Collaborative Service-Based Processes, a Formal Methods Perspective

KAIS KLAI

LIPN,
UNIVERSITY PARIS 13, SORBONNE PARIS CITÉ

IWAISE'14, November 11, 2014

Collaborative Service-Based Processes, a Formal Methods Perspective

KAIS KLAI

LIPN,
UNIVERSITY PARIS 13, SORBONNE PARIS CITÉ

Joint work with Jörg Desel, Samir Tata and Hanen Ochi

IWAISE'14, November 11, 2014

Outline

Outline

Abstraction and Verification of Collaborative Service-Based Processes

- **Service-Based Process (SbP)**: A series of logically related activities or tasks (services) performed together in order to accomplish a specific organizational goal.

Abstraction and Verification of Collaborative Service-Based Processes

- **Service-Based Process (SbP)**: A series of logically related activities or tasks (services) performed together in order to accomplish a specific organizational goal.
- **Collaborative Service-Based Process (CSbP)**: Collaboration of several local SbP designed seperately

CSbP: Caracteristics and requirements

- Relatively simple models
- Loosely coupled (in general)
- Each local process is designed and analysed locally

CSbP: Caracteristics and requirements

- Relatively simple models
- Loosely coupled (in general)
- Each local process is designed and analysed locally

- Need to collaborate with partners
- Ensure correct behaviour of the whole process
- Want to hide the trade secrets and the organisational structure of their local processes

CSbP: Caracteristics and requirements

- Relatively simple models
- Loosely coupled (in general)
- Each local process is designed and analysed locally

- Need to collaborate with partners
- Ensure correct behaviour of the whole process
- Want to hide the trade secrets and the organisational structure of their local processes

What is the right abstraction?

CSbP: Caracteristics and requirements

- Relatively simple models
- Loosely coupled (in general)
- Each local process is designed and analysed locally

- Need to collaborate with partners
- Ensure correct behaviour of the whole process
- Want to hide the trade secrets and the organisational structure of their local processes

What is the right abstraction?

- Sufficiently detailed for potential partners
- Hides the local organisation/structure (privacy)
- Suitable for checking the correction of the CSbP

Outline

Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

Goal: Check event-based $LTL \setminus X$ properties

Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

Goal: Check event-based $LTL \setminus X$ properties

Principle: Compute a reduced abstraction of the state space

- Event based $LTL \setminus X$ formula
- Observed events: events occurring in the formula (Obs)
  - $\mathsf{G}(a \implies \mathsf{F}\ b) \longrightarrow \text{Obs}=\{a, b\}$

Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

Goal: Check event-based $LTL \setminus X$ properties

Principle: Compute a reduced abstraction of the state space

- Event based $LTL \setminus X$ formula
- Observed events: events occurring in the formula (Obs)
  - $G(a \implies F\ b) \longrightarrow Obs=\{a, b\}$

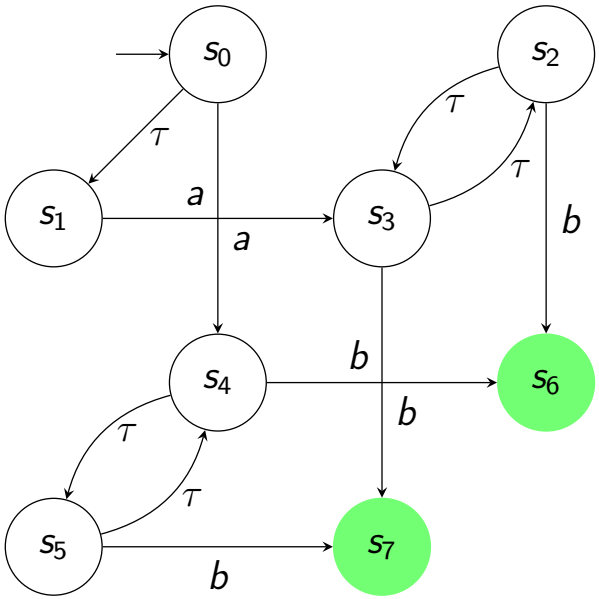
SOG

- Hybrid Graph
  - Nodes (aggregates): sets of explicit states
    - Symbolic encoding (BDDs)
    - Symbolic algorithms (deadlock, livelock)
  - Edges: labelled by observed events

Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

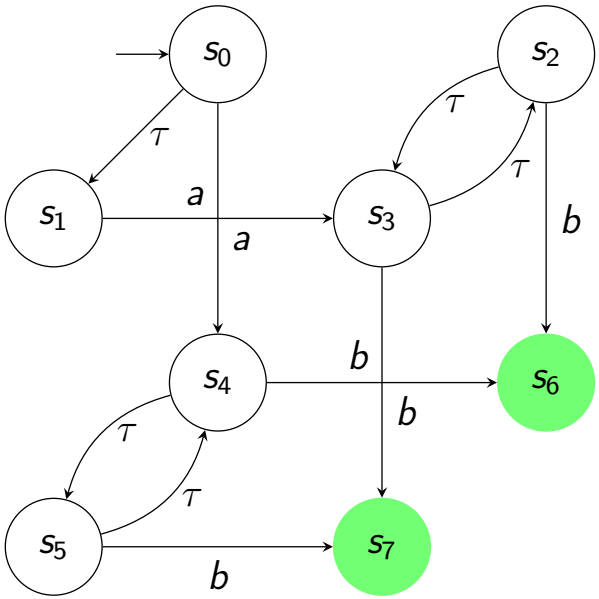
a LTS



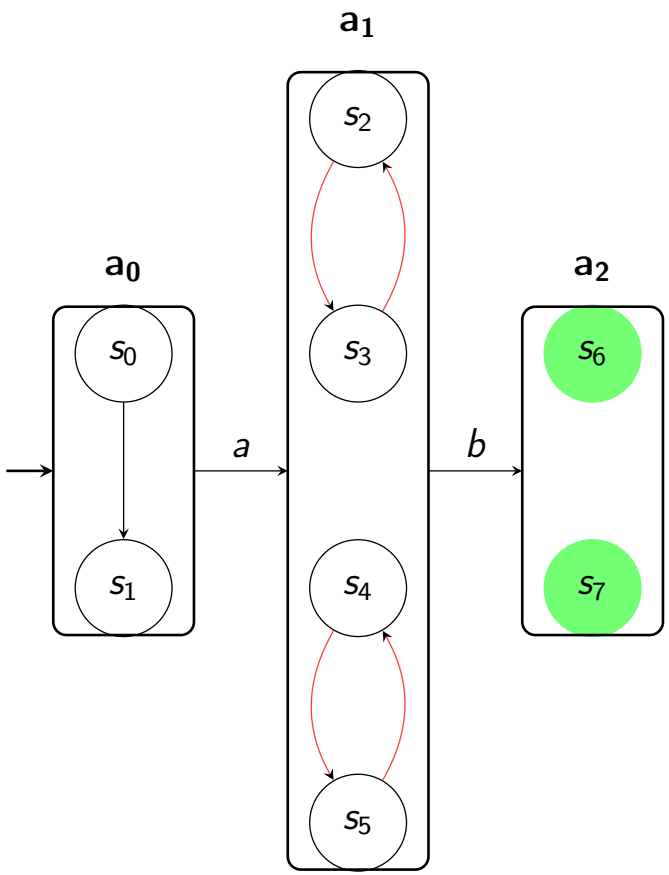
Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

