Case for support: Quantum Computation, Foundations, Security, Cryptography and Group Theory.

1. Previous track record

This project follows a successful collaboration of the principal investigator together with Rees (Newcastle), Braunstein (York) and Lawson (Heriot-Watt) on EPSRC project GR/R87406/01 "Quantum Computing and Algorithms in Group Theory". Results of this collaboration include a generalisation [4] of the Deutsch-Jozsa-Höyer algorithm, to cover a wider range of functions than before, and constructions of quantum algorithms distinguishing between Boolean functions of different weights [12]. Initial work was also carried out as part of a programme to study systematically the complexity of decision problems in finitely presented groups: in particular establishing fundamental results for partially commutative groups [23, 24]. Preliminary investigations, to be followed up in the current project, were made on the generalisation of work of Watrous detecting transitive orbits of actions of certain finite groups, as described below, and into quantum algorithms for word problems in finitely presented groups. The five institutions involved in the collaboration are Newcastle, York, Heriot-Watt, Glasgow and Manchester.

Newcastle. Newcastle is now seen as a centre for geometric group theory, with Duncan, Rees, and recent appointments Robertson and Vdovina all working on various aspects of the subject. Group theorists King and Britnell complete a strong algebra group with close connections to discrete and computational mathematics, attracting excellent visitors and postgraduate students. The North Eastern Geometric Group Theory seminar (an LMS funded network of 8 northern universities) was initiated from Newcastle in 2003 and is still run from there. Newcastle hosted a major workshop on Geometric Group Theory in 2004, with world leading mathematicians Gromov and Grigorchuk as speakers.

Andrew Duncan, at Newcastle since 1993, has worked mainly on decision problems for groups, with emphasis on equations over groups, algebraic geometry of groups and quantum computation[1] . He has supervised four EPSRC funded PhD. students including a current 2nd year student, Jonathan Longrigg, working on cryptography systems based on group theory (currently running experiments on braid group protocols). Duncan was principal investigator on EPSRC grant GR/R87406 "Quantum computation and algorithms in group theory", which employed Batty as a postdoctoral research associate, and made significant progress both in quantum computation and in algorithmic and combinatorial group theory (e.g. [4, 5, 23, 24]). Duncan is a founding member of the "Mathematical Cryptography Consortium" (www.mathcrypto.org), set up to facilitate research in cryptosystems based on algebraic problems and in related cryptanalysis.

Sarah Rees, in Newcastle since 1991, was promoted to a personal chair in 2004. She is a group theorist with experience of both theoretical and practical aspects of computation. She has developed and implemented algorithms to compute with finitely presented [41] and matrix groups [40], which have been widely distributed as standalone programs and within the groups algorithms system GAP. She has studied normal forms, the structure of geodesics and decision problems (especially the word problem) for finitely presented groups [42], and is an expert on connections between the theories of groups, automata and formal languages [55]. She has supervised four EPSRC funded PhD. students on a range of topics within geometric and computational group theory and one EPSRC funded postdoc (Röver). She was principal investigator on three EPSRC grants from 1992-5 (GR/H61056, Computation in group theory, with Holt, Warwick), 1996-8 (GR/K80150, Groups, automata and semigroups, with Epstein and Holt, Warwick) and 2000-3 (GR/M86194, MathFIT, The use of normal forms for solving the word problem, with Holt, Warwick and Thomas, Leicester, employing Röver), and co-investigator on GR/R87406, on which Duncan was principal investigator, as above.

Peter Ryan trained as a theoretical physicist and holds a PhD from the University of London for research in quantum gravity. He has been a professor in the School of Computing Science at the University of Newcastle since January 2002. He has some 20 years of experience in cryptography, information assurance and formal verification. He pioneered the application of process algebras to modelling and analysis of information flow in secure systems and was one of the developers of the groundbreaking CSP and model-checking approach to the analysis of security protocols. He has published extensively on cryptography, cryptographic protocols, security policies, mathematical models of computer security and, most recently, electronic voting systems. Prior to joining the University of Newcastle in 2002, he worked at GCHQ, CESG, the Defence Research Agency, Stanford Research Institute in Cambridge and the Software Engineering Institute, CMU Pittsburgh. Ryan sits on programme committees of several prestigious security conferences, notably: IEEE Security and Privacy, IEEE Computer Security Foundations Workshop, the European Symposium On Research In Computer Security (ESORICS), WITS (Workshop on Issues in Security). He was chair of WITS'04 (Workshop on Issues in the Theory of Security), co-chair of ESORICS'04, co-chair of Frontiers of Electronic Elections FEE 2005 and general chair of the Workshop On Trustworthy Elections (WOTE 2006) Cambridge 29-30 June 2006. Since 1999 he has been the chair

[1] www.mas.ncl.ac.uk/∼najd2/abstracts/

of the ESORICS Steering Committee.

