

# Modely konkurentných systémov

## Formálne metódy tvorby softvéru

Damas Gruska

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

Prednáška 1.

## Organizácia kurzu

Budete dostávať domáce úlohy, ich odovzdanie je povinné v termíne do najbližšej prednášky. Toleruje sa max jedna úloha odovzdaná po termíne.

Cvičenia budú pre tých, ktorí mali problém s úlohou alebo si nie sú istí, či majú dobre vyriešenú úlohu.

Dva testy počas semestra: prvý v polovici, druhý v poslednom týždni semestra.

Na testoch nebudú povolené poznámky.

Testy budem opravovať až na skúške a budú tvoriť jej jadro.

Kto nebude písať test cez semester bude ho musieť písať v čase skúšky.

Známku 'vychádzajúcu' z testu si možno opraviť na skúške.

## Organizácia kurzu

"Prednášky" (to čo budem premietat') bude na mojej web stránke.

Tieto poznámky nie sú určené na samoštúdium!!!

## O čom bude reč:

Formálne metódy = na matematike založené techniky na špecifikáciu, vývoj a verifikáciu softvérových a hardvérových systémov.

Dôraz na modely a metódy pre systémy konkurentné a paralelné.

Procesové algebry, Petriho siete, logické špecifikačné nástroje.

## Procesové algebry

C.A.R.Hoare

Communicating Sequential Processes, skrátene CSP, 1978

Hoare C. A. R.: *Communicating sequential processes*. Prentice-Hall International Series In Computer Science, 1985.

R. Milner

A Calculus of Communicating Systems, skrátene CCS, 1980

Milner R.: *Communication and concurrency*. Prentice-Hall International, New York, 1989.

J.A. Bergstra a J.W. Klop

Algebra of Communicating Processes, skrátene ACP, 1985

Baeten J.A., W.P. Weijland: *Process Algebra*. Cambridge University Press, 1990.

## Procesové algebry

C.A.R.Hoare

**Communicating Sequential** Processes, skrátene CSP, 1978

Hoare C. A. R.: *Communicating sequential processes*. Prentice-Hall International Series In Computer Science, 1985.

R. Milner

A Calculus of **Communicating** Systems, skrátene CCS, 1980

Milner R.: *Communication and concurrency*. Prentice-Hall International, New York, 1989.

J.A. Bergstra a J.W. Klop

Algebra of **Communicating** Processes, skrátene ACP, 1985

Baeten J.A., W.P. Weijland: *Process Algebra*. Cambridge University Press, 1990.

# Ďalšie procesové algebry a na nich založené jazyky

Ambient calculus, 1998, L. Cardelli and A. D. Gordon

Pi-calculus, 1999, R. Milner, J. Parrow and D. Walker

... časové, pravdepodobnostné, stochastické PA, iné komunikačné mechanizmy, lokality, ...

Jazyky odvodené z procesových algebier alebo využívajúcich procesové algebry (či ich filozofiu) ako svoj základ:

- Wrightm (CSP,
- Timed Communicating Object Z (Object-Z a Timed CSP),
- Circus (CSP a Z),
- CspCASL(CSP),
- Ease (CSP),
- Occam (CSP),
- JCSP (CSP a Occam),
- C++CSP (CSP)

Petriho siete:

J.L. Peterson, Petri Net Theory and the Modeling of Systems.  
Prentice Hall, 1981.

W. Reisig, A Primer in Petri Net Design. Springer-Verlag, 1992.

Logika:

C. Stirling, Modal and Temporal Properties of Processes.  
Springer-Verlag, 2001.



# A Calculus of Communicating Systems, CCS

Daná množina atomických akcií  
(mien, komunikačných kanálov, ...)  $A$

Ku každej akcii existuje komplementárna akcia  $\bar{a}, \bar{b}, \bar{c}, \dots$

$$\bar{\bar{a}} = a$$

Jedna interpretácia:  $\bar{a}$  znamená poslanie správy cez kanál  $a$   
(výstupná akcia) a  $a$  znamená prijatie správy cez kanál  $a$  (vstupná akcia).