a LTS



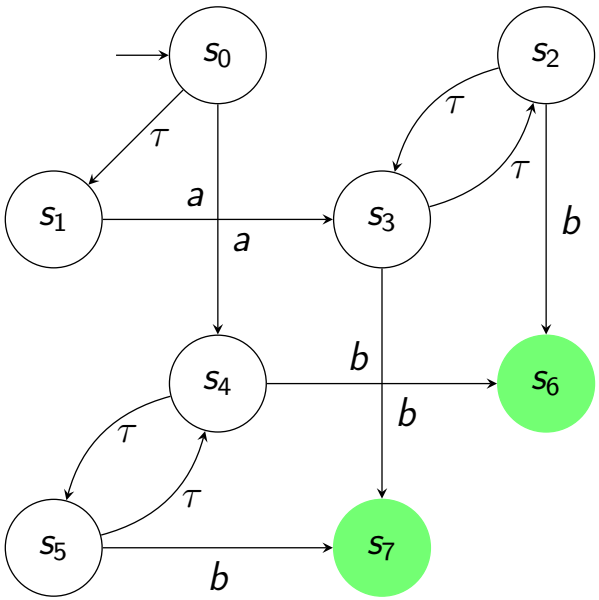
a corresponding SOG



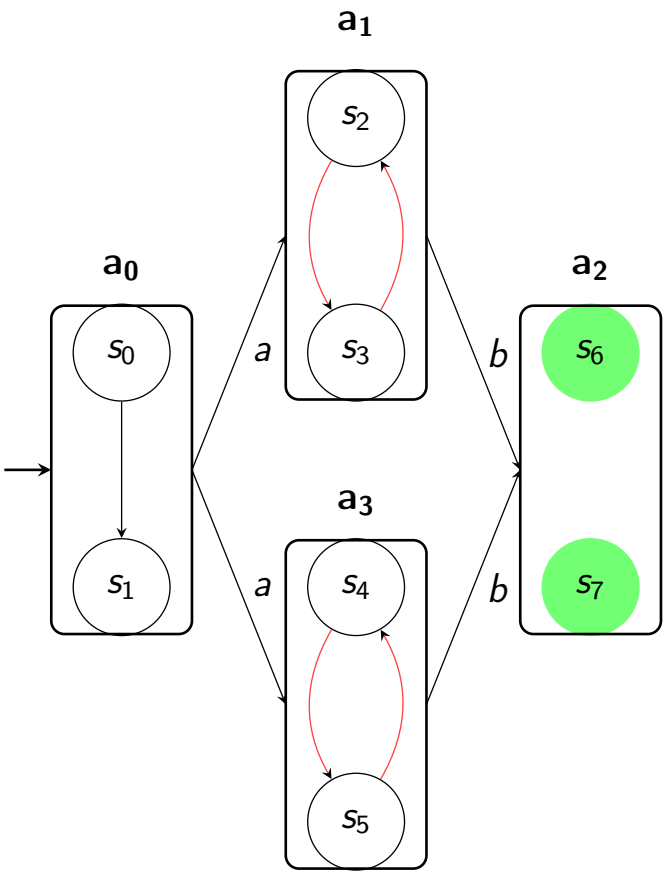
Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

a LTS



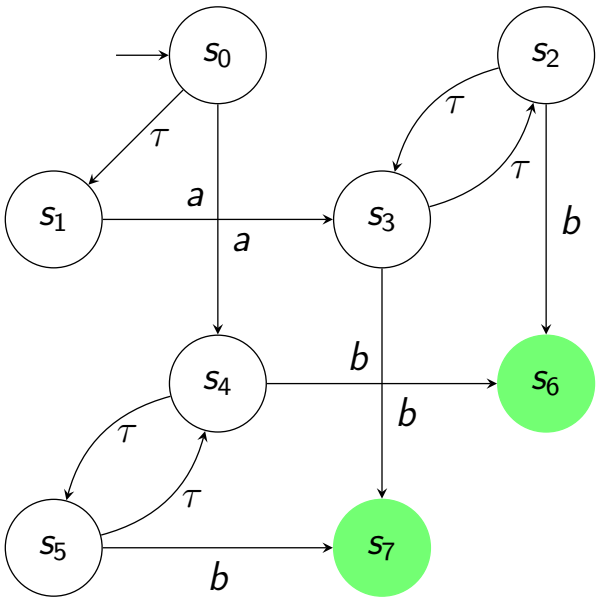
a corresponding SOG



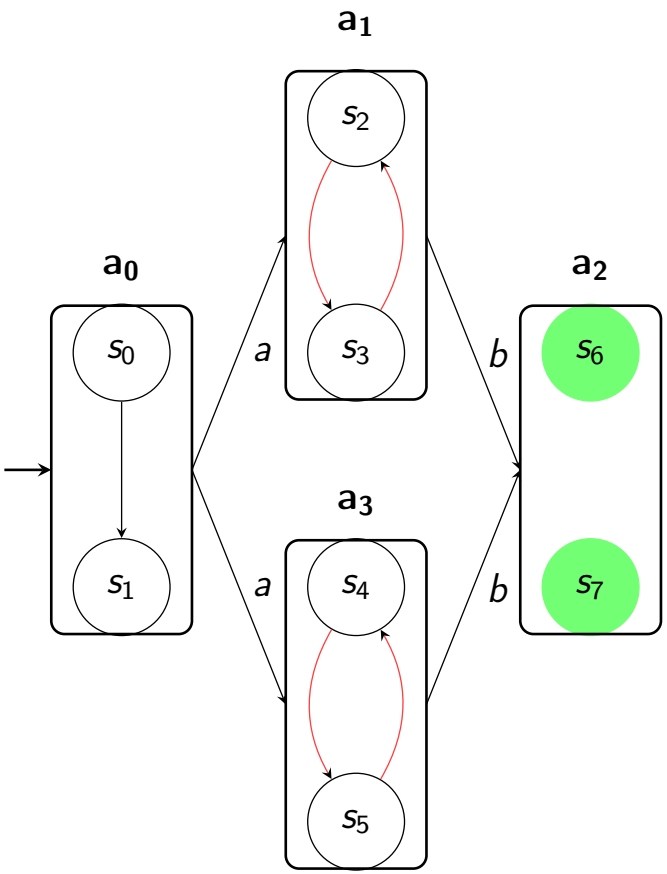
Event-Based SOG

Phd Thesis Kais Klai 2003, S. Haddad, J-M. Ilié and K. Klai ATVA'04

a LTS



a corresponding SOG



Observe collaborative actions and hide local ones

Outline

Approach

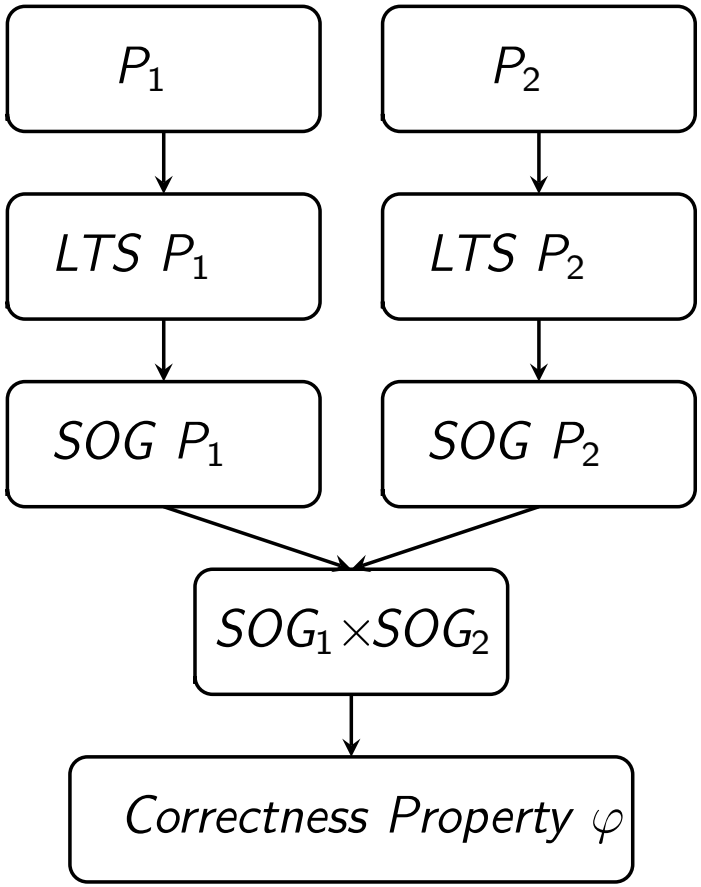
Bottom-Up approach [K. Klai, S. Tata and J. Desel BPM'09-DKE'11]

The composite model is unavailable

Approach

Bottom-Up approach [K. Klai, S. Tata and J. Desel BPM'09-DKE'11]

