QMC: A Model Checker for Quantum Systems

Simon J. Gay[1], Rajagopal Nagarajan[2⋆], and Nikolaos Papanikolaou[2⋆,⋆⋆]

[1] Department of Computing Science, University of Glasgow
[2] simon@dcs.gla.ac.uk
[3] Department of Computer Science, University of Warwick
[4] {biju,nikos}@dcs.warwick.ac.uk

1 Introduction

The novel field of quantum computation and quantum information has been growing at a rapid rate; the study of quantum information in particular has led to the emergence of communication and cryptographic protocols with no classical analogues. Quantum information protocols have interesting properties which are not exhibited by their classical counterparts, but they are most distinguished for their applications in cryptography. Notable results include the unconditional security proof [1] of quantum key distribution [2, 3] and the impossibility proof of unconditionally secure quantum bit commitment [4]. The former of these results in particular is one of the reasons for the widespread interest in this field, and it demonstrates an achievement not possible in classical cryptographic systems.

The benefits of automated verification techniques are well known for classical communication protocols, especially in the cryptographic setting. *Model-checking* has been used to uncover subtle flaws in protocols and system designs [5, 6]. Our research programme is to apply similar techniques to quantum protocols with the expectation of gaining corresponding benefits. Today, while simulation tools for quantum information systems abound (see [7] for a list), to our knowledge no other authors have developed a tool aimed at verification. In this paper we describe just such a tool, based on our earlier work [8, 9], named QMC (Quantum Model Checker); it allows for automated verification of properties of quantum systems. Properties to be verified are expressed using a subset of EQPL [10], a state logic designed specifically for quantum information. QMC analyses systems which can be expressed within the *stabiliser formalism*, which is known to be simulable in polynomial time. The systems expressible in this formalism are restricted, in the sense that the set of operations which they can perform is not universal for quantum computation. Nevertheless, stabiliser circuits are sufficient to describe a number of systems of practical interest.

2 Tool Description

The QMC tool allows the user to model-check a property of the final quantum state produced by a particular quantum protocol. A quantum protocol is perceived as a sequence of operations on both classical variables and a single quantum state consisting of n qubits. Models of protocols are expressed using a simple, imperative-style language, while properties for verification are expressed using a subset of the logic EQPL [10]. The tool functions by simulating the protocol step-by-step; whenever a measurement occurs in a protocol, it gives rise to different runs of the protocol, one for each possible outcome. The EQPL formula specifying the desired protocol behaviour is checked on the final quantum state for each possible run.

⋆ Partially supported by the EU Sixth Framework Programme (Project SecoQC: *Development of a Global Network for Secure Communication based on Quantum Cryptography*).
⋆⋆ Partially supported by the EPSRC Network EP/E006833/1 on Semantics of Quantum Computation.

```
1    init 3; // Initialise 3-qubit system state
2    int teleportme := 0; /* 0 = |0>, 1 = |1>, 2 =|0>+|1>, 3 =|0>-|1> */
3    if ((teleportme==1) \/ (teleportme==3)) do { X q0; }; //Prepare initial state
4    if (teleportme>1) do { had q0; };
5    had q1; cnot q1 q2; // Main part of the protocol
6    cnot q0 q1; had q0;
7    int a,b; a:= meas q0; b := meas q1;
8    if (b==1) do { X q2; }; if (a==1) do { Z q2; };
```

Fig. 1. Quantum teleportation expressed in QMC's modelling language.

The model shown in Figure 1 describes the quantum teleportation protocol [11] as a sequence of quantum operations on a three-qubit system. The qubit to be transmitted is qubit 0 (denoted `q0`); the second and third qubits (`q1`, `q2` respectively) are placed in an entangled quantum state, to be shared between the two protocol users.

