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 λ-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$|\rangle$: 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.

$$M \simeq N \text{ if } \forall \mathcal{C} : \mathcal{C}[M] \Downarrow \iff \mathcal{C}[N] \Downarrow$$

An example in linear PCF

$$
\begin{aligned}
f_1 &:= \mathtt{val}(\lambda x\,.\,\mathtt{val}(0) \sqcap \mathtt{val}(1)) \\
f_2 &:= \mathtt{val}(\lambda x\,.\,\mathtt{val}(0)) \sqcap \mathtt{val}(\lambda x\,.\,\mathtt{val}(1)).
\end{aligned}
$$

[Deng and Zhang, TCS, 2015]

An example

$$
\begin{aligned}
f_1 &:= \mathtt{val}(\lambda x\,.\,\mathtt{val}(0) \sqcap \mathtt{val}(1)) \\
f_2 &:= \mathtt{val}(\lambda x\,.\,\mathtt{val}(0)) \sqcap \mathtt{val}(\lambda x\,.\,\mathtt{val}(1)).
\end{aligned}
$$

$$f_1 \not\approx f_2$$

$$\mathcal{C} := \mathtt{bind}\ f = [\_]\ \mathtt{in}\ \mathtt{bind}\ x = f(0)\ \mathtt{in}\ \mathtt{bind}\ y = f(0)\ \mathtt{in}\ \mathtt{val}(x = y).$$

Linear context?

$$
\begin{aligned}
f_1 &:= \mathtt{val}(\lambda x \,.\, \mathtt{val}(0) \sqcap \mathtt{val}(1)) \\
f_2 &:= \mathtt{val}(\lambda x \,.\, \mathtt{val}(0)) \sqcap \mathtt{val}(\lambda x \,.\, \mathtt{val}(1)).
\end{aligned}
$$

Equivalence under linear contexts.

A Quantum λ-Calculus

Types

$$A, B, C ::= \mathsf{qubit} \mid A \multimap B \mid !(A \multimap B) \mid 1 \mid A \otimes B \mid A \oplus B \mid A^l$$

Terms

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

Values

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

where $c \in \{\mathtt{skip}, \mathtt{split}^A, \mathtt{meas}, \mathtt{new}, \mathtt{U}\}$.

As syntactic sugar $\mathsf{bit} = 1 \oplus 1$, $\mathtt{tt} = \mathtt{in}_r\, \mathtt{skip}$, and $\mathtt{ff} = \mathtt{in}_l\, \mathtt{skip}$.

Typing rules

$$\frac{A \text{ linear}}{!\Delta, x : A \vdash x : A} \qquad \frac{}{!\Delta, x : !(A \multimap B) \vdash x : A \multimap B}$$

$$\frac{\Delta, x : A \vdash M : B}{\Delta \vdash \lambda x^A.M : A \multimap B} \qquad \frac{!\Delta, \Delta' \vdash M : A \multimap B \quad !\Delta, \Delta'' \vdash N : A}{!\Delta, \Delta', \Delta'' \vdash MN : B}$$

$$\frac{!\Delta, \Delta' \vdash M : A}{!\Delta, \Delta' \vdash \mathtt{in}_l\, M : A \oplus B} \qquad \frac{!\Delta, \Delta' \vdash M : B}{!\Delta, \Delta' \vdash \mathtt{in}_r\, M : A \oplus B}$$

$$\frac{!\Delta, \Delta' \vdash P : A \oplus B \quad !\Delta, \Delta'', x : A \vdash M : C \quad !\Delta, \Delta'', y : B \vdash N : C}{!\Delta, \Delta', \Delta'' \vdash \mathtt{match}\ P\ \mathtt{with}\ (x^A : M \mid y^B : N) : C}$$

$$\frac{!\Delta, f : !(A \multimap B), x : A \vdash M : B \quad !\Delta, \Delta', f : !(A \multimap B) \vdash N : C}{!\Delta, \Delta' \vdash \mathtt{letrec}\ f^{A \multimap B} x = M\ \mathtt{in}\ N : C}$$

$$\frac{}{!\Delta \vdash \mathtt{new} : \mathsf{bit} \multimap \mathsf{qubit}} \qquad \frac{}{!\Delta \vdash \mathtt{meas} : \mathsf{qubit} \multimap \mathsf{bit}} \qquad \frac{\mathtt{U} \text{ of arity } n}{!\Delta \vdash \mathtt{U} : \mathsf{qubit}^{\otimes n} \multimap \mathsf{qubit}^{\otimes n}}$$