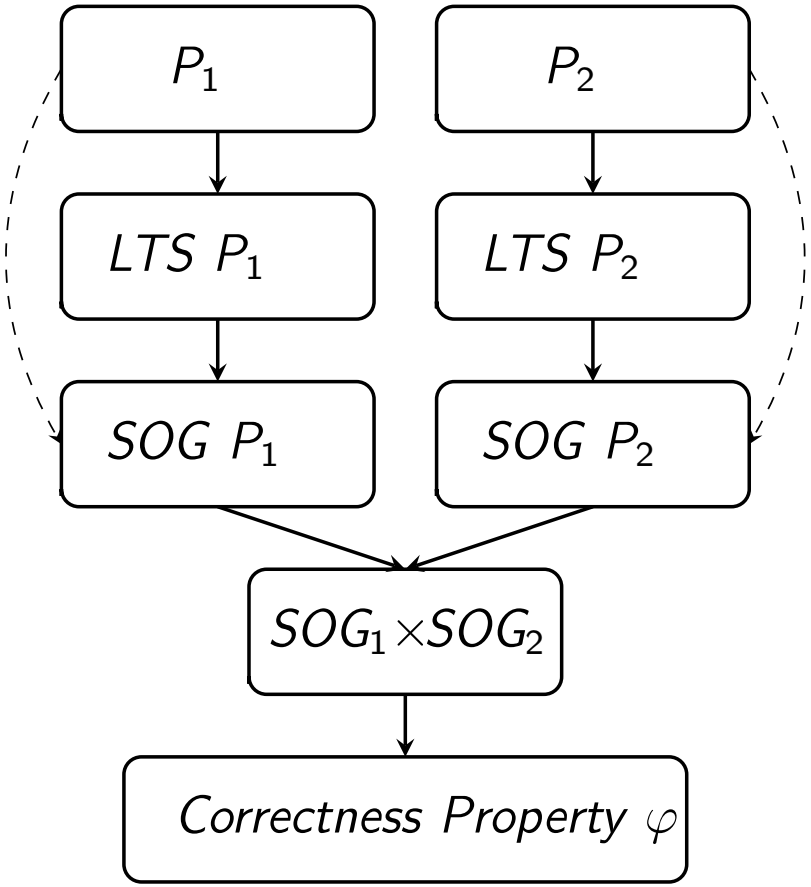
The composite model is unavailable



Approach

Bottom-Up approach [K. Klai, S. Tata and J. Desel BPM'09-DKE'11]

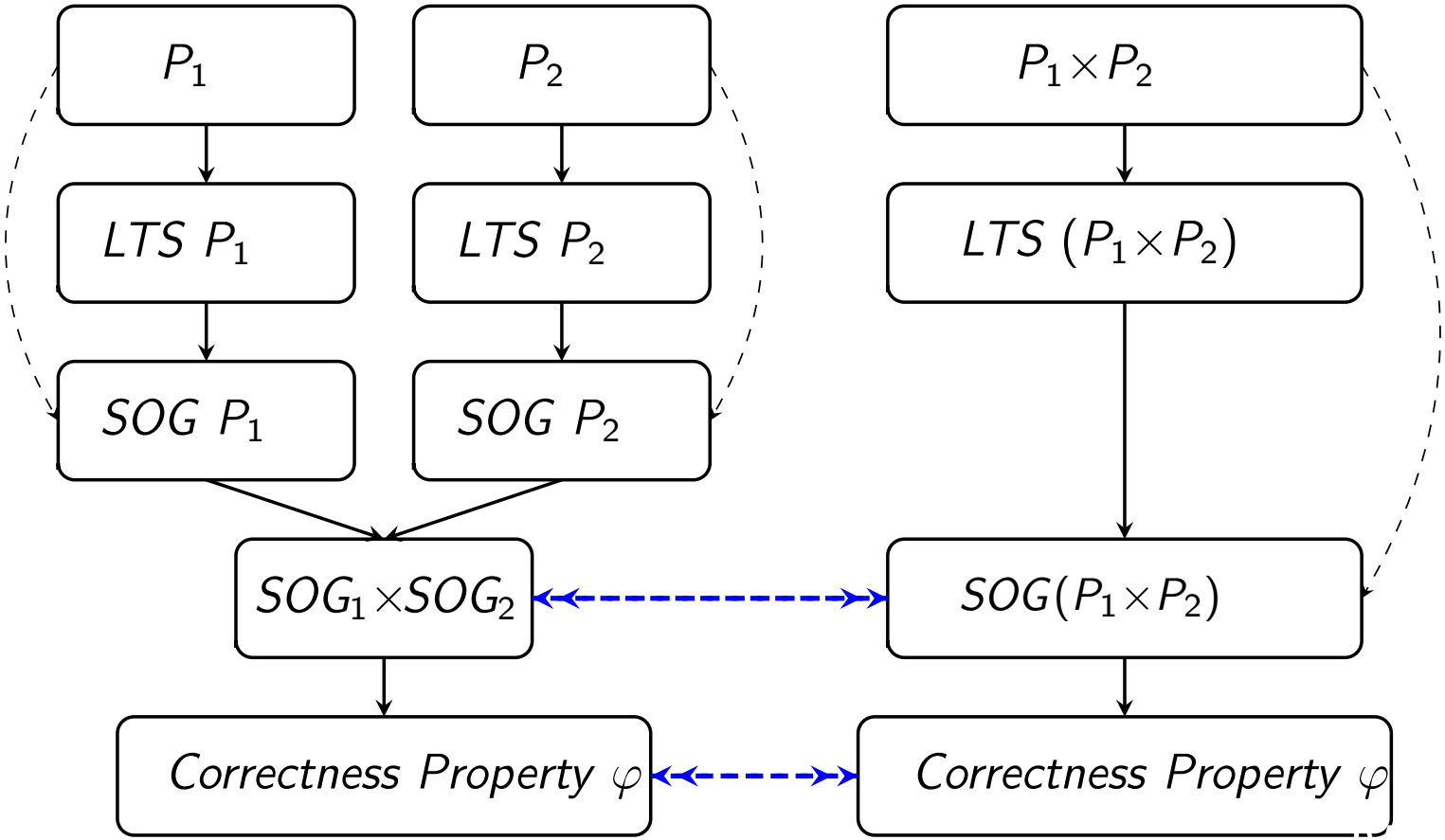
The composite model is unavailable



Approach

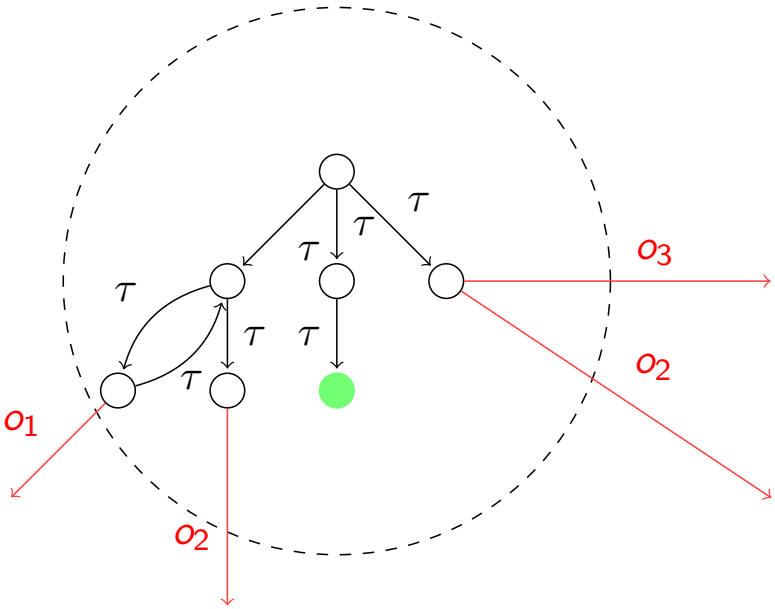
Bottom-Up approach [K. Klai, S. Tata and J. Desel BPM'09-DKE'11]

