

Modely konkurentných systémov

Formálne metódy tvorby softvéru

Damas Gruska

Katedra aplikovanej informatiky, I20, gruska@fmph.uniba.sk

Prednáška 2.

A Calculus of Communicating Systems, CCS

Proces Sender

$Sender \equiv in.\overline{send}.Nil$

Proces Sender

$Sender \equiv in.\overline{send}.Nil$

Proces Sender

$Sender \equiv in.\overline{send}.Nil$

$in.\overline{send}.Nil \xrightarrow{in} \overline{send}.Nil \xrightarrow{\overline{send}} Nil$

Proces Sender

$Sender \equiv in.\overline{send}.Nil$

$in.\overline{send}.Nil \xrightarrow{in} \overline{send}.Nil \xrightarrow{\overline{send}} Nil$

Proces Receiver

$Receiver \equiv send.\overline{out}.Nil$

Proces Sender

$$Sender \equiv in.\overline{send}.Nil$$
$$in.\overline{send}.Nil \xrightarrow{in} \overline{send}.Nil \xrightarrow{\overline{send}} Nil$$

Proces Receiver

$$Receiver \equiv send.\overline{out}.Nil$$

Proces Protokol

$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$

Proces Sender

$$Sender \equiv in.\overline{send}.Nil$$
$$in.\overline{send}.Nil \xrightarrow{in} \overline{send}.Nil \xrightarrow{\overline{send}} Nil$$

Proces Receiver

$$Receiver \equiv send.\overline{out}.Nil$$

Proces Protokol

$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$
$$Protokol \xrightarrow{in} \xrightarrow{\tau} \xrightarrow{\overline{out}}$$

Proces Sender

$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$

Proces Receiver

$$Receiver \equiv send.\overline{out}.Nil$$

Proces Protokol

$$Protokol' \equiv (Sender' | Receiver) \setminus \{send\}$$

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

ProtokolSpecifikacia $\equiv in.\tau.\overline{out}.Nil$

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$

Ktorý z procesov $Protokol$ a $Protokol'$ vyhovuje špecifikácii?

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$

Ktorý z procesov $Protokol$ a $Protokol'$ vyhovuje špecifikácii?

Formálnejšie: ktorý z procesov $Protokol$ a $Protokol'$ sa správa rovnako ako $ProtokolSpecifikacia$?

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$

Ktorý z procesov $Protokol$ a $Protokol'$ vyhovuje špecifikácii?

Formálnejšie: ktorý z procesov $Protokol$ a $Protokol'$ sa správa rovnako ako $ProtokolSpecifikacia$?

Pre obidva platí:

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$

Ktorý z procesov $Protokol$ a $Protokol'$ vyhovuje špecifikácii?

Formálnejšie: ktorý z procesov $Protokol$ a $Protokol'$ sa správa rovnako ako $ProtokolSpecifikacia$?

Pre obidva platí:

$Protokol \xrightarrow{in} \xrightarrow{\tau} \xrightarrow{\overline{out}}$

$Protokol' \xrightarrow{in} \xrightarrow{\tau} \xrightarrow{\overline{out}}$

Požadované správanie protokolu (špecifikácia) - urobiť akciu in , potom nejakú vnútornú akciu (τ) a potom akciu \overline{out} .

$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$

Ktorý z procesov $Protokol$ a $Protokol'$ vyhovuje špecifikácii?

Formálnejšie: ktorý z procesov $Protokol$ a $Protokol'$ sa správa rovnako ako $ProtokolSpecifikacia$?

Pre obidva platí:

$Protokol \xrightarrow{in} \xrightarrow{\tau} \xrightarrow{\overline{out}}$

$Protokol' \xrightarrow{in} \xrightarrow{\tau} \xrightarrow{\overline{out}}$

Znamená to, že obidva sa správajú rovnako ako $ProtokolSpecifikacia$?

Dva procesy sa správajú **rovnako**, ak to, čo vie urobiť jeden vie urobiť aj druhý a výsledné procesy sa opäť správajú **rovnako**.

Dva procesy sa správajú **rovnako**, ak to, čo vie urobiť jeden vie urobiť aj druhý a výsledné procesy sa opäť správajú **rovnako**.

