Formal Analysis of Quantum Systems using Process Calculus*

Timothy A. S. Davidson
Department of Computer Science
University of Warwick, UK
T.Davidson@warwick.ac.uk

Simon J. Gay
School of Computing Science
University of Glasgow, UK
Simon.Gay@glasgow.ac.uk

Rajagopal Nagarajan
Department of Computer Science
University of Warwick, UK
R.Nagarajan@warwick.ac.uk

Quantum communication and cryptographic protocols are well on the way to becoming an important practical technology. Although a large amount of successful research has been done on proving their correctness, most of this work does not make use of familiar techniques from formal methods such as formal logics for specification, formal modelling languages, separation of levels of abstraction, and compositional analysis. We argue that these techniques will be necessary for the analysis of large-scale systems that combine quantum and classical components, and summarize the results of initial investigation using behavioural equivalence in process calculus. This paper is a summary of Simon Gay's invited talk at ICE'11.

1 Introduction

Quantum computing and quantum communication (more generally, *quantum information processing*) appear in the media from time to time, usually with misleading statements about the principles of quantum mechanics, the nature of quantum information processing, and the power of quantum algorithms. In this article, we begin by clarifying the fundamental concepts of quantum information and discussing what quantum computing systems are and are not capable of. We then outline several reasons for being interested in quantum information processing. Moving on to the main theme, we motivate the application of formal methods, including process calculus and model-checking, to quantum systems. Finally, we focus on a particular quantum process calculus called Communicating Quantum Processes (CQP), illustrate it by defining a quantum teleportation protocol, and describe recent results about behavioural equivalence.

2 What is quantum information processing?

The idea of quantum information processing (QIP) is to represent information by means of physical systems whose behaviour *must* be described by the laws of quantum physics. Typically this means very small systems, such as a single atom (in which the spin state, up or down, gives the basic binary distinction necessary for digital information representation) or a single photon (in which polarization directions are used). Information is then processed by means of operations that arise from quantum physics. Quantum mechanics leads to several fundamental properties of quantum information, which between them lead to various counter-intuitive effects and the possiblity of behaviour that cannot occur in classical systems.

*Partially supported by the UK EPSRC: *Network on Semantics of Quantum Computation* (EP/E00623X/1) and *Quantum Computation: Foundations, Security, Cryptography and Group Theory* (EP/F020813/1). and the EU Sixth Framework Programme (Project *SecoQC: Development of a Global Network for Secure Communication based on Quantum Cryptography*).

Bliudze, S., Bruni, R., Carbone, M., Silva, A. (Eds.); ICE 2011
EPTCS 59, 2011, pp. 104–110, doi:10.4204/EPTCS.59.9

2.1 Superposition

The state of a classical bit is either 0 or 1. The state of a quantum bit (qubit) is $\alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ are the *basis states*. In general, α and β are complex numbers, and if both of them are non-zero then the state is a *superposition*, for example $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. It is not correct to say, as often stated in the media, that a qubit can be in two states at once. It is in one state, but that state may be a superposition of the basis states.

2.2 Measurement

It is not possible to inspect the contents of a quantum state. The most we can do is a measurement. Measuring a qubit that is in state $\alpha|0\rangle + \beta|1\rangle$ has a random result: with probability $\frac{1}{|\alpha|^2}$ the result is 0, and with probability $\frac{1}{|\beta|^2}$ the result is 1. After the measurement, the qubit is in the basis state corresponding to the result.

2.3 Operations on a superposition

An operation acts on every basis state in a superposition. For example, starting with the three-qubit state $\frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle - \frac{1}{2}|110\rangle - \frac{1}{2}|111\rangle$ and applying the operation "invert the second bit" produces the state $\frac{1}{2}|010\rangle + \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle - \frac{1}{2}|101\rangle$. This is sometimes known as *quantum parallelism* and in the media it is often described as carrying out an operation simultaneously on a large number of values. However, it is not possible to discover the results of these simultaneous operations. A measurement would produce just one of the basis states. This is absolutely not a straightforward route to "parallelism for free".

2.4 No cloning

It is not possible to define an operation that reliably makes a perfect copy of an unknown quantum state. This is known as the *no cloning theorem*. It contrasts sharply with the classical situation, where the existence of uniform copying procedures is one of the main advantages of digital information. Every word in the statement of the no cloning theorem is significant. For example, with the knowledge that a given qubit is either $|0\rangle$ or $|1\rangle$, it is possible to discover its state (by means of a simple measurement) and then set another qubit to the same state, thus creating a copy. It is also possible in general to create approximate copies, or to copy with a certain probability of perfect success but a certain probability of complete failure. It is possible to transfer an unknown quantum state from one physical carrier to another, but the process destroys the original state. This is known as *quantum teleportation*, and we will return to it later.

