *solution methods* (regardless of whether the latter be physical or algorithmic). That said, we iterate that we wish to consider as case studies within this framework several concrete, non-standard models of computation.

2.1 Strand 1: New measures of complexity, and a general framework therefor

We expect that the notions of precision complexity and dominant resource, discussed above, can accommodate not only analogue computers but also systems such as quantum computers, chemical/DNA computers, ground-state systems and timed automata; it is an aim of the proposed project to take as case studies some of these types of computer—and others—and make concrete this belief.

Moreover, we aim to introduce and investigate new measures of complexity besides required precision, which is formally defined in [15].

There is, further, the need of a framework in which consistently to compare the complexity of instances of diverse models of computation. Our knowledge of a *problem's* complexity very often takes the form of an upper bound given by the complexity of a known *solution method* for the problem (since reasoning directly about the problem's complexity seems inherently more difficult than reasoning about solution methods' complexity), and only when we can meaningfully compare, say, the respective complexities of a Turing machine and a DNA computer can we begin to consider larger, model-heterogeneous sets of solution methods, and hence obtain improved bounds on the complexity of problems. The aim, then, is not merely to introduce a measure of complexity for, say, analogue computers, but rather to introduce new complexity measures for various computational models *in such a way that comparison between models is possible and meaningful*. Accordingly, we wish to consider not just measures of complexity that can be applied to non-Turing computers, but also a framework in which these and traditional measures can be compared.

Having defined this framework and its complexity classes (which are tentatively defined in [15]), it is a natural step—and one that forms part of the proposed project, therefore—to investigate the internal structure of the classes' hierarchy. We wish also to establish the correspondence between the new and traditional hierarchies; this allows known results and open problems concerning the traditional hierarchy to be recast in the context of the new framework's complexity classes, and vice versa.

Besides class-inclusion theorems, etc. alluded to above, we wish to consider foundational questions: is complexity inherent in problems, or an artefact of choice of solution method?; given a computational model, which measures of complexity should we be considering, and why?; can precision effect jumps between complexity classes?; etc.

In summary, the objectives of this strand are:

O1.1 to introduce and investigate measures of complexity, including precision complexity, that apply to various models of computation;

O1.2 to develop a framework of complexity in which to compare in a meaningful and consistent way the complexity—with respect to various measures, both as in **O1.1** and otherwise—of instances of various computation models;

O1.3 to define the complexity classes corresponding to the framework of **O1.2**, and to establish the internal structure of the hierarchy of these classes;

O1.4 to establish the correspondence between new and traditional hierarchies, and to transfer known results and open problems from each hierarchy to the other; and

O1.5 to approach fundamental questions (e.g. is complexity inherent in problems, or imposed by choice of solution method?) from the novel viewpoint of our complexity framework.

Two important further objectives of this strand are:

O1.6 to refine the general theory of complexity that results from the above objectives, based on findings from having completed the case-study objectives of the following strand; and

O1.7 to study, learn from, match and test our formalism with, the relevant related work listed in Sec. 1.2.

2.2 Strand 2: Case studies

We shall study situations in which the (co-)PIs, RSs and their collaborators have strong expertise (see Background).

Factorizing and other tasks. We wish to compare the difficulty encountered whilst performing tasks within different computational models, taking into account new kinds of resources such as precision. For example, we wish to compare classical factorization, Shor's algorithm on some quantum computational model, and Blakey's analogue method for factorizing, taking into account as many resources as possible that might affect complexity. So our objective is:

O2.1 to compare the hardness of important tasks such as factorization within different computational models within the general framework of complexity derived in **O1.2**.

Precision in real-time automata and probabilistic systems. The algorithmic analysis of timed automata is limited both by the **PSPACE**-hardness of the emptiness problem (which asks whether a given timed automaton accepts some timed word) and by the undecidability of the universality problem (which asks whether a given timed automaton accepts every timed word). As noted by many researchers, the underlying cause of these difficulties is the seemingly 'excessive' expressive power that timed automata derive from their ability to differentiate points in time with infinite precision; although mathematically appealing, such a modelling abstraction obviously cannot be realized in the physical world.

