On Coinduction and Quantum Lambda Calculi

Yuxin Deng

East China Normal University

(Joint work with Yuan Feng and Ugo Dal Lago)

To appear at CONCUR’15
Outline

• Motivation
• A quantum $\lambda$-calculus
• Coinductive proof techniques
• Soundness
• Completeness
• Summary
Motivation
Quantum programming languages

Fruitful attempts of language design, e.g.

- **QUIPPER**: an expressive functional higher-order language that can be used to program many quantum algorithms and can generate quantum gate representations using trillions of gates. [Green et al. PLDI’13]

- **LIQUi⟩**: a modular software architecture designed to control quantum hardware - it enables easy programming, compilation, and simulation of quantum algorithms and circuits. [Wecker and Svore. CoRR 2014]

Open problem: Fully abstract denotational semantics wrt operational semantics
Contextual equivalence

An important notion of program equivalence in programming languages. 

\[ M \simeq N \text{ if } \forall C : C[M] \downarrow \iff C[N] \downarrow \]
An example in linear PCF

\[ f_1 \ := \ \text{val}(\lambda x.\ \text{val}(0) \sqcap \text{val}(1)) \]
\[ f_2 \ := \ \text{val}(\lambda x.\ \text{val}(0)) \sqcap \text{val}(\lambda x.\ \text{val}(1)). \]

[Deng and Zhang, TCS, 2015]
An example

\[ f_1 := \text{val}(\lambda x. \text{val}(0) \sqcap \text{val}(1)) \]
\[ f_2 := \text{val}(\lambda x. \text{val}(0)) \sqcap \text{val}(\lambda x. \text{val}(1)). \]
\[ f_1 \not\equiv f_2 \]

\[ C := \text{bind } f = [\_] \text{ in } \text{bind } x = f(0) \text{ in } \text{bind } y = f(0) \text{ in } \text{val}(x = y). \]
Equivalence under linear contexts.

\[ f_1 \quad := \quad \text{val}(\lambda x.\text{val}(0) \sqcap \text{val}(1)) \]
\[ f_2 \quad := \quad \text{val}(\lambda x.\text{val}(0)) \sqcap \text{val}(\lambda x.\text{val}(1)). \]
A Quantum $\lambda$-Calculus
Types

\[ A, B, C ::= \text{qubit} \mid A \rightarrow B \mid !(A \rightarrow B) \mid 1 \mid A \otimes B \mid A \oplus B \mid A^l \]
Terms

\[ M, N, P ::= x \]

| \( \lambda x^A \cdot M \) | \( M N \) | Variables |
| \( \text{skip} \) | \( M; N \) | Abstractions / applications |
| \( M \otimes N \) | \( \text{let } x^A \otimes y^B = M \text{ in } N \) | Skip / seq. compositions |
| \( \text{in}_l M \) | \( \text{in}_r M \) | Tensor products / proj. |
| \( \text{match } P \text{ with } (x^A : M \mid y^B : N) \) | Sums |
| \( \text{split}^A \) | Matches |
| \( \text{letrec } f^{A\to B} x = M \text{ in } N \) | Split |
| \( \text{new} \mid \text{meas} \mid U \) | Recursions |
| | Quantum operators |
Values

\[ V, W ::= x \mid c \mid \lambda x^A.M \mid V \otimes W \mid \text{in}_l V \mid \text{in}_r W \]

where \( c \in \{\text{skip}, \text{split}^A, \text{meas}, \text{new}, \text{U}\} \).

