Exploring Quantum Process Calculi

Gabriele Tedeschi

University of Pisa

October 7, 2022

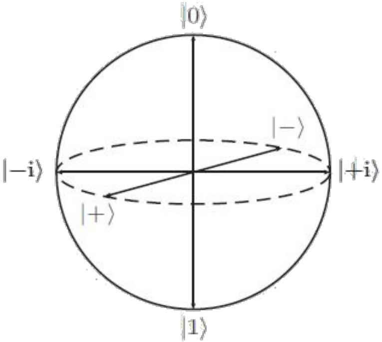
Table Of Contents

Qubits

The simplest quantum system is a **qubit**. Like a bit, a qubit has two separate states, $|0\rangle$ and $|1\rangle$.
A qubit can also be in a linear combination of states, knows as a **superposition**.

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$



Measurements

A qubit in superposition cannot be directly observed, because when it get **measured**, it **decays** in one of its basis states.

$$M_{01}\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) \begin{array}{l} \nearrow \left|0\right\rangle \text{ with probability } |\alpha|^2 \\ \searrow \left|1\right\rangle \text{ with probability } |\beta|^2 \end{array}$$

For example, when measuring the state $\left|+\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle$, we get either $\left|0\right\rangle$ or $\left|1\right\rangle$ with the same probability.

No Cloning theorem

No-Cloning

Quantum information cannot be **duplicated**. That is, given a qubit q_1 in state

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

it is impossible to prepare a qubit q_2 in the same state, without destroying the information in q_1.

This means that, contrary to classical bits, qubits cannot be freely copied, stored or broadcasted to multiple receivers.

Linear qCCS: Type System

lqCCS

Linear qCCS (lqCCS) is an asynchronous value-passing calculus, equipped with a **linear type system** to regulate quantum communication. It features parallelism, non-determinism and quantum operations.

Linear qCCS: Type System

lqCCS

Linear qCCS (lqCCS) is an asynchronous value-passing calculus, equipped with a **linear type system** to regulate quantum communication. It features parallelism, non-determinism and quantum operations.

The type system is needed to prevent **duplication** of quantum information: after receiving a qubit, a process must send it **exactly once**.

$$c?q.H(q).c!q \qquad a?q.\big(b!q \parallel c!q\big) \qquad c?q.H(q).\mathbf{0}$$

Linear qCCS: Type System

lqCCS

Linear qCCS (lqCCS) is an asynchronous value-passing calculus, equipped with a **linear type system** to regulate quantum communication. It features parallelism, non-determinism and quantum operations.

The type system is needed to prevent **duplication** of quantum information: after receiving a qubit, a process must send it **exactly once**.

$c?q.H(q).c!q$ ✓ $\qquad a?q.\big(b!q \parallel c!q\big) \qquad c?q.H(q).\mathbf{0}$

Linear qCCS: Type System

lqCCS

Linear qCCS (lqCCS) is an asynchronous value-passing calculus, equipped with a **linear type system** to regulate quantum communication. It features parallelism, non-determinism and quantum operations.

The type system is needed to prevent **duplication** of quantum information: after receiving a qubit, a process must send it **exactly once**.

$c?q.H(q).c!q$ ✓

$a?q.\big(b!q \parallel c!q\big)$ ✗

$c?q.H(q).\mathbf{0}$

Linear qCCS: Type System

lqCCS

Linear qCCS (lqCCS) is an asynchronous value-passing calculus, equipped with a **linear type system** to regulate quantum communication. It features parallelism, non-determinism and quantum operations.

The type system is needed to prevent **duplication** of quantum information: after receiving a qubit, a process must send it **exactly once**.

$c?q.H(q).c!q$	$a?q.\big(b!q \parallel c!q\big)$	$c?q.H(q).\mathbf{0}$
✓	✗	✗

Linear qCCS: Linearity

In previous calculi, there were **ambiguous** processes like

$$P = c?q.X(q).\mathbf{0} \qquad Q = c?q.H(q).\mathbf{0}$$

Linear qCCS: Linearity

In previous calculi, there were **ambiguous** processes like

$$P = c?q.X(q).\mathbf{0} \qquad Q = c?q.H(q).\mathbf{0}$$

Are P and Q **observationally equivalent**? It depends on what happens to q, different calculi followed different assumptions.

Linear qCCS: Linearity

In previous calculi, there were **ambiguous** processes like

$$P = c?q.X(q).\mathbf{0} \qquad Q = c?q.H(q).\mathbf{0}$$

Are P and Q **observationally equivalent**? It depends on what happens to q, different calculi followed different assumptions.