2.5 Entanglement

The states of two or more qubits can be correlated in a way that is stronger than any possible classical correlation. An example is the two-qubit state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Measuring either qubit produces, with equal probability, the state $|00\rangle$ or $|11\rangle$. Measuring the other qubit is then guaranteed to produce the same result as the first measurement. This correlation is preserved by quantum operations on the state, in a way that cannot be reproduced classically. This phenomenon is called *entanglement* and it is a key resource for quantum algorithms and communication protocols.

3 Quantum algorithms and protocols

We will now summarize a few algorithms and protocols in which quantum information processing has a clear advantage over classical information processing. This list is not complete; in particular, there are many more cryptographic protocols than we mention here. Teleportation is not included here as we will discuss it in more detail later.

3.1 The Deutsch-Jozsa algorithm

Suppose an unknown function $f : \{0,1\}^n \to \{0,1\}$, is given as a black box, together with information that f is either *constant* or *balanced* (meaning that its value is 0 for exactly half of its inputs). The Deutsch-Jozsa algorithm [6] works out whether f is constant or balanced, with only one evaluation of f. Classically, $2^{n-1}+1$ evaluations would be required in the worst case.

3.2 Shor's algorithm

Shor's algorithm [18] is for integer factorization. Its complexity is $O((\log n)^3)$, whereas the best known classical algorithm has complexity $O(e^{(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}})$. The RSA cryptosystem relies on the unproven assumption that factorization is intractable, so a practical implementation of Shor's algorithm would threaten current information security technology. Note, however, that there is no proved non-polynomial lower bound for classical factorization algorithms, and factorization is not believed to be an NP-complete problem. Media reports about quantum computing often give the impression that quantum computers can solve NP-complete problems efficiently, but there is no evidence for this statement.

3.3 Grover's algorithm

Grover's algorithm [12] finds an item in an unstructured list of length n, taking time $O(\sqrt{n})$. Classically, every item must be inspected, requiring $O(n)$ time on average.

3.4 Quantum key distribution

Quantum key distribution (QKD) protocols, such as the BB84 [1] protocol of Bennett and Brassard, generate shared cryptographic keys which can then be used with a classical encryption technique such as a one-time pad. QKD is secure against any attack allowed by the laws of quantum mechanics, including any future developments in quantum computing. Essentially, secrecy of the key is guaranteed by the no cloning theorem: an attacker cannot make a perfect copy of any information that she intercepts while the protocol is running, and therefore either receives negligible information or reveals her presence.

4 Why is QIP interesting, and will it become practically significant?

There are several reasons to be interested in quantum information processing. First, the subject is really about understanding the information-processing power permitted by the laws of physics, and this is a fundamental scientific question. Second, quantum algorithms might help to solve certain classes of problem more efficiently; if, however, NP-complete problems cannot be solved efficiently even by a quantum computer, then understanding why not is also a question of fundamental interest. Third, quantum cryptography provides a neat answer, in advance, to any threat that quantum computing might pose

to classical cryptography. Fourth, as integrated circuit components become smaller, quantum effects become more difficult to avoid. Quantum computing might be necessary in order to continue the historical trend of miniaturization, even if it offers no complexity-theoretic improvement. Finally, Feynman suggested that quantum computers could be used to simulate complex (quantum) physical systems whose behaviour is hard to analyze classically.

Will QIP become practically significant? Some aspects are already practical: there are companies selling QKD systems today. Whether or not there is a real demand for quantum cryptography remains to be seen, but it seems likely that the promise of absolute security will attract organizations that feel they cannot take any chances. Quantum computing seems to be feasible in principle, although there are still formidable scientific and engineering challenges. But many experimental groups are working hard, and physicists and engineers are very clever. Remember that in 1949 the statement "In the future, computers may weigh no more than 1.5 tonnes" was a very speculative prediction.

5 Formal methods for QIP

There is no doubt about the correctness of quantum algorithms and protocols. Simple protocols such as teleportation can be checked with a few lines of algebra, Shor's and Grover's algorithms have been extensively studied, and Mayers [15] and others have proved the security of quantum key distribution. But what about *systems*, which are constructed from separate components and combine quantum and classical computation and communication? Experience in classical computing science has shown that correctness of a complete implemented system is a very different question from correctness of the idealized mathematical protocol that it claims to implement. This is the *raison d'être* of the field of formal methods.

Nagarajan and Gay [16] suggested applying formal methods to quantum systems, with the same motivation as for classical systems:

- *formal modelling languages*, for unambiguous definitions;
- analysis of *systems*, rather than idealized situations;
- *systematic verification methodologies*, rather than *ad hoc* reasoning;
- the possibility of *tool support*.

