Weak Bisimulation via Generalized Parameterized Coinduction

Yannick Zakowski

Chung Kil-Hur

Paul He

Steve Zdancewic

Penn University of Pennsylvania

SEOUL NATIONAL UNIVERSITY

Weak Bisimulation via Generalized Parameterized Coinduction

1. An extension to paco:
   $\longrightarrow$ a generic library to support coinductive reasoning in Coq

2. Reasoning specifically about weak bisimulation:
   $\longrightarrow$ "Parameterized weak bisimulations"

Generalized Parameterized Coinduction

Coinductive Lists of Naturals

$$
\begin{aligned}
\mathit{streamF}\ (X : \mathit{Set}) : \mathit{Set} \triangleq\ & \{\epsilon\} \cup \\
& \{\tau \cdot s \mid s \in X\} \cup \\
& \{k \cdot s \mid k \in \mathbb{N},\ s \in X\}
\end{aligned}
$$

Coinductive Lists of Naturals

$$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$$
$$\{\tau \cdot s \mid s \in X\} \cup$$
$$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$$

Empty list

Coinductive Lists of Naturals

$$
\begin{aligned}
streamF\ (X : Set) : Set \triangleq\ & \{\epsilon\} \cup && \text{Empty list} \\
& \{\tau \cdot s \mid s \in X\} \cup && \text{Silent internal step} \\
& \{k \cdot s \mid k \in \mathbb{N},\ s \in X\}
\end{aligned}
$$

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

Coinductive Lists of Naturals

$$\begin{aligned} streamF\ (X : Set) : Set \triangleq\ & \{\epsilon\} \cup && \text{Empty list} \\ & \{\tau \cdot s \mid s \in X\} \cup && \text{Silent internal step} \\ & \{k \cdot s \mid k \in \mathbb{N},\ s \in X\} && \text{Visible event} \end{aligned}$$

$$\textbf{stream} \triangleq \nu\ streamF$$

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

stream $\triangleq \nu\ streamF$

$0 \cdot 1 \cdot \epsilon$	Finite list

Coinductive Lists of Naturals

$$\begin{aligned} streamF\ (X : Set) : Set \triangleq\ & \{\epsilon\} \cup && \text{Empty list} \\ & \{\tau \cdot s \mid s \in X\} \cup && \text{Silent internal step} \\ & \{k \cdot s \mid k \in \mathbb{N},\ s \in X\} && \text{Visible event} \end{aligned}$$

$$\textbf{stream} \triangleq \nu\ streamF$$

$0 \cdot 1 \cdot \epsilon$ Finite list

$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$ Finite list

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

stream $\triangleq \nu\ streamF$

$0 \cdot 1 \cdot \epsilon$	Finite list
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

$$\textbf{stream} \triangleq \nu\ streamF$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

stream $\triangleq \nu\ streamF$

$0 \cdot 1 \cdot \epsilon$	Finite list
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

Coinductive Lists of Naturals

$$\begin{aligned} \mathit{streamF}\ (X : \mathit{Set}) : \mathit{Set} \triangleq\ & \{\epsilon\} \cup && \text{Empty list} \\ & \{\tau \cdot s \mid s \in X\} \cup && \text{Silent internal step} \\ & \{k \cdot s \mid k \in \mathbb{N},\ s \in X\} && \text{Visible event} \end{aligned}$$

$$\textbf{stream} \triangleq \nu\ \mathit{streamF}$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$\approx$	
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

Coinductive Lists of Naturals

$\mathit{streamF}\ (X : \mathit{Set}) : \mathit{Set} \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

$$\textbf{stream} \triangleq \nu\ \mathit{streamF}$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$\wr\wr$	
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$\wr\wr$	
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

$$\textbf{stream} \triangleq \nu\ streamF$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$\approx$	
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$\approx$	
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\not\approx$	
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

Coinductive Lists of Naturals

$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$	Empty list
$\{\tau \cdot s \mid s \in X\} \cup$	Silent internal step
$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$	Visible event

$$\textbf{stream} \triangleq \nu\ streamF$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$\approx$	
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$\approx$	
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\not\approx$	
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

$$\approx\ \triangleq \nu\ euttF$$

Coinductive Lists of Naturals

$$streamF\ (X : Set) : Set \triangleq \{\epsilon\} \cup$$
$$\{\tau \cdot s \mid s \in X\} \cup$$
$$\{k \cdot s \mid k \in \mathbb{N},\ s \in X\}$$

Empty list

Silent internal step

Visible event

$$\textbf{stream} \triangleq \nu\ streamF$$

$$0 \cdot 1 \cdot \epsilon$$
Finite list

$$\approx$$

$$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$$
Finite list

$$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$$
Alternating stream

$$\approx$$

$$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$$
Alternating stream

$$\not\approx$$

$$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$$
Silently diverging stream

$$\approx\ \triangleq \nu\ euttF$$

eutt: “Equivalent Up-To Tau”

Coinductive Lists of Naturals

$$\begin{aligned} \mathit{streamF}\ (X : \mathit{Set}) : \mathit{Set} \triangleq\ & \{\epsilon\} \cup && \text{Empty list} \\ & \{\tau \cdot s \mid s \in X\} \cup && \text{Silent internal step} \\ & \{k \cdot s \mid k \in \mathbb{N},\ s \in X\} && \text{Visible event} \end{aligned}$$

$$\textbf{stream} \triangleq \nu\ \mathit{streamF}$$

$0 \cdot 1 \cdot \epsilon$	Finite list
$\wr$	
$0 \cdot \tau \cdot \tau \cdot 1 \cdot \tau \cdot \epsilon$	Finite list
$0 \cdot 2 \cdot 0 \cdot 2 \cdot 0 \cdot 2 \cdot \ldots$	Alternating stream
$\wr$	
$0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot 0 \cdot 2 \cdot \tau \cdot \ldots$	Alternating stream
$\not\wr$	
$\tau \cdot \tau \cdot \tau \cdot \tau \cdot \ldots$	Silently diverging stream

$$\approx\ \triangleq \nu\ \mathit{euttF}$$

?

eutt: “Equivalent Up-To Tau”

Parameterized Coinduction

If by ν we mean to define eutt as a Coq coinductive relation

$\hookrightarrow$ Then the tool to conduct proofs is guarded coinduction (cofix)

- Support incremental reasoning (nested cofixes) ✓
- Syntactic check (Breaks automation, composes poorly) ✗

Parameterized Coinduction

If by ν we mean to define eutt as a Coq coinductive relation

$\hookrightarrow$ Then the tool to conduct proofs is guarded coinduction (cofix)

- Support incremental reasoning (nested cofixes) ✓
- Syntactic check (Breaks automation, composes poorly) ✗

If by ν we mean the lattice-theoretic greatest fixed-point

$\hookrightarrow$ Then the (basic) tool to conduct proofs is Tarski's fixed-point theorem
A.k.a. "pick a post-fixed point"

- Does not support incremental reasoning ✗
- Semantic ✓

Parameterized Coinduction

If by ν we mean to define eutt as a Coq coinductive relation

$\hookrightarrow$ Then the tool to conduct proofs is guarded coinduction (cofix)

- Support incremental reasoning (nested cofixes) ✓
- Syntactic check (Breaks automation, composes poorly) ✗

If by ν we mean the lattice-theoretic greatest fixed-point

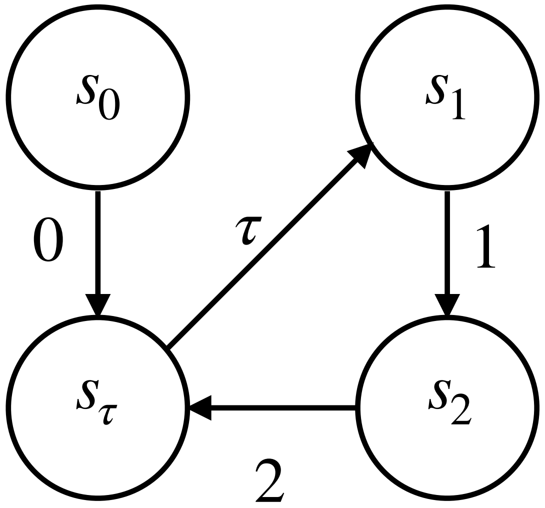
$\hookrightarrow$ Then the (basic) tool to conduct proofs is Tarski's fixed-point theorem
A.k.a. "pick a post-fixed point"