In lqCCS, the programmer must **explicitly** describe what happens to each qubit

$$P' = c?q.X(q).c!q \qquad Q' = c?q.H(q).c!q$$

$$P'' = c?q.X(q).disc(q) \qquad Q'' = c?q.H(q).disc(q)$$

Linear qCCS: Probabilistic Transition System

- Transition system made of **configurations**, of the form $\langle\, |\psi\rangle\, , P \rangle$

Linear qCCS: Probabilistic Transition System

- Transition system made of **configurations**, of the form $\langle\, |\psi\rangle\, , P \rangle$
- **Reduction system**, without labels

Linear qCCS: Probabilistic Transition System

- Transition system made of **configurations**, of the form $\left\langle\, |\psi\rangle\,, P\right\rangle$
- **Reduction system**, without labels
- Probabilistic behaviour, a configuration can evolve in a **distribution** of configurations

Linear qCCS: Probabilistic Transition System

- Transition system made of **configurations**, of the form $\langle\, |\psi\rangle\,, P\rangle$
- **Reduction system**, without labels
- Probabilistic behaviour, a configuration can evolve in a **distribution** of configurations

$$\langle\, |0\rangle\,, H(q).c!q \parallel c?x.M_{01}[x \triangleright y].disc(x)\rangle$$
$$\downarrow$$
$$\langle\, |+\rangle\,, c!q \parallel c?x.M_{01}[x \triangleright y].disc(x)\rangle$$
$$\downarrow$$
$$\langle\, |+\rangle\,, M_{01}[q \triangleright y].disc(q)\rangle$$
$$\downarrow$$
$$\langle\, |0\rangle\,, disc(q)\rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |1\rangle\,, disc(q)\rangle$$

Linear qCCS: Bisimilarity via barbs and contexts

Saturated Bisimilarity

Two processes are **saturated bisimilar** if they express the same **observable behaviour** under any **context**

Linear qCCS: Bisimilarity via barbs and contexts

Saturated Bisimilarity

Two processes are **saturated bisimilar** if they express the same **observable behaviour** under any **context**

- Observable behaviour (barb): the capability of sending some value on a specific channel

Linear qCCS: Bisimilarity via barbs and contexts

Saturated Bisimilarity

Two processes are **saturated bisimilar** if they express the same **observable behaviour** under any **context**

- Observable behaviour (barb): the capability of sending some value on a specific channel
- Context: a "program" with a hole, like $[-] \parallel R$. We compare P and Q "inside" this context, i.e. we study $P \parallel R$ and $Q \parallel R$.

Linear qCCS: Bisimilarity via barbs and contexts

Saturated Bisimilarity

Two processes are **saturated bisimilar** if they express the same **observable behaviour** under any **context**

- Observable behaviour (barb): the capability of sending some value on a specific channel
- Context: a "program" with a hole, like $[-] \parallel R$. We compare P and Q "inside" this context, i.e. we study $P \parallel R$ and $Q \parallel R$.

The two processes seen before

$$P' = c?q.X(q).c!q \qquad Q' = c?q.H(q).c!q$$

are not bisimilar, because there is a context R which tells them apart

$$R = c?q.M_{01}[q \triangleright x].\,(disc(q) \parallel \textbf{if } x = 0 \textbf{ then } a!0 \textbf{ else } b!0)$$

Probabilistic Bisimilarity

Thanks to lqCCS, we can compare the existing bisimilarities, and find the more appropriate for the quantum setting.

Probabilistic Bisimilarity

Thanks to lqCCS, we can compare the existing bisimilarities, and find the more appropriate for the quantum setting. Consider the two configurations

$$\mathcal{C} = \langle\, |+\rangle\,, M_{01}[q \rhd x].c!q \rangle \to \langle\, |0\rangle\,, c!q \rangle\ {}_{\frac{1}{2}}\!\oplus \langle\, |1\rangle\,, c!q \rangle$$

$$\mathcal{C}' = \langle\, |0\rangle\,, M_{\pm}[q \rhd x].c!q \rangle \to \langle\, |+\rangle\,, c!q \rangle\ {}_{\frac{1}{2}}\!\oplus \langle\, |-\rangle\,, c!q \rangle$$

Probabilistic Bisimilarity

Thanks to lqCCS, we can compare the existing bisimilarities, and find the more appropriate for the quantum setting. Consider the two configurations

$$\mathcal{C} = \langle\, |+\rangle\, , M_{01}[q \rhd x].c!q \rangle \to \langle\, |0\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |1\rangle\, , c!q \rangle$$
$$\mathcal{C}' = \langle\, |0\rangle\, , M_{\pm}[q \rhd x].c!q \rangle \to \langle\, |+\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |-\rangle\, , c!q \rangle$$

According to the usual notion of **probabilistic bisimilarity**, two distributions are bisimilar if they assign the same probability to bisimilar processes. In our example, the two configurations are **not** bisimilar, because they evolve in two non-bisimilar distributions.