Quantum closure

Def. A quantum closure is a triple $[q, l, M]$ where

- q is a normalized vector of $\mathbb{C}^{2^n}$, 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 $fqv(M)$ 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. $[\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \{x \mapsto 1\}, x]$

Small-step reduction axioms

$$[q,\, l,\, (\lambda x^A.M)V] \overset{1}{\rightsquigarrow} [q,\, l,\, M\{V/x\}]$$

$$[q,\, l,\, \mathtt{let}\ x^A \otimes y^B = V \otimes W\ \mathtt{in}\ N] \overset{1}{\rightsquigarrow} [q,\, l,\, N\{V/x, W/y\}]$$

$$[q,\, l,\, \mathtt{skip}; N] \overset{1}{\rightsquigarrow} [q,\, l,\, N]$$

$$[q,\, l,\, \mathtt{match}\ \mathtt{in}_l\, V\ \mathtt{with}\ (x^A : M \mid y^B : N)] \overset{1}{\rightsquigarrow} [q,\, l,\, M\{V/x\}]$$

$$[q,\, l,\, \mathtt{match}\ \mathtt{in}_r\, V\ \mathtt{with}\ (x^A : M \mid y^B : N)] \overset{1}{\rightsquigarrow} [q,\, l,\, N\{V/y\}]$$

$$[q,\, l,\, \mathtt{letrec}\ f^{A \multimap B} x = M\ \mathtt{in}\ N] \overset{1}{\rightsquigarrow} [q,\, l,\, N\{(\lambda x^A.\mathtt{letrec}\ f^{A \multimap B} x = M\ \mathtt{in}\ M)/f\}]$$

$$[q,\, \emptyset,\, \mathtt{new}\,\mathtt{ff}] \overset{1}{\rightsquigarrow} [q \otimes |0\rangle,\, \{x \mapsto n+1\},\, x]$$

$$[q,\, \emptyset,\, \mathtt{new}\,\mathtt{tt}] \overset{1}{\rightsquigarrow} [q \otimes |1\rangle,\, \{x \mapsto n+1\},\, x]$$

$$[\alpha q_0 + \beta q_1,\, \{x \mapsto i\},\, \mathtt{meas}\, x] \overset{|\alpha|^2}{\rightsquigarrow} [r_0,\, \emptyset,\, \mathtt{ff}]$$

$$[\alpha q_0 + \beta q_1,\, \{x \mapsto i\},\, \mathtt{meas}\, x] \overset{|\beta|^2}{\rightsquigarrow} [r_1,\, \emptyset,\, \mathtt{tt}]$$

$$[q,\, l,\, \mathtt{U}(x_1 \otimes \cdots \otimes x_k)] \overset{1}{\rightsquigarrow} [r,\, l,\, (x_1 \otimes \cdots \otimes x_k)]$$

Structural rule

$$\frac{[q,\, l,\, M] \overset{p}{\rightsquigarrow} [r,\, i,\, N]}{[q,\, j \uplus l,\, \mathcal{E}[M]] \overset{p}{\rightsquigarrow} [r,\, j \uplus i,\, \mathcal{E}[N]]}$$

where $\mathcal{E}$ is any *evaluation context* generated by the grammar

$$\begin{aligned}\mathcal{E} ::= \quad & [\,] \mid \mathcal{E}\, M \mid V\, \mathcal{E} \mid \mathcal{E}; M \mid \mathcal{E} \otimes M \mid V \otimes \mathcal{E} \mid \mathtt{in}_l\, \mathcal{E} \mid \mathtt{in}_r\, \mathcal{E} \\ & \mid \mathtt{let}\ x^A \otimes y^B = \mathcal{E}\ \mathtt{in}\ M \mid \mathtt{match}\ \mathcal{E}\ \mathtt{with}\ (x^A : M \mid y^B : N).\end{aligned}$$