Definition

Binárna relácia $S \subseteq CCS \times CCS$ je (silná) bisimulácia, ak $(P, Q) \in S$ implikuje

- 1) ak $P \xrightarrow{x} P'$ tak existuje Q' také, že $Q \xrightarrow{x} Q'$ a platí $(P', Q') \in S$
- 2) ak $Q \xrightarrow{x} Q'$ tak existuje P' také, že $P \xrightarrow{x} P'$ a platí $(P', Q') \in S$

Dva procesy sa správajú **rovnako**, ak to, čo vie urobiť jeden vie urobiť aj druhý a výsledné procesy sa opäť správajú **rovnako**.

Definition

Binárna relácia $S \subseteq CCS \times CCS$ je (silná) bisimulácia, ak $(P, Q) \in S$ implikuje

- 1) ak $P \xrightarrow{x} P'$ tak existuje Q' také, že $Q \xrightarrow{x} Q'$ a platí $(P', Q') \in S$
- 2) ak $Q \xrightarrow{x} Q'$ tak existuje P' také, že $P \xrightarrow{x} P'$ a platí $(P', Q') \in S$

Definition

Procesy P a Q sú silne bisimulárne ($P \sim Q$) ak $(P, Q) \in S$ pre nejakú silnú bisimuláciu S .

Ekvivalentná formulácia:

$$\sim = \bigcup \{ S \mid S \text{ je silná bisimulácia} \}$$

Theorem

$P \sim Q$ iff $\forall x \in Act$

- 1) ak $P \xrightarrow{x} P'$ tak existuje Q' také, že $Q \xrightarrow{x} Q'$ a platí $P' \sim Q'$
- 2) ak $Q \xrightarrow{x} Q'$ tak existuje P' také, že $P \xrightarrow{x} P'$ a platí $P' \sim Q'$

Sender \equiv *in.* $\overline{\text{send}}$.*Nil*

$$\text{Sender} \equiv in.\overline{send}.Nil$$
$$\text{Sender}' \equiv in.(\overline{send}.Nil + \tau.Nil)$$

$Sender \equiv in.\overline{send}.Nil$

$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$

$Receiver \equiv send.\overline{out}.Nil$

$$Sender \equiv in.\overline{send}.Nil$$
$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$
$$Receiver \equiv send.\overline{out}.Nil$$
$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$

$$Sender \equiv in.\overline{send}.Nil$$
$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$
$$Receiver \equiv send.\overline{out}.Nil$$
$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$
$$Protokol' \equiv (Sender'|Receiver) \setminus \{send\}$$

$$Sender \equiv in.\overline{send}.Nil$$
$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$
$$Receiver \equiv send.\overline{out}.Nil$$
$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$
$$Protokol' \equiv (Sender'|Receiver) \setminus \{send\}$$
$$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$$

$$Sender \equiv in.\overline{send}.Nil$$
$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$
$$Receiver \equiv send.\overline{out}.Nil$$
$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$
$$Protokol' \equiv (Sender'|Receiver) \setminus \{send\}$$
$$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$$

Platí $Protokol \sim ProtokolSpecifikacia$?

$$Sender \equiv in.\overline{send}.Nil$$

$$Sender' \equiv in.(\overline{send}.Nil + \tau.Nil)$$

$$Receiver \equiv send.\overline{out}.Nil$$

$$Protokol \equiv (Sender|Receiver) \setminus \{send\}$$

$$Protokol' \equiv (Sender'|Receiver) \setminus \{send\}$$

$$ProtokolSpecifikacia \equiv in.\tau.\overline{out}.Nil$$

Platí $Protokol \sim ProtokolSpecifikacia$?

Platí $Protokol' \sim ProtokolSpecifikacia$?

$Clock \equiv \mu X tick.X$

$Clock \equiv \mu X tick.X$

$Clock_1 \equiv \mu X tick.tick.X$

$$\text{Clock} \equiv \mu X \text{tick}.X$$
$$\text{Clock}_1 \equiv \mu X \text{tick}. \text{tick}.X$$
$$\text{Clock}_2 \equiv \mu X (\text{tick}. \text{tick}.X + \text{tick}.X)$$

$$Clock \equiv \mu X tick.X$$
$$Clock_1 \equiv \mu X tick.tick.X$$
$$Clock_2 \equiv \mu X (tick.tick.X + tick.X)$$
$$Clock_3 \equiv \mu X (tick.tick.X + tick.Nil)$$

$$Clock \equiv \mu X tick.X$$

$$Clock_1 \equiv \mu X tick.tick.X$$

$$Clock_2 \equiv \mu X (tick.tick.X + tick.X)$$

$$Clock_3 \equiv \mu X (tick.tick.X + tick.Nil)$$

Úloha: zistite, ktoré z horeuvedených procesov sú bisimulárne.