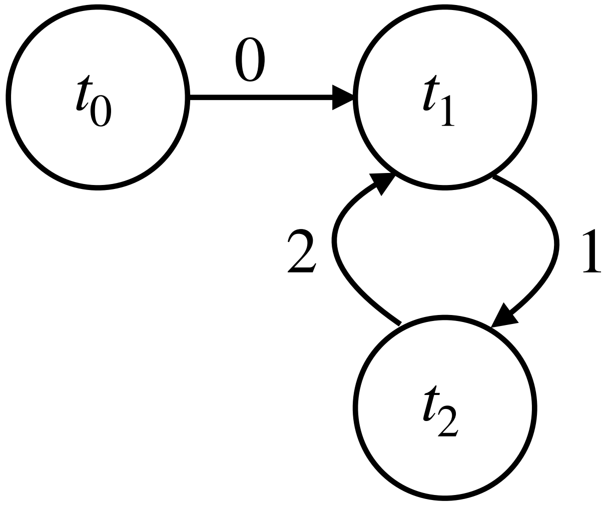
- Does not support incremental reasoning ✗
- Semantic ✓

Let ν be the parameterized greatest fixed-point (Hur et al., POPL'13)
$\longrightarrow$ Implemented in Coq by the paco library

- Support incremental reasoning ✓
- Semantic ✓

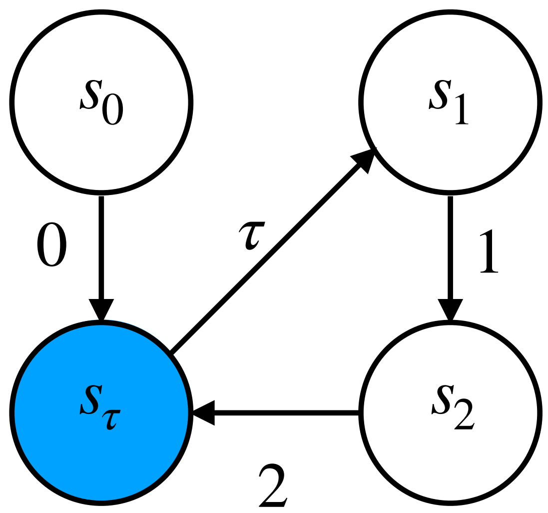
A Minimal Example

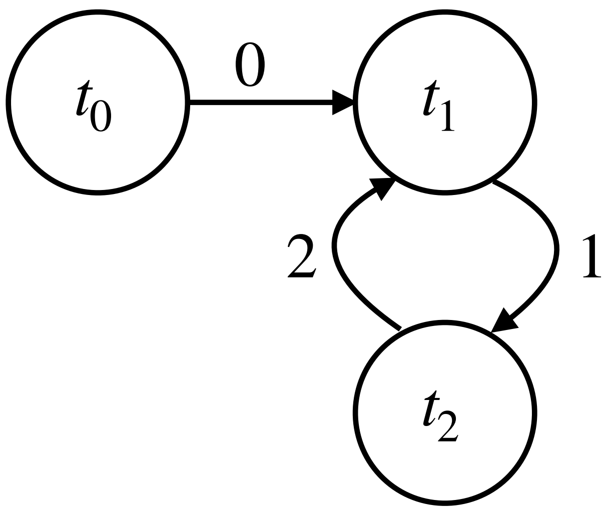




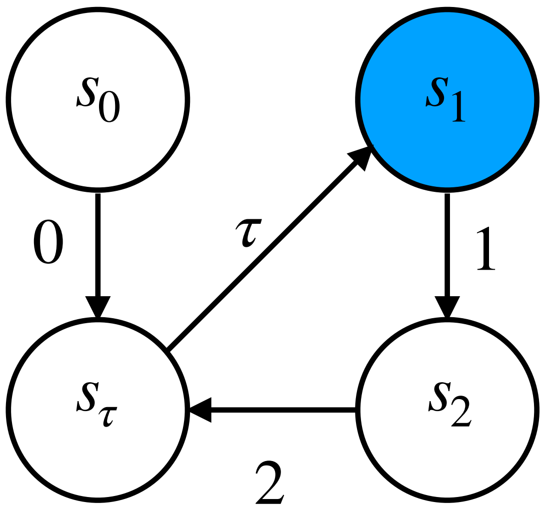
A Minimal Example

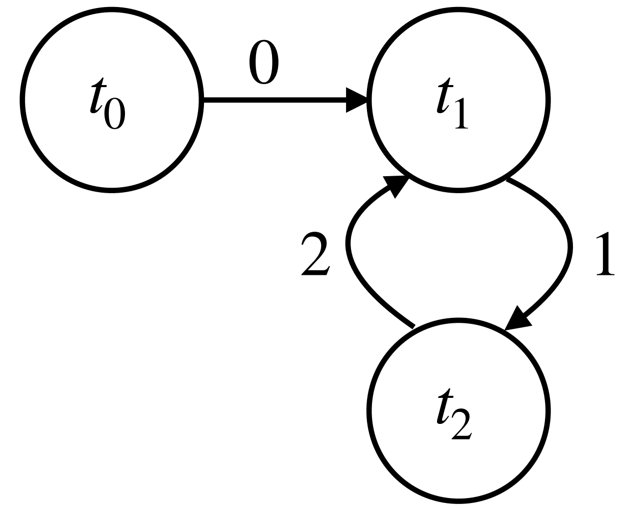
A Minimal Example



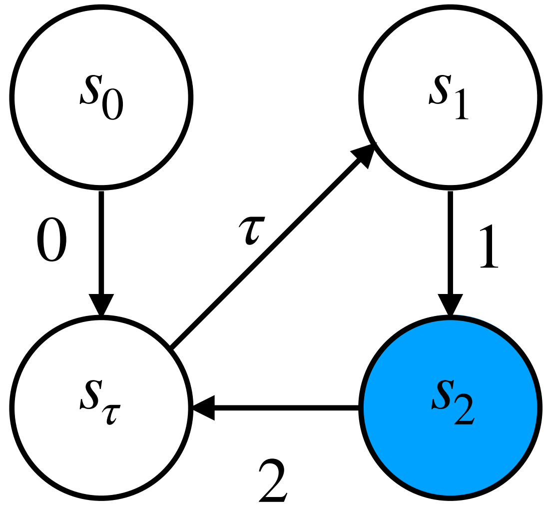


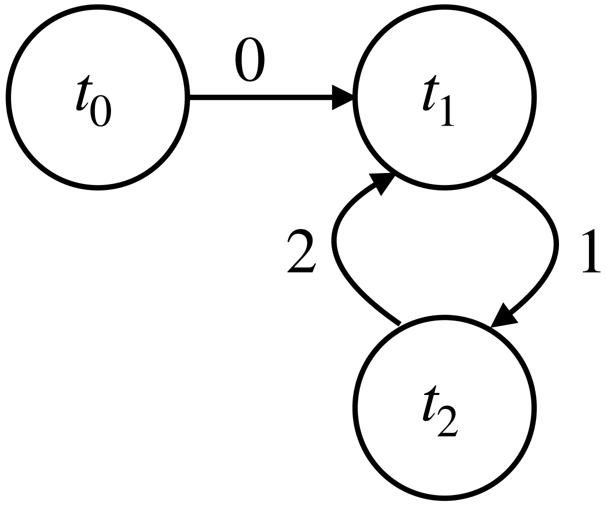
A Minimal Example



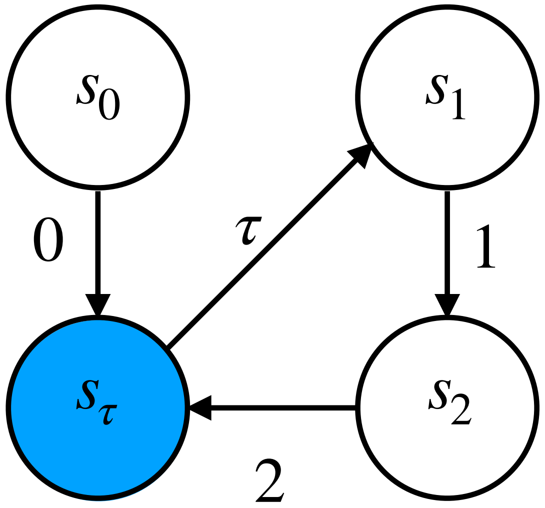


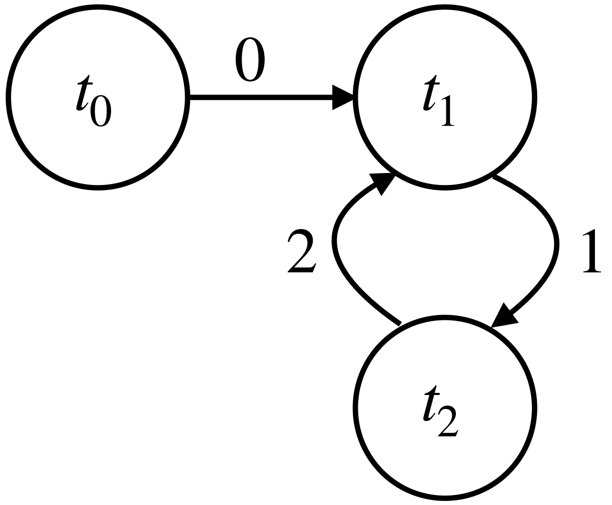
A Minimal Example





A Minimal Example





A Minimal Example

Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

A Minimal Example

Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

