Noninterference in Reversible Systems: Nondeterminism, Probability, Time

Andrea Esposito

University of Urbino

Noninterference

- The notion of noninterference was introduced for the first time by Goguen & Meseguer (1982).
- Used to reason about the way in which illegitimate information flows can occur in multi-level security systems by exploiting covert channels.
- Noninterference guarantees that low-level agents can never infer from their observations what high-level agents are doing.
- Security property verification is carried out with different approaches: type theory, abstract interpretation, model checking, etc.
- Regardless of the specific implementation, noninterference is closely tied to the notion of behavioral equivalence among processes.
- We studied noninterference for four types of reversible systems:
  - Nondeterministic systems.
  - Probabilistic systems.
  - Stochastically timed systems.
  - Deterministically timed systems.

Noninterference Analysis of Nondeterministic Reversible Systems

Noninterference in Reversible Systems

- In the process algebraic framework one of the most established formal definitions of equivalence employed for noninterference properties is weak bisimilarity (Milner 1989).
- Focardi & Gorrieri (2001) provided a characterization of these properties in a process algebraic framework, resulting in a study of their features and comparisons between them.

Noninterference in Reversible Systems

- In the process algebraic framework one of the most established formal definitions of equivalence employed for noninterference properties is weak bisimilarity (Milner 1989).
- Focardi & Gorrieri (2001) provided a characterization of these properties in a process algebraic framework, resulting in a study of their features and comparisons between them.
- Is it adequate to study noninterference in reversible systems?

Noninterference in Reversible Systems

- In the process algebraic framework one of the most established formal definitions of equivalence employed for noninterference properties is weak bisimilarity (Milner 1989).
- Focardi & Gorrieri (2001) provided a characterization of these properties in a process algebraic framework, resulting in a study of their features and comparisons between them.
- Is it adequate to study noninterference in reversible systems?
- Branching bisimilarity (Van Glabbeek & Weijland 1996) has been proven to coincide with weak back-and-forth bisimilarity (De Nicola, Montanari & Vandraager 1990).
- We thus study noninterference of reversible systems based on branching bisimilarity.

Labeled Transition Systems

- To represent process behavior we use a labeled transition system, a state-transition graph whose transitions are labeled with actions.

Definition

A *labeled transition system (LTS)* is a triple $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ where:

- $\mathcal{S} \neq \emptyset$ is an at most countable set of states.
- $\mathcal{A} \neq \emptyset$ is a countable set of actions with $\tau \in \mathcal{A}$ denoting the unobservable action.
- $\longrightarrow \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ is a transition relation.

Weak Bisimilarity

- Weak bisimilarity was introduced by Milner (1989) to abstract from the invisible (or internal) τ-action.
- $\stackrel{\tau^*}{\Longrightarrow}$ is a finite (possibly empty) sequence of $\stackrel{\tau}{\longrightarrow}$.
- $\stackrel{\hat{a}}{\Longrightarrow}$ is $\stackrel{\tau^*}{\Longrightarrow}$ if $a = \tau$, $\stackrel{\tau^*}{\Longrightarrow}\stackrel{a}{\longrightarrow}\stackrel{\tau^*}{\Longrightarrow}$ otherwise.

Definition

$s_1 \approx_{\mathrm{w}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some weak bisimulation $\mathcal{B}$.
A symmetric relation $\mathcal{B}$ over $\mathcal{S}$ is a *weak bisimulation* iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

- For each $s_1 \stackrel{a}{\longrightarrow} s_1'$ there exists $s_2 \stackrel{\hat{a}}{\Longrightarrow} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.

Branching Bisimilarity

- Introduced by Van Glabbeek & Wejland (1996) as a refinement of weak bisimilarity that preserves the branching structure of processes even when abstracting from τ-actions.

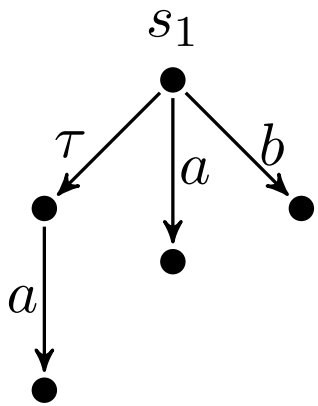
Definition

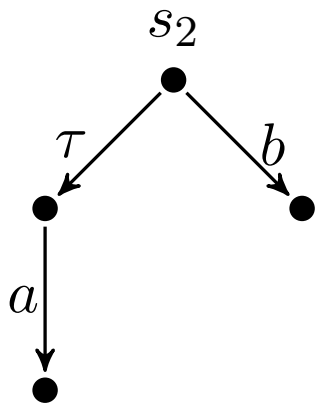
$s_1 \approx_b s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some branching bisimulation $\mathcal{B}$.
A symmetric relation $\mathcal{B}$ over $\mathcal{S}$ is a *branching bisimulation* iff, whenever $(s_1, s_2) \in \mathcal{B}$:

- For each $s_1 \xrightarrow{a} s_1'$, then:
  - either $a = \tau$ and $(s_1', s_2) \in \mathcal{B}$;
  - or there exists $s_2 \xRightarrow{\tau^*} \bar{s}_2 \xrightarrow{a} s_2'$ s.t. $(s_1, \bar{s}_2) \in \mathcal{B}$ and $(s_1', s_2') \in \mathcal{B}$.

Weak and Branching Bisimilarity

- States s_1 and s_2 are related by $\approx_{\mathrm{w}}$ but distinguished by $\approx_{\mathrm{b}}$:





Nondeterministic Process Language

- The set of process terms $\mathbb{P}_{\mathrm{nd}}$ is the following, where $a \in \mathcal{A}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:

$$
\begin{array}{rcll}
\mathbb{P}_{\mathrm{nd}} & ::= & \underline{0} & \text{terminated process} \\
& | & a \,.\, P & \text{action prefix} \\
& | & P_1 + P_2 & \text{nondeterministic choice} \\
& | & P_1 \parallel_L P_2 & \text{parallel composition} \\
& | & P \setminus L & \text{restriction} \\
& | & P \,/\, L & \text{hiding} \\
& | & K & \text{constant}
\end{array}
$$

Nondeterministic Process Language

- The set of process terms $\mathbb{P}_{\mathrm{nd}}$ is the following, where $a \in \mathcal{A}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:

$$
\begin{array}{rcll}
\mathbb{P}_{\mathrm{nd}} & ::= & \underline{0} & \text{terminated process} \\
& | & a \,.\, P & \text{action prefix} \\
& | & P_1 + P_2 & \text{nondeterministic choice} \\
& | & P_1 \parallel_L P_2 & \text{parallel composition} \\
& | & P \setminus L & \text{restriction} \\
& | & P \,/\, L & \text{hiding} \\
& | & K & \text{constant}
\end{array}
$$

- Two sets of actions for multi-level security systems:
  - Low level actions: $\mathcal{A}_{\mathcal{L}}$.
  - High level actions: $\mathcal{A}_{\mathcal{H}}$.
- Overall set of actions: $\mathcal{A} := \mathcal{A}_{\mathcal{L}} \cup \mathcal{A}_{\mathcal{H}} \cup \{\tau\}$.
- Restriction and hiding are needed to formalize noninterference.

Weak-Bisimulation-Based Properties

- The first property we examine is the *Bisimulation-based Strong Nondeterministic Non Interference* (BSNNI).
- It is satisfied by any process that behaves the same when its high-level actions are forbidden or are hidden.

Definition

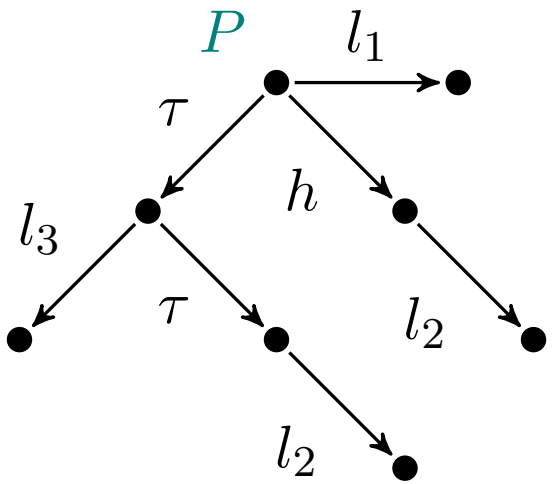
Let $P \in \mathbb{P}_{\mathrm{nd}}$. $P \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P / \mathcal{A}_{\mathcal{H}}$.

Weak-Bisimulation-Based Properties

- The first property we examine is the *Bisimulation-based Strong Nondeterministic Non Interference* (BSNNI).
- It is satisfied by any process that behaves the same when its high-level actions are forbidden or are hidden.

Definition

Let $P \in \mathbb{P}_{\mathrm{nd}}$. $P \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P \,/\, \mathcal{A}_{\mathcal{H}}$.

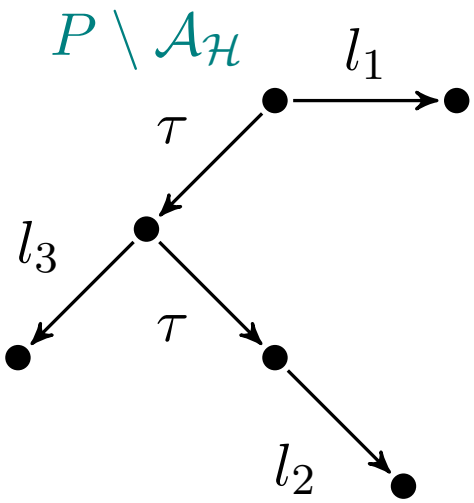


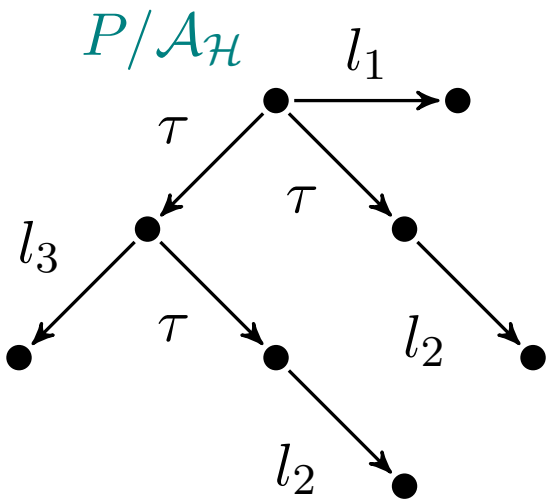
Weak-Bisimulation-Based Properties

- The first property we examine is the *Bisimulation-based Strong Nondeterministic Non Interference* (BSNNI).
- It is satisfied by any process that behaves the same when its high-level actions are forbidden or are hidden.

Definition

Let $P \in \mathbb{P}_{\mathrm{nd}}$. $P \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P / \mathcal{A}_{\mathcal{H}}$.





Bisimulation-Based Properties

- BSNNI is not powerful enough to capture covert channels that derive from the behavior of high-level agents interacting with the system, so other stronger properties have been studied in the literature.
- *Non Deducibility on Composition* (BNDC) requires to check the interaction between the system and every possible high-level agent.
- *Strong* BSNNI (SBSNNI) requires that at any reachable state the property BSNNI must be satisfied.
- *Persistent* BNDC (P_BNDC) requires that at any reachable state the property BNDC must be satisfied.
- *Strong* BNDC (SBNDC) requires that the low-level view of every reachable state of a system must be the same before and after the execution of every high-level action.

Weak-Bisimulation-Based Properties

Definition

Let $P \in \mathbb{P}_{\mathrm{nd}}$:

- $P \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx_{\mathrm{w}}} \iff$ for all $Q \in \mathbb{P}_{\mathrm{nd}}$ such that each of its actions belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} ((P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{SBSNNI}_{\approx_{\mathrm{w}}} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}}$.
- $P \in \mathrm{P\_BNDC}_{\approx_{\mathrm{w}}} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BNDC}_{\approx_{\mathrm{w}}}$.
- $P \in \mathrm{SBNDC}_{\approx_{\mathrm{w}}} \iff$ for all $P', P'' \in \mathit{reach}(P)$ such that $P' \xrightarrow{h} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P'' \setminus \mathcal{A}_{\mathcal{H}}$.

Relation among Properties

- Focardi & Gorrieri showed the following taxonomy:

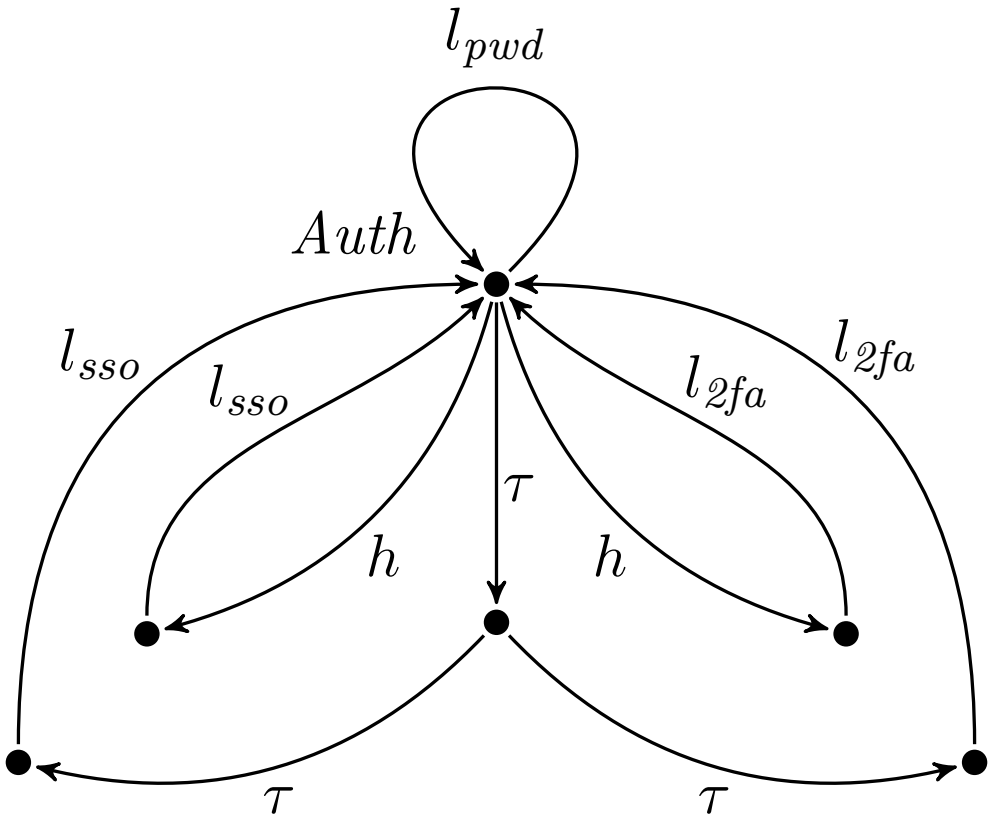
$$\mathrm{SBNDC}_{\approx_w} \longrightarrow \mathrm{SBSNNI}_{\approx_w} \longrightarrow \mathrm{BNDC}_{\approx_w} \longrightarrow \mathrm{BSNNI}_{\approx_w}$$

- Later on, $\mathrm{P\_BNDC}_{\approx_w}$ was proven to be equivalent to $\mathrm{SBSNNI}_{\approx_w}$ (Focardi & Rossi 2006).

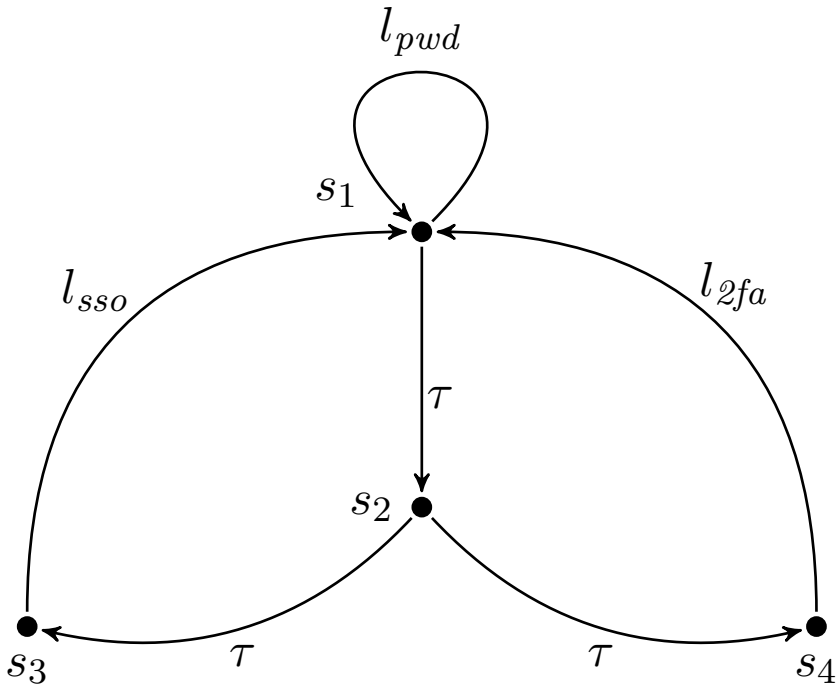
DBMS Example: Part 1

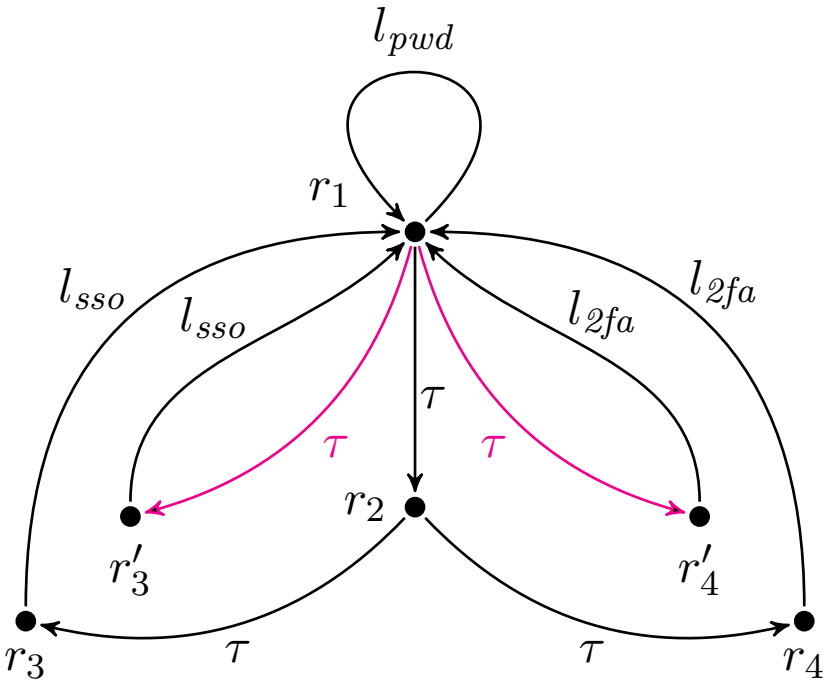
- Consider a multi-threaded system supporting the execution of concurrent transactions operating on a healthcare database.
- Only authorized users can write their data.
- The data can be shared with a dedicated module feeding the training set of a machine learning facility, which is responsible for building a trained model for data analysis purposes.
- Different authentication mechanisms to identify users:
  - A simple password-based mechanism (pwd).
  - A two-factor authentication system ($2fa$).
  - A scheme based on single sign on (sso).

DBMS Example: Part 1



DBMS Example: Part 1





$$Auth \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} Auth/\mathcal{A}_{\mathcal{H}}$$

- Assuming a standard forward-only semantics, no interference occurs.

Branching-Bisimulation-Based Properties

- We recast information-flow security definitions in terms of branching bisimilarity and investigate their characteristics as well as their relationships with the definitions based on weak bisimilarity.

Definition

Let $P \in \mathbb{P}_{\mathrm{nd}}$:

- $P \in \mathrm{BSNNI}_{\approx_{\mathrm{b}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx_{\mathrm{b}}} \iff$ for all $Q \in \mathbb{P}_{\mathrm{nd}}$ such that each of its actions belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} ((P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{SBSNNI}_{\approx_{\mathrm{b}}} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BSNNI}_{\approx_{\mathrm{b}}}$.
- $P \in \mathrm{P\_BNDC}_{\approx_{\mathrm{b}}} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BNDC}_{\approx_{\mathrm{b}}}$.
- $P \in \mathrm{SBNDC}_{\approx_{\mathrm{b}}} \iff$ for all $P', P'' \in \mathit{reach}(P)$ such that $P' \xrightarrow{h} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} P'' \setminus \mathcal{A}_{\mathcal{H}}$.

Preservation

- $\approx_{\mathrm{b}}$ preserves all the five properties.

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{nd}}$ *and*
$\mathcal{P} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{b}}}, \mathrm{BNDC}_{\approx_{\mathrm{b}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{b}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{b}}}, \mathrm{SBNDC}_{\approx_{\mathrm{b}}}\}$.
If $P_1 \approx_{\mathrm{b}} P_2$, *then* $P_1 \in \mathcal{P} \iff P_2 \in \mathcal{P}$.

- This is very useful in automated property verification as it can be more convenient to work with a reduced system, i.e., a system equivalent to the one we are checking but with a smaller state space.