York. Samuel Braunstein is now in the 6* (RAE) rated Computer Science at York. He has been a prominent figure in the field of quantum information since its emergence in the early 1990s. Among his most well-known works are the experimental demonstration of unconditional teleportation [27], the proposal of continuous-variable teleportation [13], the proof that there is no entanglement in the states usually used in NMR implementations of "quantum computing" [11], and the demonstration that Bell inequalities can be maximally violated by mixed states [14]. Most recently, he participated in the first experimental demonstration of unconditional quantum telecloning of coherent states [46, 50]. He is editor of three books, *Quantum Computing*, *Scalable Quantum Computing* and *Quantum Information with Continuous Variables*, and serves on the editorial board of the journal *Fortschritte der Physik* for which he has prepared two special issues on quantum computation. Before joining the University of York, he held a German Humboldt Fellowship (spent at the University of Ulm), and he currently holds a Royal Society Wolfson Research Merit Award. He has been principal investigator on four EPSRC grants and co-investigator on a joint EPSRC/LMS grant for an investigation into quantum computing and algorithms. He has also held a grant under the EU Fifth Framework and one from the Royal Academy of Engineering. Braunstein has over 90 papers in refereed journals and his work has been cited over 4000 times. He has initiated and is a Founding Managing Editor of Quantum Information and Computation – the first journal dedicated specifically to this field. Its first issue appeared in July 2001. By ISI impact factor this journal now ranks 14th of 352 Computer Science journals and 27th of 297 Physics journals.

It is anticipated that Peter Hines will be in the Computer Science department at York, during the project. Hines has interests in the fields of category theory and categorical logic, reversible computation, and automata theory. A focus of his work is the Geometry of Interaction program, a novel interpretation of logic and lambda calculus, where he gave categorical interpretations [35] and showed that this program has interpretations as both finite state machines and (space-bounded) Turing machines [36]. This work has since been put in a general setting via domain-theoretic ideas, giving applications to arbitrary systems with a notion of either iteration or feedback [37, 38]. He has recently completed a 3 year research project at Oxford University Computing Laboratory on the foundations of reversible and quantum computation, with an emphasis on applying ideas and structures from the Geometry of Interaction to both reversible and quantum computation.

Glasgow Simon Gay received his PhD from Imperial College London in 1995 and is now a senior lecturer in the Department of Computing Science, University of Glasgow, where he has been since 2000. He is internationally known for his research on the theory of concurrent and distributed systems, especially programming languages and type systems for distributed programming. During the last few years he has moved successfully into quantum computing, proposing [52] and further developing [28, 53, 29] the idea of applying formal methods to quantum protocols. He is a member of the steering committee of the International Workshop on Quantum Programming Languages and is active in that community [30], and is joint coordinator of the EPSRC Network on Semantics of Quantum Computation (EP/E00623X).

Heriot-Watt. Mark V Lawson's main interests are in semigroup theory, category theory, and automata theory. Lawson was a Junior Research Fellow at Lincoln College Oxford from 1985 to 1988. He was a Royal Society European Exchange Scheme fellow at the TH Darmstadt from 1988 to 1989. In 1989, he became a lecturer and subsequently senior lecturer at the University of Wales. In 2004 he moved to Heriot-Watt University. He has successfully supervised 4 PhD students and published over 40 journal papers. He is one of the algebra editors for the Proc. Edin. Math. Soc. He has written two books, the most recent on automata theory appearing in 2003. He was invited to contribute a chapter on finite automata for the 'Handbook of networked and embedded control systems' (eds D Hristu-Varsakelis and W S Levine, Birkhaüser, 2005). In 2003, he was awarded the tender by DSTL to carry out research for them on finite automata, worth 53,000 pounds. Lawson's research work is most closely connected to the theory of reversible computation, and it is such foundational aspects of the project, together with his expertise in automata, which will be his main contribution to the project.

Manchester. Mark Kambites was appointed to an RCUK Academic Fellowship in the School of Mathematics at Manchester, from September 2006. He specialises in the interactions between algebra and theoretical computer science, and the remit of his Fellowship is to investigate parallel, generic and quantum complexity of algorithmic problems in algebra, and applications in fields such as cryptography. Since obtaining his PhD from York in 2003, he has held a Leverhulme Trust postdoctoral research position at Carleton University (2003-05) and a Marie Curie Intra-European Fellowship at Universität Kassel (2005-06). He has made numerous contributions to areas including group-theoretic algorithms, the theory of automatic semigroups and categories, the Krohn-Rhodes decomposition theory of finite semigroups and automata, the structural theory of abundant semigroups and the spectral theory of random walks on groups. He is presently supervising a PhD student (Elaine Render) in algebra and applications to cryptography.