Množina všetkých  $Act = A \cup \bar{A} \cup \{\tau\}$  kde  $\tau$  je špeciálna (interná) akcia nevyskytujúca sa v  $A$ .

Prvky z  $A \cup \bar{A}$  budeme označovať  $a, b, c, \dots$

Prvky z  $Act$  budeme označovať  $x, y, z, \dots$

# CCS, neformálny úvod

*Nil* - proces, ktorý nerobí nič

*a.Nil* - proces, ktorý vie urobiť akciu *a* a potom sa správa ako proces *Nil*

*b.a.Nil* - proces, ktorý vie urobiť akciu *b* a potom sa správa ako proces *a.Nil*

$b.a.Nil \xrightarrow{b} a.Nil \xrightarrow{a} Nil$

*a.Nil + b.Nil* - proces, ktorý vie urobiť akciu *a* a potom sa správa ako proces *Nil* alebo akciu *b* a potom sa správa ako proces *Nil*

*c.(a.Nil + b.Nil)* - proces, ktorý vie urobiť akciu *c* a potom sa správa ako proces *(a.Nil + b.Nil)*

$c.(a.Nil + b.Nil) \xrightarrow{c} a.Nil + b.Nil$

# CCS, neformálny úvod

$a.Nil|b.Nil$  - proces, ktorý vie urobiť buď akciu  $a$  a potom sa správa ako proces  $Nil|b.Nil$  **alebo** akciu  $b$  a potom sa správa ako proces  $a.Nil|Nil$

$$a.Nil|b.Nil \xrightarrow{a} Nil|b.Nil \xrightarrow{b} Nil|Nil$$

$$a.Nil|b.Nil \xrightarrow{b} a.Nil|Nil \xrightarrow{a} Nil|Nil$$

$a.Nil|\bar{a}.Nil$  - proces, ktorý vie urobiť buď akciu  $a$  a potom sa správa ako proces  $Nil|\bar{a}.Nil$  **alebo** akciu  $\bar{a}$  a potom sa správa ako proces  $a.Nil|Nil$  **alebo** akciu  $\tau$  a potom sa správa ako  $Nil|Nil$

$\tau$  predstavuje v tomto prípade internú komunikáciu cez kanál  $a$

$$a.Nil|\bar{a}.Nil \xrightarrow{a} Nil|\bar{a}.Nil \xrightarrow{\bar{a}} Nil|Nil$$

$$a.Nil|\bar{a}.Nil \xrightarrow{\bar{a}} a.Nil|Nil \xrightarrow{a} Nil|Nil$$

$$a.Nil|\bar{a}.Nil \xrightarrow{\tau} Nil|Nil$$

Úlohy:

1. aký je rozdiel medzi:

a)  $a.Nil$  a  $a.Nil + a.Nil$ ?

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

c)  $a.Nil|b.Nil$  a  $a.b.Nil + b.a.Nil$ ?

d)  $a.Nil|a.Nil$  a  $a.Nil$ ?

e)  $a.Nil|a.Nil$  a  $a.a.Nil + a.a.Nil$ ?

2. Napíšte proces, ktorý reprezentuje hodiny, ktoré vedia:

a) raz tiknúť (akcia *tick*) a skončia,

b) tri razy tiknúť (akcia *tick*) a skončia,

c) raz alebo tri razy tiknúť (akcia *tick*) a skončia.

