Párhuzamos folyamatok II.

Horváth Zoltán

Eötvös Loránd, Tudományegyetem
Általános Számítástudományi Tanszék
E-mail: hz@inf.elte.hu

Folyamatok algebrai elemzése

Témakörök: - általános algebrai ismeretek

- algebrai nyelvek jellemzõi

- példák: CSP, CCS

- implementációs eszközök: ARATools (Lotos)

Megközelítés:

- mûveleti (cimkézett állapotátmenet rendszerek)
- leíró
- axiomatikus szemantika

Cimkézett állapotátmenetrendszerek

Mgj.: Forrás könyv: Hennessy: Algebric Theory Process/

D.: • /LTS(C,A,$\rightarrow$)/

C - konfiguráció A - esemény

$\rightarrow$ - átmenet $\rightarrow \subseteq$ C $\times$ A $\times$ C

c $\xrightarrow{a}$ c', $<$c,a,c'$>\in\rightarrow$ $\{\xrightarrow{a} \subseteq$ C $\times$ C $|$ a $\in$A$\}$

Jelölés: $\cup\{\xrightarrow{a}$ $|$ a $\in$A$\}\simeq\rightarrow$ /környezet eldönti/

c $\rightarrow$ c' ::= $\exists$ a $\in$A: c $\xrightarrow{a}$ c'

$c \xrightarrow{a}$ ::= $\exists$ c'$\in$C: $c \xrightarrow{a}$ c'

c $\not\to$ ::= $\nexists$ c'$\in$C: c $\to$ c'. ($\nexists$a)

$\to$* $\subseteq$ C $\times$ A* $\times$ C /tranzitív lezárt/

(c, ε, c)$\in\to$*

Ha (c,a,c')$\in\to$ és (c',s,c'')$\in\to$*,
akkor (c,as,c'')$\in\to$*, ahol a$\in$A, s$\in$A*.

C $\times$ C felett $\to$* a $\to$ reflexív, tranzitív lezártja.

Ált.: C definíciója induktív (nyelvtan)

$\rightarrow$ definíciója struktúrális indukcióval adott. Ekkor struktúrális mûveleti szemantikát adtunk meg.

Pl.: A; P - folyamat kif.

$p ::= nil \mid ap \mid p+q \qquad a \in A;\ p,q \in P;$

$+$: nem determinisztikus választás ($\sim$ szelektív várakozás)

/**Levezetési szabályok (**$\rightarrow_1$definíciója)**:**/

(1) ap $\xrightarrow{a}_1$p /az ap összetett konfiguráció, az a esemény után p-ként viselkedik./

(2) $\dfrac{\text{p} \xrightarrow{a}_1 \text{p'}}{\text{p+q} \xrightarrow{a}_1 \text{p'}}$ /Ha p az a után p'-ként viselkedik, akkor p+q az a után tud p'-ként viselkedni./

(3) $\dfrac{\text{p} \xrightarrow{a}_1 \text{p'}}{\text{q+p} \xrightarrow{a}_1 \text{p'}}$

A nil-re nincs levezetési szabály, mert nem kezdeményez eseményt.

<u>D.:</u> *Folyamat és környezete*

(p,e) $\in$ P $\times$ P   p $\|$ e: $\quad \dfrac{p \xrightarrow{a}_1 p' \quad e \xrightarrow{a}_1 e'}{p \parallel e \xrightarrow{a}_2 p' \parallel e'}$

Specifikációs módszer: "e" megadása (absztrakció).

<u>D.:</u> *p megfelel e környezetnek*, ha

$\forall$ e',p': p $\|$ e $\rightarrow_2^*$ p' $\|$ e'$\not\rightarrow_2$: e'=nil

Minden esetben, ha elakad a "lebontás" e'=nil kell legyen.

D.: *Ekvivalencia:*

p equ q ($p \equiv q$), ha $\forall$ e:: p megfelel e-nek $\Leftrightarrow$ q megfelel e-nek

Mgj.: - erõs megkötés

- itt a folyamat jelentése a tesztfolyamatok halmaza.

- megszorítás utáni ekvivalencia használható.

II. *Leíró szemantika*

Mgj.: - Nem lépésenként hasonlítom.

- Egyszerre elvileg egy képet kapok, és az alapján döntök.

D.: $\mathcal{P}$(A*) trace (történet !)

(lineáris szerkezet, elemi események sorozatainak halmaza)

τ: P $\rightarrow$ $\mathcal{P}$(A*) /- szemantikus leképezés/

/P - folyamat./

Szabályok:

(1) τ[[nil]] = $\{\varepsilon\}$ (#)

(2) τ[[ap]] = a τ[[p]]

- $\forall$ olyan sorozat, amit "p" produkál és "a" van az elején.

(3) τ[[p+q]] = τ[[p]] $\cup$ τ[[q]] /- τ homomorfizmus/

- aT = $\{$at | t$\in$T$\}$, T$\subseteq$A*

Mgj.: I. és II. nem egyenlõ és egyik sem szigorúbb a másiknál.

Kérdés: A két szemantika azonos-e?

$$\left(\mathsf{p}_1 \equiv \mathsf{p}_2 \overset{?}{\Leftrightarrow} \tau(\mathsf{p}_1)=\tau(\mathsf{p}_2)\right)$$

/Válasz: nem/

D.: $\mathcal{O}$: $\mathsf{P} \rightarrow \mathcal{P}(\mathsf{p})$ $\qquad \mathcal{O}(\mathsf{p}) \overset{def}{=} \{\mathsf{e} \mid \mathsf{p}$ megfelel e-nek$\}$

Lemma: $\mathsf{p} \equiv \mathsf{q} \Leftrightarrow \mathcal{O}(\mathsf{p}) = \mathcal{O}(\mathsf{q})$

Lemma: $\tau[[a(p+q)]] = \tau[[ap+aq]]$

/A szelektív várakozást csak a bal oldal képes megoldani./

ui.: $\tau[[a(p+q)]] \underset{(2)}{=} a\ \tau[[p+q]] \underset{(3)}{=} a\ (\tau[[p]] \cup \tau[[q]]) =$

$\underset{\text{halmazkonkatenáció}}{=} a\ \tau[[p]] \cup a\ \tau[[q]]$

$\tau[[ap+aq]] \underset{(3)}{=} \tau[[ap]] \cup \tau[[aq]] \underset{(2)}{=} a\ \tau[[p]] \cup a\ \tau[[q]] \qquad \diamond$

Lemma: $\exists$ p,q$\in$P: $\mathcal{O}(\mathrm{a(p+q)}) \neq \mathcal{O}(\mathrm{ap+aq})$

ui.: /Kell olyan környezet, ami a baloldalt elfogadja, a jobboldalt nem./

$\mathrm{p = ap_1}, \qquad \mathrm{q = bq_1}, \qquad \mathrm{e = aa\underline{nil}}$

$\mathrm{a(p+q)} \xrightarrow{a} \mathrm{(p+q)} \xrightarrow{a} \mathrm{p_1} \qquad \mathrm{ap+aq} \xrightarrow{a} \mathrm{q}$!

$\mathrm{aa\underline{nil}} \qquad \mathrm{a\underline{nil}} \qquad \mathrm{\underline{nil}} \qquad \mathrm{aa\underline{nil}} \qquad \mathrm{anil}$

/nem megy tovább,
ha ezt az ágat választja/

Mgj.: A leíró szemantika absztraktabb, de (!)

$\mathcal{O}$(p+nil) = $\mathcal{O}$(p)

p $\neq$ nil τ[[p+nil]] $\neq$ τ[[p]]

Javítás: Új (2) szabály (#)-hoz:
/Ezzel már a leíró egyértelmûen absztraktabb./

(2') τ[[ap]] = a τ[[p]] $\cup$ $\{\varepsilon\}$ esetén

már τ[[p+nil]] = τ[[p]]

Köv.: $\forall$ p$\in$P: τ[[p]] halmaz prefix-zárt.

D.: *Axiomatikus szemantika*

E1: p+(q+r) = (p+q)+r

E2: p+q = q+p

E3: p+p = p

E4: p+nil = p

E5: a(p+q) = ap+aq

Mgj.: E5-öt csak a leíró szemantika tudja.

T.: Teljes és helyes (1),(2'),(3)-ra az E1-E5

Az ekvivalencia kérdése a két szemantikában egyforma választ ad.

(E1-E4 helyes a mûveletiben is)

Mgj.: E5 elhagyásával ellentmondásmentes a mûveletiben, de nem teljes.

Pl.: $\text{ab}\underline{\text{nil}} + \text{ac}\underline{\text{nil}} \overset{m\hat{u}v.}{=} (\text{ab}\underline{\text{nil}}+\text{ac}\underline{\text{nil}}) + \text{a}(\text{b}\underline{\text{nil}}+\text{c}\underline{\text{nil}})$

(E1-E4-bõl nem levezethetõ.)

D.: *Új mûveleti szemantika*

$L_1 = <C_1, A, \rightarrow_1>, \qquad L_2 = <C_2, A, \rightarrow_2>,$

$p_1 \in C_1, \qquad p_2 \in C_2$:

$p_1 \approx_B p_2 \overset{def.}{::=} \exists\ R \subseteq C_1 \times C_2$

(1) $(p_1, p_2) \in R$

(2) $(x,y) \in R$ és $x \xrightarrow{a}_1 z \Rightarrow (\exists w\colon\ y \xrightarrow{a}_2 w\colon\ (z,w) \in R)$

(3) $/(x,y) \in R$ és $y \xrightarrow{a}_2 w \Rightarrow (\exists z\colon\ x \xrightarrow{a}_1 z\colon\ (z,w) \in R)/$

T.: $\forall$ p,q$\in$P: p$\approx_B$q $\Leftrightarrow$ p $\overset{ax.}{=}$ q /E1-E4/

Mgj.: /- A mûveleti def. elõzõ megfogalmazása és ez nem
ekvivalens. - Ez teljességet is biztosít./

- E5: a(p+q) = ap+aq *Lineáris idõ axiómája*

(elõrehozott/elhalasztott döntések)

- a $\|$ b = ab+ba *összefésülés axiómája*

Mgj.: - axiomatikus szemantika

- verifikálás (helyességellenõrzés) miatt kell

- leíró szemantika

- részprogramok viselkedésébõl tudnak következtetni az összetett programra (program szintézis)

- mûveleti szemantika

- milyen lépéseket hajt végre a program (helyesség bizonyításra nem alkalmas)

- összehasonlításuk nehéz

Pl.: Példanyelv CSP

- szekvenciális folyamatok

- együttmûködés: aszinkron

- kommunikáció: szinkron, szimmetrikus

Szinkron, szimmetrikus miatt holtpontba vagy divergenciába juthat a rendszer. Dolgozik a rendszer csak semmit nem csinál (abort)

Jel.: Com - kommunikációs események,

Id - folyamatazonosítók

D.: P := stop - holtpont

| div - divergencia (abort)

| a $\rightarrow$ P - prefix

| P $\sqcap$ Q - belsõ nem determinizmus (maga dönt, hogy merre megy, nem látszik hogyan)

| P $\Box$ Q - szelektív várakozás /külsõ partner hatására dönt/

| P $\|_A$ Q - szinkronizált párhuzamosság

| P[b/a] - átnevezés /a-ról b-re/

| P\a - lezárás (megszorítás) /a-t adjuk meg/

| x - folyamat név (változó)

| rec x.P - rekurzió /x-re vonatkozóan rekurzív a P/

$a \in Com$, $A \subseteq Com$, $x \in Id$, $P,Q \in Rec$

/A Rec halmazt definiáljuk/,

$\text{Proc} = \{p \in \text{Rec} | \text{FV}(p) = \emptyset\}$

FV(p) - p szabad változóinak halmaza (free variable)

Pl.: P folyamat abc-je: αP /néha A-val jelölik/

$\alpha VMS = \{coin, choc\}$ /- csokigép/

$\alpha VMC = \{in1p, in2p, small, large, out1p\}$
/- módosított csokigép/

Mgj.: $\alpha(x \rightarrow P) = \alpha P$ $x \in \alpha P$ /kikötés/

(1) $(\text{coin} \rightarrow \text{STOP}_{\alpha\text{VMS}})$

/- bevesz egy érmét és megáll/ (X1)

(2) $(\text{coin} \rightarrow \text{choc} \rightarrow \text{coin} \rightarrow \text{choc} \rightarrow \text{STOP}_{\alpha\text{VMS}})$ (X2)

(3) $\alpha\text{CTR} = \{\text{up, right}\}$

$\text{CTR} = (\text{right} \rightarrow \text{up} \rightarrow \text{right} \rightarrow \text{right} \rightarrow \text{STOP}_{\alpha\text{CTR}})$

(4) αCLOCK = {tick}

Rekurzió: (tick $\rightarrow$ CLOCK) = CLOCK
$\uparrow$ /óraketyegés/

(tick $\rightarrow$ tick $\rightarrow$ CLOCK) = CLOCK

CLOCK = (tick $\rightarrow$ tick $\rightarrow$ tick $\rightarrow$ CLOCK)

Mgj.: X = F(X) stílusban adtuk meg a CLOCK-ot.