2. Description of proposed research

2.1. **Background.**

Quantum Computation At the 1998 International Congress of Mathematicians, Peter Shor won the Nevanlinna Prize for his profound 1994 result that there exists a quadratic time algorithm factoring integers on a quantum computer [61, 62]. In particular, this has implications for the security of the RSA cryptosystem. Further impressive illustrations of the power of quantum computation are provided by Grover's algorithm [31] to search an unstructured list of n items in time $O(\sqrt{n})$ (a conventional computer needs $O(n)$ steps) and by the Deutsch-Jozsa-Höyer algorithm [20], which distinguishes between constant and balanced functions in one call to a function oracle (a conventional computer requires $n/2$ calls). In all these examples it is the careful preparation of the problem and the finesse with which the output is interpreted which makes it possible to exploit the power of quantum mechanics.Though these results seem encouraging, roughly speaking these are the only known quantum algorithms and the efforts of the last 10 years have led to disappointingly few new results. This suggests that a systematic study of low level quantum computation processes is required to establish fundamental structures from which algorithms may be constructed. A natural approach to this task is to emulate the methods of classical computation: for example to construct quantum versions of Turing machines and λ-calculus. However, although quantum Turing machines and quantum automata have been defined and studied by many authors [6, 7, 15, 51, 54, 64] they do not seem to be as useful as their classical counterparts in modelling quantum computation or clarifying the structure of basic processes. One possible reason for the relative lack of success in the quantum versions of these classical notions is that people have started with the classical theories and then tried to "quantise" them. On the other hand, if we were to follow Turing's lead it would be more appropriate to go directly to quantum processes perceived from the point of view of information processing and try to formalise them directly. Just as in the classical case, we would expect that highlighting different aspects of quantum processing would lead to different theories of computation. We would expect that these theories would be the quantum analogues of the classical theories but that they would arise directly out of quantum mechanics rather than being adaptations of existing classical theories.

Group Theory, Decision Problems Many mathematical computations involving groups boil down to working with presentations, and immediately computability issues arise. For example the *word problem* asks whether a given word in the generators of the presentation is trivial in the group. A fundamental result of Novikov and Boone shows that there exist finitely presented groups for which the word problem is not solvable, although it is known to be solvable for many classes of groups. Another example is the conjugacy problem which asks, given two words u and v, whether or not these words represent conjugate elements of the group. Such problems, defined in terms of group presentations, provide a rich source of potential security schemes and much effort has recently gone into the formulation of a complexity theory which is appropriate for such applications [10, 44]. For instance variants of the conjugacy problem have been used to formulate cryptography protocols based on group presentations ([3, 33]) and several authors have proposed attacks on these systems. On the other hand most of the known quantum algorithms can be regarded as algorithms for groups: for example, Shor's algorithm is a special case of the hidden subgroup problem, and the Deutsch-Jozsa-Höyer algorithm, as generalised in [20], distinguishes between certain types of element of a group ring. Despite this, very few quantum algorithms for finitely presented infinite groups are known, which explains why little or no work has been done to investigate whether or not group theoretic cryptology might be susceptible to a quantum attack. With this in mind we plan to investigate quantum algorithms and complexity for problems in finitely presented groups.

Quantum Information Assurance and Formal Verification.

We intend to pursue two lines of research in the area of quantum information assurance. The first is to build on the success of the process algebraic approach to the analysis of classical cryptographic protocols, [58], and extend this to a unified framework for reasoning about classical and quantum mechanisms. Quantum cryptographic protocols typically involve classical phases and so such a unified framework is essential for sound and complete analysis. Such a framework should also provide insights into the interaction between classical and quantum phenomena and suggest novel applications. We envisage extending a classical process algebra such as CSP or CCS to model interacting quantum as well as classical or hybrid processes. Initial investigation suggest that establishing an operation semantics for such a hybrid process should be quite feasible (and will avoid our becoming embroiled in issues of interpretation of quantum models).

The second strand of our quantum information assurance work will be to investigate uses of quantum phenomena in information assurance. To date, virtually all quantum cryptographic protocols are for key establishment. It is clear however that there is scope to exploit quantum phenomena to support many other security requirements and policies. Prime examples of such requirements, that are problematic to enforce classically, are information erasure and non-copying. These arise in the context of verifiable voting schemes such as Prêt à Voter, [57], for example during auditing where it is essential to reveal only one of

two complementary pieces of information. Notions of fairness are also often desirable but difficult or even impossible to achieve classically. It seems likely that here again quantum phenomena may open up novel possibilities.

Summary. We need to understand more deeply the roles played by the classical theories of computation with respect to classical computation. This requires a critique of the classical theories and an analysis of the extent to which that critique can be applied to quantum computing. By analogy, consider an example from the history of physics: classical Newtonian mechanics was analysed in more depth to yield Hamiltonian mechanics — there are then procedures for passing from classical Hamiltonians to quantum mechanical ones. Perhaps we should view classical theories of computation as being at the Newtonian level; it is our aim to investigate whether a deeper analysis of the classical theories, inspired by quantum mechanics, could lead to a deeper understanding of classical computing as a prerequisite for a deeper understanding of quantum computing. An understanding of basic principles governing the fundamental quantum processes will enable the design of quantum algorithms to progress at a more satisfactory pace and will underpin the further development of quantum complexity theory. In particular the implications of quantum complexity for information security need to be understood now, while the use of quantum phenomena in such areas is still fairly uncommon (and certainly before the advent of useable quantum computers). Given that quantum algorithms are naturally group theoretic and that group theoretic problems are a rich potential source of problems for cryptography schemes, there is an obvious need to develop quantum algorithms and complexity theory for groups. We plan to develop the tools to allow us to construct such algorithms, to realise the corresponding complexity theory and to begin to build up a theory suitable for application to cryptology. There is also work to be done on the design and analysis of quantum protocols and we shall do this simultaneously, both to give a sound basis to our theoretical results and to focus attention on those problems which are likely to be important in information assurance.

