Context Equivalences and Metrics in Probabilistic λ-Calculi

Ugo Dal Lago

(Based on joint work with *Michele Alberti*, *Alberto Cappai*,
Raphaëlle Crubillé, *Davide Sangiorgi*,...)

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Inria informatiques mathématiques

QSLC, Marseille, September 3rd, 2016

Syntax and Operational Semantics of $\Lambda_\oplus$

- **Terms**: $M ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M;$

Syntax and Operational Semantics of $\Lambda_{\oplus}$

- **Terms**: $M ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M$;
- **Values**: $V ::= \lambda x.M$;

Syntax and Operational Semantics of $\Lambda_\oplus$

- **Terms**: $M ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M$;
- **Values**: $V ::= \lambda x.M$;
- **Value Distributions**:

$$V \xrightarrow{\mathcal{D}} \mathcal{D}(V) \in \mathbb{R}_{[0,1]} \qquad\qquad \sum \mathcal{D} = \sum_{V} \mathcal{D}(V) \leq 1.$$

Syntax and Operational Semantics of $\Lambda_\oplus$

- **Terms**: $M ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M$;
- **Values**: $V ::= \lambda x.M$;
- **Value Distributions**:

$$V \xrightarrow{\mathcal{D}} \mathcal{D}(V) \in \mathbb{R}_{[0,1]} \qquad\qquad \sum \mathcal{D} = \sum_{V} \mathcal{D}(V) \leq 1.$$

- **Semantics**: $[\![M]\!] = \sup_{M \Downarrow \mathcal{D}} \mathcal{D}$;

Syntax and Operational Semantics of $\Lambda_\oplus$

$$\frac{}{M \Downarrow \emptyset} \qquad \frac{}{V \Downarrow \{V^1\}} \qquad \frac{M \Downarrow \mathcal{D} \qquad N \Downarrow \mathcal{E}}{M \oplus N \Downarrow \frac{1}{2}\mathcal{D} + \frac{1}{2}\mathcal{E}}$$

$$\frac{M \Downarrow \mathscr{K} \qquad \{P[N/x] \Downarrow \mathscr{E}_P\}_{\lambda x.P \in \mathsf{S}\mathscr{K}}}{MN \Downarrow \sum_{\lambda x.P \in \mathsf{S}\mathscr{K}} \mathscr{K}(\lambda x.P) \cdot \mathscr{E}_P}$$

$V \mapsto \mathcal{D}(V) \in \mathbb{R}_{[0,1]}$ $\quad \sum \mathcal{D} = \sum_{V} \mathcal{D}(V) \leq 1.$

- **Semantics**: $[\![M]\!] = \sup_{M \Downarrow \mathcal{D}} \mathcal{D}$;

Syntax and Operational Semantics of $\Lambda_\oplus$

- **Terms**: $M ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M$;
- **Values**: $V ::= \lambda x.M$;
- **Value Distributions**:

$$V \xrightarrow{\mathcal{D}} \mathcal{D}(V) \in \mathbb{R}_{[0,1]} \qquad\qquad \sum \mathcal{D} = \sum_{V} \mathcal{D}(V) \leq 1.$$

- **Semantics**: $[\![M]\!] = \sup_{M \Downarrow \mathcal{D}} \mathcal{D}$;
- **Context Equivalence**: $M \equiv N$ iff for every context C it holds that $\sum [\![C[M]]\!] = \sum [\![C[N]]\!]$.

Syntax and Operational Semantics of $\Lambda_{\oplus}$

- **Terms**: $M ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M;$
- **Values**: $V ::= \lambda x.M;$
- **Value Distributions**:

$C ::= [\cdot] \;\big|\; \lambda x.C \;\big|\; CM \;\big|\; MC \;\big|\; C \oplus M \;\big|\; M \oplus C$

$V) \leq 1.$

- **Semantics**: $[\![M]\!] = \sup_{M \Downarrow \mathcal{D}} \mathcal{D};$
- **Context Equivalence**: $M \equiv N$ iff for every context C it holds that $\sum [\![C[M]]\!] = \sum [\![C[N]]\!]$.

