QMC: A Model Checker For Quantum Systems

Nick Papanikolaou
`nikos@dcs.warwick.ac.uk`

Department of Computer Science
University of Warwick

Joint work with **Rajagopal Nagarajan** (Warwick)
and **Simon Gay** (Glasgow).

Tuesday 26th June 2007
Fourth Central European Quantum Information Processing Workshop
24-27 June 2007, Valtice, Czech Republic

Outline

Context

- Quantum communication and quantum cryptographic protocols are among the greatest successes of QIP research
  - QI protocols combine quantum and classical phenomena in a practical way
  - QI protocols do not require very sophisticated physical resources
  - QI protocols are implementable **today**
  - QC systems are already available
- Some considerations:
  - Quantum phenomena enable protocols with advantages over classical counterparts (e.g. unconditional security for QKD) and also protocols with no classical equivalent (e.g. teleportation)
  - Protocols tend to combine classical computations with quantum transmissions (e.g. BB84 + secret-key reconciliation, privacy amplification) and include quantum computations conditioned on classical measurements

Motivation

Key Point Design of classical communication and cryptographic protocols is a notoriously difficult task with known (and unknown) pitfalls.

- Analysis and verification of **classical protocols** and **systems** is an active and fruitful research area with important benefits
  - Discovery of flaw in Needham–Schröder Public Key Protocol (Lowe, 1996)
  - Pentium V, ARIANE, ...
- Increasing need for **design**, **simulation**, **analysis tools** for quantum communication and cryptographic protocols

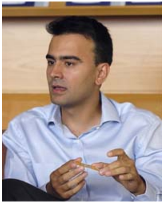
Intended Contribution

- No dedicated tool currently exists for automated verification of *quantum* protocols and communication systems
- (Joint) research programme:
  - To develop a **verification framework** for analysing quantum protocols, esp. for reasoning about **quantum state**, **time**, and **knowledge**.
  - Approach: **Model–checking** (Clarke and Emerson, 1981; Quielle and Sifakis, 1981)

Raja

Simon

Nick



Paulo^{++}

History

- Application of verification techniques to quantum protocols initiated by Nagarajan and Gay **(2002)**
  - Modelled **BB84 protocol** for quantum cryptography in **CCS** and verified simple property using CWB tool.
- Extension of CCS model, first attempt at **PRISM** model by Papanikolaou **(2002-3)**
- Verification of core BB84 protocol using PRISM by Papanikolaou **(2004)**
- Development of CQP specification formalism by Gay, Nagarajan **(2004-5)**
- Verification of simple quantum protocols using PRISM by Gay, Nagarajan, Papanikolaou **(2005)**
- Development of QMC tool and extensions by Gay, Papanikolaou, Nagarajan, Mateus, Baltazar **(2005-present)**

Related Work

- Quantum Programming Languages
  - QCL (Ömer, 1998), QPL (Selinger 2003), ...
  - Quantum process algebras: QPA (Jorrand and Lalire, 2004), **CQP** (Gay and Nagarajan, 2004)
- Quantum Simulators
  - `QCL`, `jaQuzzi`, `QCSim`, `QuIDD`, ...
  - `CHP` (Aaronson and Gottesman, 2005)
- Logics for Quantum Information
  - Abramsky and Duncan, 2004
  - Baltag and Smets, 2004
  - Mateus and Sernadas, 2005+
  - Van Der Meyden and Patra, 2004

Formal Methods

Formal Methods is a branch of TCS which deals with the mathematical description (**specification**) of complex computing systems and comprises techniques for automated analysis and testing (**verification** or **validation**) of such systems.

Specification is important for eliminating ambiguities from an informal system description; specification formalisms are designed so as to have well-defined semantics.

Verification involves the use of specialised algorithms for checking whether a system specification satisfies any number of given properties, usually expressed in some formal logic (e.g. propositional logic, predicate logic, temporal logic, logic of knowledge, . . .)

A verification framework comprises a **modelling language** (for describing systems), a **property specification language or logic**, and an **algorithmic method** for comparing the two.

A Specification Language: CQP

- Simon Gay (Glasgow) and Rajagopal Nagarajan (Warwick) have developed a quantum process algebra, CQP, for modelling such protocols.
- CQP has a formal semantics and a type system.
- Example: modelling the dense coding protocol in CQP:

$$\begin{aligned}&\mathit{Alice}(x:\mathrm{Qbit}, q:\hat{}[\mathrm{Qbit}], n:0..3)\\&\qquad = x \mathrel{*}= \sigma_n \,.\, q![x] \,.\, \mathbf{0}\end{aligned}$$

$$\begin{aligned}&\mathit{Bob}(y:\mathrm{Qbit}, q:\hat{}[\mathrm{Qbit}])\\&\qquad = q?[x:\mathrm{Qbit}] \,.\, x, y \mathrel{*}= \mathrm{CNot} \,.\, x \mathrel{*}= \mathrm{H} \,.\, \mathit{Use}(\mathrm{measure}\ x, y)\end{aligned}$$

$$\begin{aligned}&\mathit{System}(x:\mathrm{Qbit}, y:\mathrm{Qbit}, n:0..3)\\&\qquad = (\mathrm{new}\ q:\hat{}[\mathrm{Qbit}])(\mathit{Alice}(x, q, n) \mid \mathit{Bob}(y, q))\end{aligned}$$