As syntactic sugar \( \text{bit} = 1 \oplus 1 \), \( \text{tt} = \text{in}_r \text{skip} \), and \( \text{ff} = \text{in}_l \text{skip} \).
Typing rules

<table>
<thead>
<tr>
<th>A linear</th>
<th>!Δ, x : A ⊢ x : A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δ, x : A ⊢ M : B</td>
<td>!Δ, Δ' ⊢ M : A ⊸ B</td>
</tr>
<tr>
<td>Δ ⊢ λx^A.M : A ⊸ B</td>
<td>!Δ, Δ', Δ'' ⊢ MN : B</td>
</tr>
<tr>
<td>!Δ, Δ' ⊢ M : A</td>
<td>!Δ, Δ' ⊢ M : B</td>
</tr>
<tr>
<td>!Δ, Δ' ⊢ in_l M : A ⊕ B</td>
<td>!Δ, Δ' ⊢ in_r M : A ⊕ B</td>
</tr>
<tr>
<td>!Δ, Δ' ⊢ P : A ⊕ B</td>
<td>!Δ, Δ'', x : A ⊢ M : C</td>
</tr>
<tr>
<td>!Δ, Δ'', y : B ⊢ N : C</td>
<td>!Δ, Δ'', y : B ⊢ N : C</td>
</tr>
<tr>
<td>!Δ, Δ', Δ'' ⊢ match P with (x^A : M</td>
<td>y^B : N) : C</td>
</tr>
<tr>
<td>!Δ, Δ' ⊢ letrec f^A−^B x = M in N : C</td>
<td>!Δ, Δ' ⊢ letrec f^A−^B x = M in N : C</td>
</tr>
<tr>
<td>!Δ ⊢ new : bit ⊸ qubit</td>
<td>!Δ ⊢ meas : qubit ⊸ bit</td>
</tr>
<tr>
<td>!Δ ⊢ new : bit ⊸ qubit</td>
<td>!Δ ⊢ meas : qubit ⊸ bit</td>
</tr>
</tbody>
</table>

U of arity n

| !Δ ⊢ U : qubit ⊗ n ⊸ qubit ⊗ n |
Quantum closure

Def. A quantum closure is a triple \([q, l, M]\) where

- \(q\) is a normalized vector of \(C^{2n}\), for some integer \(n \geq 0\). It is called the quantum state;
- \(M\) is a term, not necessarily closed;
- \(l\) is a linking function that is an injective map from \(fv(M)\) to the set \([1, \ldots, n]\).

A closure \([q, l, M]\) is total if \(l\) is surjective. In that case we write \(l\) as \(\langle x_1, \ldots, x_n \rangle\) if \(dom(l) = \{x_1, \ldots, x_n\}\) and \(l(x_i) = i\) for all \(i \in \{1 \ldots n\}\).

Non-total closures are allowed. E.g. \(\left[\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \{x \mapsto 1\}, x\right]\)
Small-step reduction axioms

\[
[q, l, (\lambda x^A.M)V] \xrightarrow{1} [q, l, M\{V/x\}]
\]
\[
[q, l, \text{let } x^A \otimes y^B = V \otimes W \text{ in } N] \xrightarrow{1} [q, l, N\{V/x, W/y\}]
\]
\[
[q, l, \text{skip; } N] \xrightarrow{1} [q, l, N]
\]
\[
[q, l, \text{match in } l V \text{ with } (x^A : M \mid y^B : N)] \xrightarrow{1} [q, l, M\{V/x\}]
\]
\[
[q, l, \text{match in } r V \text{ with } (x^A : M \mid y^B : N)] \xrightarrow{1} [q, l, N\{V/y\}]
\]
\[
[q, l, \text{letrec } f^A \mapsto B x = M \text{ in } N] \xrightarrow{1} [q, l, N\{\lambda x^A.\text{letrec } f^A \mapsto B x = M \text{ in } M)/f\}]
\]
\[
[q, \emptyset, \text{new ff}] \xrightarrow{1} [q \otimes |0\rangle, \{x \mapsto n + 1\}, x]
\]
\[
[q, \emptyset, \text{new tt}] \xrightarrow{1} [q \otimes |1\rangle, \{x \mapsto n + 1\}, x]
\]
\[
[\alpha q_0 + \beta q_1, \{x \mapsto i\}, \text{meas } x] \xrightarrow{1 \alpha^2} [r_0, \emptyset, \text{ff}]
\]
\[
[\alpha q_0 + \beta q_1, \{x \mapsto i\}, \text{meas } x] \xrightarrow{1 \beta^2} [r_1, \emptyset, \text{tt}]
\]
\[
[q, l, U(x_1 \otimes \cdots \otimes x_k)] \xrightarrow{1} [r, l, (x_1 \otimes \cdots \otimes x_k)]
\]
Structural rule