Syntax and Operational Semantics of $\Lambda_\oplus$

- **Terms**: $M ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M$;
- **Values**: $V ::= \lambda x.M$;
- **Value Distributions**:

$$V \xrightarrow{\mathcal{D}} \mathcal{D}(V) \in \mathbb{R}_{[0,1]} \qquad\qquad \sum \mathcal{D} = \sum_{V} \mathcal{D}(V) \leq 1.$$

- **Semantics**: $[\![M]\!] = \sup_{M \Downarrow \mathcal{D}} \mathcal{D}$;
- **Context Equivalence**: $M \equiv N$ iff for every context C it holds that $\sum [\![C[M]]\!] = \sum [\![C[N]]\!]$.
- **Context Distance**: $\delta^C(M, N) = \sup_C |\sum [\![C[M]]\!] - \sum [\![C[N]]\!]|$.

Examples

$$I \oplus \Omega \qquad \text{vs.} \qquad I$$

Examples

$\lambda x.x$

$$I \oplus \Omega \qquad \text{vs.} \qquad I$$

Examples

$\Delta\Delta = (\lambda x.xx)(\lambda x.xx)$

$$I \oplus \Omega \qquad \text{vs.} \qquad I$$

Exam

Not Context Equivalent: $C = [\cdot]$.

Context Distance? Consider $C_n = (\lambda x.\ \underbrace{x \ldots x}_{n \text{ times}})[\cdot]$.

$$I \oplus \Omega \qquad \text{vs.} \qquad I$$

Examples

$I \oplus \Omega$ vs. I

$I \oplus \Omega$ vs. Ω

Examples

Not Context Equivalent: $C = [\cdot]$.
Context Distance? Cannot Easily Amplify.

$I \oplus \Omega$ vs. I

$I \oplus \Omega$ vs. Ω

Examples

$$I \oplus \Omega \qquad \text{vs.} \qquad I$$

$$I \oplus \Omega \qquad \text{vs.} \qquad \Omega$$

$$(\lambda x.I) \oplus (\lambda x.\Omega) \qquad \text{vs.} \qquad \lambda x.I \oplus \Omega$$

Examples

$I \oplus \Omega$ vs. I

Not Context Equivalent in CBV: $C = (\lambda x.x(xI))[\cdot]$
Apparently Context Equivalent in CBN.