Compositionality

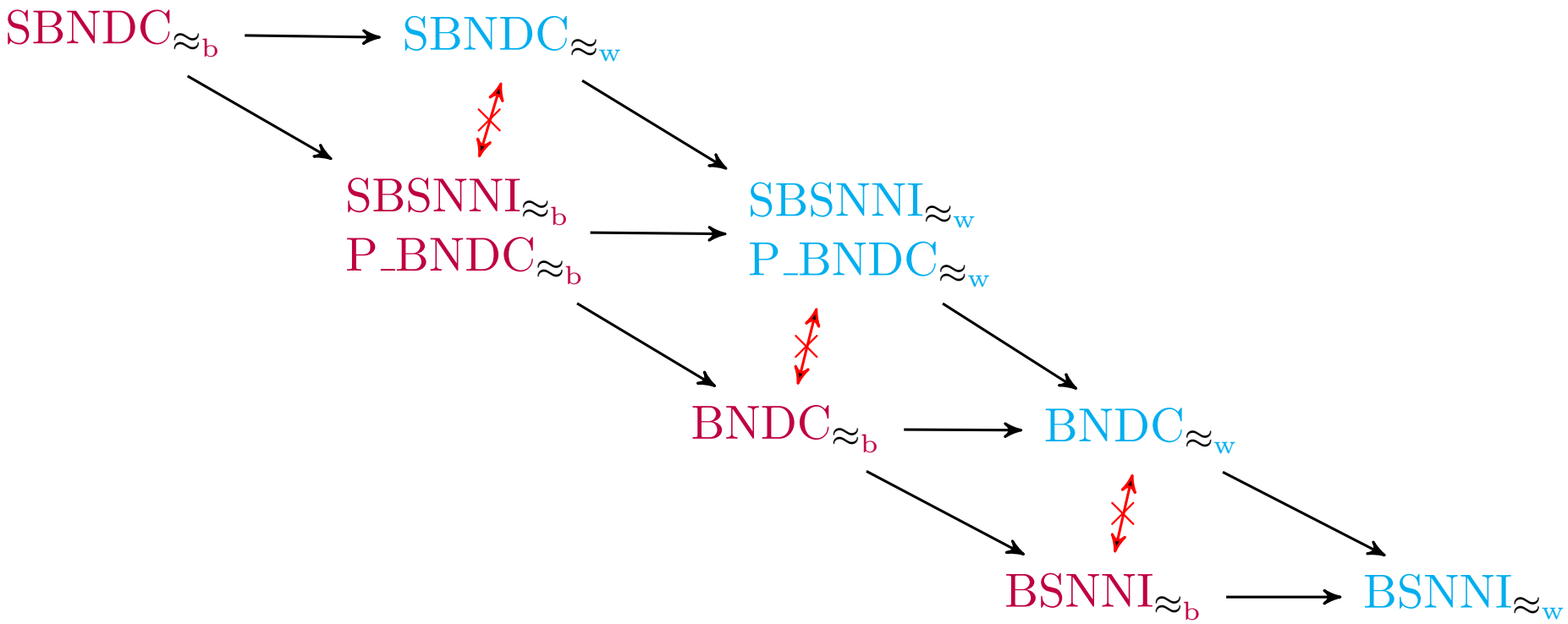
- The local properties are preserved by (most of) the operators of $\mathbb{P}_{\mathrm{nd}}$.

Theorem

Let $P, P_1, P_2 \in \mathbb{P}_{\mathrm{nd}}$, $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{b}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{b}}} \mathrm{SBNDC}_{\approx_{\mathrm{b}}}\}$. *Then:*

1. $P \in \mathcal{P} \Longrightarrow a \,.\, P \in \mathcal{P}$ *for all* $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$.
2. $P_1, P_2 \in \mathcal{P} \Longrightarrow P_1 \parallel_L P_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{b}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{b}}}\}$, $L \subseteq \mathcal{A}$ *if* $\mathcal{P} \in \{\mathrm{SBNDC}_{\approx_{\mathrm{b}}}\}$.
3. $P \in \mathcal{P} \Longrightarrow P \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
4. $P \in \mathcal{P} \Longrightarrow P / L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$.

Extended Taxonomy



Back-and-Forth Bisimilarities

- Introduced by De Nicola, Montanari and Vandraager (1990).
- Back-and-forth bisimulations are defined over *computational paths* instead of states.
- This is needed to remain in an interleaving setting of concurrency.
- It preserves not only causal consistency but also history.
- Whenever a process returns to a past state it must do it by reverting the same computational path performed in going forward.

Weak Back-and-Forth Bisimilarity

Definition

$s_1 \approx_{\mathrm{bf}} s_2$ iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak back-and-forth bisimulation $\mathcal{B}$.

A symmetric relation $\mathcal{B}$ over $\mathcal{U}$ is a *weak back-and-forth bisimulation* iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:

- For each $\rho_1 \xrightarrow{a} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ s.t. $(\rho_1', \rho_2') \in \mathcal{B}$;
- For each $\rho_1' \xrightarrow{a} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ s.t. $(\rho_1', \rho_2') \in \mathcal{B}$.

Weak Back-and-Forth Bisimilarity

- Weak back-and-forth bisimilarity is finer than weak bisimilarity.
- Weak back-and-forth bisimilarity coincides with branching bisimilarity.

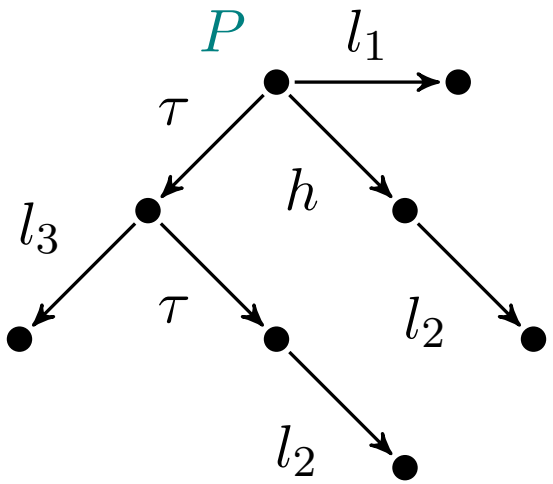
Theorem

$$s_1 \approx_{\mathrm{bf}} s_2 \textit{ iff } s_1 \approx_{\mathrm{b}} s_2.$$

- We can reason about reversible systems without resorting to a reversible calculus nor a path-based equivalence.
- All the results for branching-bisimulation-based properties can be extended to reversible systems.

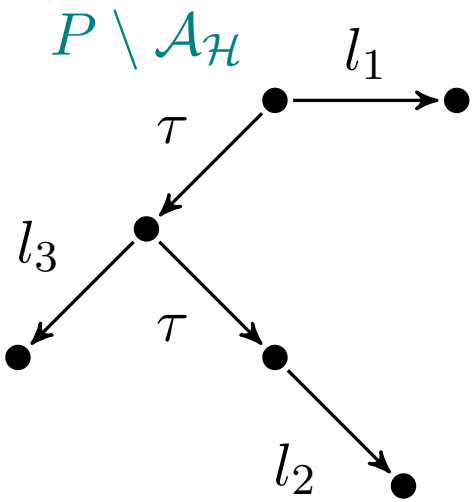
Example

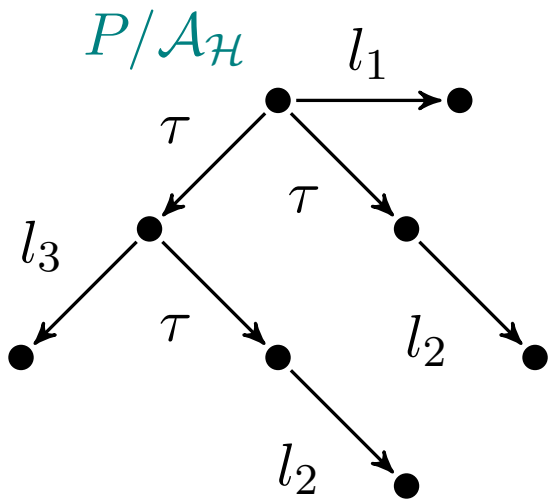
- Let us look again at the $\mathrm{BSNNI}_{\approx_w}$-secure process P:



Example

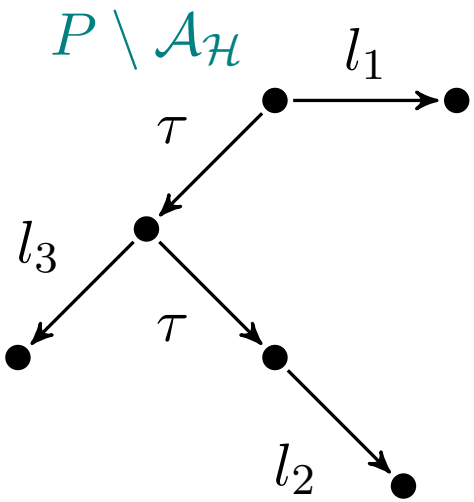
- If we take P as a reversible system we can see that it is not secure:

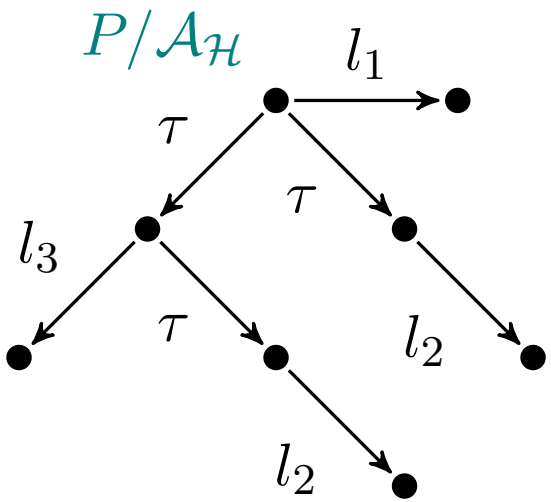




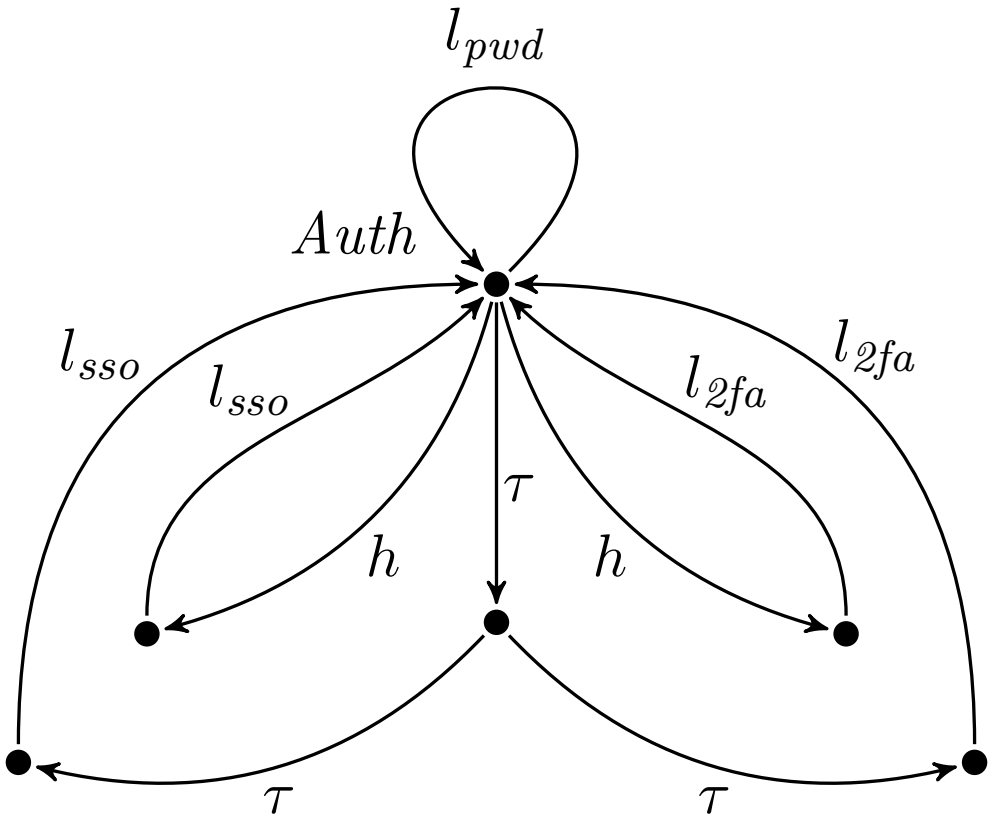
Example

- The information-flow can be also detected by employing $\mathrm{BSNNI}_{\approx_b}$:

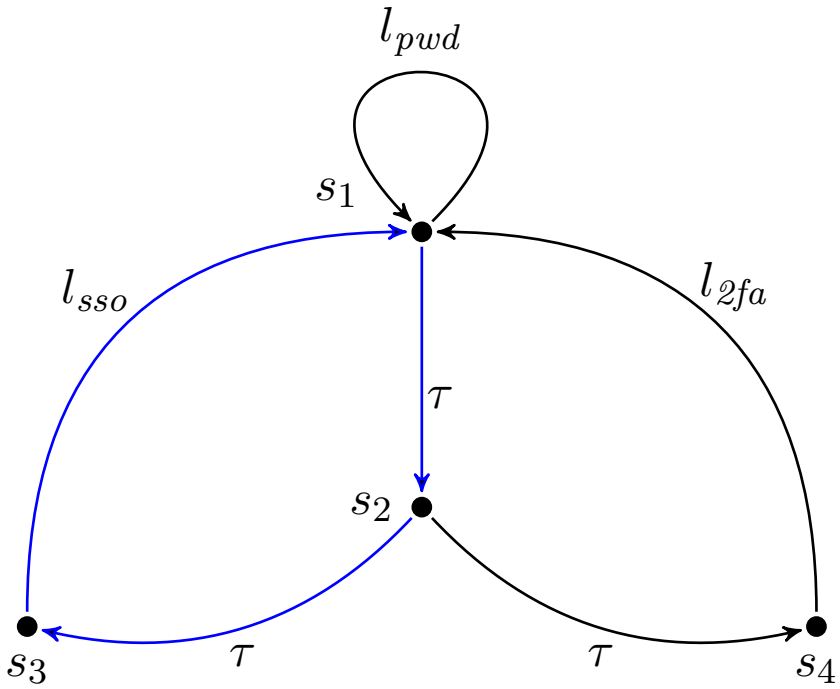


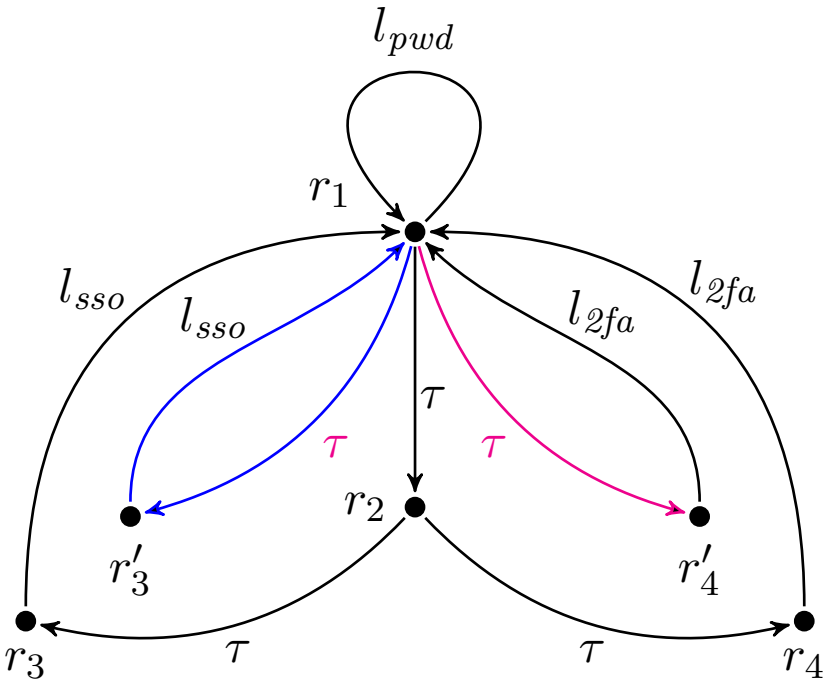


DBMS Example: Part 2



DBMS Example: Part 2





$$Auth \setminus \mathcal{A}_{\mathcal{H}} \not\approx_b Auth/\mathcal{A}_{\mathcal{H}}$$

- Assuming a reversible semantics, interference occurs.

Noninterference Analysis of Probabilistic Reversible Systems

Noninterference in Probabilistic Reversible Systems

- How to analyze noninterference in probabilistic reversible systems?

Noninterference in Probabilistic Reversible Systems

- How to analyze noninterference in probabilistic reversible systems?
- Probabilistic noninterference has been investigated by Aldini, Bravetti, & Gorrieri (2004) in the generative-reactive model, where only a very limited form of nondeterminism is allowed.
- In their calculus, in addition to probabilistic choice, other operators such as parallel composition and hiding are decorated with a probabilistic parameter.
- This complicates the definitions of noninterference properties as they require universal quantifications over probabilistic parameters.

Noninterference in Probabilistic Reversible Systems

- We want to study noninterference for reversible systems that feature both nondeterminism and probabilities.
- A more expressive probabilistic model is the strictly alternating model introduced by Hansson & Jonsson (1990):
  - States are divided into nondeterministic ($\mathcal{S}_{\mathrm{n}}$) and probabilistic ($\mathcal{S}_{\mathrm{p}}$).
  - Transitions are divided into:
    - action transitions, from $\mathcal{S}_{\mathrm{n}}$ to $\mathcal{S}_{\mathrm{p}}$
    - probabilistic transitions, from $\mathcal{S}_{\mathrm{p}}$ to $\mathcal{S}_{\mathrm{n}}$.
- We use weak and branching bisimilarities for this model to recast a variety of noninterference properties.
- A process calculus in which to express noninterference properties, where only the probabilistic choice operator is decorated.

Probabilistic Labeled Transition Systems

Definition

A *probabilistic labeled transition system (PLTS)* is a triple $(\mathcal{S}, \mathcal{A}, \longrightarrow)$:

- $\mathcal{S} = \mathcal{S}_{\mathrm{n}} \cup \mathcal{S}_{\mathrm{p}} \neq \emptyset$ is an at most countable set of nondet. ($\mathcal{S}_{\mathrm{n}}$) and prob. ($\mathcal{S}_{\mathrm{p}}$) states with $\mathcal{S}_{\mathrm{n}} \cap \mathcal{S}_{\mathrm{p}} = \emptyset$.
- $\mathcal{A} \neq \emptyset$ is a countable set of actions with $\tau \in \mathcal{A}$ denoting the unobservable action.
- $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{p}}$ is a transition relation where:
  - $\longrightarrow_{\mathrm{a}} \subseteq \mathcal{S}_{\mathrm{n}} \times \mathcal{A} \times \mathcal{S}_{\mathrm{p}}$ is the action transition relation.
  - $\longrightarrow_{\mathrm{p}} \subseteq \mathcal{S}_{\mathrm{p}} \times \mathbb{R}_{]0,1[} \times \mathcal{S}_{\mathrm{n}}$ is the probabilistic transition relation where $\sum_{s \xrightarrow{p}_{\mathrm{p}} s'} p \in \{0, 1\}$ for all $s \in \mathcal{S}_{\mathrm{p}}$.

Probabilistic Bisimilarities

- Identifying nondeterministic (resp. probabilistic) states when they behave the same based on their transitions [HJ90].
- Philippou, Lee, & Sokolsky (2000) additionally allow a nondeterministic state and a probabilistic state to be identified when the latter concentrates all of its probabilistic mass in reaching the former:

$$\mathit{prob}(s, s') = \begin{cases} p & \text{if } s \in \mathcal{S}_{\mathrm{p}} \wedge \sum_{s \xrightarrow{p'}_{\mathrm{p}} s'} p' = p > 0 \\ 1 & \text{if } s \in \mathcal{S}_{\mathrm{n}} \wedge s' = s \\ 0 & \text{otherwise} \end{cases}$$

- The function is then lifted to a set C of states by letting $\mathit{prob}(s, C) = \sum_{s' \in C} \mathit{prob}(s, s')$.

Weak Probabilistic Bisimilarity

- $\Longrightarrow$ is a finite sequence of alternating $\xrightarrow{\tau}_{\mathrm{a}}$ and $\xrightarrow{p}_{\mathrm{p}}$.
- $\overset{\hat{a}}{\Longrightarrow}$ is $\Longrightarrow$ if $a = \tau$, $\Longrightarrow \xrightarrow{a}_{\mathrm{a}} \Longrightarrow$ otherwise.

Definition

$s_1 \approx_{\mathrm{pw}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some weak probabilistic bisimulation $\mathcal{B}$.
An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a weak probabilistic bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$:

- For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ there exists $s_2 \overset{\hat{a}}{\Longrightarrow} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.
- $\mathit{prob}(s_1, C) = \mathit{prob}(s_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.

- By restricting the definition to nondeterministic states and ignoring *prob* we obtain $\approx_{\mathrm{w}}$.

Probabilistic Branching Bisimilarity

- A probabilistic variant for the non-strictly alternating model was introduced by Andova, Georgievska, and Trčka (2012).

Definition

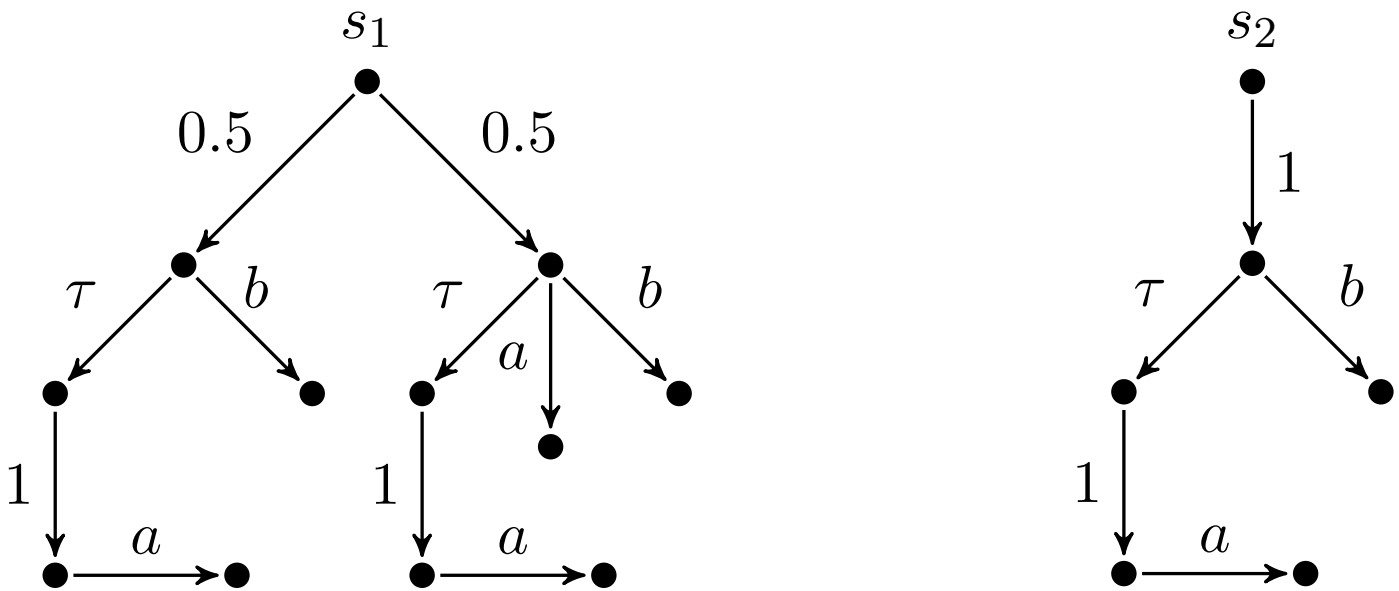
$s_1 \approx_{\mathrm{pb}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some probabilistic branching bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a probabilistic branching bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

- For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$:
  - either $a = \tau$ and $(s_1', s_2) \in \mathcal{B}$;
  - or there exists $s_2 \Longrightarrow \bar{s}_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ s.t. $(s_1, \bar{s}_2) \in \mathcal{B}$ and $(s_1', s_2') \in \mathcal{B}$.
- $\mathit{prob}(s_1, C) = \mathit{prob}(s_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.