\[
\begin{align*}
[q, l, M] & \xrightarrow{p} [r, i, N] \\
[q, j \oplus l, \mathcal{E}[M]] & \xrightarrow{p} [r, j \oplus i, \mathcal{E}[N]]
\end{align*}
\]

where \( \mathcal{E} \) is any evaluation context generated by the grammar

\[
\mathcal{E} ::= \ [ ] \mid \mathcal{E} M \mid V \mathcal{E} \mid \mathcal{E}; M \mid \mathcal{E} \otimes M \\
\mid V \otimes \mathcal{E} \mid \text{in}_l \mathcal{E} \mid \text{in}_r \mathcal{E} \\
\mid \text{let } x^A \otimes y^B = \mathcal{E} \text{ in } M \mid \text{match } \mathcal{E} \text{ with } (x^A : M \mid y^B : N).
\]
Extreme derivative

**Def.** Suppose we have subdistributions $\mu, \mu_0^\rightarrow, \mu_k^\times$ for $k \geq 0$ with the following properties:

\[
\mu = \mu_0^\rightarrow + \mu_0^\times
\]

\[
\mu_0^\rightarrow \rightarrow \mu_1^\rightarrow + \mu_1^\times
\]

\[
\mu_1^\rightarrow \rightarrow \mu_2^\rightarrow + \mu_2^\times
\]

\[
\vdots
\]

and each $\mu_k^\times$ is stable in the sense that $C \not\rightarrow$, for all $C \in [\mu_k^\times]$. Then we call $\mu' := \sum_{k=0}^{\infty} \mu_k^\times$ an extreme derivative of $\mu$, and write $\mu \Rightarrow \mu'$.

NB: $\mu'$ could be a proper subdistribution.
Example

Consider a Markov chain with three states \( \{s_1, s_2, s_3\} \) and two transitions \( s_1 \to \frac{1}{2}s_2 + \frac{1}{2}s_3 \) and \( s_3 \to s_3 \). Then \( s_1 \Rightarrow \frac{1}{2}s_2 \).

Let \( C \) be a quantum closure in the Markov chain \( (Cl, \to) \). Then \( \overline{C} \Rightarrow [C] \) for a unique subdistribution \([C] \).
Big-step reduction

\[
\begin{align*}
C \Downarrow \varepsilon & \quad [q, l, V] \Downarrow [q, l, V] \\
[q, l, M] \Downarrow \sum_{k \in K} p_k \cdot [r_k, i_k, V_k] & \quad \{[r_k, i_k, N] \Downarrow \mu_k\}_{k \in K} \\
[q, l, M \otimes N] \Downarrow \sum_{k \in K} p_k (V_k \otimes \mu_k) & \\
[q, l, M] \Downarrow \sum_{k \in K} p_k \cdot [r_k, i_k, V_k \otimes W_k] & \quad \{[r_k, i_k, (N\{V_k/x, W_k/y\})] \Downarrow \mu_k\}_{k \in K} \\
[q, l, \text{let } x^A \otimes y^B = M \text{ in } N] \Downarrow \sum_{k \in K} p_k \mu_k
\end{align*}
\]

Lem. \([C] = \sup\{\mu \mid C \Downarrow \mu\}\)
Linear contextual equivalence

**Def.** A linear context is a term with a hole, written $C(\Delta; A)$, such that $C[M]$ is a closed program when the hole is filled in by a term $M$, where $\Delta \triangleright M : A$, and the hole lies in linear position.