2.2 **Programme and Methodology**

2.2.1 *Overall Aims.* We aim to establish a coherent and natural framework for low level quantum processing, analogous to that provided by automata for classical computation, and then apply these results to develop algorithms in group theory, cryptography and secure distributed computation.

2.2.2 *Detailed aims and methodology.* **1. Foundations of Quantum processing.** We shall review classical models of computation with particular emphasis on processes at a low level of the Chomsky Hierarchy (which have not been so intensively studied to date) to try and find natural frameworks for their implementation. Turing machines encode such mechanical events as movement left or right, erasing or writing a symbol. We shall investigate how best to interpret such events in the context of quantum mechanics and computation, and attempt to construct similarly "natural" quantum models of quantum mechanical processing. We shall examine recent models of quantum computation, using, for example, arrays of entangled states or linear optics, (see [8, 32]) to see how this should be done. One approach to this is to study quantum computers whose states correspond to finite graphs (perhaps of various specific types) and to characterise the computations arising from such systems.

2. Algebraic Models of Quantum processes. The aim of this part of the project is to develop algebraic models of state machines and semantics of combinatory algebras corresponding to the findings of 1 above. We shall attempt to characterise the various levels of basic quantum processing in purely algebraic terms as, for example regular and context-free languages characterise finite state and push-down automata.One approach is to use methods of category theory. The categorical framework for finite state machines developed by Hines [36] demonstrates that state machines with a notion of iteration or feedback (such as 2-way automata, or space-bounded Turing machines) have algebraic models that rely heavily on a certain type of categorical trace. The categorical trace, in a purely abstract setting, has the intuition of feedback or recursion and was originally used in computational models of linear logic. However, it has since found applications in a much wider range of topics – of particular interest are the very concrete, automata-like, models of linear combinatory logic (equivalent to the untyped pure λ-calculus) given by Abramsky, Haghverdi and Scott [1]. Recent work of Hines and Scott [39] has extended this categorical trace to cover categories based on Hilbert spaces and linear maps and suggests a connection with quantum computation. A potentially interesting feature of this approach is that notions of recognition of languages (and implicitly, halting schemes for Turing machines or other automata-like devices such as two-way automata) are not as well-established in the quantum case as in the classical case [6, 48]. The aim in this case is to use the algebraic models to form a general description of recognition, in order to describe classes of formal languages. In the case of combinatory algebras the situation is completely open because no definition of an (untyped) quantum combinatory algebra has yet been given. The intention is to take the translation of algebraic models provided by [39], and use this to motivate a reasonable definition of a quantum combinatory algebra. It would then be a significant step to decide whether this is equivalent, or inequivalent, to existing classical or quantum λ-calculi.

3. Quantum Algorithms and Complexity of Problems in Group Theory Using the results above we shall develop quantum algorithms for some basic decision problems in free groups, partially

commutative groups and braid groups. Of particular interest will be results on the quantum complexity of the subgroup membership problem in free groups, and the conjugacy search problem in the braid groups. The latter forms the basis of the most common of the possible public key cryptography systems based on group theory ([3, 33]). Moreover braid groups underlie certain models of quantum computation ([26, 45, 9]) and as such are particularly suitable for quantum computation [2]. Even in cases when quantum algorithms themselves do not emerge we believe this study may lead to the realisation of more efficient classical algorithms. Many computational problems for groups defined by presentations involve searching an infinite tree and can therefore be very slow and, in many cases, are not even guaranteed to terminate. It is natural to attempt to parallelise in this situation and one way of doing so is to consider using quantum computation. We plan in particular to study Todd–Coxeter coset enumeration, various extensions of the Reidemeister–Schreier procedure and rewriting techniques such as the Knuth–Bendix rewriting procedure (which is closely related to Buchberger's algorithm for Gröbner bases). The standard Knuth–Bendix procedure, with a finite system of rules, frequently does not terminate but alternative approaches using finite state automata to store infinite systems of rules have been investigated [25, 34]. We shall investigate the possible implications of our models of low-level quantum computation to see if, for example, Knuth-Bendix can be further developed, using such models in place of classical finite state automata.

4. Quantum Automatic Groups. The family of automatic groups is defined by the existence of automata for normal forms which behave well with respect to multiplication; the existence of these automata ensures upper bounds on the complexity of certain decision problems. Other mechanisms and other models of classical computation have also been used to define families of groups: some of these ideas more successfully encapsulate computational complexity in terms of algebraic properties than others. For instance the classifications of groups with regular, one-counter and context-free word problems are very straightforward (although the proofs of the last two are non-trivial). We shall investigate how low-level quantum processes can be used for computation in group presentations and make suitable definitions of families of groups defined in terms of these processes (giving a quantum analogue of automatic groups). We shall investigate the relationship between *quantum* complexity of decision problems (such as the word problem) and algebraic properties of the groups.