Automated Verification Techniques

Model–checking A system is first described using a **modelling language;** the variables in the model are used to describe important system states. **Properties** are expressed using some logic ranged over those variables. A **model-checking algorithm** checks whether the properties are satisfied in all the various states of the system. Model–checking tends to involve an **exhaustive search** over all possible system behaviours. Tools include `SPIN`, `SMV`, `FDR`, ...

Automated Theorem Proving A system and its properties are described using a **formal logic** (typically predicate logic); the **inference rules** of the logic are built into **theorem-proving software**, which may be used to prove results about the system. The `HOL` theorem-prover is widely used.

Towards Verification of Quantum Protocols

For a verification technique to be developed, one must have an **adequate model** of the types of system to be analysed. For quantum protocols, an adequate model should account for:

- Quantum states*
- Unitary operators
- Measurements
- Classical bits and operations

Model We will model a QI protocol as a **finite, ordered set** of operators applied to a **finite, closed set** of pure quantum states.
Properties We will use the logic **EQPL** (Mateus and Sernadas, 2005) to express properties of quantum states arising in protocols.
Quantum States* We will restrict ourselves to protocols involving quantum states within the **stabiliser formalism** (Gottesman, 1997).

The Pauli Group

- The Pauli operators $\sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z$, along with the identity operator I, and an additional phase of $\pm 1, \pm i$ form a **group**.
- For a 1-qubit system, the Pauli group is defined as follows:

$$\mathcal{P} = \{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\}$$

$\cdot$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	iZ	$-iY$
Y	Y	$-iZ$	I	iX
Z	Z	iY	$-iX$	I

Note: Elements in the full group either commute, or anticommute.

The Stabilizer Subspace

- It turns out that any commuting (abelian) subgroup $\mathcal{S}$ of the Pauli group $\mathcal{P}^{2^n}$, which does not contain $-I$, uniquely defines a **subspace** of Hilbert space $\mathcal{H}^{2^n}$. It is known as a **stabilizer group**.
- The subspace corresponding to $\mathcal{S}$ is known as a **stabilizer subspace.** It contains quantum states which are stabilized by all the operators in $\mathcal{S}$:

$$\mathcal{H}_s^n = \{|\psi\rangle \mid |\psi\rangle \in \mathcal{H}^{2^n}, \forall S \in \mathcal{S} : S|\psi\rangle = |\psi\rangle\}$$

- **Benefit:** instead of specifying the states in the particular subspace of $\mathcal{H}^{2^n}$, we just specify the stabilizer group.
- **Greater Benefit:** instead of specifying the states in the particular subspace of $\mathcal{H}^{2^n}$, we just specify the **generators** of the stabilizer group, each of which has length $\boxed{2 \cdot n + 1 \text{ bits}}$ for an n-qubit system.

The Clifford Group

- The set of operators $U = \{CNot, H, Phase\}$, has the property that:

$$UPU^{\dagger} = P' \qquad \text{where } P, P' \in \mathcal{P}^{2^n}$$

- The operators with this property form a group, known as the **normalizer** of $\mathcal{P}^{2^n}$. This group is also referred to as the **Clifford group**, and is generated by $U = \{CNot, H, Phase\}$.

Example (Hadamard gate)

$\cdot$	H	$Phase$
X	Z	Y
Z	X	Z

Note: by definition $Y = XZ$.

The Stabilizer Formalism

- The operators in the Clifford group are those which arise in most simple quantum protocols.
- The **stabilizer formalism** allows us to capture the effect of these operators and of standard qubit measurement without looking at the actual quantum states.
- Circuits involving only stabilizer operations can be efficiently simulated on a classical computer (**Gottesman–Knill Theorem**).
- We have implemented a **polynomial-time algorithm** for simulating stabilizer circuits (Aaronson and Gottesman, 2004).
- These operators are **not universal**, not even for classical computing: the problem of simulating stabilizer circuits is **complete for the classical complexity class $\oplus L$ (parity-L).**

A Model Checking Tool for Quantum Protocols

- We have built a **dedicated model–checking tool**, QMC, for protocols which can be modelled within the stabilizer formalism.
- QMC has a high–level modelling language related to **CQP** (Gay and Nagarajan, 2005) and **LanQ** (Mlnarík, 2006).
- It allows model–checking of EQPL state formulas over stabilizer states.
- Stabilizer states are represented internally using a binary check matrix, denoting the generators of the corresponding stabilizer group.