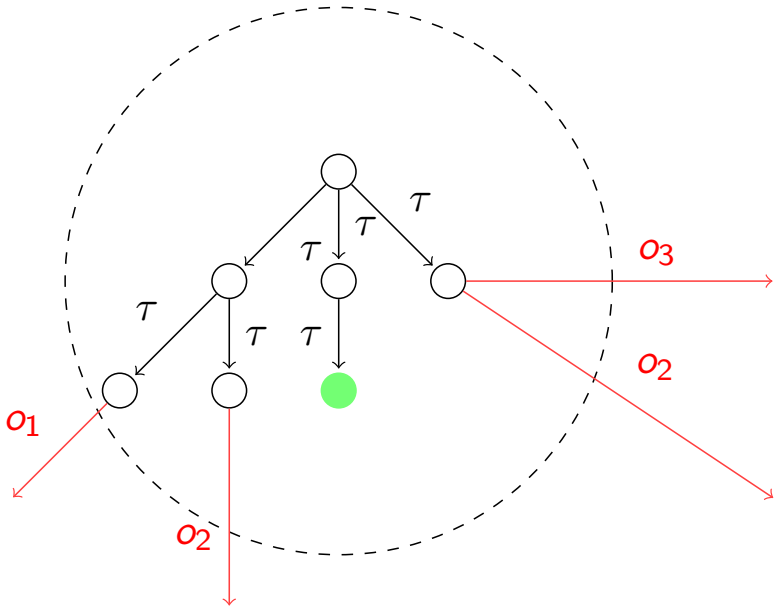
The composite model is unavailable



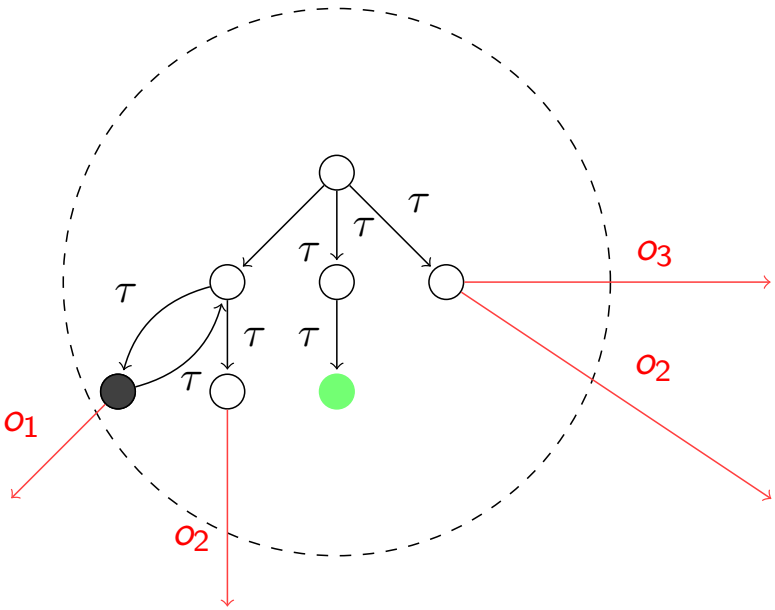
Outline

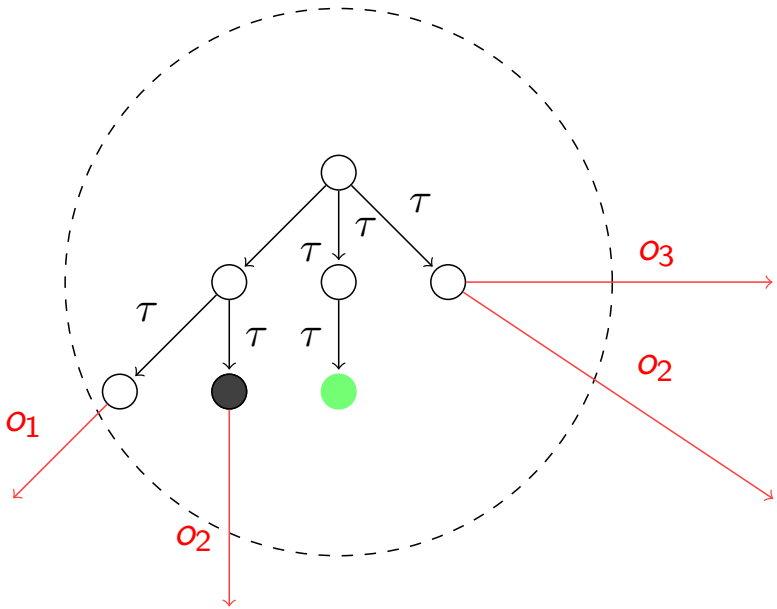
Composition of SOGs: Deadlock freeness property





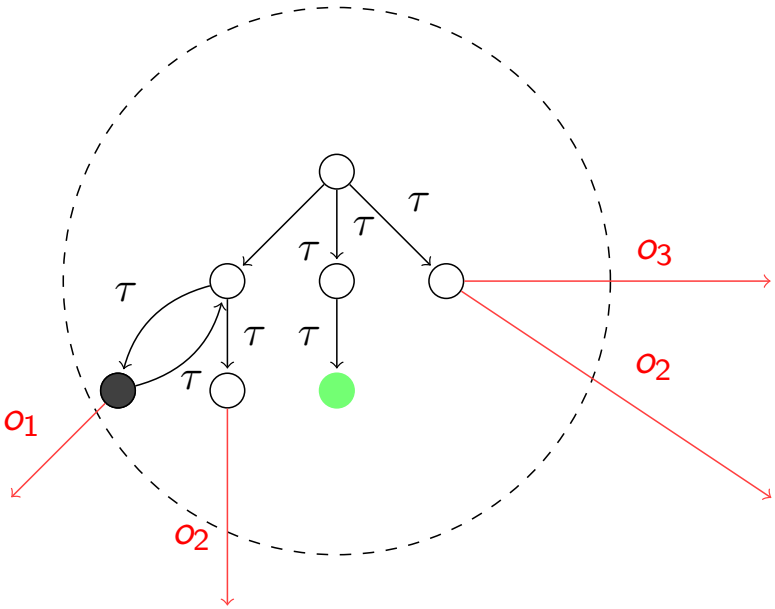
Composition of SOGs: Deadlock freeness property