5. Orbit Transitivity of Group Actions We shall consider the problem of detecting transitivity and identifying orbits, for a finite group acting on a set. (In particular a solution to the latter problem implies a solution to the graph isomorphism problem which is of intrinsic interest in complexity theory and has a well established connection to the hidden-subgroup problem.) For the transitivity problem we aim to construct an algorithm which creates a superposition of the elements of the orbit of one element of the set. The idea is to use classical methods to obtain Erdös–Rényi generators for the group in question. Then given these generators a uniform superposition of the elements of an orbit will be constructed using methods similar to those developed by Watrous [63] to find superpositions of elements of polycyclic groups. The problem is that in this case we can't use properties of polycylic groups, as Watrous does. However the description of the group elements in terms of Erdös–Rényi generators is simpler than it is for Watrous, in polycyclic groups.

6. Cryptography, Information Assurance and Formal Verification.

Process Algebras: Ryan et al developed a process algebra based approach to the analysis of classical cryptographic protocols [56] which has been shown to be very successful and led to highly automated model-checking and theorem proving tools. Our intention is to adapt and extend this to deal with quantum as well as classical processes. Gay and Nagarajan [28, 29] have developed a quantum process calculus based on pi-calculus, and their techniques can easily be adapted to a CCS- or CSP-based language if necessary. Jorrand and Lalire [43, 47] have taken a different approach with similar aims, and their work may also provide a useful starting point. Recent work of Coecke and Pavlovic clarifies the relation between classical and quantum information [16]. It is hoped that this will lead to a unified framework for the modelling and analysis of both classical and quantum mechanisms and protocols. Such a unified approach is essential as quantum protocols typically have classical phases and so complete security analysis requires the capability to reason about both quantum and classical aspects. We will also investigate the possibility of exploiting quantum phenomena to implement other security mechanisms and requirements. for example, helping to enforce fairness aspects of certain protocols (contract signing, fair exchange, anonymity etc.). Another class of security requirement for which quantum phenomena seem well suited, but hitherto unexploited, is enforcing information erasure. We discuss this further under the topic of secure distributed quantum computation below.

Secure Distributed Computation: Distributed quantum computing has received little attention; the main work is that of D'Hondt *et al.* [17, 21, 18, 19], which, however, does not discuss security. As a particular problem domain involving distribution and security, we are interested in electronic voting. A promising classical voting scheme is the Prêt à Voter developed by Ryan [57]. This provides voter-verifiability: voters are able to check that their vote is accurately included in the tally whilst not being able to demonstrate to a third party how they voted (coercion-resistance). In the classical scheme there are several places at

which trust assumptions have to be made. However, quantum phenomena look promising as a way of enforcing such requirements in an unconditional fashion. For example, quantum mechanisms might be used to enforce information erasure (of the ballot form randomised candidate list) or to ensure that only one element of a pair of coupled values can be revealed (during the audits of the anonymising mix phase). Preliminary investigation of these possibilities is presented at the CalTech Workshop on Classical and Quantum Information Assurance, Dec 2005, [59].

2.3 **Timeliness**

The rate at which new quantum algorithms have appeared over the last 10 years has been very low, in spite of the sustained efforts of many researchers. However the existence of quantum algorithms, whether we know of them or not, has profound implications for information assurance and our belief in security systems, as well as for computation in general. Therefore it is very important that good progress is made in the construction of such algorithms and the development of the corresponding complexity theory. This project aims to overcome the obstacles holding up the development of the subject by re-examining the foundations of computation in the light of the physical processes on which quantum computation is based. Cryptographic protocols, both classical and quantum, based on group presentations may prove important in the future; and at worst we need to analyse their potential. The study of the algorithmic complexity of problems posed for groups is therefore of current importance and their analysis must be made quickly, so that we are in a position to understand how they may be used, and attacked, before such time as they may be employed as platforms for cryptosystems. The implications of quantum computation for various aspects of security, described above, have not been much studied and there is both a need for awareness of these implications and the potential for their use in several practical applications. In particular there is an urgent need for more work to be done on the security of electronic voting systems; which are already in widespread use in spite of the fact that their current security is questionable (see http://avirubin.com/). The methods proposed in this project if successful could lead to major improvements in the reliability and security of such systems and so need to be pushed forward as fast as possible.