We have been working on two strands: quantum process calculus [8, 9], most recently in collaboration with Davidson [5], and model-checking, in collaboration with Papanikolaou [10, 11, 17]. In general these approaches are not mutually exclusive. However, our work on process calculus has focussed on the development of basic theory, leading up to the definition of behavioural equivalence; our work on model-checking uses a different style of specification language, more closely related to Promela. Some recent work [4] makes connections between the two themes.

Other approaches to quantum process calculus include Jorrand and Lalire's QPAlg [13] and Ying *et al.*'s qCCS [20].

6 Quantum teleportation in CQP

Teleportation [2] is a protocol for transferring an unknown qubit state from one participant, Alice, to another, Bob. The protocol uses classical communication — in fact, communication of just two classical bits — to achieve the transfer of a quantum state which is specified by two complex numbers. The trick is that there must be some pre-existing entanglement, shared by Alice and Bob.

Let x and y refer to two qubits that, together, are in the entangled state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Let u be a qubit in an unknown state, that is given to Alice. The protocol consists of the following steps.

1. Alice applies the *controlled not* operator to u and x. This is a two-qubit operator whose effect on each basis state is to invert the second bit if and only if the first bit is 1.
2. Alice applies the *Hadamard* operator to x. This operator is a change of basis from $\{|0\rangle, |1\rangle\}$ to $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.
3. Alice measures u and x, obtaining a two-bit classical result.
4. Alice sends this two-bit classical value to Bob.
5. Bob uses this classical value to determine which of four operators should be applied to y.
6. The state of y is now the original state of u (and u has lost its original state and is in a basis state).

Although the measurement in step 3 has a probabilistic result, the use of the classical value to determine a compensating operation in step 5 means that the complete protocol is deterministic in its effect on the state of Bob's qubit.

The following definitions in the process calculus CQP (Communicating Quantum Processes) [8, 9] model the teleportation protocol. *Alice*, *Bob* and *Teleport* are processes; q is a formal parameter representing a qubit; *in*, *out*, a and b are formal parameters representing channels; c is a private channel; x, y are local names for freshly allocated qubits, which will be instantiated with the names of actual qubits during execution. The language is based on pi-calculus and most of the syntax should be familiar.

$$\begin{array}{l} \mathit{Alice}(q,\mathit{in},\mathit{out}) = \mathit{in}?[u] \,.\, \{u,q *= \mathsf{CNot}\} \,.\, \{u *= \mathsf{H}\} \,.\, \mathit{out}![\mathsf{measure}\ u,q] \,.\, \mathbf{0} \\ \mathit{Bob}(q,\mathit{in},\mathit{out}) = \mathit{in}?[r] \,.\, \{y *= \sigma_r\} \,.\, \mathit{out}![y] \,.\, \mathbf{0} \\ \mathit{Teleport}(a,b) = (\mathsf{qbit}\ x,y)(\{x *= \mathsf{H}\} \,.\, \{x,y *= \mathsf{CNot}\} \,.\, (\mathsf{new}\ c)(\mathit{Alice}(x,a,c) \mid \mathit{Bob}(y,c,b)) \end{array}$$

In *Teleport*, the actions before $(\mathsf{new}\ c)$ put the qubits x and y into the necessary entangled state. In order to help with writing a specification, *Alice* is given the qubit to be teleported as a message on channel *in*, and at the end of the protocol, *Bob* outputs the final qubit on *out*.

CQP has an operational semantics defined by labelled transition rules; it also has a type system in which the no cloning theorem is represented by linear typing. The example above, for simplicity, does not include type declarations.

The desired behaviour of teleportation is that a qubit (quantum state) is received on a and the same quantum state is sent on b; the protocol should behave like an identity operation:

$$\mathit{Identity}(c,d) = c?[x] \,.\, d![x] \,.\, \mathbf{0}$$

We can now write a specification of teleportation:

$$\mathit{Teleport}(c,d) \cong \mathit{Identity}(c,d)$$

where $\cong$ is a behavioural equivalence. Equivalent processes cannot be distinguished by any observer: they output the same values in the same circumstances, they produce the same probability distributions of measurement results, and in general interact in the same way with their environment.

As usual, we would like behavioural equivalence to be a congruence:

$$\forall P,Q,C. \quad P \cong Q \Rightarrow C[P] \cong C[Q]$$

where C is a process context. Congruence supports equational reasoning, and the universal composability properties defined by Canetti [3] in a different setting. Developing a congruence for a quantum process calculus was an open problem for several years [14], but very recently we have defined a congruence for CQP [5] and Feng *et al.* have independently defined one for qCCS [7]. Our equivalence is a form of probabilistic branching bisimulation [19], with appropriate extensions to deal with the quantum state. We have proved that the specification of teleportation is satisfied.