Problem with Coq's cofix:

```
cofix CIH.
auto.
```

$\square$

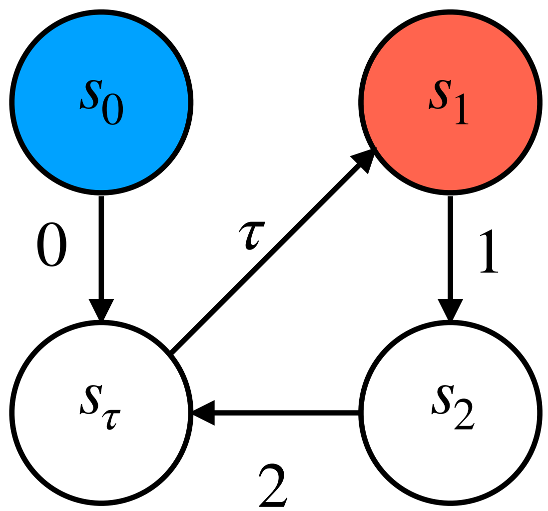
A Minimal Example

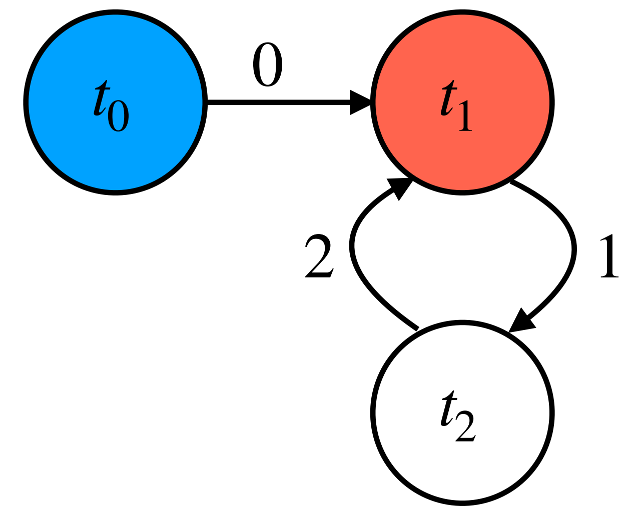
Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

Problem with Coq's cofix:

```
cofix CIH.
auto.
```

A Minimal Example





Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

Problem with Coq's cofix:

```
cofix CIH.

auto.
```

Problem with Tarski:

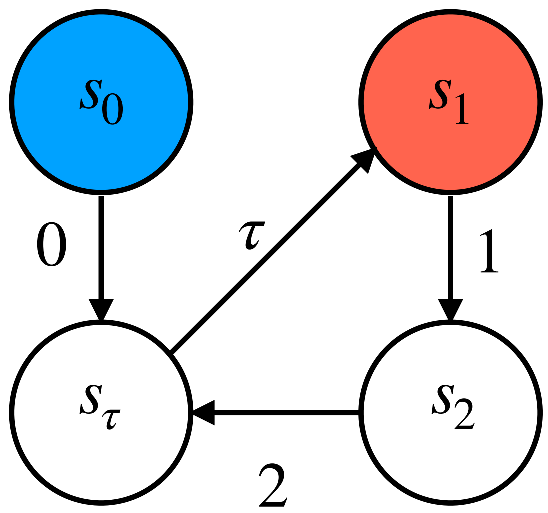
Let $\mathscr{R} \triangleq \{(s_0, t_0), (s_1, t_1), (s_\tau, t_1), (s_2, t_2)\}$

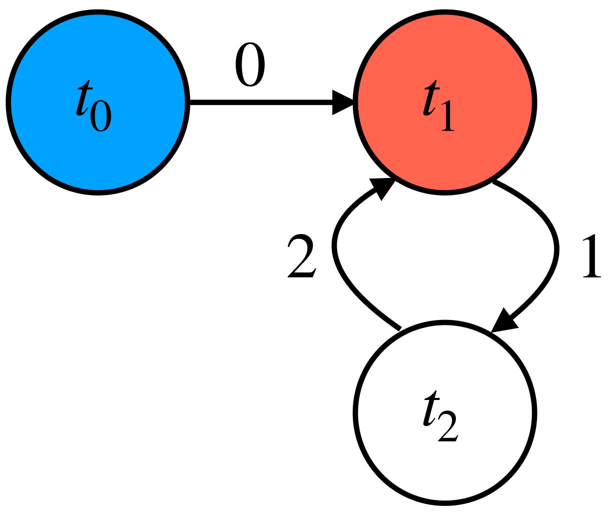
A Minimal Example

Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

$$\{(s_0, t_0), (s_1, t_1)\} \subseteq G_{euttF}\ \varnothing$$

A Minimal Example



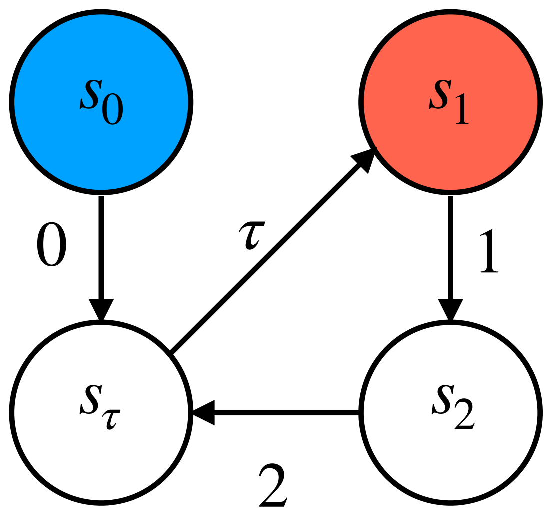


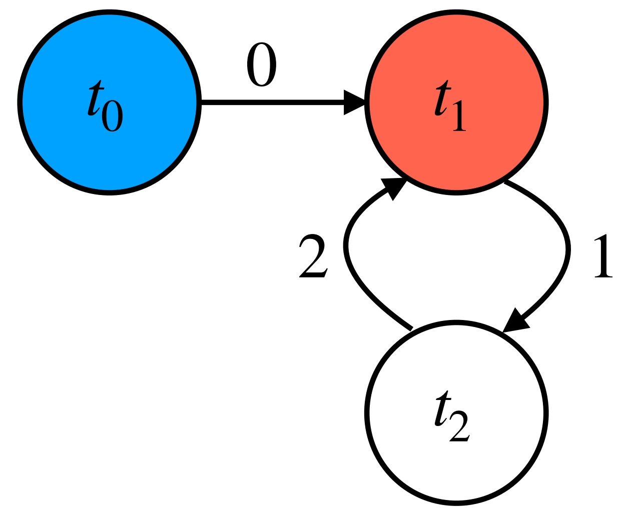
Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