D.: $x \to P$ ''*õrzött*'', mert esemény van a folyamat leírás elején.

Á.: $X = F(X)$-nek A abc mellett egyértelmûen létezik megoldása, ha $F(X)$ õrzött.

$X = F(X)$ megoldás jele: $\mu X: A.F(X)$.

Biz.: késõbb $\diamond$

Pl.: (1) CLOCK = μX:{tick}.(tick$\rightarrow$X)

(2) VMS = (coin$\rightarrow$choc$\rightarrow$VMS)

VMS = μX:{coin, choc}.(coin$\rightarrow$choc$\rightarrow$X)

(3) 5p váltó: αCH5A = {in5p, out2p, out1p}

CH5A = (in5p$\rightarrow$out2p$\rightarrow$out1p$\rightarrow$out2p$\rightarrow$CH5A)

CH5B = (in5p$\rightarrow$out1p$\rightarrow$out1p$\rightarrow$out1p$\rightarrow$out2p$\rightarrow$CH5B)

<u>D.:</u> */Összetett folyamat abc-je/*

$$\alpha(\mathrm{x} \rightarrow \mathrm{P} \mid \mathrm{y} \rightarrow \mathrm{Q}) = \alpha\mathrm{P}, \quad \{\mathrm{x,y}\} \subseteq \alpha\mathrm{P}, \quad \alpha\mathrm{P} = \alpha\mathrm{Q}$$

<u>Pl.:</u> (1) (up $\rightarrow$ STOP | right $\rightarrow$ right $\rightarrow$ up $\rightarrow$ STOP)

(2) CH5C = in5p$\rightarrow$(out1p$\rightarrow$out2p$\rightarrow$out1p$\rightarrow$out1p$\rightarrow$CH5C)
| (out2p$\rightarrow$out1p$\rightarrow$out2p$\rightarrow$CH5C)

(3) VMCT = μX.coin$\rightarrow$(choc$\rightarrow$X|toffee$\rightarrow$X) (X4)

VMCT = coin$\rightarrow$(choc$\rightarrow$VMCT|toffee$\rightarrow$VMCT)

/<u>Mgj.:</u> - Eldönti, hogy mit ad, és folytatja a mûködését.
- Az abc elhagyható ha világos, hogy mi az./

(4) VMC = (in2p$\rightarrow$(large$\rightarrow$VMC|small$\rightarrow$out1p$\rightarrow$VMC) |
in1p$\rightarrow$(small$\rightarrow$VMC|in1p$\rightarrow$(large$\rightarrow$VMC|in1p$\rightarrow$STOP)))
/VMC - rossz gép/

(5) VMCRED = μX.(coin$\rightarrow$choc$\rightarrow$X|choc$\rightarrow$coin$\rightarrow$X)
- hitelezõ gép.

(6) VMS2 = (coin$\rightarrow$VMCRED) /- ez is hitelez/

(7) $\xrightarrow{\text{in}} \boxed{\text{COPYBIT}} \xrightarrow{\text{out}}$ αCOPYBIT = {in.0, in.1, out.0, out.1}

COPYBIT = μX.(in.0$\rightarrow$out.0$\rightarrow$X|in.1$\rightarrow$out.1$\rightarrow$X)

Mgj.: $P \mid Q$ nem megengedett $(x \rightarrow P)$

csak: $(x \rightarrow P | y \rightarrow Q | \ldots | z \rightarrow R)$ $(x \neq y,\ y \neq z,\ x \neq z$ determinisztikus$)$

$(x \rightarrow P | (y \rightarrow Q | z \rightarrow R))$ hibás!!! a belsõ elágazást nem bírja
az õrzés miatt.

D.: *Általánosítás* $B \subseteq \alpha P$ $x\!: B \rightarrow P(x)$ /folyamat menü/

Pl.: $B = \{x,y,z\}$ $(s\!: B \rightarrow P(s)) = (x \rightarrow P(x) | y \rightarrow P(y) | z \rightarrow P(z))$

Pl.: (1) αRUN$_A$ = A   A=$\{$x$_1$,...,x$_n\}$

RUN$_A$ = (x: A$\rightarrow$RUN$_A$) = (x$_1$ $\rightarrow$RUN$_A$| ... | x$_n$ $\rightarrow$RUN$_A$)
bármikor, bármelyik esemény kiválasztható

(2) (x: $\{$e$\}$$\rightarrow$P(x)) = (e$\rightarrow$P(e))   (1 eset)

(y: $\{\}$$\rightarrow$Q(y)) = STOP   (leállt)

Mgj.: |,$\rightarrow$,STOP mint speciális esetek megadhatók.

Pl.: (kölcsönös rekurzió)

(1) αDD $= \alpha$G $= \alpha$W $=$ {setorange,setlemon,coin,orange,lemon}

DD $=$ (setorange$\rightarrow$G$|$setlemon$\rightarrow$W)

G $=$ (coin$\rightarrow$orange$\rightarrow$G$|$setlemon$\rightarrow$W)

W $=$ (coin$\rightarrow$lemon$\rightarrow$W$|$setorange$\rightarrow$G)

(2) Mgj.: ∞ egyenlõséghalmaz is megadható

CT_n, ha n távolsára van a földtõl.

$CT_0 = (up \rightarrow CT_1 | around \rightarrow CT_0)$

$CT_{n+1} = (up \rightarrow CT_{n+2} | down \rightarrow CT_n)$ $\quad n \in N_0$

Mgj.: gépi állapottal megjeleníthetõ

<u>Axiómák:</u> /Axiomatikus szemantika megadásához/

$$(x \rightarrow P \mid y \rightarrow Q) = (y \rightarrow Q \mid x \rightarrow P)$$

$$(x \rightarrow P) \neq STOP$$

$\boxed{\text{L1:}}$ /Law (törvény)/

$$(x\colon A \rightarrow P(x)) = (y\colon B \rightarrow Q(y)) \Leftrightarrow A = B \wedge \forall x \in A\colon P(x) = Q(x)$$

(és az abc is "=")

Alkalmazás /axiomatikus szemantikában/:

L1A: STOP $\neq$ (d$\rightarrow$P) /- L1 alkalmazásából jön/

Biz.: STOP = (x: $\{\}$$\rightarrow$P) $\neq$ (x: $\{d\}$$\rightarrow$P) = d$\rightarrow$P $\diamond$

L1B: (c$\rightarrow$P) $\neq$ (d$\rightarrow$ Q), ha c$\neq$d

Biz.: $\{c\}\neq\{d\}$ $\diamond$

L1C: (c$\rightarrow$P|d$\rightarrow$Q) = (d$\rightarrow$Q|c$\rightarrow$P)

Biz.: Jel.: R(x) = $\{$P , ha x = c; Q, ha x = d$\}$

(c$\rightarrow$P|d$\rightarrow$Q)=(x:$\{c,d\}$$\rightarrow$R(x))=

=(x:$\{d,c\}$$\rightarrow$R(x))=(d$\rightarrow$Q|c$\rightarrow$P) $\diamond$

L1D: $(c \to P) = (c \to Q) \Leftrightarrow P = Q$

Pl.:

(1) $(\text{coin} \to \text{choc} \to \text{coin} \to \text{choc} \to \text{STOP}) \neq (\text{coin} \to \text{STOP})$

Biz.: L1D, L1A

(2) $\mu X.(\text{coin} \to (\text{choc} \to X | \text{toffee} \to X)) = \mu X.(\text{coin} \to (\text{toffee} \to X | \text{choc} \to X))$

Biz.: L1C

$\boxed{\text{L2:}}$ Ha F(X) prefix, õrzött kifejezés, akkor Y=F(Y)-nak

egyértelmûen létezik megoldása.

($Y=F(Y) \Leftrightarrow Y=\mu X.F(X)$)

/Ez az egyenlõség azért jó, mert leíró szemantikában is igaz./

<u>L2A:</u> $\mu X.F(X) = F(\mu X.F(X))$

Pl.:
(3) VM1 = (coin$\rightarrow$VM2)   VM2 = (choc$\rightarrow$VM1)

Á.: VM1 = VMS

ui.: VM1 = (coin$\rightarrow$VM2) = (coin$\rightarrow$(choc$\rightarrow$VM1))

VM1 ugyanannak a rekurzív egyenlõségnek a megoldása, mint a VMS. $\diamond$

Mgj.: rekurzív egyenleteknek nem mindig egyértelmû a megoldása $\Rightarrow$ monotonitás kihasználható

<u>D.:</u> *Kölcsönösen rekurzív egyenlõségek halmaza*

$$\left.\begin{array}{ll} i \in S & \text{- indexhalmaz (S) eleme} \\ X(i) & \text{- folyamat} \\ F(i,X) & \text{- õrzött kifejezés} \end{array}\right\} \Rightarrow X(i)=F(i,X),\ X(i)=F_i\ (X)$$

<u>Axióma:</u> Ha $\forall i \in S$: ($X_i = \underline{F}(i,X)$ és $Y_i = \underline{F}(i,Y)$) $\quad\Rightarrow\quad X=Y$

/X,Y - megoldáshalmazok/

($\exists!$ X(1) ... X(i) ... X(m) megoldáshalmaz)

Mgj.: - $\forall$ folyamat x:B$\rightarrow$F(x) alakra hozható, /így/ μX.(x:B$\rightarrow$F(x,X)) is:

$$(x:B \rightarrow F(x, \mu X.(x:B \rightarrow F(x,X)))) \quad \text{(L2A)}$$

x=x:B $\rightarrow$ F(x,X) megoldása

- Az elsõ x$\in$B eseménytõl függ a viselkedés.

- A nyelv kifejezései leírhatóak funkcionális nyelvre.

Leíró szemantika

D.: Történetek: <x,y>, <x>, <> eseménysorozat

Mgj.: Nincs jelölés a tranzakció kezdetére/végére.

Pl.: (1) <coin, choc, coin, choc>

<coin, choc, coin>

<>

(2) egyikre kerül sor.

{ <in2p> <in1p>
<in2p,large> <in2p,small> <in1p,in1p > <in1p,small>

Jelölések: s, t, u - konkrét történetek

S, T, U - történethalmazok

f, g, h - függvények

D.: Összefűzés: $s\hat{\ }t$.

pl.: $\langle coin, choc\rangle\hat{\ }\langle coin, toffee\rangle = \langle coin, choc, coin, toffee\rangle$

L1: $s\hat{\ }\langle\rangle = \langle\rangle\hat{\ }s = s$ /az üres sorozat ($\langle\rangle$) az egységelem/

L2: $s\hat{\ }(t\hat{\ }u) = (s\hat{\ }t)\hat{\ }u$ /asszociatív/

L3: $s\hat{\ }t = s\hat{\ }u \Leftrightarrow t = u$

L4: $s\hat{}t = u\hat{}t \quad \Leftrightarrow \quad s = u$

L5: $s\hat{}t = <> \quad \Leftrightarrow \quad s = <>$ és $t = <>$

D.: strict (szigorú) függvény az f, ha $f(<>) = <>$.

D.: f disztributív, ha $f(s\hat{}t) = f(s)\hat{}f(t)$
/elemenként alkalmazható, definiálható egyelemű s-re/

Lemma: Amelyik függvény disztributív az szigorú.

/Ha disztributív, akkor üreshez üreset kell rendeljen./

D.: A t n-szer összefûzve: t^n.