A property is always checked against a single quantum state, in particular, the final state of the whole n-qubit system at the end of a protocol. The logic used for specifying properties of a protocol is a subset of the state logic EQPL [10]. The requirement for the teleportation protocol is that, at the end of the protocol, no matter the measurement outcomes, the third qubit will be in the same state as the first qubit was to begin with, and this qubit will be disentangled from the rest of the system. We can express this requirement, for the case where the input is the quantum state $|0\rangle$, in the input language of QMC using the statement `formula ([q2]) #/\ (!q2);` which corresponds to the EQPL formula $[q_2] \curlywedge (\neg q_2)$. The first part of the formula asserts that the last qubit (`q2`) is disentangled from the rest of the system, while the second part asserts that the current valuation assigns to this qubit a value of 0. The entire formula is true if both parts are true.

QMC implements algorithms for evaluating EQPL formulas over stabiliser states, which are represented internally using a matrix representation (see [12]). In order to check the truth of a particular formula, its truth need to be determined for all possible valuations; the tool automatically extracts all valuations from the internal representation. More interestingly, the tool has been designed to explore all possible executions of a particular protocol arising from different measurement outcomes. Quantum measurement is known to be probabilistic, although at the moment QMC treats it as a source of nondeterminism. Each possible measurement outcome gives rise to a different run of the protocol model, and formulae supplied for verification are automatically checked on the final state produced by each such run. The teleportation example described in previous sections has been model-checked in this manner, and shown to perform its intended function for a given input, for all possible measurement results.

3 Conclusion and Future Work

We have described QMC, a model-checking tool for quantum protocols. As far as we know, it is the first dedicated verification tool (as opposed to simulation systems) for quantum protocols. QMC allows the modelling and verification of properties of protocols expressible in the quantum stabiliser formalism. The logic for expressing properties is a subset of EQPL. Future extensions will include implementing the whole of EQPL, including its constructs for specifying probabilities and coefficients in states; a temporal extension of EQPL [13] will also be implemented, and also the ability to computer the probability that a property is satisfied. We intend to move to a more expressive modelling language, such as CQP [14].

References

[1] Mayers, D.: Unconditional security in quantum cryptography. Journal of the ACM **48** (2001) 351—406

[2] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing. (1984)
[3] Ekert, A.: Quantum cryptography based on Bell's theorem. Physical Review Letters **67** (1991) 661—663
[4] Mayers, D.: Unconditionally secure quantum bit commitment is impossible. In: Fourth Workshop on Physics and Computation — PhysComp '96, Springer–Verlag (1996)
[5] Ryan, P., Schneider, S., Goldsmith, M., Lowe, G., Roscoe, B.: Modelling and Analysis of Security Protocols. Pearson Education (2001)
[6] Holzmann, G.: The SPIN Model Checker: Primer and Reference Manual. Pearson Education (2003)
[7] Glendinning, I.: Links on simulation, modelling, and error prevention for quantum computers (2006) `http://www.vcpc.univie.ac.at/~ian/hotlist/qc/simulation.shtml`.
[8] Nagarajan, R., Gay, S.J.: Formal verification of quantum protocols. Available at arXiv.org. Record: quant-ph/0203086 (2002)
[9] Gay, S.J., Nagarajan, R., Papanikolaou, N.: Probabilistic model–checking of quantum protocols. DCM 2006: Proceedings of the 2nd International Workshop on Developments in Computational Models (2005) arXiv:quant-ph/0504007.
[10] Mateus, P., Sernadas, A.: Weakly complete axiomatization of exogenous quantum propositional logic. Information and Computation **204** (2006) 771—794
[11] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
[12] Aaronson, S., Gottesman, D.: Improved simulation of stabilizer circuits. Physical Review A **70** (2004)
[13] P. Baltazar, R. Chadha, P.M., Sernadas, A.: Towards model-checking quantum security protocols. In P. Dini *et al.*, ed.: Proceedings of the First Workshop on Quantum Security: QSec'07, IEEE Press (2007)
[14] Gay, S.J., Nagarajan, R.: Communicating quantum processes. In: POPL '05: Proceedings of the 32nd ACM Symposium on Principles of Programming Languages, Long Beach, California. (2005)