- By restricting the definition to nondeterministic states and ignoring *prob* we obtain $\approx_{\mathrm{b}}$.

Weak and Branching Probabilistic Bisimilarities

- States s_1 and s_2 related by $\approx_{\mathrm{pw}}$ but distinguished by $\approx_{\mathrm{pb}}$:



Process Language: Nondeterministic Processes

- The overall set of process terms is $\mathbb{P}_{\mathrm{pr}} = \mathbb{P}_{\mathrm{n}} \cup \mathbb{P}_{\mathrm{p}}$.
- The set of nondeterministic process terms $\mathbb{P}_{\mathrm{n}}$ is the following where $a \in \mathcal{A}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:

$$
\begin{array}{rcll}
N & ::= & \underline{0} & \text{terminated process} \\
 & | & a \,.\, P & \text{action prefix} \\
 & | & N_1 + N_2 & \text{nondeterministic choice} \\
 & | & N_1 \parallel_L N_2 & \text{parallel composition} \\
 & | & N \setminus L & \text{restriction} \\
 & | & N \,/\, L & \text{hiding} \\
 & | & N K & \text{nondeterministic constant}
\end{array}
$$

- Set of visible actions: $\mathcal{A} := \mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$.

Process Language: Probabilistic Processes

- The set of probabilistic process terms $\mathbb{P}_{\mathrm{p}}$ is the following:

$$
\begin{array}{rcll}
P & ::= & \bigoplus_{i \in I} [p_i] N_i & \text{probabilistic choice} \\
 & | & P_1 \parallel_L P_2 & \text{parallel composition} \\
 & | & P \setminus L & \text{restriction} \\
 & | & P \,/\, L & \text{hiding} \\
 & | & PK & \text{probabilistic constant}
\end{array}
$$

Process Language: Probabilistic Processes

- The set of probabilistic process terms $\mathbb{P}_{\mathrm{p}}$ is the following:

$$
\begin{array}{rcll}
P & ::= & \bigoplus_{i \in I} [p_i] N_i & \text{probabilistic choice} \\
 & | & P_1 \parallel_L P_2 & \text{parallel composition} \\
 & | & P \setminus L & \text{restriction} \\
 & | & P \,/\, L & \text{hiding} \\
 & | & PK & \text{probabilistic constant}
\end{array}
$$

- $\bigoplus_{i \in I} [p_i] \_$ is the generalized probabilistic composition operator expressing a probabilistic choice among finitely many processes each with probability $p_i \in \mathbb{R}_{]0,1]}$ and such that $\sum_{i \in I} p_i = 1$.
- Parallel composition multiplies probabilistic transition labels.
- Restriction and hiding do not apply to probabilistic transitions.

Probabilistic Noninterference Properties

- We can recast the noninterference properties using the probabilistic bisimilarities.

Definition

Let $E \in \mathbb{P}_{\mathrm{pr}}$ and $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$:

- $E \in \mathrm{BSNNI}_{\approx} \iff E \setminus \mathcal{A}_{\mathcal{H}} \approx E \,/\, \mathcal{A}_{\mathcal{H}}$.
- $E \in \mathrm{BNDC}_{\approx} \iff$ for all $F \in \mathbb{P}_{\mathrm{pr}}$ such that each of its actions belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $E \setminus \mathcal{A}_{\mathcal{H}} \approx ((E \,\|_L\, F) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $E \in \mathrm{SBSNNI}_{\approx} \iff$ for all $E' \in \mathit{reach}(E)$, $E' \in \mathrm{BSNNI}_{\approx}$.
- $E \in \mathrm{P\_BNDC}_{\approx} \iff$ for all $E' \in \mathit{reach}(E)$, $E' \in \mathrm{BNDC}_{\approx}$.
- $E \in \mathrm{SBNDC}_{\approx} \iff$ for all $E', E'' \in \mathit{reach}(E)$ such that $E' \xrightarrow{h} E''$, $E' \setminus \mathcal{A}_{\mathcal{H}} \approx E'' \setminus \mathcal{A}_{\mathcal{H}}$.

Preservation and Compositionality

Theorem

Let $E_1, E_2 \in \mathbb{P}_{\mathrm{pr}}$, $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$, *and* $\mathcal{P} \in \{\mathrm{BSNNI}_{\approx}, \mathrm{BNDC}_{\approx}, \mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx}, \mathrm{SBNDC}_{\approx}\}$.

If $E_1 \approx E_2$, *then* $E_1 \in \mathcal{P} \iff E_2 \in \mathcal{P}$.

Theorem

Let $E, E_1, E_2 \in \mathbb{P}_{\mathrm{pr}}$, $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$, $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx} \mathrm{SBNDC}_{\approx}\}$. *Then:*

1. $E \in \mathcal{P} \Longrightarrow a \,.\, E \in \mathcal{P}$ *for all* $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$ *and* $E \in \mathbb{P}_{\mathrm{p}}$.
2. $E_1, E_2 \in \mathcal{P} \Longrightarrow E_1 \parallel_L E_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}\}$, $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{pw}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{pw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{pw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{pb}}}\}$.
3. $E \in \mathcal{P} \Longrightarrow E \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
4. $E \in \mathcal{P} \Longrightarrow E \,/\, L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$.

Up-to Techniques

- The usual up-to technique fails with quantititative equivalences.
- $\approx \mathcal{B} \approx$ is not always an equivalence relation.
- We take $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^+$ instead (Bravetti, Bernardo, & Gorrieri 1998).

Definition

A relation $\mathcal{B}$ over $\mathbb{P}_{\mathrm{pr}}$ is a *weak probabilistic bisimulation up to* $\approx_{\mathrm{pw}}$ iff, whenever $(E_1, E_2) \in \mathcal{B}$, then:

- For each $E_1 \stackrel{a}{\Longrightarrow} E_1'$ there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $(E_1', E_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\mathrm{pw}})^+$, and vice versa.
- $\mathit{prob}(E_1, C) = \mathit{prob}(E_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\mathrm{pr}}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\mathrm{pw}})^+$.

Definition

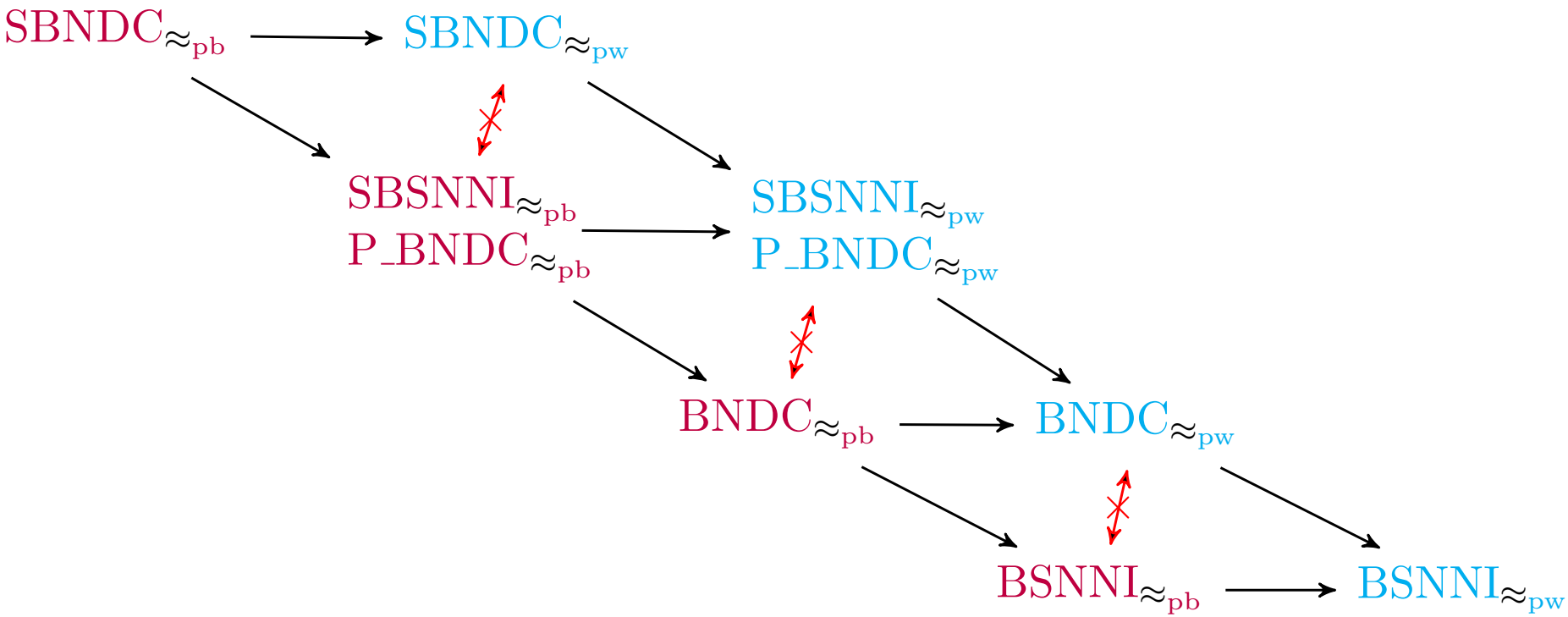
A relation $\mathcal{B}$ over $\mathbb{P}_{\mathrm{pr}}$ is a *probabilistic branching bisimulation up to* $\approx_{\mathrm{pb}}$ iff, whenever $(E_1, E_2) \in \mathcal{B}$, then:

- For each $E_1 \Longrightarrow \bar{E}_1 \xrightarrow{a}_{\mathrm{a}} E_1'$ with $E_1 \approx_{\mathrm{pb}} \bar{E}_1$:
  - either $a = \tau$ and $\bar{E}_1 \approx_{\mathrm{pb}} E_1'$;
  - or there exists $E_2 \Longrightarrow \bar{E}_2 \xrightarrow{a}_{\mathrm{a}} E_2'$ such that $(\bar{E}_1, \bar{E}_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\mathrm{pb}})^+$ and $(E_1', E_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\mathrm{pb}})^+$;

  and vice versa.
- $\mathit{prob}(E_1, C) = \mathit{prob}(E_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\mathrm{pr}}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\mathrm{pb}})^+$.

- The two definitions imply the corresponding bisimilarities.

Extended Probabilistic Taxonomy



Relating Nondeterministic and Probabilistic Taxonomies

- Given a process $E \in \mathbb{P}_{\mathrm{pr}}$, we can obtain its nondet. variant $nd(E)$ by replacing each $\bigoplus_{i \in I} [p_i] E_i$ with $\sum_{i \in I} \tau \,.\, E_i$.

Theorem

Let $E_1, E_2 \in \mathbb{P}_{\mathrm{pr}}$. *Then:*

- $E_1 \approx_{\mathrm{pw}} E_2 \Longrightarrow nd(E_1) \approx_{\mathrm{w}} nd(E_2)$.
- $E_1 \approx_{\mathrm{pb}} E_2 \Longrightarrow nd(E_1) \approx_{\mathrm{b}} nd(E_2)$.

Relating Nondeterministic and Probabilistic Taxonomies

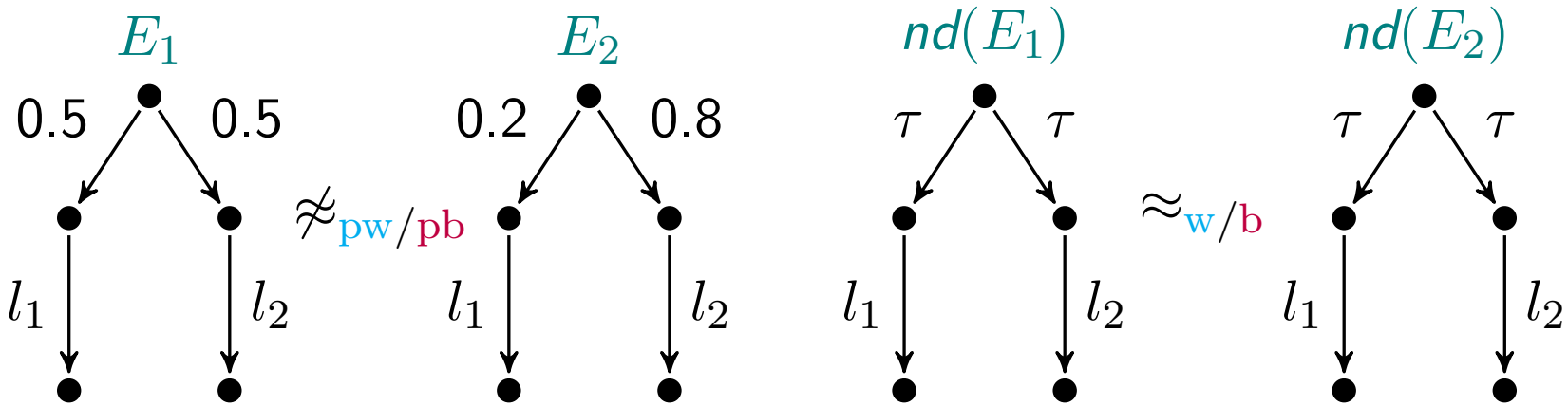
- Given a process $E \in \mathbb{P}_{\mathrm{pr}}$, we can obtain its nondet. variant $nd(E)$ by replacing each $\bigoplus_{i \in I} [p_i] E_i$ with $\sum_{i \in I} \tau \,.\, E_i$.

Theorem

Let $E_1, E_2 \in \mathbb{P}_{\mathrm{pr}}$. *Then:*

- $E_1 \approx_{\mathrm{pw}} E_2 \Longrightarrow nd(E_1) \approx_{\mathrm{w}} nd(E_2)$.
- $E_1 \approx_{\mathrm{pb}} E_2 \Longrightarrow nd(E_1) \approx_{\mathrm{b}} nd(E_2)$.

- The inverse is not true:



Relating Nondeterministic and Probabilistic Taxonomies

- A consequence is that if a process E is secure under a probabilistic noninterference property, then $nd(E)$ is secure under the corresponding nondeterministic property.

Corollary

Let $E \in \mathbb{P}_{\mathrm{pr}}, \approx_{\mathrm{pr}} \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}, \approx_{\mathrm{nd}} \in \{\approx_{\mathrm{w}}, \approx_{\mathrm{b}}\}$,
$\mathcal{P}_{\mathrm{pr}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{pr}}}, \mathrm{BNDC}_{\approx_{\mathrm{pr}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{pr}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{pr}}}, \mathrm{SBNDC}_{\approx_{\mathrm{pr}}}\}$,
$\mathcal{P}_{\mathrm{nd}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBNDC}_{\approx_{\mathrm{nd}}}\}$.
Then:

$$E \in \mathcal{P}_{\mathrm{pr}} \Longrightarrow nd(E) \in \mathcal{P}_{\mathrm{nd}}$$

- This means that our results further extend the nondeterministic taxonomy.

Weak Probabilistic Back-and-Forth Bisimilarity

- We establish a connection with reversibility through a probabilistic back-and-forth bisimilarity:

Definition

$s_1 \approx_{\mathrm{pbf}} s_2$ iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak probabilistic back-and-forth bisimulation $\mathcal{B}$.

An equivalence relation $\mathcal{B}$ over $\mathcal{U}$ is a weak probabilistic back-and-forth bisimulation iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:

- For each $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ s.t. $(\rho_1', \rho_2') \in \mathcal{B}$.
- For each $\rho_1' \xrightarrow{a}_{\mathrm{a}} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ s.t. $(\rho_1', \rho_2') \in \mathcal{B}$.
- $\mathit{prob}(\rho_1, C) = \mathit{prob}(\rho_2, C)$ for all equivalence classes $C \in \mathcal{U}/\mathcal{B}$.

Weak Probabilistic Back-and-Forth Bisimilarity

- As in the nondeterministic case, weak probabilistic back-and-forth bisimilarity coincides with probabilistic branching bisimilarity.

Theorem

$$s_1 \approx_{\mathrm{pbf}} s_2 \textit{ iff } s_1 \approx_{\mathrm{pb}} s_2.$$

- Therefore:
  - We can reason about reversible systems without resorting to a reversible calculus nor a path-based equivalence.
  - All the results for probabilistic branching-bisimulation-based properties can be extended to probabilistic reversible systems.

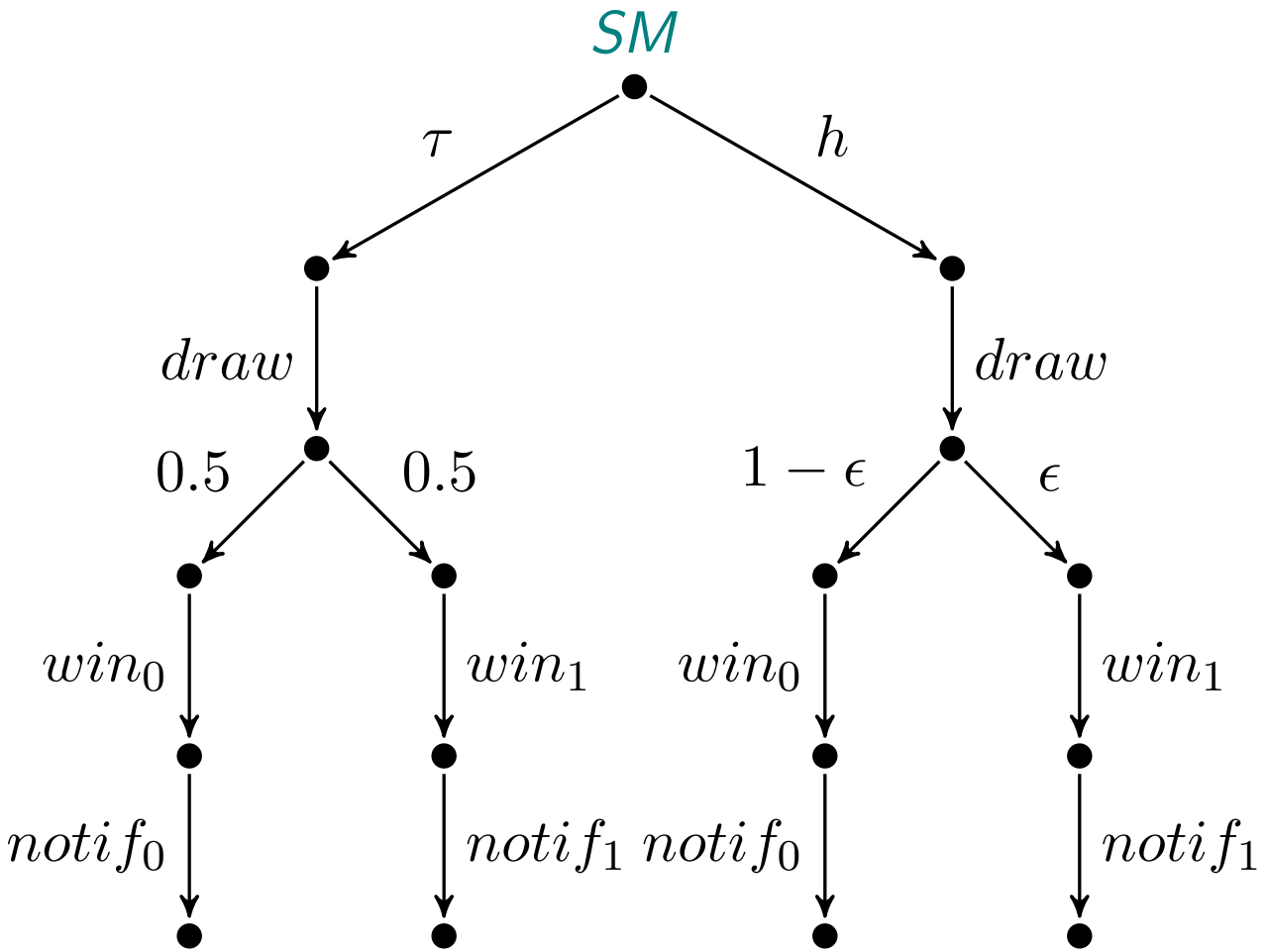
Case Study: Probabilistic Smart Contract

- Consider a lottery implemented in a probabilistic smart contract.
- Anyone can buy a ticket through a smart contract function.
- When the lottery is closed, anyone can invoke another smart contract function, draw(), in which a random number x, between 0 and the amount of sold tickets, is drawn and the entire money is paid to the owner of the extracted value x.
- We will examine two vulnerabilities:
  - The first one emphasizes the need for passing from the nondeterministic noninterference to the probabilistic one.
  - The second one emphasizes inadequacy of weak probabilistic bisimilarity when dealing with reversible systems.