Extreme derivative

Def. Suppose we have subdistributions μ, $\mu_k^{\rightarrow}$, $\mu_k^{\times}$ for $k \geq 0$ with the following properties:

$$\begin{array}{rcl} \mu & = & \mu_0^{\rightarrow} + \mu_0^{\times} \\ \mu_0^{\rightarrow} & \rightarrow & \mu_1^{\rightarrow} + \mu_1^{\times} \\ \mu_1^{\rightarrow} & \rightarrow & \mu_2^{\rightarrow} + \mu_2^{\times} \\ & \vdots & \end{array}$$

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

NB: μ' could be a proper subdistribution.

Example

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

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

$$\frac{}{C \Downarrow \varepsilon} \qquad \frac{}{[q,l,V] \Downarrow \overline{[q,l,V]}}$$

$$\frac{[q,l,M] \Downarrow \sum_{k\in K} p_k \cdot \overline{[r_k, i_k, V_k]} \quad \{[r_k, i_k, N] \Downarrow \mu_k\}_{k\in K}}{[q,l,M \otimes N] \Downarrow \sum_{k\in K} p_k (V_k \otimes \mu_k)}$$

$$\frac{[q,l,M] \Downarrow \sum_{k\in K} p_k \cdot \overline{[r_k, i_k, V_k \otimes W_k]} \quad \{[r_k, i_k, (N\{V_k/x, W_k/y\})] \Downarrow \mu_k\}_{k\in K}}{[q,l,\mathtt{let}\ x^A \otimes y^B = M\ \mathtt{in}\ N] \Downarrow \sum_{k\in K} p_k \mu_k}$$

Lem. $[\![C]\!] = \sup\{\mu \mid C \Downarrow \mu\}$

Linear contextual equivalence

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

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

$$|[\![[q, l, \mathcal{C}[M]]]\!]| \; = \; |[\![[q, l, \mathcal{C}[N]]]\!]|$$

Coinductive proof techniques

A Probabilistic Labelled Transition System

$$\frac{}{[q, l, x_1 \otimes \cdots \otimes x_n] \xrightarrow{\texttt{i U}} [q, l, \texttt{U}(x_1 \otimes \cdots \otimes x_n)]} \qquad \frac{}{[q, l, x] \xrightarrow{\texttt{i meas}} [q, l, \texttt{meas}\, x]}$$

$$\frac{}{[q, \emptyset, \texttt{skip}] \xrightarrow{\texttt{skip}} [q, \emptyset, \boldsymbol{\Omega}]} \qquad \frac{\emptyset \rhd V : A \multimap B \quad \emptyset \rhd W : A}{[q,\ l,\ V] \xrightarrow{@[r,W]} [q,\ l \uplus r,\ VW]}$$

$$\frac{\emptyset \rhd \texttt{in}_l\, V : A \oplus B \quad x : A \rhd M : C}{[q, l, \texttt{in}_l\, V] \xrightarrow{\texttt{l}\,[r,M]} [q, l \uplus r, M\{V/x\}]}$$

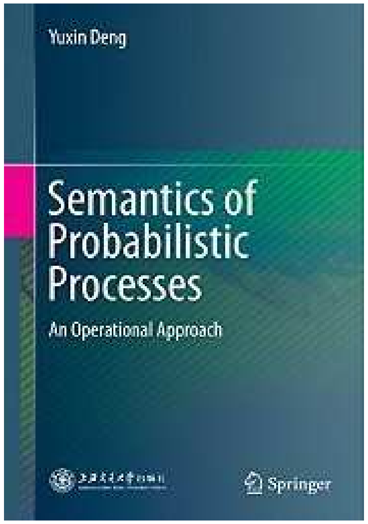
$$\frac{\emptyset \rhd V \otimes W : A \otimes B \qquad x : A, y : B \rhd M : C}{[q, l, V \otimes W] \xrightarrow{\otimes[r,M]} [l \uplus r, M\{V/x, W/y\}]} \qquad \frac{}{C \xrightarrow{eval} [\![C]\!]}$$

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

- $env(C) = env(D)$;
- $[\![C]\!] \sim_s{}^\dagger [\![D]\!]$;
- if C, D are values then $C \xrightarrow{a} \mu$ implies $D \xrightarrow{a} \nu$ with $\mu \sim_s{}^\dagger \nu$, 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.

