

## Buffer s kapacitou $n$

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$

$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$

$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

## Buffer s kapacitou 1

$$B_0^1 \stackrel{\text{def}}{=} in.B_1^1$$

$$B_1^1 \stackrel{\text{def}}{=} \overline{out}.B_0^1$$

## Buffer s kapacitou $n$

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$

$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$

$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

## Buffer s kapacitou 1

$$B_0^1 \stackrel{\text{def}}{=} in.B_1^1$$

$$B_1^1 \stackrel{\text{def}}{=} \overline{out}.B_0^1$$

# Příklad – buffer

## Buffer s kapacitou $n$

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$

$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$

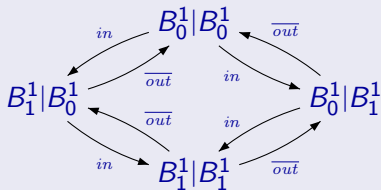
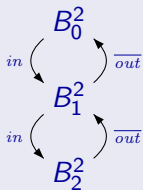
$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

## Buffer s kapacitou 1

$$B_0^1 \stackrel{\text{def}}{=} in.B_1^1$$

$$B_1^1 \stackrel{\text{def}}{=} \overline{out}.B_0^1$$

Příklad:  $B_0^2 \sim B_0^1|B_0^1$



# Příklad – buffer

## Buffer s kapacitou $n$

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$

$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$

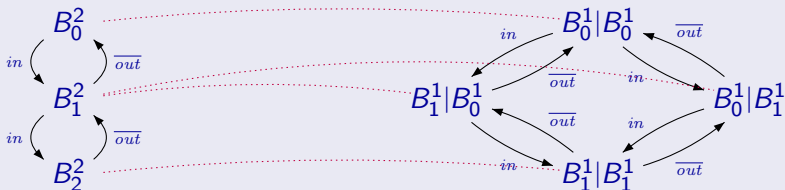
$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

## Buffer s kapacitou 1

$$B_0^1 \stackrel{\text{def}}{=} in.B_1^1$$

$$B_1^1 \stackrel{\text{def}}{=} \overline{out}.B_0^1$$

## Příklad: $B_0^2 \sim B_0^1|B_0^1$



## Věta

Pro všechna přirozená čísla  $n$ :  $B_0^n \sim \underbrace{B_0^1 | B_0^1 | \dots | B_0^1}_{n\text{-krát}}$

## Důkaz.

Sestrojíme následující binární relaci, kde  $i_1, i_2, \dots, i_n \in \{0, 1\}$ .

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

- $(B_0^n, B_0^1 | B_0^1 | \dots | B_0^1) \in R$
- $R$  je silná bisimulace



## Vlastnosti ~

- relace ekvivalence
- největší silná bisimulace
- kongruence
- dostatečná k dokázání některých přirozených pravidel, např.:
  - $P|Q \sim Q|P$
  - $P|Nil \sim P$
  - $(P|Q)|R \sim Q|(P|R)$
  - ...

## Vlastnosti ~

- relace ekvivalence
- největší silná bisimulace
- kongruence
- dostatečná k dokázání některých přirozených pravidel, např.:
  - $P|Q \sim Q|P$
  - $P|Nil \sim P$
  - $(P|Q)|R \sim Q|(P|R)$
  - ...

## Otázka

Měli bychom hledat dále???

## Otázka

Platí  $a.\tau.Nil \sim a.Nil$  ?



## Otázka

Platí  $a.\tau.Nil \sim a.Nil$  ? **NE!**

# Problém s vnitřními akcemi

## Otázka

Platí  $a.\tau.Nil \sim a.Nil$  ? **NE!**

## Problém

Silná bisimilarita neabstrahuje od  $\tau$  akcí.

# Problém s vnitřními akcemi

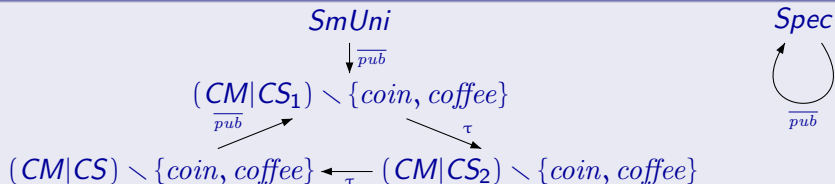
## Otázka

Platí  $a.\tau.Nil \sim a.Nil$  ? **NE!**

## Problém

Silná bisimilarita neabstrahuje od  $\tau$  akcí.