Case Study: Probabilistic Smart Contract

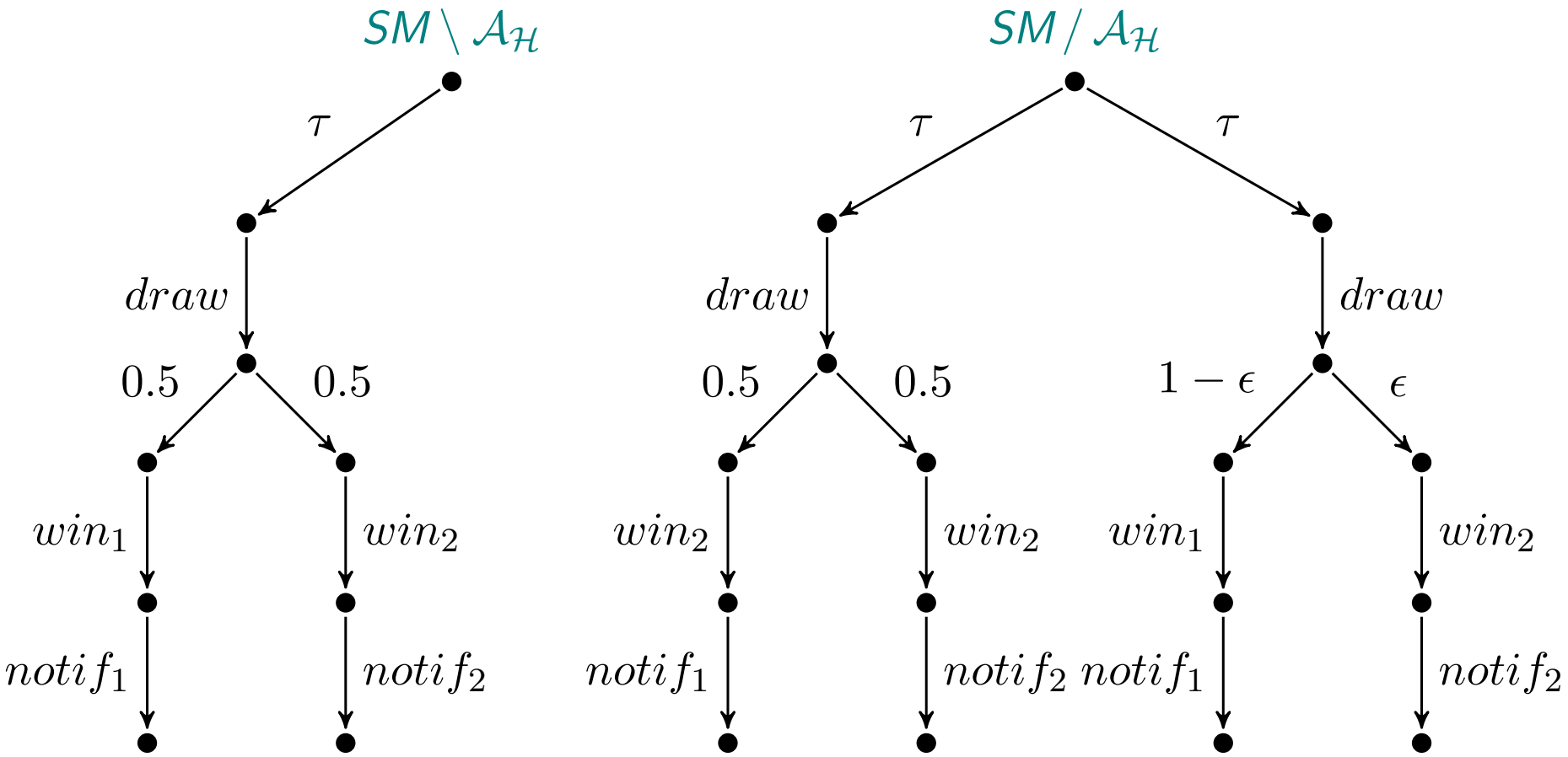
- First vulnerability: the critical point is the randomization process of the function draw().
- A widely adopted approach consists of using the timestamp of the block including the transaction of the draw invocation as the seed for random number generation.
- This approach is vulnerable in the presence of an adversary that buys a ticket and succeeds in mining the block above by using a timestamp that allows the adversary to win the lottery.
- We consider the following transitions:
  - h representing the interaction of a malicious miner.
  - win_i expressing the determination of the winner.
  - $notif_i$ expressing the notification of the winner.

Case Study: Probabilistic Smart Contract



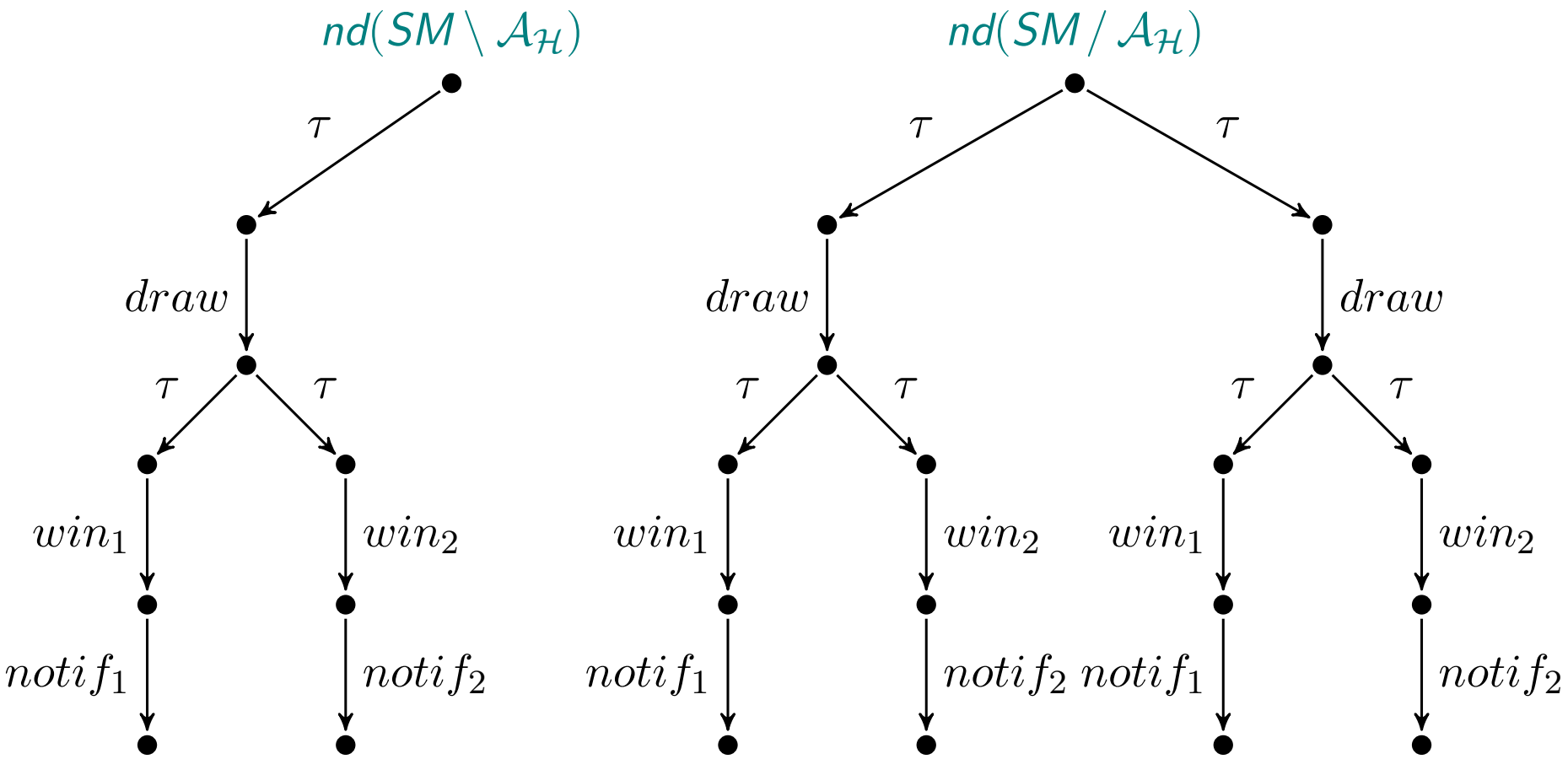
Case Study: Probabilistic Smart Contract

- The processes $SM \setminus \mathcal{A}_{\mathcal{H}}$ and $SM / \mathcal{A}_{\mathcal{H}}$ are not $\not\approx_{\mathrm{pw}/\mathrm{pb}}$:



Case Study: Probabilistic Smart Contract

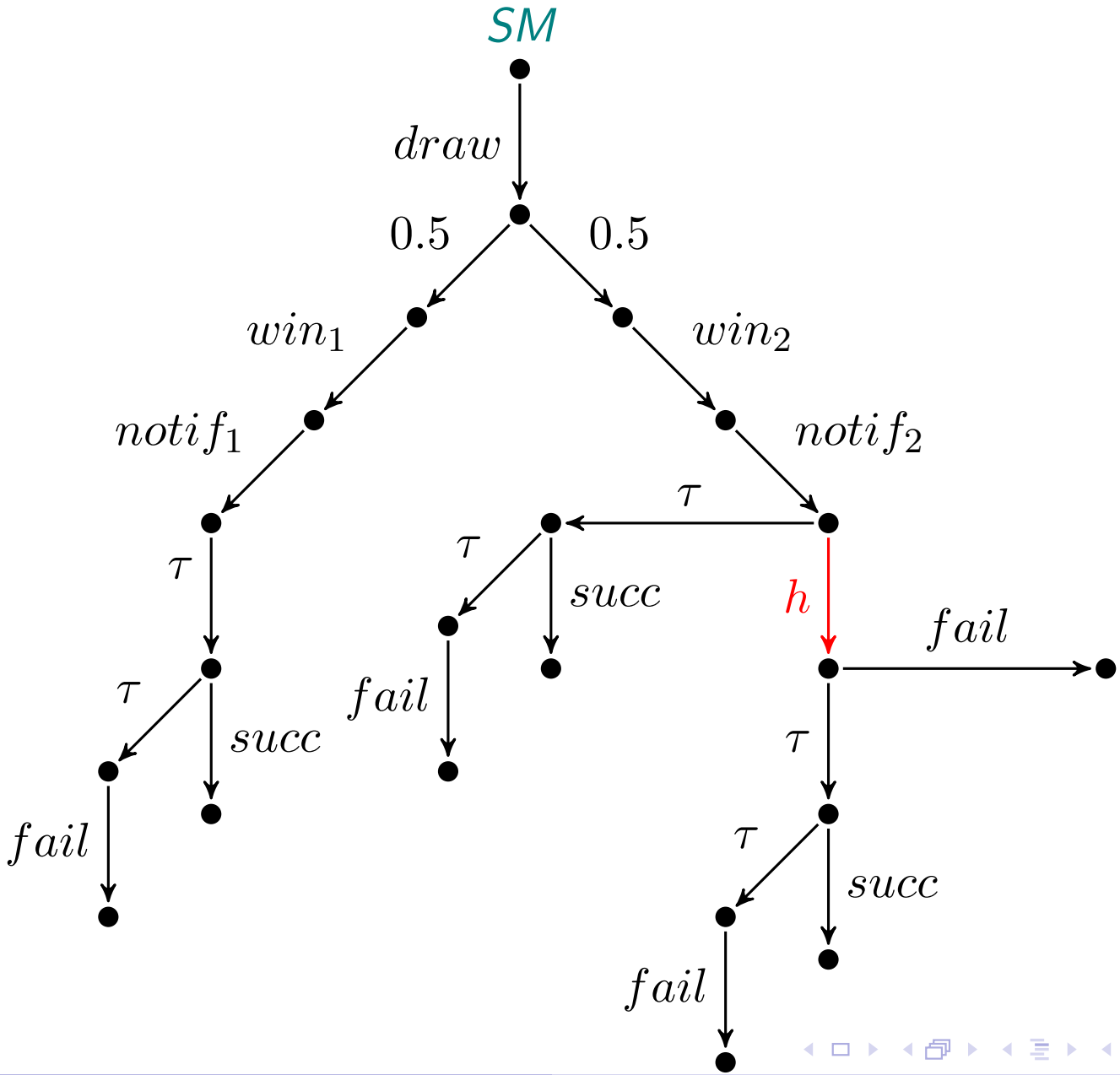
- Both processes $nd(SM \setminus \mathcal{A}_{\mathcal{H}})$ and $nd(SM \,/\, \mathcal{A}_{\mathcal{H}})$ are $\approx_{\mathrm{pw}/\mathrm{pb}}$:



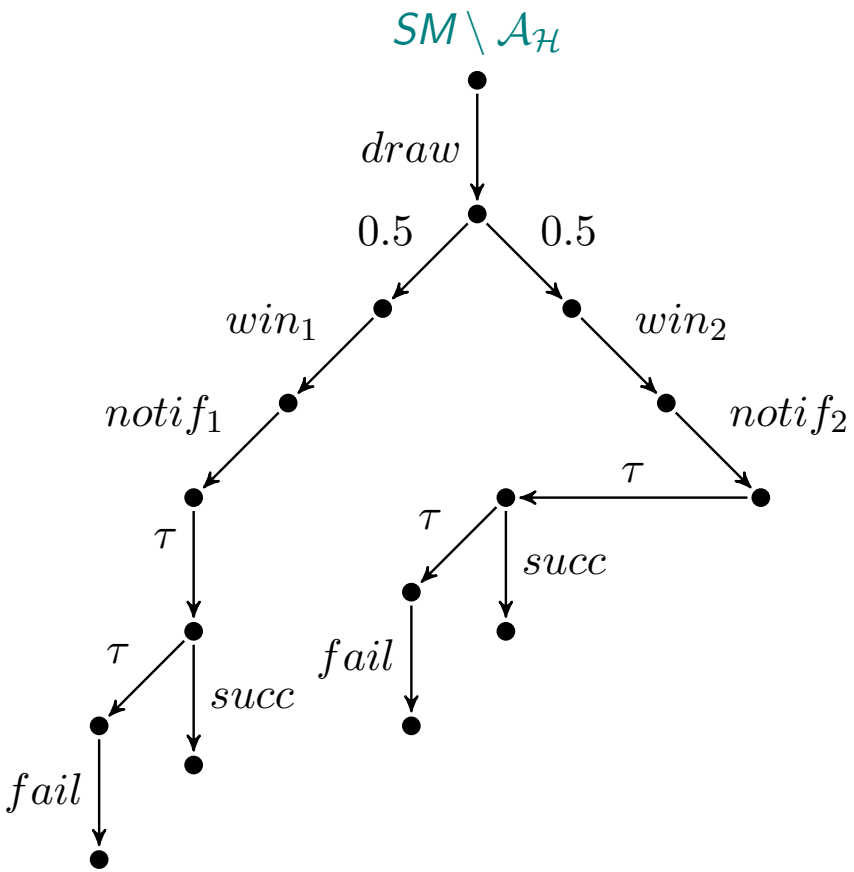
Case Study: Probabilistic Smart Contract

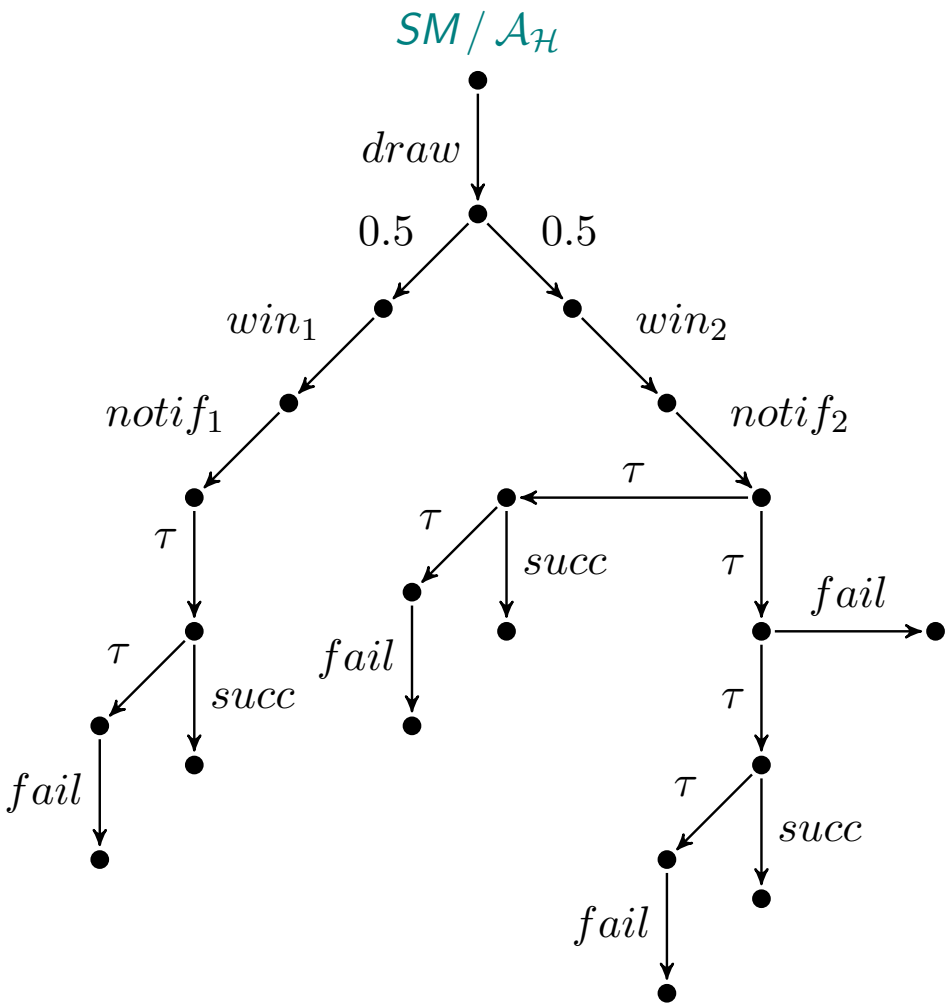
- Second vulnerability: the critical point is the mining procedure.
- Even assuming that the seed governing the probabilistic extraction cannot be manipulated, if the miner invoking the function draw() is malicious and is going to lose the lottery, that miner can ignore the related block and force the mining failure and a rollback of the lottery.
- We add the following transitions:
  - τ expressing the mining of a block, by either a honest or dishonest miner.
  - $succ$ expressing the successful termination of the mining.
  - $fail$ expressing the failed termination of the mining, it can either be forced or occur for other reasons (a wrong transaction in the block or a fork in the blockchain).

Case Study: Probabilistic Smart Contract

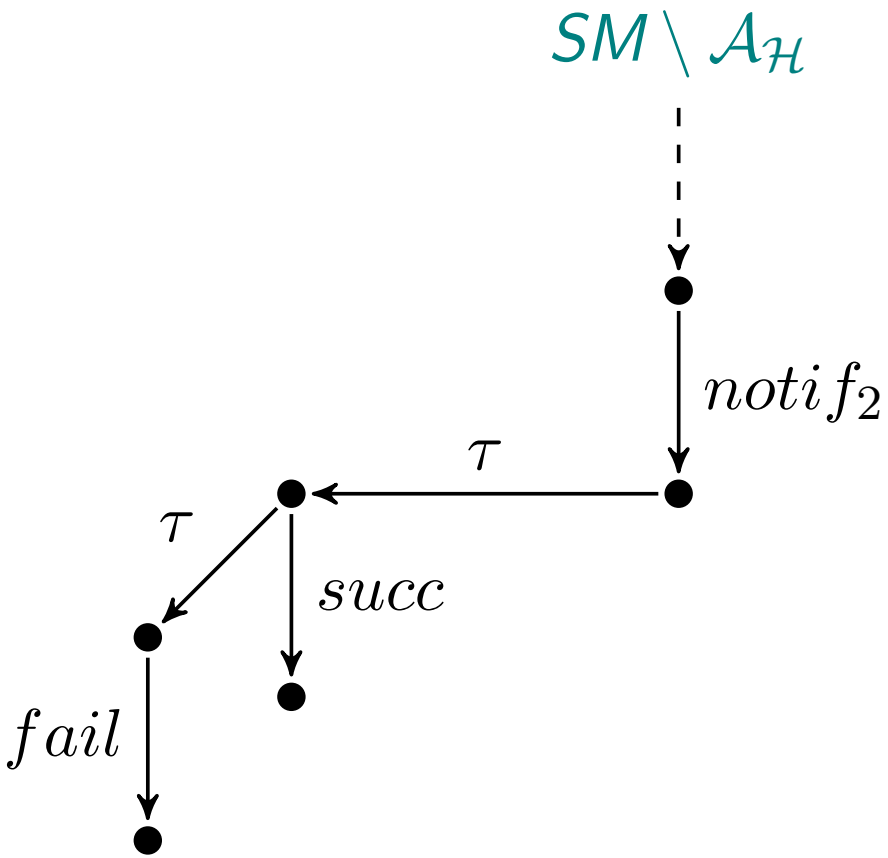


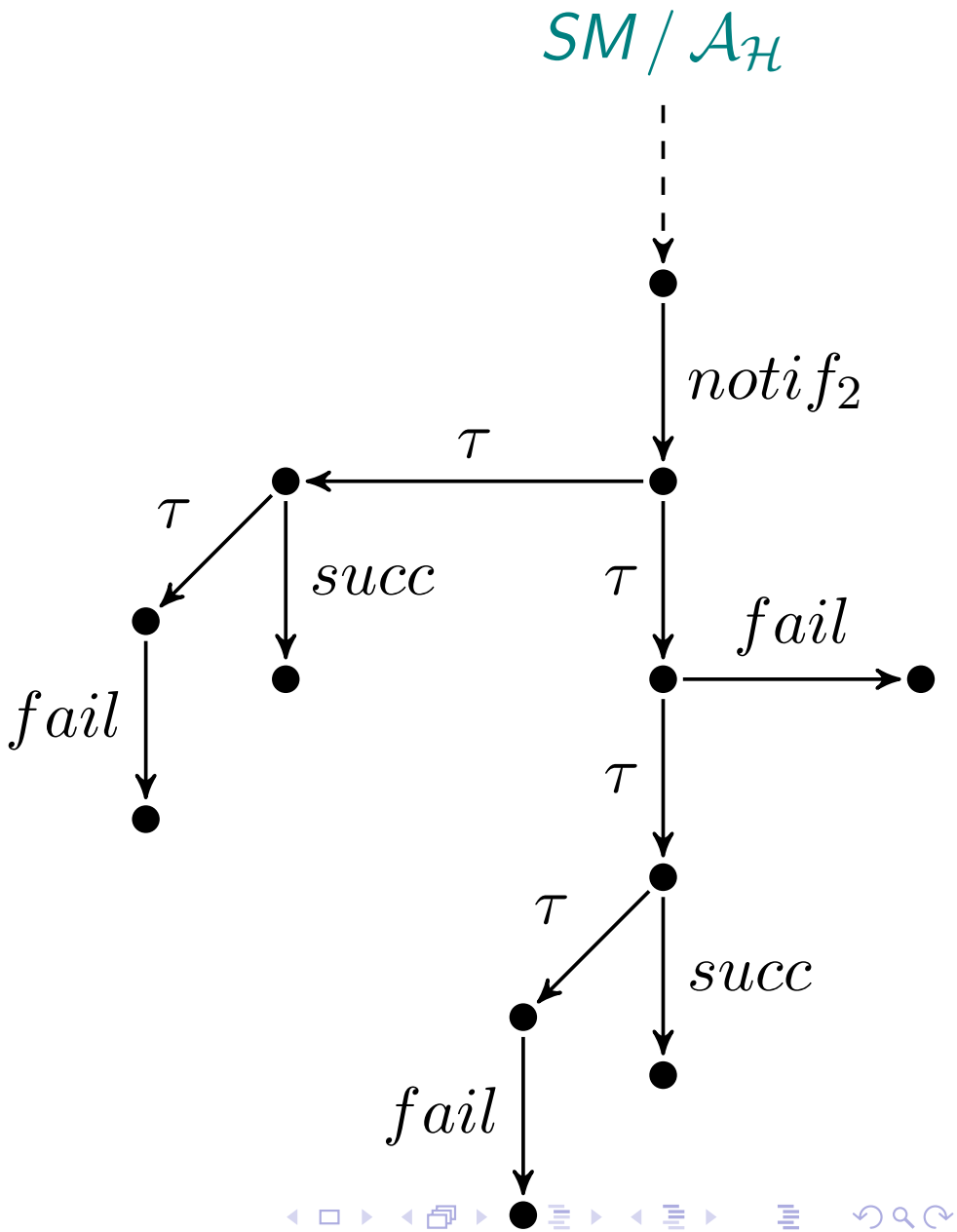
Case Study: Probabilistic Smart Contract