2.4 **Programme of work**

Initial stages of the project will concentrate on the foundations of quantum computing, where the goal will be to find a natural mathematical framework for quantum computing. This will draw on Braunstein's expertise in quantum mechanics and computer science, combined with Lawson's and Kambites' expertise in automata theory and category theory and Duncan and Rees's previous experience in quantum computation. Much of this work will be based at Heriot-Watt and will involve visits by Kambites (and the other participants) to Edinburgh. Meanwhile Ryan will coordinate work on the Security and Cryptography aspects, beginning with the extension of process algebras into quantum processes and collaborating with Gay in Glasgow. After the first 6 to 9 months the application of initial results to formal languages and computation and algorithms in group theory will begin. This will involve Duncan, Rees, Kambites and the postdoc in visits to the "Mathematical Cryptography Consortium" at Steven's Institute of Technology, where work will be carried out together with (among others) Professor R. Gilman and Professor A. Miasnikov on complexity of problems in group theory and foundations of formal languages based on quantum processes. Gilman and Miasnikov have been instrumental in the development of generic complexity as a tool for understanding algebraic problems relevant to cryptology and the collaboration at Steven's will allow us to develop our ideas, discuss them with other experts, compare our findings to results with those arising from the work being done in Steven's and focus attention on the issues that are most important for the application of quantum complexity to algebraic problems and to cryptography. Diekert (Stuttgart) will visit Newcastle for 2 weeks during the second part of the project to work with Duncan and Rees on the development of algebraic models of quantum computation and complexity of algorithms. His expertise in theoretical computer science and in particular traces [22], as well as complexity of problems in groups and semigroups will be invaluable. We plan to work with Diekert on the use of quantum computational methods in algebraic algorithms involving large search trees, such as some of those mentioned in Section 2.2.2.3 above. It will also be useful to have his expertise available to help understand possible involvment of quantum processes in algorithms such as Makanin's for deciding whether or not equations over certain groups and semigroups have solution. At roughly the mid-point of the project it is planned that the postdoctoral researcher will spend 6 weeks in Waterloo, Canada, working with M Mosca and J Watrous, who are both leading figures in quantum computation. This will give us important new perspective on the ideas developed to this point and will enable us to benefit from the great depth of expertise and active research in quantum computation at Waterloo. Duncan will also visit Waterloo for 2 weeks, later in the project to consolidate the work done there. These visits will be very important in helping us to progress the research with the help of the best expertise available at the point of the project where we are likely to have come up against the most difficult obstacles.

The postgraduate will be supervised primarily by Duncan. An initial task will be to assist with the review of models of classical computation. Therafter the focus will be on investigations of quantum algorithms for groups, with emphasis on quantum complexity of problems arising from crytography. There will also be work to be done at postgraduate level in the analysis of quantum cryptography protocols

under the guidance of Ryan. The postgraduate student will have the opportunity to visit Waterloo and Steven's Institute, to present and discuss results and make contacts both with leading figures in the field and with other postgraduate students.

2.5 **Relevance to beneficiaries**

Quantum computation and those involved in developing it will be the main beneficiaries: particularly if we help to break the deadlock in the production of quantum algorithms. In the long term this will benefit all computer users, but this is dependant on the scaling up of quantum computers, which could take many years. Group theory and formal language theory will benefit from the deeper understanding of both quantum and classical complexity. There are long term practical applications in particular to cryptography, based on group presentations. Information Security is important to a wide range of people and organisations who will all benefit from the outcomes of this research, in the short to medium term. There will be major benefits to current and future users of electronic voting systems.

2.6 **Dissemination and exploitation**

We shall announce our results at international (and national) conferences and publish our work in appropriate journals. We shall also construct a web page describing our research, giving contact addresses and containing links to the literature and to other groups working in the area.

2.7 **Justification of resources**

See the "Justification of Resources" sheet attached. In addition to the investigators and researchers, their time and travel to conferences etc. the project includes visits to and from various overseas institutions. Here we give some further justification for these visits.

Overseas visits. Visits to Waterloo, Canada, to work with M Mosca and J Watrous, who are both leading figures in quantum computation, will give us access to a wealth of expertise and activity in quantum computation. It is likely that whatever ideas for models of quantum computation we devise in the first year of the project there will be very substantial difficulties in developing these into useful working models of computation. Once we have worked on these problems for some months the postdoctoral researcher will spend some time at Waterloo presenting results and seeking help with outstanding problems. This may prove a decisive moment in the project so it is important for us to find as much support as possible. We therefore plan for the PDRA to spend 6 weeks in Waterloo. To consolidate results and push forward further progress we plan later 2 week visits by an investigator and the postgraduate student.

Visits to Steven's Institute, New Jersey, will be important for the development of our research into quantum algorithms and complexity in group theory. There is a large group of researchers working there, led by Gilman and Miasnikov, and we shall have the opportunity to discuss our results, work on outstanding problems and learn what other people have discovered in the area. More details are given in the Programme of Work above. We have planned for 4 people to visit Steven's Institute for 2 weeks each.

External visitor. Diekert (Stuttgart) will visit Newcastle for 2 weeks during the second part of the project to work with Duncan and Rees. Diekert will help us to focus attention on those problems that are important from the viewpoint of theoretical computer science, as opposed to group theory and in addition collaborate in detailed work on the construction of algorithms (see the Programme of Work above for further information).

References

[1] S.Abramsky,E.Haghverdi,P.Scott, *Geometry of Interaction and Linear Combinatory Algebras*, Math. Structures in Comp.Sci., 12(5) (2002)

[2] D.Aharonov,V.F.R.Jones,Z.Landau *A polynomial quantum algorithm for approximating the Jones polynomial.* Proc. 38th annual ACM symp. on Theory of comp. STOC '06, (2006) 427 – 436.

[3] http://www-cs.engr.ccny.cuny.edu/ csmma/mmabgcqc

[4] M.Batty,S.L.Braunstein,A.J.Duncan, *Extending the Promise of the Deutsch–Jozsa–Hoyer Algorithm for Finite Groups* LMS J.Comp.Math., to appear.

[5] M.Batty,S.L.Braunstein,A.J.Duncan,S.Rees, *Quantum algorithms in group theory.* Computational and experimental group theory, 1–62, Contemp.Math., **349**, AMS, Providence, RI, 2004.

