EPSRC
Polaris House, North Star Avenue,
Swindon, Wiltshire,
United Kingdom SN2 1ET
Telephone +44 (0) 1793 444000
Web http://www.epsrc.ac.uk/

Standard Peer Review

EPSRC Reference: EP/I020020/1

Document Status: With Council

none

Applicant Details

Applicant	Dr Thorsten Altenkirch	Organisation	University of Nottingham

Title of Research Project

Quantum Computing Meets Type Theory: A Framework for Certified Quantum Information Processing

Review Information

Response Due Date	01/11/2010	Reviewer Reference:	MTBZQM

Research Council Contact Details

EPSRC Administration Contact: Mrs Jill McBride	Email: jill.mcbride@epsrc.ac.uk	Telephone: 01793 444033

Quality

Please comment on the degree of excellence of the proposal, making reference to:
(1) The novelty, relationship to the context, and timeliness;
(2) The ambition, adventure, and transformative aspects identified;
(3) The appropriateness of the proposed methodology.

(For multi-disciplinary proposals please state which aspects of the proposal you feel qualified to assess)

The applicants and proposing to create a framework for the formal development and certification of algorithms and protocols in quantum computation. There is indeed an urgent need for such methods, especially in quantum cryptography, which already exists as a commercial technology, but also in compilation of quantum algorithms for general-purpose quantum computers, which is still a decade or more away. Experience shows that cryptographic protocols are inherently difficult to design and formal verification has been a useful tool in classical cryptography. When general-purpose quantum computer become available, it is expected that they will initially be of limited capacity, and therefore efficient and sound compilation techniques
will be of great importance particularly in the early phases of that technology.

As the technical basis for their work, the applicants propose to use an emerging technology known as dependent type theory. In the last few years, the use of dependent types has been successfully demonstrated in a number of areas, for example in the formalization of mathematics, and as a software engineering tool.

The applicants are in a unique position to carry out this research. The research will benefit from their existing strength in functional programming, as well as their experience with type-safe embeddings of quantum computation primitives in a functional programming framework via the so-called quantum I/O monad, which was developed by the applicants.

The proposal is timely, because dependently typed programming has only emerged in the last few years as a viable framework for a project of this magnitude.

In summary, this is a very novel and ambitious project, which the applicants are in a unique position to carry out.

The excellence of this proposal has been demonstrated

☐ Not at all	☐ Adequately	☒ Fully

Impact

Please comment on the extent to which the proposal shows the potential impact of the project, making reference to:
(1) The relevance and appropriateness of any beneficiaries or collaborators;
(2) Whether appropriate routes and resources have been identified for dissemination and knowledge exchange.

The proposal identifies several areas in which the project may have an impact. The proposed framework and tools for the certification of quantum algorithms (WP2 and WP3), and the work on high level structures in quantum computing (WP4), will be particularly useful to other researchers in quantum information theory. The applicants are already part of a network of potential collaborators, via the former EPSRC QNET on Semantics of Quantum Computing, and the recently completed EU QICS network. They have identified potential collaborators at Oxford (the group led by Abramsky and Coecke), Edinburgh (Dixon, Duncan), and Glasgow (Gay), among others.

Another important potential group of beneficiaries for this project is private companies, particularly those providing commercial solutions in quantum cryptography and communication.

The routes for dissemination that have been identified are entirely appropriate; this includes exchanges with other researchers; traditional publications; teaching; workshops; and the dissemination of concrete software applications and tools.

In summary, the beneficiaries, collaborations, and routes to dissemination that have been identified in the proposal are appropriate and extensive. Based on the applicants' track record, it is realistic to expect the successful completion of these activities. The potential impact of the proposal is high.

Potential impact has been demonstrated

☐ Not at all	☐ Adequately	☒ Fully

Applicant

Please comment on the applicant's ability to deliver the proposed project, making reference to:
(1) Appropriateness of the track record of the applicant(s);
(2) Balance of skills of the project team, including academic collaborators

The principal applicant (Dr. Altenkirch) has an excellent track record in computer science, particularly in the use of type theory, functional programming, category theory, and quantum programming. He has published widely, and is known for his work on normalization by evaluation, normalization proofs for system F, extensional equality in type theory, and a number of other related areas. As already pointed out in Dr. Coecke's letter of support, Dr. Altenkirch was the author of the first paper on quantum programming languages to have been accepted at the prestigious IEEE LICS conference. He has regularly been on the program committees of conferences and workshops, as well as having given numerous invited lectures. He has also organized a number of workshops and international seminars.