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

Distribution-based bisimilarity

Def. $\mu \xrightarrow{a} \rho$ if $\rho = \sum_{s \in \lceil \mu \rceil} \mu(s) \cdot \mu_s$, where μ_s is determined as follows:

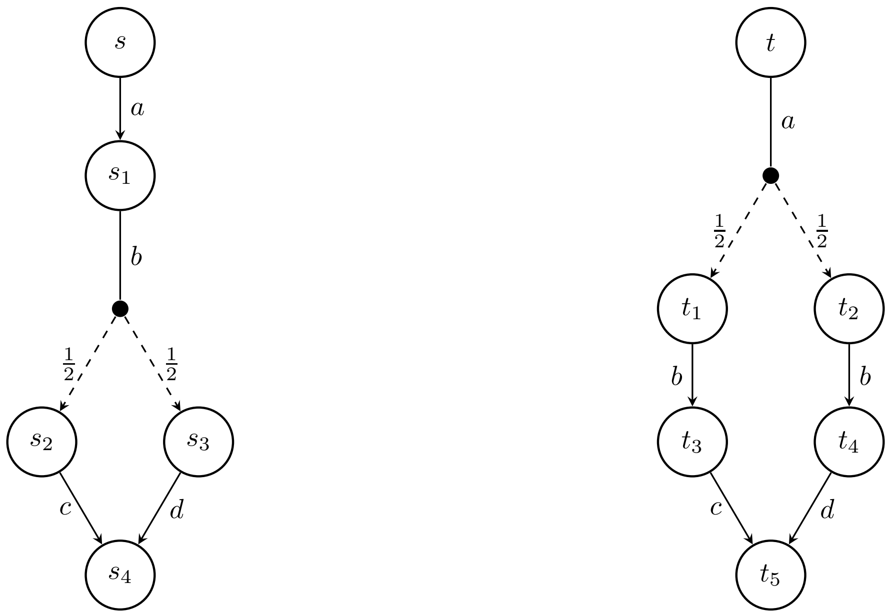
- either $s \xrightarrow{a} \mu_s$
- or there is no ν with $s \xrightarrow{a} \nu$, and in this case we set $\mu_s = \varepsilon$.

Def. $\mu \sim_d \nu$ iff

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

Write $\emptyset \rhd M \sim_d N : A$ 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

$$\begin{tikzcd}
& {[\emptyset, \emptyset, (\lambda xy.\mathtt{meas}(\mathtt{H}(\mathtt{new}\,\mathtt{ff})))x]} \arrow[d, "eval"] & \\
& {[\emptyset, \emptyset, \lambda y.\mathtt{meas}(\mathtt{H}(\mathtt{new}\,\mathtt{ff}))]} \arrow[d, "@[\emptyset, V]"] & \\
& {[\emptyset, \emptyset, \mathtt{meas}(\mathtt{H}(\mathtt{new}\,\mathtt{ff}))]} \arrow[d, dash, "eval"] & \\
& \bullet \arrow[dl, dashed, "\frac{1}{2}"'] \arrow[dr, dashed, "\frac{1}{2}"] & \\
{[\emptyset, \emptyset, \mathtt{ff}]} \arrow[dr, "\mathtt{ff}"'] & & {[\emptyset, \emptyset, \mathtt{tt}]} \arrow[dl, "\mathtt{tt}"] \\
& {[\emptyset, \emptyset, \mathbf{\Omega}]} &
\end{tikzcd}$$

