A Priori Conformance Verification for Guaranteeing Interoperability in Open Environments

Matteo Baldoni, Cristina Baroglio, Viviana Patti

Dipartimento di Informatica – Università degli Studi di Torino
c.so Svizzera, 185, Torino (Italy)
Web Services

- Web services are heterogeneous devices that can be *invoked* over the web
- Executable description of their business process (especially the interactive behavior)
- Tasks: composition, selection, ...
- *Dynamic dimension* due to the openness of the web
WS interoperability

- How to guarantee the interoperability of a dynamically composed set of WS?
- Interoperability is the capability of a peer of interacting with others
- This means they will actually produce a successful “conversation” (sequence of message invocation)
• Verification of the property of the interoperability among a set of processes: widely studied in the literature
• The web adds for Web Services a **dynamic feature**: the set of available processes evolves in time, they can be **reused**, they can be **assembled** dynamically and they are, in principle, **unknown** to each other
The summer school example

- In open environments services are identified and composed on demand:
  - retrieval done component by component
  - components behaviour could be private, not accessible for inspection
Choreographies and protocols: public specifications

- Need for a “distributed verification” of interoperability

- It should be possible to perform each verification without knowledge of the actual partners
Choreographies and protocols: public specifications

- Define and **make public** the set of interaction rules that the group should follow (protocol or choreography), eg. by means of a standardized language such as WS-CDL, and that **already guarantees** the interoperability
To perform the conformance test against the role specification

- “a-priori” interoperability test
- static interoperability checking

Verify-once run-always
The summer school example

• **Desire**: to check interoperability *without* any knowledge of the services that will play other roles

• **Solution**: a-priori verification of interoperability in terms of *conformance* relation w.r.t a protocol
Conformance test w.r.t. a protocol

- A service can enter the society only if its interactive behavior **conforms** to the communication protocol.

- The **conformance test** w.r.t. a protocol guarantees a-priori the interoperability and that the generated conversations will be "**legal**" w.r.t. the protocol.
The **conformance** is a relation between an implementation and a specification, between a policy and a specification (a signature) of a role.

The **interoperability** is a relation among a set of implementations, among a set of policies.
Choreographies and protocols: public specifications

- Each peer knows:
  - its policy
  - the role specification it would like to play
  - Maybe, the rest of the protocol

- Why?
  - dynamic selection of the partners
  - privacy of the used policies
A Priori Conformance Verification for Guaranteeing Interoperability in Open Environments

M. Baldoni, C. Baroglio, V. Patti

Conformance and interoperability

- The conformance test is similar to a static type checking, it is aimed to guarantee statically (a-priori) that the behavior at run-time respect the specification
- It does not guarantee by itself the interoperability

Conformance

Interoperability

Can I play that role?

Can we interoperate?
Conformance and interoperability

- Chopra and Singh's works [DALT 2006, DALT 2007 workshops]: interoperability in an agent settings
- Conformance and interoperability are orthogonal properties: They focus on interoperability of agents
Conformance and interoperability

- Chopra and Singh's works [DALT 2006, DALT 2007 workshops]
- Agents could be interoperable even if they fail conformance test w.r.t. specification
- For example: at the school all *might* speak another common language (French)
Conformance and interoperability

- For example: at the school all *might* speak another common language (French)

- ... however at the school all *might not* speak another common language...
Conformance and substitutability

- **Verify-once run-always**: by the conformance test one checks that a desired property of the specification (that should hold) still hold when I substitute to the specification a real implementation.

- **Substitutability**

  If “I conforms to R” and $P = R_1 | ... | R | ... | R_n$ is any protocol such that $R_1 | ... | R | ... | R_n$ satisfies $\varphi$

  then $R_1 | ... | I | ... | R_n$ satisfies $\varphi$
Conformance and stuck-freeness

- **Interoperability as stuck-freeness**
  a message sent by a sender will not get stuck without some receiver ever receiving it, and a receiver waiting for a message will not get stuck without some sender ever sending it

- **Substitutability for conformance relation**
  If “I conforms to $R$” and $P=R_1|...|R|...|R_n$ is any protocol such that $R_1|...|R|...|R_n$ is stuck-free then $R_1|...|I|...|R_n$ is stuck-free
But what does “to conform to” mean?

- The relation "I conforms to R" is intuitively meant to say that R has more behavioral options than I.

- Every behavioral option realized by implementation I is allowed by role specification R.
Reusing components: the coffee break example

- Existing components *might slightly differ* from the specification ...
- ... but *when interacting* they could anyway behave as desired
Conformance test
w.r.t. a role specification

- (b) and (c) do not compromise the interoperability

- A conformant policy never utters speech acts that are not expected, according to the protocol, and it should be able to handle any message that can possibly be received, according to the protocol.
Message invocation paradigm

- Similarity with method invocation over objects
  - An object must necessarily be able to handle messages sent by other objects in the context of its public interface
  - An object is not obliged to use all methods offered in the public interface
  - An object can have more methods than the interface requires
But what does “to conform to” mean?

- Every *behavioral option* realized by implementation $I$ is allowed by specification $R$.