$I \oplus \Omega$ vs. Ω

$(\lambda x.I) \oplus (\lambda x.\Omega)$ vs. $\lambda x.I \oplus \Omega$

A Labelled Markov Chain for $\Lambda_\oplus$

Terms

A Labelled Markov Chain for $\Lambda_{\oplus}$

Terms

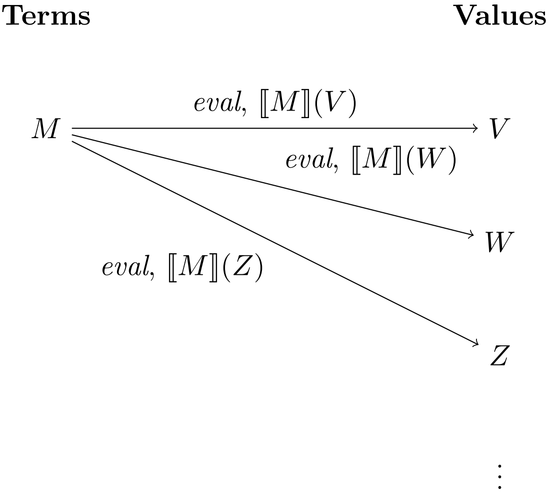
Values

A Labelled Markov Chain for $\Lambda_{\oplus}$

Terms **Values**

M

A Labelled Markov Chain for $\Lambda_\oplus$



A Labelled Markov Chain for $\Lambda_\oplus$

Terms	**Values**
	$\lambda x.N$

A Labelled Markov Chain for $\Lambda_\oplus$

$$\begin{tikzcd}
\textbf{Terms} & & \textbf{Values} \\
N\{W/x\} & & \lambda x.N \arrow[ll, "{W,\ 1}"']
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\lambda x.M \;\; \mathcal{R} \;\; \lambda x.N$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N & M\{L/x\}
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rr, bend right, "L"'] & M\{L/x\} & N\{L/x\}
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrr, bend right, "L"'] & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrr, bend right, "L"'] & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$M \quad \mathcal{R} \quad N$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrrr, bend right, "L"'] & & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & \llbracket M \rrbracket \\
M \arrow[rrru, bend left, "eval"] & \mathcal{R} & N &
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrrr, bend right, "L"'] & & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & \llbracket M \rrbracket \\
M \arrow[urrr, bend left, "eval"] & \mathcal{R} & N \arrow[dr, bend right, "eval"'] & \\
 & & & \llbracket N \rrbracket
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrr, bend right, "L"'] & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & \llbracket M \rrbracket \arrow[dr, bend left] & \\
M \arrow[urrr, bend left, "eval"] & \mathcal{R} & N \arrow[dr, bend right, "eval"'] & & \llbracket M \rrbracket(E) \\
 & & & \llbracket N \rrbracket &
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrr, bend right, "L"'] & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & \llbracket M \rrbracket \arrow[dr, bend left] & & \\
M \arrow[urrr, bend left, "\mathit{eval}"] & \mathcal{R} & N \arrow[dr, bend right, "\mathit{eval}"'] & & \llbracket M \rrbracket(E) & \llbracket N \rrbracket(E) \\
 & & & \llbracket N \rrbracket \arrow[urr, bend right] & &
\end{tikzcd}$$

Probabilistic Bisimulation Relations

$$\begin{tikzcd}
\lambda x.M \arrow[rrr, bend left, "L"] & \mathcal{R} & \lambda x.N \arrow[rrr, bend right, "L"'] & M\{L/x\} & \mathcal{R} & N\{L/x\}
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & \llbracket M \rrbracket \arrow[dr, bend left] & \\
M \arrow[urrr, bend left, "eval"] & \mathcal{R} & N \arrow[dr, bend right, "eval"'] & & \llbracket M \rrbracket(E) = \llbracket N \rrbracket(E) \\
 & & & \llbracket N \rrbracket \arrow[ur, bend right] &
\end{tikzcd}$$

Bisimilarity vs. Context Equivalence

- **Bisimilarity**: the union $\sim$ of all bisimulation relations.
- Is it that $\sim$ is included in $\equiv$? How to prove it?
- Natural strategy: is $\sim$ a congruence?
  - If this is the case:

$$\begin{aligned} M \sim N &\implies C[M] \sim C[N] \implies \sum [\![C[M]]\!] = \sum [\![C[N]]\!] \\ &\implies M \equiv N. \end{aligned}$$

  - This is a necessary sanity check anyway.
- The naïve proof by induction **fails**, due to application: from $M \sim N$, one cannot directly conclude that $LM \sim LN$.

Howe's Technique

$\mathcal{R}$ $\mathcal{R}^H$

Howe's Technique

$$\begin{tikzcd}
\mathcal{R} \arrow[rr, bend left, "\subseteq"] & & \mathcal{R}^H
\end{tikzcd}$$

Howe's Technique

$\mathcal{R}^H$ is a **Congruence** whenever $\mathcal{R}$ is an equivalence

$$\begin{tikzcd}
\mathcal{R} \arrow[rr, bend left, "\subseteq"] & & \mathcal{R}^H
\end{tikzcd}$$

Howe's Technique

$\sim^H$ is a **Congruence**

$$\begin{tikzcd}
\sim \arrow[rr, bend left, "\subseteq"] & & \sim^H
\end{tikzcd}$$

Howe's Technique

$\sim^H$ is a **Congruence**

$$\begin{tikzcd}
\sim \arrow[r, bend left, "\subseteq"] & \sim^H \arrow[l, bend left, "\supseteq"]
\end{tikzcd}$$

Key Lemma

Our Neighborhood

- Λ, where we observe **convergence**

	$\sim \subseteq \equiv$	$\equiv \subseteq \sim$
CBN	✓	✓
CBV	✓	✓

[Abramsky1990, Howe1993]

- $\Lambda_{\oplus}$ with nondeterministic semantics, where we observe **convergence**, in its **may** or **must** flavors.