L6: $t^0 = <>$

L7: $t^{n+1} = t\hat{}t^{n}$

L8: $t^{n+1} = t^{n}\hat{}t$

L9: $(s\hat{}t)^{n+1} = s\hat{}(t\hat{}s)^{n}\hat{}t$ /L8 és L9 következmények/

D.: Vetítés (megszorítás) A-ra: $t{\upharpoonright}A$

Pl.: $(<\text{around, up, down, around}>){\upharpoonright}\{\text{up, down}\} = <\text{up, down}>$

L1: $<>{\upharpoonright}A = <>$ /szigorú/

L2: $(s\hat{}t){\upharpoonright}A = (s{\upharpoonright}A)\hat{}(t{\upharpoonright}A)$ /disztr./

L3: $<x>{\upharpoonright}A = <x>$, ha $x \in A$ /disztr. miatt $\forall$ sorozatra def./

L4: $<x> \upharpoonright A = <>$, ha $x \notin A$ /disztr. miatt $\forall$ sorozatra def./

L5: $s \upharpoonright \{\} = <>$ /elõzõekbõl kijön/ (biz.: s hossza szerinti indukcióval)

L6: $(s \upharpoonright A) \upharpoonright B = s \upharpoonright (A \cap B)$ (biz.: s hossza szerinti indukcióval)

D.: lov: $<x,y,z>_0 = x$

lorem: $<x,y,z>' = <y,z>$

L1: $(<x>\hat{\ }s)_0 = x$

L2: $(<x>\hat{\ }s)' = s$

L3: $s = (<s_0>\hat{\ }s')$, ha $s \neq <>$

L4: $s = t \quad \Leftrightarrow \quad ((s = t = <>) \vee (s_0 = t_0 \wedge t' = s'))$

D.: A* - Az A elemeinek összes véges sorozata (<> is)

D.: $A^* = \{s \mid s{\uparrow}A = s\}$

L1: $<> \in A^*$

L2: $<x> \in A^* \quad \Leftrightarrow \quad x \in A$

L3: $(s\hat{\ }t) \in A^* \quad \Leftrightarrow \quad s \in A^* \wedge t \in A^*$

L4: $A^* = \{t \mid t = <> \vee (t_0 \in A \wedge t' \in A^*)\}$

A* rekurzív definiciója

Rendezés (parciális)

D.: ($s \leq t$) s prefixe t-nek, ha $\exists u$: $s\hat{\ }u = t$.

Mgj.: legkisebb elem: $<>$

L1: $<> \leq s$ $\quad$ $/<>\hat{\ }s = s/$ $\quad$ legkisebb

L2: $s \leq s$ $\quad$ $/s\hat{\ }<> = s/$ $\quad$ reflexív a rendezés

L3: $s \leq t \wedge t \leq s \Rightarrow s = t$ $\quad$ antiszimmetrikus

L4: $s \leq t \wedge t \leq u \Rightarrow s \leq u$ $\quad$ tranzitív

L5: $(<x>\hat{\ }s) \leq t \Leftrightarrow t \neq <> \wedge x = t_0 \wedge s \leq t'$

(prefix rekurzív)

L6: $s \leq u \wedge t \leq u \quad \Rightarrow \quad s \leq t \vee t \leq s$

D.: $s \text{ in } t = (\exists u,v\!: \; t = u \hat{} s \hat{} v)$

L1: $<> \text{ in } t$

L2: $t \text{ in } t$

L3: $t \text{ in } s \wedge s \text{ in } t \quad \Rightarrow \quad s = t$

L4: $s \text{ in } t \wedge t \text{ in } u \quad \Rightarrow \quad s \text{ in } u$ /L1-L4 is parciális rendezés/

L5:(L7) $(<x>\hat{}s) \text{ in } t \quad \Rightarrow$

$$t \neq <> \wedge \; (\; (t_0 = x \wedge s \leq t') \vee (<x>\hat{}s \text{ in } t') \;)$$

L6:(L8) $\quad s \leq t \quad \Rightarrow \quad (s{\uparrow}A) \leq (t{\uparrow}A)$

($\uparrow$ monoton a prefix parciális rendezésre nézve;
a vetítés megtartja a rendezést)

Lemma: $\forall$ disztributív (sorozatra elemenként feld.) fv.
monoton a prefix parciális rendezésre.

Biz.: $\quad s \leq t, \quad s\hat{\ }u = t$

$\rightarrow \quad f(t) = f(s\hat{\ }u) = f(s)\hat{\ }f(u)$

$\rightarrow \quad f(s) \leq f(t) \quad \diamond$

Lemma: "^" monoton a második argumentumára nézve (kétváltozós)

Biz.: $t \leq u \quad \Rightarrow \quad s\hat{\ }t \leq s\hat{\ }u \quad \diamond$

D.: Minden argumentumában monoton többváltozós függvényt monotonnak nevezünk.

D.: Hossz: #t $\qquad \#\langle x,y,x \rangle = 3$

L1: $\#\langle\rangle = 0$

L2: $\#\langle x \rangle = 1$

L3: $\#\langle s\hat{\ }t \rangle = \#s + \#t$

L4: $\#(t{\uparrow}(A \cup B)) = \#(t{\uparrow}A) + \#(t{\uparrow}B) - \#(t{\uparrow}(A \cap B))$

L5: $s \leq t \quad \Rightarrow \quad \#s \leq \#t$

L6: $\#(t^n) = n(\#t)$

D.: $s{\downarrow}x = \#(s{\uparrow}\{x\})$ /hányszor fordul elõ egy (x) esemény s-ben/

Folyamatok történethalmaza

Pl.: (1) $\text{traces}(\text{STOP}) = \{<>\}$

(2) $\text{traces}(\text{coin}\rightarrow\text{STOP}) = \{<>, <\text{coin}>\}$

(3) $\text{traces}(\mu \text{X.coin}\rightarrow\text{choc}\rightarrow\text{X}) = \{\text{s} \mid \exists \text{n: s} \leq <\text{coin,choc}>^{n}\}$
/rekurzív csokigép/

(4) $\text{traces}(\mu \text{X.tick}\rightarrow\text{X}) = \{\text{tick}\}^*$

L1: $traces(STOP) = \{t \mid t = <>\}$

L2: $traces(c \rightarrow P) = \{t \mid t = <> \vee (t_0 = c \wedge t' \in traces(P))\} =$
$\{<>\} \cup \{<c>\hat{}t \mid t \in traces(P)\}$

L3: $traces(c \rightarrow P | d \rightarrow Q) = \{t \mid t = <> \vee (t_0 = c \wedge t' \in traces(P)) \vee$
$(t_0 = d \wedge t' \in traces(Q))\}$

L4: $traces(x{:}B \rightarrow P(x))$
$= \{t \mid t = <> \vee (t_0 \in B \wedge t' \in traces(P(t_0))) \}$

L5: X = F(X) rekurzív folyamat esetén:

$F^0(X) = X$ (*)

$F^{n+1}(X) = F(F^n(X))$ /F^ω - végtelen hatványa F-nek/

Ha F õreseménnyel definiált, akkor

$$\text{traces}(\mu X{:}A.F(X)) = \bigcup_{n\geq 0} \text{traces}(F^n(\text{STOP}_A))$$

Pl.: (1) $\text{RUN}_A = \mu X{:}A.F(X)$ ($\text{RUN}_A := x{:}A \rightarrow \text{RUN}_A$)

$F(X) = (x{:}A \rightarrow X)$ ($\sim$)

Á.: $\text{Traces}(\text{RUN}_A) = A^*$

<u>Biz.:</u> L5 alapján elegendõ belátni, hogy

$$\forall \text{n-re traces}(F^n(STOP_A)) = \{s \mid s \in A^* \wedge \#s \leq n\}$$

$\boxed{n=0:}$ $\text{traces}(STOP_A) = \{<>\} = \{s \mid s \in A^* \text{ és } \#s \leq 0\}$ (**)

mert: $F^0(STOP_A) = STOP_A$

$\boxed{n \rightarrow n+1:}$ $\text{traces}(F^{n+1}(STOP_A)) \underset{(*)}{=}$

$\text{traces}(F(F^n(STOP_A))) \underset{(\sim)}{=}$

$\text{traces}(x:A \rightarrow F^n(STOP_A)) \underset{(L4)}{=}$

$\{ t \mid t = <> \vee (t_0 \in A \wedge t' \in \text{traces}(F^n(STOP_A)))\} =$

$$\underset{(\textit{indukció})}{=} \{\, t \mid t = \langle\rangle \vee (\, t_0 \in A \wedge (t' \in A^* \wedge \#t' \leq n)\,)\,\} \underset{(\textit{konkat.},\ \#)}{=}$$

$$= \{\ t \mid t = \langle\rangle \vee ((t_0 \in A \wedge t' \in A^*) \wedge \#t' \leq n)\} =$$

$$= \{\ t \mid t \in A^* \wedge \#t \leq n+1)\} \diamond$$

(2) traces(VMS) = $\bigcup_{n\geq 0}\{$ s | s $\leq$ <coin,choc>$^n\}$;

<u>Biz.:</u> indukcióval:

traces(F^n_{VMS}(STOP$_A$))=$\{$ t | t $\leq$<coin,choc>$^n\}$,

ahol F(X)=(coin$\rightarrow$choc$\rightarrow$X)

$\boxed{\text{n=0:}}$ traces(STOP$_A$) = $\{$<>$\}$ = $\{$ s | s $\leq$<coin,choc>$^0\}$

$\boxed{\text{n}\rightarrow\text{n+1:}}$ traces(coin$\rightarrow$choc$\rightarrow$F^n(STOP$_A$)) $\underset{L2,L2}{=}$

$\{$<>,<coin>$\}$ $\cup$ $\{$<coin,choc>$\}$ $\cup$ $\{$ t | traces(F^n(STOP$_A$))$\}$ $\underset{ind.hip.}{=}$

$\{$<>,<coin>$\}$ $\cup$ $\{$<coin,choc>^t | t $\leq$ <coin,choc>$^n\}$ =

$\{$ s $|$ s $=<>$ $\vee$ s $=$ $<$coin$>$ $\vee$

$\exists$ t $>$ s$=<$coin,choc$>$^t $\wedge$ t $\leq$ $<$coin,choc $>^n\}$ $=$

$\{$ s $|$ s $\leq$ $<$coin,choc$>^{n+1}$ $\}$ $\diamond$

Prefix zárt:

L6: $<>$ $\in$traces(P)

L7: s^t $\in$ traces(P) $\Rightarrow$ s $\in$ traces(P)

L8: traces(P) $\subseteq$ (αP)*

További mûveletek

D.: • $f:A \to B$ $f^*:A^* \to B^*$ (f elemenként)

$$f^*(<>) = <>$$

$$f^*(<x>) = <f(x)>$$

$$f^*(s\hat{}t) = f^*(s)\hat{}f^*(t)$$

• $\hat{}/<<1,3>,<>,<7>> = <1,3>\hat{}<>\hat{}<7> = <1,3,7>$; $\hat{}/s$

• összefésülés $s \in interleaving(t,u)$

/az összes lehetséges módon összefésüli/

$\underline{\text{pl.:}}$ $t = <1,6,5,2,7>$ $\quad u = <3,1,4>$ $\quad \Rightarrow \quad s = <1,6,3,1,5,4,2,7>$

- s[i] - az s i. eleme /0-val kezdõdik az indexelés/

- megfordítás: $\overline{<3,5,37>} = <37,5,3>$

- kiválasztás: $s = <\underbrace{a.7}, b.9, a.8, c.0>$

$s \downarrow a = <7,8>$

$s \downarrow d = <>$

ha párok sorozatára értelmezzük "$\downarrow$"-ot, rendezett pár

- kompozíció: "$\surd$" - sikeres terminálás, a történet utolsó eleme

$\underline{\text{L1:}}$ $s;t = s \quad , \text{ha } \neg(<\surd> \text{ in } s)$ szigorú konkatenáció: ";"

/ha nincs $\surd$, akkor nem tudom folytatni/

$\underline{\text{L2:}}$ $(s\hat{}<\surd>);t = s\hat{}t \quad , \text{ha } \neg(<\surd> \text{ in } s)$

$\underline{\text{L2A:}}$ $(s\hat{}<\surd>\hat{}u);t = s\hat{}t \quad , \text{ha } \neg(<\surd> \text{ in } s)$

Specifikáció (leíró szemantikai def-ja annak, hogy mikor felel meg a prg. a feladatnak)

(1) NOLOSS $= (\#(tr\uparrow\{choc\}) \leq \#(tr\uparrow\{coin\})$

/- a gyártó szempontjából; tr - sorozat/

(2) FAIR1 $= ((tr\downarrow coin) \leq (tr\downarrow choc)+1)$ /- fairplay/

(3) VMSPEC =

$= \text{NOLOSS} \wedge \text{FAIR1} = (0 \leq ((tr\downarrow coin)-(tr\downarrow choc)) \leq 1)$

(4) VMCFIX = $(\neg(<\text{in1p}>^3 \text{ in tr}))$ /- 3 db. 1 penny-s nincs egymás után/

(5) MENDVMC = $(\text{tr}\in\text{traces(VMC)} \wedge \text{VMCFIX})$ /a (4)-es javítása/

(6) $0 \leq ((\text{tr}\downarrow\text{coin})\text{-}(\text{tr}\downarrow\text{choc})) \leq 2$

/az (5)-ösre vonatkozó kikötés/

D.: (P sat S) P megfelel S-nek, ha $\forall$tr: tr$\in$traces(P) $\Rightarrow$ S(tr).

