Ca’ Foscari, University of Venice

Enhancing PEPA Eclipse Plugin

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

Background

- PEPA is Performance Evaluation Process Algebra

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

Background

- PEPA is Performance Evaluation Process Algebra
- Such theoretical framework has been deeply investigated in the literature

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

Background

- PEPA is Performance Evaluation Process Algebra
- Such theoretical framework has been deeply investigated in the literature
- PEPA Eclipse Plugin serves as a tool for testing and visualizing the results of such investigation

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

Our Goal

- We increased the set of features of the PEPA Eclipse Plugin

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

Our Goal

- We increased the set of features of the PEPA Eclipse Plugin
- We added a (time) reversibility control

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

Our Goal

- We increased the set of features of the PEPA Eclipse Plugin
- We added a (time) reversibility control
- We implemented all the mechanisms to handle PSNI

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

Our Goal

- We increased the set of features of the PEPA Eclipse Plugin
- We added a (time) reversibility control
- We implemented all the mechanisms to handle PSNI
- To conclude, we introduced the notion of reversible actions

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

- What I will not explain

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

- What I will not explain
- PEPA 101

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

- What I will not explain
- PEPA 101
- PEPA Eclipse Plugin
  - Reversible processes

Outline of the Talk

- What I will not explain
- PEPA 101
- PEPA Eclipse Plugin
  - Reversible processes
  - Reversible actions

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

- What I will not explain
- PEPA 101
- PEPA Eclipse Plugin
  - Reversible processes
  - Reversible actions
  - High and Low level actions

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

Assumptions

I assume you all have heard, at least once, about the following topics:

- Stochastic Processes
- Markov Chains (either Discrete or Continuous Time)
- Markov Property
- Representation of Markov Chains

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

Encoding stochastic processes

- The description of stochastic processes via Markov chains is a cumbersome and often unfeasible activity
- Moreover, it is hard to check if the stochastic process is correct or not
- Adding an abstraction layer by using a compact representation that is easy to produce and verify, can be a way to address both the issues
- Stochastic process algebras fit this role of *additional layer*
- We adopt PEPA as process algebra to model stochastic processes.

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

Performance Evaluation Process Algebra

- A PEPA model consists of a set of components that engage either individually or cooperatively in activities
- Components represent identifiable units, and can be either atomic or composed
- Activities capture actions performed by the components. Every activity is associated with an action type
- Activities are not instantaneous. The probability that an activity a with rate r happens within a period of time of length t is given by $F_a(t) = 1 - e^{-rt}$
- Hence, an activity with action type α and rate r is completely defined by the pair (α, r).

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

PEPA - Syntax and Semantics

Definition - PEPA Syntax

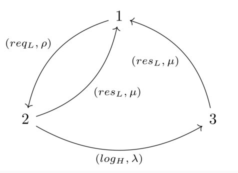
Let $\mathcal{A}$ be a set of actions with $\tau \in \mathcal{A}$
Let $\alpha \in \mathcal{A}$, $A \subseteq \mathcal{A}$, and $r \in \mathbb{R} \cup \{\top\}$

$$
\begin{array}{rcl}
S & ::= & \mathbf{0} \mid (\alpha, r).S \mid S + S \mid X \\
P & ::= & P \underset{A}{\bowtie} P \mid P/A \mid P \setminus A \mid S
\end{array}
$$

Each variable X is associated to a definition $X \stackrel{\text{def}}{=} P$

PEPA defines Labeled Continuous Time Markov Chains

Example



$$\begin{aligned} X_1 &= (req_L, \rho).X_2 \\ X_2 &= (res_L, \mu).X_1 + (log_H, \lambda).X_3 \\ X_3 &= (res_L, \mu).X_1 \end{aligned}$$

PEPA - Semantics for Synchronization

$$\frac{P \xrightarrow{(\alpha,r)} P'}{P \underset{A}{\bowtie} Q \xrightarrow{(\alpha,r)} P' \underset{A}{\bowtie} Q} \; (\alpha \notin A) \qquad \frac{Q \xrightarrow{(\alpha,r)} Q'}{P \underset{A}{\bowtie} Q \xrightarrow{(\alpha,r)} P \underset{A}{\bowtie} Q'} \; (\alpha \notin A)$$

$$\frac{P \xrightarrow{(\alpha,r_1)} P' \quad Q \xrightarrow{(\alpha,r_2)} Q'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,R)} P' \underset{A}{\bowtie} Q'} \quad (\alpha \in A)$$

$$\text{where} \quad R = \frac{r_1}{r_\alpha(P)} \frac{r_2}{r_\alpha(Q)} \min(r_\alpha(P), r_\alpha(Q))$$

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

New feature #1

- Reversibility of Markovian Processes can be modelled in two ways
- Time reversibility deals with inverting the flow of time
- Causal reversibility deals with *undoing* operations in the correct order