Definition

Binárna relácia $S \subseteq CCS \times CCS$ je silná bisimulácia až na \sim , ak $(P, Q) \in S$ implikuje

1) ak $P \xrightarrow{x} P'$ tak existuje Q' také, že $Q \xrightarrow{x} Q'$ a platí

$$(P', Q') \in \sim S \sim$$

2) ak $Q \xrightarrow{x} Q'$ tak existuje P' také, že $P \xrightarrow{x} P'$ a platí

$$(P', Q') \in \sim S \sim$$

Theorem

Ak S je silná bisimulácia až na \sim , potom $\sim S \sim$ je silná bisimulácia.

Theorem

Ak S je silná bisimulácia až na \sim , potom $\sim S \sim$ je silná bisimulácia.

Úloha: dokážte predchádzajúcu vetu.

Theorem

Ak S je silná bisimulácia až na \sim , potom $\sim S \sim$ je silná bisimulácia.

Úloha: dokážte predchádzajúcu vetu.

Theorem

Ak S je silná bisimulácia až na \sim tak , potom $S \subseteq \sim$.

Theorem

Ak S je silná bisimulácia až na \sim , potom $\sim S \sim$ je silná bisimulácia.

Úloha: dokážte predchádzajúcu vetu.

Theorem

Ak S je silná bisimulácia až na \sim tak, potom $S \subseteq \sim$.

Úloha: dokážte predchádzajúcu vetu.

Theorem

$$P + Q \sim Q + P$$

$$P + (Q + R) \sim (P + Q) + R$$

$$P + P \sim P$$

$$P + Nil \sim P$$

Theorem

$$\begin{aligned}P + Q &\sim Q + P \\P + (Q + R) &\sim (P + Q) + R \\P + P &\sim P \\P + Nil &\sim P\end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

Theorem

$$\begin{aligned}P + Q &\sim Q + P \\P + (Q + R) &\sim (P + Q) + R \\P + P &\sim P \\P + Nil &\sim P\end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

Theorem

$$P|Q \sim Q|P$$

$$P|(Q|R) \sim (P|Q)|R$$

$$P|Nil \sim P$$

$$P \setminus K \setminus L \sim P \setminus (K \cup L)$$

$$P[id] \sim P$$

$$P[f][f'] \sim P[f \circ f']$$

Theorem

$$P|Q \sim Q|P$$

$$P|(Q|R) \sim (P|Q)|R$$

$$P|Nil \sim P$$

$$P \setminus K \setminus L \sim P \setminus (K \cup L)$$

$$P[id] \sim P$$

$$P[f][f'] \sim P[f \circ f']$$

Úloha: dokážte predchádzajúcu vetu.

Theorem

Nech $P \equiv P_1|P_2|\dots|P_n$ potom

$$\begin{aligned} P &\sim \sum x.(P_1|P_2|\dots|P'_i|\dots|P_n), 1 \leq i \leq n, \text{ ak } P_i \xrightarrow{x} P'_i \\ &+ \sum \tau.(P_1|P_2|\dots|P'_i|\dots|P'_j|\dots|P_n), \\ &1 \leq i, j \leq n, \text{ ak } P_i \xrightarrow{a} P'_i, P_j \xrightarrow{\bar{a}} P'_j \end{aligned}$$

Theorem

Nech $P \equiv P_1|P_2|\dots|P_n$ potom

$$\begin{aligned} P &\sim \sum x.(P_1|P_2|\dots|P'_i|\dots|P_n), 1 \leq i \leq n, \text{ ak } P_i \xrightarrow{x} P'_i \\ &+ \sum \tau.(P_1|P_2|\dots|P'_i|\dots|P'_j|\dots|P_n), \\ &1 \leq i, j \leq n, \text{ ak } P_i \xrightarrow{a} P'_i, P_j \xrightarrow{\bar{a}} P'_j \end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

Theorem

Nech $P_1 \sim P_2$. Potom

$$x.P_1 \sim x.P_2$$

$$P_1 + Q \sim P_2 + Q$$

$$P_1|Q \sim P_2|Q$$

$$P_1 \setminus L \sim P_2 \setminus L$$

$$P_1[f] \sim P_2[f]$$

Theorem

Nech $P_1 \sim P_2$. Potom

$$\begin{aligned}x.P_1 &\sim x.P_2 \\P_1 + Q &\sim P_2 + Q \\P_1|Q &\sim P_2|Q \\P_1 \setminus L &\sim P_2 \setminus L \\P_1[f] &\sim P_2[f]\end{aligned}$$

Úloha: dokážte predchádzajúcu vetu.