/Mgj.: Minden olyan specifikációnak, amihez van neki megfelelõ P, annak tartalmaznia kell az $<>$ sorozatot, azaz a STOP is megfelel neki. Ezek mindig csak biztonsági kikötések./

L1: P sat true

L2A: Ha P sat S és P sat T "$\Rightarrow$" P sat S$\wedge$T

L2: Ha $\forall$n:(P sat S_n) "$\Rightarrow$" P sat ($\forall$n:S_n)

L3: P sat S és $S \Rightarrow T$ "$\Rightarrow$" P sat T

L4A: STOP sat (tr = <>)

L4B: P sat S "$\Rightarrow$" $c \rightarrow P$ sat $(tr = \langle\rangle \vee tr_0 = c \wedge S(tr'))$

L4C: P sat S "$\Rightarrow$" $c \rightarrow d \rightarrow P$ sat $(tr \leq \langle c,d\rangle$
$\vee\ (tr \geq \langle c,d\rangle \wedge S(tr'')))$

/ha $tr \leq \langle c,d\rangle \quad \Rightarrow \quad tr \in \{\langle\rangle, \langle c\rangle, \langle c,d\rangle\}$/

L4D: P sat S és Q sat T "$\Rightarrow$"

$$(c \rightarrow P | d \rightarrow Q) \text{ sat } (tr = \langle\rangle \vee (tr_0 = c \wedge S(tr')) \vee (tr_0 = d \wedge T(tr')))$$

L4: Ha $\forall x \in B$: (P(x) sat S_x) "$\Rightarrow$"

$$(x{:}B \rightarrow P(x)) \text{ sat } (tr = \langle\rangle \vee (tr_0 \in B \wedge S_{tr_0}(tr')))$$

/elágazás lev. szabálya/

D.: $P/s ::= P$ az s-beli események után. /P folytatása s után/

pl.: $(d \rightarrow Q)/d = Q$

/Rekurzió lev. szabályai:/

L5: P sat S és $s \in traces(P)$ "$\Rightarrow$" $\forall\, tr \in (P/s)$: $S(s\hat{}tr)$

L6: Ha F(X) õreseménnyel ellátott $\wedge$ STOP sat S

$\wedge$ (X sat S $\Rightarrow$ F(X) sat S)

"$\Rightarrow$" $\mu X.F(X)$ sat S

Pl.: VMS sat VMSPEC

$$\mathrm{VMS} = (\mathrm{coin} \rightarrow (\mathrm{choc} \rightarrow \mathrm{VMS})) \qquad \mathrm{F(X)} = (\mathrm{coin} \rightarrow (\mathrm{choc} \rightarrow \mathrm{X}))$$

$$\mathrm{VMS} = \mu \mathrm{X}{:}\{\mathrm{coin},\mathrm{choc}\}.(\mathrm{coin} \rightarrow (\mathrm{choc} \rightarrow \mathrm{X}))$$

$$\mathrm{VMSPEC} = (0 \leq ((\mathrm{tr}{\downarrow}\mathrm{coin}) - (\mathrm{tr}{\downarrow}\mathrm{choc})) \leq 1)$$

Biz.:

$(\text{tr} = <>) \Rightarrow \text{VMSPEC}$

$\text{STOP sat } (\text{tr} = <>) \underset{(L3)}{\Rightarrow} \text{STOP sat VMSPEC}$

Tfh. $\quad$ $\text{X sat } (0 \leq ((\text{tr}\downarrow\text{coin})-(\text{tr}\downarrow\text{choc})) \leq 1)$ $\qquad \underset{(L4C)}{\Rightarrow}$

$\text{F(X)} = (\text{coin} \rightarrow \text{choc} \rightarrow \text{X}) \text{ sat}$
$(\text{tr} \leq <\text{coin,choc}>$
$\vee\ (\text{tr} \geq <\text{coin,choc}> \wedge 0 \leq ((\text{tr''}\downarrow\text{coin})-(\text{tr''}\downarrow\text{choc})) \leq 1))$

$\underset{(*,L3)}{\Rightarrow} \text{F(X) sat VMSPEC}$

(*)

(1) $<>\downarrow \text{coin} = <>\downarrow \text{choc} = 0$

$(<\text{coin}>\downarrow \text{coin})=(<\text{coin,choc}>\downarrow \text{coin})=(<\text{coin,choc}>\downarrow \text{choc})=1;$

$<\text{coin}>\downarrow \text{choc}=0$

(2) $\text{tr} \geq <\text{coin,choc}> \quad \Rightarrow \quad \text{tr}\downarrow \text{coin}=\text{tr''}\downarrow \text{coin}+1 \ \wedge \ \text{tr}\downarrow \text{choc}=\text{tr''}\downarrow \text{choc}+1.$

$\diamond$

Párhuzamosság

/folyamatokat (+ környezeteket) rakunk össze zárt rendszerré/

Egyenlõre: αP = αQ (spec. eset) /α - az abc/

P $\|$ Q /ha van 2 részmegoldás, akkor kompozíciójuk megold-e valamilyen feladatot v. sem/

Pl.: (1) $\mathrm{GRCUST} = (\mathrm{toffee} \to \mathrm{GRCUST} | \mathrm{choc} \to \mathrm{GRCUST}$
$| \mathrm{coin} \to \mathrm{choc} \to \mathrm{GRCUST})$

/ha kap egy karamellát v. egy csokit, akkor alapállapotba kerül; kapzsi/

$\mathrm{VMCT} = \mu X.\mathrm{coin} \to (\mathrm{choc} \to X |\ \mathrm{toffee} \to X)$

$(\mathrm{GRCUST} \parallel \mathrm{VMCT}) = \mu X.(\mathrm{coin} \to \mathrm{choc} \to X)$

(Így karamellát sosem ad.)

(2)

$$\text{FOOLCUST} = (\text{in2p}\rightarrow\text{large}\rightarrow\text{FOOLCUST} \mid \text{in1p}\rightarrow\text{large}\rightarrow\text{FOOLCUST})$$

$$\begin{aligned}\text{VMC} = (&\text{in2p}\rightarrow(\text{large}\rightarrow\text{VMC}\mid\text{small}\rightarrow\text{out1p}\rightarrow\text{VMC}) \mid \\ &\text{in1p}\rightarrow(\text{small}\rightarrow\text{VMC}\mid\text{in1p}\rightarrow(\text{large}\rightarrow\text{VMC}\mid\text{in1p}\rightarrow\text{STOP})))\end{aligned}$$

$$(\text{FOOLCUST} \parallel \text{VMC}) = \mu X.(\text{in2p}\rightarrow\text{large}\rightarrow X\mid\text{in1p}\rightarrow\text{STOP})$$

/in1p esetén holtpontba kerül a gép/

L1: $P \parallel Q = Q \parallel P$ /azonos abc-k mellett/

L2: $P \parallel (Q \parallel R) = (P \parallel Q) \parallel R$

L3A: $P \parallel STOP_{\alpha P} = STOP_{\alpha P}$

L3B: $P \parallel RUN_{\alpha P} = P$

L4A: $(c \rightarrow P) \,||\, (c \rightarrow Q) = (c \rightarrow (P \,||\, Q))$

L4B: $(c \rightarrow P) \,||\, (d \rightarrow Q) = STOP$, ha $c \neq d$ (holtpont)

L4: $(x{:}A \rightarrow P(x)) \,||\, (y{:}B \rightarrow Q(y)) = (z{:}(A \cap B) \rightarrow (P(z) \,||\, Q(z)))$

Pl.: $P = (a \rightarrow b \rightarrow P | b \rightarrow P)$
$Q = (a \rightarrow (b \rightarrow Q | c \rightarrow Q))\}$

$\Rightarrow P||Q = (a \rightarrow ((b \rightarrow P)||(b \rightarrow Q|c \rightarrow Q)) = a \rightarrow (b \rightarrow (P||Q))$
$= \mu X.(a \rightarrow b \rightarrow X)$

Történetekre vonatkozó szabályok:

<u>L1:</u> $\text{traces}(P||Q) = \text{traces}(P) \cap \text{traces}(Q)$

<u>L2:</u> $(P||Q)/s = (P/s)||(Q/s)$ (Q/s - Q mûködése s eseménysorozat után)

Általánosítás: $\alpha P \neq \alpha Q$,

$$\alpha(P||Q) = \alpha P \cup \alpha Q$$

Pl.: (1) αNOISYVM = {coin,choc,toffee,clink,clunk}

NOISYVM = (coin→clink→choc→clunk→NOISYVM)

αCUST = {coin,choc,curse,toffe} /curse - szidalmaz/

CUST = (coin→(toffee→CUST|curse→choc→CUST))
(káromkodni szinkronizáció nélkül is lehet)

(NOISYVM||CUST) =
μX.(coin → (clink→curse→choc→clunk→X
|curse→clink→choc→clunk→X)

(2) αP = {up,down}   P = (up→down→P)

αQ = {left,right}   Q = (right→left→Q|left→right→Q)

i∈{1,2}   j∈{1,2,3}

P||Q = R_{12}, ahol R_{12} = (up→R_{22}|left→R_{11}|right→R_{13})

L1: kommutatív $/P \parallel Q = Q \parallel P/$

L2: asszociatív $/P \parallel (Q \parallel R) = (P \parallel Q) \parallel R/$

L3A: $P \parallel STOP_{\alpha P} = STOP_{\alpha P}$

L3B: $P \parallel RUN_{\alpha P} = P$

Mgj.: Legyen $a \in (\alpha P \setminus \alpha Q)$, $b \in (\alpha Q \setminus \alpha P)$, $\{c,d\} \in (\alpha P \cap \alpha Q)$

L4A: $(c \rightarrow P) \parallel (c \rightarrow Q) = (c \rightarrow (P \parallel Q))$

L4B: $(c \rightarrow P) \parallel (d \rightarrow Q) = STOP$, ha $c \neq d$

L5A: $(a \rightarrow P) \parallel (c \rightarrow Q) = a \rightarrow (P \parallel (c \rightarrow Q))$

L5B: $(c \rightarrow P) \parallel (b \rightarrow Q) = b \rightarrow ((c \rightarrow P) \parallel Q)$

L6: $(a \rightarrow P) \parallel (b \rightarrow Q) = (a \rightarrow (P \parallel (b \rightarrow Q))) \mid (b \rightarrow ((a \rightarrow P) \parallel Q))$

<u>L7:</u> P = (x:A $\rightarrow$ P(x)), A $\subseteq \alpha$P

Q = (y:B $\rightarrow$ Q(y)), B $\subseteq \alpha$Q

$\Rightarrow$ (P||Q) = (z:C $\rightarrow$ P'||Q'), ahol

C = (A$\cap$B) $\cup$ (A$\setminus\alpha$Q) $\cup$ (B$\setminus\alpha$P)
/(A$\cap$B) - erre szinkronizálni kell (*)/

P' = {P(z), ha z $\in$ A
P , különben
/(A$\setminus\alpha$Q) - P azt csinál, amit akar (#)/

Q' = {Q(z), ha z $\in$ B
Q , különben
/(B$\setminus\alpha$P) - Q azt csinál, amit akar/

Pl.: αP={a,c}, αQ={b,c},

$$P=(a\to c\to P),\ Q=(c\to b\to Q)$$

$$P||Q = (a\to c\to P)||(c\to b\to Q) \stackrel{(*)}{=} a\to((c\to P)||(c\to b\to Q))$$
$$\stackrel{(\#)}{=} a\to c\to(P||(b\to Q))$$

$$P||(b\to Q) \stackrel{L6}{=} (a\to((c\to P)||(b\to Q)) \mid b\to(P||Q))$$

$$= (a\to b\to((c\to P)||Q) \mid b\to(P||Q)) = (a\to b\to c\to(P||(b\to Q))$$

$$\mid b\to a\to c\to(P||(b\to Q))) = \mu X.(a\to b\to c\to X|b\to a\to c\to X)$$

$$P||Q = (a\to c\to \mu X.(a\to b\to c\to X|b\to a\to c\to X))$$

Történetekre vonatkozó szabályok:

L1: traces(P||Q) =

$$\{t \mid (t\uparrow \alpha P) \in traces(P) \wedge (t\uparrow \alpha Q) \in traces(Q) \wedge t \in (\alpha P \cup \alpha Q)^*\}$$

L2: $(P||Q)/s = (P/(s\uparrow \alpha P))||(Q/(s\uparrow \alpha Q))$

Pl.: NOISYVM || CUST

t1 = <coin, clink, curse>

$t1 \uparrow \alpha NOISYVM = \langle coin, clink\rangle \in traces(NOISYVM)$
$t1 \uparrow \alpha CUST = \langle coin, curse\rangle \in traces(CUST)$

$\Rightarrow t1 \in traces(NOISYVM \,||\, CUST)$

$t2 = \langle coin,curse,clink \rangle \in traces(NOISYVM \parallel CUST)$

<u>L3A:</u> Ha $\alpha P \cap \alpha Q = \{\} \Rightarrow traces(P \| Q)$
$= \{s \mid \exists t \in traces(P) \wedge \exists u \in traces(Q) \wedge s \in interleaving(t,u)\}$

<u>L3B:</u> Ha $\alpha P = \alpha Q \Rightarrow traces(P \| Q) = traces(P) \cap traces(Q)$

Pl.: **Evõ filozófusok:** i = 0,1,2,3,4

αPHIL$_i$ = {i.sits down, i.gets up, i.picks up fork.i,
i.picks up fork.(i$\oplus$1), i.puts down fork.i,
i.puts down fork.(i$\oplus$1)}

PHIL$_i$ = (i.sits down $\rightarrow$ i.picks up fork.i
$\rightarrow$ i.picks up fork.(i$\oplus$1) $\rightarrow$ i.puts down fork.i
$\rightarrow$ i.puts down fork.(i$\oplus$1) $\rightarrow$ i.gets up $\rightarrow$ PHIL$_i$)

$$\alpha\mathsf{FORK}_i = \{\ \mathsf{i.picks\ up\ fork.i,\ (i}\ominus\mathsf{1).picks\ up\ fork.i,}$$
$$\mathsf{i.puts\ down\ fork.i,\ (i}\ominus\mathsf{1).puts\ down\ fork.i}\ \}$$

$$\mathsf{FORK}_i = (\ \mathsf{i.picks\ up\ fork.i} \rightarrow \mathsf{i.puts\ down\ fork.i} \rightarrow \mathsf{FORK}_i$$
$$\mid\ \mathsf{(i}\ominus\mathsf{1).picks\ up\ fork.i} \rightarrow \mathsf{(i}\ominus\mathsf{1).puts\ down\ fork.i}$$
$$\rightarrow \mathsf{FORK}_i\ )$$

$$\mathsf{PHILOS} = (\mathsf{PHIL}_0 || \mathsf{PHIL}_1 || \mathsf{PHIL}_2 || \mathsf{PHIL}_3 || \mathsf{PHIL}_4)$$

$$\mathsf{FORKS} = (\mathsf{FORK}_0 || \mathsf{FORK}_1 || \mathsf{FORK}_2 || \mathsf{FORK}_3 || \mathsf{FORK}_4)$$

$$\mathsf{COLLEGE} = (\mathsf{PHILOS} || \mathsf{FORKS})$$

Módosítás (sorrendfüggetlen a villák felvétele) :

$$\alpha\text{LEFT}_i = \{\text{i.sits down, i.picks up fork.i, i.puts down fork.i,}\\ \text{i.gets up}\}$$

$$\text{LEFT}_i = (\text{i.sits down} \rightarrow \text{i.picks up fork.i} \rightarrow \text{i.puts down fork.i}\\ \rightarrow \text{i.gets up} \rightarrow \text{LEFT}_i)$$

$$\alpha\text{RIGHT}_i = \{\text{i.sits down, i.picks up fork.(i}\oplus\text{1),}$$
$$\text{i.puts down fork.(i}\oplus\text{1), i.gets up}\}$$

$$\text{RIGHT}_i = (\text{i.sits down} \rightarrow \text{i.picks up fork.(i}\oplus\text{1)}$$
$$\rightarrow \text{i.puts down fork.(i}\oplus\text{1)} \rightarrow \text{i.gets up}\rightarrow\text{RIGHT}_i)$$

$$\text{PHIL}_i = \text{LEFT}_i || \text{RIGHT}_i$$

Módosítás (többször is ehet, mielött feláll) :

$$\mathsf{LEFT}_i = (\mathsf{i.sits\ down} \rightarrow \mu \mathsf{X}.(\mathsf{i.picks\ up\ fork.i} \rightarrow \mathsf{i.puts\ down\ fork.i} \rightarrow \mathsf{X} \mid \mathsf{i.gets\ up} \rightarrow \mathsf{LEFT}_i))$$

Holtpont megelőzése, egyszerre csak 4 filozófus lehet az asztalnál :

$$\alpha\text{FOOT} = \bigcup_{i=0}^{4} \{\text{i.sits down, i.gets up}\},$$

$$\text{U} = \bigcup_{i=0}^{4} \{\text{i.gets up}\},$$

$$\text{D} = \bigcup_{i=0}^{4} \{\text{i.sits down}\}$$

$$\mathsf{FOOT}_0 = (x{:}D \rightarrow \mathsf{FOOT}_1)$$

$$\mathsf{FOOT}_j = (x{:}D \rightarrow \mathsf{FOOT}_{j+1} \mid y{:}U \rightarrow \mathsf{FOOT}_{j-1}) \qquad j \in \{1,2,3\}$$

$$\mathsf{FOOT}_4 = (y{:}U \rightarrow \mathsf{FOOT}_3)$$

$$\mathsf{NEWCOLLEGE} = (\mathsf{COLLEGE} \parallel \mathsf{FOOT}_0)$$

Á.: $\forall s \in traces(NEWCOLLEGE)$: $(NEWCOLLEGE/s) \neq STOP$
/Holtpontmentes/

/Mgj.: Ha nem több, mint 4-en ülnek az asztalnál, akkor nincs holtpont./

Biz.:

Def.: $seated(s) = \#(s{\uparrow}D) - \#(s{\uparrow}U)$
/- most hányan ülnek; $\forall s \in traces(NEWCOLLEGE)$/

SÁ.: Mivel $s{\uparrow}(U \cup D) \in traces(FOOT_0) \Rightarrow seated(s) \leq 4$
/biz. kellene/

Ha seated(s)$\leq$3 $\Rightarrow$ valaki leülhet, $\Rightarrow$ nincs holtpont

Ha seated(s)=4

$\Rightarrow$ ha $\exists$ evõ,

$\Rightarrow$ leteheti a villát (elõbb a balt)

ha $\nexists$ evõ,

$\Rightarrow$ felvett villák$\leq$3, $\Rightarrow$ 1-et felvehetnek

felvett villák=4,

$\Rightarrow$ az üres hely bal oldalán levõ villa vehetõ fel.

Mindegyik esetben van végrehajtható esemény

$\Rightarrow$ nincs holtpont. $\diamond$

Géppel: Állapotok száma: PHIL: 6

FORK: 3

COLLEGE: $6^5 \times 3^5 \approx 18$ millió

$\longrightarrow$ sok ellenõrzés

Livelock: (fair ütemezés)

- ha leült, akkor nem elõzhetõ meg végtelen sokszor a villa felemelésében

(pl.: FOOT megakadályozza, hogy a szomszéd túl gyorsan újra leüljön.)

- de: FOOT vlkit túl sokáig is fenntarthat íly módon.

Impl.: a lehetségessé vált események elõbb-utóbb bekövetkeznek.

D.: Folyamatcsaládok (viselkedési mintát jelent)

f:αP $\rightarrow$ A (eseménynévcsere)
f(P) — f(c)-t hajt végre, amikor P c-t hajt végre
$\Rightarrow$ α(f(P)) = f(α(P))

traces(f(P)) = {f*(s) | s$\in$traces(P)}

Pl.: (1) infláció $f(in2p) = in10p$

$f(out1p) = out5p$

$f(large) = large$

$f(in1p) = in5p$

$f(small) = small$

$NEWVMC = f(VMC)$

(2) $f(up) = right$,

$f(down) = left$,

$f(around) = around$ (Síkba rakott UFO)

$LR_0 = f(CT_0)$ /Lásd 33.0/

(3) a sarokban around

$$\mathrm{LRUD} = \mathrm{LR}_0 || \mathrm{CT}_0$$

(4) copybit-ek összekapcsolása

$$\begin{aligned}
&f(\mathrm{out}.0) = g(\mathrm{in}.0) = \mathrm{mid}.0\\
&f(\mathrm{out}.1) = g(\mathrm{in}.1) = \mathrm{mid}.1\\
&f(\mathrm{in}.0) = \mathrm{in}.0\\
&f(\mathrm{in}.1) = \mathrm{in}.1\\
&g(\mathrm{out}.0) = \mathrm{out}.0\\
&g(\mathrm{out}.1) = \mathrm{out}.1
\end{aligned}$$

$$\mathrm{CHAIN2} = f(\mathrm{COPYBIT}) || g(\mathrm{COPYBIT})$$

/szinkronizált kommunikáció a mid eseményekre/

(5) Logikai vált. (0,1)

assign.0 assign.1 $\text{assign} \leftrightarrow \binom{\text{setlemon}}{\text{setorange}}$

fetch.0 fetch.1 $\text{fetch} \leftrightarrow \binom{\text{coin}\rightarrow\text{lemon}}{\text{coin}\rightarrow\text{orange}}$

BOOL = f(DD)

$\text{DD} = (\text{setorange}\rightarrow\text{G} \mid \text{setlemon}\rightarrow\text{W})$
$\text{G} = (\text{coin}\rightarrow\text{orange}\rightarrow\text{G} \mid \text{setlemon}\rightarrow\text{W})$
$\text{W} = (\text{coin}\rightarrow\text{lemon}\rightarrow\text{W} \mid \text{setorange}\rightarrow\text{G})$

Jel.: $f(B) = \{f(x) \mid x \in B\}$

f^{-1} inverz fv.; $f \circ g$; f^* (elemenként)

Átcimkézés:

(1) $f(STOP_A) = STOP_{f(A)}$

(2) $f(x{:}B \to P(x)) = (y{:}f(B) \to f(P(f^{-1}(y))))$

(3) $f(P||Q) = f(P)||f(Q)$

(4) $f(\mu X{:}A.F(X)) = (\mu Y{:}f(A).f(F(f^{-1}(Y))))$

(5) $f(g(P)) = (f \circ g)(P)$

(6) $traces(f(P)) = \{f^*(s) \mid s \in traces(P)\}$

(7) $f(P)/f^*(s) = f(P/s)$

D.: Címkézés: $\quad P \quad l{:}P \overset{\text{def.}}{::=} f_l(P)$

$$\forall x \in \alpha P\text{: } f_l(x) = l.x$$

Pl.: (1) $(\text{left:VMS}) \parallel (\text{right:VMS}) \neq (\text{VMS} \parallel \text{VMS}) = \text{VMS}$

(2) $b{:}\text{BOOL} \parallel c{:}\text{BOOL} \parallel \text{USER}$

$b{:=}\text{false};\ P \leadsto b.\text{assign}.0 \to P$

$b{:=}\neg c;\ P \leadsto (c.\text{fetch}.0 \to b.\text{assign}.1 \to P \mid c.\text{fetch}.1 \to b.\text{assign}.0 \to P)$

$\uparrow$ ennek az értelmezése ez $\uparrow$

(3) l, m számlálók (kezdetben: l=0, m=3)

l.around, m.around - teszt l illetve m nulla-e

$(l{:}CT_0 \| m{:}CT_3 \| USER)$

$\boxed{m := m+1;}$ $P \rightsquigarrow m.up \rightarrow P$

$\boxed{\text{if } l=0 \text{ then } P \text{ else } Q}$ $\rightsquigarrow$ $l.around \rightarrow P \mid l.down \rightarrow l.up \rightarrow Q$

$\boxed{\text{m:=m+l;}}$ $\quad P \rightsquigarrow \text{ADD}$

$$\text{ADD} = \text{DOWN}_0$$

$$\text{DOWN}_i = (\text{l.down}\to\text{DOWN}_{i+1} | \text{l.around}\to\text{UP}_i)$$

$$\text{UP}_0 = \text{P}$$

$$\text{UP}_{i+1} = \text{l.up}\to\text{m.up}\to\text{UP}_i$$

Pl.: Kis egészek halmaza

αEL = {in, no, yes}

EL = in$\rightarrow$no$\rightarrow$ μX.(in$\rightarrow$yes$\rightarrow$X)
/azt vizsgálja volt-e már in esemény/

SET3 = (0:EL) || (1:EL) || (2:EL) || (3:EL)

Halmazt lehet így kezelni:

m:SET3 $||$ USER

α(m:SET3) = {m.2.in, ...}

if 2$\in$m then P else (m:=m$\cup${2};Q)

m.2.in$\rightarrow$(m.2.yes$\rightarrow$P | m.2.no$\rightarrow$Q)

Halmazzal cimkézés

/D.:/ L : P   c helyett l.c   l$\in$L

minden alkalommal más l választható (környezet)

/több folyamat nem jön létre/

/Pl.:/ αLACKEY = {sits down, gets up}

LACKEY = (sits down$\rightarrow$gets up$\rightarrow$LACKEY)

L = {0,1,2,3,4}

SHARED LACKEY = (L : LACKEY)

1 lakáj, de 5·2=10 esemény

(ha a filozófusoknál alk., akkor csak 1 lehet
egyidejûleg az asztalnál.)