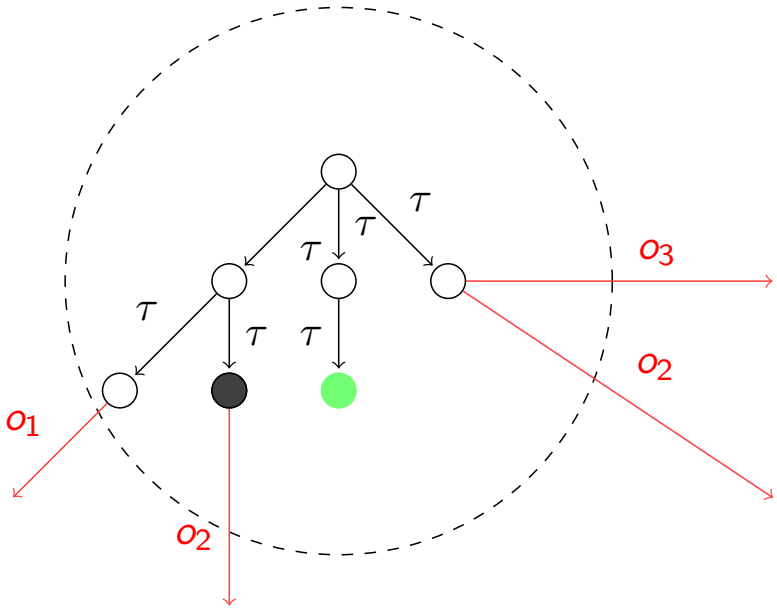


- Interlock: Deadlock caused by the interaction

Composition of SOGs: Deadlock freeness property



$\lambda(a_1) : \{\{o_1\}, \{o_2\}, \{term\}\}$

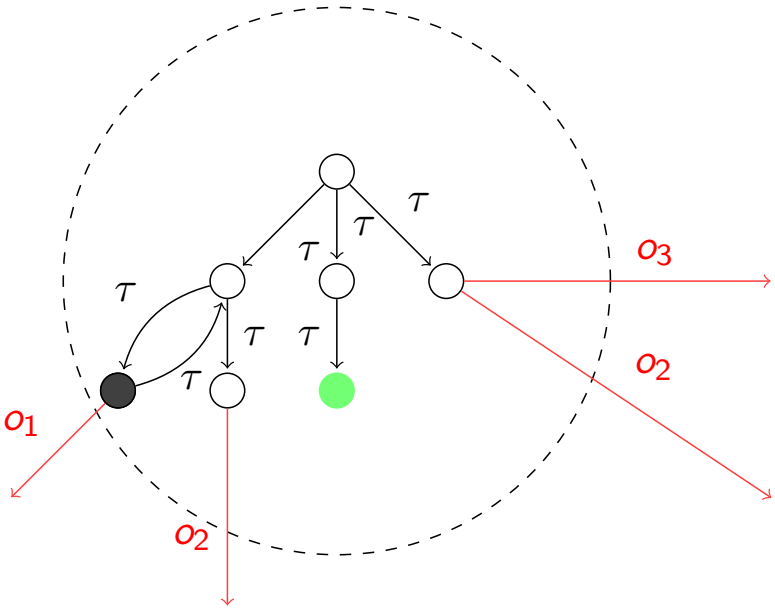


$\lambda(a_2) : \{\{o_1\}, \{o_2\}, \{term\}\}$

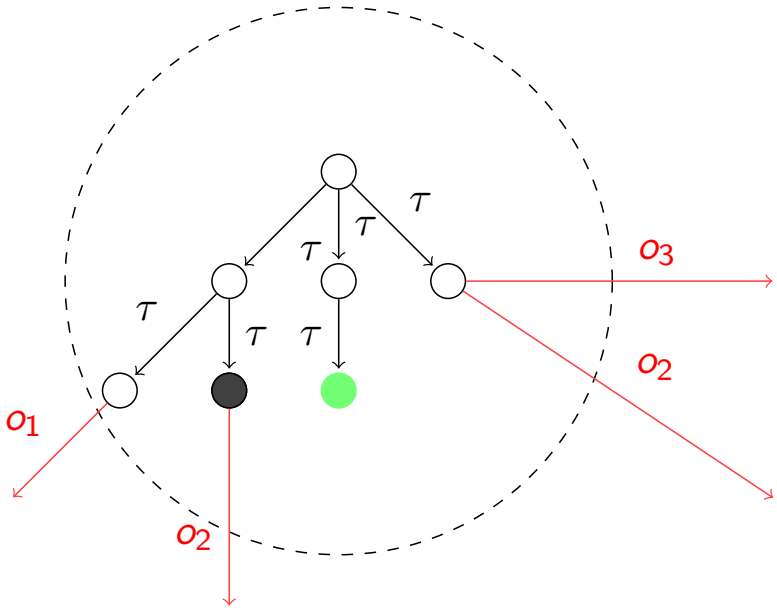
- Interlock: Deadlock caused by the interaction

Composition of SOGs: Deadlock freeness property

- $a = \langle a_1, a_2 \rangle$: $\lambda(a)$ obtained from $\lambda(a_1)$ and $\lambda(a_2)$



$\lambda(a_1) : \{\{o_1\}, \{o_2\}, \{term\}\}$

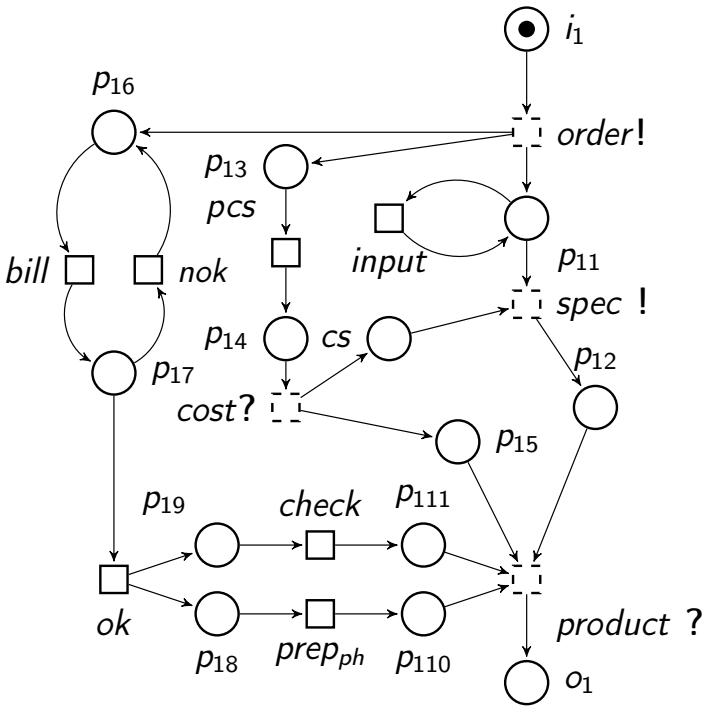


$\lambda(a_2) : \{\{o_1\}, \{o_2\}, \{term\}\}$

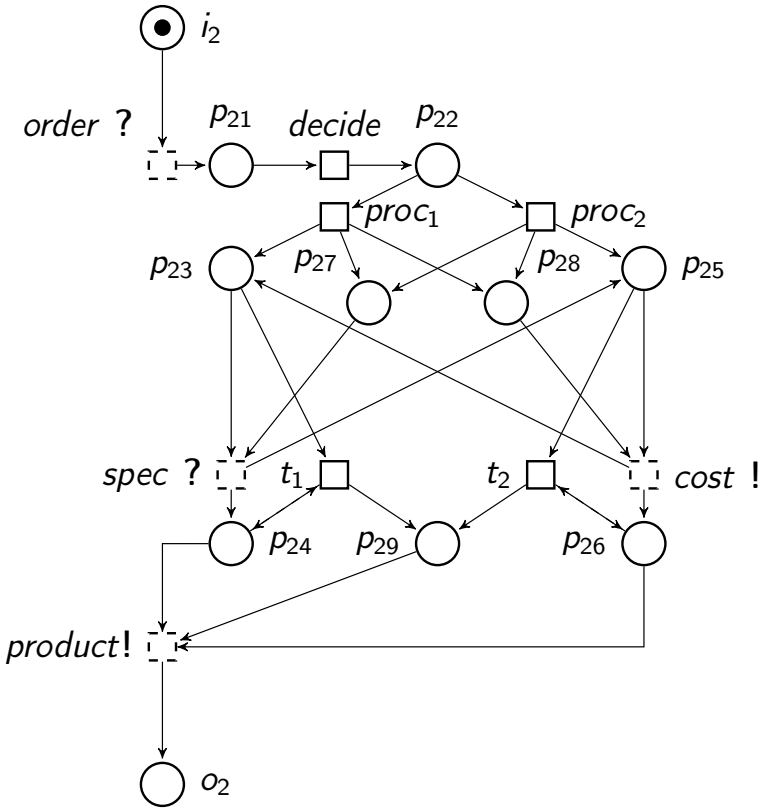
- Interlock: Deadlock caused by the interaction

From BP models to Petri nets

WF-nets [Van Der Aalst 98]