Several attempts have been made to circumvent these problems. In particular, a number of *robustness* approaches have been proposed, for example by postulating small amounts of 'noise' in the semantics of timed automata—see, e.g., [29, 48, 44, 27, 7]. The results obtained have been quite mixed, sometimes improving and sometimes worsening the tractability of the various decision problems for timed automata.

In our view, an alternative approach to the problem is to form a better understanding of the *precision complexity* of the various decision problems involved.

Two objectives of this section are:

O2.2 to investigate the precision complexity of various algorithmic problems for timed automata; and

O2.3 to recast the existing results in the literature under the conceptual framework of precision complexity, and to investigate further problems.

Probabilistic automata [49], also known as Labelled Markov Processes [18], are a natural model of probabilistic systems. The transitions of these automata are labelled with actions as well as with probabilities. A probabilistic automaton accepts any (ordinary) word with a certain probability (which can be zero or one, or anything in between), according to the probabilistic weights of the various paths in the automaton along which the word can be accepted. Although *equivalence* of two probabilistic automata (i.e., their accepting the same words with the same probabilities) is decidable in polynomial time [51], such basic problems as *threshold* (which asks whether, given a rational number $\lambda \in [0,1]$, the probabilistic automaton accepts some word with probability at least λ) and *approximation* (which asks whether two given automata accept all words with probabilities differing by no more than some pre-defined $\varepsilon > 0$) are undecidable. One more objective, then, is:

O2.4 to work out and understand the precision complexity of problems such as *threshold* and *approximation* for probabilistic automata, and, if possible, to provide a precision-theoretic framework in which such problems become 'tractable' under the right assumptions.

Relevant resources in quantum and ground-state computing. The relevance of the framework that we intend to develop was already outlined in Sections 1.1.3 and 1.1.4.

We immediately state our explicit objectives:

O2.5 to investigate the precision complexity within, consider other relevant resources for, and apply the general framework of complexity to, unconventional quantum computational architectures—measurement-based, adiabatic, etc.—, and to evaluate and compare the hardness to perform certain tasks within these architectures;

O2.6 to analyse using the general framework of complexity existing disputes in the literature, e.g., the proposed quantum adiabatic algorithm for Hilbert's Tenth Problem [34, 35], and to analyse the role that precision plays in the proofs of the Kochen-Specker theorem and its impact on the experiments verifying the existence of hidden variables [23, 38]; and

O2.7 to preform the investigation of **O2.5** for the existing ground-state computing architectures.

For evidence that the (co-)PIs, RSs, and existing/proposed collaborators have the required expertise for realizing these objectives, please consult our Research Track Record.

2.3 Project management

The project will be jointly managed by the PI and co-Pi. They will have weekly meetings with RSs to monitor their progress and co-ordinate their activity. They will also consult their collaborators for the relevant input to steer the work. In this context they will also organise some small workshops to nourish this interaction with the collaborators; the RSs will pay short visits to the collaborators, as part of their overall preparation for the proposed work.

3 Relevance to beneficiaries

This work addresses the seventh Grant Challenge on *Journeys in non-classical computation*, as outlined by the UK Computing Research Committee (UKCRC) in its recent Grand Challenges Exercise [32]. Hence, the British Computer Science community regards this kind of work as of key importance for the advance of knowledge and technology. In particular, the work on quantum computing bolsters the UK's role as a world leader in this field. The work on timed and probabilistic automata would be of particular interest to the Theoretical Computer Science community. The specific development of the general complexity framework fits within the activity of the Computability in Europe (CIE) community. More generally, this work is inherently interdisciplinary: physicists, mathematicians, computer scientists and engineers alike could benefit from our results.

4 Dissemination and exploitation

We shall present our work at leading international conferences and in leading journals. Because of its interdisciplinary nature, it is particularly important to reach (and to some extent educate) the various communities. Typical journals would be *Unconventional Computing* and *Theoretical Computer Science*; typical events would be the *Unconventional Computing* and *Computability in Europe* conferences, the *Developments in Computational Models* workshops, theoretical computer science conferences such as ICALP and LICS, the meetings of the QNET and QICS quantum computing networks, and many more.

