Ca' Foscari, University of Venice

Exact Non-Interference

Riccardo Romanello[1]

[1] Ca' Foscari, University of Venice

May 30, 2025

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Goal

- We investigate the notion of Persistence Stochastic Non-Interference

Goal

- We investigate the notion of Persistence Stochastic Non-Interference
- Current approaches [2] are built upon the notion of Lumpable Bisimulation, aka *Strong Equivalence*

Goal

- We investigate the notion of Persistence Stochastic Non-Interference
- Current approaches [2] are built upon the notion of Lumpable Bisimulation, aka *Strong Equivalence*
- We want to obtain similar results using *Exact Equivalence*

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Goal

- We investigate the notion of Persistence Stochastic Non-Interference
- Current approaches [2] are built upon the notion of Lumpable Bisimulation, aka *Strong Equivalence*
- We want to obtain similar results using *Exact Equivalence*
- Roughly speaking:
  - Strong: looks at ougoing rates
  - Exact: looks at incoming rates

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Outline of the Talk

- An High-Level view of PSNI
- Observational Equivalence
- PSNI and strong equivalence
- Exact Equivalence
- Weak-exact equivalence

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

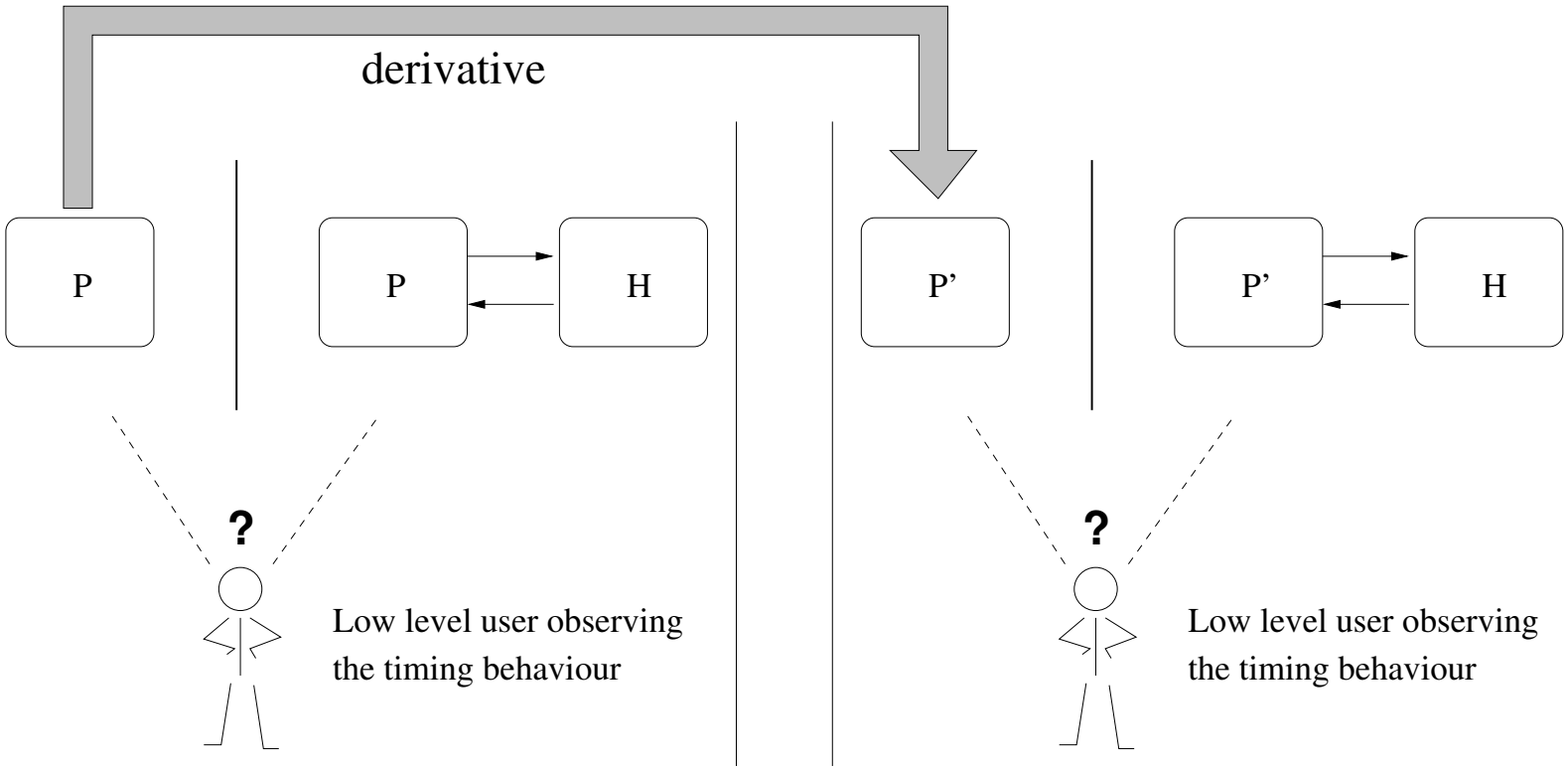
Persistent Stochastic Non-Interference

The Context

- Non-Interference aims at protecting sensitive data from undesired accesses
- Goguen-Meseguer'82: information does not flow from high (confindential) to low (public) if the high behavior cannot be observed at low level
- Persistency: Non-Interference has to be guaranteed in all the states of the system, if processes migrate during execution

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

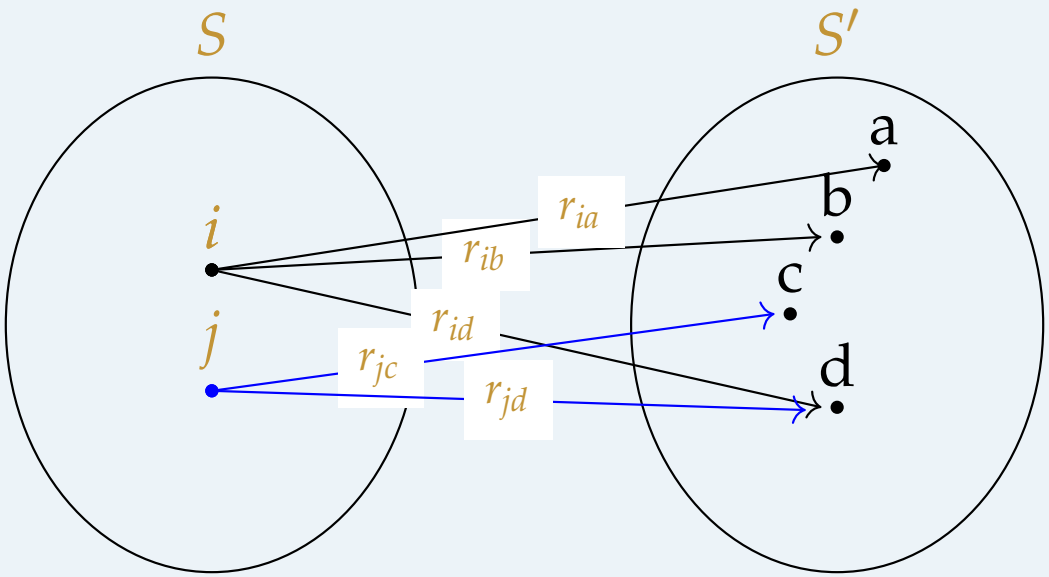
Intuitively



Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Observation Equivalence

Lumpability on the CTMC



$$r_{ia} + r_{ib} + r_{id} = r_{jc} + r_{jd}$$

Users cannot distinguish lumpable bisimilar PEPA components

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Observation Equivalence

Definition - Lumpable bisimilarity

It is the largest equivalence relation $\approx_l$ such that if $P \approx_l Q$, then for all α and for each S equivalence class