Theorem

Nech $P_1 \sim P_2$. Potom

$$x.P_1 \sim x.P_2$$

$$P_1 + Q \sim P_2 + Q$$

$$P_1|Q \sim P_2|Q$$

$$P_1 \setminus L \sim P_2 \setminus L$$

$$P_1[f] \sim P_2[f]$$

Úloha: dokážte predchádzajúcu vetu.

Ako definovať bisimuláciu medzi termami?

Ako definovať bisimuláciu medzi termami?

Definition

Nech E a F sú CCS termy s jednou voľnou premennou X . Potom $E \sim F$ ak pre každý CCS proces P platí $E[P/X] \sim F[P/X]$

Ako definovať bisimuláciu medzi termami?

Definition

Nech E a F sú CCS termy s jednou voľnou premennou X . Potom $E \sim F$ ak pre každý CCS proces P platí $E[P/X] \sim F[P/X]$

Theorem

Nech $E \sim F$. Potom $\mu X E \sim \mu X F$.

Dôkaz:

Dôkaz:

Ukážeme, že $S = \{(G[P/X], G[Q/X])\}$

je silná bisimulácia až na \sim , kde G obsahuje len jednu voľnú premennú X a $P = \mu XE, Q = \mu XF$.

Bisimulácia ako kongruencia

Dôkaz:

Ukážeme, že $S = \{(G[P/X], G[Q/X])\}$

je silná bisimulácia až na \sim , kde G obsahuje len jednu voľnú premennú X a $P = \mu XE, Q = \mu XF$.

Potom zoberieme $G \equiv X$.

Dôkaz:

Ukážeme, že $S = \{(G[P/X], G[Q/X])\}$

je silná bisimulácia až na \sim , kde G obsahuje len jednu voľnú premennú X a $P = \mu XE, Q = \mu XF$.

Potom zoberieme $G \equiv X$.

Ukážeme, že:

Ak $G[P/X] \xrightarrow{x} P'$ tak existuje Q', Q'' také, že
 $G[Q/X] \xrightarrow{x} Q'', Q'' \sim Q', (P', Q') \in S$.

Dôkaz:

Ukážeme, že $S = \{(G[P/X], G[Q/X])\}$

je silná bisimulácia až na \sim , kde G obsahuje len jednu voľnú premennú X a $P = \mu XE, Q = \mu XF$.

Potom zoberieme $G \equiv X$.

Ukážeme, že:

Ak $G[P/X] \xrightarrow{x} P'$ tak existuje Q', Q'' také, že
 $G[Q/X] \xrightarrow{x} Q'', Q'' \sim Q', (P', Q') \in S$.

Indukciou podľa dĺžky odvodu a štruktúry termu G .

1. Nech $G \equiv X$.

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekurziu dostaneme $E[P/X] \xrightarrow{x} P'$,

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekurziu dostaneme $E[P/X] \xrightarrow{x} P'$,
čo je kratšie odvedenie a podľa indukčného predpokladu máme

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekurziu dostaneme $E[P/X] \xrightarrow{x} P'$,
čo je kratšie ododenie a podľa indukčného predpokladu máme
 $E[Q/X] \xrightarrow{x} Q''$ a $P'S \sim Q''$.

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekúziu dostaneme $E[P/X] \xrightarrow{x} P'$,
čo je kratšie odvodenie a podľa indukčného predpokladu máme
 $E[Q/X] \xrightarrow{x} Q''$ a $P'S \sim Q''$.

Z predpokladu $E \sim F$ dostaneme $F[Q/X] \xrightarrow{x} Q'$ a $Q' \sim Q''$

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekúziu dostaneme $E[P/X] \xrightarrow{x} P'$,
čo je kratšie odvodenie a podľa indukčného predpokladu máme
 $E[Q/X] \xrightarrow{x} Q''$ a $P'S \sim Q''$.

Z predpokladu $E \sim F$ dostaneme $F[Q/X] \xrightarrow{x} Q'$ a $Q' \sim Q''$
keďže

$$\frac{F[\mu XF/X] \xrightarrow{x} Q'}{\mu XF \xrightarrow{x} Q'}$$

a keďže $Q = \mu XF$ máme t.j. $Q \xrightarrow{x} Q'$.