**Def.** Linear contextual equivalence is the typed relation $\simeq$ given by $\Delta \triangleright M \simeq N : A$ if for every linear context $C$, quantum state $q$ and linking function $l$ such that $\emptyset \triangleright C(\Delta; A) : B$, and both $[q, l, C[M]]$ and $[q, l, C[N]]$ are total quantum closures,

$$|[[q, l, C[M]]]| = |[[q, l, C[N]]]|$$
Coinductive proof techniques
A Probabilistic Labelled Transition System

\[ [q, l, x_1 \otimes \cdots \otimes x_n] \xrightarrow{\text{iU}} [q, l, \mathcal{U}(x_1 \otimes \cdots \otimes x_n)] \]

\[ [q, l, x] \xrightarrow{\text{imeas}} [q, l, \text{meas } x] \]

\[ [q, \emptyset, \text{skip}] \xrightarrow{\text{skip}} [q, \emptyset, \Omega] \]

\[ \emptyset \triangleright V : A \rightarrow B \quad \emptyset \triangleright W : A \]

\[ [q, l, V] \xrightarrow{\oplus[r, W]} [q, l \uplus r, VW] \]

\[ \emptyset \triangleright \text{in}_l V : A \oplus B \quad x : A \triangleright M : C \]

\[ [q, l, \text{in}_l V] \xrightarrow{1[r, M]} [q, l \uplus r, M \{V/x\}] \]

\[ \emptyset \triangleright V \otimes W : A \otimes B \quad x : A, y : B \triangleright M : C \]

\[ [q, l, V \otimes W] \xrightarrow{\otimes[r, M]} [l \uplus r, M \{V/x, W/y\}] \]

\[ C \xrightarrow{\text{eval}} [C] \]
Lifting relations

**Def.** Let $S, T$ be two countable sets and $\mathcal{R} \subseteq S \times T$ be a binary relation. The lifted relation $\mathcal{R}^\dagger \subseteq \mathcal{D}(S) \times \mathcal{D}(T)$ is defined by letting $\mu \mathcal{R}^\dagger \nu$ iff $\mu(X) \leq \nu(\mathcal{R}(X))$ for all $X \subseteq S$.

Here $\mathcal{R}(X) = \{t \in T \mid \exists s \in X. \ s \mathcal{R} t\}$ and $\mu(X) = \sum_{s \in X} \mu(s)$.

There are alternative formulations; related to the Kantorovich metric and the maximum network flow problem. See e.g.
State-based bisimilarity

Def. $C \sim_s D$ iff

- $\text{env}(C) = \text{env}(D)$;
- $[C] \sim_s [D]$;
- if $C, D$ are values then $C \xrightarrow{a} \mu$ implies $D \xrightarrow{a} \nu$ with $\mu \sim_s \nu$, and vice-versa.

Write $\emptyset \triangleright M \sim_s N : A$ if $[q, l, M] \sim_s [q, l, N]$ for any $q$ and $l$ such that $[q, l, M]$ and $[q, l, N]$ are both typable quantum closures.

$$\text{env}(\mu) = \sum_i p_i \cdot \text{tr}_{fv(M)} q_i q_i^\dagger$$ for any $\mu = \sum_i p_i \cdot [q_i, l_i, M_i]$. 

24
Distribution-based bisimilarity

**Def.** \( \mu \xrightarrow{a} \rho \) if \( \rho = \sum_{s \in [\mu]} \mu(s) \cdot \mu_s \), where \( \mu_s \) is determined as follows:

- either \( s \xrightarrow{a} \mu_s \)
- or there is no \( \nu \) with \( s \xrightarrow{a} \nu \), and in this case we set \( \mu_s = \varepsilon \).

**Def.** \( \mu \sim_d \nu \) iff

- \( \text{env}(\mu) = \text{env}(\nu) \);
- \([\mu] \sim_d [\nu] \);
- if \( \mu \) and \( \nu \) are value distributions and \( \mu \xrightarrow{a} \rho \), then \( \nu \xrightarrow{a} \xi \) for some \( \xi \) with \( \rho \sim_d \xi \), and vice-versa.