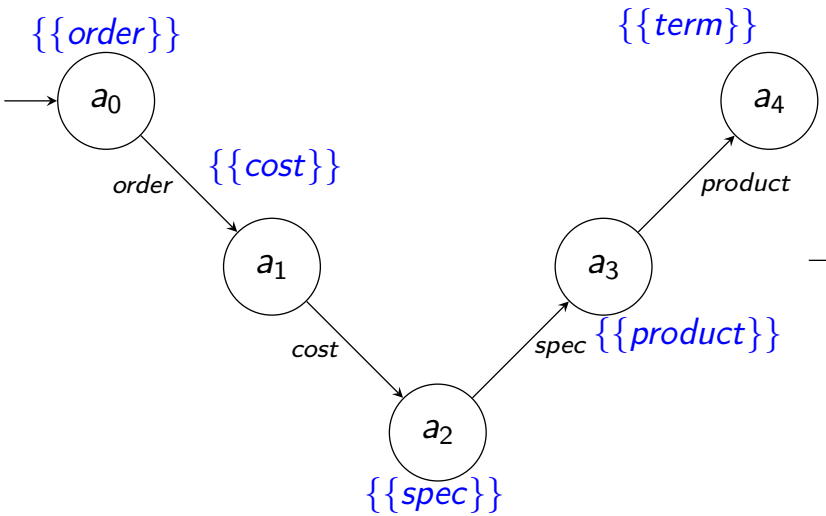


WF-net contractor

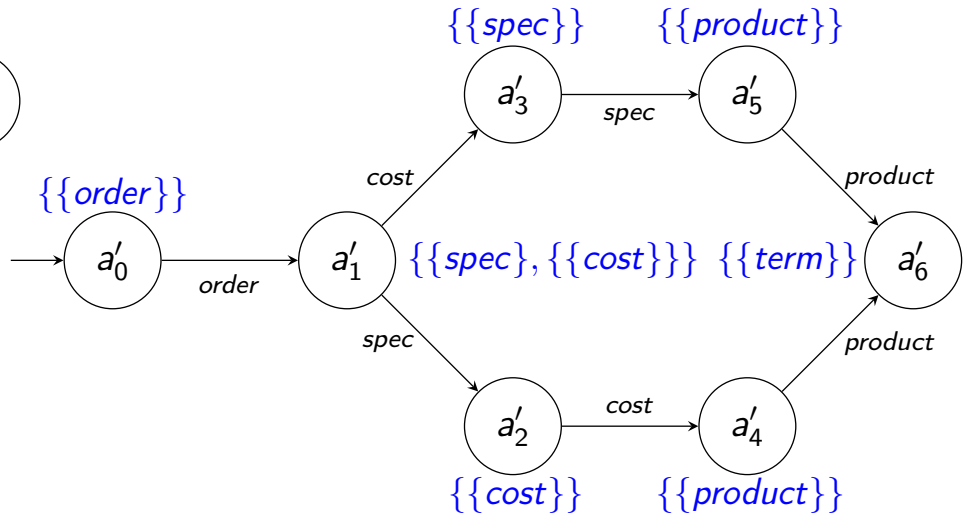


WF-net sub-contractor

Event-Based SOGs: Example



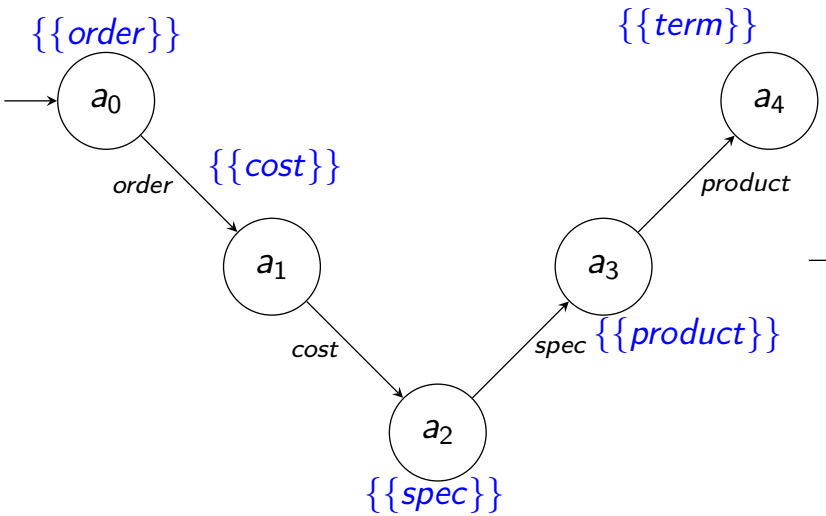
SOG contractor



SOG sub-contractor

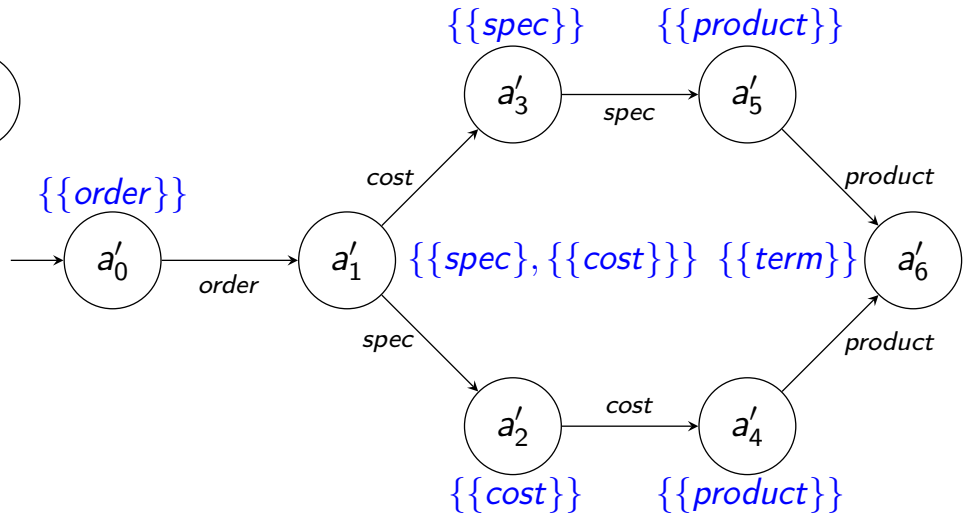
Event-Based SOGs: Example

explicit size: 38/104



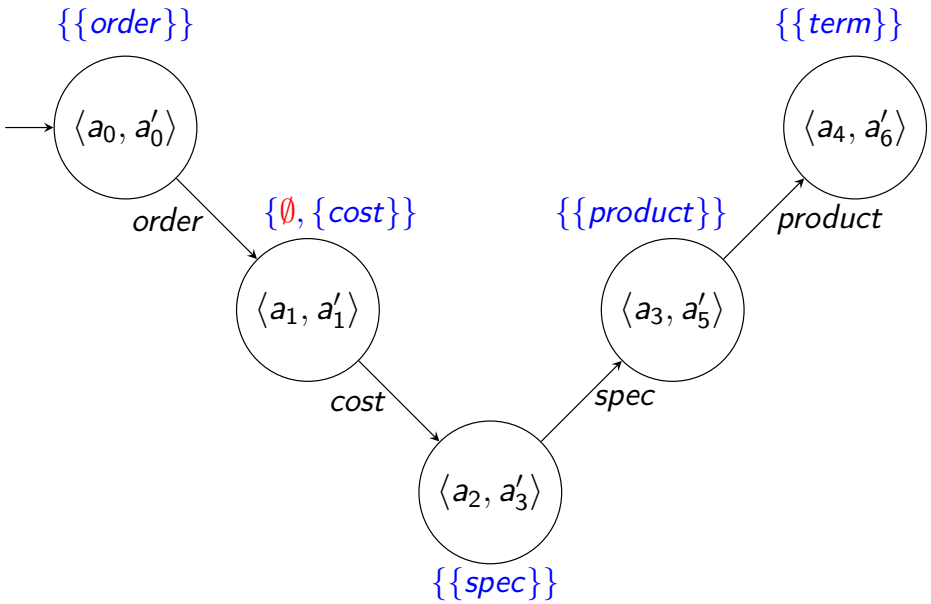
SOG contractor

explicit size: 14/22



SOG sub-contractor

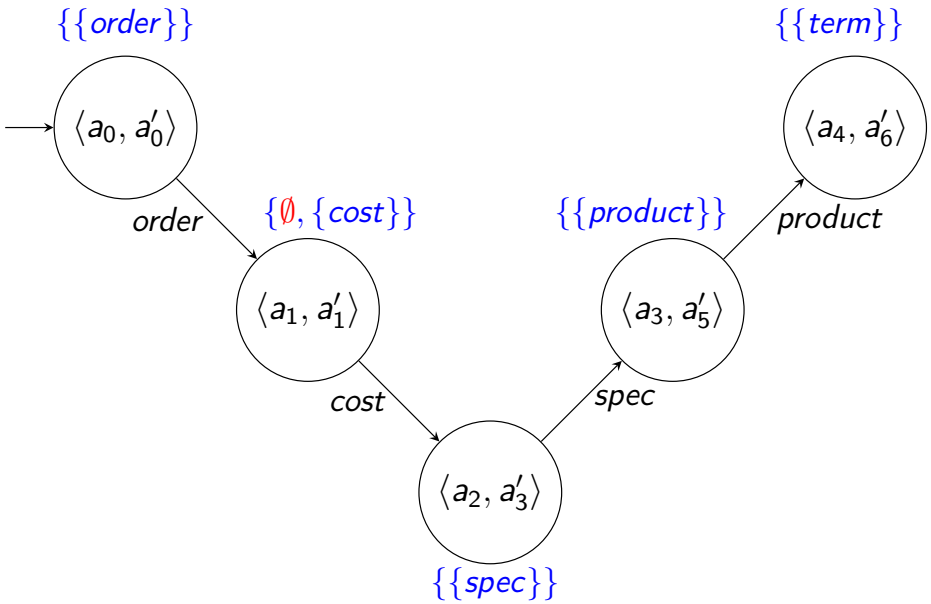
Synchronous Composition



Synchronous SOGs product

Synchronous Composition

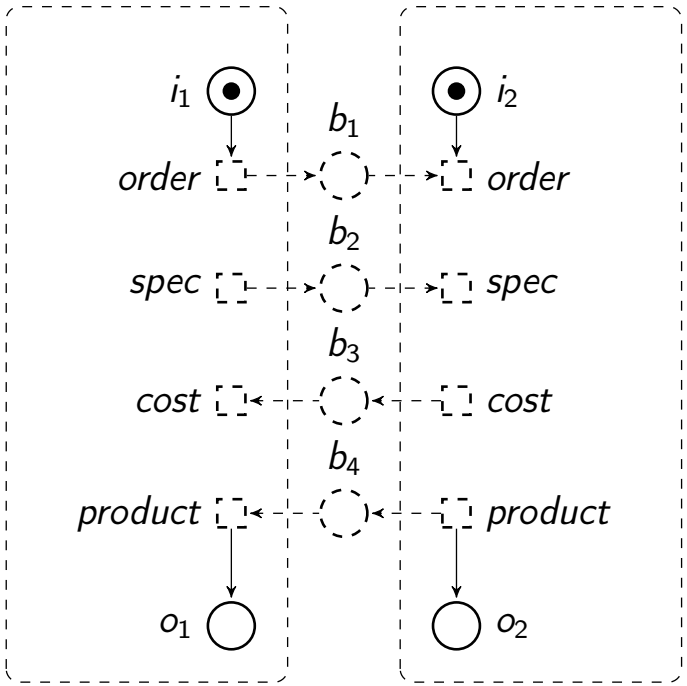
explicit size: 99/320



Synchronous SOGs product

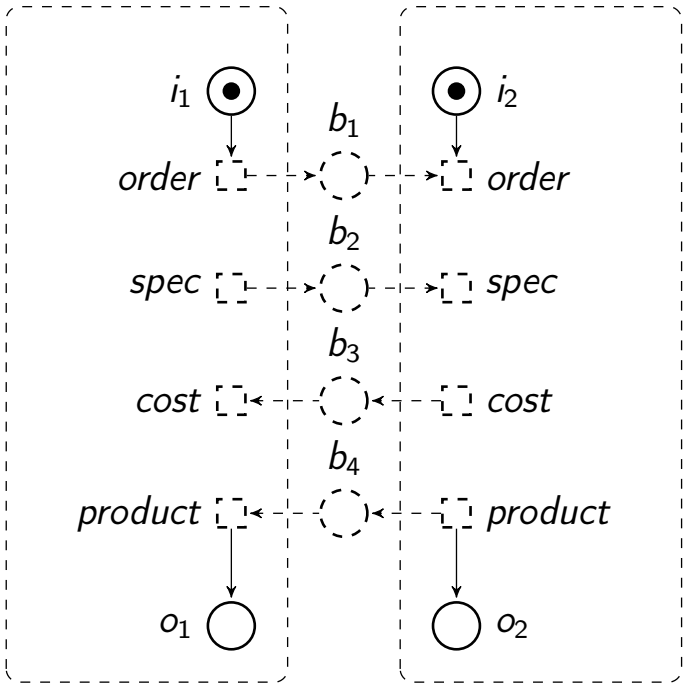
Asynchronous Composition

Interface medium

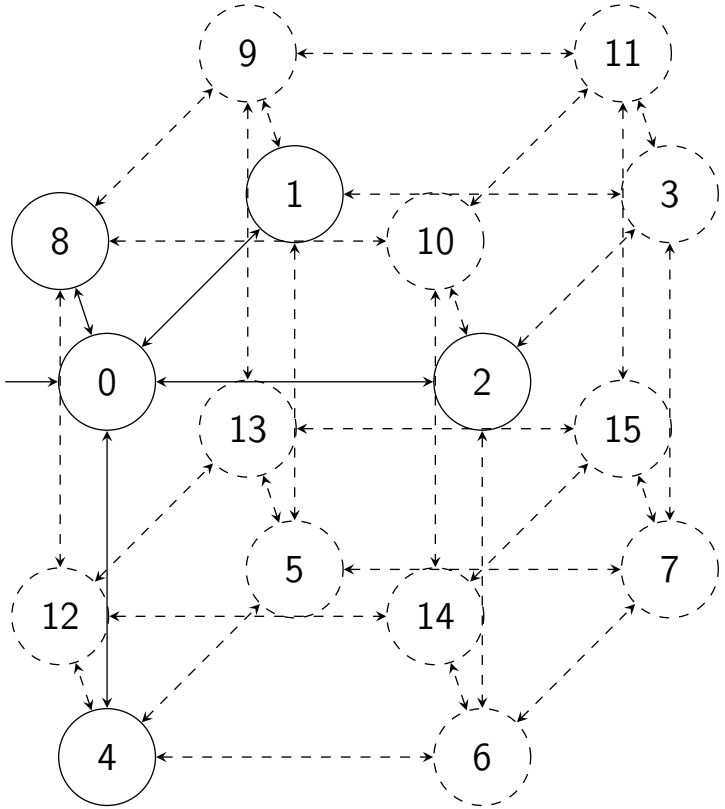


Asynchronous Composition

Interface medium

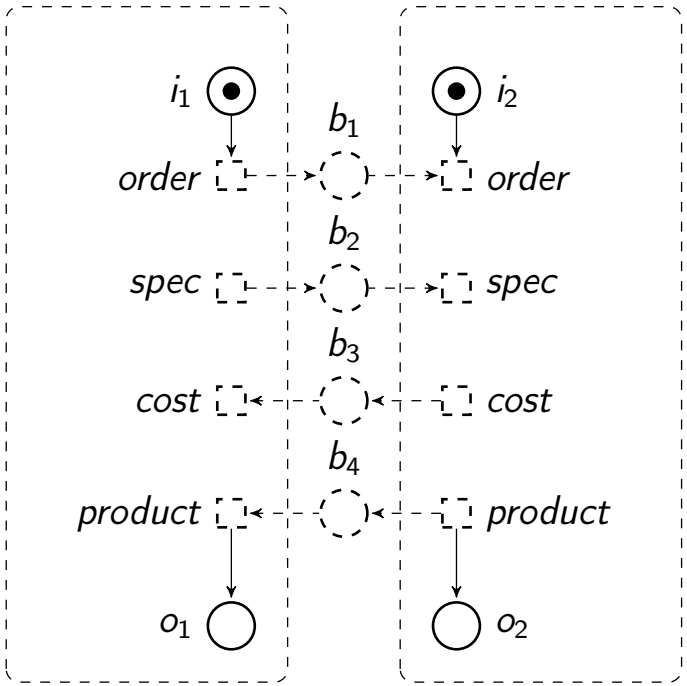


Interface Graph

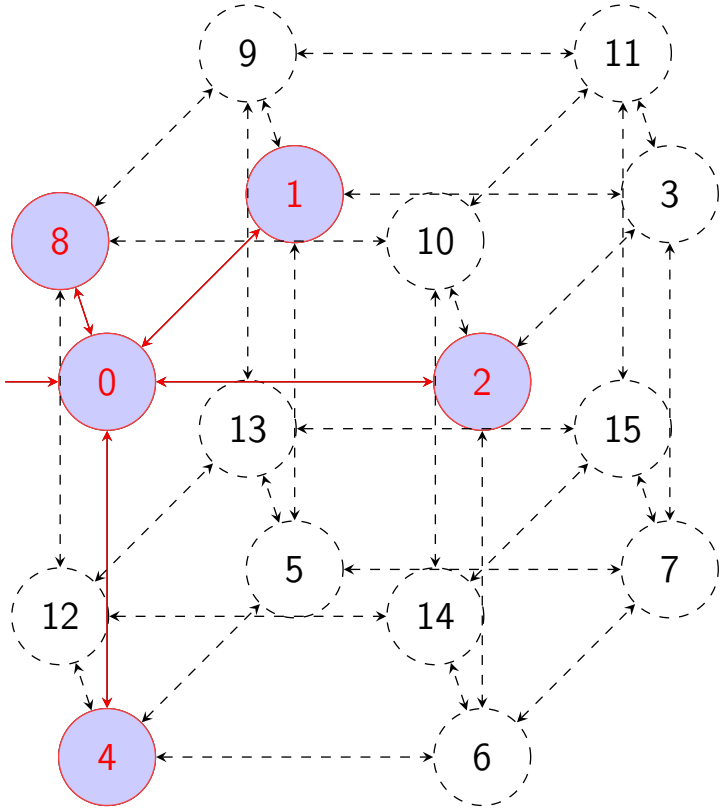


Asynchronous Composition

Interface medium

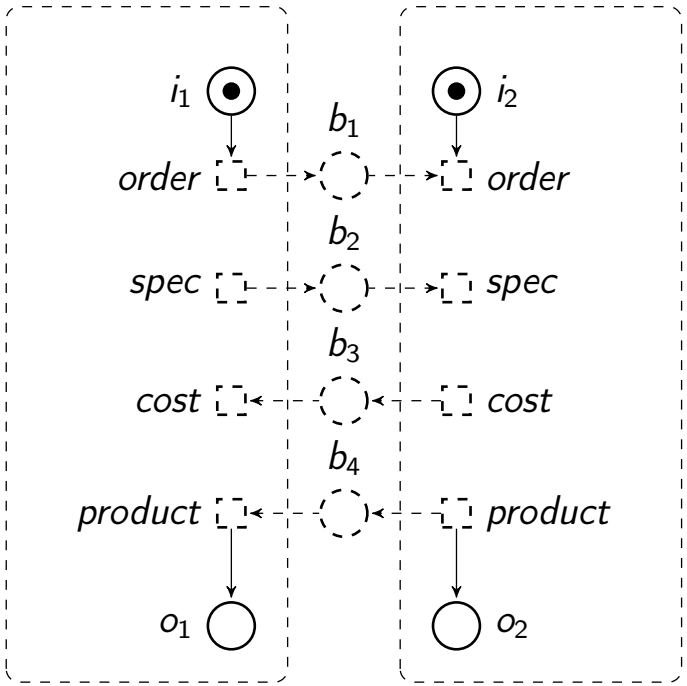


Interface Graph

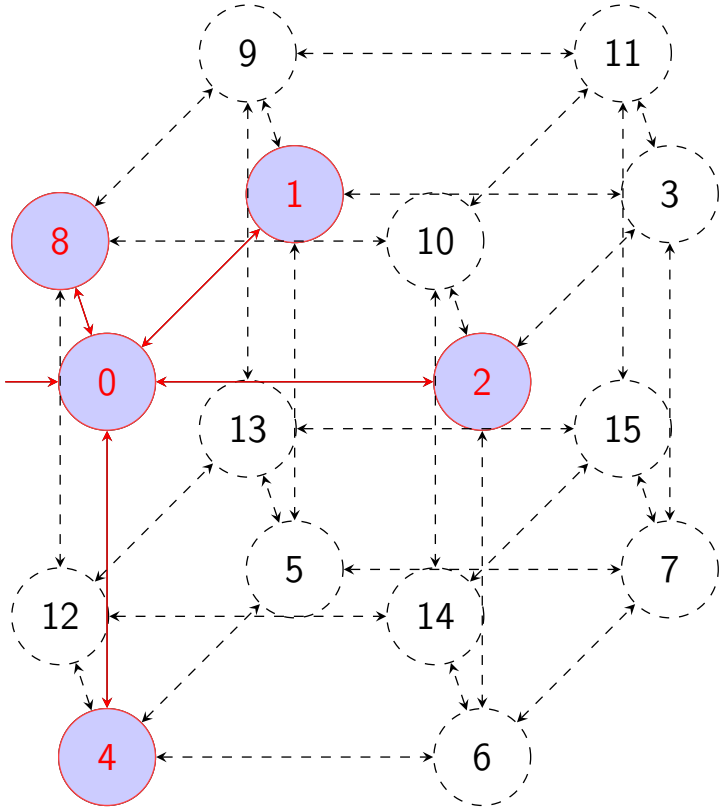


Asynchronous Composition

Interface medium



Interface Graph



explicit size: 109/373 vs 8/9

Outline

Other Correction Criteria

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)

- Specific criteria (expressed with LTL)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness **[Van Der Aalst ICATPN'97]**
    - Option to complete
    - Proper completion
    - No dead transitions
- Specific criteria (expressed with LTL)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness **[Van Der Aalst ICATPN'97]**
    - Option to complete
    - Proper completion
    - No dead transitions
  - Weak Soundness
    - Option to complete

- Specific criteria (expressed with LTL)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness **[Van Der Aalst ICATPN'97]**
    - Option to complete
    - Proper completion
    - No dead transitions
  - Weak Soundness