References

[1] S. Abramsky, S. L. Braunstein, H.-J. Briegel, B. Coecke, V. Danos, P. Jorrand, R. Jozsa, P. Panangaden and R. F. Werner (2006) *Foundational Structures for Quantum Information and Computation*. Specific Targeted Research Project within the 6th Framework Program of the European Commission, Jan 1st 2007 – Dec 31st 2009, within the Future and Emerging Technologies Open Scheme. `Click here`

[2] S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols*. In: Proceedings of 19th IEEE conference on Logic in Computer Science, 415–425. IEEE Press. `quant-ph/0402130`

[3] A. Adamatzky, Ed. (2005+) *International Journal of Unconventional Computing*. Old City Publishing

[4] R. Alur and D. Dill (1994) *A theory of timed automata*. Theoretical Computer Science **126**, 183–235

[5] A. Ambainis and O. Regev (2006) *An elementary proof of the quantum adiabatic theorem*. `quant-ph/0411152`

[6] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love and M. Head-Gordon (2005) *Simulated Quantum Computation of Molecular Energies*. Science **309**, 1704

[7] C. Baier, N. Bertrand, P. Bouyer, T. Brihaye and M. Größer (2007) *Probabilistic and topological semantics for timed automata*. In FSTTCS

[8] F. Barahona (1982) *On the computational complexity of the Ising spin glass models*. J. Phys. A **15**, 3241

[9] E. Beggs, S. F. Costa, B. Loff and J. Tucker (2007) *The complexity of measurement in classical physics*. `Click here`

[10] J. D. Biamonte and M. Perkowski (2007) *Quantum mechanics reduces test and validation time*. `quant-ph/0501108`

[11] J. D. Biamonte et al. (2006) *Logical fault models for quantum switching networks*. Journal of Electronic Testing: Theory and Applications (to appear). `quant-ph/0508147`

[12] J. D. Biamonte and P. J. Love (2007) *Towards the simplest QMA-complete Hamiltonian*. Physical Review A (to appear). `quant-ph/0704.1287`

[13] E. Blakey (2007) *An analogue solution to the problem of factorization*. Oxford University Computing Science Research Report `CS-RR-07-04`

[14] E. Blakey (2007) *System and method for finding integer solutions*. United States patent application 20070165313

[15] E. Blakey (2007) *On the computational complexity of physical computing systems*. Proceedings of Unconventional Computing 2007, 95–115. `Click here`

[16] E. Blakey (2007) *Factorizing RSA keys, an improved analogue solution*. Proceedings of the Second International Workshop on Natural Computing, Nagoya, Japan, 10–12 December 2007 (to appear)

[17] L. Blum, F. Cucker, M. Shub and S. Smale (1997) *Complexity and Real Computation*. Springer

[18] R. Blute, J. Desharnais, A. Edalat, and P. Panangaden (1997) *Bisimulation for labelled markov processes*. In *LiCS*, 149–158

[19] O. Bournez, M. Campagnolo, D. Graça and E. Hainry (2006) *The General Purpose Analog Computer and Computable Analysis are Two Equivalent Raradigms of Analog Computation*. Theory and Applications of Models of Computation **3959** LNCS, 631–643

[20] P. Bouyer, N. Markey, J. Ouaknine, and J. Worrell (2007) *The cost of punctuality*. In *LICS*, 109–120

[21] S. L. Braunstein and A. K. Pati (2003) *Quantum Information with Continuous Variables*. Springer-Verlag

[22] J. Brooke, D. Bitko, T.F. Rosenbaum, and G. Aeppli (1999) *Quantum annealing of a disordered magnet*. Science **284**, 779. `cond-mat/0105238`

[23] A. Cabello (2002) *Finite-precision measurement does not nullify the Kochen-Specker theorem*. Physical Review A **65**, 052101

[24] B. Coecke (2002) *Entropic geometry from logic*. In MFPS XIX. ENTCS **83**. `quant-ph/0212065`

[25] B. Coecke and K. Martin (2002) *A partial order on classical and quantum states*. `PRG-RR-02-07`

[26] D. Deutsch (1985) *Quantum theory, the church-turing principle, and the universal quantum computer*. Proc. Royal Society of London A **400**, 97–117