Indistinguishable distributions

According to quantum mechanics, it's impossible to distinguish the two sources S and S':

$$S \text{ emits a qubit } |0\rangle \text{ or } |1\rangle \text{ with the same probability}$$
$$S' \text{ emits a qubit } |+\rangle \text{ or } |-\rangle \text{ with the same probability}$$

Suppose we receive a qubit from either S or S', and measure it in the 01 basis. If we measure a qubit from S, it would result in either $|0\rangle$ or $|1\rangle$. If we measure a qubit from S', a $|+\rangle$ qubit would decay in either $|0\rangle$ or $|1\rangle$, and a $|-\rangle$ qubit would decay in either $|0\rangle$ or $|1\rangle$ as well.

Indistinguishable distributions

According to quantum mechanics, it's impossible to distinguish the two sources S and S':

$$S \text{ emits a qubit } |0\rangle \text{ or } |1\rangle \text{ with the same probability}$$
$$S' \text{ emits a qubit } |+\rangle \text{ or } |-\rangle \text{ with the same probability}$$

Suppose we receive a qubit from either S or S', and measure it in the 01 basis. If we measure a qubit from S, it would result in either $|0\rangle$ or $|1\rangle$. If we measure a qubit from S', a $|+\rangle$ qubit would decay in either $|0\rangle$ or $|1\rangle$, and a $|-\rangle$ qubit would decay in either $|0\rangle$ or $|1\rangle$ as well.

Inadequacy of Probabilistic Bisimilarity

The usual notion of probabilistic bisimilarity is too fine, when comparing distributions of quantum configurations.

Solution I: Quantum Bisimilarity

Quantum Bisimilarity

We introduce an *equivalence* relation

$$\equiv \subseteq \mathfrak{D}(Conf) \times \mathfrak{D}(Conf)$$

and a new notion of **quantum bisimilarity**. Two processes are quantum bisimilar if they evolve in distributions that are bisimilar **up to equivalence**.

Solution I: Quantum Bisimilarity

Quantum Bisimilarity

We introduce an *equivalence* relation

$$\equiv \subseteq \mathfrak{D}(Conf) \times \mathfrak{D}(Conf)$$

and a new notion of **quantum bisimilarity**. Two processes are quantum bisimilar if they evolve in distributions that are bisimilar **up to equivalence**.

$$\left\langle\, |+\rangle \,, M_{01}[q \triangleright x].c!q \right\rangle \rightarrow \left\langle\, |0\rangle \,, c!q \right\rangle \,{}_{\frac{1}{2}}\!\oplus \left\langle\, |1\rangle \,, c!q \right\rangle$$

$$\not\sim$$

$$\left\langle\, |0\rangle \,, M_{\pm}[q \triangleright x].c!q \right\rangle \rightarrow \left\langle\, |+\rangle \,, c!q \right\rangle \,{}_{\frac{1}{2}}\!\oplus \left\langle\, |-\rangle \,, c!q \right\rangle$$

Solution I: Quantum Bisimilarity

Quantum Bisimilarity

We introduce an *equivalence* relation

$$\equiv \subseteq \mathfrak{D}(Conf) \times \mathfrak{D}(Conf)$$

and a new notion of **quantum bisimilarity**. Two processes are quantum bisimilar if they evolve in distributions that are bisimilar **up to equivalence**.

$$\langle\, |+\rangle\, , M_{01}[q \triangleright x].c!q \rangle \rightarrow \langle\, |0\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |1\rangle\, , c!q \rangle \equiv \langle\, |+\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |-\rangle\, , c!q \rangle$$

$$\langle\, |0\rangle\, , M_{\pm}[q \triangleright x].c!q \rangle \rightarrow \langle\, |+\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |-\rangle\, , c!q \rangle \equiv \langle\, |+\rangle\, , c!q \rangle \;{}_{\frac{1}{2}}\!\oplus \langle\, |-\rangle\, , c!q \rangle$$

Solution I: Quantum Bisimilarity

Quantum Bisimilarity

We introduce an *equivalence* relation

$$\equiv \subseteq \mathfrak{D}(Conf) \times \mathfrak{D}(Conf)$$

and a new notion of **quantum bisimilarity**. Two processes are quantum bisimilar if they evolve in distributions that are bisimilar **up to equivalence**.