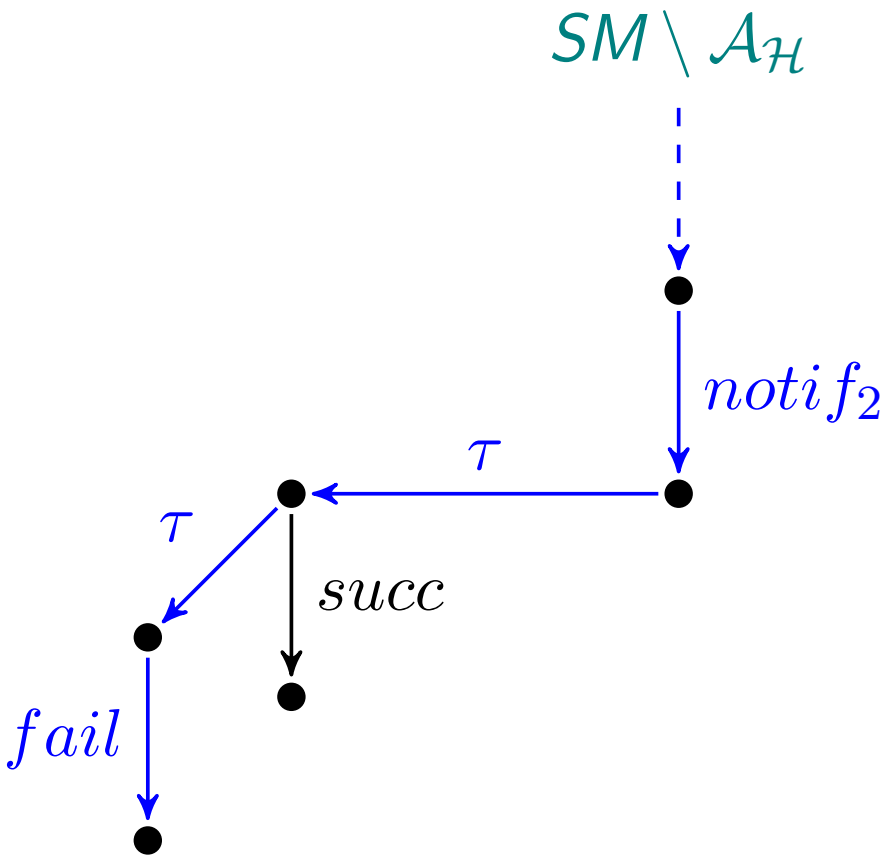


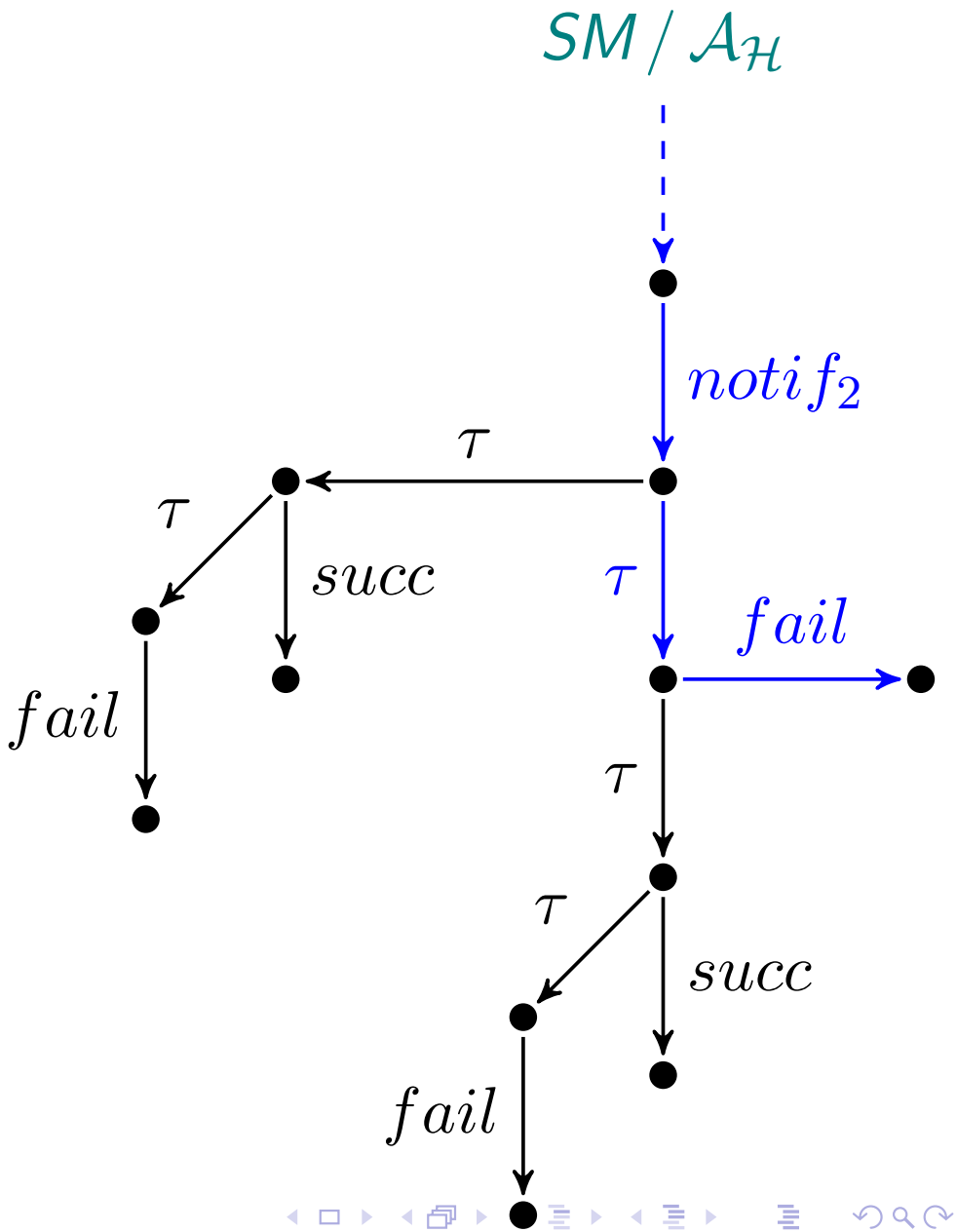
Case Study: Probabilistic Smart Contract



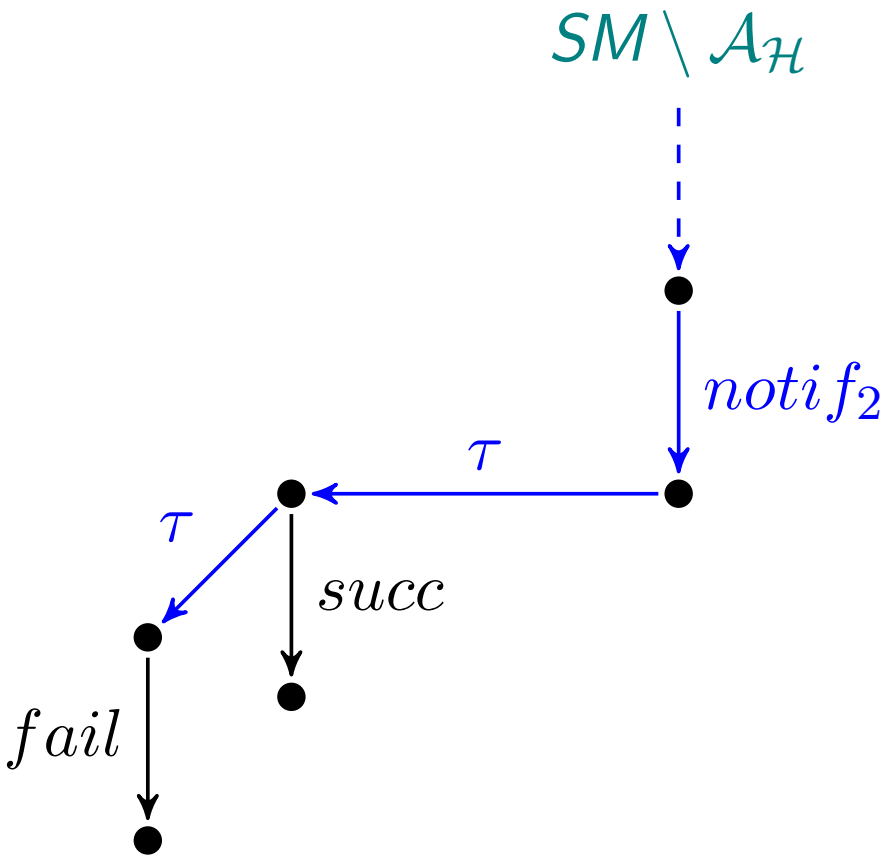


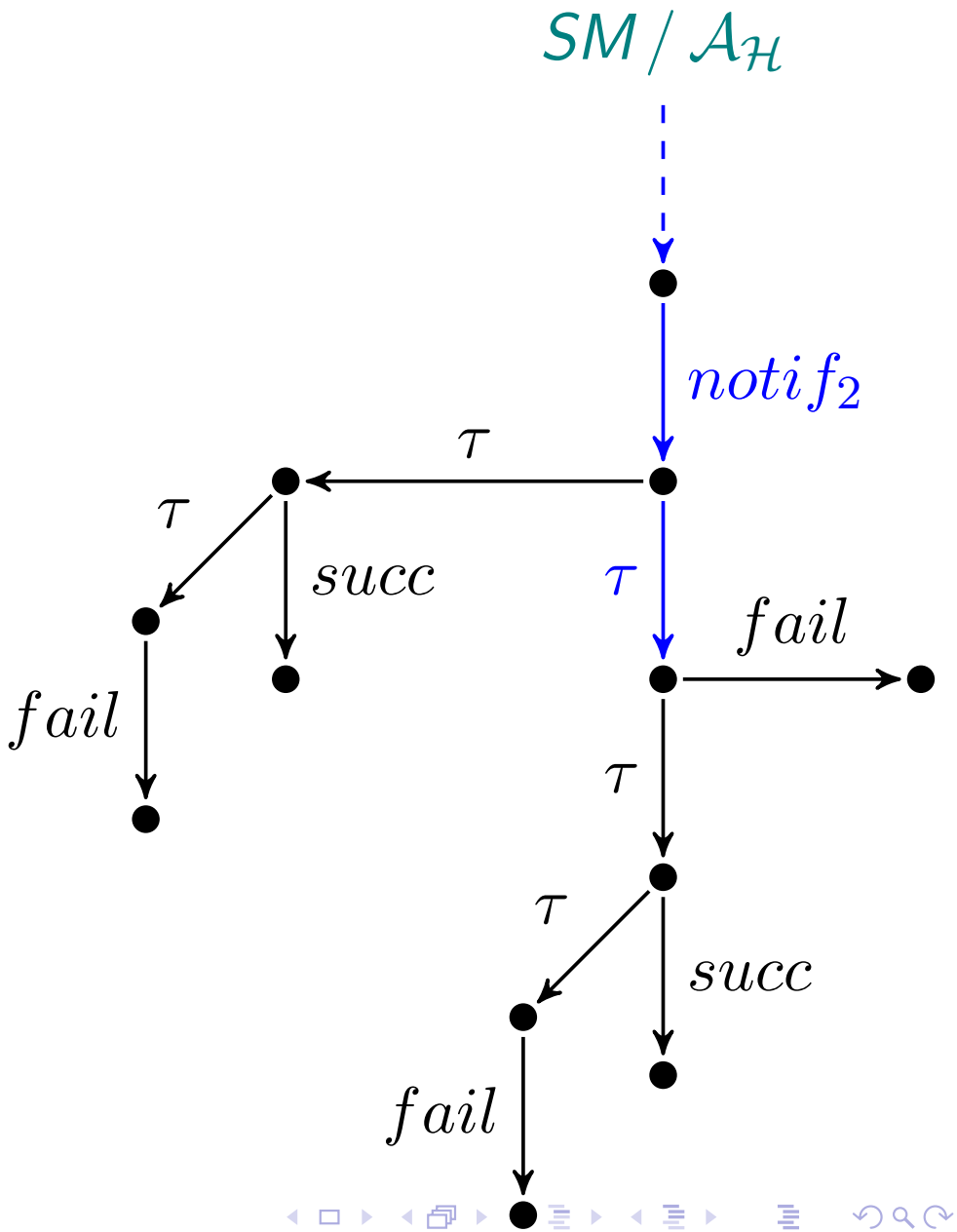
Case Study: Probabilistic Smart Contract





Case Study: Probabilistic Smart Contract





Noninterference Analysis of Stochastically Timed Reversible Systems

Noninterference in Stoch. Timed Reversible Systems

- How to analyze noninterference in stochastically timed reversible systems?

Noninterference in Stoch. Timed Reversible Systems

- How to analyze noninterference in stochastically timed reversible systems?
- Stochastic noninterference has been investigated in models where actions and rates are integrated.
  - Aldini & Bernardo (2009): variants of BSNNI and SBNDC.
  - Hillston, Marin, Piazza, & Rossi (2021): variants of $(\mathrm{P\_})\mathrm{BNDC}$.

Noninterference in Stoch. Timed Reversible Systems

- We want to study noninterference for reversible systems that feature both nondeterminism and stochastic time.
- We adopt the model of interactive Markov chains introduced by Hermanns (2002):
  - Transitions are divided into:
    - action transitions, labeled with actions.
    - rate transitions, labeled with positive real numbers.
  - Rates express exponentially distributed delays (*memoryless property*).
- We assume *maximal progress*.
- We use weak and branching bisimilarities for this model to recast a variety of noninterference properties.

Markovian Labeled Transition Systems

Definition

A *Markovian labeled transition system (MLTS)* is a triple $(\mathcal{S}, \mathcal{A}, \longrightarrow)$:

- $\mathcal{S} \neq \emptyset$ is an at most countable set of states.
- $\mathcal{A} \neq \emptyset$ is a countable set of actions
  with $\tau \in \mathcal{A}$ denoting the unobservable action.
- $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{r}}$ is a transition relation where:
  - $\longrightarrow_{\mathrm{a}} \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ is the action transition relation.
  - $\longrightarrow_{\mathrm{r}} \subseteq \mathcal{S} \times \mathbb{R}_{>0} \times \mathcal{S}$ is the rate transition relation.

Weak Markovian Bisimilarity

- Cumulative rate function: $\mathit{rate}(s, C) = \sum_{s \xrightarrow{\lambda}_{\mathrm{r}} s', s' \in C} \lambda$.
- $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ is a finite (possibly empty) sequence of $\xrightarrow{\tau}_{\mathrm{a}}$.
- $\stackrel{\hat{a}}{\Longrightarrow}_{\mathrm{a}}$ is $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ if $a = \tau$, $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \xrightarrow{a}_{\mathrm{a}} \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ otherwise.

Definition

$s_1 \approx_{\mathrm{mw}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some weak Markovian bisimulation $\mathcal{B}$.
An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a weak Markovian bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

- For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ there exists $s_2 \stackrel{\hat{a}}{\Longrightarrow} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.
- If $s_1 \not\xrightarrow{\tau}_{\mathrm{a}}$ then there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{s}_2$ such that $\bar{s}_2 \not\xrightarrow{\tau}_{\mathrm{a}}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and $\mathit{rate}(s_1, C) = \mathit{rate}(s_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.

- By ignoring the second clause we obtain $\approx_{\mathrm{w}}$.

Markovian Branching Bisimilarity

Definition

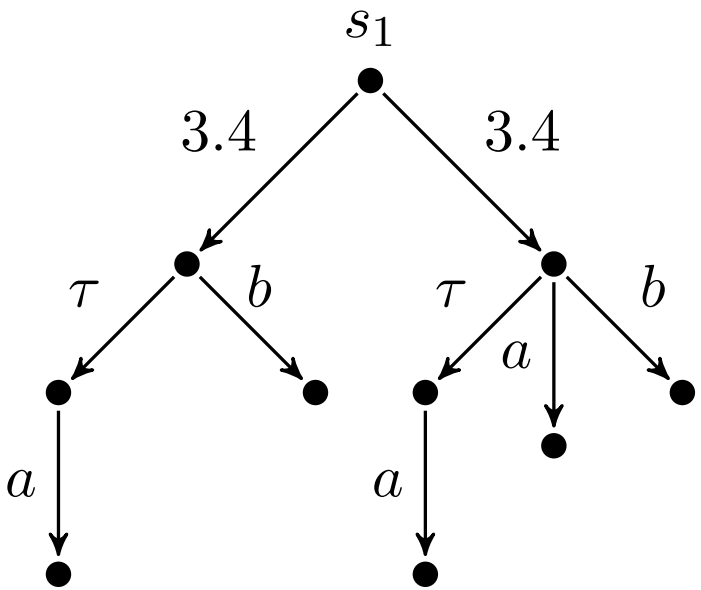
$s_1 \approx_{\mathrm{mb}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some Markovian branching bisimulation $\mathcal{B}$.
An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a Markovian branching bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

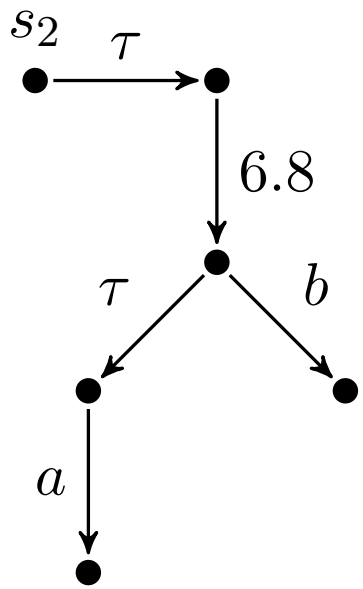
- For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$:
  - either $a = \tau$ and $(s_1', s_2) \in \mathcal{B}$;
  - or there exists $s_2 \Longrightarrow \bar{s}_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ s.t. $(s_1, \bar{s}_2) \in \mathcal{B}$ and $(s_1', s_2') \in \mathcal{B}$.
- If $s_1 \not\xrightarrow{\tau}_{\mathrm{a}}$ then there exists $s_2 \xRightarrow{\tau^*}_{\mathrm{a}} \bar{s}_2$ such that $\bar{s}_2 \not\xrightarrow{\tau}_{\mathrm{a}}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and $\mathit{rate}(s_1, C) = \mathit{rate}(s_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.

- By ignoring the second clause we obtain $\approx_{\mathrm{b}}$.

Weak and Branching Markovian Bisimlarities

- States s_1 and s_2 related by $\approx_{\mathrm{mw}}$ but distinguished by $\approx_{\mathrm{mb}}$:





Markovian Process Language

- The set of process terms $\mathbb{P}_{\mathrm{mk}}$ is the following where $a \in \mathcal{A}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:

$$
\begin{array}{rcll}
\mathbb{P}_{\mathrm{mk}} & ::= & \underline{0} & \text{terminated process} \\
& | & a \,.\, P & \text{action prefix} \\
& | & (\lambda) \,.\, P & \text{rate prefix} \\
& | & P_1 + P_2 & \text{nondeterministic choice} \\
& | & P_1 \parallel_L P_2 & \text{parallel composition} \\
& | & P \setminus L & \text{restriction} \\
& | & P \,/\, L & \text{hiding} \\
& | & K & \text{constant}
\end{array}
$$

- Overall set of actions: $\mathcal{A} := \mathcal{A}_{\mathcal{L}} \cup \mathcal{A}_{\mathcal{H}} \cup \{\tau\}$.
- Rate transitions do not synchronize.
- Restriction and hiding do not apply to rate transitions.