Bisimulácia ako kongruencia

1. Nech $G \equiv X$.

Potom $G[P/X] \equiv P$ a teda $P \xrightarrow{x} P'$.

Z toho podľa pravidiel pre rekúziu dostaneme $E[P/X] \xrightarrow{x} P'$,
čo je kratšie odvodenie a podľa indukčného predpokladu máme
 $E[Q/X] \xrightarrow{x} Q''$ a $P'S \sim Q''$.

Z predpokladu $E \sim F$ dostaneme $F[Q/X] \xrightarrow{x} Q'$ a $Q' \sim Q''$
keďže

$$\frac{F[\mu XF/X] \xrightarrow{x} Q'}{\mu XF \xrightarrow{x} Q'}$$

a keďže $Q = \mu XF$ máme t.j. $Q \xrightarrow{x} Q'$.

Máme teda $Q \equiv G[Q/X] \xrightarrow{x} Q'$ a $P'S \sim Q'$

2. Nech $G \equiv x.G'$.

2. Nech $G \equiv x.G'$.

$G[P/X] \equiv x.G'[P/X]$ teda

2. Nech $G \equiv x.G'$.

$G[P/X] \equiv x.G'[P/X]$ teda

$G[P/X] \xrightarrow{x} G'[P/X]$

a

2. Nech $G \equiv x.G'$.

$G[P/X] \equiv x.G'[P/X]$ teda

$$G[P/X] \xrightarrow{x} G'[P/X]$$

a

$$G[Q/X] \xrightarrow{x} G'[Q/X]$$

2. Nech $G \equiv x.G'$.

$G[P/X] \equiv x.G'[P/X]$ teda

$$G[P/X] \xrightarrow{x} G'[P/X]$$

a

$$G[Q/X] \xrightarrow{x} G'[Q/X]$$

3. Nech $G \equiv G_1 + G_2$.

Každé odvodenie má kratšiu dĺžku a teda môžeme použiť indukčný predpoklad.

2. Nech $G \equiv x.G'$.

$G[P/X] \equiv x.G'[P/X]$ teda

$$G[P/X] \xrightarrow{x} G'[P/X]$$

a

$$G[Q/X] \xrightarrow{x} G'[Q/X]$$

3. Nech $G \equiv G_1 + G_2$.

Každé ododenie má kratšiu dĺžku a teda môžeme použiť indukčný predpoklad.

3. Nech $G \equiv G_1 | G_2$.

Potom $G[P/X] \equiv G_1[P/X] | G_2[P/X]$

Nech $G[P/X] \xrightarrow{x} P'$

S tri možnosti:

3. Nech $G \equiv G_1|G_2$.

Potom $G[P/X] \equiv G_1[P/X]|G_2[P/X]$

Nech $G[P/X] \xrightarrow{x} P'$

S tri možnosti:

1. $x = \tau$ a $G_1[P/X] \xrightarrow{a} P'_1$, $G_2[P/X] \xrightarrow{\bar{a}} P'_2$ a $P' \equiv P'_1|P'_2$

3. Nech $G \equiv G_1|G_2$.

Potom $G[P/X] \equiv G_1[P/X]|G_2[P/X]$

Nech $G[P/X] \xrightarrow{x} P'$

S tri možnosti:

1. $x = \tau$ a $G_1[P/X] \xrightarrow{a} P'_1$, $G_2[P/X] \xrightarrow{\bar{a}} P'_2$ a $P' \equiv P'_1|P'_2$

Podľa indukčného predpokladu

3. Nech $G \equiv G_1|G_2$.

Potom $G[P/X] \equiv G_1[P/X]|G_2[P/X]$

Nech $G[P/X] \xrightarrow{x} P'$

S tri možnosti:

1. $x = \tau$ a $G_1[P/X] \xrightarrow{a} P'_1$, $G_2[P/X] \xrightarrow{\bar{a}} P'_2$ a $P' \equiv P'_1|P'_2$