	$\sim \subseteq \equiv$	$\equiv \subseteq \sim$
CBN	✓	×
CBV	✓	×

[Ong1993, Lassen1998]

The Probabilistic Case

- $\Lambda_{\oplus}$ with probabilistic semantics.

	$\sim \subseteq \equiv$	$\equiv \subseteq \sim$
CBN	✓	✗
CBV	✓	✓

The Probabilistic Case

- $\Lambda_{\oplus}$ with probabilistic semantics.

	$\sim\ \subseteq\ \equiv$	$\equiv\ \subseteq\ \sim$
CBN	✓	✗
CBV	✓	✓

- Counterexample for CBN: $(\lambda x.I) \oplus (\lambda x.\Omega) \not\sim \lambda x.I \oplus \Omega$
- **Where** these discrepancies come from?

The Probabilistic Case

- $\Lambda_\oplus$ with probabilistic semantics.

	$\sim\ \subseteq\ \equiv$	$\equiv\ \subseteq\ \sim$
CBN	✓	✗
CBV	✓	✓

- Counterexample for CBN: $(\lambda x.I) \oplus (\lambda x.\Omega) \not\sim \lambda x.I \oplus \Omega$
- **Where** these discrepancies come from?
- From **testing**!

The Probabilistic Case

- $\Lambda_{\oplus}$ with probabilistic semantics.

	$\sim\ \subseteq\ \equiv$	$\equiv\ \subseteq\ \sim$
CBN	✓	✗
CBV	✓	✓

- Counterexample for CBN: $(\lambda x.I) \oplus (\lambda x.\Omega) \not\sim \lambda x.I \oplus \Omega$
- **Where** these discrepancies come from?
- From **testing**!
- Bisimulation can be characterized by testing equivalence as follows:

Calculus	**Testing**
Λ	$T ::= \omega \mid a \cdot T$
$P\Lambda_{\oplus}$	$T ::= \omega \mid a \cdot T \mid \langle T, T \rangle$
$N\Lambda_{\oplus}$	$T ::= \omega \mid a \cdot T \mid \wedge_{i \in I} T_i \mid \ldots$

The Probabilistic Case

- $\Lambda_{\oplus}$ with probabilistic semantics.

	$\precsim\ \subseteq\ \leq$	$\leq\ \subseteq\ \precsim$
CBN	✓	×
CBV	✓	×

The Probabilistic Case

- $\Lambda_{\oplus}$ with probabilistic semantics.

	$\precsim \subseteq \leq$	$\leq \subseteq \precsim$
CBN	✓	×
CBV	✓	×

- Probabilistic simulation can be characterized by testing as follows:

$$T ::= \omega \;\Big|\; a \cdot T \;\Big|\; \langle T, T \rangle \;\Big|\; T \vee T$$

The Probabilistic Case

- $\Lambda_\oplus$ with probabilistic semantics.

	$\precsim \subseteq \leq$	$\leq \subseteq \precsim$
CBN	✓	✗
CBV	✓	✗

- Probabilistic simulation can be characterized by testing as follows:

$$T ::= \omega \;\Big|\; a \cdot T \;\Big|\; \langle T, T \rangle \;\Big|\; T \vee T$$

- Full abstraction can be recovered if endowing $\Lambda_\oplus$ with parallel disjunction [CDLSV2015].

	$\precsim \subseteq \leq$	$\leq \subseteq \precsim$
CBN	✓	✗
CBV	✓	✓

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M;$

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M$;
- **Terms**: any preterm M such that $\Gamma \vdash M$.

Con

$$\frac{}{\Gamma, x \vdash x} \qquad \frac{x, \Gamma \vdash M}{\Gamma \vdash \lambda x.M} \qquad \frac{\Gamma \vdash M \qquad \Delta \vdash N}{\Gamma, \Delta \vdash MN} \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash N}{\Gamma \vdash M \oplus N}$$

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M$;
- **Terms**: any preterm M such that $\Gamma \vdash M$.

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M$;
- **Terms**: any preterm M such that $\Gamma \vdash M$.
- **Behavioural Distance** δ^b.
  - The metric analogue to bisimilarity.