3. Napíšte proces pozostávajúci z dvoch paralelne bežiacich procesov, kde jeden vie prijať niečo z kanálu *in* a pošle to do kanálu *send*. Druhý vie prijať niečo z kanálu *send* a poslať to na kanál *out*.

$$(a.Nil + b.Nil) \xrightarrow{a} Nil$$

$$(a.Nil + b.Nil) \xrightarrow{b} Nil$$

$(a.Nil + b.Nil) \setminus \{a\}$  vie urobiť len akciu b - akcia a je zakázaná

$$(a.Nil + b.Nil) \setminus \{a\} \xrightarrow{b} Nil$$

$$(a.Nil + b.Nil) \setminus \{a\} \not\xrightarrow{a}$$

Použitie:

nech  $P = a.Nil$ ,  $Q = \bar{a}.Nil$  - v procese  $P|Q$  môže P komunikovať s Q cez kanál a ale nemusí - cez tento kanál môže procesu P poslať správu aj niekto iný.

$$(P|Q) \setminus \{a\} \xrightarrow{\tau} Nil|Nil$$

$$(P|Q) \setminus \{a\} \not\xrightarrow{a}$$

Zatiaľ máme len konečné procesy.

$Clock = tick.Clock$

Nekonečný proces ako riešenie rovnice  $X = tick.X$

Budeme ho značiť ako  $\mu X tick.X$

Úloha:

a) napíšte proces reprezentujúci hodiny, ktoré idú bezchybne alebo raz tiknú naposledy.

b) napíšte systém pozostávajúci z procesu  $K$  a hodín, ktoré môžu ísť bezchybne alebo im proces  $K$  pošle signál na zastavenie. Pričom nikto iný im takýto signál nemôže poslať.



Dané *Act* a procesové premenné  $X, Y, Z, \dots$

Množina CCS termov:

$P ::=$	$Nil$	prázdny proces
	$X$	procesová premenná
	$x.P$	$x \in Act$ operácia prefixu
	$P + Q$	nedeterministický výber $P$ alebo $Q$
	$P   Q$	paralelná kompozícia
	$P \setminus L$	reštrikcia $L \subseteq A$
	$P[f]$	premenovanie funkciou $f : A \rightarrow A$
	$\mu X P$	rekurzia $X$ je procesová premenná

Premonovávacia funkcia:  $f : Act \rightarrow Act$  taká, že  
 $f(\bar{a}) = \overline{f(a)}$ ,  $f(\tau) = \tau$ .

Zátvorkovanie - konvencia: silnejšie viažu reštrikcia, premenovanie, prefix, paralelná kompozícia a sumácia

$R + a.P|b.Q \setminus L$  znamená  $R + ((a.P))|(b.(Q \setminus L))$

Monožina CCS procesov - uzavrené CCS termy (budeme ju značiť CCS).

Uzáverový operátor je  $\mu X$ .

Príklad:

$a.X, b.X|b.Nil$  - otvorené termy

$\mu X a.X, \mu X (b.X|b.Nil)$  uzavrené termy - t.j. procesy

$\mu Y a.X$  - otvorený term

# Značkové prechodové systémy

Značkový prechodový systém je trojica  $(S, \rightarrow, \Lambda)$  kde  $S$  je množina stavov,  $\Lambda$  je množina značiek a  $\rightarrow \subseteq S \times \Lambda \times S$ .

Ak  $p, q \in S$  a  $\alpha \in \Lambda$  tak miesto  $(p, \alpha, q) \in \rightarrow$  budeme písať  $p \xrightarrow{\alpha} q$ .

Príklady množiny značiek: inštrukcie programu, vstupy alebo výstupy, množina odpálených prechodov pri Petriho sietiach, splnené podmienky, plynutie času atď.

Vlastnosti: nástroj pre definovanie operačnej sémantiky iných modelov, veľmi jednoduchý, neobsahuje žiadne konštruktory, priama súvislosť s Kripkeho štruktúrou