$$\begin{tikzcd}
& {[\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \langle x_1 x_2 \rangle, (\lambda xy.\mathtt{meas}\, x_1)(\mathtt{meas}\, x_2)]} \arrow[d, dash, "eval"] & \\
& \bullet \arrow[dl, dashed, "\frac{1}{2}"'] \arrow[dr, dashed, "\frac{1}{2}"] & \\
{[|0\rangle, \langle x_1 \rangle, \lambda y.\mathtt{meas}\, x_1]} \arrow[d, "@[\emptyset, V]"'] & & {[|1\rangle, \langle x_1 \rangle, \lambda y.\mathtt{meas}\, x_1]} \arrow[d, "@[\emptyset, V]"] \\
{[|0\rangle, \langle x_1 \rangle, \mathtt{meas}\, x_1]} \arrow[d, "eval"'] & & {[|1\rangle, \langle x_1 \rangle, \mathtt{meas}\, x_1]} \arrow[d, "eval"] \\
{[\emptyset, \emptyset, \mathtt{ff}]} \arrow[dr, "\mathtt{ff}"'] & & {[\emptyset, \emptyset, \mathtt{tt}]} \arrow[dl, "\mathtt{tt}"] \\
& {[\emptyset, \emptyset, \mathbf{\Omega}]} &
\end{tikzcd}$$

Soundness

Congruence

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

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

$$\frac{\begin{array}{c} !\Delta, \Delta' \rhd [q, l, M] \ \mathcal{R}^H \ [r, j, N] \\ !\Delta, \Delta'' \rhd [q, i, L] \ \mathcal{R}^H \ [r, m, P] \\ !\Delta, \Delta', \Delta'' \rhd [r, j \uplus m, NP] \ \mathcal{R} \ [s, n, Q] \end{array}}{!\Delta, \Delta', \Delta'' \rhd [q, l \uplus i, ML] \ \mathcal{R}^H \ [s, n, Q]}$$

$$\frac{\begin{array}{c} !\Delta, \Delta' \rhd [q, l, M] \ \mathcal{R}^H \ [r, j, N] \\ !\Delta, \Delta'' \rhd [q, i, L] \ \mathcal{R}^H \ [r, m, P] \\ !\Delta, \Delta', \Delta'' \rhd [r, j \uplus m, N \otimes P] \ \mathcal{R} \ [s, n, Q] \end{array}}{!\Delta, \Delta', \Delta'' \rhd [q, l \uplus i, M \otimes L] \ \mathcal{R}^H \ [s, n, Q]}$$

Congruence

Lem. If $\emptyset \rhd [q, l, M] \sim_s{}^H [r, j, N]$ then $[\![[q, l, M]]\!] \left(\sim_s{}^H\right)^\dagger [\![[r, j, N]]\!]$.

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

Consequently, $\sim_s = \sim_s{}^H$. Similar arguments apply to $\sim_d$.

Soundness

Thm. Both $\sim_s$ and $\sim_d$ are included in $\simeq$.

Completeness

A simple testing language

The tests: $\mathtt{t} ::= \omega \mid a \cdot \mathtt{t}$

Apply a test to a distribution in a reactive pLTS

$$\begin{array}{rcl} Pr(\mu, \omega) & = & |\mu| \\ Pr(\mu, a \cdot \mathtt{t}) & = & Pr(\rho, \mathtt{t}) \text{ where } \mu \xrightarrow{a} \rho \end{array}$$

$\mu =^{\mathcal{T}} \nu$ iff $\forall \mathtt{t} \in \mathcal{T} : Pr(\mu, \mathtt{t}) = Pr(\nu, \mathtt{t})$.

Characterisation of $\sim_d$ by tests

Thm. Let μ and ν be two distributions in a reactive pLTS. Then $\mu \sim_d \nu$ if and only if $\mu =^{\mathcal{T}} \nu$.

Converting a test into a context

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

$$Pr([q, l, M], \mathtt{t}) \;=\; |[\![[q, l, \mathcal{C}_{\mathtt{t}}^{A}[M]]]\!]|$$

where $[q, l, M]$ and $[q, l, \mathcal{C}_{\mathtt{t}}^{A}[M]]$ are quantum closures for any q and l.

Full abstraction

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

Summary

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!