$$G_{euttF} \equiv paco\ euttF \equiv \nu\ euttF$$

$$\{(s_0, t_0), (s_1, t_1)\} \subseteq G_{euttF}\ \varnothing$$

A Minimal Example





Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

We start with only the pairs of interest

$$G_{euttF} \equiv paco\ euttF \equiv \nu\ euttF$$

$$\{(s_0, t_0), (s_1, t_1)\} \subseteq G_{euttF}\ \varnothing$$

A Minimal Example

Let's show that $s_0 \approx t_0$ and $s_1 \approx t_1$

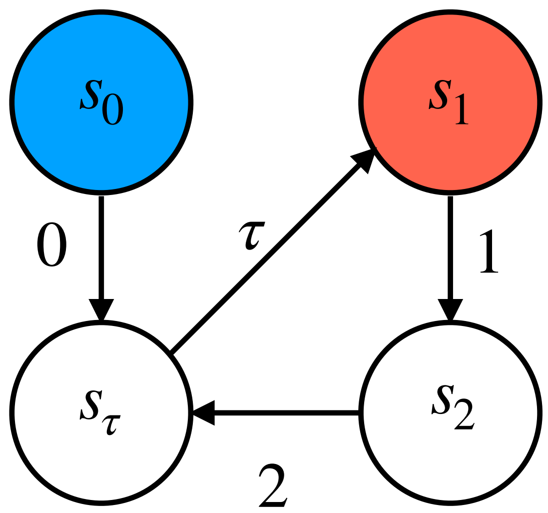
We start with only the pairs of interest

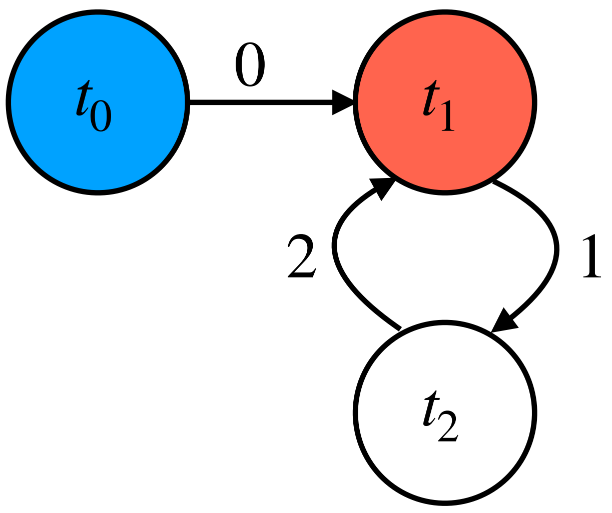
$G_{euttF} \equiv paco\ euttF \equiv \nu\ euttF$

$$\{(s_0, t_0), (s_1, t_1)\} \subseteq G_{euttF}\ \varnothing$$

The bisimulation is built incrementally
by recording knowledge in this parameter

A Minimal Example





$X = \{(s_0, t_0), (s_1, t_1)\}$

$X \subseteq G_{euttF}\ \varnothing$

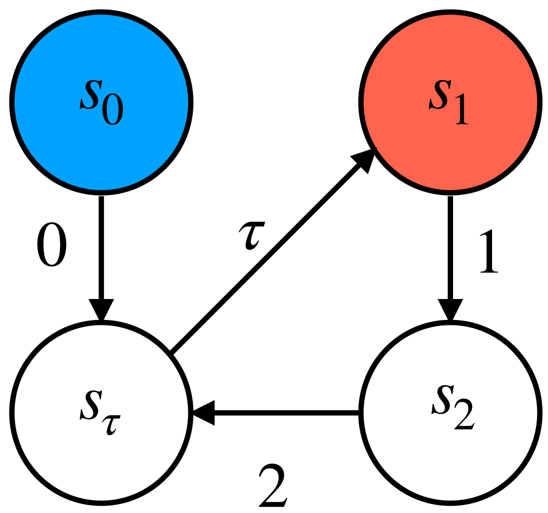
A Minimal Example

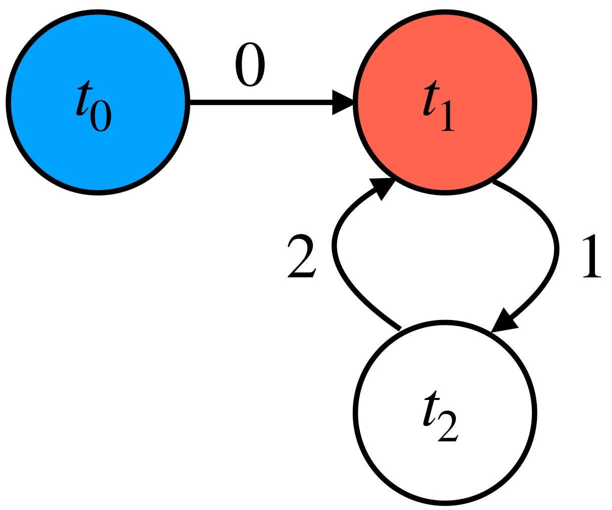
$X = \{(s_0, t_0), (s_1, t_1)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

A Minimal Example





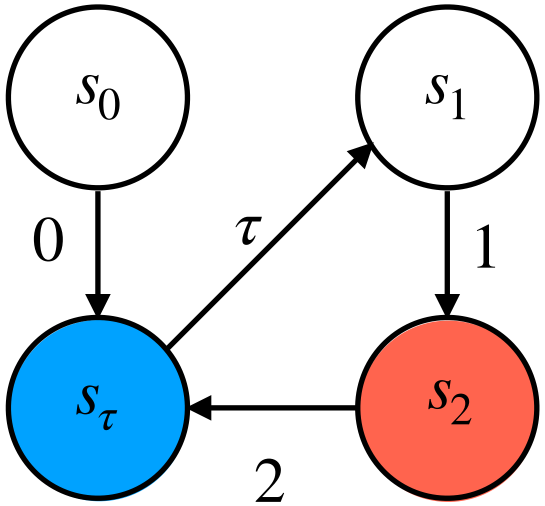
$X = \{(s_0, t_0), (s_1, t_1)\}$

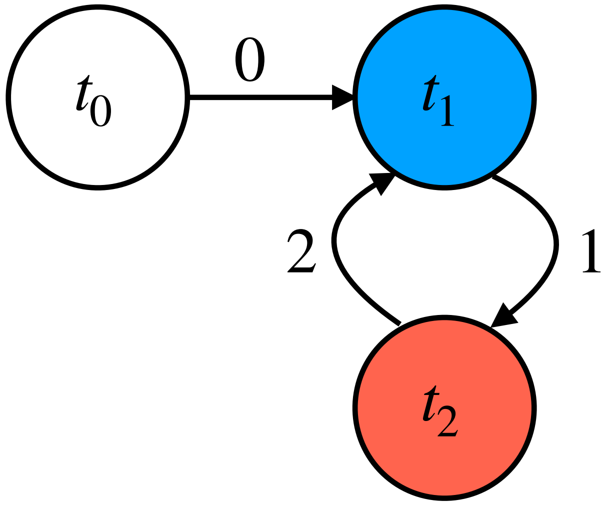
$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\}$ $Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

A Minimal Example

$X = \{(s_0, t_0), (s_1, t_1)\}$ $Y = \{(s_\tau, t_1), (s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