Markovian Noninterference Properties

Definition

Let $P \in \mathbb{P}_{\mathrm{mk}}$ and $\approx \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}$:

- $P \in \mathrm{BSNNI}_{\approx} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx} \iff$ for all $Q \in \mathbb{P}_{\mathrm{mk}}$ such that each of its prefixes belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx ((P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{SBSNNI}_{\approx} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BSNNI}_{\approx}$.
- $P \in \mathrm{P\_BNDC}_{\approx} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BNDC}_{\approx}$.
- $P \in \mathrm{SBNDC}_{\approx} \iff$ for all $P', P'' \in \mathit{reach}(P)$ such that $P' \xrightarrow{h} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx P'' \setminus \mathcal{A}_{\mathcal{H}}$.

- The process Q in BNDC cannot have any rate prefix.

Preservation and Compositionality

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{mk}}$, $\approx \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}$, *and* $\mathcal{P} \in \{\mathrm{BSNNI}_{\approx}, \mathrm{BNDC}_{\approx}, \mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx}, \mathrm{SBNDC}_{\approx}\}$.

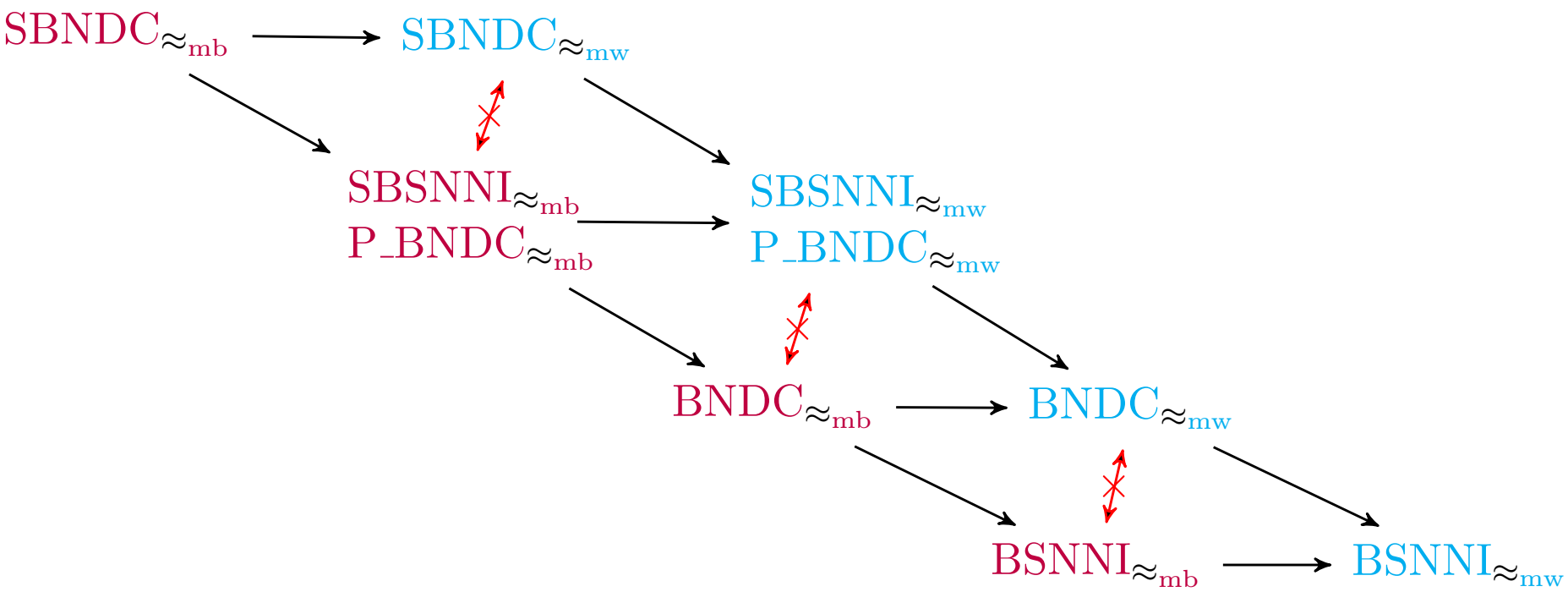
If $P_1 \approx P_2$, *then* $P_1 \in \mathcal{P} \iff P_2 \in \mathcal{P}$.

Theorem

Let $P, P_1, P_2 \in \mathbb{P}_{\mathrm{mk}}$, $\approx \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}$, $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx} \mathrm{SBNDC}_{\approx}\}$. *Then:*

1. $P \in \mathcal{P} \Longrightarrow a\,.\,P \in \mathcal{P}$ *for all* $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$.
2. $P \in \mathcal{P} \Longrightarrow (\lambda)\,.\,P \in \mathcal{P}$ *for all* $\lambda \in \mathbb{R}_{>0}$.
3. $P_1, P_2 \in \mathcal{P} \Longrightarrow P_1 \parallel_L P_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{mb}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{mb}}}\}$, $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{mw}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{mw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{mw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{mb}}}\}$.
4. $P \in \mathcal{P} \Longrightarrow P \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
5. $P \in \mathcal{P} \Longrightarrow P / L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$.

Markovian Taxonomy



- The taxonomy holds for processes without high-level cycles.
- The up-to technique for Markovian bisimilarities have the same problems as the probabilistic ones.

Relating Nondeterministic and Markovian Taxonomies

- Given a process $P \in \mathbb{P}_{\mathrm{mk,seq}}$, we can obtain its nondet. variant $nd(P)$.
- To comply with maximal progress we cut each λ in choice with a τ and then we replace each remaining $(\lambda)\,.\,P'$ with $\tau\,.\,P'$.

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{mk,seq}}$. *Then:*

- $P_1 \approx_{\mathrm{mw}} P_2 \Longrightarrow nd(P_1) \approx_{\mathrm{w}} nd(P_2)$.
- $P_1 \approx_{\mathrm{mb}} P_2 \Longrightarrow nd(P_1) \approx_{\mathrm{b}} nd(P_2)$.

Relating Nondeterministic and Markovian Taxonomies

- A consequence is that if a process P is secure under a Markovian noninterference property, then $nd(P)$ is secure under the corresponding nondeterministic property.

Corollary

Let $P \in \mathbb{P}_{\mathrm{mk,seq}}, \approx_{\mathrm{mk}} \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}, \approx_{\mathrm{nd}} \in \{\approx_{\mathrm{w}}, \approx_{\mathrm{b}}\}$,
$\mathcal{P}_{\mathrm{mk}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{mk}}}, \mathrm{BNDC}_{\approx_{\mathrm{mk}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{mk}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{mk}}}, \mathrm{SBNDC}_{\approx_{\mathrm{mk}}}\}$,
$\mathcal{P}_{\mathrm{nd}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBNDC}_{\approx_{\mathrm{nd}}}\}$.
Then:

$$P \in \mathcal{P}_{\mathrm{mk}} \Longrightarrow nd(P) \in \mathcal{P}_{\mathrm{nd}}$$

- This means that our results extend the nondeterministic taxonomy.

Relating Probabilistic and Markovian Taxonomies

- Given a process $P \in \mathbb{P}_{\mathrm{mk,alt,seq}}$, we can obtain its prob. variant $\mathit{pr}(P)$ by replacing $\sum_{i \in I} (\lambda_i) \,.\, P_i$ with $\bigoplus_{i \in I} [p_i] P_i$, where $p_i = \lambda_i / \sum_{j \in I} \lambda_j$.

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{mk,alt,seq}}$. *Then:*

- $P_1 \approx_{\mathrm{mw}} P_2 \Longrightarrow \mathit{pr}(P_1) \approx_{\mathrm{pw}} \mathit{pr}(P_2)$.
- $P_1 \approx_{\mathrm{mb}} P_2 \Longrightarrow \mathit{pr}(P_1) \approx_{\mathrm{pb}} \mathit{pr}(P_2)$.

Relating Probabilistic and Markovian Taxonomies

- A consequence is that if a process P is secure under a Markovian noninterference property, then $pr(P)$ is secure under the corresponding probabilistic property.

Corollary

Let $P \in \mathbb{P}_{\mathrm{mk,alt,seq}}, \approx_{\mathrm{mk}} \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}, \approx_{\mathrm{pr}} \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$,
$\mathcal{P}_{\mathrm{mk}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{mk}}}, \mathrm{BNDC}_{\approx_{\mathrm{mk}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{mk}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{mk}}}, \mathrm{SBNDC}_{\approx_{\mathrm{mk}}}\}$,
$\mathcal{P}_{\mathrm{pr}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{pr}}}, \mathrm{BNDC}_{\approx_{\mathrm{pr}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{pr}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{pr}}}, \mathrm{SBNDC}_{\approx_{\mathrm{pr}}}\}$.
Then:

$$P \in \mathcal{P}_{\mathrm{mk}} \Longrightarrow pr(P) \in \mathcal{P}_{\mathrm{pr}}$$

- This means that our results also extend the probabilistic taxonomy.

Weak Markovian Back-and-Forth Bisimilarity

Definition

$s_1 \approx_{\mathrm{mbf}} s_2$ iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak Markovian back-and-forth bisimulation $\mathcal{B}$.

An equivalence relation $\mathcal{B}$ over $\mathcal{U}$ is a weak Markovian back-and-forth bisimulation iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:

- For each $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ with $(\rho_1', \rho_2') \in \mathcal{B}$.
- For each $\rho_1' \xrightarrow{a}_{\mathrm{a}} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ with $(\rho_1', \rho_2') \in \mathcal{B}$.
- For each $\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_1'$ with $\rho_1' \not\xrightarrow{\tau}_{\mathrm{a}}$ there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_2'$ with $\rho_2' \not\xrightarrow{\tau}_{\mathrm{a}}$ such that $(\rho_1', \rho_2') \in \mathcal{B}$ and $\mathit{rate}(\rho_1', C) = \mathit{rate}(\rho_2', C)$ for all $C \in \mathcal{U}/\mathcal{B}$.
- For each $\rho_1' \xrightarrow{\lambda_1}_{\mathrm{r}} \rho_1$ with $\rho_1' \not\xrightarrow{\tau}_{\mathrm{a}}$ there exists $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{\rho}_2' \xrightarrow{\lambda_2}_{\mathrm{r}} \bar{\rho}_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_2$ with $\bar{\rho}_2' \not\xrightarrow{\tau}_{\mathrm{a}}$ such that $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$, $(\rho_1', \bar{\rho}_2') \in \mathcal{B}$, and $(\rho_1', \rho_2') \in \mathcal{B}$.

Weak Markovian Back-and-Forth Bisimilarity

- As in the nondet. and prob. cases, weak Markovian back-and-forth bisimilarity coincides with Markovian branching bisimilarity.

Theorem

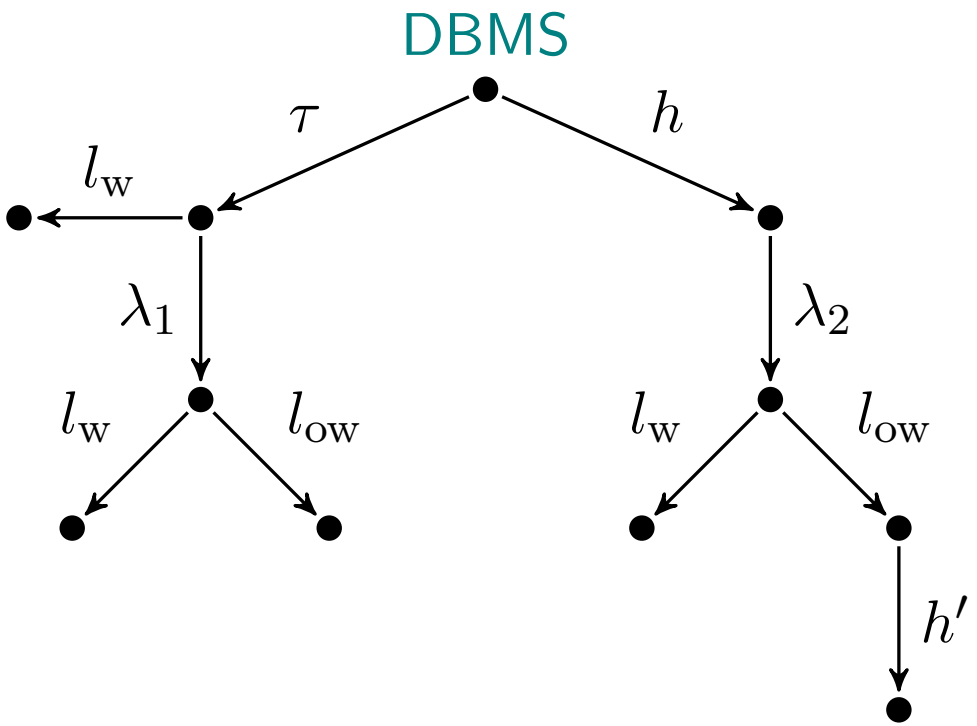
$$s_1 \approx_{\mathrm{mbf}} s_2 \textit{ iff } s_1 \approx_{\mathrm{mb}} s_2.$$

- Again, all of our results for Markovian branching-bisimulation-based properties can be extended to Markovian reversible systems.

DBMS and Obfuscation Mechanisms

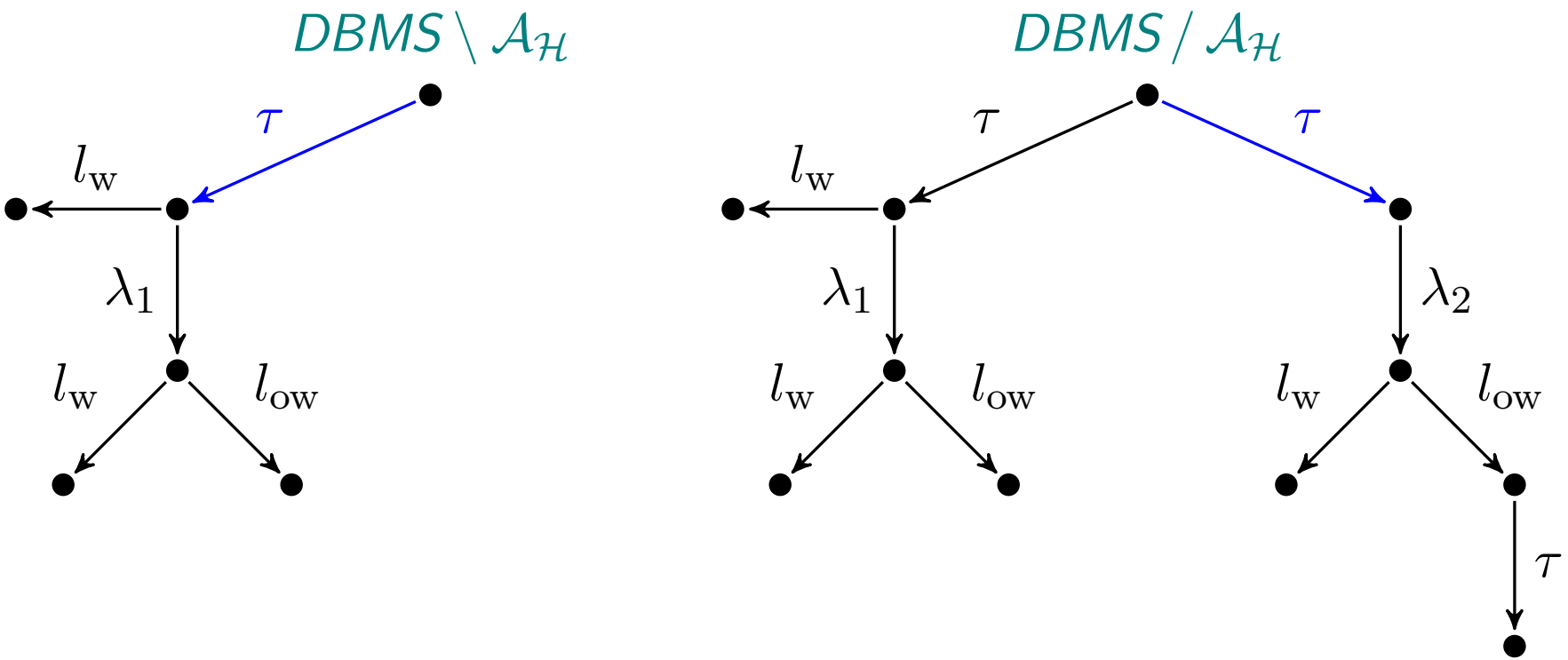
- We resume the DBMS example.
- Data written on the DBMS can be fed to a machine learning module.
- An obfuscation mechanism is introduced to ensure data privacy.
- Rates indicate the time spent by the DBMS before the obfuscation.
- We consider the following actions:
  - h, h' expressing the interaction with the machine learning module.
  - l_{w}expressing the execution of a write transaction.
  - l_{ow} expressing an obfuscated write transaction.

DBMS and Obfuscation Mechanisms



DBMS and Obfuscation Mechanisms

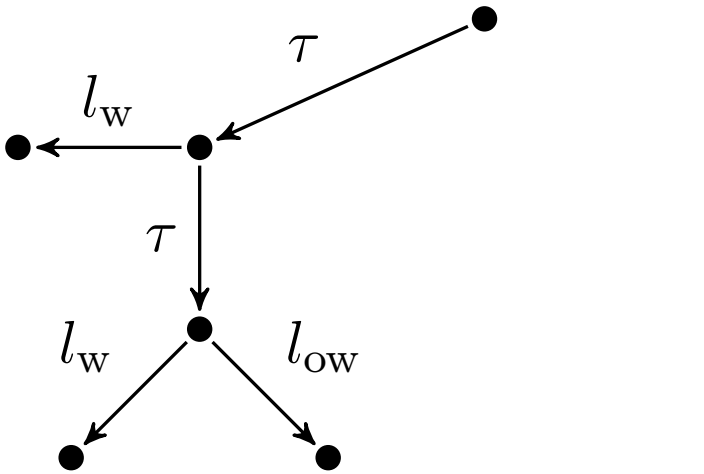
- The processes DBMS$\backslash\mathcal{A}_{\mathcal{H}}$ and DBMS $/\,\mathcal{A}_{\mathcal{H}}$ are not $\approx_{\mathrm{mw}/\mathrm{mb}}$:



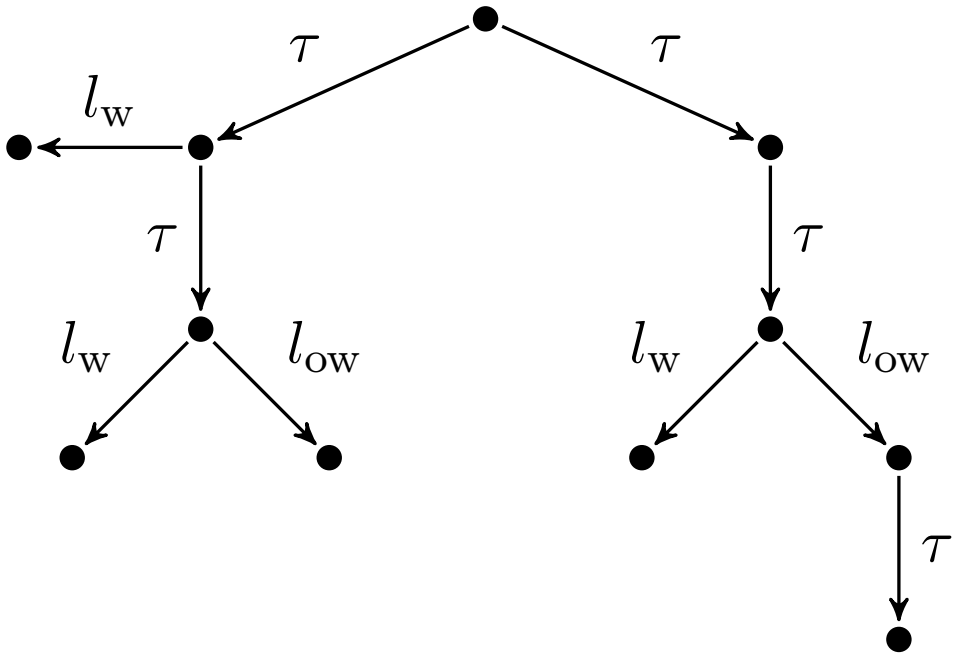
DBMS and Obfuscation Mechanisms

- But their nondeterministic variants are $\approx_{\mathrm{w}/\mathrm{b}}$:

$nd(DBMS) \setminus \mathcal{A}_{\mathcal{H}}$



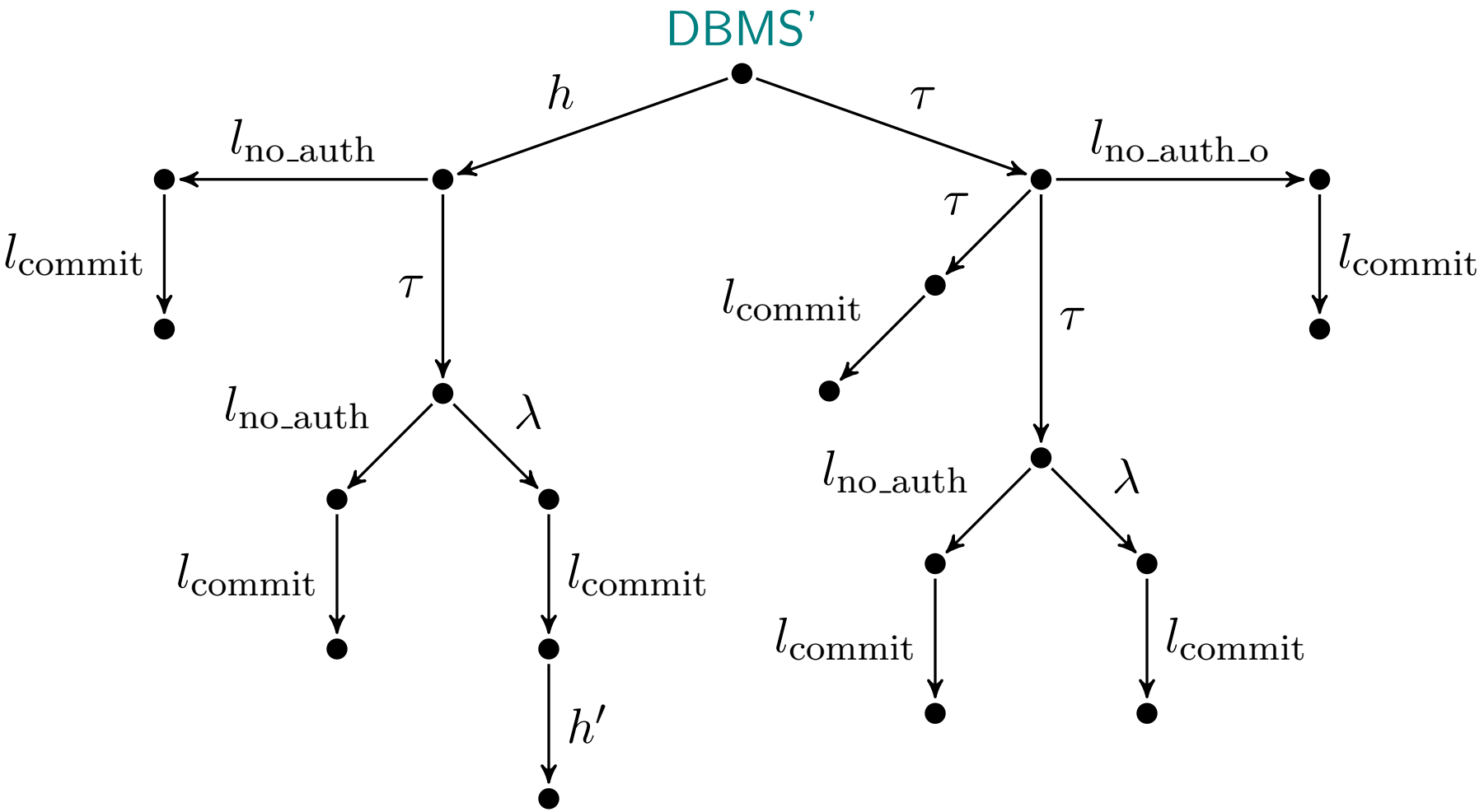
$nd(DBMS) \,/\, \mathcal{A}_{\mathcal{H}}$



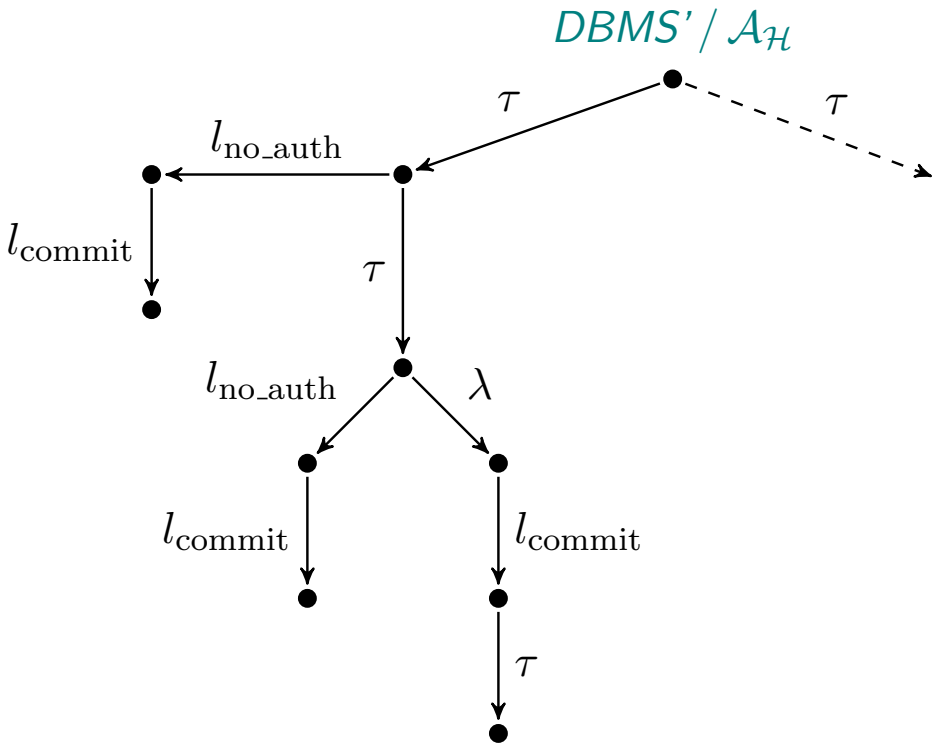
DBMS and Obfuscation Mechanisms

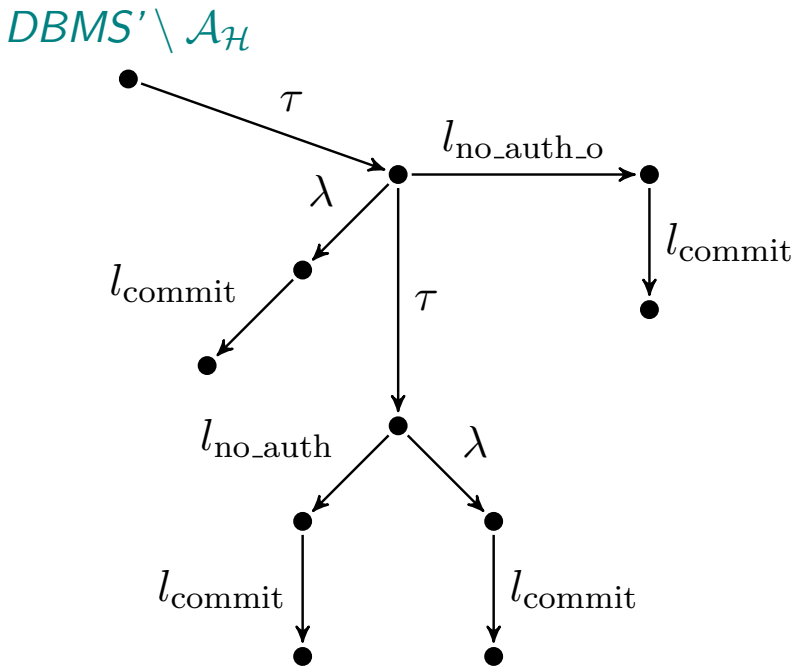
- We move to a more sophisticated case where user can explicitly authorize the use of their data.
- We add the following actions:
  - $l_{\text{no\_auth}}$ expressing that the users do not authorize the use of their data.
  - $l_{\text{no\_auth}}$ expressing that the users do not authorize the obfuscation of their data.
  - l_{commit} expressing the execution of the transaction.

DBMS and Obfuscation Mechanisms

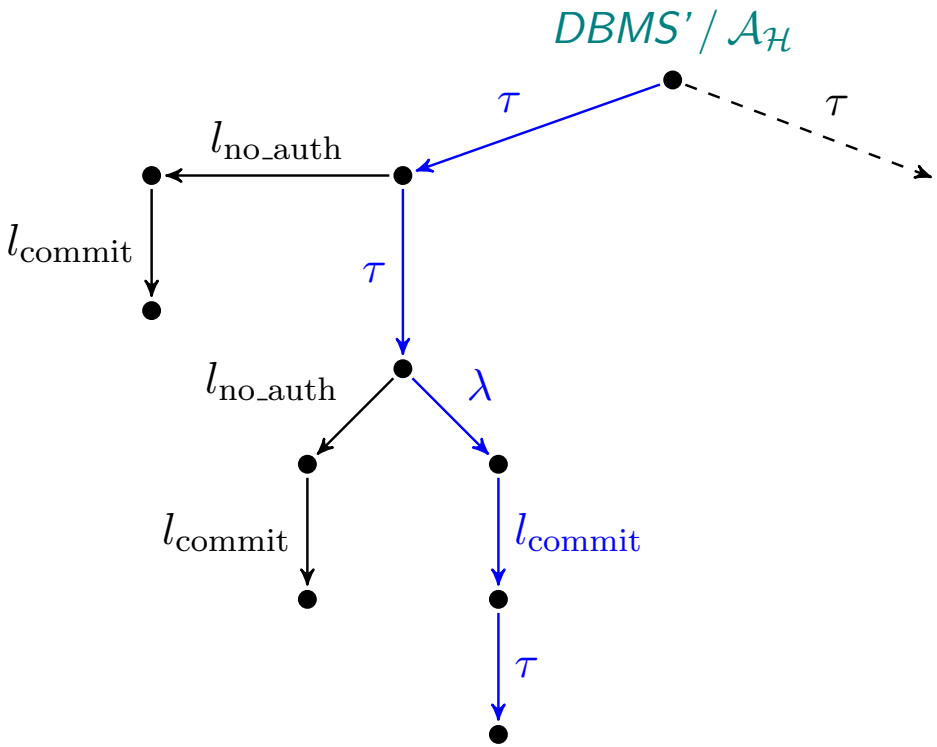


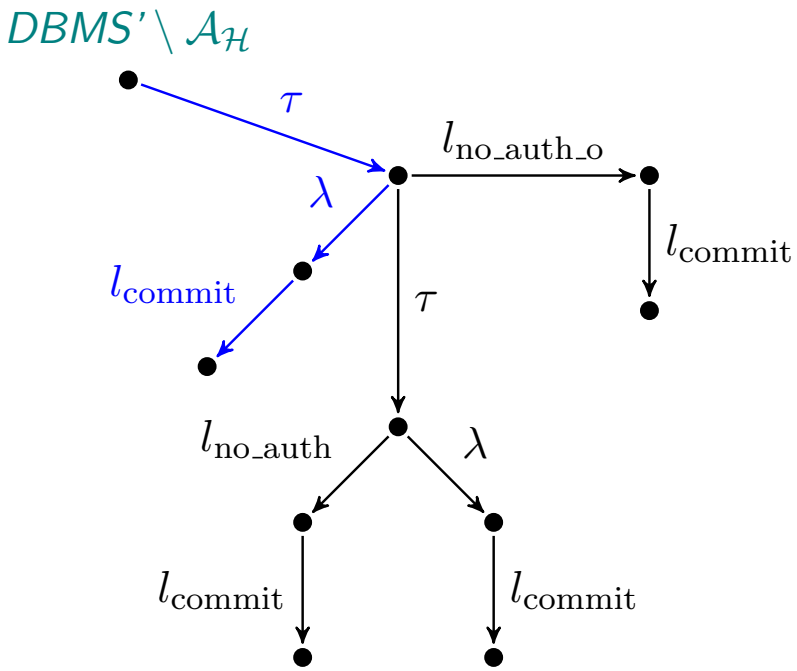
DBMS and Obfuscation Mechanisms



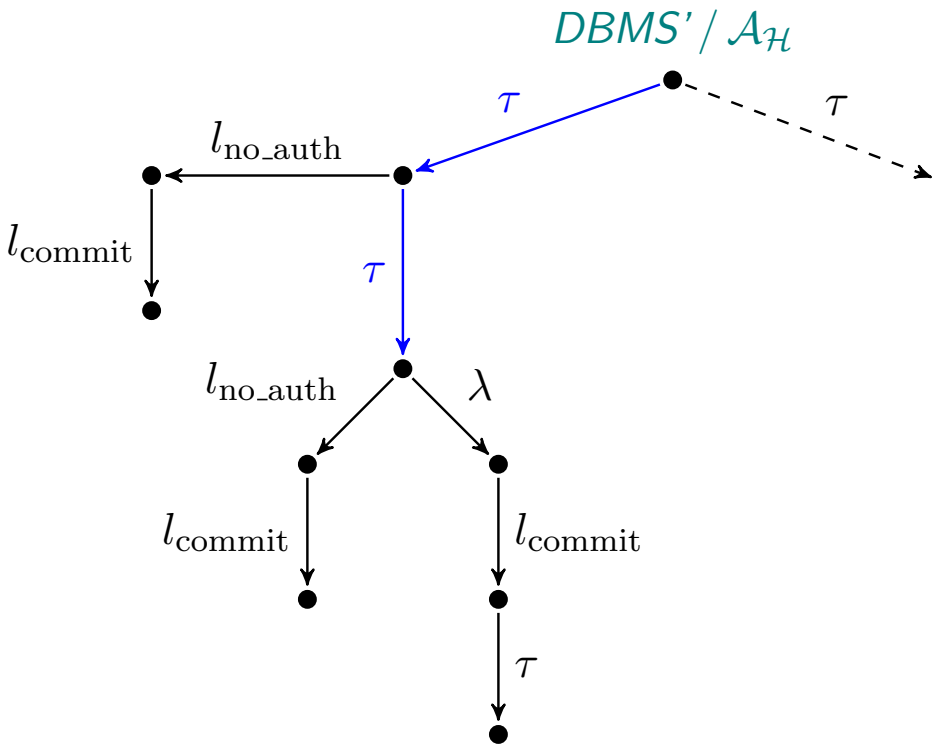


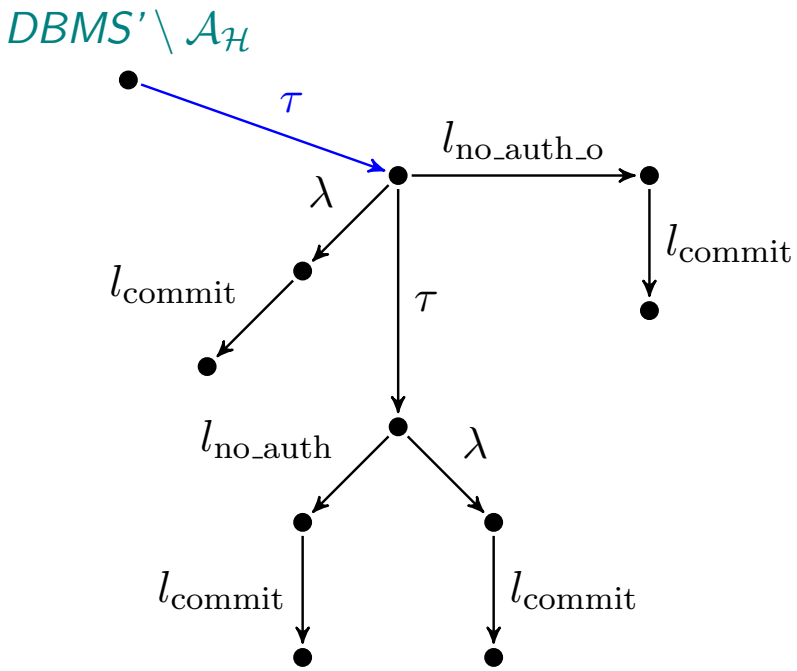
DBMS and Obfuscation Mechanisms





DBMS and Obfuscation Mechanisms





Noninterference Analysis of Deterministically Timed Reversible Systems

Noninterference in Determ. Timed Reversible Systems

- How to analyze noninterference in deterministically timed reversible systems?

Noninterference in Determ. Timed Reversible Systems

- How to analyze noninterference in deterministically timed reversible systems?
- Timed noninterference has been investigated by Focardi, Gorrieri & Martinelli (2000) for variants of BSNNI, BNDC, and SBSNNI.

Noninterference in Determ. Timed Reversible Systems

- We want to study noninterference for reversible systems that feature both nondeterminism and deterministic time.
- We adopted the model of Moller and Tofts (1990):
  - Transitions are divided into:
    - action transitions, labeled with actions.
    - delay transitions, labeled with natural numbers.
  - Delay transitions respect time additivity and time determinism.
- We assume *maximal progress* and *eagerness* for action transitions.
- We use weak and branching bisimilarities for this model to recast a variety of noninterference properties.

Timed Labeled Transition Systems

Definition

A *Timed labeled transition system (TLTS)* is a triple $(\mathcal{S}, \mathcal{A}, \longrightarrow)$:

- $\mathcal{S} \neq \emptyset$ is an at most countable set of states.
- $\mathcal{A} \neq \emptyset$ is a countable set of actions
  with $\tau \in \mathcal{A}$ denoting the unobservable action.
- $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{t}}$ is a transition relation where:
  - $\longrightarrow_{\mathrm{a}} \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ is the action transition relation.
  - $\longrightarrow_{\mathrm{t}} \subseteq \mathcal{S} \times \mathbb{N}_{>0} \times \mathcal{S}$ is the timed transition relation.

Weak Timed Bisimilarity

- $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ is a finite (possibly empty) sequence of $\stackrel{\tau}{\longrightarrow}_{\mathrm{a}}$.
- $\stackrel{\hat{a}}{\Longrightarrow}_{\mathrm{a}}$ is $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ if $a = \tau$, $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \stackrel{a}{\longrightarrow}_{\mathrm{a}} \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ otherwise.
- $\stackrel{t}{\Longrightarrow}_{\mathrm{t}}$ is $\stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \stackrel{t_1}{\longrightarrow}_{\mathrm{t}} \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \cdots \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \stackrel{t_n}{\longrightarrow}_{\mathrm{t}} \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}}$ with $\sum_{1 \leq i \leq n} t_i = t$.

Definition

$s_1 \approx_{\mathrm{tw}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some weak timed bisimulation $\mathcal{B}$.
An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a weak timed bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

- For each $s_1 \stackrel{a}{\longrightarrow}_{\mathrm{a}} s_1'$ there exists $s_2 \stackrel{\hat{a}}{\Longrightarrow} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.
- If $s_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ then there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{s}_2$ such that $\bar{s}_2 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and for each $s_1 \stackrel{t}{\longrightarrow}_{\mathrm{t}} s_1'$ there exists $s_2 \stackrel{t}{\Longrightarrow}_{\mathrm{t}} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.

- By ignoring the second clause we obtain $\approx_{\mathrm{w}}$.

Timed Branching Bisimilarity

Definition

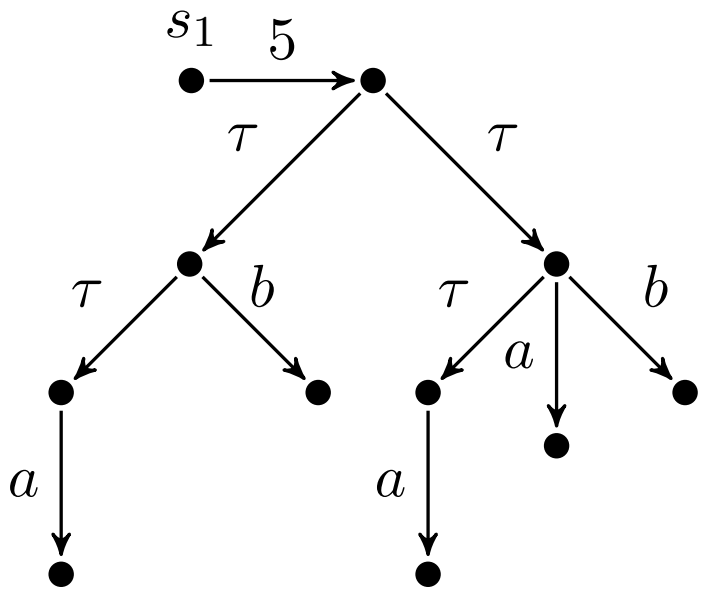
$s_1 \approx_{\mathrm{tb}} s_2$ iff $(s_1, s_2) \in \mathcal{B}$ for some timed branching bisimulation $\mathcal{B}$.
An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a timed branching bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:

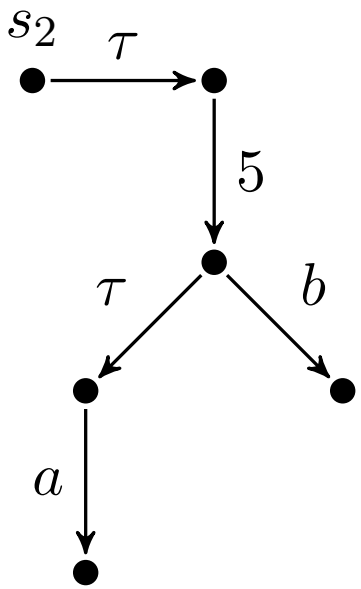
- For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$:
  - either $a = \tau$ and $(s_1', s_2) \in \mathcal{B}$;
  - or there exists $s_2 \xRightarrow{\tau^*}_{\mathrm{a}} \bar{s}_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ s.t. $(s_1, \bar{s}_2) \in \mathcal{B}$ and $(s_1', s_2') \in \mathcal{B}$.
- If $s_1 \not\xrightarrow{\tau}_{\mathrm{a}}$ then there exists $s_2 \xRightarrow{\tau^*}_{\mathrm{a}} \bar{s}_2$ such that $\bar{s}_2 \not\xrightarrow{\tau}_{\mathrm{a}}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and for each $s_1 \xrightarrow{t}_{\mathrm{t}} s_1'$ there exists $s_2 \xRightarrow{t}_{\mathrm{t}} s_2'$ s.t. $(s_1', s_2') \in \mathcal{B}$.

- By ignoring the second clause we obtain $\approx_{\mathrm{b}}$.

Weak and Branching Timed Bisimlarities

- States s_1 and s_2 related by $\approx_{\mathrm{tw}}$ but distinguished by $\approx_{\mathrm{tb}}$:





Timed Process Language

- The set of process terms $\mathbb{P}_{\mathrm{dt}}$ is the following where $a \in \mathcal{A}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:

$$
\begin{array}{rcll}
\mathbb{P}_{\mathrm{dt}} & ::= & \underline{0} & \text{terminated process} \\
& | & a \,.\, P & \text{action prefix} \\
& | & (t) \,.\, P & \text{delay prefix} \\
& | & P_1 + P_2 & \text{nondeterministic choice} \\
& | & P_1 \parallel_L P_2 & \text{parallel composition} \\
& | & P \setminus L & \text{restriction} \\
& | & P \,/\, L & \text{hiding}
\end{array}
$$

- Overall set of actions: $\mathcal{A} := \mathcal{A}_{\mathcal{L}} \cup \mathcal{A}_{\mathcal{H}} \cup \{\tau\}$.
- Delay transitions must synchronize.
- Restriction and hiding do not apply to delay transitions.