Podľa indukčného predpokladu

$G_1[Q/X] \xrightarrow{a} Q'_1$, $Q''_1 \sim Q'_1$, $(P'_1, Q'_1) \in S$

$G_2[Q/X] \xrightarrow{\bar{a}} Q'_2$, $Q''_2 \sim Q'_2$, $(P'_2, Q'_2) \in S$

$Q' \equiv Q'_1|Q'_2$, $Q'' \equiv Q''_1|Q''_2$

3. Nech $G \equiv G_1|G_2$.

Potom $G[P/X] \equiv G_1[P/X]|G_2[P/X]$

Nech $G[P/X] \xrightarrow{x} P'$

S tri možnosti:

1. $x = \tau$ a $G_1[P/X] \xrightarrow{a} P'_1$, $G_2[P/X] \xrightarrow{\bar{a}} P'_2$ a $P' \equiv P'_1|P'_2$

Podľa indukčného predpokladu

$G_1[Q/X] \xrightarrow{a} Q'_1$, $Q''_1 \sim Q'_1$, $(P'_1, Q'_1) \in S$

$G_2[Q/X] \xrightarrow{\bar{a}} Q'_2$, $Q''_2 \sim Q'_2$, $(P'_2, Q'_2) \in S$

$Q' \equiv Q'_1|Q'_2$, $Q'' \equiv Q''_1|Q''_2$

$G[Q/X] \equiv G_1[Q/X]|G_2[Q/X] \xrightarrow{\tau} Q''$, $Q'' \sim Q'$

Ostáva ukázať, že $(P'Q') \in S$.

Ostáva ukázať, že $(P'Q') \in S$.

Ale $(P'_i, Q'_i) \in S$ a teda pre nejaké H_i platí:

$P'_i \equiv H_i[P/X], Q'_i \equiv H_i[Q/X]$.

Ostáva ukázať, že $(P'Q') \in S$.

Ale $(P'_i, Q'_i) \in S$ a teda pre nejaké H_i platí:

$$P'_i \equiv H_i[P/X], Q'_i \equiv H_i[Q/X].$$

Zoberme $H \equiv H_1|H_2$ a potom

$$(P'Q') \equiv H_1[P/X]|H_2[Q/X] \in S.$$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

a. $X + Y$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

a. $X + Y$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

a. $X + Y$

X je strážené, Y nie je strážené

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

a. $X + Y$

X je strážené, Y nie je strážené

b. $(a.X + Y)$

Definition

X je slabo strážené v E ak každý výskyt X je vnútri nejakého podtermu tvaru $y.F$

a. $Nil|X$

X nie je strážené

a. $X + Y$

X je strážené, Y nie je strážené

b. $(a.X + Y)$

X, Y sú strážené

Lemma

Ak premenná X je slabo strážené v E a $E[P/X] \xrightarrow{x} P'$ potom $P' \equiv E'[P/X]$ a navyše pre každé Q platí $E[Q/X] \xrightarrow{x} E'[Q/X]$.

Lemma

Ak premenná X je slabo strážené v E a $E[P/X] \xrightarrow{x} P'$ potom $P' \equiv E'[P/X]$ a navyše pre každé Q platí $E[Q/X] \xrightarrow{x} E'[Q/X]$.

Úloha: dokážte predchádzajúcu Lemu.

Theorem

$$\mu XE \sim E[\mu XE/X]$$

Theorem

$$\mu XE \sim E[\mu XE/X]$$

Úloha: dokážte predchádzajúcu Lemu.

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Dôkaz

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Dôkaz

Stačí ukázať, že ak $P \sim E[P/X]$ a $Q \sim E[Q/X]$ potom $P \sim Q$.

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Dôkaz

Stačí ukázať, že ak $P \sim E[P/X]$ a $Q \sim E[Q/X]$ potom $P \sim Q$.
Ukážeme, že $S = \{(G[P/X], G[Q/X])\} \cup I_d$ je silná bisimulácia až na \sim .

T.j. ak $G[P/X] \xrightarrow{x} P'$ tak existuje Q' také, že
 $G[Q/X] \xrightarrow{x} Q'$ a $P' \sim S \sim Q'$.

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Dôkaz

Stačí ukázať, že ak $P \sim E[P/X]$ a $Q \sim E[Q/X]$ potom $P \sim Q$.
Ukážeme, že $S = \{(G[P/X], G[Q/X])\} \cup I_d$ je silná bisimulácia až na \sim .

T.j. ak $G[P/X] \xrightarrow{x} P'$ tak existuje Q' také, že
 $G[Q/X] \xrightarrow{x} Q'$ a $P' \sim S \sim Q'$.

Potom zoberieme za $G \equiv X$.