Key Point QMC allows the user to simulate a stabilizer circuit. At each step of the simulation, a state formula can be checked.

Simple example

Creation of EPR state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Initial state: $|00\rangle$.

Protocol:

1. Apply $H \otimes I$.
2. Apply $CNot_{12}$.

QMC Input:

```
init 2 2; had 0; cnot 1 2; formula (...);
```

Stabilizer generators:

$$\{Z \otimes I, I \otimes Z\} \xrightarrow{H \otimes I} \{X \otimes I, I \otimes Z\} \xrightarrow{CNot_{12}} \{X \otimes X, Z \otimes Z\}$$

Properties in QMC: EQPL formulae

Core Syntax for Classical Formulae:

$$\phi := \mathbf{q_k} \mid (\neg\phi) \mid (\phi \rightarrow \phi)$$

Core Syntax for Quantum Formulae:

$$\gamma := \phi \mid (t \leq t) \mid [S] \mid (\boxminus\gamma) \mid (\gamma \sqsupset \gamma)$$

Core Syntax for Terms:

$$\begin{array}{lll} t & := & r \mid (\int \alpha) \mid (t + t) \mid (t \cdot t) \mid Re(u) \mid Im(u) \mid \ldots \\ u & := & z \mid |\top\rangle_{FA} \mid (t + it) \mid te^{it} \mid \ldots \end{array}$$

where t is a term, S a list of qubit constants. Note $[S]$ is true if the qubits in S are disentangled from the rest of the system.

Interpretation of EQPL Over Stabilizer Generators

Example

Consider quantum state $|\psi\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |101\rangle)$. These formulae are true:

$$(\mathbf{q_0} \vee \mathbf{q_3}), \qquad (\int(\mathbf{q_0}) \leq \frac{1}{2}), \qquad [\mathbf{q_0}]$$

- EQPL is defined over arbitrary pure states in $\mathcal{H}^{2^n}$.
- We have restricted our implementation of EQPL to stabilizer states.
- Formulae must be checked efficiently, without computing state vector representation if possible.
  - This computation has worst-case complexity $O(2^n)$
- Most formulae seem to require this computation (!) but some optimisations are possible.

Entanglement Normal Forms

Mateus and Sernadas (*Inform. and Comput.* **204** (2006)) place emphasis on the **separability** of Hilbert space considered; this is significant for reasoning about:

- non-entanglement or "F**–factorizability,**" where F is subset of qubit constants;
- **logical amplitudes**, i.e. amplitudes of classical valuations over F.

QMC implements special algorithms and can determine satisfaction of formulae $[S]$ efficiently, viz.:

- Detection of bipartite entanglement in stabiliser states can be performed by placing the stabiliser generators in a **normal form**. Originally studied in (D. Fattal et al., **arXiv:quant-ph/0406168**)
- Polynomial time algorithms for various normal forms for stabilizer states given by K. Audenaert and M.B. Plenio, **arXiv:quant-ph/0505036**

Model–checking algorithms

QMC has two main modes of operation:

Simulation mode EQPL formulae are checked on an individual quantum state arising during simulation of a quantum protocol.

Model–checking mode A protocol is simulated several times, each time with a different measurement outcome. QMC automatically computes all possible measurement outcomes, producing a different protocol run in each case. An EQPL formula is checked on the final quantum state **for all runs**.

Simulation of protocols is efficient: QMC implements a polynomial time algorithm for simulation of stabiliser circuits due to Aaronson and Gottesman (2005).

Implementation of temporal EQPL will involve developing extensions of classical CTL model–checking algorithms.

Goals for Future Work

1. to overcome **efficiency limitations** within current approach
2. to implement **temporal extension of EQPL**!
   - need to consider mixed states - redefinition of EQPL in terms of **density operators**
3. to formalise semantics of the modelling language; also to consider concurrency
4. to consider going **outside stabiliser formalism**
5. Proof system for the logic
6. SAT algorithm and complexity analysis for the logic

Collaboration

We have started a joint Warwick–Glasgow–Lisbon collaboration working towards these goals. (P. Baltazar, S. Gay, P. Mateus, R. Nagarajan, N. Papanikolaou, A. Sernadas)

Review and Conclusion

- We have presented an overview of the QMC model-checking tool for quantum protocols.
- The background and motivation for our automated verification techniques have been discussed.
- The use of the quantum stabiliser formalism for representing and simulating a selected class of protocols has been detailed.
- We have also covered the EQPL logic and aspects of its implementation.

Thanks for listening!