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

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

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

Proces Receiver

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

Proces Protokol

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

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

Úlohy

2. Napíšte strom odvodenia priecestie.
pozastáva z troch procesov: Cesta, Zeleznica, Signály
akcie:
auto, *vlak* - blíži sa auto, vlak
hore, *dolu* - pohyb rámp
akrizuje, *vkrizuje* - auto, vlak križuje priecestie
závory sú stále dole, až kým sa neblíži auto

$Cesta = auto.hore.\overline{akrizuje}.\overline{dole}.Cesta$
$Zeleznica = vlak.zelena.\overline{vkrizuje}.\overline{cervena}.Zeleznica$
$Signaly = \overline{zelna}.cervena.Signaly + \overline{hore}.dole.Signaly$
$Priecestie \equiv$
$(Cesta|Zeleznica|Signaly) \setminus \{zelena, cervena, hore, dole\}$

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 $\overline{out}$.

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

Ktorý z procesov *Protokol* a *Protokol′* vyhovuje špecifikácií?

Formálnejšie: ktorý z procresov *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*?

Ekvivalencie

$a.Nil + a.Nil$ vs. $a.Nil$

$(a.Nil) \setminus \{a\}$ vs. Nil

$a.(b.Nil + c.Nil)$ vs. $a.b.Nil + a.c.Nil$

$a.b.Nil + b.a.Nil$ vs $a.Nil|b.Nil$

Porovnanie procesov:

- pozorovateľ nevidí syntax (to jest popis procesu)

- black box scénar

- ak nevie rozlíšiť medzi dvoma procesmi, tak ich považuje za ekvivalentné

- rôzne možnosti pozorovateľa vedú k rôznym ekvivalenciam medzi procesmi

Bisimulácia

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

Poznámka - aj prázdna relácia je bisimulácia.

Úloha: napíšte, ak existuje, bisimuláciu obsahujúcu dvojice
$a.Nil + a.Nil$ a $a.Nil$
$(a.Nil) \setminus \{a\}$ a Nil
$a.(b.Nil + c.Nil)$ a $a.b.Nil + a.c.Nil$
$a.b.Nil + b.a.Nil$ a $a.Nil|b.Nil$

Bisimulácia

Označenie:

$S^{-1} = \{(y, x) | (x, y) \in S\}$
$S_1 S_2 = \{(x, z) | \exists y, (x, y) \in S_1, (y, z) \in S_2\}$
I_d - identická relácia t.j. $I_d = \{(x, x) | \forall x\}$

Theorem

Nech S_1, S_2 sú silné bisimulácie. Potom aj nasledovné relácie sú silné bisimulácie
1) I_d
2) S^{-1}
3) $S_1 S_2$
4) $S_1 \cup S_2$

Úloha: dokážte predchádzajúcu vetu.

Bisimulácia

Definition

Procesy P a Q sú silne bisimulárne ($P \sim Q$) ak $(P, Q) \in S$ pre nejakú silnú bisimuláciu S.
Ekvivalentná formulácia:
$\sim = \bigcup\{S | S \text{ je silná bisimulácia } \}$

Theorem

$\sim$ *je najväčšia silná bisimulácia*
$\sim$ *je ekvivalencia*

Úloha: dokážte predchádzajúcu vetu.

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

Platí $Protokol \sim ProtokolSpecifikacia$?
Platí $Protokol' \sim ProtokolSpecifikacia$?

Bisimulácia

$Clock \equiv \mu X tick.X$

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

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

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

Úloha: zistite, ktoré z horeuvedených procesov sú bisimulárne.

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* $P' \sim Q'$

Úloha: dokážte predchádzajúcu vetu.

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

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 $\sim$ tak , potom $S \subseteq \sim$.

Úloha: dokážte predchádzajúcu vetu.

Bisimulácia

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.

Bisimulácia

Theorem

$$
\begin{aligned}
P|Q &\sim Q|P \\
P|(Q|R) &\sim (P|Q)|R \\
P|Nil &\sim P \\
P \setminus K \setminus L &\sim P \setminus (K \cup L) \\
P[i_d] &\sim P \\
P[f][f'] &\sim P[f \circ f']
\end{aligned}
$$

Úloha: dokážte predchádzajúcu vetu.

Expanzný zákon

Theorem

Nech $P \equiv P_1|P_2|\ldots|P_n$ *potom*

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

Úloha: dokážte predchádzajúcu vetu.

Bisimulácia ako kongruencia

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.

Bisimulácia ako kongruencia

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 $\mu XE \sim \mu XF$.

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 $G \equiv X$.
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 odvodenia a štruktúry termu G.

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 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 $Q' \sim Q''$
kedže

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

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

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

Bisimulácia ako kongruencia

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.

Bisimulácia ako kongruencia

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
$G_1[Q/X] \xrightarrow{a} Q'_1$, $Q''_1 \sim Q'_1, (P'_1, Q'_1) \in S$
$G_2[Q/X] \xrightarrow{a} Q'_2$, $Q''_2 \sim Q'_2, (P'_2, Q'_2) \in S$
$Q' \equiv Q'_1|Q'_2$, $Q'' \equiv Q''_1|Q''_2$

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

Bisimulácia ako kongruencia

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

Bisimulácia, jednoznačnosť riešenia

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

Bisimulácia, jednoznačnosť riešenia

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.

Bisimulácia

Theorem

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

Úloha: dokážte predchádzajúcu Lemu.

Bisimulácia

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.

Bisimulácia

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

$$\begin{array}{ccc} E[Q/X] & \xrightarrow{x} & E'[Q/X] \\ \wr & & \wr \\ Q & \xrightarrow{x} & Q' \end{array}$$

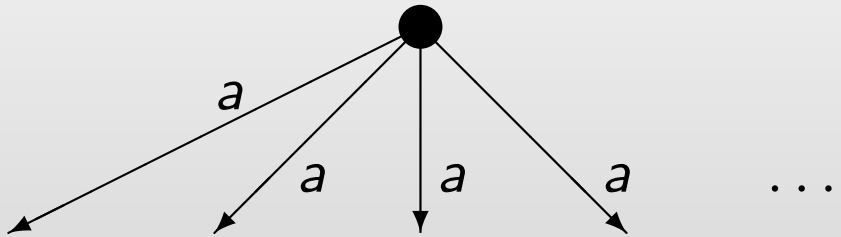
$G[Q/X] \xrightarrow{x} Q', Q' \sim E'[Q/X]$

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

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

Podmienka slabej stráženosti

$X = a.Nil + X$



Obrázok: 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.