Theorem

*Nech premenná X je slabo strážené v E a platí $F \sim E[F/X]$.
Potom $F \sim \mu X E$.*

Dôkaz

Stačí ukázať, že ak $P \sim E[P/X]$ a $Q \sim E[Q/X]$ potom $P \sim Q$.
Ukážeme, že $S = \{(G[P/X], G[Q/X])\} \cup I_d$ je silná bisimulácia až na \sim .

T.j. ak $G[P/X] \xrightarrow{x} P'$ tak existuje Q' také, že
 $G[Q/X] \xrightarrow{x} Q'$ a $P' \sim S \sim Q'$.

Potom zoberieme za $G \equiv X$.

Indukciou podľa dĺžky odvodenia.

Nech $G \equiv X$.

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P'', P'' \sim P'$.

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P'', P'' \sim P'$.

Podľa a lemy $P'' \equiv E'[P/X]$ a

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P''$, $P'' \sim P'$.

Podľa a lemy $P'' \equiv E'[P/X]$ a

$E[Q/X] \xrightarrow{x} E'[Q/X]$

$\{ \quad \}$

$Q \xrightarrow{x} Q'$

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P'', P'' \sim P'$.

Podľa a lemy $P'' \equiv E'[P/X]$ a

$E[Q/X] \xrightarrow{x} E'[Q/X]$

$\{ \quad \}$

$Q \xrightarrow{x} Q'$

$G[Q/X] \xrightarrow{x} Q', Q' \sim E'[Q/X]$

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P'', P'' \sim P'$.

Podľa a lemy $P'' \equiv E'[P/X]$ a

$E[Q/X] \xrightarrow{x} E'[Q/X]$

$\{ \quad \}$

$Q \xrightarrow{x} Q'$

$G[Q/X] \xrightarrow{x} Q', Q' \sim E'[Q/X]$

$G[P/X] \xrightarrow{x} P' \sim E'[P/X]$

$G[Q/X] \xrightarrow{x} Q' \sim E'[Q/X]$

Nech $G \equiv X$.

Nech $G[P/X] \equiv P \xrightarrow{x} P'$.

Podľa predpokladu ($P \sim E[P/X]$) platí $E[P/X] \xrightarrow{x} P'', P'' \sim P'$.

Podľa a lemy $P'' \equiv E'[P/X]$ a

$E[Q/X] \xrightarrow{x} E'[Q/X]$

$\{ \quad \}$

$Q \xrightarrow{x} Q'$

$G[Q/X] \xrightarrow{x} Q', Q' \sim E'[Q/X]$

$G[P/X] \xrightarrow{x} P' \sim E'[P/X]$

$G[Q/X] \xrightarrow{x} Q' \sim E'[Q/X]$

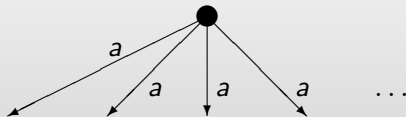
$(E'[P/X], E'[Q/X]) \in S$

Podmienka slabej stráženosti

$$X = a.Nil + X$$

Podmienka slabej stráženosti

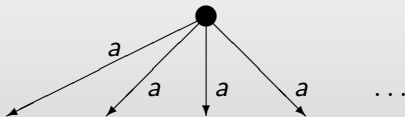
$$X = a.Nil + X$$



Obr.: Proces P_0

Podmienka slabej stráženosti

$$X = a.Nil + X$$

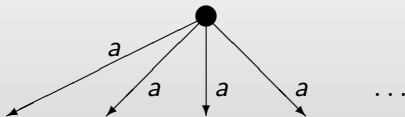


Obr.: Proces P_0

$P_0 + R$ je tiež riešenie pre každé R , lebo

Podmienka slabej stráženosti

$$X = a.Nil + X$$



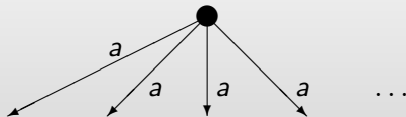
Obr.: Proces P_0

$P_0 + R$ je tiež riešenie pre každé R , lebo

$$P_0 + R = a.Nil + P_0 + R,$$

Podmienka slabej stráženosti

$$X = a.Nil + X$$



Obr.: Proces P_0

$P_0 + R$ je tiež riešenie pre každé R , lebo

$$P_0 + R = a.Nil + P_0 + R,$$

t.j. rovnica má nekonečne veľa riešení, ktoré nie sú navzájom bisumulárne.