Behavioural, Functional, and Non-Functional Contracts for Dynamic Selection of Services

Carlos G. Lopez Pombo
@UNRN&CONICET

Hernán Melgratti
@UBA&CONICET

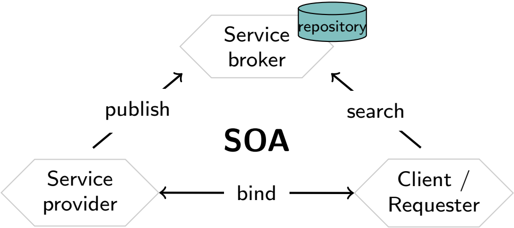
Agustín E. Martinez-Suñé
@ University of Oxford

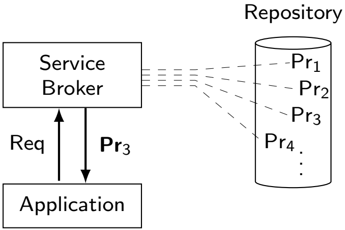
Diego Senarruzza Anabia
@UBA

Emilio Tuosto
@ GSSI

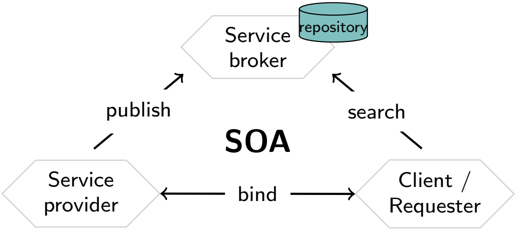
Work partly supported by the PRIN 2022 PNRR project DeLiCE (F53D23009130001)

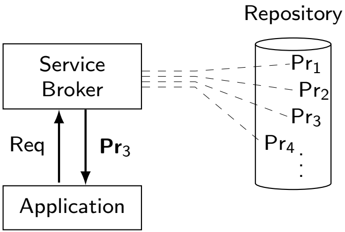
In the next few minutes...



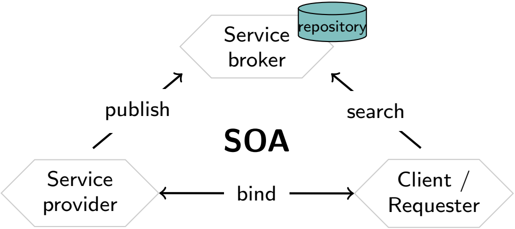


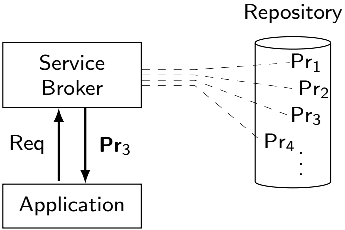
In the next few minutes...



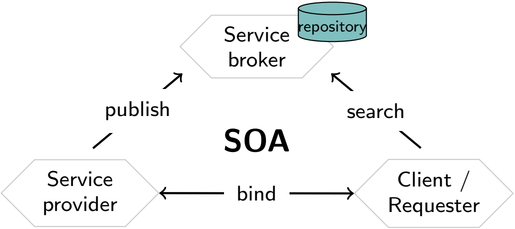


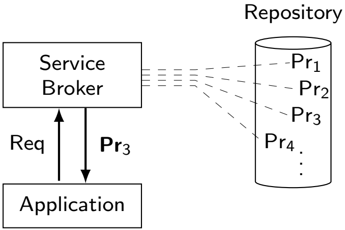
In the next few minutes...





In the next few minutes...



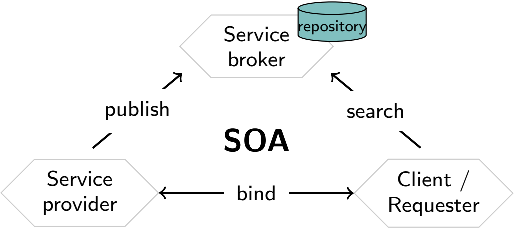


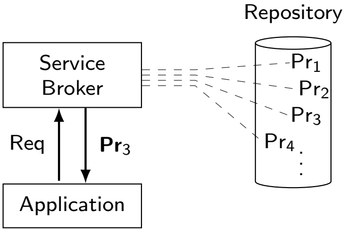
Prologue . . . . A bird-eye view

A proposal . . . . Some details & peculiarities

Conclusions . . . . Remarks & future work

In the next few minutes...