[27] C. Dima (2007) *Dynamical properties of timed automata revisited*. In FORMATS

[28] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser (2000) *Quantum adiabatic evolution algorithms with different paths*. Science **292**, 472–475. `quant-ph/0208135`

[29] V. Gupta, T. A. Henzinger and R. Jagadeesan (1997) *Robust timed automata*. In HART, 331–345

[30] R. Harris et al. (2007) *Sign and magnitude tunable coupler for superconducting flux qubits*. Physical Review Letters **98**, 177001. cond-mat/0608253

[31] W. Hioe and E. Goto (1991) *Quantum Flux Parametron: A Single Quantum Flux Superconducting Logic Device*. World Scientific Publishing Company

[32] C. A. R. Hoare and R. Milner, Eds. (2004) *Grand Challenges in Computing*. The British Computer Soc.

[33] J. A. Jones and M. Mosca (1998) *Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer*. Journal of Chemical Physics **109**, 1648–1653

[34] T. D. Kieu (2004) *Hypercomputation with quantum adiabatic processes*. Theor. Comp. Sc. **317**, 93–104

[35] T. D. Kieu (2003) *Quantum adiabatic algorithm for Hilbert's tenth problem*. `quant-ph/0310052`

[36] S. Kirkpatrick et al. (1983) *Optimization by simulated annealing*. Science **220**, 671–680

[37] S. Lee et al. (2006) *The cost of quantum gates*. Journal of Multiple-Valued Logic and Soft Computing **12**, 561

[38] D. A. Meyer (1999) *Finite-precision measurement nullifies the Kochen-Specker theorem*. Physical Review Letters **83**, 052101

[39] A. S. Murawski and J. Ouaknine (2005) *On probabilistic program equivalence and refinement*. In *CONCUR*, 156–170

[40] M. A. Nielsen and L. Chuang (2000) *Quantum computation and quantum information*. Cambridge UP

[41] M. A. Nielsen, M. Dowling, M. Gu and A. Doherty (2006) *Quantum computing as geometry*, Science **311**, 1133

[42] J. Ouaknine (2002) *Digitisation and full abstraction for dense-time model checking*. In TACAS, 37

[43] J. Ouaknine and J. Worrell (2003) *Universality and language inclusion for open and closed timed automata*. In HSCC, 375–388

[44] J. Ouaknine and J. Worrell (2003) *Revisiting digitization, robustness, and decidability for timed automata*. In LiCS, 198–207

[45] J. Ouaknine and J. Worrell (2003) *Timed csp = closed timed epsilon-automata*. Nord. J. Comput. **10**, 99–133

[46] J. Ouaknine and J. Worrell (2005) *On the decidability of metric temporal logic*. In LICS, 188–197

[47] J. Ouaknine and J. Worrell (2006) *Safety metric temporal logic is fully decidable*. In TACAS, 411–425

[48] A. Puri (1998) *Dynamical properties of timed automata*. In FTRTFT, 210–227

[49] M. O. Rabin (1963) *Probabilistic automata*. Information and Control **6**, 230–245

[50] R. Raussendorf, D. E. Browne and H.-J. Briegel (2003) *Measurement-based quantum computation on cluster states*. Physical Review A **68**, 022312. `quant-ph/0301052`

[51] W.-G. Tzeng (1992) *A polynomial-time algorithm for the equivalence of probabilistic automata*. SIAM J. Comput. **21**, 216–227

[52] F. van Breugel, M. W. Mislove, J. Ouaknine and J. Worrell (2005) *Domain theory, testing and simulation for labelled markov processes*. Theoretical Computer Science **333**, 171–197

[53] A. Vergis, K. Steiglitz and B. Dickinson (1986) *The Complexity of Analog Computation*. Mathematics and Computers in Simulation **28**, 91–113

[54] D. Woods (2005) *Computational Complexity of an optical model of computation*. PhD Thesis, NUI Maynooth

[55] D. Woods (2006) *Optical computing and computational complexity*. In: Proc. 5th International Conference on Unconventional Computation. Springer Lecture Notes in Computer Science **4135**, 27-40

[56] A. C. Yao (2003) *Classical physics and the Church-Turing thesis*. Journal of ACM **50**, 100–105