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\big|\; \lambda x.M \;\big|\; MM \;\big|\; M \oplus M$;
- **Terms**: any preterm M such that $\Gamma \vdash M$.
- **Behavioural Distance** δ^b.
  - The metric analogue to bisimilarity.
- **Trace Distance** δ^t.
  - The maximum distance induced by traces, i.e., sequences of actions: $\delta^t(M, N) = \sup_{\mathsf{T}} |Pr(M, \mathsf{T}) - Pr(N, \mathsf{T})|$.

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M;$
- **Terms**: any preterm M such that $\Gamma \vdash M$.
- **Behavioural Distance** δ^b.
  - The metric analogue to bisimilarity.
- **Trace Distance** δ^t.
  - The maximum distance induced by traces, i.e., sequences of actions: $\delta^t(M, N) = \sup_{\mathsf{T}} |Pr(M, \mathsf{T}) - Pr(N, \mathsf{T})|$.
- **Soundness and Completeness Results:**

$\delta^b \leq \delta^c$	$\delta^c \leq \delta^b$	$\delta^t \leq \delta^c$	$\delta^c \leq \delta^t$
✓	✗	✓	✓

Context Distance: the Affine Case [CDL2015]

- Let us consider a simple fragment of $\Lambda_{\oplus}$, first.
- **Preterms**: $M, N ::= x \;\Big|\; \lambda x.M \;\Big|\; MM \;\Big|\; M \oplus M$;
- **Terms**: any preterm M such that $\Gamma \vdash M$.
- **Behavioural Distance** δ^b.
  - The metric analogue to bisimilarity.
- **Trace Distance** δ^t.
  - The maximum distance induced by traces, i.e., sequences of actions: $\delta^t(M, N) = \sup_{\mathsf{T}} |Pr(M, \mathsf{T}) - Pr(N, \mathsf{T})|$.
- **Soundness and Completeness Results:**

$\delta^b \leq \delta^c$	$\delta^c \leq \delta^b$	$\delta^t \leq \delta^c$	$\delta^c \leq \delta^t$
✓	×	✓	✓

- **Example**: $\delta^t(I, I \oplus \Omega) = \delta^t(I \oplus \Omega, \Omega) = \frac{1}{2}$.

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.
- The underlying LMC **does not** reflect copying.

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.
- The underlying LMC **does not** reflect copying.
- **A Tuple LMC**.
  - **Preterms**:
    $M ::= x \;\Big|\; \lambda x.M \;\Big|\; \lambda !x.M \;\Big|\; MM \;\Big|\; M \oplus M \;\Big|\; !M$
  - **Terms**: any preterm M such that $\Gamma \vdash M$.
  - **States**: *sequences* of terms, rather than terms.
  - **Actions** not only model parameter passing, but also *copying* of terms.

Context Distance: the General Case [CDL2016]

$$\frac{}{!\Gamma, x \vdash x} \qquad \frac{}{!\Gamma, !x \vdash x} \qquad \frac{x, \Gamma \vdash M}{\Gamma \vdash \lambda x.M} \qquad \frac{!x, \Gamma \vdash M}{\Gamma \vdash \lambda !x.M}$$

$$\frac{!\Gamma \vdash M}{!\Gamma \vdash !M} \qquad \frac{\Gamma, !\Theta \vdash M \qquad \Delta, !\Theta \vdash N}{\Gamma, \Delta, \Theta \vdash MN} \qquad \frac{\Gamma \vdash M \qquad \Gamma \vdash N}{\Gamma \vdash M \oplus N}$$

- N
  δ
- T
- A Tuple LMC:
  - **Preterms**:
    $M ::= x \;\big|\; \lambda x.M \;\big|\; \lambda !x.M \;\big|\; MM \;\big|\; M \oplus M \;\big|\; !M$
  - **Terms**: any preterm M such that $\Gamma \vdash M$.
  - **States**: *sequences* of terms, rather than terms.
  - **Actions** not only model parameter passing, but also *copying* of terms.

