

# Bisimulation and Congruence Relations for Communicating Quantum Processes

Tim Davidson

`tim@dcs.warwick.ac.uk`

Warwick Postgraduate Colloquium in Computer Science 2008

# Outline

- 1 Introduction
- 2 Quantum Information
- 3 Equivalence Relations
- 4 Conclusion and Future Work

# Motivation

- Formal analysis of **system behaviour**.
- Objective is to show **correctness** of a system, or uncover design/implementation flaws.
- Leads to **reliability** and **robustness**.
- Important where **safety** and **security** are high priorities.

- **Specification:** Formal description of the system and its requirements.
  - Language syntax
  - Semantics
- **Verification:** Proof that the system conforms to its requirements.
  - Mathematical proofs
  - Model checking

- **Specification:** Formal description of the system and its requirements.
  - Language syntax
  - Semantics
- **Verification:** Proof that the system conforms to its requirements.
  - **Mathematical proofs**
  - Model checking

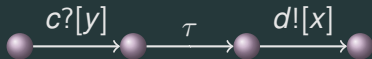
# Process Algebra

- Process algebras are one approach to modelling concurrent systems.
- A process algebra provides a language and semantics to specify the system.
- It defines algebraic laws to manipulate and reason about equivalences between processes.

# Communicating Quantum Processes (CQP)

- *Communicating Quantum Processes (CQP)* is a process algebra designed for **quantum processes** [GN05].
- It is based on the  $\pi$ -calculus (designed for modelling mobile processes).

## Example

$$(c?[y].\{x, y * = CNot\}.d![x].\mathbf{0})$$


- Other quantum process algebras exist:
  - QPAIg [Lal06]
  - qCCS [YFD07]
- The major selling point for CQP is the **type system**.
- No equivalence relations have been defined for CQP.
- No congruence relations exist for general quantum processes.



# Quantum Processes

- Quantum processes are systems in which there is manipulation of **quantum bits** (qubits).
- This could be
  - Computation
  - Communication
  - Other protocols (eg. coin-flipping)

# Quantum Operations

- Quantum processes may involve the following:
  - Preparation of quantum states.
  - Operations on qubits.
  - Transmission of qubits.
  - Quantum measurement.
  - Classical data.

# Quantum Processes in Practice

- Quantum processes have already been implemented and are commercially available:
  - Quantum cryptography over fibre optic cable.
  - Random number generators.
- What is different about quantum processes?
  - **Probabilistic Measurement:** reading the “value” of a qubit does not give a definite result.
  - **No-cloning:** quantum states cannot be copied.
  - **Entanglement:** measuring one qubit can fix the value of another qubit even if they are physically separated.

# What is an equivalence relation?

## Equivalence Relation

An **equivalence relation** is a binary relation between two elements of a set satisfying

- Reflexivity:  $P \sim P$
- Symmetry:  $P \sim Q \Rightarrow Q \sim P$
- Transitivity:  $P \sim Q$  and  $Q \sim R \Rightarrow P \sim R$

## Example

$$P = c?[x].\{x * = Z\}.\{x * = X\}.d![x].0$$

$$Q = c?[x].\{x * = Y\}.d![x].0$$

# What is an equivalence relation?

## Equivalence Relation

An **equivalence relation** is a binary relation between two elements of a set satisfying

- Reflexivity:  $P \sim P$
- Symmetry:  $P \sim Q \Rightarrow Q \sim P$
- Transitivity:  $P \sim Q$  and  $Q \sim R \Rightarrow P \sim R$