Prologue

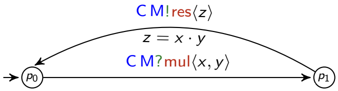
This talk in 1 slide

The problem

This talk in 1 slide

The problem

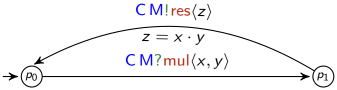
$z = x \cdot y$

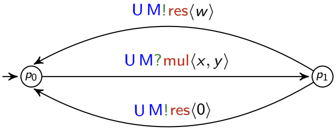


This talk in 1 slide

The problem

$z = x \cdot y$
$w = x \cdot y \neq 0$



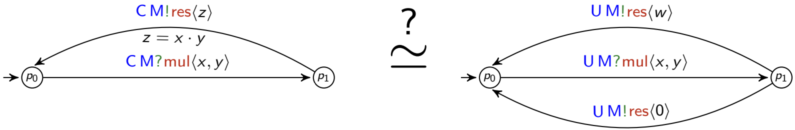


This talk in 1 slide

The problem

$z = x \cdot y$

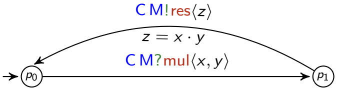
$w = x \cdot y \neq 0$



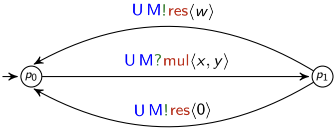
This talk in 1 slide

The problem

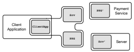
$z = x \cdot y$
$w = x \cdot y \neq 0$



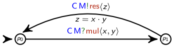
$\overset{?}{\simeq}$

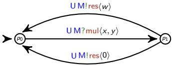


Our proposal: [1, 7] + [3] + [4, 6]



+





+ QoS-CFSMs

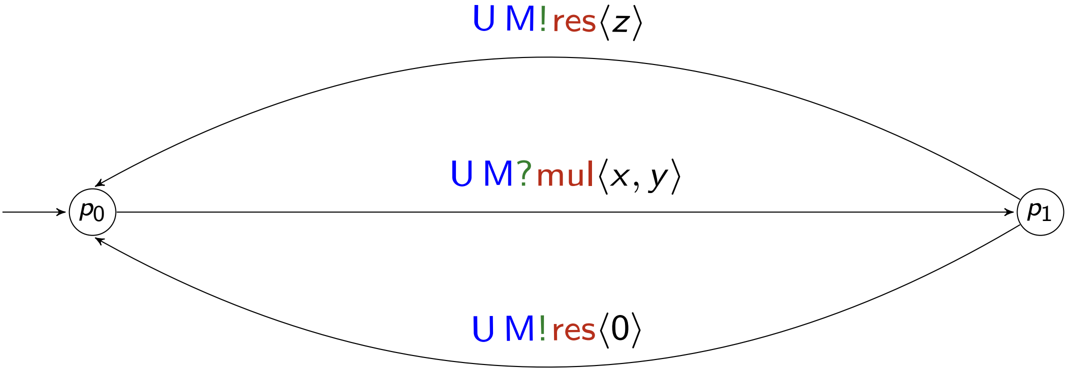
which yields

- ✓ A semantic-based discovery relying on behavioural and (non-)functional contracts
- ✓ Bisimulation-based compliance
- ✓ A bisimulation algorithm of service compliance modulo name matching