## Příklad: $SmUni \not\sim Spec$



# Problém s vnitřními akcemi

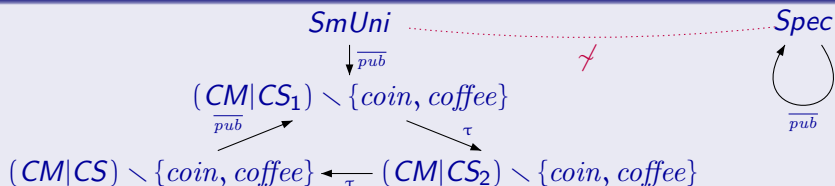
## Otázka

Platí  $a.\tau.Nil \sim a.Nil$  ? **NE!**

## Problém

Silná bisimilarita neabstrahuje od  $\tau$  akcí.

## Příklad: $SmUni \not\sim Spec$



# Slabá přechodová relace

Nechť  $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$  je LTS takový, že  $\tau \in Act$ .

## Definice slabé přechodové relace

$$\xRightarrow{a} = \begin{cases} (\xrightarrow{\tau})^* \circ \xrightarrow{a} \circ (\xrightarrow{\tau})^* & \text{pokud } a \neq \tau \\ (\xrightarrow{\tau})^* & \text{pokud } a = \tau \end{cases}$$

# Slabá přechodová relace

Nechť  $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$  je LTS takový, že  $\tau \in Act$ .

## Definice slabé přechodové relace

$$\xRightarrow{a} = \begin{cases} (\xrightarrow{\tau})^* \circ \xrightarrow{a} \circ (\xrightarrow{\tau})^* & \text{pokud } a \neq \tau \\ (\xrightarrow{\tau})^* & \text{pokud } a = \tau \end{cases}$$

Co  $s \xRightarrow{a} t$  znamená neformálně?

- Pokud  $a \neq \tau$ , pak  $s \xRightarrow{a} t$  znamená, že z  $s$  můžeme přejít do  $t$  provedením nuly nebo více  $\tau$  akcí, následovaných akcí  $a$ , následovanou nula nebo více  $\tau$  akcemi.
- Pokud  $a = \tau$ , pak  $s \xRightarrow{\tau} t$  znamená, že z  $s$  můžeme přejít do  $t$  provedením nuly nebo více  $\tau$  akcí.

# Slabá bisimilarita

Nechť  $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$  je LTS takové, že  $\tau \in Act$ .

## Slabá bisimulace (Weak Bisimulation)

Binární relace  $R \subseteq Proc \times Proc$  je **slabá bisimulace** (weak bisimulation) právě tehdy, když kdykoliv  $(s, t) \in R$  potom pro každé  $a \in Act$  (včetně  $\tau$ ):

- jestliže  $s \xrightarrow{a} s'$ , pak  $t \xRightarrow{a} t'$  pro nějaké  $t'$  takové, že  $(s', t') \in R$
- jestliže  $t \xrightarrow{a} t'$ , pak  $s \xRightarrow{a} s'$  pro nějaké  $s'$  takové, že  $(s', t') \in R$ .

# Slabá bisimilarita

Nechť  $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$  je LTS takové, že  $\tau \in Act$ .

## Slabá bisimulace (Weak Bisimulation)

Binární relace  $R \subseteq Proc \times Proc$  je **slabá bisimulace** (weak bisimulation) právě tehdy, když kdykoliv  $(s, t) \in R$  potom pro každé  $a \in Act$  (včetně  $\tau$ ):

- jestliže  $s \xrightarrow{a} s'$ , pak  $t \xRightarrow{a} t'$  pro nějaké  $t'$  takové, že  $(s', t') \in R$
- jestliže  $t \xrightarrow{a} t'$ , pak  $s \xRightarrow{a} s'$  pro nějaké  $s'$  takové, že  $(s', t') \in R$ .

## Slabá bisimilarita (Weak Bisimilarity)

Dva procesy  $p_1, p_2 \in Proc$  jsou **slabě bisimulačně ekvivalentní** (weakly bisimilar,  $p_1 \approx p_2$ ) právě tehdy, když existuje slabá bisimulace  $R$  tž.  $(p_1, p_2) \in R$ .

$$\approx = \cup \{R \mid R \text{ je slabá bisimulace}\}$$

Relaci  $\approx$  nazýváme **slabá bisimulační ekvivalence** nebo **slabá bisimilarita**.