- either $\alpha \neq \tau$,
- or $\alpha = \tau$ and $P, Q \notin S$,

it holds

$$\sum_{P' \in S,\ P \xrightarrow{(\alpha, r_\alpha)} P'} r_\alpha = \sum_{Q' \in S,\ Q \xrightarrow{(\alpha, r_\alpha)} Q'} r_\alpha$$

It is *contextual*, *action preserving*, and induces a *lumpability*

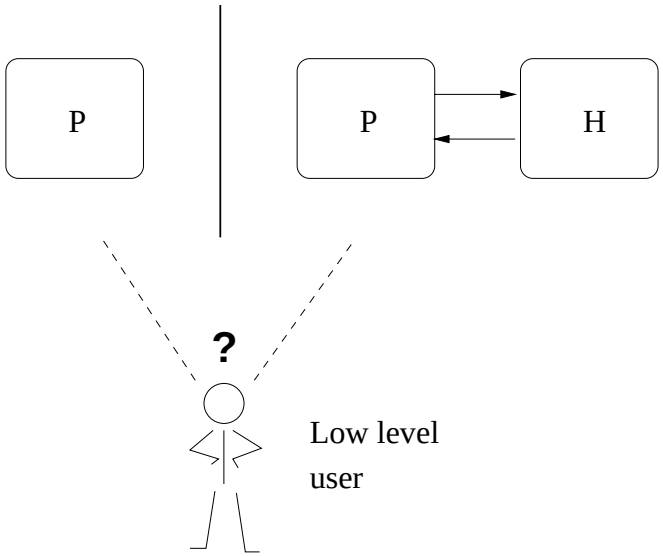
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Non-Interference

A general definition [Focardi-Gorrieri'95]

$P \in NI$ iff $\forall$ high level process H, $(P|\ 0) \sim^{low} (P|H)$

where $\sim^{low}$ denotes a low level observation equivalence



Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Stochastic Non-Interference (SNI)

- We partition the actions into $\mathcal{L}$ (low), $\mathcal{H}$ (high), $\{\tau\}$ (synch.)
- High (low) level processes can only perform(/observe) high (low) level actions

Definition - SNI

$P \in SNI$ iff $\forall$ high level PEPA component H

$$(P \underset{\mathcal{H}}{\bowtie} 0) \sim^{low} (P \underset{\mathcal{H}}{\bowtie} H)$$

The above can be rewritten as:

$$(P \underset{\mathcal{H}}{\bowtie} 0)/\mathcal{H} \approx_l (P \underset{\mathcal{H}}{\bowtie} H)/\mathcal{H}$$

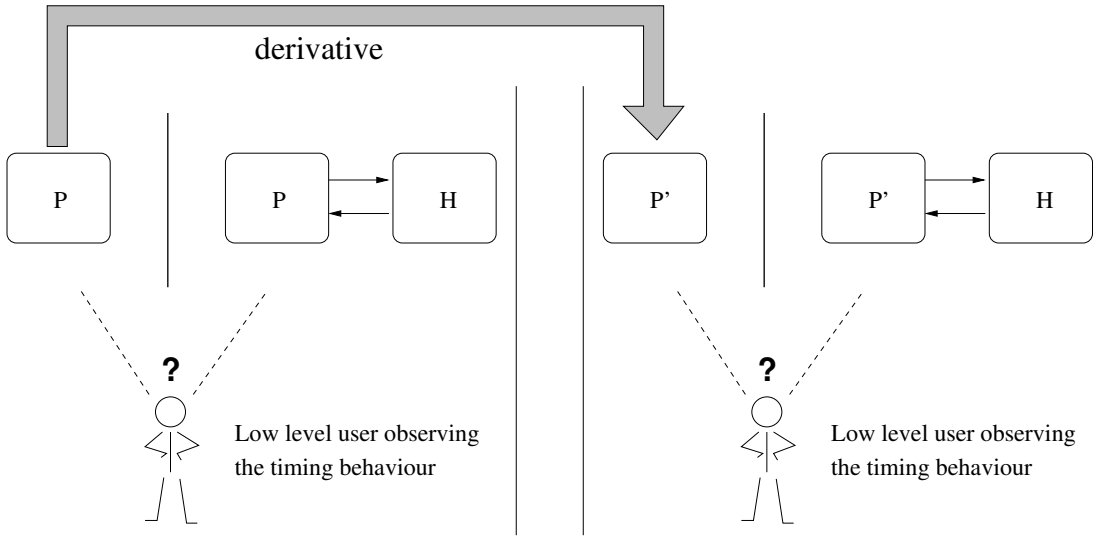
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Persistent SNI (PSNI)