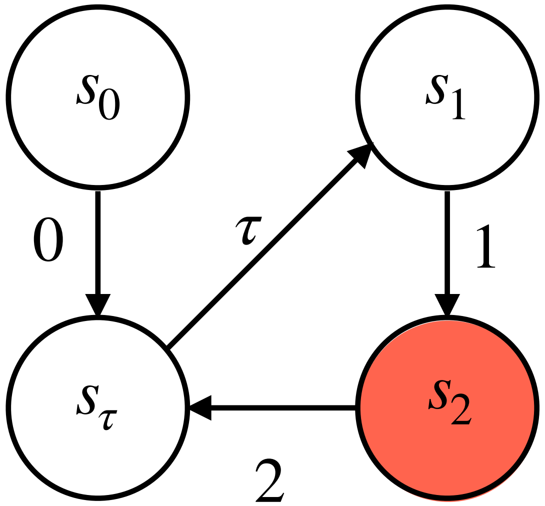
Accumulate $X \subseteq G_{euttF}\ X$

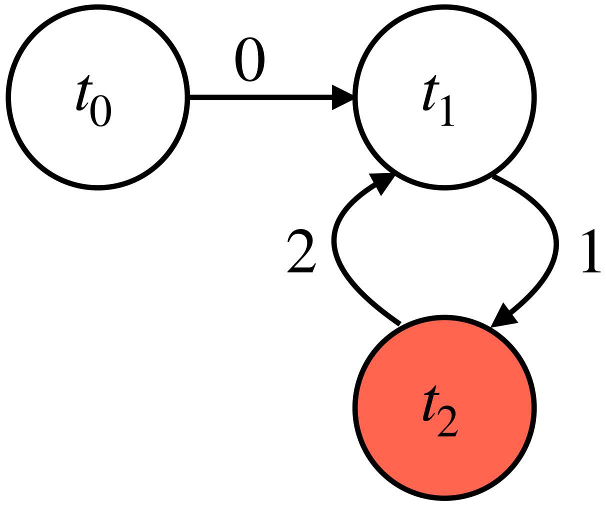
Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

A Minimal Example

$X = \{(s_0, t_0),(s_1, t_1)\}$ $Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

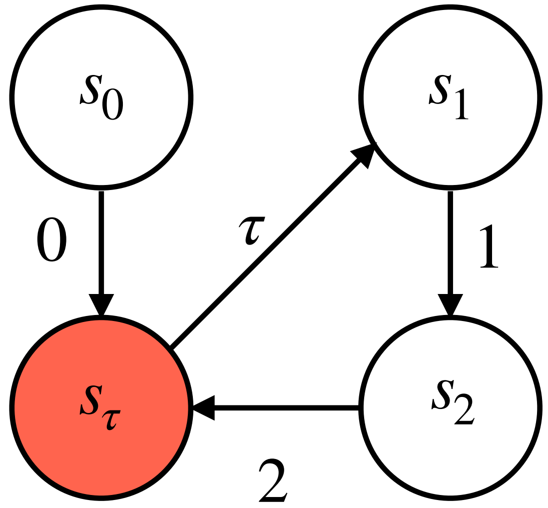
Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

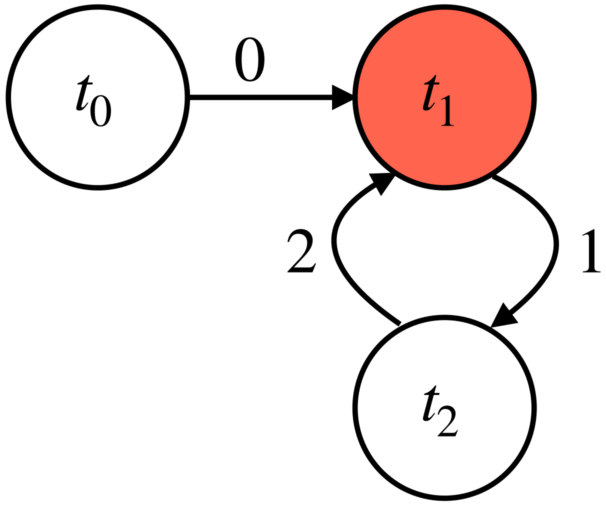
Two cases:

$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

$(s_\tau, t_1) \in X \cup Y \cup G_{euttF}\ (X \cup Y)$ **Step**

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

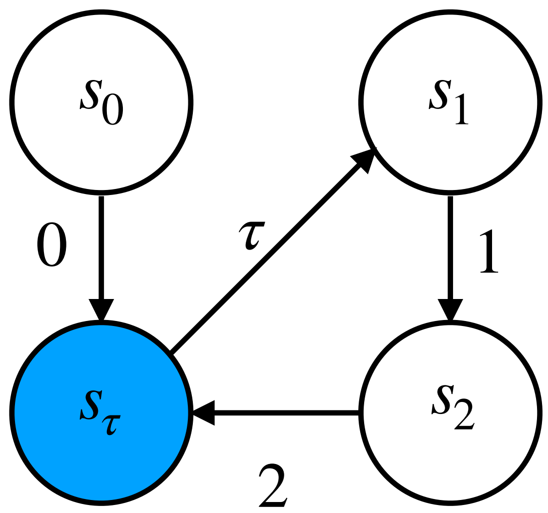
Two cases:

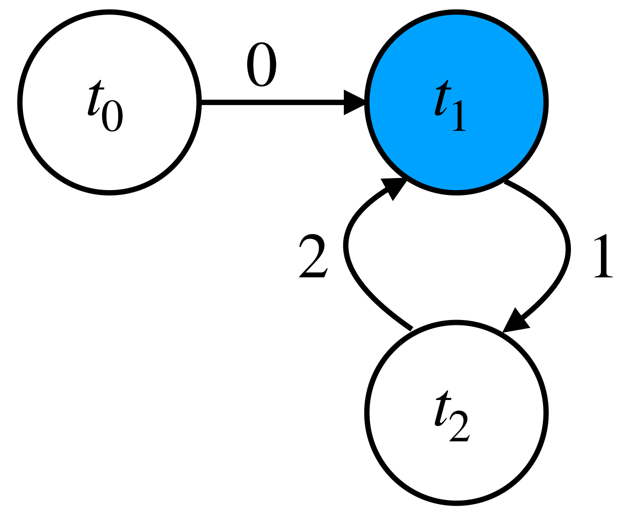
$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

$(s_\tau, t_1) \in X \cup Y \cup G_{euttF}\ (X \cup Y)$ **Step**

$\square$

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

Two cases:

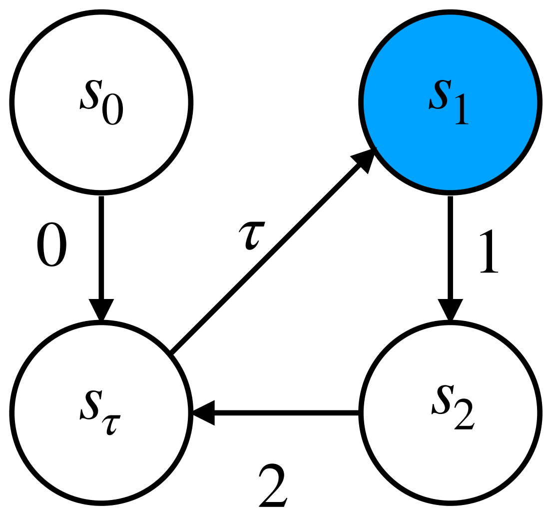
$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