Preliminaries

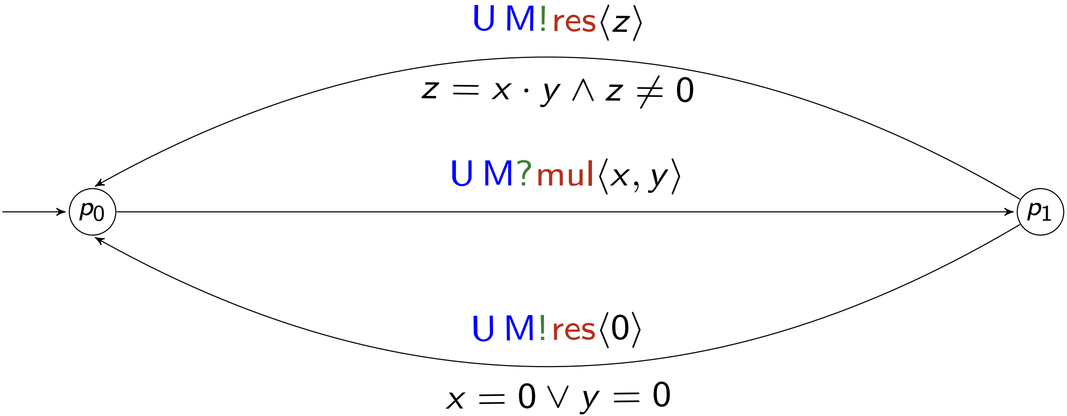
Our behavioural

We borrow (with some adaptation) ________ CFSM from [2]



Our behavioural and functional contracts

We borrow (with some adaptation) asserted CFSM from [3]



Our non-functional contracts

A variant of CFSMs yields our behavioural contracts; our non-functional contracts are

$$\underline{\text{QoS constraints}} = \text{FOL}_{=} + \text{Real Close Fields}$$

Our non-functional contracts

A variant of CFSMs yields our behavioural contracts; our non-functional contracts are

$$\text{QoS constraints} = \text{FOL}_{=} + \text{Real Close Fields}$$

where RCF are totally ordered fields such that

- positive elements have square roots
- polynomial of odd degrees have zeros

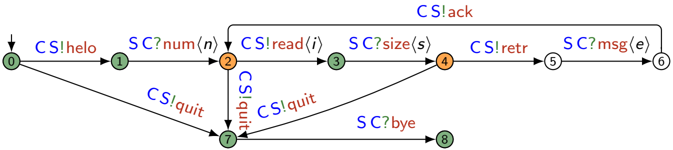
Our non-functional contracts

A variant of CFSMs yields our behavioural contracts; our non-functional contracts are

$$\underline{\text{QoS constraints}} = \text{FOL}_{=} + \text{Real Close Fields}$$

where RCF are totally ordered fields such that

- positive elements have square roots
- polynomial of odd degrees have zeros



$$\Gamma_{\text{Low}} = \{\mathsf{t} \leq 0.01,\ \mathsf{c} \leq 0.01,\ \mathsf{m} \leq 0.01\}$$

$$\Gamma_{\text{DB}} = \{\mathsf{t} \leq 3 \implies (\exists x)(0.5 \leq x \leq 1 \land \mathsf{c} = \mathsf{t} \cdot x),\ \mathsf{t} > 3 \implies \mathsf{c} = 10,\ \mathsf{m} \leq 5\}$$

...

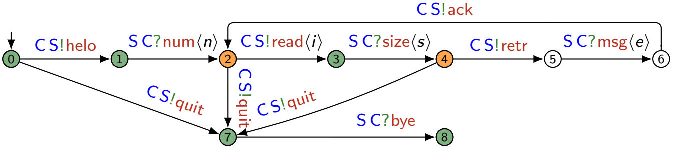
Our non-functional contracts

A variant of CFSMs yields our behavioural contracts; our non-functional contracts are

$$\text{QoS constraints} = \text{FOL}_{=} + \text{Real Close Fields}$$

where RCF are totally ordered fields such that

- positive elements have square roots
- polynomial of odd degrees have zeros



$$\Gamma_{\text{Low}} = \{\mathsf{t} \leq 0.01,\ \mathsf{c} \leq 0.01,\ \mathsf{m} \leq 0.01\}$$

$$\Gamma_{\text{DB}} = \{\mathsf{t} \leq 3 \implies (\exists x)(0.5 \leq x \leq 1 \wedge \mathsf{c} = \mathsf{t} \cdot x),\ \mathsf{t} > 3 \implies \mathsf{c} = 10,\ \mathsf{m} \leq 5\}$$