Definition - PSNI

$$P \in PSNI \text{ iff } \forall \text{ derivative } P' \text{ of } P$$

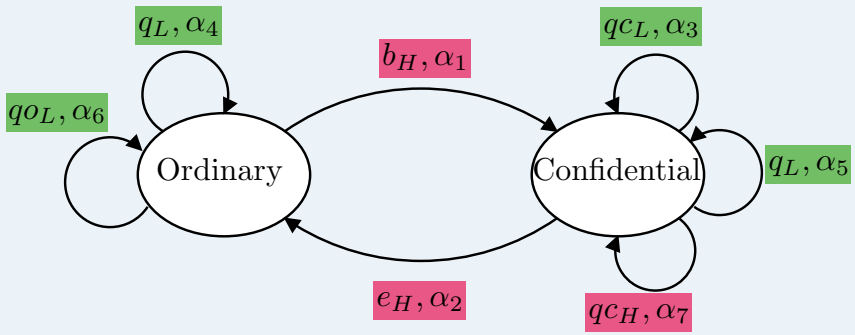
$$P' \in SNI$$



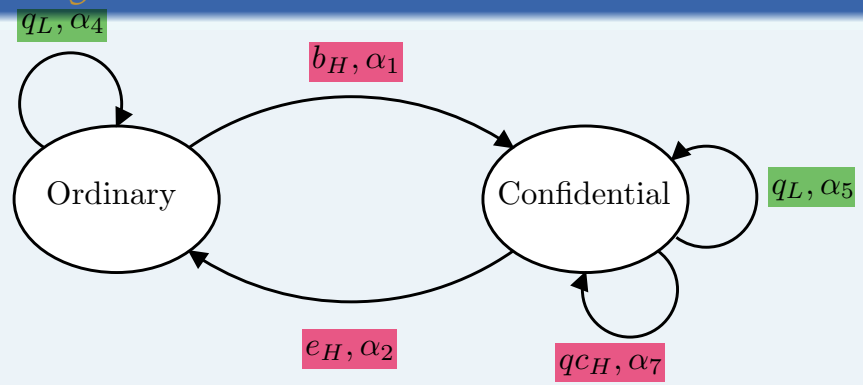
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Toy Example: Unsecure Vs Secure System

Unsecure



Secure iff $\alpha_4 = \alpha_5$



Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Our new approach

- The above notion of PSNI is based on strong equivalence/lumpable bisimilarity
- What if we leverage such notion to exact equivalence?
- We are defining a weak exact equivalence that treats τ actions in different ways that classical exact equivalence does
- Addressing the problems of:
  - Formalize PSNI in terms of such new notion
  - Provide an efficient algorithm to test this newly introduced concept

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Exact Equivalence

Exact Equivalence on CTMC

Let $X(t)$ be a CTMC with state space $S = \{0, 1, \ldots, n\}$ and $\sim$ be an equivalence relation over S. We say that $X(t)$ is exactly lumpable with respect to $\sim$ if for any $[k], [l] \in S/\sim$ and $i, j \in [l]$, it holds that $q_{[k],i} = q_{[k],j}$.