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.
- The underlying LMC **does not** reflect copying.
- **A Tuple LMC**.
  - **Preterms**:
    $M ::= x \;\Big|\; \lambda x.M \;\Big|\; \lambda!x.M \;\Big|\; MM \;\Big|\; M \oplus M \;\Big|\; !M$
  - **Terms**: any preterm M such that $\Gamma \vdash M$.
  - **States**: *sequences* of terms, rather than terms.
  - **Actions** not only model parameter passing, but also *copying* of terms.
- **Soundness and Completeness Results:**

$\delta^t \leq \delta^c$	$\delta^c \leq \delta^t$
✓	✓

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.
- The underlying LMC **does not** reflect copying.
- **A Tuple LMC**.
  - **Preterms**:
    $M ::= x \;\Big|\; \lambda x.M \;\Big|\; \lambda !x.M \;\Big|\; MM \;\Big|\; M \oplus M \;\Big|\; !M$
  - **Terms**: any preterm M such that $\Gamma \vdash M$.
  - **States**: *sequences* of terms, rather than terms.
  - **Actions** not only model parameter passing, but also *copying* of terms.
- **Soundness and Completeness Results:**

$\delta^t \leq \delta^c$	$\delta^c \leq \delta^t$
✓	✓

- **Examples**: $\delta^t(!(I \oplus \Omega), !\Omega) = \frac{1}{2}$ $\qquad$ $\delta^t(!(I \oplus \Omega), !I) = 1$.

Context Distance: the General Case [CDL2016]

- None of the abstract notions of distance δ gives us that $\delta(I, I \oplus \Omega) = 1$.
- The underlying LMC **does not** reflect copying.
- **A Tuple LMC**.
  - **Preterms**:
    $M ::= x \mid \lambda x.M \mid \lambda !x.M \mid MM \mid M \oplus M \mid !M$
  - **Terms**: any preterm M such that $\Gamma \vdash M$.
  - **States**: *sequences* of terms, rather than terms.
  - **Actions** not only model parameter passing, but also *copying* of terms.
- **Soundness and Completeness Results:**

$\delta^t \leq \delta^c$	$\delta^c \leq \delta^t$
✓	✓

- **Examples**: $\delta^t(!(I \oplus \Omega), !\Omega) = \frac{1}{2}$ $\qquad \delta^t(!(I \oplus \Omega), !I) = 1$.
- **Trivialisation** does not hold in general, but becomes true in *strongly normalising* fragments or in presence of *parellel disjuction*.

Open Problems

- Would it be possible to read the distance between two terms M and N from their interpretations $[\![M]\!]$ and $[\![N]\!]$ (given in a suitable denotational model?).

Open Problems

- Would it be possible to read the distance between two terms M and N from their interpretations $[\![M]\!]$ and $[\![N]\!]$ (given in a suitable denotational model?).
- Applications to Cryptography?
  - **Computational indistinguishability** is a key notion of cryptography, and can be seen as a form of parametric equivalence.
  - We have a preliminary work on characterizing it as trace equivalence in a λ-calculus for polynomial time, called RSLR [CDL2015].

C

$\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{\mathcal{E}_n\}_{n\in\mathbb{N}}$ (where both $\mathcal{D}_n$ and $\mathcal{E}_n$ are distributions on binary strings) are said to be *computationally indistinguishable* iff for every PPT algorithm $\mathcal{A}$ the following quantity is a negligible function of $n \in \mathbb{N}$:

$$\left|\Pr_{x\leftarrow\mathcal{D}_n}(\mathcal{A}(x,1^n)=\epsilon)-\Pr_{x\leftarrow\mathcal{E}_n}(\mathcal{A}(x,1^n)=\epsilon)\right|.$$

ween two

$]\!]$ and $[\![N]\!]$

( )

- Applications to Cryptography?
  - **Computational indistinguishability** is a key notion of cryptography, and can be seen as a form of parametric equivalence.
  - We have a preliminary work on characterizing it as trace equivalence in a λ-calculus for polynomial time, called RSLR [CDL2015].

Open Problems

- Would it be possible to read the distance between two terms M and N from their interpretations $[\![M]\!]$ and $[\![N]\!]$ (given in a suitable denotational model?).
- Applications to Cryptography?
  - **Computational indistinguishability** is a key notion of cryptography, and can be seen as a form of parametric equivalence.
  - We have a preliminary work on characterizing it as trace equivalence in a λ-calculus for polynomial time, called RSLR [CDL2015].
- Higher-order computational indistinguishability?

Thank You!

Questions?