Bisimulation and Congruence Relations for Communicating Quantum Processes

Tim Davidson
tim@dcs.warwick.ac.uk

28th May 2008

Quantum Computing offers the prospect of a radically new paradigm for information processing, with the enticing possibility of being able to crack existing cryptosystems. Quantum Cryptography, on the other hand, promises secure communication even with the advent of a quantum computer in the future. However, achieving the promised level of security requires a thorough analysis of implementations to reveal any potential weaknesses. Existing theoretical techniques are not sufficient for this task since quantum information is subject to the principles of quantum mechanics. Therefore it is necessary to develop new techniques that respect these principles and allow us to reason about quantum processes.

Process calculi are theoretical tools that can be used to analyse the interactions between different components of a system, to establish whether the components work together as intended and to reveal potential flaws in the design. Communicating Quantum Processes (CQP), Quantum Process Algebra (QPAlg), and qCCS are three process calculi that are designed to model processes that use quantum information, while respecting the laws of quantum physics.

Communicating Quantum Processes (CQP) is a language based on the π-calculus and extended by including primitives for measurement and transformations of quantum states, designed for modelling systems that combine quantum and classical communication. This research investigates equivalence relations on CQP processes with bisimilar behaviours, and aims to determine whether there can exist a congruence relation for processes which can be both classical and quantum.

The quest for a congruence for quantum processes was initiated by Lalire. She was able to show that her definition of bisimilarity was preserved under arbitrary contexts by all operators of QPAlg, except for parallel composition. In their paper, Ying et. al. were able to obtain a congruence for all operators of their calculus qCCS, with the caveat that parallel composition only involved processes that were classical. Subsequently, they were able to obtain a congruence for qCCS if all the processes were restricted to be purely quantum.

Quantum entanglement is a property where two or more quantum systems are linked in a way that the manipulation of one can affect the others regardless of physical separation; this is the so-called "spooky action at a distance". Entanglement is therefore an extremely powerful tool and is used extensively in quantum computation and communication, yet at the same time it significantly increases the complexity when reasoning about quantum systems.

It is no surprise therefore that entanglement is the reason why the existing relations are not congruences. Quantum systems are not limited to discrete states like their classical counterparts; while the state of a classical bit can be either 0 or 1, a qubit can be in a superposition of $|0\rangle$ and $|1\rangle$. However, the act of measuring a quantum system irreversibly collapses the state into one of the basis states, destroying any superposition in the process.

When combined with entanglement, measurement of one qubit will collapse the state of another qubit in a separate process. To obtain a congruence relation therefore requires careful consideration of the effects of entanglement between individual processes. Ultimately the aim of this research is to determine the exact conditions in which such a relation can exist. The result will be significant when considering the interactions of component processes in a larger implementation, particularly where security is important.