[6] E.Bernstein,U.Vazirani, *Quantum Complexity Theory*, SIAM J.Comp. **25** 1411–1473 (1997).

[7] V.D.Blondel,E.Jeandel,P.Koiran, N.Portier, *Decidable and undecidable problems about quantum automata*, SIAM J.Comp., to appear.

[8] R.Raussendorf,H.J.Briegel *A One-Way Quantum Computer.* Phys.Rev.Lett. 86, 5188Ž0135191 (2001).

[9] N.E. Bonesteel,L.Hormozi,G.Zikos,S.H. Simon *Braid Topologies for Quantum Computation.* quant-ph/0505065

[10] A.V.Borovik,A.G.Myasnikov,V.N.Remeslennikov. *Multiplicative measures on free groups.* Int. J.Alg. Comput., 13 (2003), No. 6, 705–731.

[11] S.L.Braunstein,C.M.Caves,R.Jozsa,N.Linden,S.Popescu,R.Schack, Phys.Rev.Lett. **83**, 1054 (1999).

[12] S.L.Braunstein,B.-S.Choi,S.Maitra,D.Chakrabarti,S.Ghosh,P.Mukhopadhyay, *Quantum algorithm to distinguish Boolean functions of different weights* Int. J.Quantum Inf., submitted.

[13] S.L.Braunstein,H.J.Kimble, Phys.Rev.Lett. **80**, 869 (1998).

[14] S.L.Braunstein,A.Mann,M.Revzen Phys.Rev.Lett. **68**, 3259 (1992).

[15] A.Brodsky,N.Pippenger, *Characterizations of 1-Way quantum finite automata*, SIAM J.Comp. 31(5): 1456-1478 (2002)

[16] B.Coecke, D.Pavlovic *Quantum measurements without sums*, to appear in: The Mathematics of Quantum Computation and Technology; Chen, Kauffman and Lomonaco (eds.); Taylor and Francis

[17] Ellie D'Hondt. *Distributed quantum computation: a measurement-based approach.* PhD. Thesis, Vrije Universiteit Brussel (2005).

[18] Ellie D'Hondt and Prakash Panangaden. *Reasoning about quantum knowledge*. In: Proceedings of FSTTCS'05, Lecture Notes in Computer Science, **3821**, 544, (2005) Springer.

[19] Ellie D'Hondt and Prakash Panangaden. *The Computational Power of the W and GHZ States*. Journal of Quantum Information and Computation, **6**, 173, (2005).

[20] D.Deutsch,R.Jozsa,*Rapid solutions of problems by quantum computation* Proc. Royal Soc. London Ser.A, 439–553 (1992).

[21] Vincent Danos and Ellie D'Hondt and Elham Kashefi and Prakash Panangaden. *Distributed measurement-based quantum computation*. In: SelingerP:qpl2005. Also arXiv:quant-ph/0506070, http://www.arxiv.org/abs/quant-ph/0506070.

[22] V.Diekert, G.Rozenberg, *The Book of Traces.* World Scientific, Singapore, 1995.

[23] A.J.Duncan,I.V.Kazachkov,V.N.Remeslennikov *Centraliser Dimension and Universal Classes of Groups*, SEMR, V. 3(2006), p. 197-215, available at www.arxiv.org;

[24] A.J.Duncan,I.V.Kazachkov,V.N.Remeslennikov *Centraliser Dimension of Partially Commutative Groups*, to appear in Int. J.Alg. Comput., available at www.arxiv.org;

[25] D.B.A.Epstein,P.J.Sanders, *Knuth-Bendix for groups with infinitely many rules.* Int. J.Alg. Comput. 10 (2000), no. 5, 539–589.

[26] M.H.Freedman,A.Kitaev,M.J.Larsen,Z.Wang *Topological quantum computation.* Bull. AMS 40 (2003), 31-38.

[27] A.Furusawa, J.L.Sorensen,S.L.Braunstein,C.A.Fuchs,H.J. Kimble,E.S.Polzik, Science **282**, 706 (1998).

[28] S.J. Gay and R. Nagarajan, *Communicating Quantum Processes.* In: Proceedings of the 32nd ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL) ACM Press, Also arXiv:quant-ph/0409052, http://dx.doi.org/10.1145/1040305.1040318, 2005

[29] S.J. Gay and R. Nagarajan, *Types and Typechecking for Communicating Quantum Processes.* Mathematical Structures in Computer Science, **16** (3) 375–406, http://dx.doi.org/10.1017/S0960129506005263, 2006.

[30] S.J. Gay, *Quantum Programming Languages: Survey and Bibliography.* Mathematical Structures in Computer Science, **16** (4) 2006, http://www.dcs.gla.ac.uk/ simon/publications/QPLsurvey.pdf

[31] L.K.Grover, *A fast quantum mechanical algorithm for database search* Proc. 28th Annual ACM Symp. on the Theory of Computation, 212 – 219 ACM Press, New York (1996).

[32] M.Hein,J.Eisert,H.J.Briegel *Multi-party entanglement in graph states.* Phys.Rev.A 69, 062311 (2004).