- There are two kinds of interpretations for behavioral options:
  - global interpretations as sequences of observables (*execution trace*)
  - local interpretations as successor observables at individual states (*simulation*)
Execution trace

- [CLIMA VI, WS-FM 05] trace semantics, protocols and conversation policies represented as FSA
- Giordano, Martelli (AI*IA, 2007): trace semantics, commitment-based representation of the protocols by means of a DLTL logic
- Foster et al. 06, Alberti et al. 06
Conformance test is not an inclusion test

- [CLIMA VI, WS-FM 05] trace semantics, protocols and conversation policies represented as FSA
- Giordano, Martelli (AI*IA, 2007): trace semantics, commitment-based representation of the protocols by means of a DLTL logic
- Foster et al. 06, Alberti et al. 06

\[ L(p_{lang}^{ag}) \] vs. \[ L(p_{spec}) \]

Do they “match”?
Conformance test is not an inclusion test

- The policy allows a subset of the conversation w.r.t. the role description.
- However, if a partner, that implements (exactly) the role B, decides to send message m3, the system is going to stuck!
Conformance test is not a (bi)simulation test

- The role description and the policy allow the same conversations but the structure differs
- Only (b) and (c) compromise the interoperability
- (bi)simulation is too strong: all cases are not bisimilar
- Bisimulation in [Busi et al. 05, Zhao et al. 06]
Action and Re-Action

- An outgoing message is interpreted *an action* while an incoming message is interpreted as *a re-action*
- Sending a message implies a decision to perform an action while receiving a message does not
- Sending a message means *to request for an execution* of a task while receiving a message means *executing a task*

- *Asymmetric behaviour* w.r.t. the standard interpretation for sending and receiveing messages in process algebra and (bi)simulation techniques
Internal and External choice

• It is a fact of internal and external choice (Alur et al. 1998, de Alfaro and Henzinger, 2001)

• Receiving is, normally, interpretated as an external choice

• Sending is, instead, interpreted as an internal choice
Conformant simulation

- **Our proposal**: an asymmetric simulation for dealing with outgoing and incoming messages in a different way.
Our proposal: an asymmetric simulation for dealing with outgoing and incoming messages in a different way
Our proposal: an asymmetric simulation for dealing with outgoing and incoming messages in a different way.
Conformant simulation

- **Our proposal**: an *asymmetric simulation* for dealing with outgoing and incoming messages in a different way

![Diagram showing symmetric and asymmetric simulation](image-url)
Conformant simulation

- **Our proposal**: an asymmetric simulation for dealing with outgoing and incoming messages in a different way

- **Conformance simulation**

  Given two FSA's $A_1$ and $A_2$. $A_1$ is conformant simulation of $A_2$, $A_1 \preceq A_2$ iff there is a binary relation $R$ between $A_1$ and $A_2$ such that

  - $A_1.s_0 R A_2.s_0$

  - for every outgoing message $m!$ in $A_1.L$ and for every state $s_i$ in $A_1.S$, for every $s_j$ in $A_2.S$ s.t. $s_i R Sj$ and $(s_i, m!, s_{i+1})$ in $A_1.T$, then there is a state $s_{j+1}$ in $A_2.S$ s.t. $(s_j, m!, s_{j+1})$ in $A_2.T$ and $s_{i+1} R s_{j+1}$

  - for every incoming message $m?$ in $A_2.L$ and for every state $s_j$ in $A_2.S$, for every $s_i$ in $A_1.S$ s.t. $s_i R sj$ and $(s_j, m?, s_{j+1})$ in $A_2.T$, then there is a state $s_{i+1}$ in $A_1.S$ s.t. $(s_i, m!, s_{i+1})$ in $A_1.T$ and $s_{i+1} R s_{j+1}$
Conformant simulation

“$A_1 \leq A_2$” does not entail “$L(A_1) \subseteq L(A_2)$”

- However, with “$A_1 \leq A_2$” we capture the fact that $A_1$ will actually produce a subset of the conversations foreseen by the role, when interacting with entities that play the other roles in the protocol.

- **Proposition**

  Let $A_1 \otimes A_2$ be a protocol, and let $A'_1$, $A'_2$ be 2 policies s.t. $A'_i \leq A_i$, for $i=1,2$, then $A'_1 \otimes A'_2 \subseteq A_1 \otimes A_2$
Complete conformance simulation

- We assume that in a protocol it is always possible to conclude a conversation whatever the point at which the interaction arrived. We expect a similar property to hold also for a set of conformant policies.

- Conformant complete simulation

  Given two FSA’s $A_1$ and $A_2$ we say that $A_1$ is a complete conformant simulation of $A_2$, written $A_1 \leq^1 A_2$, iff $A_1$ is a conformant simulation of $A_2$ under a binary relation $R$ and for all $s_i \in A_1.F$ such that $s_i R s_j$, then $s_j \in A_2.F$; for all $s_j \in A_2.S$ such that $s_j$ is alive and $s_i R s_j$, $s_i \in A_1.S$, then $s_i$ is alive.
Substitutability w.r.t. stuck-freeness

- Let $A_1 \otimes A_2$ be a protocol and let $A_1', A_2'$ be 2 policies such that $A_i'$ complete conforms simulation to $A_i$, for $i = 1, 2$. For any common string $\sigma'$ of $A_1 \otimes A_2$ and $A_1 \otimes A_2$ there is a run $\sigma'\sigma''$ of the protocol such that $\sigma'\sigma''$ is an accepted string of $A_1 \otimes A_2$.

- They will be able to conclude their interaction producing a legal accepted run (interoperability)
Conclusions and future work

- We face the problem of verifying the interoperability of a set of peers by exploiting an abstract description of the desired interaction: \textit{static interoperability checking}

- Can an agent/peer, having its own strategies, profitably take part to a “game”? In other words, does an agent/peer have the capabilities that allow it \textit{to reach its own goal by playing a given role}? [IJBPIIM07, WESOA07, WEWST07]

- A calculus for the “a-priori” interoperability test
- Autonomy and flexibility of an implementation
References

References


References


References


References