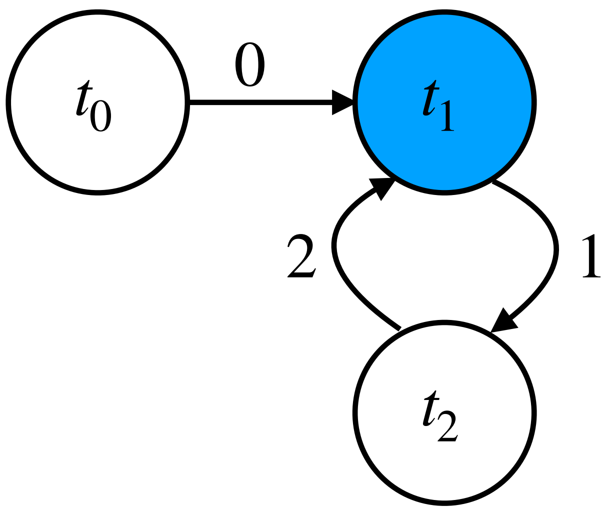
$(s_\tau, t_1) \in X \cup Y \cup G_{euttF}\ (X \cup Y)$ **Step**

$\square$

$(s_\tau, t_1) \in G_{euttF}\ (X \cup Y)$

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\} \quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

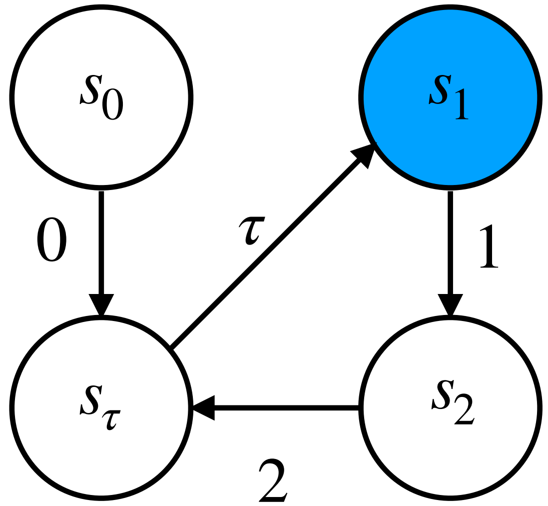
$(s_\tau, t_1) \in X \cup Y \cup G_{euttF}\ (X \cup Y)$ **Step**

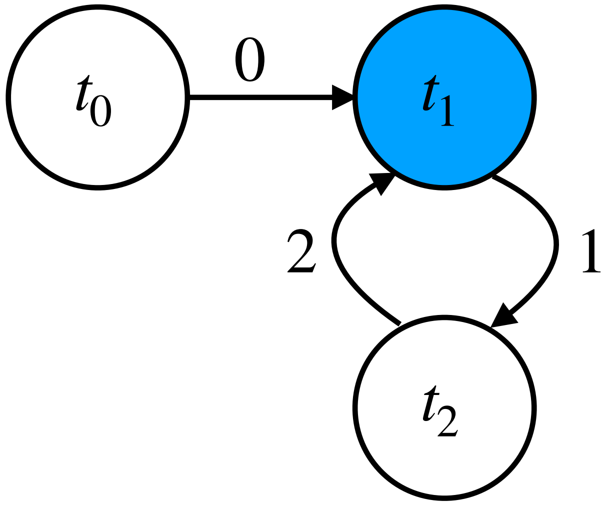
$\square$

$(s_\tau, t_1) \in G_{euttF}\ (X \cup Y)$

$(s_1, t_1) \in G_{euttF}\ (X \cup Y)$ **Easy Lemma**

A Minimal Example





$X = \{(s_0, t_0),(s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Accumulate $X \subseteq G_{euttF}\ X$

Unfold $X \subseteq euttF(X \cup G_{euttF}\ X)$

Step $Y \subseteq X \cup G_{euttF}\ X$

Accumulate $Y \subseteq G_{euttF}\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in G_{euttF}\ (X \cup Y)$

$(s_\tau, t_1) \in X \cup Y \cup G_{euttF}\ (X \cup Y)$ **Step**

$\square$

$(s_\tau, t_1) \in G_{euttF}\ (X \cup Y)$

$(s_1, t_1) \in G_{euttF}\ (X \cup Y)$ **Easy Lemma**

We *should* be able to conclude!

Extending Paco with a Second Parameter

$$\hat{G}_F\ R\ G \triangleq R \cup G_F(R \cup G)$$

Released Guarded

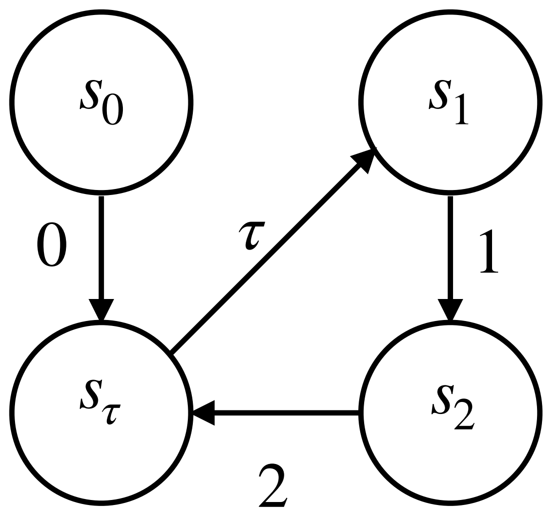
- The released information is *always* available

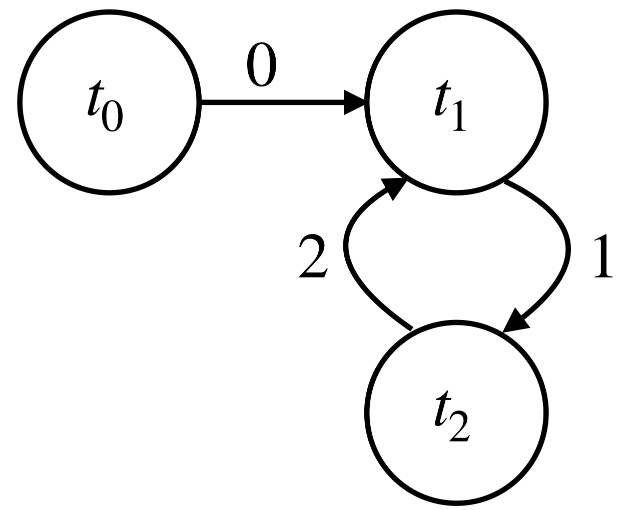
$$\frac{}{R \subseteq \hat{G}_F\ R\ G}\ \textbf{Base}$$

- The approach is entirely backward-compatible with paco
  - ⟶ Definitions require no change to use the new reasoning principles
  - ⟶ The "generalized world" is a proof intermediary

$$\frac{}{\hat{G}_F\ \varnothing\ \varnothing \equiv G_F\ \varnothing}\ \textbf{Init} \qquad \frac{}{R \cup G_F\ G \subseteq \hat{G}_F\ R\ G}\ \textbf{Final}$$

Extending Paco with a Second Parameter





$X = \{(s_0, t_0),(s_1, t_1)\} \quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Init $X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$

Accumulate $X \subseteq \hat{G}_{euttF}\ \varnothing\ X$

Step $Y \subseteq \hat{G}_{euttF}\ X\ X$

Accumulate $Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

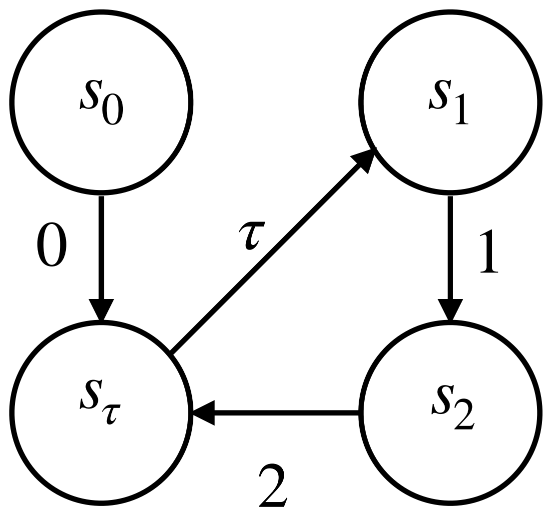
$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step**