$\dots$

RCFs allow us to formalise QoS aggregation operators [4, 6]

[A proposal]

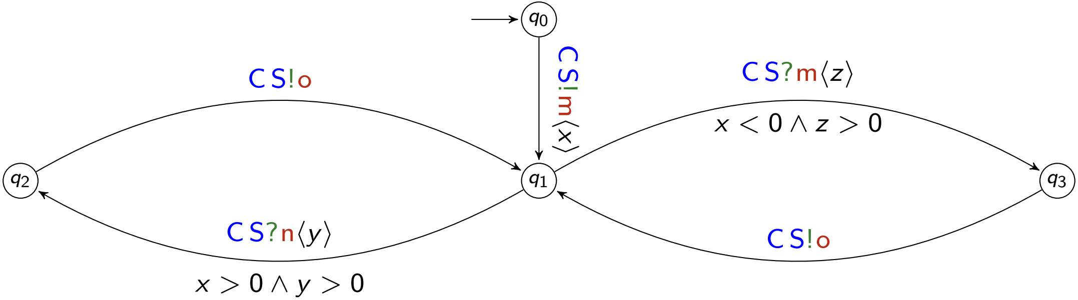
Extended CFSMs

An extended CFSM (e-CFSM for short) is a tuple $\langle M, F, \mathsf{qos}, \mathsf{asrt} \rangle$ where:

- $M = \langle Q, q_0, \rightarrow \rangle$ is a CFSM with $F \subseteq Q$ the set of final states ,
- asrt maps transitions of M to $\mathsf{FOL}_{=}$
- $\mathsf{qos} : Q \rightarrow \mathcal{C}$ maps states of M to set of QoS constraints

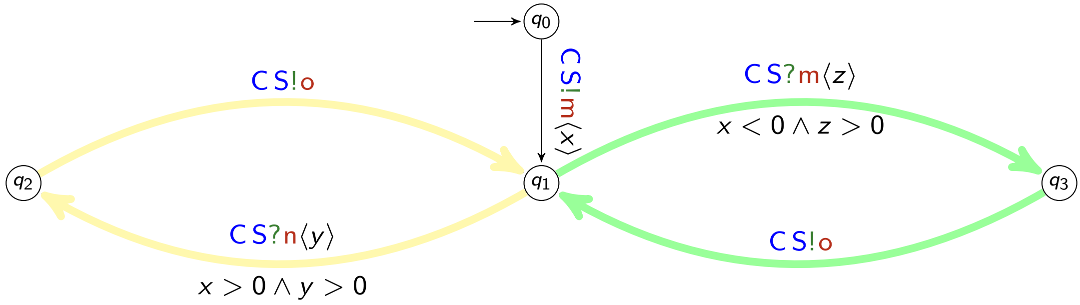
An extended communicating system is a map $(M_{\mathsf{A}})_{\mathsf{A} \in \mathcal{P}}$ assigning an A-local e-CFSM M_{A} to each $\mathsf{A} \in \mathcal{P}$.

Oddities

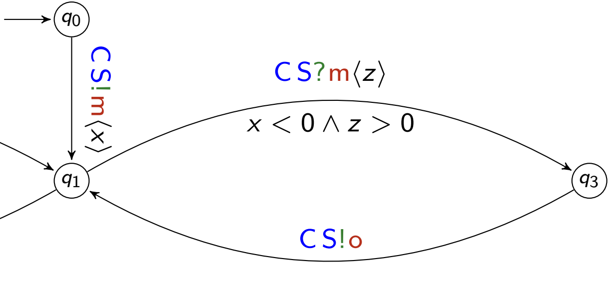


q_0
q_1
q_2
q_3
C S!o
C S!m$\langle x\rangle$
C S?m$\langle z\rangle$
$x < 0 \wedge z > 0$
C S?n$\langle y\rangle$
$x > 0 \wedge y > 0$
C S!o