7 Conclusion

We have outlined the principles of quantum information processing, and argued that formal methods will be necessary in order to guarantee the correctness of practical quantum systems. We have illustrated a particular approach — specification and verification via behavioural equivalence in quantum process calculus — with reference to quantum teleportation.

Future work on the theoretical side will include the development of equational axiomatizations of behavioural equivalence in CQP, and the automation of equivalence checking. On the practical side, we intend to work on more substantial examples including cryptographic systems.

References

[1] C. H. Bennett & G. Brassard (1984): *Quantum Cryptography: Public-key Distribution and Coin Tossing*. In: *IEEE Conf. on Comp., Sys. and Sig. Proc.*

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres & W. K. Wootters (1993): *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. *Phys. Rev. Lett.* 70, pp. 1895–1899, doi:10.1103/PhysRevLett.70.1895.

[3] R. Canetti (2001): *Universally Composable Security: A New Paradigm for Cryptographic Protocols*. In: *42nd IEEE Symp. Found. Comp. Sci.*, doi:10.1109/SFCS.2001.959888.

[4] T. Davidson, S. J. Gay, H. Mlnařík, R. Nagarajan & N. Papanikolaou (2011): *Model Checking for Communicating Quantum Processes*. *International Journal of Unconventional Computing* (to appear).

[5] T. A. S. Davidson (2011): *Formal Verification Techniques using Quantum Process Calculus*. Ph.D. thesis, University of Warwick.

[6] D. Deutsch & R. Jozsa (1992): *Rapid solutions of problems by quantum computation*. *Proceedings of the Royal Society of London A* 439(1907), pp. 553–558, doi:10.1098/rspa.1992.0167.

[7] Y. Feng, R. Duan & M. Ying (2011): *Bisimulation for quantum processes*. In: *38th ACM Symp. on Principles of Prog. Langs.*, doi:10.1145/1926385.1926446.

[8] S. J. Gay & R. Nagarajan (2005): *Communicating Quantum Processes*. In: *32nd ACM Symp. on Principles of Prog. Langs.*, doi:10.1145/1040305.1040318. Also arXiv:quant-ph/0409052.

[9] S. J. Gay & R. Nagarajan (2006): *Types and typechecking for Communicating Quantum Processes*. *Mathematical Structures in Computer Science* 16(3), pp. 375–406, doi:10.1017/S0960129506005263.

[10] S. J. Gay, N. Papanikolaou & R. Nagarajan (2008): *QMC: a model-checker for quantum systems*. In: *Proceedings of the 20th International Conference on Computer Aided Verification (CAV), Springer LNCS* 5123, pp. 543–547, doi:10.1007/978-3-540-70545-1_51.

[11] S. J. Gay, N. Papanikolaou & R. Nagarajan (2010): *Specification and verification of quantum protocols*. In: *Semantic Techniques in Quantum Computation*, Cambridge University Press.

[12] L. Grover (1996): *A Fast Quantum Mechanical Algorithm for Database Search*. In: *Proc. 28th Annual ACM Symposium on the Theory of Computation*, ACM Press, pp. 212–219, doi:10.1145/237814.237866.

[13] P. Jorrand & M. Lalire (2004): *Toward a Quantum Process Algebra*. In: *1st ACM Conf. on Computing Frontiers*, doi:10.1145/977091.977108.

[14] M. Lalire (2006): *Relations among quantum processes: bisimilarity and congruence*. *Math. Struct. Comp. Sci.* 16(3), pp. 407–428, doi:10.1017/S096012950600524X.

[15] D. Mayers (2001): *Unconditional Security in Quantum Cryptography*. *J. ACM* 48(3), pp. 351–406, doi:10.1145/382780.382781.

[16] R. Nagarajan & S. J. Gay (2002): *Formal Verification of Quantum Protocols*. arXiv:quant-ph/0203086.

[17] N. K. Papanikolaou (2009): *Model Checking Quantum Protocols*. Ph.D. thesis, University of Warwick.

[18] P. W. Shor (1994): *Algorithms for quantum computation: discrete logarithms and factoring*. In: *35th IEEE Symp. Found. Comp. Sci.*, doi:10.1109/SFCS.1994.365700.

[19] N. Trčka & S. Georgievska (2008): *Branching bisimulation congruence for probabilistic systems*. *Electronic Notes in Theoretical Computer Science* 220(3), pp. 129–143, doi:10.1016/j.entcs.2008.11.023.

[20] M. Ying, Y. Feng, R. Duan & Z. Ji (2009): *An algebra of quantum processes*. *ACM Trans. Comp. Logic* 10(3), p. 19, doi:10.1145/1507244.1507249.