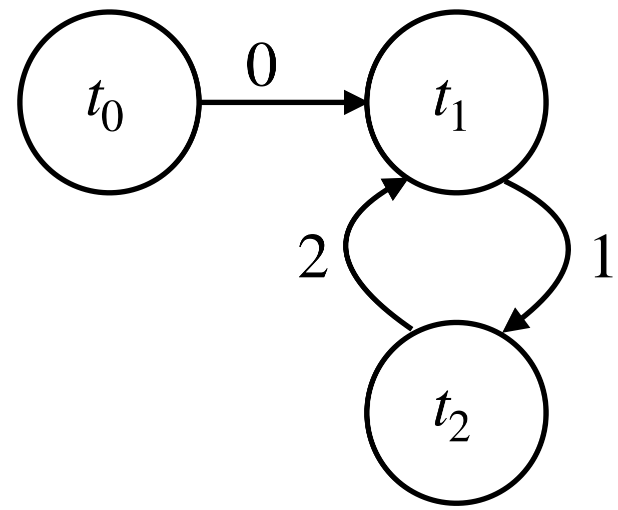
$\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

Extending Paco with a Second Parameter





$X = \{(s_0, t_0),(s_1, t_1)\}$ $Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Init $X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$ ←

Accumulate $X \subseteq \hat{G}_{euttF}\ \varnothing\ X$

Step $Y \subseteq \hat{G}_{euttF}\ X\ X$

Accumulate $Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

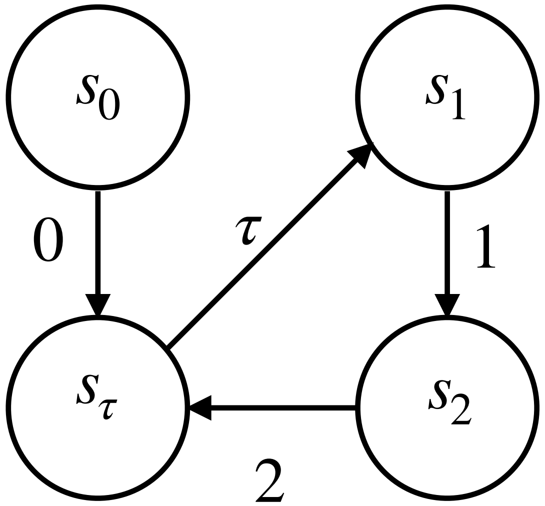
$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step**

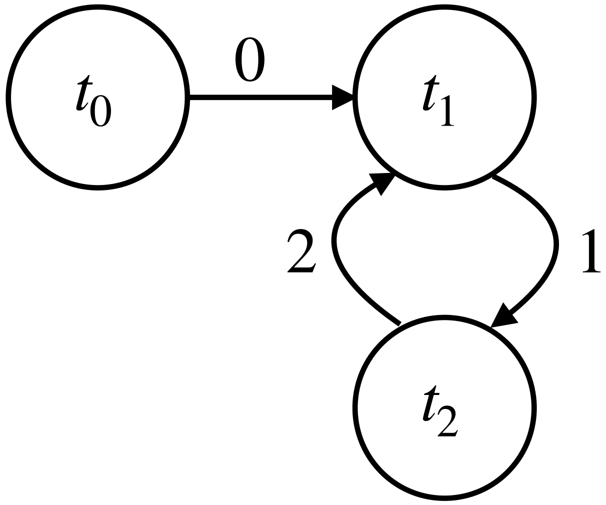
$\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

Extending Paco with a Second Parameter





$X = \{(s_0, t_0),(s_1, t_1)\} \quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Init $X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$

Accumulate $X \subseteq \hat{G}_{euttF}\ \varnothing\ X$

Step $Y \subseteq \hat{G}_{euttF}\ X\ X$

Accumulate $Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

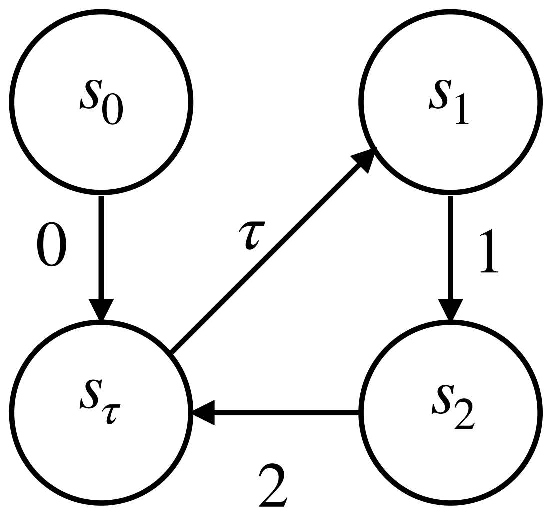
$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step**

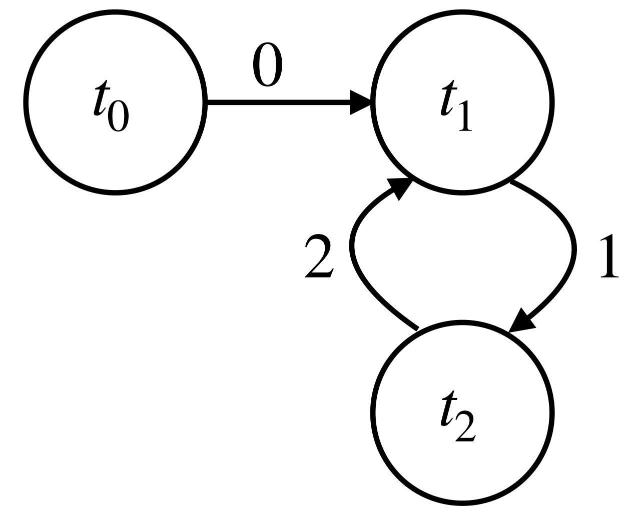
$\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

Extending Paco with a Second Parameter





$X = \{(s_0, t_0), (s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1), (s_2, t_2)\}$

	$X \subseteq G_{euttF}\ \varnothing$
Init	$X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$
Accumulate	$X \subseteq \hat{G}_{euttF}\ \varnothing\ X$
Step	$Y \subseteq \hat{G}_{euttF}\ X\ X$
Accumulate	$Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step**

$\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

Extending Paco with a Second Parameter

$X = \{(s_0, t_0),(s_1, t_1)\}$ $Y = \{(s_\tau, t_1),(s_2, t_2)\}$

$X \subseteq G_{euttF}\ \varnothing$

Init $X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$

Accumulate $X \subseteq \hat{G}_{euttF}\ \varnothing\ X$

Step $Y \subseteq \hat{G}_{euttF}\ X\ X$

Accumulate $Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

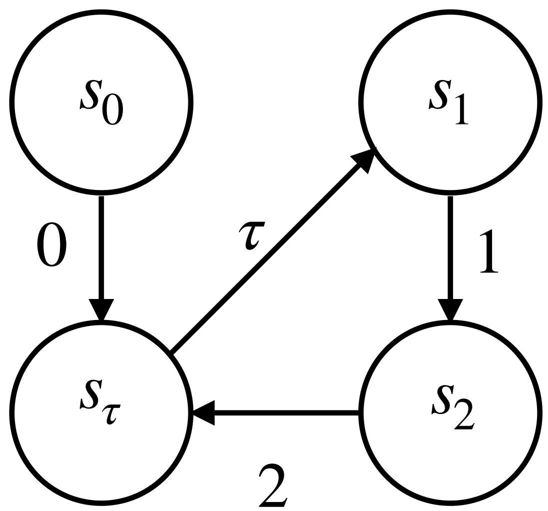
$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

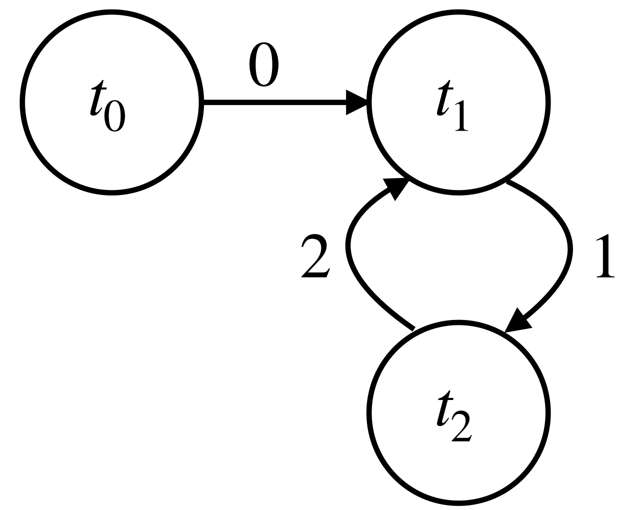
$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step** $\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