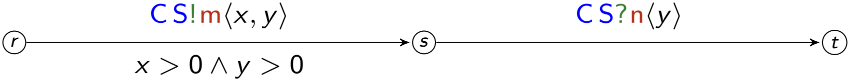
Oddities



Oddities



q_0
q_1
q_2
q_3
C S!m⟨x⟩
C S!o
C S?m⟨z⟩
$x < 0 \wedge z > 0$
C S?n⟨y⟩
$x > 0 \wedge y > 0$
C S!o



r
s
t
C S!m⟨x, y⟩
$x > 0 \wedge y > 0$
C S?n⟨y⟩

Knowledge

The residual $\phi \,\overline{\wedge}\, l$ of an assertion ϕ after l is $\perp$ unless

$$
\begin{aligned}
p(x_1, \ldots, x_n) \,\overline{\wedge}\, l &= p(x_1, \ldots, x_n) && \text{if } \mathit{var}(l) \cap \{x_1, \ldots, x_n\} = \emptyset \\
(\neg\phi) \,\overline{\wedge}\, l &= \neg(\phi \,\overline{\wedge}\, l) && \text{if } \phi \,\overline{\wedge}\, l \neq \perp \\
(\phi_1 \vee \phi_2) \,\overline{\wedge}\, l &= (\phi_1 \,\overline{\wedge}\, l) \vee (\phi_2 \,\overline{\wedge}\, l) && \text{if } \phi_1 \,\overline{\wedge}\, l \neq \perp \text{ and } \phi_2 \,\overline{\wedge}\, l \neq \perp \\
((\exists x)\phi) \,\overline{\wedge}\, l &= (\exists x)(\phi \,\overline{\wedge}\, l) && \text{if } x \notin \mathit{var}(l) \text{ and } \phi \,\overline{\wedge}\, l \neq \perp \\
((\exists x)\phi) \,\overline{\wedge}\, l &= ((\exists x)\phi) \,\overline{\wedge}\, l((\exists y)(\phi[y/x])) \,\overline{\wedge}\, l && \text{if } x \in \mathit{var}(l),\ y \text{ fresh, and } \phi \,\overline{\wedge}\, l \neq \perp
\end{aligned}
$$

Knowledge

The residual $\phi \,\overline{\wedge}\, l$ of an assertion ϕ after l is $\bot$ unless

$$
\begin{aligned}
p(x_1,\ldots,x_n) \,\overline{\wedge}\, l &= p(x_1,\ldots,x_n) && \text{if } var(l) \cap \{x_1,\ldots,x_n\} = \emptyset \\
(\neg\phi) \,\overline{\wedge}\, l &= \neg(\phi \,\overline{\wedge}\, l) && \text{if } \phi \,\overline{\wedge}\, l \neq \bot \\
(\phi_1 \vee \phi_2) \,\overline{\wedge}\, l &= (\phi_1 \,\overline{\wedge}\, l) \vee (\phi_2 \,\overline{\wedge}\, l) && \text{if } \phi_1 \,\overline{\wedge}\, l \neq \bot \text{ and } \phi_2 \,\overline{\wedge}\, l \neq \bot \\
((\exists x)\phi) \,\overline{\wedge}\, l &= (\exists x)(\phi \,\overline{\wedge}\, l) && \text{if } x \notin var(l) \text{ and } \phi \,\overline{\wedge}\, l \neq \bot \\
((\exists x)\phi) \,\overline{\wedge}\, l &= ((\exists x)\phi) \,\overline{\wedge}\, l((\exists y)(\phi[y/x])) \,\overline{\wedge}\, l && \text{if } x \in var(l),\ y \text{ fresh, and } \phi \,\overline{\wedge}\, l \neq \bot
\end{aligned}
$$

The knowledge $\mathcal{K}(\pi)$ on π is $K(\pi, \{True\})$ where

$$
K(\pi, X) = \begin{cases} \bigwedge_{\psi \in X} \psi, & \pi \text{ is the empty path} \\ K(\pi', \{\psi \mid \psi \in X \text{ and } \psi \,\overline{\wedge}\, l \neq \bot\} \cup \{\phi\}), & \pi = q \xrightarrow[\phi]{l} \pi' \end{cases}
$$