New feature #1

- Time Reversibility is usually characterized by means of two results:
  - Kolmogorov condition
  - Detailed Balance Equations

ρ-Reversibility [3]

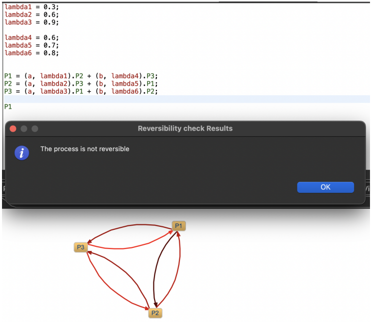
Algorithm 1: ReversibleUpTo($\mathcal{S}, \mathbf{P}, \rho$)

```
for i ∈ S do
    color[i] = white
    Π[i] = +∞
end
Π[1] = 1
return DFS-ReversibleUpTo(S, P, 1, ρ)
```

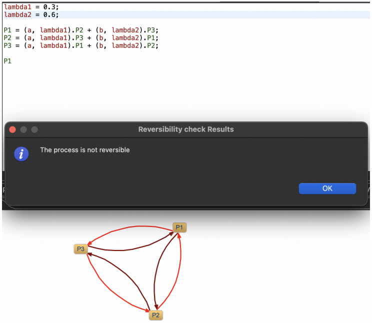
Algorithm 2: DFS-ReversibleUpTo($\mathcal{S}, \mathbf{P}, i, \rho$)

```
bool = true
for bool ∧ p[i,j] ≠ 0 do
    if (p[ρ[j], ρ[i]] = 0) then
        bool = false
    end
    if (color[j] ≠ white ∧ Π[i]p[i,j] ≠ Π[j]p[ρ[j], ρ[i]])
     then
        bool = false
    end
    if (color[j] = white) then
        color[j] = grey
        Π[j] = Π[i] p[i,j] / p[ρ[j], ρ[i]]
        bool = bool ∧ DFS-ReversibleUpTo(S, P, j, ρ)
    end
end
return bool
```

What we did



(a) A non-reversible process.



(b) Yet Another Non-Reversible process.

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

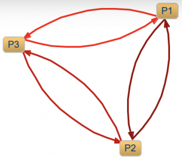
A Positive Case

```
lambda1 = 0.3;
lambda2 = 0.4;
lambda3 = 0.5;

P1 = (a, lambda1).P2 + (b, lambda3).P3;
P2 = (a, lambda2).P3 + (b, lambda1).P1;
P3 = (a, lambda3).P1 + (b, lambda2).P2;

P1
```

Reversibility check Results

The process is reversible

OK



Another Positive Case

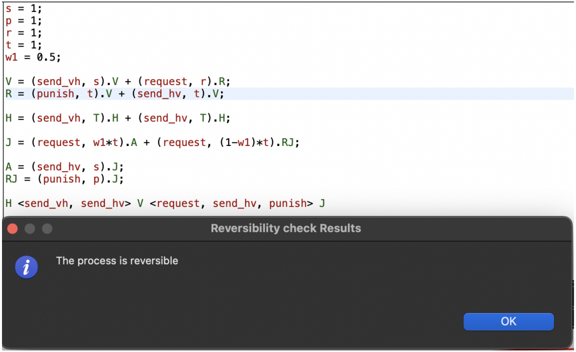


Figure 4: An (Hacked) Blockchain with punish mechanism. Process defined in a yet to be published work.

New Feature #2

- The second feature deals with *reversibility*

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

New Feature #2

- The second feature deals with *reversibility*
- Starting from the previous work presented in [1]

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

New Feature #2

- The second feature deals with *reversibility*
- Starting from the previous work presented in [1]
- We defined a set of reversible actions

New Feature #2

- The second feature deals with *reversibility*
- Starting from the previous work presented in [1]
- We defined a set of reversible actions
- If a process is reached via a reversible action, it cannot be reached by any other action

New Feature #2

- The second feature deals with *reversibility*
- Starting from the previous work presented in [1]
- We defined a set of reversible actions
- If a process is reached via a reversible action, it cannot be reached by any other action
- In the LTS we introduce a *backward* edge per each reversible transition