    - Option to complete
  - Relaxed Soundness
    - Each transition belongs to a proper execution

- Specific criteria (expressed with LTL)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness **[Van Der Aalst ICATPN'97]**
    - Option to complete
    - Proper completion
    - No dead transitions
  - Weak Soundness
    - Option to complete
  - Relaxed Soundness
    - Each transition belongs to a proper execution
  - Easy Soundness
    - There exists a proper execution
- Specific criteria (expressed with LTL)

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness **[Van Der Aalst ICATPN'97]**
    - Option to complete
    - Proper completion
    - No dead transitions
  - Weak Soundness
    - Option to complete
  - Relaxed Soundness
    - Each transition belongs to a proper execution
  - Easy Soundness
    - There exists a proper execution
- Specific criteria (expressed with LTL)
  - Any LTL property involving local/collaborative activities

Other Correction Criteria

- Generic criteria (deadlock, soundness variants)
  - Soundness [Van Der Aalst ICATPN'97]
    - Option to complete
    - Proper completion
    - No dead transitions
  - Weak Soundness
    - Option to complete
  - Relaxed Soundness
    - Each transition belongs to a proper execution
  - Easy Soundness
    - There exists a proper execution
- Specific criteria (expressed with LTL)
  - Any LTL property involving local/collaborative activities

Enrich aggregates with locally computed information

Outline

Conclusion and Perspectives

Applying Formal Methods to CSbP

Conclusion and Perspectives

Applying Formal Methods to CSbP

Correction criteria [K. Klai and H. Ochi FSEN'12, + S. Tata ICWS'13, IJWSR'13]

- generic criteria (deadlock, soundness variants)
- specific criteria (expressed with LTL)

Conclusion and Perspectives

Applying Formal Methods to CSbP

Correction criteria [K. Klai and H. Ochi FSEN'12, + S. Tata ICWS'13, IJWSR'13]