/Mindig más lehet a cimke./

{0,1}:LACKEY : teljes bináris fát ad

Specifikációk

L1:

P sat S

Q sat T

$\Rightarrow \forall$ tr $\in$ traces(P||Q): S(tr$\uparrow \alpha$P) $\wedge$ T(tr$\uparrow \alpha$Q))

Mgj.: $\rightarrow$ unió tétel

kompozícionális

Ez a modell használhatóságát biztosítja.

Példa: (1) $\alpha P = \{a,c\}$ $P = (a \to c \to P)$

$\alpha Q = \{b,c\}$ $Q = (c \to b \to Q)$

Mgj.: $(tr \uparrow A) \downarrow a = tr \downarrow a$, ha $a \in A$ (*)

Állítás: $(P || Q)$ sat $0 \leq tr \downarrow a - tr \downarrow b \leq 2$

Biz.:

$$\text{P sat } (0 \le \text{tr}{\downarrow}\text{a} - \text{tr}{\downarrow}\text{c} \le 1)$$

$$\text{Q sat } (0 \le \text{tr}{\downarrow}\text{c} - \text{tr}{\downarrow}\text{b} \le 1)$$

$$\underset{(L1,*)}{\Rightarrow} \text{(P||Q) sat } (0 \le \text{tr}{\downarrow}\text{a} - \text{tr}{\downarrow}\text{c} \le 1 \land 0 \le \text{tr}{\downarrow}\text{c} - \text{tr}{\downarrow}\text{b} \le 1) \quad \diamond$$

D.: Egy folyamat soha nem áll le, ha $\forall$s: P/s $\neq$ STOP.

L2: Ha P és Q soha nem áll le és $|(\alpha P \cap \alpha Q)| \leq 1$,
akkor (P||Q) soha nem áll le.

Pl.: P||Q (az elõzõ pl.) soha nem áll le, mert $\alpha P \cap \alpha Q = \{c\}$

L3: P sat S $\Rightarrow$ $\forall$ tr $\in$ traces(f(P)): (S(f^{-1}(tr))).

Determinisztikus folyamatok elmélet (Leíró szemantika)

Emlékeztető (58.o):

traces(P) prefix-zárt:

L6: $<> \in$ traces(P)

L7: s^t $\in$ traces(P) $\Rightarrow$ s $\in$ traces(P)

L8: traces(P) $\subseteq$ (αP)*

Mgj.: (αP, traces(P)) megfelel L6, L7, L8-nak.

Mgj.: Egy (A,S) pár, ami kielégíti L6,L7,L8-at
(kölcsönösen egyértelműen) azonosít egy folyamatot (P)

Mgj.:

- $P^0 = \{x \mid <x> \in S\}$ $(\subseteq \alpha P)$ $S \subseteq A^*$ és prefix-zárt.

  $\forall x \in P^0$: $P(x) = \{t \mid <x>\hat{\ }t \in S\}$

  $\alpha P = A$, $P = (x{:}P^0 \rightarrow P(x))$

- Ezzel a történet alapján megkonstruáltuk a folyamatot.

Def.: Determinisztikus folyamat (a külsõ program el tudja dönteni mit csinál ...)

egy (A,S) pár, ahol $S \subseteq A^*$ és $<> \in S$, $\forall s,t$: $s\hat{}t \in S \Rightarrow s \in S$

Def.: $STOP_A = (A,\{<>\})$

Def.: $RUN_A = (A,A^*)$

Def.: $(x{:}B \rightarrow (A, S(x)))$

$$= (A, \{<>\} \cup \{<x>\hat{\ }s \mid x \in B \wedge s \in S(x)\})$$

ha $B \subseteq A$

Def.: $(A,S)/s = (A, \{t, (s\hat{\ }t) \in S\})$, ha $s \in S$

Def.: $\mu X.A.F(X) = (A, \bigcup_{n \geq 0} \mathrm{traces}(F^n(STOP_A)))$,

ha F õreseménnyel ellátott.

Def.: $(A,S) \parallel (B,T)$

$$= (A \cup B, \{s \mid s \in (A \cup B)^* \wedge (s \uparrow A) \in S \wedge (s \uparrow B) \in T\})$$

Def.: $f(A,S) = (f(A), \{f^*(s) \mid s \in S\})$, ha f függvény

Mgj.: a jobb oldali párok megfelelnek a prefix-zártság követelményének.

Nemdeterminisztikus folyamatok

a) Belső nemdeterminizmus (belső eseménytől függ)

$$\mathsf{P} \sqcap \mathsf{Q}$$

$$\alpha(\mathsf{P} \sqcap \mathsf{Q}) = \alpha\mathsf{P} = \alpha\mathsf{Q}$$

Példa:

$$\begin{aligned}\mathsf{CH5D} = (\mathsf{in5p} \rightarrow ((&\mathsf{out1p}\rightarrow\mathsf{out1p}\rightarrow\mathsf{out1p}\rightarrow\mathsf{out2p}\rightarrow\mathsf{CH5D}) \\ &\sqcap (\mathsf{out2p}\rightarrow\mathsf{out1p}\rightarrow\mathsf{out2p}\rightarrow\mathsf{CH5D})))\end{aligned}$$

(L1) $P \sqcap P = P$

(L2) $P \sqcap Q = Q \sqcap P$

(L3) $P \sqcap (Q \sqcap R) = (P \sqcap Q) \sqcap R$

(L4) $x \rightarrow (P \sqcap Q) = (x \rightarrow P) \sqcap (x \rightarrow Q)$

(L5) $(x{:}B \rightarrow (P(x) \sqcap Q(x))) = (x{:}B \rightarrow P(x)) \sqcap (x{:}B \rightarrow Q(x))$

(L6) $P || (Q \sqcap R) = (P || Q) \sqcap (P || R)$

(L7) $(P \sqcap Q) || R = (P || R) \sqcap (Q || R)$

(L8) $f(P \sqcap Q) = f(P) \sqcap f(Q)$

Mj.: $P = \mu X.((a \rightarrow X) \sqcap (b \rightarrow X))$

$Q = (\mu X.(a \rightarrow X)) \sqcap (\mu X.(b \rightarrow X))$

$P \neq Q$

Pl.: $<a,b,b,a,b> \in$ traces(P)

$<a,b,b,a,b> \notin$ traces(Q)

/traces(Q) $\subseteq$ traces(P)/

Történetek:

(1) $\text{traces}(P \sqcap Q) = \text{traces}(P) \cup \text{traces}(Q)$

(2)
$$
\begin{aligned}
(P \sqcap Q)/s &= Q/s &&, \text{ha } s \in (\text{traces}(Q) \text{ - } \text{traces}(P))\\
&= P/s &&, \text{ha } s \in (\text{traces}(P) \text{ - } \text{traces}(Q))\\
&= (P/s) \sqcap (Q/s) &&, \text{ha } s \in (\text{traces}(P) \cap \text{traces}(Q))
\end{aligned}
$$

b) Külső nemdeterminizmus (környezettől függ)

$$\mathsf{P} \;\Box\; \mathsf{Q}$$

$$\alpha(\mathsf{P} \;\Box\; \mathsf{Q}) = \alpha\mathsf{P} = \alpha\mathsf{Q}$$

Mj.: $(\mathsf{c}{\rightarrow}\mathsf{P} \;\Box\; \mathsf{d}{\rightarrow}\mathsf{Q}) = (\mathsf{c}{\rightarrow}\mathsf{P} \mid \mathsf{d}{\rightarrow}\mathsf{Q})$ ha $\mathsf{c}{\neq}\mathsf{d}$

$$(\mathsf{c}{\rightarrow}\mathsf{P} \;\Box\; \mathsf{c}{\rightarrow}\mathsf{Q}) = (\mathsf{c}{\rightarrow}\mathsf{P}) \sqcap (\mathsf{c}{\rightarrow}\mathsf{Q})$$

(L1) $P \square P = P$

(L2) $P \square Q = Q \square P$

(L3) $P \square (Q \square R) = (P \square Q) \square R$

(L4) $P \square STOP = P$

(L5) $(x{:}A \rightarrow P(x)) \, \Box \, (y{:}B \rightarrow Q(y))$

$= (z{:}(A \cup B) \rightarrow (\textbf{if } z \in (A - B) \textbf{ then } P(z)$

$\textbf{else if } z \in (B - A) \textbf{ then } Q(z)$

$\textbf{else if } z \in (A \cap B) \textbf{ then } (P(z) \sqcap Q(z))))$

(L6) $P \, \Box \, (Q \sqcap R) = (P \, \Box \, Q) \sqcap (P \, \Box \, R)$

(L7) $P \sqcap (Q \, \Box \, R) = (P \sqcap Q) \, \Box \, (P \sqcap R)$

Történetek:

(1) $\text{traces}(P \;\square\; Q) = \text{traces}(P) \cup \text{traces}(Q)$

(2)
$$
\begin{aligned}
(P \;\square\; Q)/s &= Q/s &&\text{, ha } s \in (\text{traces}(Q) \text{ - } \text{traces}(P))\\
&= P/s &&\text{, ha } s \in (\text{traces}(P) \text{ - } \text{traces}(Q))\\
&= (P/s) \sqcap (Q/s) &&\text{, ha } s \in (\text{traces}(P) \cap \text{traces}(Q))\\
& && \text{és } s \neq <>
\end{aligned}
$$

Megszorítás:

$$P \backslash C$$

$$\alpha(P \backslash C) = (\alpha P) - C$$

Pl.: VMS = NOISYVM$\backslash${clink,clunk,toffee}

$$(L1)\ P\backslash\{\} = P$$

$$(L2)\ (P\backslash B)\backslash C = P\backslash(B \cup C)$$

$$(L3)\ (P \sqcap Q)\backslash C = (P\backslash C) \sqcap (Q\backslash C)$$

$$(L4)\ (STOP_A)\backslash C = STOP_{A\ -\ C}$$

$$\text{(L5) } (x \to P) \backslash C = x \to (P \backslash C) \quad \text{, ha } x \notin C$$
$$= P \backslash C \quad \text{, ha } x \in C$$

$$\text{(L6) } (P || Q) \backslash C = (P \backslash C) || (Q \backslash C) \text{ , ha } (\alpha P \cap \alpha Q) \cap C = \{\}$$

$$\text{(L7) } f(P \backslash C) = f(P) \backslash f(C)$$

$$\text{(L8) } (x{:}B \to P(x)) \backslash C = (x{:}B \to (P(X) \backslash C)) \text{, ha } B \cap C = \{\}$$

(L9) $(x{:}B \rightarrow P(x)) \backslash C = \bigsqcap_{x:B} (P(X) \backslash C)$,
, ha $B \subseteq C$ és B véges, illetve nem üres.

(L10) $(x{:}B \rightarrow P(x)) \backslash C = Q \sqcap (Q \,\square\, (x{:}(B - C) \rightarrow (P(x) \backslash C)))$,
, ha $C \cap B \neq \{\}$ és véges.