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.
A relation $\mathcal{R} \subseteq (Q_1 \times \mathrm{FOL}_=) \times (Q_2 \times \mathrm{FOL}_=)$ is a simulation if $\big(p, K\big)\mathcal{R}\big(q, K'\big)$ and $p \xrightarrow[\phi]{l} p'$ in M_1 imply that there is $T = \{q \xrightarrow[\psi_1]{l} q_1, \ldots, q \xrightarrow[\psi_k]{l} q_k\} \neq \emptyset$ in M_2 and

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.
A relation $\mathcal{R} \subseteq (Q_1 \times \mathrm{FOL}_=) \times (Q_2 \times \mathrm{FOL}_=)$ is a simulation if $\big(p, K\big)\mathcal{R}\big(q, K'\big)$ and $p \xrightarrow[\phi]{l} p'$ in M_1 imply that there is $T = \{q \xrightarrow[\psi_1]{l} q_1, \ldots, q \xrightarrow[\psi_k]{l} q_k\} \neq \emptyset$ in M_2 and

1. $\neg\big(((K \,\overline{\wedge}\, l) \wedge \phi) \implies \bigvee_{q \xrightarrow[\psi]{l} q' \in T}((K' \,\overline{\wedge}\, l) \wedge \psi)\big)$ unsat

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.

A relation $\mathcal{R} \subseteq (Q_1 \times \mathsf{FOL}_=) \times (Q_2 \times \mathsf{FOL}_=)$ is a simulation if $\big(p, K\big)\mathcal{R}\big(q, K'\big)$ and $p \xrightarrow[\phi]{l} p'$ in M_1 imply that there is $T = \{q \xrightarrow[\psi_1]{l} q_1, \ldots, q \xrightarrow[\psi_k]{l} q_k\} \neq \emptyset$ in M_2 and

1. $\neg\big(((K \,\overline{\wedge}\, l) \wedge \phi) \implies \bigvee_{q \xrightarrow[\psi]{l} q' \in T}((K' \,\overline{\wedge}\, l) \wedge \psi)\big)$ unsat
2. for all $q \xrightarrow[\psi]{l} q' \in T$, $\big(p', \overline{(K \,\overline{\wedge}\, l) \wedge \phi \wedge \psi}\big)\mathcal{R}\big(q', \overline{(K' \,\overline{\wedge}\, l) \wedge \psi}\big)$

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.

A relation $\mathcal{R} \subseteq (Q_1 \times \mathrm{FOL}_=) \times (Q_2 \times \mathrm{FOL}_=)$ is a simulation if $(p, K)\mathcal{R}(q, K')$ and $p \xrightarrow[\phi]{l} p'$ in M_1 imply that there is $T = \{q \xrightarrow[\psi_1]{l} q_1, \ldots, q \xrightarrow[\psi_k]{l} q_k\} \neq \emptyset$ in M_2 and

1. $\neg(((K \,\overline{\wedge}\, l) \wedge \phi) \implies \bigvee_{q \xrightarrow[\psi]{l} q' \in T}((K' \,\overline{\wedge}\, l) \wedge \psi))$ unsat
2. for all $q \xrightarrow[\psi]{l} q' \in T$, $(p', \overline{(K \,\overline{\wedge}\, l) \wedge \phi \wedge \psi})\mathcal{R}(q', \overline{(K' \,\overline{\wedge}\, l) \wedge \psi})$
3. if $p \in F_1$, then $q \in F_2$ and $\mathrm{qos}(p) = \langle \Sigma, \Gamma_1 \rangle$ and $\mathrm{qos}(q) = \langle \Sigma, \Gamma_2 \rangle$ then $\neg(\bigwedge_{\phi \in \Gamma_1} \phi \implies \bigwedge_{\phi \in \Gamma_2} \phi)$ unsat

Bisimulating e-CFSMs

Let M_1 and M_2 be two e-CFSMs respectively with states Q_1 and Q_2 and initial states $p_0 \in Q_1$ and $q_0 \in Q_2$.
A relation $\mathcal{R} \subseteq (Q_1 \times \mathsf{FOL}_=) \times (Q_2 \times \mathsf{FOL}_=)$ is a simulation if $\big(p, K\big)\mathcal{R}\big(q, K'\big)$ and $p \xrightarrow[\phi]{l} p'$ in M_1 imply that there is $T = \{q \xrightarrow[\psi_1]{l} q_1, \ldots, q \xrightarrow[\psi_k]{l} q_k\} \neq \emptyset$ in M_2 and

