# Lecture 4

- properties of strong bisimilarity
- weak bisimilarity and weak bisimulation games
- properties of weak bisimilarity
- example: a communication protocol and its modelling in CCS
- software tool CAAL http://caal.cs.aau.dk/

# Strong Bisimilarity – Properties

## Strong Bisimilarity is a Congruence for All CCS Operators

Let $P$ and $Q$ be CCS processes such that $P \sim Q$. Then

- $\alpha.P \sim \alpha.Q$ for each action $\alpha \in Act$
- $P + R \sim Q + R$ and $R + P \sim R + Q$ for each CCS process $R$
- $P \mid R \sim Q \mid R$ and $R \mid P \sim R \mid Q$ for each CCS process $R$
- $P[f] \sim Q[f]$ for each relabelling function $f$
- $P \setminus L \sim Q \setminus L$ for each set of labels $L$.

## Following Properties Hold for any CCS Processes $P$, $Q$ and $R$

- $P + Q \sim Q + P$
- $P \mid Q \sim Q \mid P$
- $P + Nil \sim P$
- $P \mid Nil \sim P$
- $(P+Q)+R \sim P+(Q+R)$
- $(P \mid Q) \mid R \sim P \mid (Q \mid R)$

# Example – Buffer

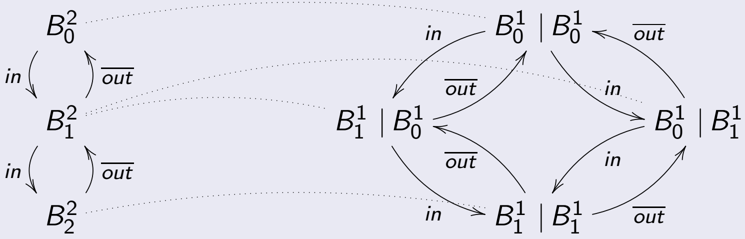
## Buffer of Capacity 1

$$B^1_0 \stackrel{\text{def}}{=} in.B^1_1$$
$$B^1_1 \stackrel{\text{def}}{=} \overline{out}.B^1_0$$

## Buffer of Capacity $n$

$$B^n_0 \stackrel{\text{def}}{=} in.B^n_1$$
$$B^n_i \stackrel{\text{def}}{=} in.B^n_{i+1} + \overline{out}.B^n_{i-1} \quad \text{for } 0 < i < n$$
$$B^n_n \stackrel{\text{def}}{=} \overline{out}.B^n_{n-1}$$

## Example: $B^2_0 \sim B^1_0 \mid B^1_0$



# Example – Buffer

## Theorem

*For all natural numbers n:* $\quad B_0^n \sim \underbrace{B_0^1 \mid B_0^1 \mid \cdots \mid B_0^1}_{n \text{ times}}$

## Proof.

Construct the following binary relation where $i_1, i_2, \ldots, i_n \in \{0, 1\}$.

$$R = \{\big(B_i^n,\ B_{i_1}^1 \mid B_{i_2}^1 \mid \cdots \mid B_{i_n}^1\big) \mid \sum_{j=1}^{n} i_j = i\}$$

- $\big(B_0^n,\ B_0^1 \mid B_0^1 \mid \cdots \mid B_0^1\big) \in R$
- $R$ is strong bisimulation

$\square$

# Strong Bisimilarity – Summary

## Properties of $\sim$

- an equivalence relation
- the largest strong bisimulation
- a congruence
- enough to prove some natural rules like
  - $P \mid Q \sim Q \mid P$
  - $P \mid Nil \sim P$
  - $(P \mid Q) \mid R \sim Q \mid (P \mid R)$
  - $\cdots$

## Question

Should we look any further???

# Problems with Internal Actions

## Question

Does $a.\tau.Nil \sim a.Nil$ hold? NO!

## Problem

Strong bisimilarity does not abstract away from $\tau$ actions.

## Example: SmUni $\not\sim$ Spec

$$
\begin{tikzcd}
\mathrm{SmUni} \arrow[d, "\overline{pub}"] & \not\sim & \mathrm{Spec} \arrow[loop below, "\overline{pub}"] \\
(CM \mid CS_1) \smallsetminus \{coin, coffee\} \arrow[d, "\tau"] & & \\
(CM_1 \mid CS_2) \smallsetminus \{coin, coffee\} \arrow[d, "\tau"] & & \\
(CM \mid CS) \smallsetminus \{coin, coffee\} \arrow[uu, bend right, "\overline{pub}"'] & &
\end{tikzcd}
$$

# Weak Transition Relation

Let $(Proc, Act, (\xrightarrow{a})_{a \in Act})$ be an LTS such that $\tau \in Act$.

## Definition of Weak Transition Relation

$$\stackrel{a}{\Longrightarrow} = \begin{cases} (\xrightarrow{\tau})^* \circ \xrightarrow{a} \circ (\xrightarrow{\tau})^* & \text{if } a \neq \tau \\ (\xrightarrow{\tau})^* & \text{if } a = \tau \end{cases}$$

## What does $s \stackrel{a}{\Longrightarrow} t$ informally mean?

- If $a \neq \tau$ then $s \stackrel{a}{\Longrightarrow} t$ means that
  from $s$ we can get to $t$ by doing zero or more $\tau$ actions, followed by the action $a$, followed by zero or more $\tau$ actions.
- If $a = \tau$ then $s \stackrel{\tau}{\Longrightarrow} t$ means that
  from $s$ we can get to $t$ by doing zero or more $\tau$ actions.