, ahol $Q = \bigsqcap_{x:B \cap C} (P(X) \backslash C)$

Történetek:

(1) traces(P$\backslash$C) = $\{$t$\uparrow$(αP - C) | t $\in$ traces(P)$\}$

, feltéve, hogy $\forall$ s $\in$ traces(P): $\neg$diverges(P/s,C)

, ahol diverges(P,C) = $\forall$ n: $\exists$ s $\in$ traces(P)$\cap$C*: #s>n

(2) (P$\backslash$C)/s = ($\bigsqcap_{t \in T}$ P/t)$\backslash$C

, ahol T = traces(P)$\cap\{$t | t$\uparrow$(αP - C) = s$\}$

, feltéve, hogy T véges és s $\in$ traces(P$\backslash$C)

Specifikációk:

Ha P sat S
és Q sat T

$\Rightarrow$ (P $\sqcap$ Q) sat (S $\vee$ T)

Ha P sat S
és Q sat T
és sem P sem Q nem tartalmaz végtelen sok belső eseményt

$\Rightarrow$ (P $\Box$ Q) sat (**if** tr = <> **then** (S $\wedge$ T) **else** (S $\vee$ T))

Kommunikáció

- speciális esemény

- Jele: $c.v$, ahol c a csatorna neve, v az átküldött érték

- c-n átküldhető üzenetek: $\alpha c(P) = \{v \mid c.v \in \alpha P\}$

- $channel(c.v) = c \qquad message(c.v) = v$

$(c!v \rightarrow P) = (c.v \rightarrow P)$

$(c?x \rightarrow P(x)) = (y:\{y \mid channel(y) = c\} \rightarrow P(message(y)))$

Pl.: COPYBIT = $\mu X.(in?x \rightarrow (out!x \rightarrow X))$

, ahol $\alpha in(COPYBIT) = \alpha out(COPYBIT) = \{0,1\}$

– input csatorna

– output csatorna

Pl.: c a P folyamat output csatornája és a Q folyamat input csatornája

(P || Q) rendszer kommunikálhat a c-n keresztül (egy irányban)

$\alpha c\mathsf{P} = \alpha c\mathsf{Q}$

Példák:

(1) $\alpha left$(COPY) = $\alpha right$(COPY)

COPY = μX(left?x$\rightarrow$right!x$\rightarrow$X)

(2) $\alpha left = \alpha right =$ **N**

DOUBLE = μX(left?x$\rightarrow$right!(x+x)$\rightarrow$X)

(3) $\alpha left = \{s \mid s \in \alpha right^* \ \wedge \ \#s = 80\}$

UNPACK = $P_{<>}$

, ahol $P_{<>}$ = left?s$\rightarrow P_s$

és $P_{<x>}$ = right!x$\rightarrow P_{<>}$

és $P_{<x>\frown s}$ = right!x$\rightarrow P_s$

(4) $\alpha left_1 = \alpha left_2 = \alpha right$

MERGE = (left$_1$?x→right!x→MERGE
| left$_2$?x→right!x→MERGE)

(5) $\alpha left = \alpha right$

VAR = left?x→VAR$_x$

, ahol VAR$_x$ = (left?y→VAR$_y$
| right!x→VAR$_x$)

$$\text{(6)} \quad \mathsf{BUFFER} = \mathsf{P}_{<>}$$

$$, \text{ ahol } \mathsf{P}_{<>} = \mathsf{left?x}{\rightarrow}\mathsf{P}_{<x>}$$

$$\text{és } \mathsf{P}_{<x>\hat{}s} = (\mathsf{left?y}{\rightarrow}\mathsf{P}_{<x>\hat{}s\hat{}<y>} \mid \mathsf{right!x}{\rightarrow}\mathsf{P}_{s})$$

$$\text{(7)} \quad \mathsf{STACK} = \mathsf{P}_{<>}$$

$$, \text{ ahol } \mathsf{P}_{<>} = (\mathsf{empty}{\rightarrow}\mathsf{P}_{<>} \mid \mathsf{left?x}{\rightarrow}\mathsf{P}_{<x>})$$

$$\text{és } \mathsf{P}_{<x>\hat{}s} = (\mathsf{right!x}{\rightarrow}\mathsf{P}_{s} \mid \mathsf{left?y}{\rightarrow}\mathsf{P}_{<y>\hat{}<x>\hat{}s})$$

Specifikációk

$$tr \downarrow c \; = \; message^*(tr \uparrow \alpha c)$$

Jelölés: $tr \downarrow right \leq tr \downarrow left$ helyett $right \leq left$

$$s \overset{n}{\leq} t \; = \; (s \leq t \land \#t \leq \#s + n)$$

Pl: $s \overset{0}{\leq} t \Longleftrightarrow s = t$

$$s \overset{n}{\leq} t \;\land\; t \overset{m}{\leq} u \Rightarrow s \overset{m+n}{\leq} u$$

$$s \leq t \;\Rightarrow\; s \overset{n}{\leq} t$$

COPY **sat** $right \overset{1}{\leq} left$

DOUBLE **sat** $right \overset{1}{\leq} double^*(left)$

UNPACK **sat** $right \leq \hat{}/left$

, ahol $\hat{}/< s_0, s_1, ..., s_{n-1} > = s_0\hat{}s_1\hat{}...\hat{}s_{n-1}$

MERGE **sat** $\exists r : right \overset{1}{\leq} r \;\wedge\; r \; interleaves(left_1, left_2)$

BUFFER **sat** $right \leq left$

Kommunikációs szabályok:

(L1) $(\mathsf{c!v} \rightarrow \mathsf{P}) \parallel (\mathsf{c?x} \rightarrow \mathsf{Q(x)}) = \mathsf{c!v} \rightarrow (\mathsf{P} \parallel \mathsf{Q(v)})$

(L2) $((\mathsf{c!v} \rightarrow \mathsf{P}) \parallel (\mathsf{c?x} \rightarrow \mathsf{Q(x)})) \backslash \mathsf{C} = (\mathsf{P} \parallel \mathsf{Q(v)}) \backslash \mathsf{C}$

, ahol $\mathsf{C} = \{c.v \mid v \in \alpha c\}$

Adatcsatorna

$$\xrightarrow{left} \boxed{\text{P}} \xrightarrow{right}$$

$$\xrightarrow{left} \boxed{\text{Q}} \xrightarrow{right}$$

A P és Q folyamatot összeilleszthetjük úgy, hogy a P folyamat $left$ csatornáját összekapcsoljuk a Q folyamat $right$ csatornájával.

Jelölés: P$\gg$Q

$$\xrightarrow{left} \boxed{\text{P}} \longrightarrow \boxed{\text{Q}} \xrightarrow{right}$$

$$\alpha(\mathsf{P}\gg\mathsf{Q}) = \alpha left(\mathsf{P})\cup\alpha left(\mathsf{Q})$$

$$\alpha right(\mathsf{P}) = \alpha left(\mathsf{Q})$$

Példák:

$$QUADRUPLE \ = \ DOUBLE \gg DOUBLE$$

$$UNPACK \gg PACK$$

, ahol $PACK$:

$\alpha right = \{s \mid s \in \alpha left^* \wedge \#s = 125\}$

$PACK = P_{<>}$

$P_s = right!s \to P_{<>}$ ha $\#s = 125$

$P_s = left?x \to P_{s\hat{}<x>}$ ha $\#s < 125$

$$UNPACK \gg BUFFER \gg PACK$$

$$COPY \gg UNPACK \gg PACK \gg COPY$$

$$COPY \gg COPY$$

Szabályok

(L1) $P \gg (Q \gg R) = (P \gg Q) \gg R$

(L2) $(right!v \to P) \gg (left?y \to Q(y)) = P \gg Q(v)$

(L3) $(right!v \to P) \gg (right!w \to Q)$
$$= right!w \to ((right!v \to P) \gg Q)$$

(L4) $(left?x \to P(x)) \gg (left?y \to Q(y))$
$$= left?x \to (P(x) \gg (left?y \to Q(y)))$$

$$
\begin{aligned}
\text{(L5)}\ (left?x \to P(x)) \gg (right!w \to Q)& \\
= (left?x \to (P(x) \gg (right!w \to Q))& \\
|right!w \to ((left?x \to P(x)) \gg Q))&
\end{aligned}
$$

$$
\begin{aligned}
\text{(L6)}\ (left?x \to P(x)) \gg R \gg (right!w \to Q)& \\
= (left?x \to (P(x) \gg R \gg (right!w \to Q))& \\
|right!w \to ((left?x \to P(x)) \gg R \gg Q))&
\end{aligned}
$$

(L7) Ha R egy folyamatlánc és a folyamatok mindegyike úgy indul, hogy ír a kimenő ($right$) csatornájára:

$$R \gg (right!w \rightarrow Q) = right!w \rightarrow (R \gg Q)$$

(L7) Ha R egy folyamatlánc és a folyamatok mindegyike úgy indul, hogy olvas a bemenő ($left$) csatornájáról:

$$(left?x \rightarrow P(x)) \gg R = left?x \rightarrow (P(x) \gg R)$$

Mûveleti szemantika

D.: $<$Proc, Act, $\rightarrow>$, ahol Act $=$ Com $\cup \{\tau\}$
(τ - nem lehet rá szinkronizálni)

$\rightarrow$: /konfiguráció átmenet/

(1) div $\xrightarrow{\tau}$ div   div: divergáló folyamat

(2) P $\xrightarrow{\tau}$ div

(3) (a$\rightarrow$P) $\xrightarrow{a}$ P   /a két $\rightarrow$ nem ugyanaz/

(4a) $P \sqcap Q \xrightarrow{\tau} P$ belsõ nemdeterminisztikusság

(4b) $P \sqcap Q \xrightarrow{\tau} Q$

(5a) $$\frac{P \xrightarrow{a} P'}{P \Box Q \xrightarrow{a} P' \quad Q \Box P \xrightarrow{a} P'}$$ külsõ nemdeterminisztikusság

(5b) $$\frac{P \xrightarrow{\tau} P'}{P \Box Q \xrightarrow{\tau} P' \Box Q \quad Q \Box P \xrightarrow{\tau} Q \Box P'}$$

(6) $$\frac{\mathsf{P} \xrightarrow{a} \mathsf{P'} \qquad \mathsf{Q} \xrightarrow{a} \mathsf{Q'}}{\mathsf{P}||_A\mathsf{Q} \xrightarrow{a} \mathsf{P'}||_A\mathsf{Q'}} \quad a \in \mathsf{A}$$ szinkronizálni kell

$$\frac{\mathsf{P} \xrightarrow{\alpha} \mathsf{P'}}{\mathsf{P}||_A\mathsf{Q} \xrightarrow{\alpha} \mathsf{P'}||_A\mathsf{Q} \qquad \mathsf{Q}||_A\mathsf{P} \xrightarrow{\alpha} \mathsf{Q}||_A\mathsf{P'}} \quad \alpha \notin \mathsf{A}$$

nem kell szinkronizálni

(7) átnevezés

$$\frac{\mathsf{P} \xrightarrow{a} \mathsf{P'}}{\mathsf{P[b/a]} \xrightarrow{b} \mathsf{P'[b/a]}} \qquad \frac{\mathsf{P} \xrightarrow{\alpha} \mathsf{P'}}{\mathsf{P[b/a]} \xrightarrow{\alpha} \mathsf{P'[b/a]}} \quad \alpha \neq \mathsf{a}$$

(8) $$\frac{\mathsf{P} \xrightarrow{a} \mathsf{P'}}{\mathsf{P}\backslash\mathsf{a} \xrightarrow{\tau} \mathsf{P'}\backslash\mathsf{a}}$$

$$\frac{\mathsf{P} \xrightarrow{\alpha} \mathsf{P'}}{\mathsf{P}\backslash\mathsf{a} \xrightarrow{\alpha} \mathsf{P'}\backslash\mathsf{a}} \quad \alpha \neq \mathsf{a}$$

(9) $$\frac{\mathsf{P[rec\ x.P/x]} \xrightarrow{\alpha} \mathsf{Q}}{\mathsf{rec\ x.P} \xrightarrow{\alpha} \mathsf{Q}}$$

Mgj.: A három szemantika ugyanazt jelenti.

Vajon tényleg ugyanaz-e? Be kell bizonyítani!

Felépítünk egy algebrai nyelvet. Ezzel az ilyen kérdés bizonyítható.

Robin Milner CCS – A Calculus of Communicating Systems

Keretrendszer párhuzamos, egymással kommunikáló folyamatok elemzésére szolgáló rendszerekhez.

CCS	CSP
$a.P$	$a \longrightarrow P$
$(a.P) + (b.Q)$	$(a \longrightarrow P \mid b \longrightarrow Q)$
NIL	$STOP$

$P|Q$ kompozíció

$P \setminus \alpha$ megszorítás (α-t, $\widehat{\alpha}$-t kivesszük)

$P[S]$ átnevezés (S függvény, ahol $\widehat{S(\alpha)} = S(\widehat{\alpha})$)

Különbség CCS-ben megjelenik a belső esemény: τ.