Extending Paco with a Second Parameter





$X = \{(s_0, t_0),(s_1, t_1)\}$ $\quad Y = \{(s_\tau, t_1),(s_2, t_2)\}$

	$X \subseteq G_{euttF}\ \varnothing$
Init	$X \subseteq \hat{G}_{euttF}\ \varnothing\ \varnothing$
Accumulate	$X \subseteq \hat{G}_{euttF}\ \varnothing\ X$
Step	$Y \subseteq \hat{G}_{euttF}\ X\ X$
Accumulate	$Y \subseteq \hat{G}_{euttF}\ X\ (X \cup Y)$

Two cases:

$(s_2, t_2) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ (X \cup Y)\ (X \cup Y)$ **Step**

$\square$

$(s_\tau, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$

$(s_1, t_1) \in \hat{G}_{euttF}\ X\ (X \cup Y)$ **Easy Lemma**

X is still accessible! $\square$

Generalized Paco

- Parameterized Coinduction had a leak: a second parameter fixes it
- Other increment not covered here: “native" support for up-to reasoning
- Backward compatible: relations are still defined in term of **paco**, but **gpaco** can be used to conduct proofs about them

See the paper for more details!

Integrated to paco, and on opam!

https://github.com/snu-sf/paco

A Parameterized Weak Bisimulation

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ \color{green}{R}\ \color{red}{G}}{(s, t) \in \hat{G}_{euttF}\ \color{green}{R}\ \color{red}{G}}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✗

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s',t) \in \hat{G}_{euttF}\ R\ G}{(s,t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✘

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✗

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Init $\quad (0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \varnothing$

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✗

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Init $(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \varnothing$

Accumulate $(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✘

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Init	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \varnothing$
Accumulate	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$
Rewrite	$(\tau \cdot 0 \cdot \epsilon, \tau \cdot 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✘

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Init	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \varnothing$
Accumulate	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$
Rewrite	$(\tau \cdot 0 \cdot \epsilon, \tau \cdot 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$
Step	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}\ \textbf{Rewrite}$$

Is such a rewriting rule sound?

In general: no! ✗

Let's assume this rule and prove that $0 \cdot \epsilon \approx 1 \cdot \epsilon$:

Init	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \varnothing$
Accumulate	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$
Rewrite	$(\tau \cdot 0 \cdot \epsilon, \tau \cdot 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \varnothing\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$
Step	$(0 \cdot \epsilon, 1 \cdot \epsilon) \in \hat{G}_{euttF}\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}\ \{(0 \cdot \epsilon, 1 \cdot \epsilon)\}$

The rule is unsound, but only the silent step is to be blamed!

A Parameterized Weak Bisimulation

Objective: define euttG, a sound parameterized generalization of eutt

$\approx$: relation stream

euttG(R_β R_τ G_β G_τ: relation stream): relation stream

A Parameterized Weak Bisimulation

Objective: define euttG, a sound parameterized generalization of eutt

$\approx$: relation stream

"Released" "Guarded"

euttG(R_β R_τ G_β G_τ: relation stream): relation stream

A Parameterized Weak Bisimulation

Objective: define euttG, a sound parameterized generalization of eutt

$\approx$: relation stream

"Released" "Guarded"

euttG(R_β R_τ G_β G_τ: relation stream): relation stream

"By a Vis" "By a Tau"

A Parameterized Weak Bisimulation

Objective: define euttG, a sound parameterized generalization of eutt

$\approx$: relation stream

"Released" "Guarded"

euttG(R_β R_τ G_β G_τ: relation stream): relation stream

"By a Vis" "By a Tau"

Let's look at the reasoning principles it supports
(for the construction itself, we refer to the paper)

Rewriting eutt-Equations

$$\frac{s \approx s' \qquad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G}$$

Distinguishing τ from β steps allows for a **weaker** but **sound** principle:

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G} \quad ✗$$

Distinguishing τ from β steps allows for a **weaker** but **sound** principle:

$$\frac{s \approx s' \qquad (s', t) \in \text{euttG}\ R_\beta\ R_\beta\ G_\beta\ R_\beta}{(s, t) \in \text{euttG}\ R_\beta\ R_\tau\ G_\beta\ G_\tau}$$

Rewriting eutt-Equations

$$\frac{s \approx s' \quad (s', t) \in \hat{G}_{euttF}\ R\ G}{(s, t) \in \hat{G}_{euttF}\ R\ G} \quad \text{✗}$$

Distinguishing τ from β steps allows for a **weaker** but **sound** principle:

We forget all τ-knowledge

$$\frac{s \approx s' \qquad (s', t) \in \text{euttG}\ R_\beta\ R_\beta\ G_\beta\ R_\beta}{(s, t) \in \text{euttG}\ R_\beta\ R_\tau\ G_\beta\ G_\tau} \quad \text{✓}$$

Soundness

euttG is an proof intermediary to $\approx$ the way **gpaco** is to **paco**

Initiates a parameterized proof:

$$\frac{(s,t) \in \text{euttG } \varnothing\ \varnothing\ \varnothing\ \varnothing}{s \approx t}\ \textbf{Init}$$

Allows for using any pre-established $\approx$-equation:

$$\frac{s \approx t}{(s,t) \in \text{euttG } R_\beta\ R_\tau\ G_\beta\ G_\tau}\ \textbf{Final}$$

Knowledge Manipulation

Released knowledge is fair game:

$$\frac{(s,t) \in R_\tau \cup R_\beta}{(s,t) \in \text{euttG } R_\beta\ R_\tau\ G_\beta\ G_\tau}\ \textbf{Base}$$

Information can be accumulated in the style of gpaco:

$$\frac{(s,t) \in \text{euttG } R_\beta\ R_\tau\ (G_\beta \cup \{(s,t)\})\ (G_\tau \cup \{(s,t)\})}{(s,t) \in \text{euttG } R_\beta\ R_\tau\ G_\beta\ G_\tau}\ \textbf{Accumulate}$$

Stream Processing

Tau guards release the tau guarded information:

$$\frac{(s, t) \in \text{euttG}\ R_\beta\ G_\tau\ G_\beta\ G_\tau}{(\tau \cdot s, \tau \cdot t) \in \text{euttG}\ R_\beta\ R_\tau\ G_\beta\ G_\tau}\ \textbf{Tau}$$

Vis guards release the vis guarded information:

$$\frac{(s, t) \in \text{euttG}\ G_\beta\ G_\beta\ G_\beta\ G_\beta}{(k \cdot s, k \cdot t) \in \text{euttG}\ R_\beta\ R_\tau\ G_\beta\ G_\tau}\ \textbf{Vis}$$

Invariant: $R_\beta \subseteq R_\tau \subseteq G_\tau \subseteq G_\beta$

Parameterized Weak Bisimulation

- The intuition behind gpaco can be specialized to specific applications
- Reasoning principles that differentiate the constructors
- More in the paper: up-to concatenation, up-to directed weak bisimulation
- More in the paper: the construction itself of euttG is quite subtle

See the paper for more details!

Conclusion

Conclusion

Generalized paco:

- Backward-compatible with paco
- Don’t lose knowledge + native support for up-to reasoning
- Available on Opam and Github!

https://github.com/snu-sf/paco

Parameterized Weak Bisimulation:

- High level reasoning principles
- Differentiates the constructors used in the proof

Large scale application: Interaction Trees

- The project was born of necessity to prove the meta-theory of **interaction trees**
- Join us for the talk Friday at 11:13!