Značkový prechodový systém

Množina stavov - množina procesov  $CCS$

Množina značiek -  $Act$

Ostáva definovať množinu  $\rightarrow \subseteq CCS \times Act \times CCS$

$$\frac{}{x.P \xrightarrow{x} P}$$

$$\frac{P \xrightarrow{x} P'}{P + Q \xrightarrow{x} P', Q + P \xrightarrow{x} P'}$$

$$\frac{P \xrightarrow{u} P'}{P | Q \xrightarrow{u} P' | Q, Q | P \xrightarrow{u} Q | P'}$$

$$\frac{P \xrightarrow{a} P', Q \xrightarrow{\bar{a}} Q'}{P | Q \xrightarrow{\tau} P' | Q'}$$

$$\frac{P \xrightarrow{x} P'}{P \setminus L \xrightarrow{x} P' \setminus L}, (x, \bar{x} \notin L)$$

$$\frac{P \xrightarrow{x} P'}{P[f] \xrightarrow{f(x)} P'[f]}$$

$$\frac{P[\mu XP/X] \xrightarrow{x} P'}{\mu XP \xrightarrow{x} P'}$$

$$a.(b.c.Nil + c.(d.Nil + c.Nil)) \xrightarrow{a} (b.c.Nil + c.(d.Nil + c.Nil)) \\ \xrightarrow{b} c.Nil \xrightarrow{c} Nil$$

$$a.(b.c.Nil + c.(d.Nil + c.Nil)) \xrightarrow{a} (b.c.Nil + c.(d.Nil + c.Nil)) \\ \xrightarrow{c} (d.Nil + c.Nil) \xrightarrow{d} Nil$$

$$a.(b.c.Nil + c.(d.Nil + c.Nil)) \xrightarrow{a} (b.c.Nil + c.(d.Nil + c.Nil)) \\ \xrightarrow{c} (d.Nil + c.Nil) \xrightarrow{c} Nil$$

$$\mu X a.X \xrightarrow{a} \mu X a.X \xrightarrow{a} \mu X a.X \xrightarrow{a} \dots$$

Strom odvodenia pre proces  $P$  - značený orientovaný graf s vrcholom  $P$

hrana označená  $x$  vedie z  $R$  do  $Q$  ak  $R \xrightarrow{x} Q$ .

Úloha

Napíšte stromy odvodenia pre procesy:

1.  $(a.(b.Nil + c.Nil))$
2.  $(a.(b.Nil|c.Nil))$
3.  $(a.(b.Nil + c.Nil) \setminus \{b\})$
4.  $(a.(b.Nil|\bar{b}.Nil))$
5.  $(a.(b.Nil|\bar{b}.Nil) \setminus \{b\})$
6.  $\mu X(a.X + b.X + c.Nil)$
7.  $\mu X(X|a.Nil)$

1. Napíšte procesy popisujúce automat na predaj napojov:  
vie prijať mincu (akcia coin)  
dá sa na ňom stlačiť tlačítka tea alebo coffee  
vydá tea alebo coffee  
Napíšte používateľa, ktorý si vyberá medzi tea a coffee a takého,  
čo pije len kávu.



2. Napíšte strom odvedenia 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

$Cesta = auto.\overline{hore}.\overline{akrizuje}.\overline{dole}.Cesta$

$Zeleznica = vlak.\overline{zelena}.\overline{vkrizuje}.\overline{cervena}.Zeleznica$

$Signaly = zelna.\overline{cervena}.Signaly + hore.\overline{dole}.Signaly$

$Priecestie \equiv$

$(Cesta|Zeleznica|Signaly) \setminus \{zelena, cervena, hore, dole\}$

$a.Nil + a.Nil$  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 je popis procesu)
- black box scénár
- ak nevie rozlíšiť medzi dvoma procesmi, tak ich považuje za ekvivalentné
- rôzne možnosti pozorovateľa vedú k rôznym ekvivalenciám medzi procesmi

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  $a.Nil|b.Nil$

Označenie:

$$S^{-1} = \{(y, x) | (x, y) \in S\}$$

$$S_1 S_2 = \{(x, z) | \exists y, (x, y) \in S_1, (y, z) \in S_2\}$$

$$I_d - \text{identická relácia t.j. } I_d = \{(x, x) | \forall x\}$$

## 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.

## 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

$\sim$  je najväčšia silná bisimulácia

$\sim$  je ekvivalencia

Úloha: dokážte predchádzajúcu vetu.

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