A Legal Reversible Action

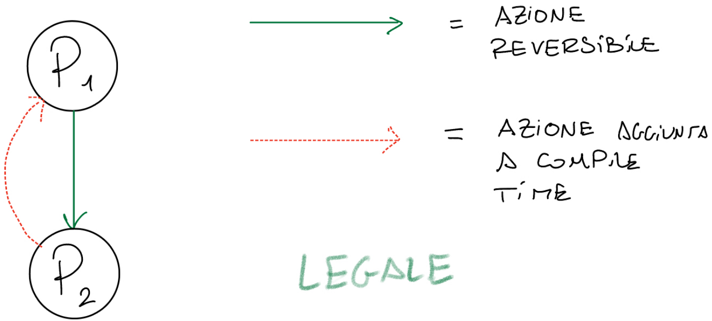


Figure 5: A correctly used reversible action

An Illegal Reversible Action

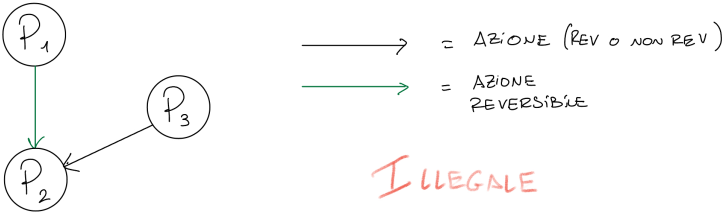
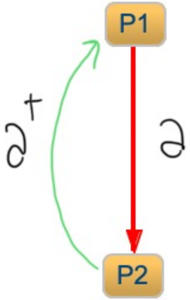


Figure 6: An incorrectly used reversible action

A simple reversible tree

```
one = 1.0;

rev_actions a;

P1 = (a, one).P2;

P1
```

(a) PEPA process.



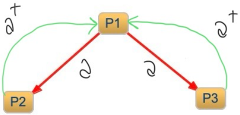
(b) (Edited) induced LTS.

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

Yet Another Simple Reversible Tree

```
one = 1.0;

rev_actions a;

P1 = (a, one).P2 + (a, one).P3;

P1
```

(a) PEPA process.



(b) (Edited) induced LTS.

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

New feature #3

- The last feature concerns Persistent Stochastic Non-Interference

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

New feature #3

- The last feature concerns Persistent Stochastic Non-Interference
- Non-Interference aims at protecting sensitive data from undesired accesses

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

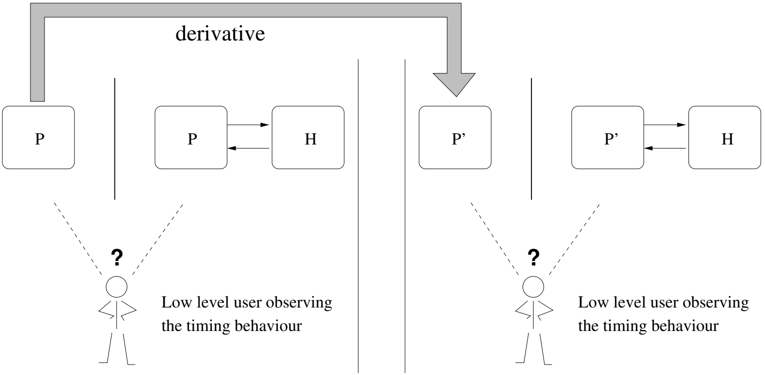
New feature #3

- The last feature concerns Persistent Stochastic Non-Interference
- 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

New feature #3

- The last feature concerns Persistent Stochastic Non-Interference
- 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

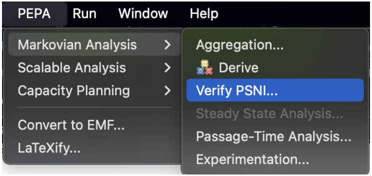
Intuitively



An example

```
set_default_level low;
high a;
low b;

lambda1 = 0.5;

lambda2 = 0.6;

P1 = (a, lambda1).P2;
P2 = (b, lambda2).P1;

P1 <> P2
```

(a) Setting High and Low level actions



(b) Verifying PSNI

A Lottery Ticket Example

```
one = 1.0;
half = 0.5;
epsilon = 0.000001;

set_default_level low;

high drawh;

F = (w1, half).W1 + (w2, half).W2;

UF = (tau, 1).UF1;

UF1 = (w1, one-epsilon).W1 + (w2, epsilon).W2;

W1 = (tau, one).W1;
W2 = (tau, one).W2;

P = (tau, one).F + (drawh, one).UF + (tau, one).P;

P
```

Figure 10: A Non-PSNI process, modelled from an example provided in [2].

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

[1] **Marco Bernardo and Sabina Rossi.**
Reverse bisimilarity vs. forward bisimilarity.
In Orna Kupferman and Pawel Sobocinski, editors, *Foundations of Software Science and Computation Structures*, pages 265–284, Cham, 2023. Springer Nature Switzerland.

[2] **Andrea Esposito, Alessandro Aldini, and Marco Bernardo.**
Noninterference analysis of irreversible or reversible systems with nondeterminism and probabilities, 2025.

[3] **Matteo Sottana, Carla Piazza, and Andrea Albarelli.**
Efficient computation of renaming functions for p-reversible discrete and continuous time markov chains.
In *Proceedings of the 11th EAI International Conference on Performance Evaluation Methodologies and Tools,*

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

VALUETOOLS 2017, page 52–59. Association for Computing Machinery, 2017.

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