$$\big\langle\, |+\rangle\, , M_{01}[q \triangleright x].c!q \big\rangle \to \big\langle\, |0\rangle\, , c!q \big\rangle \;{}_{\frac{1}{2}}\!\oplus \big\langle\, |1\rangle\, , c!q \big\rangle \equiv \big\langle\, |+\rangle\, , c!q \big\rangle \;{}_{\frac{1}{2}}\!\oplus \big\langle\, |-\rangle\, , c!q \big\rangle$$

$$\sim$$

$$\big\langle\, |0\rangle\, , M_{\pm}[q \triangleright x].c!q \big\rangle \to \big\langle\, |+\rangle\, , c!q \big\rangle \;{}_{\frac{1}{2}}\!\oplus \big\langle\, |-\rangle\, , c!q \big\rangle \equiv \big\langle\, |+\rangle\, , c!q \big\rangle \;{}_{\frac{1}{2}}\!\oplus \big\langle\, |-\rangle\, , c!q \big\rangle$$

Minimal Quantum Process Algebra

Solution II: mQPA

We introduce a new calculus, equipped with a minimal set of features: communication, non-determinism and quantum measurement.
In mQPA, the transitions are of the form

$$\rightarrow \subseteq S \times \mathfrak{D}(S)^{\mathcal{H}}$$

i.e. the probabilistic observable behaviour is **parametric** with respect to an input quantum state.

Minimal Quantum Process Algebra

Solution II: mQPA

We introduce a new calculus, equipped with a minimal set of features: communication, non-determinism and quantum measurement.
In mQPA, the transitions are of the form

$$\rightarrow \subseteq S \times \mathfrak{D}(S)^{\mathcal{H}}$$

i.e. the probabilistic observable behaviour is **parametric** with respect to an input quantum state.

In mQPA, the previous example can be rewritten as

$$(S \ {}_{|0\rangle\langle 0|}\boxplus \ S')(|+\rangle) = S \ {}_{\frac{1}{2}}\oplus \ S'$$
$$(S \ {}_{|+\rangle\langle +|}\boxplus \ S')(|0\rangle) = S \ {}_{\frac{1}{2}}\oplus \ S'$$

What have we seen

What have we seen

- **lqCCS**, an asynchronous linear calculus inspired by qCCS. It rephrases the syntax e semantics of previous calculi in a more standard formalism, and allows to compare different notions of bisimilarity.

What have we seen

- **lqCCS**, an asynchronous linear calculus inspired by qCCS. It rephrases the syntax e semantics of previous calculi in a more standard formalism, and allows to compare different notions of bisimilarity.
- Even though quantum systems exhibit a probabilistic behaviour, **probabilistic bisimilarity** is not really well suited for the quantum setting.

What have we seen

- **lqCCS**, an asynchronous linear calculus inspired by qCCS. It rephrases the syntax e semantics of previous calculi in a more standard formalism, and allows to compare different notions of bisimilarity.
- Even though quantum systems exhibit a probabilistic behaviour, **probabilistic bisimilarity** is not really well suited for the quantum setting.
- **mQPA**, a minimal calculus, pursuing a foundational approach on which are the dynamics and observable properties of quantum systems.

Future work

Future work

- We will work on **non-strong extensions** (weak or barbed bisimilarity), as for example protocol implementation should be weakly bisimilar to its specification.

Future work

- We will work on **non-strong extensions** (weak or barbed bisimilarity), as for example protocol implementation should be weakly bisimilar to its specification.
- From weak transitions, it is possible to define reachability, temporal logics and **model checking**.

Future work

- We will work on **non-strong extensions** (weak or barbed bisimilarity), as for example protocol implementation should be weakly bisimilar to its specification.
- From weak transitions, it is possible to define reachability, temporal logics and **model checking**.
- Saturated bisimilarity can be cumbersome to prove, it will be interesting to explore how the existing **proof techniques** adapt to the quantum setting.

Future work

- We will work on **non-strong extensions** (weak or barbed bisimilarity), as for example protocol implementation should be weakly bisimilar to its specification.
- From weak transitions, it is possible to define reachability, temporal logics and **model checking**.
- Saturated bisimilarity can be cumbersome to prove, it will be interesting to explore how the existing **proof techniques** adapt to the quantum setting.
- We will investigate the relation between **mQPA** semantics and the usual, configuration-based semantics, together with their respective bisimilarities.

Thank you for your attention!