Exact Equivalence on PEPA components

An equivalence relation over PEPA components, $\mathcal{R} \subseteq \mathcal{C} \times \mathcal{C}$ is an *exact equivalence* if whenever $(P, Q) \in \mathcal{R}$, then for all $\alpha \in \mathcal{A}$:

- $q[P, \alpha] = q[S, \alpha]$
- $q[S, P, \alpha] = q[S, Q, \alpha] \quad \forall S \in \mathcal{C}/\mathcal{R}$

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Are they equivalent?

- The two definitions seem different
- The one on PEPA components seems *stricter* than the other on CTMCs

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Are they equivalent?

- The two definitions seem different
- The one on PEPA components seems *stricter* than the other on CTMCs
- The condition on total outgoing rates was introduced in [1]

Are they equivalent?

- The two definitions seem different
- The one on PEPA components seems *stricter* than the other on CTMCs
- The condition on total outgoing rates was introduced in [1]
- It must be introduced because of the diagonal elements in the infinitesimal generator
- That have no counterpart in the PEPA settings

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Are they equivalent?

- The two definitions seem different
- The one on PEPA components seems *stricter* than the other on CTMCs
- The condition on total outgoing rates was introduced in [1]
- It must be introduced because of the diagonal elements in the infinitesimal generator
- That have no counterpart in the PEPA settings
- The outgoing rate condition is fundamental for the equiprobability of the partition induced by the relation

Exact Equivalence, τ transitions, and PSNI

- Recalling that the property we want to ensure is the following: $(P \underset{\mathcal{H}}{\bowtie} 0)/\mathcal{H} \approx_l (P \underset{\mathcal{H}}{\bowtie} H)/\mathcal{H}$
- It is fundamental to carefully deal with τ-transitions

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Exact Equivalence, τ transitions, and PSNI

- Recalling that the property we want to ensure is the following: $(P \underset{\mathcal{H}}{\bowtie} 0)/\mathcal{H} \approx_l (P \underset{\mathcal{H}}{\bowtie} H)/\mathcal{H}$
- It is fundamental to carefully deal with τ-transitions
- Lumpable bisimulation achieves such endeavor by imposing different conditions according to the symbol α
- Defining PSNI with exact equivalence would have led to a trivial property

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

Weak Exact Equivalence

Weak Exact Equivalence

An equivalence relation over PEPA components, $\mathcal{R} \subseteq \mathcal{C} \times \mathcal{C}$ is a *weak exact equivalence* if whenever $(P, Q) \in \mathcal{R}$, then for all $\alpha \in \mathcal{A}$:

- either $\alpha \neq \tau$ and;
  - $q[P, \alpha] = q[Q, \alpha]$
  - $q[S, P, \alpha] = q[S, Q, \alpha] \quad \forall S \in \mathcal{C}/\mathcal{R}$
- or $\alpha = \tau$ and:
  - $q[S, P, \alpha] = q[S, Q, \alpha] \quad \forall S \in \mathcal{C}/\mathcal{R} \,.\, P, Q \notin S$
  - $q[S, P, \alpha] - q[P, \alpha] = q[S, Q, \alpha] - q[Q, \alpha] \quad P, Q \in S$

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

The results so far

- We were able to prove that our new notion induces an equiprobable stationary distribution in the underlying CTMC
- This implies that the reversed CTMC has a strong equivalence
- We are now mimicking the proofs for PSNI by substituting strong equivalence with the weak exact equivalence.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia

[1] **S. Baarir, M. Beccuti, C. Dutheillet, G. Franceschinis, and S. Haddad.**
Lumping partially symmetrical stochastic models.
Performance Evaluation, 68(1):21–44, 2011.

[2] **Jane Hillston, Carla Piazza, and Sabina Rossi.**
Persistent stochastic non-interference.
Electronic Proceedings in Theoretical Computer Science, 276:53–68, 2018.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università Ca'Foscari Venezia