Příklad – buffer

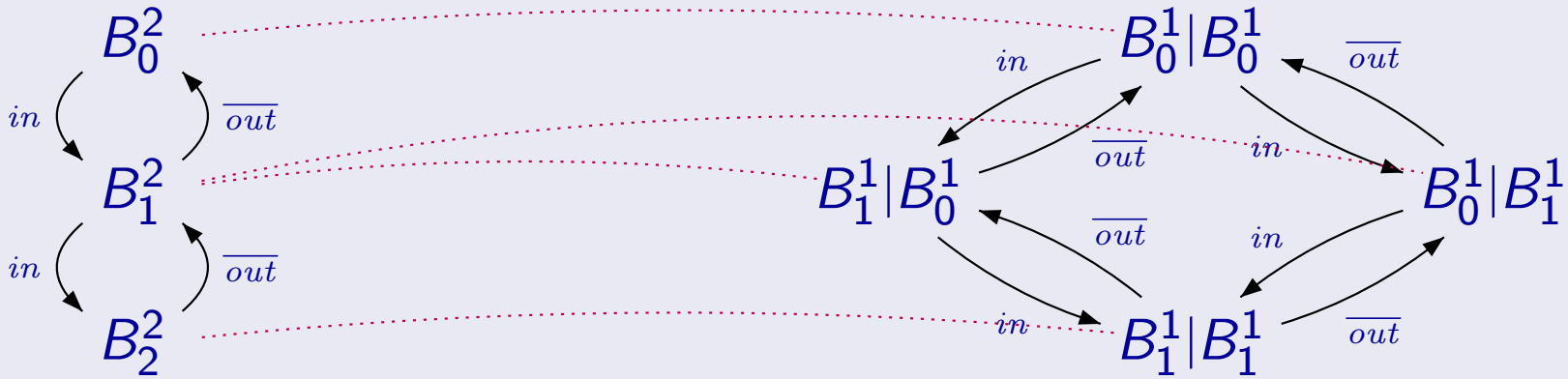
Buffer s kapacitou n

$$B_0^n \stackrel{\text{def}}{=} in.B_1^n$$
$$B_i^n \stackrel{\text{def}}{=} in.B_{i+1}^n + \overline{out}.B_{i-1}^n \quad \text{for } 0 < i < n$$
$$B_n^n \stackrel{\text{def}}{=} \overline{out}.B_{n-1}^n$$

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

Věta

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

Důkaz.

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

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

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

Silná bisimilarita – shrnutí

Vlastnosti $\sim$

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

Otázka

Měli bychom hledat dále???

Problém s vnitřními akcemi

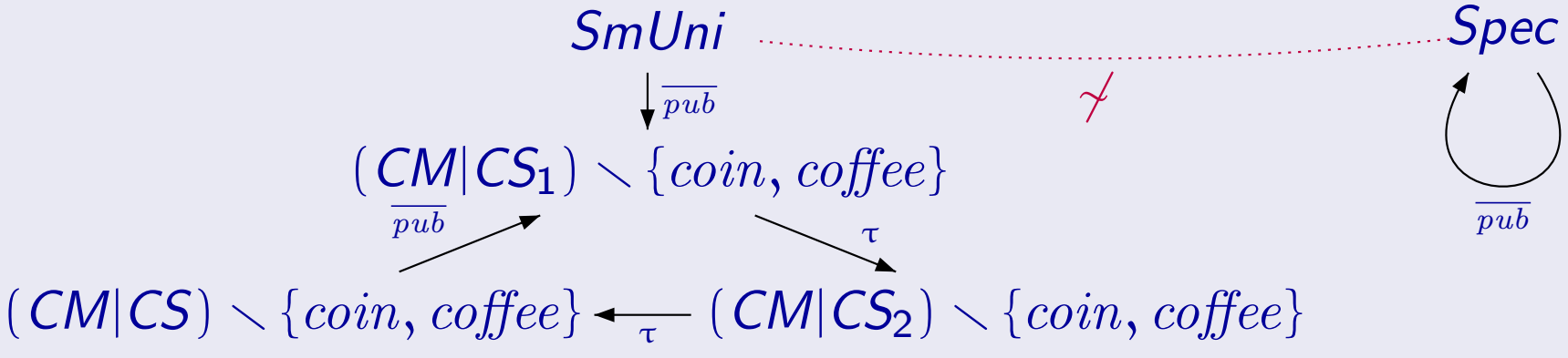
Otázka

Platí $a.\tau.Nil \sim a.Nil$? NE!