## Definice

Stejná jako silná bisimulační hra

- obránce může nyní odpovědět využitím  $\xRightarrow{a}$  tahů.

Útočník nadále využívá jen  $\xrightarrow{a}$  tahy.

## Věta

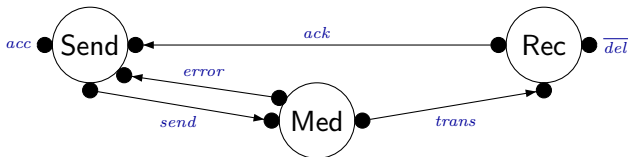
- Stav  $s$  a  $t$  jsou slabě bisimulačně ekvivalentní právě tehdy, když obránce má **univerzální vítěznou strategii** (universal winning strategy) ve slabé bisimulační hře z počáteční konfigurace  $(s, t)$ .
- Stav  $s$  a  $t$  nejsou slabě bisimulačně ekvivalentní právě tehdy, když útočník má **univerzální vítěznou strategii** ve slabé bisimulační hře z počáteční konfigurace  $(s, t)$ .

## Vlastnosti $\approx$

- je ekvivalence
- je největší slabá bisimulace
- platí s ní mnoho přirozených zákonů, např.
  - $a.\tau.P \approx a.P$
  - $P + \tau.P \approx \tau.P$
  - $a.(P + \tau.Q) \approx a.(P + \tau.Q) + a.Q$
  - $P + Q \approx Q + P$      $P|Q \approx Q|P$      $P + Nil \approx P$     ...
- silná bisimilarita je podmnožinou slabé bisimilarity ( $\sim \subseteq \approx$ )
- abstrahuje od  $\tau$  cyklů



# Případová studie: komunikační protokol



Send  $\stackrel{\text{def}}{=} acc.Sending$

Sending  $\stackrel{\text{def}}{=} \overline{send.Wait}$

Wait  $\stackrel{\text{def}}{=} ack.Send + error.Sending$

Rec  $\stackrel{\text{def}}{=} trans.Del$

Del  $\stackrel{\text{def}}{=} \overline{del.Ack}$

Ack  $\stackrel{\text{def}}{=} \overline{ack.Rec}$

Med  $\stackrel{\text{def}}{=} send.Med'$

Med'  $\stackrel{\text{def}}{=} \tau.Err + \overline{trans.Med}$

Err  $\stackrel{\text{def}}{=} \overline{error.Med}$

$$\text{Impl} \stackrel{\text{def}}{=} (\text{Send} \mid \text{Med} \mid \text{Rec}) \setminus \{\text{send}, \text{trans}, \text{ack}, \text{error}\}$$
$$\text{Spec} \stackrel{\text{def}}{=} \text{acc}.\overline{\text{del}}.\text{Spec}$$

Otázka

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

# Je slabá bisimilarita kongruence pro CCS?

## Věta

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

- $\alpha.P \approx \alpha.Q$  pro každou akci  $\alpha \in Act$
- $P|R \approx Q|R$  a  $R|P \approx R|Q$  pro každý CCS proces  $R$
- $P[f] \approx Q[f]$  pro každou funkci přejmenování  $f$
- $P \setminus L \approx Q \setminus L$  pro každou množinu návěstí  $L$ .

# Je slabá bisimilarita kongruence pro CCS?

## Věta

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

- $\alpha.P \approx \alpha.Q$  pro každou akci  $\alpha \in Act$
- $P|R \approx Q|R$  a  $R|P \approx R|Q$  pro každý CCS proces  $R$
- $P[f] \approx Q[f]$  pro každou funkci přejmenování  $f$
- $P \setminus L \approx Q \setminus L$  pro každou množinu návěstí  $L$ .

A co nedeterministická volba?

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

# Je slabá bisimilarita kongruence pro CCS?

## Věta

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

- $\alpha.P \approx \alpha.Q$  pro každou akci  $\alpha \in Act$
- $P | R \approx Q | R$  a  $R | P \approx R | Q$  pro každý CCS proces  $R$
- $P[f] \approx Q[f]$  pro každou funkci přejmenování  $f$
- $P \setminus L \approx Q \setminus L$  pro každou množinu návěstí  $L$ .

A co nedeterministická volba?

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

## Závěr

Slabá bisimilarita **není** kongruence pro CCS.