# Weak Bisimilarity

Let $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ be an LTS such that $\tau \in Act$.

## Weak Bisimulation

A binary relation $R \subseteq Proc \times Proc$ is a weak bisimulation iff whenever $(s, t) \in R$ then for each $a \in Act$ (including $\tau$):

- if $s \xrightarrow{a} s'$ then $t \overset{a}{\Longrightarrow} t'$ for some $t'$ such that $(s', t') \in R$
- if $t \xrightarrow{a} t'$ then $s \overset{a}{\Longrightarrow} s'$ for some $s'$ such that $(s', t') \in R$.

## Weak Bisimilarity

Two processes $p_1, p_2 \in Proc$ are weakly bisimilar ($p_1 \approx p_2$) if and only if there exists a weak bisimulation $R$ such that $(p_1, p_2) \in R$.

$$\approx \; = \; \cup\{R \mid R \text{ is a weak bisimulation}\}$$

# Weak Bisimulation Game

## Definition

All the same except that

- defender can now answer using $\stackrel{a}{\Longrightarrow}$ moves.

The attacker is still using only $\stackrel{a}{\longrightarrow}$ moves.

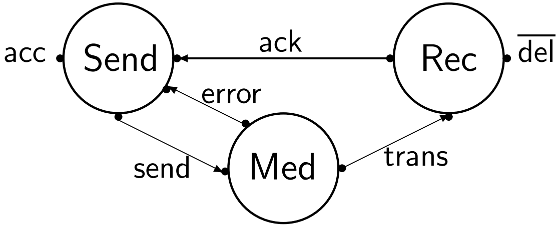
## Theorem

- States $s$ and $t$ are weakly bisimilar if and only if the defender has a universal winning strategy starting from the configuration $(s, t)$.
- States $s$ and $t$ are not weakly bisimilar if and only if the attacker has a universal winning strategy starting from the configuration $(s, t)$.

## Properties of $\approx$

- an equivalence relation
- the largest weak bisimulation
- validates lots of natural laws, e.g.
  - $a.\tau.P \approx a.P$
  - $P + \tau.P \approx \tau.P$
  - $a.(P + \tau.Q) \approx a.(P + \tau.Q) + a.Q$
  - $P + Q \approx Q + P \qquad P \mid Q \approx Q \mid P \qquad P + Nil \approx P \qquad \ldots$
- strong bisimilarity is included in weak bisimilarity ($\sim \subseteq \approx$)
- abstracts from $\tau$ loops

# Case Study: Communication Protocol




$$\begin{aligned} \text{Send} &\stackrel{\text{def}}{=} \text{acc.Sending} \\ \text{Sending} &\stackrel{\text{def}}{=} \overline{\text{send}}.\text{Wait} \\ \text{Wait} &\stackrel{\text{def}}{=} \text{ack.Send} + \text{error.Sending} \end{aligned} \qquad \begin{aligned} \text{Rec} &\stackrel{\text{def}}{=} \text{trans.Del} \\ \text{Del} &\stackrel{\text{def}}{=} \overline{\text{del}}.\text{Ack} \\ \text{Ack} &\stackrel{\text{def}}{=} \overline{\text{ack}}.\text{Rec} \end{aligned}$$

$$\begin{aligned} \text{Med} &\stackrel{\text{def}}{=} \text{send.Med}' \\ \text{Med}' &\stackrel{\text{def}}{=} \tau.\text{Err} + \overline{\text{trans}}.\text{Med} \\ \text{Err} &\stackrel{\text{def}}{=} \overline{\text{error}}.\text{Med} \end{aligned}$$

# Verification Question

$$\mathsf{Impl} \stackrel{\mathrm{def}}{=} (\mathsf{Send} \mid \mathsf{Med} \mid \mathsf{Rec}) \smallsetminus \{\mathsf{send}, \mathsf{trans}, \mathsf{ack}, \mathsf{error}\}$$

$$\mathsf{Spec} \stackrel{\mathrm{def}}{=} \mathsf{acc}.\overline{\mathsf{del}}.\mathsf{Spec}$$

**Question**

$$\mathsf{Impl} \stackrel{?}{\approx} \mathsf{Spec}$$

1. Draw the LTS of Impl and Spec and prove (by hand) the equivalence.
2. Use CAAL.

# Is Weak Bisimilarity a Congruence for CCS?

**Theorem**

*Let $P$ and $Q$ be CCS processes such that $P \approx Q$. Then*

- $\alpha.P \approx \alpha.Q$ *for each action* $\alpha \in Act$
- $P \mid R \approx Q \mid R$ *and* $R \mid P \approx R \mid Q$ *for each CCS process* $R$
- $P[f] \approx Q[f]$ *for each relabelling function* $f$
- $P \setminus L \approx Q \setminus L$ *for each set of labels* $L$.

What about choice?

$\tau.a.Nil \approx a.Nil$ but $\tau.a.Nil + b.Nil \not\approx a.Nil + b.Nil$

**Conclusion**

Weak bisimilarity is not a congruence for CCS.