CCS keretrendszer különböző modellek részére.

Egy modellben a folyamatok között lehet gyengébb egyenlőség mint CCS-ben (több egyezés), de erősebb (kevesebb egyezés) nem.

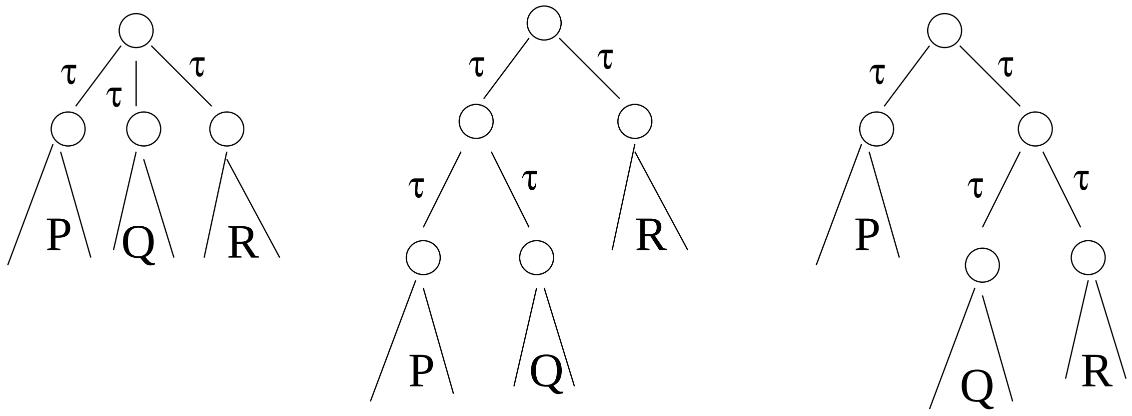
CCS-ben nincs $\sqcap$, de lehet modellezni:

$(\tau.P) + (\tau.Q)$ megfelel $P \sqcap Q$-nak

$(\tau.P) + (a.Q)$ megfelel $P \sqcap (P \Box (a \to Q))$-nak

nem teljes egyezés, pl. nem asszociatív

Az alábbi folyamatok különböznek:

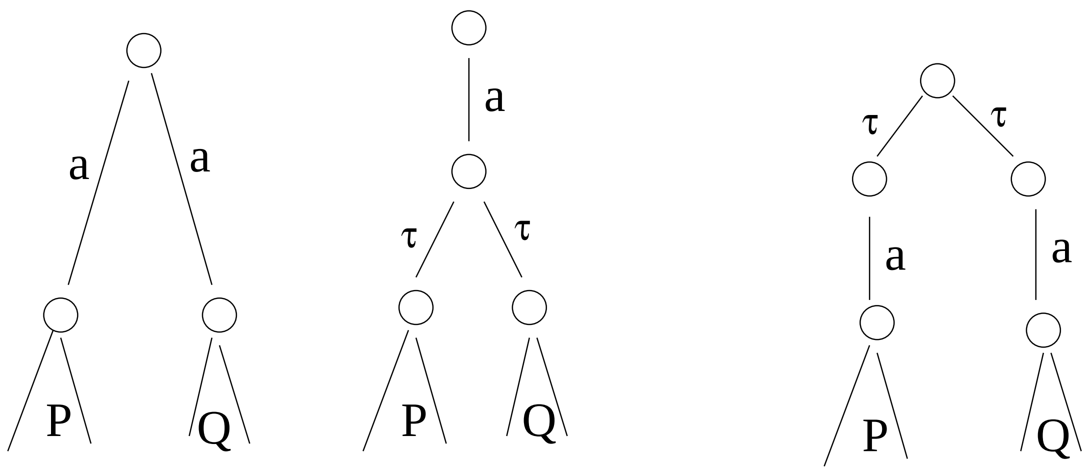


$$(\tau.P) + (\tau.Q) + (\tau.R)$$

$$(\tau.((\tau.P) + (\tau.Q))) + (\tau.R)$$

$$(\tau.P) + (\tau.((\tau.Q) + (\tau.R)))$$

Az alábbi folyamatok is különböznek,ha $P \neq Q$:



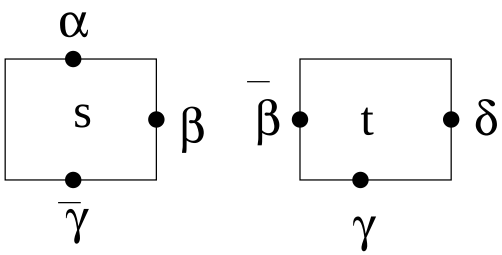
$(a.P) + (a.Q)$

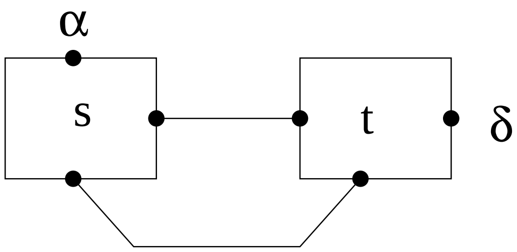
$a.((\tau.P) + (\tau.Q))$

$(\tau.(a.P)) + (\tau.(a.Q))$

Szinkronizáció bonyolultabb.

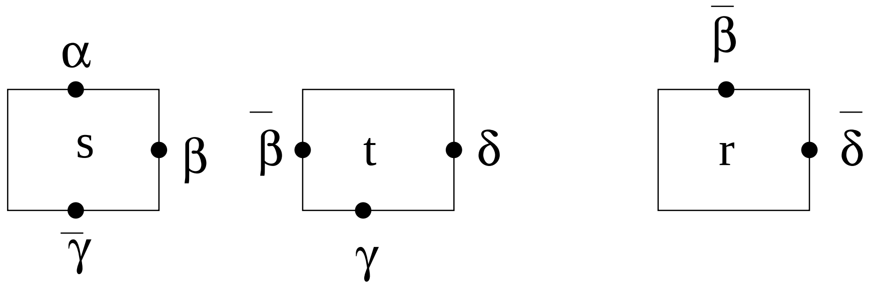
Egy a eseményt $\widehat{a}$ eseménnyel szinkronizálunk.

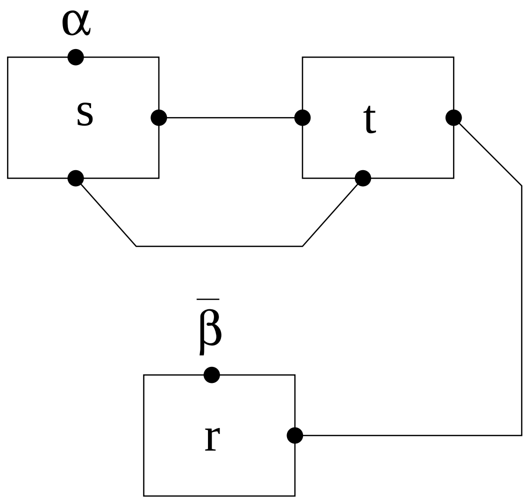


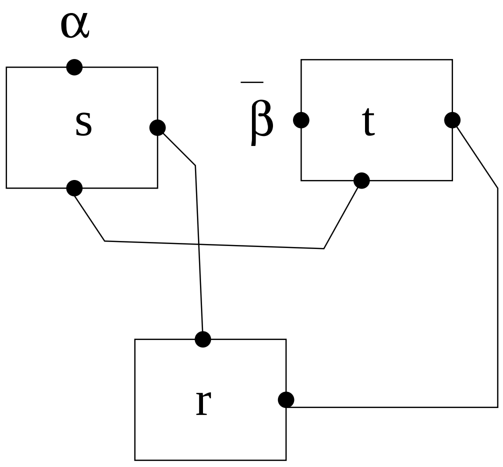


s||t

Ez a művelet nem asszociatív.



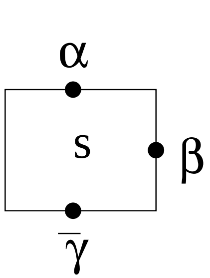


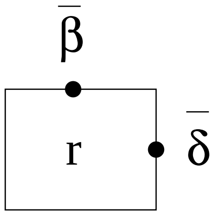


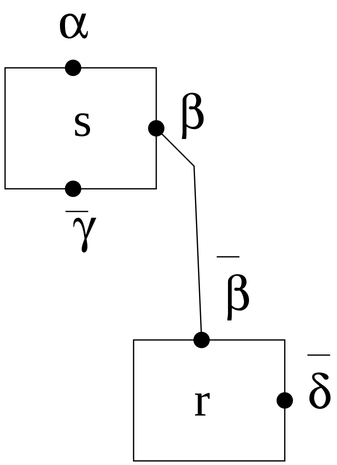
$r \parallel (s \parallel t)$

$(r \parallel s) \parallel t$

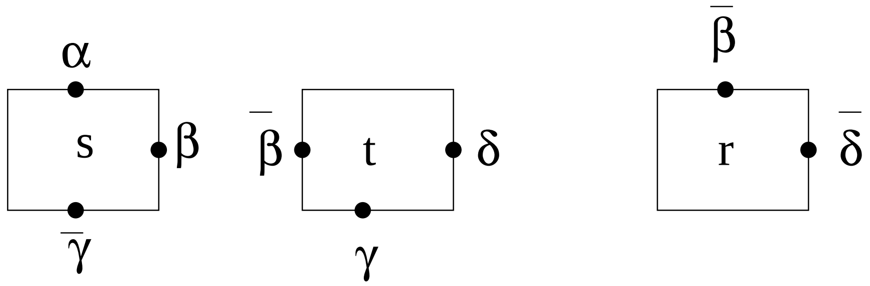
Kompozíció.

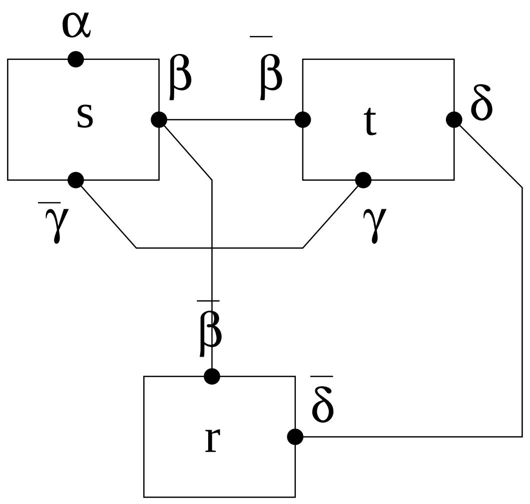






$r \mid s$


s
t
r
α
β
$\bar{\beta}$
$\bar{\gamma}$
γ
δ
$\bar{\delta}$


s
t
r
α
β
$\bar{\beta}$
$\bar{\gamma}$
γ
δ
$\bar{\delta}$

r | (s| t)

$$(a.P)|(b.Q) = a.(P|(b.Q)) + b.((a.P)|Q)$$

$$(a.P)|(a.Q) = a.(P|(a.Q)) + a.((a.P)|Q)$$

$$(a.P)|(\widehat{a}.Q) = \tau.(P|Q) + a.(P|\widehat{a}.Q) + \widehat{a}.((a.P)|Q)$$

Tételsor:

(1) Cimkézett állapotátmenetrendszer, műveleti szemantika (levezetési szabályok, equ).

(2) Leíró szemantika fogalma, kapcsolata a műveleti szemantikával.

(3) Axiomatikus szemantika, kapcsolata előző szemantikákkal, új műveleti szemantika.

(4) CSP, folyamat, abc, stop, $a \rightarrow P$, $X = F(X)$, $x \rightarrow P | y \rightarrow Q$, példák (kölcsönös rekurzióig).

(5) CSP alap axiómák (L1, L2), ezek alapján folyamatok ekvivalenciája, pl.

(6) Történethalmazok, mûveletek a történeteken, mûveletek alapvető tulajdonságai, parciális rendezés történetek felett, monotonitás.

(7) CSP folyamatok leíró szemantikájának definíciója (folyamatok történethalmazai), pl.

(8) CSP folyamatok specifikációja. Megfelelés definíciója, pl.

(9) Párhuzamosság CSP-ban (megegyező,eltérő abc), evõ filozófusok.

(10) Folyamatcsaládok, címkézés, halmazzal címkézés.

(11) Determinisztikus folyamatok elmélet, belső nemdeterminizmus.

(12) Külső nemdeteminizmus, megszorítás.

(13) Kommunikáció, adatcsatorna (példák).

(14) CSP folyamatok mûveleti szemantikája.

(15) CCS, CCS és CSP közötti különbségek.