Timed Noninterference Properties

Definition

Let $P \in \mathbb{P}_{\mathrm{dt}}$ and $\approx \in \{\approx_{\mathrm{tw}}, \approx_{\mathrm{tb}}\}$:

- $P \in \mathrm{BSNNI}_{\approx} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx} \iff$ for all $Q \in \mathbb{P}_{\mathrm{dt}}$ such that each of its actions belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx ((P \,\|_L\, Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{SBSNNI}_{\approx} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BSNNI}_{\approx}$.
- $P \in \mathrm{P\_BNDC}_{\approx} \iff$ for all $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BNDC}_{\approx}$.
- $P \in \mathrm{SBNDC}_{\approx} \iff$ for all $P', P'' \in \mathit{reach}(P)$ such that $P' \xrightarrow{h} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx P'' \setminus \mathcal{A}_{\mathcal{H}}$.

- The process Q in BNDC must allow to pass the same time as P.

Preservation and Compositionality

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{dt}}$, $\approx \in \{\approx_{\mathrm{tw}}, \approx_{\mathrm{tb}}\}$, *and* $\mathcal{P} \in \{\mathrm{BSNNI}_{\approx}, \mathrm{BNDC}_{\approx}, \mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx}, \mathrm{SBNDC}_{\approx}\}$.

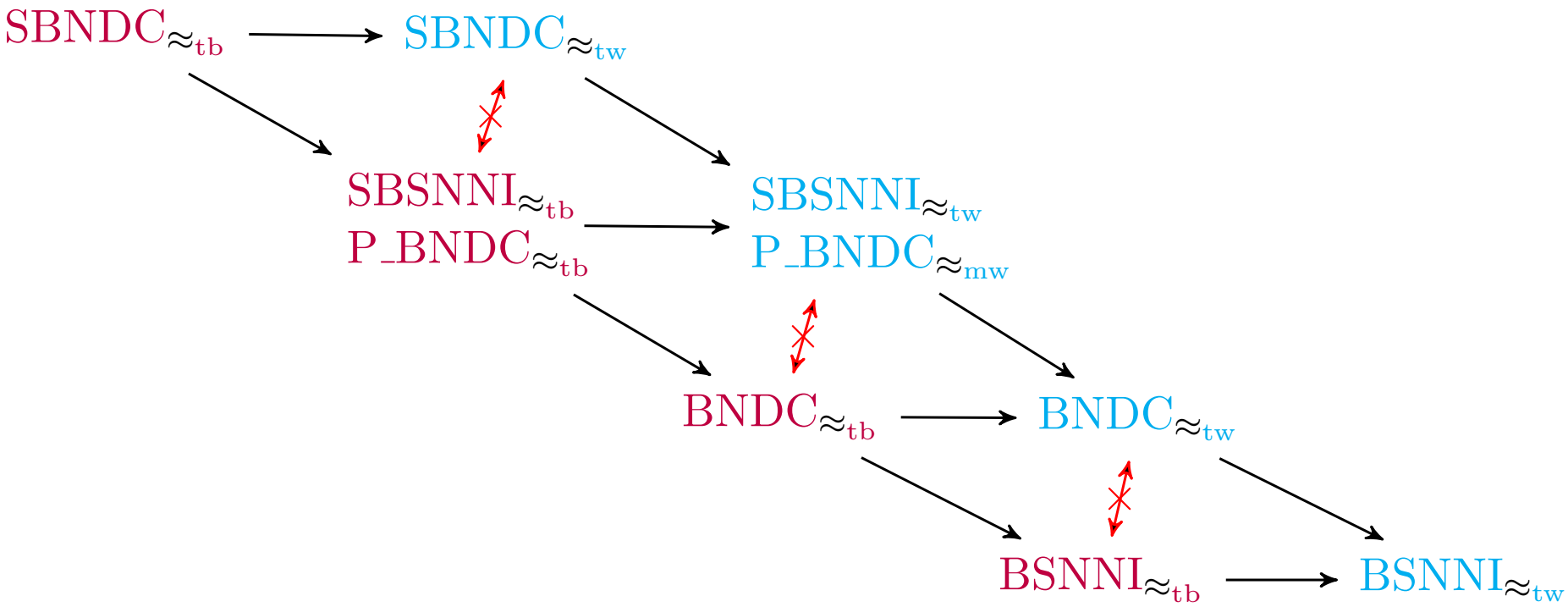
If $P_1 \approx P_2$, *then* $P_1 \in \mathcal{P} \iff P_2 \in \mathcal{P}$.

Theorem

Let $P, P_1, P_2 \in \mathbb{P}_{\mathrm{dt}}$, $\approx \in \{\approx_{\mathrm{tw}}, \approx_{\mathrm{tb}}\}$, $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx} \mathrm{SBNDC}_{\approx}\}$. *Then:*

1. $P \in \mathcal{P} \Longrightarrow a \,.\, P \in \mathcal{P}$ *for all* $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$.
2. $P \in \mathcal{P} \Longrightarrow (t) \,.\, P \in \mathcal{P}$ *for all* $t \in \mathbb{N}_{>0}$.
3. $P_1, P_2 \in \mathcal{P} \Longrightarrow P_1 \parallel_L P_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{tb}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{tb}}}\}$, $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_{\mathrm{tw}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{tw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{tw}}}, \mathrm{SBNDC}_{\approx_{\mathrm{tb}}}\}$.
4. $P \in \mathcal{P} \Longrightarrow P \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
5. $P \in \mathcal{P} \Longrightarrow P \,/\, L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_{\mathcal{L}}$.

Timed Taxonomy



Relating Nondeterministic and Timed Taxonomies

- Given a process $P \in \mathbb{P}_{\mathrm{dt,seq}}$, we can obtain its nondet. variant $\mathit{nd}(P)$.
- To comply with maximal progress we cut each t in choice with a τ and then we replace each remaining $(t)\,.\,P'$ with $\tau\,.\,P'$.

Theorem

Let $P_1, P_2 \in \mathbb{P}_{\mathrm{dt,seq}}$. *Then:*

- $P_1 \approx_{\mathrm{tw}} P_2 \Longrightarrow \mathit{nd}(P_1) \approx_{\mathrm{w}} \mathit{nd}(P_2)$.
- $P_1 \approx_{\mathrm{tb}} P_2 \Longrightarrow \mathit{nd}(P_1) \approx_{\mathrm{b}} \mathit{nd}(P_2)$.

Relating Nondeterministic and Timed Taxonomies

- A consequence is that if a process P is secure under a timed noninterference property, then $nd(P)$ is secure under the corresponding nondeterministic property.

Corollary

Let $P \in \mathbb{P}_{\mathrm{dt,seq}}, \approx_{\mathrm{dt}} \in \{\approx_{\mathrm{tw}}, \approx_{\mathrm{tb}}\}, \approx_{\mathrm{nd}} \in \{\approx_{\mathrm{w}}, \approx_{\mathrm{b}}\}$,
$\mathcal{P}_{\mathrm{dt}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{dt}}}, \mathrm{BNDC}_{\approx_{\mathrm{dt}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{dt}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{dt}}}, \mathrm{SBNDC}_{\approx_{\mathrm{dt}}}\}$,
$\mathcal{P}_{\mathrm{nd}} \in \{\mathrm{BSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBSNNI}_{\approx_{\mathrm{nd}}}, \mathrm{P\_BNDC}_{\approx_{\mathrm{nd}}}, \mathrm{SBNDC}_{\approx_{\mathrm{nd}}}\}$.
Then:

$$P \in \mathcal{P}_{\mathrm{dt}} \Longrightarrow nd(P) \in \mathcal{P}_{\mathrm{nd}}$$

- This means that our results extend the nondeterministic taxonomy.

Weak Timed Back-and-Forth Bisimilarity

Definition

$s_1 \approx_{\mathrm{tbf}} s_2$ iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak timed back-and-forth bisimulation $\mathcal{B}$.

An equivalence relation $\mathcal{B}$ over $\mathcal{U}$ is a weak timed back-and-forth bisimulation iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:

- For each $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ with $(\rho_1', \rho_2') \in \mathcal{B}$.
- For each $\rho_1' \xrightarrow{a}_{\mathrm{a}} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ with $(\rho_1', \rho_2') \in \mathcal{B}$.
- For each $\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_1'$ with $\rho_1' \not\xrightarrow{\tau}_{\mathrm{a}}$ there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_2'$ with $\rho_2' \not\xrightarrow{\tau}_{\mathrm{a}}$ such that $(\rho_1', \rho_2') \in \mathcal{B}$ and for each $\rho_1' \xrightarrow{t}_{\mathrm{t}} \rho_1''$ there exists $\rho_2' \stackrel{t}{\Longrightarrow}_{\mathrm{t}} \rho_2''$ with $(\rho_1'', \rho_2'') \in \mathcal{B}$.
- For each $\rho_1' \xrightarrow{t}_{\mathrm{t}} \rho_1$ with $\rho_1' \not\xrightarrow{\tau}_{\mathrm{a}}$ there exists $\rho_2' \stackrel{t}{\Longrightarrow}_{\mathrm{t}} \rho_2$ with $\rho_2' \not\xrightarrow{\tau}_{\mathrm{a}}$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.

Weak Timed Back-and-Forth Bisimilarity

- As in the previous cases, weak timed back-and-forth bisimilarity coincides with timed branching bisimilarity.

Theorem

$$s_1 \approx_{\mathrm{tbf}} s_2 \textit{ iff } s_1 \approx_{\mathrm{tb}} s_2.$$

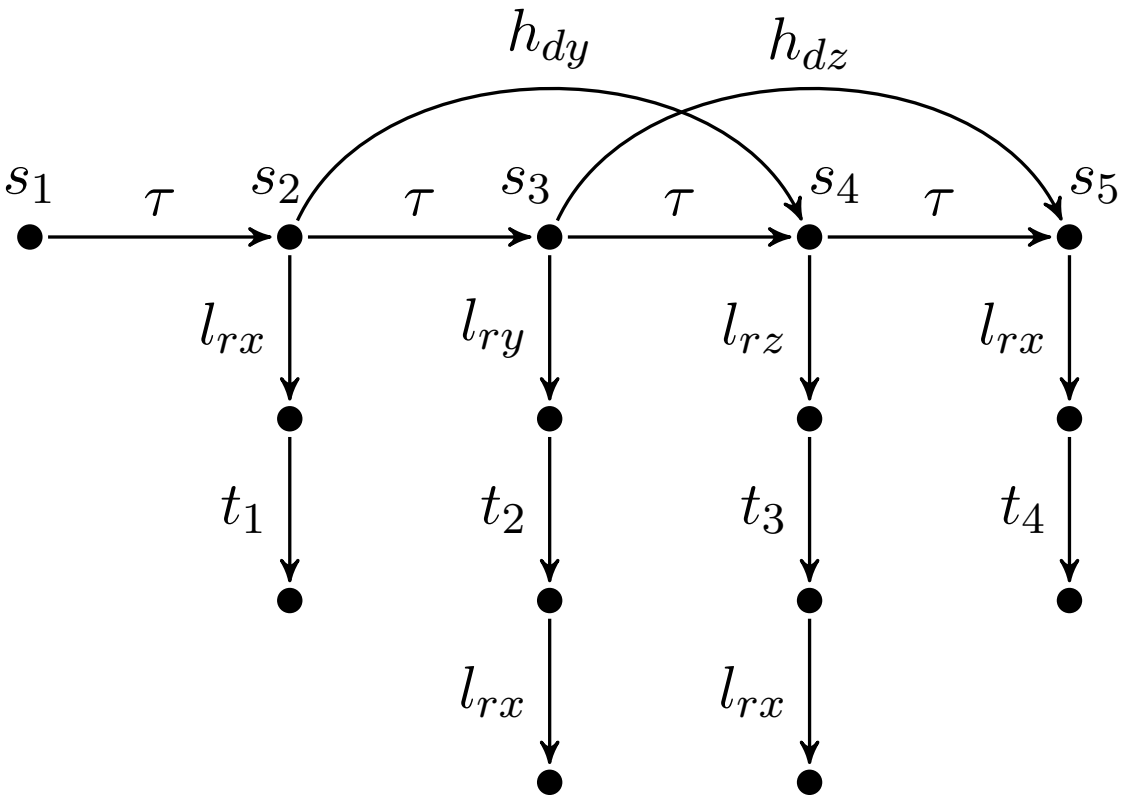
- Again, all of our results for timed branching-bisimulation-based properties can be extended to timed reversible systems.

DBMS Example

- We recover the DBMS example adding priorities for certain actions.
- A concurrent system where users can read different values: x, y, z.
- High-level users can delete values and this operation should be transparent, even in the case of some form of recovery.
- We consider the following actions:
  - l_{rv} representing the reading of value v.
  - h_{dv} representing the deletion of value v.

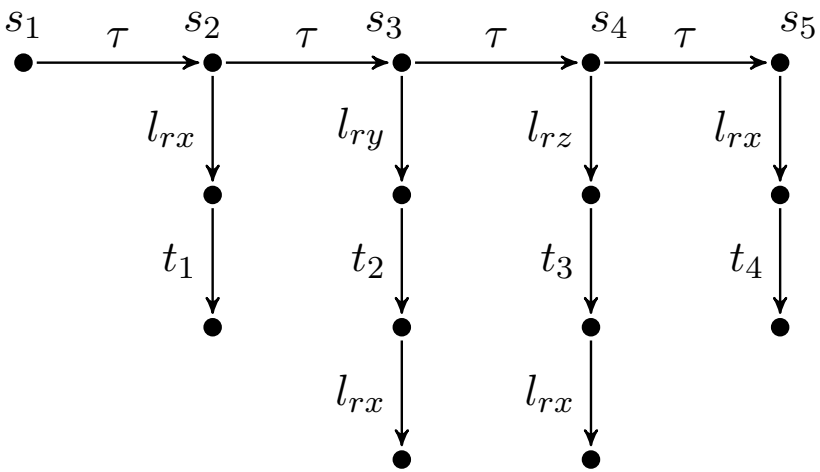
DBMS Example

DBMS

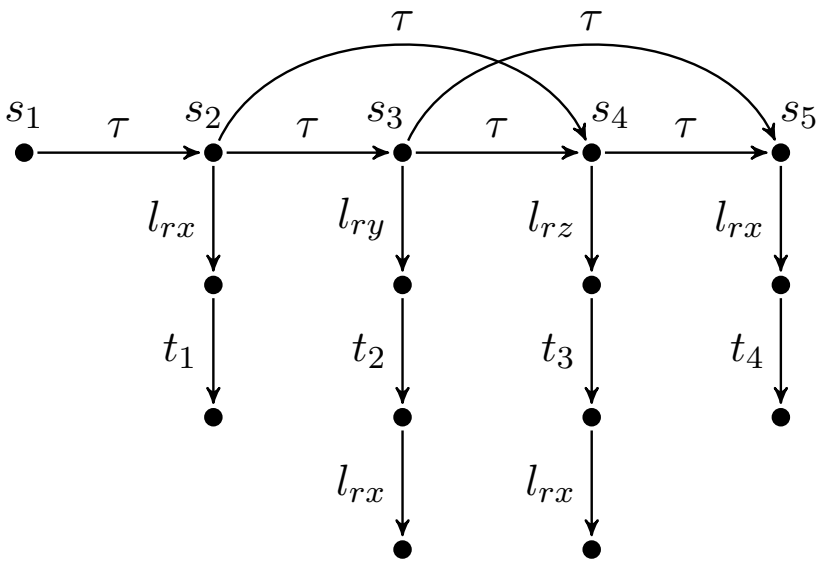


DBMS Example

$DBMS \setminus \mathcal{A}_{\mathcal{H}}$

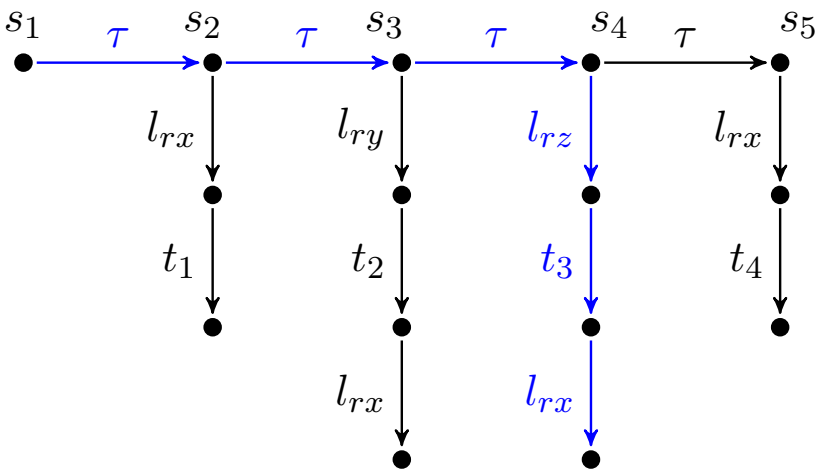


$DBMS \,/\, \mathcal{A}_{\mathcal{H}}$

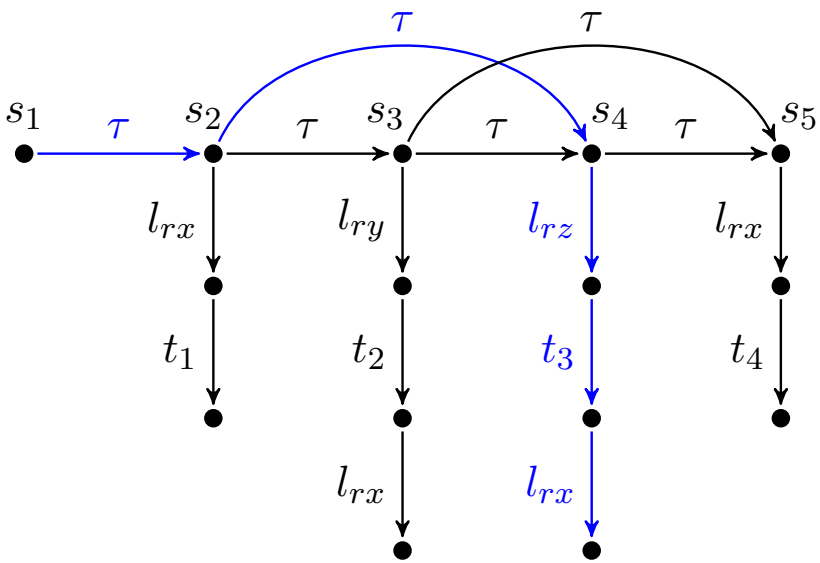


DBMS Example

$DBMS \setminus \mathcal{A}_{\mathcal{H}}$

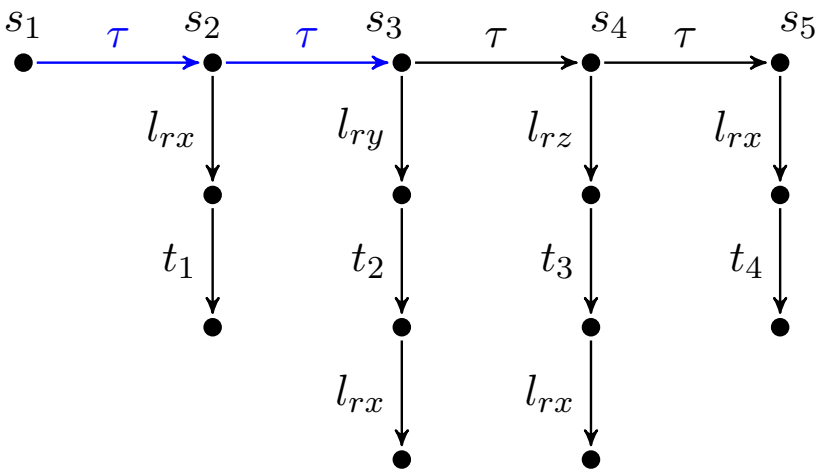


$DBMS \,/\, \mathcal{A}_{\mathcal{H}}$

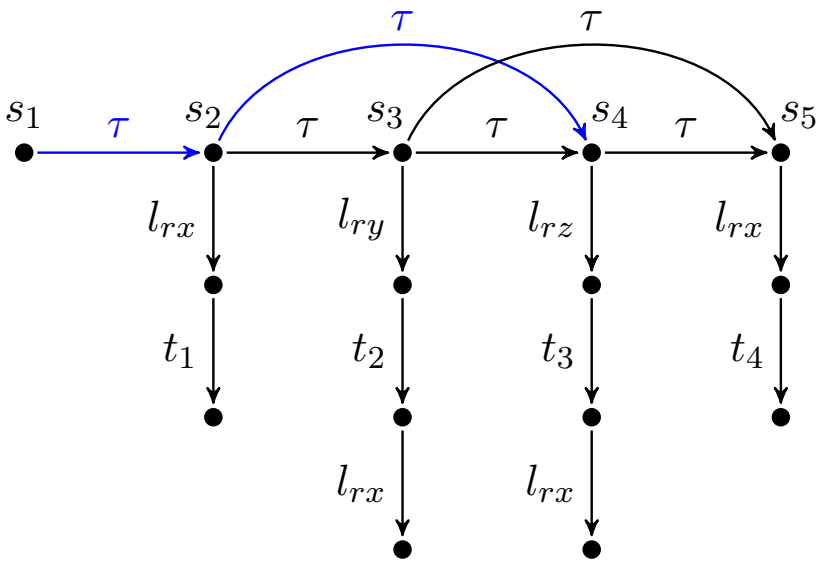


DBMS Example

$DBMS \setminus \mathcal{A}_{\mathcal{H}}$



$DBMS \,/\, \mathcal{A}_{\mathcal{H}}$



Conclusions and Future Work

- A comprehensive information-flow theory of irreversible ($\approx_{\mathrm{w}}$) and reversible ($\approx_{\mathrm{b}}$) systems encompassing nondeterminism and probabilities / stochastic time / deterministic time.
- We have real-world use case examples based on DBMSs and probabilistic smart contracts that prove the adequacy of our approach when dealing with noninterference and reversibility.
- *Extend the study of deterministically timed noninterference for reversible systems with recursion.*
- *We are working on implementing noninterference in the tool CADP for an extensive validation of Algorand.*