[33] http://www.tcs.hut.fi/ helger/crypto/link/public/braid/

[34] A.Heyworth *Using Automata to obtain Regular Expressions for Induced Actions.* UWB Math Preprint 99.19 (1999). arXiv Mathematics math.CO/9906153.

[35] P.Hines *The Categorical Theory of Self-Similarity*, Theory and Applications of Categories (1999).

[36] P.Hines *A categorical framework for finite state machines*. In: Math. Struct. in Comp. Sci. 2002.

[37] P.Hines *Physical Systems as Constructive Logics*, Springer LNCS (2006).

[38] P.Hines *Machine Semantics, an Abstract Approach to Computing Machines*, Theoretical Computer Science (submitted).

[39] P.Hines,P.Scott, *The Unitary trace on Hilbert spaces* http://www.hines.uklinux.net/papers/

[40] D.F.Holt,C.R.Leedham-Green,E.A.O'Brien,S.Rees, *Testing matrix groups for primitivity*, J. Alg. 184 (1996) 795 – 817.

[41] D.F.Holt,S.Rees, *Software for automatic groups, isomorphism testing and finitely presented groups*, in Geometric Group Theory, Vol. 1, LMS Lecture Notes 181 (1993) 120 – 125.

[42] D.F.Holt,S.Rees, *Solving the word problem in real time*, J. LMS 63 (2001), 623–639.

[43] Philippe Jorrand and Marie Lalire. *Toward a Quantum Process Algebra*. In: Proceedings of the 1st ACM Conference on Computing Frontiers, ACM Press (2004). Also arXiv:quant-ph/0312067, http://www.arxiv.org/abs/quant-ph/0312067.

[44] I.Kapovich,A.Myasnikov,P.Schupp,V.Shpilrain *Generic-case complexity and decision problems in group theory* J. Alg. 264 (2003), pp.665-694.

[45] L.H.Kauffman,S.J.Lomonaco Jr *Braiding Operators are Universal Quantum Gates* quant-ph/0401090 *A scheme for efficient quantum computation with linear optics*. Nature 409, 46 (2001).

[46] S.Koike,H.Takahashi,H.Yonezawa,N.Takei,S.L.Braunstein,T.Aoki,A Furusawa Phys.Rev.Lett., **96**, 060504 (2006).

[47] Marie Lalire. *Relations among Quantum Processes: Bisimilarity and Congruence*. Mathematical Structures in Computer Science, **16** 3 (2006) 407–428. http://dx.doi.org/10.1017/S096012950600524X.

[48] N.Linden,S.Popescu *The Halting Problem for Quantum Computers* quant-ph/9806054 v.2 (1998)

[49] London Mathematical Society *The International Review of Mathematics*. Available from http://www.cms.ac.uk/irm/.

[50] P.van Loock,S.L.Braunstein Phys.Rev.Lett. **87**, 060504 (2001).

[51] C.Moore,J.P.Crutchfield, *Quantum Automata and Quantum Grammars*, Theor. Comp. Sci. 237 (2000) 275-306.

[52] R.Nagarajan, S.J. Gay, *Formal Verification of Quantum Protocols* arXiv:quant-ph/0203086.

[53] R. Nagarajan, N. Papanikolaou, G. Bowen and S.J. Gay, *An Automated Analysis of the Security of Quantum Key Distribution*, arXiv:cs.CR/0502048, 2005.

[54] A.Nayak *Optimal Lower Bounds for Quantum Automata and Random Access Codes*, FOCS archive, Proc.40th Annual Symp. Foundations Comp.Sci., 1999

[55] S.Rees, Hairdressing in groups; a survey of combings and formal languages, *Geometry and Topology Monographs* 1 (1998), The Epstein Birthday Schrift, 493–509.

[56] P.Ryan,S.Schneider,M.Goldsmith,G.Lowe,A.Roscoe *Modelling and Analysis of Security Protocols*. Pearsonn 2001.

[57] P.Y.A.Ryan,S.A.Schneider, *A Practical, Voter-verifiable Election Scheme*.

[58] P.Y.A.Ryan et al, *Modelling and Analysis of Security Protocols*. Pearson 2000.

[59] P.Y.A.Ryan. *Spooky Voting at a Distance*, http://www.cpi.caltech.edu/quantum-security/slides/ryan.pdf

[60] Peter Selinger. *Proceedings of the 3rd International Workshop on Quantum Programming Languages*. Proceedings of the 3rd International Workshop on Quantum Programming Languages. Electronic Notes in Theoretical Computer Science, publisher=Elsevier Science (2005). http://www.mathstat.dal.ca/ selinger/qpl2005/proceedings.html.

[61] P.W.Shor, Algorithms for quantum computation: Discrete logs and factoring Proc. 35th Symp. Foundations of Comp. Sci. 124–134 (Nov. 1994).

[62] P.W.Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. Society for Industrial and Applied Mathematics Journal on Computing **26** 5 (1997), 1484-1509.

[63] J.Watrous. *Quantum algorithms for solvable groups*. Proceedings of the 33rd ACM Symposium on Theory of Computing, pages 60-67, 2001.

[64] Yamasaki, Tomohiro; Kobayashi, Hirotada; Imai, Hiroshi *Two-way Quantum One-counter Automata*, arXiv.org/abs/cs/0110005