- generic criteria (deadlock, soundness variants)
- specific criteria (expressed with LTL)

Implementation:

- Deadlock-freeness (integrated to CosyVerif)
- Soundness variants
- LTL modular model checking (not finished yet)

Performs much better than LoLA and better than Woflan

Conclusion and Perspectives

- Abstraction and Modularity
  - Monolethic Verification
  - Domain-specific Verification

Conclusion and Perspectives

- Abstraction and Modularity
  - Monolethic Verification
  - Domain-specific Verification
- Perspectives
  - Finish and disseminate our tools

Conclusion and Perspectives

- Abstraction and Modularity
  - Monolethic Verification
  - Domain-specific Verification
- Perspectives
  - Finish and disseminate our tools
  - Time in Business Processes
  - Ressources in Business Processes
  - Timed Constraints as Compatibility Criteria for Web Services

Conclusion and Perspectives

- Abstraction and Modularity
  - Monolethic Verification
  - Domain-specific Verification
- Perspectives
  - Finish and disseminate our tools
  - Time in Business Processes
  - Ressources in Business Processes
  - Timed Constraints as Compatibility Criteria for Web Services
  - Service-Based Business Processes in the Cloud
    - Elastic Processes [K. Klai and S. Tata SCC'13, M. Amziani et al [CloudCom'13]]
    - Multi-tenancy, ...

Conclusion and Perspectives

- Abstraction and Modularity
  - Monolethic Verification
  - Domain-specific Verification
- Perspectives
  - Finish and disseminate our tools
  - Time in Business Processes
  - Ressources in Business Processes
  - Timed Constraints as Compatibility Criteria for Web Services
  - Service-Based Business Processes in the Cloud
    - Elastic Processes [K. Klai and S. Tata SCC'13, M. Amziani et al [CloudCom'13]]
    - Multi-tenancy, ...
  - Security Properties (Opacity [N. Hamdi, K. Klai and N.B-H Alouane WETICE'14])

THANK YOU