1. $\neg\big(((K \,\overline{\wedge}\, l) \wedge \phi) \implies \bigvee_{q \xrightarrow[\psi]{l} q' \in T}((K' \,\overline{\wedge}\, l) \wedge \psi)\big)$ unsat
2. for all $q \xrightarrow[\psi]{l} q' \in T$, $\big(p', \overline{(K \,\overline{\wedge}\, l) \wedge \phi \wedge \psi}\big)\mathcal{R}\big(q', \overline{(K' \,\overline{\wedge}\, l) \wedge \psi}\big)$
3. if $p \in F_1$, then $q \in F_2$ and $\mathsf{qos}(p) = \langle \Sigma, \Gamma_1 \rangle$ and $\mathsf{qos}(q) = \langle \Sigma, \Gamma_2 \rangle$ then $\neg\big(\bigwedge_{\phi \in \Gamma_1} \phi \implies \bigwedge_{\phi \in \Gamma_2} \phi\big)$ unsat

M_2 simulates M_1 if there is a simulation $\mathcal{R}$ such that $\big(p_0, \mathit{True}\big)\mathcal{R}\big(q_0, \mathit{True}\big)$.

Conclusions

In the paper

- an example on the POP protocol
- bisimulation checking algorithm module name matching

In the paper

- an example on the POP protocol
- bisimulation checking algorithm module name matching

Some doubts...

- is the approach feasible? (From one reviewer)
- isn't bisimulation to strong a notion for compliance?

In the paper

- an example on the POP protocol
- bisimulation checking algorithm module name matching

Some doubts...

- is the approach feasible? (From one reviewer)
- isn't bisimulation to strong a notion for compliance?

We are planning to

- to consider simulation akin to behavioural subtyping
- extend **SEArch** to support [5]
- generalise to name embeddings

Thank you

&

Thank reviewers

References I

[1] and. An interface theory for service-oriented design.
TCS, 503:1–30, 2013.

[2] D. Brand and P. Zafiropulo. On Communicating Finite-State Machines.
JACM, 30(2):323–342, 1983.

[3] L. Gheri, I. Lanese, N. Sayers, E. Tuosto, and N. Yoshida. Design-By-Contract for Flexible Multiparty Session Protocols.
In K. Ali and J. Vitek, editors, *36th European Conference on Object-Oriented Programming, ECOOP 2022, June 6-10, 2022, Berlin, Germany*, volume 222 of *LIPIcs*, pages 8:1–8:28. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[4] C. Pombo, A. Suñé, and E. Tuosto. A dynamic temporal logic for quality of service in choreographic models.
In E. Ábrahám, C. Dubslaff, and S. Tarifa, editors, *Theoretical Aspects of Computing – ICTAC 2023*, pages 119–138. Springer, 2023.

References II

[5] C. G. L. Pombo, P. Montepagano, and E. Tuosto. Search: An execution infrastructure for service-based software systems.
In I. Castellani and F. Tiezzi, editors, *Coordination Models and Languages - 26th IFIP WG 6.1 International Conference, COORDINATION 2024, Held as Part of the 19th International Federated Conference on Distributed Computing Techniques, DisCoTec 2024, Groningen, The Netherlands, June 17-21, 2024, Proceedings*, volume 14676 of *Lecture Notes in Computer Science*, pages 314–330. Springer, 2024.

[6] C. L. Pombo, A. E. M. Suñé, and E. Tuosto. A dynamic temporal logic for quality of service in choreographic models.
Theor. Comput. Sci., 1043:115247, 2025.

References III

[7] I. Vissani, C. G. L. Pombo, and E. Tuosto. Communicating machines as a dynamic binding mechanism of services.
In S. Gay and J. Alglave, editors, *Proceedings Eighth International Workshop on Programming Language Approaches to Concurrency- and Communication-cEntric Software, PLACES 2015, London, UK, 18th April 2015*, volume 203 of *EPTCS*, pages 85–98, 2015.