Dr. Altenkirch's previous work on the programming language QML, as well as his work (with Dr. Green) on the quantum I/O monad, are particularly relevant to this proposal, as is his extensive experience with intentional type theory and dependently typed programming. He brings ample experience to this project and is uniquely qualified to carry it out.

The co-applicant, Dr. Green, has recently completed a Ph.D. under Dr. Altenkirch's supervision, and has been primarily responsible for the development of the quantum I/O monad, which will play a pivotal role in the proposed research. He has presented his work at numerous workshops. He also has extensive experience with the new generation of dependently typed programming languages, such as Agda.

The University of Nottingham, with its Functional Programming Lab, is an ideal location for this research project.

The proposed collaborators (at Oxford, Edinburgh, Glasgow, and Warwick) are all of the highest caliber. They also represent a good balance of skills, bringing different backgrounds (such as physics, category theory, quantum information theory) to the project.

In summary, all of the criteria have been amply met by the applicant and his team.

The applicant's track record and ability to deliver this project is

☐ Not appropriate	☐ Adequate	☒ Appropriate

Resources and Management

Please comment on the effectiveness of the proposed planning and management and on whether the requested resources are appropriate and have been fully justified.

The proposal includes a detailed work plan for a 4-year project duration. The applicants have identified appropriate work units (WP1 through WP4), as well as a workshop (WP5). Each work unit describes a detailed plan for addressing a challenging problem. Specific goals, resources and potential collaborators are identified within each work unit as appropriate. The distribution of work units, with WP1 starting in year 1, WP2 and WP3 starting in year 2, and WP4 starting in year 4, is appropriate, given the foundational nature of WP1 for the remaining portions of the project.

The financial resources requested are well justified.

The level of planning and justification of resources is

☐ Unacceptable	☐ Adequate	☒ Good

Overall Assessment

Please summarise your view of this proposal

This is a promising proposal, and highly deserving of support. It could still be many years until a general-purpose quantum computer will become available. However, it is already clear that when such a device is built, computing time will initially be a very limited and valuable resource. It will therefore be necessary, much like in the early days of classical computing, to do much of the development and testing of quantum software offline. In that context, it will be extremely useful to have available powerful tools and formalisms for developing, reasoning about, and certifying the correctness, of quantum software. Moreover, hardware for quantum communication is already commercially available today, and in that context too, it is potentially useful to have formally certified correctness proofs, especially of security properties.

This proposal represents an important step towards building such an infrastructure. Naturally, there are many possible avenues towards this goal, and some of them will likely be pursued by competing researchers around the world. However, the particular avenue outlined in this proposal has a good chance of success. The investigators are uniquely positioned in the U.K. to engage in this research, because of their extensive experience with dependent type theory (a formalism that is emerging to be useful for many kinds of modeling), functional programming (a programming paradigm that is especially well-suited for reasoning and certification), and their prior work on the quantum I/O monad (a way to integrate quantum computing into functional programming while preserving the good theoretical properties of the latter).

The researchers also have access to a network of potential collaborators, who work in related areas such as physics, high-level quantum structures, or quantum information theory. These collaborators will be available as early testers of the proposed formalisms, will be able to provide real-world examples of the kinds of properties the researchers are aiming to certify, and will in turns benefit from the tools and automation that this project will deliver.

In summary, I believe this proposal is innovative, has a high probability of success, and would have a noticeable impact. In my opinion, it should be funded.

My judgement is that:
1) This proposal is scientifically or technically flawed
2) This proposal does not meet one or more of the assessment criteria
3) This proposal meets all assessment criteria but with clear weaknesses
4) This is a good proposal that meets all assessment criteria but with minor weaknesses
5) This is a strong proposal that broadly meets all assessment criteria
6) This is a very strong proposal that fully meets all assessment criteria

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☒ 6

My confidence level in assessing this is:

☐ Low	☐ Medium	☒ High

Reviewer Expertise

Please indicate your areas of expertise that are relevant to your assessment. Take care not to reveal your identity to the applicant.

Functional programming; programming languages; quantum computing; high-level structures in quantum information theory