Write \( \emptyset \triangleright M \sim_d N : A \) if \([ [q, l, M] ] \sim_d [ [q, l, N] ] \) for any \( q \) and \( l \) such that \([q, l, M] \) and \([q, l, N] \) are quantum closures.
\( \sim_s \) is finer than \( \sim_d \)

\[ s \not\sim_s t \]
Similar behaviour by quantum closures
Soundness
Basic idea: Given a relation $\mathcal{R}$, construct a congruence candidate $\mathcal{R}^H$, and then show $\mathcal{R} = \mathcal{R}^H$. 
Howe’s construction

$$\Delta, x : A \triangleright [q, l, M] \mathcal{R}^H [r, j, N] \quad \Delta \triangleright [r, j, \lambda x.A.N] \mathcal{R} [p, i, L]$$

$$\Delta \triangleright [q, l, \lambda x.A.M] \mathcal{R}^H [p, i, L]$$

$$!\Delta, \Delta' \triangleright [q, l, M] \mathcal{R}^H [r, j, N]$$

$$!\Delta, \Delta'' \triangleright [q, i, L] \mathcal{R}^H [r, m, P]$$

$$!\Delta, \Delta', \Delta'' \triangleright [r, j \oplus m, NP] \mathcal{R} [s, n, Q]$$

$$!\Delta, \Delta', \Delta'' \triangleright [q \oplus i, ML] \mathcal{R}^H [s, n, Q]$$

$$!\Delta, \Delta' \triangleright [q, l, M] \mathcal{R}^H [r, j, N]$$

$$!\Delta, \Delta'' \triangleright [q, i, L] \mathcal{R}^H [r, m, P]$$

$$!\Delta, \Delta', \Delta'' \triangleright [r, j \oplus m, N \otimes P] \mathcal{R} [s, n, Q]$$

$$!\Delta, \Delta', \Delta'' \triangleright [q \oplus i, M \otimes L] \mathcal{R}^H [s, n, Q]$$
Congruence

**Lem.** If $\emptyset \triangleright [q, l, M] \sim_s H [r, j, N]$ then $[[q, l, M]] (\sim_s H)^\dagger [[r, j, N]]$.

**Lem.** If $\emptyset \triangleright [q, l, V] \sim_s H [r, j, W]$ then we have that $[q, l, V] \xrightarrow{a} \mu$ implies $[r, j, W] \xrightarrow{a} \nu$ and $\mu (\sim_s H)^\dagger \nu$.

Consequently, $\sim_s = \sim_s H$. Similar arguments apply to $\sim_d$. 
Soundness

Thm. Both $\sim_s$ and $\sim_d$ are included in $\sim$. 
Completeness
A simple testing language

The tests: \[ t ::= \omega \mid a \cdot t \]

Apply a test to a distribution in a reactive pLTS

\[ Pr(\mu, \omega) = |\mu| \]
\[ Pr(\mu, a \cdot t) = Pr(\rho, t) \text{ where } \mu \xrightarrow{a} \rho \]

\[ \mu =\succeq^{T} \nu \text{ iff } \forall t \in T : Pr(\mu, t) = Pr(\nu, t). \]
Characterisation of ∼d by tests

Thm. Let μ and ν be two distributions in a reactive pLTS. Then μ ∼d ν if and only if μ =^T ν.
Converting a test into a context

**Lem.** Let $A$ be a type and $t$ a test. There is a context $C^A_t$ such that $\emptyset \triangleright C^A_t(\emptyset; A): \text{bit}$ and for every $M$ with $\emptyset \triangleright M : A$, we have

$$Pr([q, l, M], t) = |[[q, l, C^A_t[M]]]|$$

where $[q, l, M]$ and $[q, l, C^A_t[M]]$ are quantum closures for any $q$ and $l$. 
Full abstraction

Thm. $\simeq$ coincides with $\sim_d$. 
Conclusion

- Two notions of bisimilarity for reasoning about higher-order quantum programs
- Both bisimilarities are sound with respect to the linear contextual equivalence
- The distribution-based one is complete.
Future work

A denotational model fully abstract with respect to the linear contextual equivalence.
Thank you!