## Example

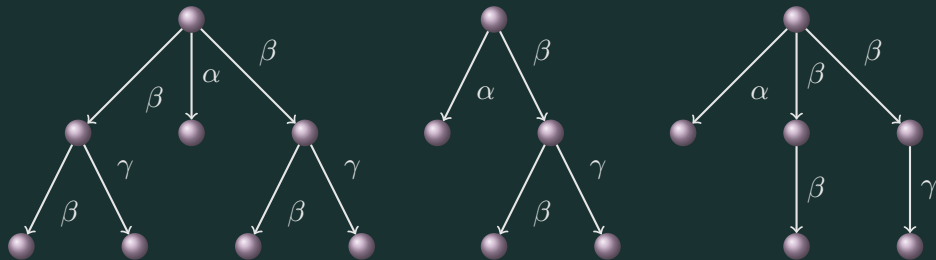
$$P = c?[x].\{x * = Z\}.\{x * = X\}.d![x].0$$

$$Q = c?[x].\{x * = Y\}.d![x].0$$

# Bisimilarity

- **Bisimilarity**

- If process  $P$  can perform action  $\alpha$  then so can  $Q$ , and the resulting processes are also bisimilar.
- If process  $Q$  can perform action  $\alpha$  then so can  $P$ , and the resulting processes are also bisimilar.
- In this case we are only interested in external (observable) actions - **sending** and **receiving**.



- **Congruence**

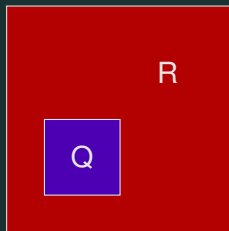
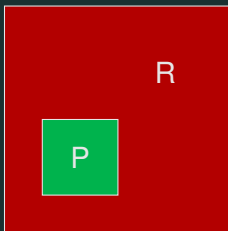
- Processes are equivalent in **any context** (not just in isolation).
- Allows **substitution** of processes.



# Congruence

- **Congruence**

- Processes are equivalent in **any context** (not just in isolation).
- Allows **substitution** of processes.





## Issues: 'Bisimilar' processes that are different

- Processes that perform different (internal) actions may be bisimilar!

### Example

$$P = (\{x * = X\}.0) \quad Q = (\{x * = Z\}.0)$$

## Issues: 'Bisimilar' processes that are different

- Processes that perform different (internal) actions may be bisimilar!

### Example

$$P = (\{x * = X\}.0) \quad Q = (\{x * = Z\}.0)$$

- That's OK because the final quantum state is irrelevant if it is not sent to another process. . .

# Issues: 'Bisimilar' processes that are different

- Processes that perform different (internal) actions may be bisimilar!

## Example

$$P = (\{x * = X\}.0) \quad Q = (\{x * = Z\}.0)$$

- That's OK because the final quantum state is irrelevant if it is not sent to another process. . .
- . . . BUT entanglement can interfere!

# Issues: Entanglement, Measurement and Congruence

- Measurement of an entangled qubit affects the state of other qubits.

# Issues: Entanglement, Measurement and Congruence

- Measurement of an entangled qubit affects the state of other qubits.
- If measurement of an entangled qubit occurs after all observable actions this may have an unconsidered effect on the state of a qubit in a parallel process.

# Issues: Entanglement, Measurement and Congruence

- Measurement of an entangled qubit affects the state of other qubits.
- If measurement of an entangled qubit occurs after all observable actions this may have an unconsidered effect on the state of a qubit in a parallel process.
- This occurs because “different” processes may be bisimilar.

# Issues: Entanglement, Measurement and Congruence

- Measurement of an entangled qubit affects the state of other qubits.
- If measurement of an entangled qubit occurs after all observable actions this may have an unconsidered effect on the state of a qubit in a parallel process.
- This occurs because “different” processes may be bisimilar.
- However many processes rely on qubits that are measured but not observed.

# Summary

- Aiming to find a **congruence relation** for quantum processes.
- Quantum processes are subject to **entanglement** and **probabilistic measurement**.
- Entanglement and measurement prevent this bisimilarity from being a congruence.
- Entanglement and measurement **do not interfere in all cases**
- Identifying these cases should reveal a congruence!



# References

 Simon J. Gay and Rajagopal Nagarajan.


Communicating quantum processes.

In *POPL '05: Proceedings of the 32nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 145–157, New York, NY, USA, 2005. ACM Press.

 Marie Lalire.

Relations among quantum processes: bisimilarity and congruence.

*Mathematical. Structures in Comp. Sci.*, 16(3):407–428, 2006.

 Mingsheng Ying, Yuan Feng, and Runyao Duan.

An algebra of quantum processes.

<http://arxiv.org/abs/0707.0330v1>, Jul 2007.