Problém

Silná bisimilarita neabstrahuje od τ akcí.

Příklad: SmUni $\not\sim$ Spec



Slabá přechodová relace

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

Definice slabé přechodové relace

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

Co $s \stackrel{a}{\Longrightarrow} t$ znamená neformálně?

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

Slabá bisimilarita

Nechť $(Proc, Act, \{\xrightarrow{a} | \ a \in Act\})$ 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 τ):

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

Slabá bisimulační hra

Definice

Stejná jako silná bisimulační hra

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

Útočník nadále využívá jen $\stackrel{a}{\longrightarrow}$ tahy.

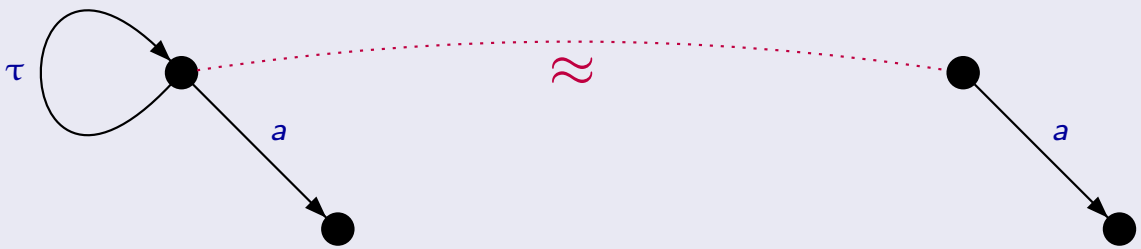
Věta

- Stavy 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).
- Stavy s a t nejsou slabě bisimulačně ekvivalentní právě tehdy, když útočník má univerzální vítěznou strategii ve slabé bisimulační hře z počáteční konfigurace (s, t).

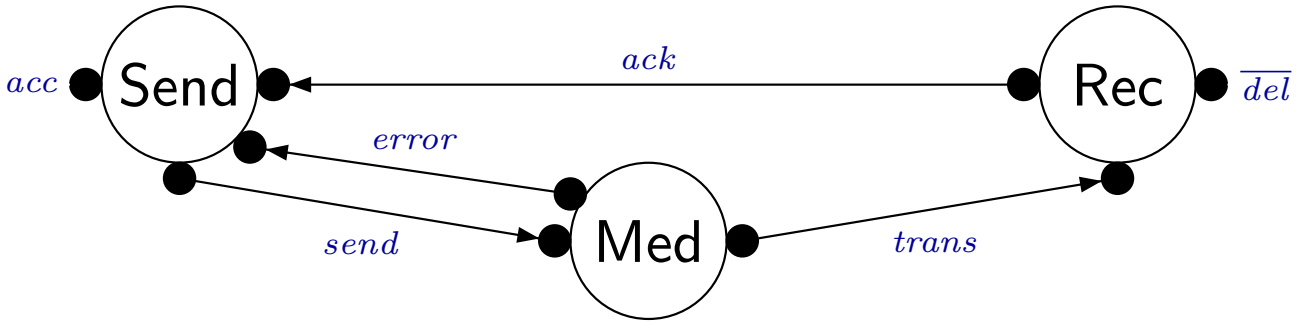
Slabá bisimilarita – vlastnosti

Vlastnosti $\approx$

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



Případová studie: komunikační protokol



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

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

Verifikační otázka

$$\mathsf{Impl} \stackrel{\text{def}}{=} (\mathsf{Send} \,|\, \mathsf{Med} \,|\, \mathsf{Rec}) \setminus \{\mathsf{send}, \mathsf{trans}, \mathsf{ack}, \mathsf{error}\}$$

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

Otázka

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

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 $\alpha \in Act$
- $P \mid R \approx Q \mid R$ a $R \mid P \approx R \mid Q$ 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 návěští 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.