Tételsor:

(1) Cimkézett állapotátmenetrendszer, pl.

(2) Mûveleti és leíró szemantika fogalma, pl. (equ, PS)

(3) CSP, folyamat, abc, stop, a$\rightarrow$P, X=F(X), x$\rightarrow$P|y$\rightarrow$Q, pl.

(4) CSP alap axiómák, folyamatok ekvivalenciája, pl.

(5) Történethalmazok, mûveletek a történeteken, mûveletek tulajdonságai, parciális rendezés történetek felett, monotonitás

(6) CSP folyamatok leíró szemantikájának definíciója, pl.

(7) CSP folamatok mûveleti szemantikája.

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

(9) Párhuzamosság CSP-ban, evõ filozófusok

(10) Cimkézés, többszörös cimkézés

---

(11) folyamat algebra fogalom rendszere, szignatúra, $\sum$ algebra, kifejezés algebra, $\sum$ homomorfizmus, kongruencia, hányados algebra, pl.

(12) Homomorfizmus tétel, izomorfia tétel, kezdeti-, elérhetõ- algebra, pl.

(13) Kongruencia és algebra vizsonya, teljesen absztrakt algebra tételek, pl., leíró szemantikával ekvivalens mûveleti szemantika.

(14) Szabad kifejezés algebra, egyértelmû kiterjesztési tétele, helyettesítés, helyettesítési lemma

(15) Egyenlõségi axióma következtetési szabályai, a modell fogalma, pl.

(16) Leíró és axiomatikus szemantika kapcsolata (teljesség, helyesség), pl.

Tematika: - CSP
- CCS /- gyak-ban nem haszn. $\rightarrow$ Okam $\rightarrow$ Ada taszk/
- Lotos (eszköze: ARATools) /gyak-ban használják/

/Mgj.: Ezekhez a nyelvekhez különféle/ szemantikák /adhatók/: - mûveleti
- leíró
- axiomatikus

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

• $\rightarrow^* \subseteq$ C $\times$ A* $\times$ C /tranzitív lezárt/
(c, $\varepsilon$, c)$\in\rightarrow^*$
Ha (c,a,c')$\in\rightarrow$ és (c',s,c")$\in\rightarrow^*$, akkor (c,as,c")$\in\rightarrow^*$, ahol a$\in$A, s$\in$A*.
C $\times$ C felett $\rightarrow^*$ a $\rightarrow$ 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 | ap | p+q 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) $\dfrac{p \xrightarrow{a}_1 p'}{p+q \xrightarrow{a}_1 p'}$ /Ha p az a után p'-ként viselkedik, akkor p+q az a után tud p'-ként viselkedni./
(3) $\dfrac{p \xrightarrow{a}_1 p'}{q+p \xrightarrow{a}_1 p'}$
nil-re nincs levezetési szabály, mert nem kezdeményez eseményt.

D.: *Folyamat és környezete*
(p,e)$\in$P $\times$ P p $\|$ e: $\dfrac{p \xrightarrow{a}_1 p' \quad e \xrightarrow{a}_1 e'}{p \| e \xrightarrow{a}_2 p' \| e'}$ /Ha "a" és "b" $\Rightarrow$ elakad, és ha "a" és $\emptyset$ $\Rightarrow$ még mûködik./ (*)
Specifikációs módszer: "e" megadása (absztrakció).

D.: *p megfelel e környezetnek*, ha ($\forall$ e',p': p $\|$ e $\rightarrow_2^*$ p' $\|$ e': e'=nil)
/$\rightarrow_2^*$ itt folyamat párokra vonatkozik. (p' $\|$ e' $\not\rightarrow_2$)/

D.: /I. *Mûveleti szemantika*/

/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 ellvileg egy képet kapok, és az alapján döntök./

/D.:/ $\mathcal{P}(A^*)$ trace (történet !) (lineáris szerkezet /, elemi események sorozatainak halmaza/)

$\tau$: $P \to \mathcal{P}(A^*)$ /- szemantikus leképezés/

/P - folyamat./

/**Szabályok:**/ (1) $\tau[[nil]] = \{\varepsilon\}$ (#)

(2) $\tau[[ap]] = a\,\tau[[p]]$ /- $\forall$ olyan sorozat, amit "p" produkál és "a" van az elején/

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

Mgj.: /- Közös eseményekre szinkronizálni kell!!!/

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

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

Kérdés: A két szemantika azonos-e? $\left(p_1 \equiv p_2 \overset{?}{\Leftrightarrow} \tau(p_1)=\tau(p_2)\right)$

/Válasz: nem/

/D.:/ $\mathcal{O}$: $P \to \mathcal{P}(p)$ $\mathcal{O}(p) \overset{def}{=} \{e \mid p \text{ megfelel e-nek}\}$

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

Lemma: $\tau[[a(p+q)]] = \tau[[ap+aq]]$ /A szelektív várakozást csak a bal oldal képes megoldani./

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

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

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

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

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

$a(p+q) \overset{a}{\to} (p+q) \overset{a}{\to} p_1$ $ap+aq \longrightarrow p \to p_1$

$aa\underline{nil}$ $a\underline{nil}$ $\underline{nil}$ $aa\underline{nil}$ $\searrow$ q ! /nem megy tovább/

$a\underline{nil}$ $\diamond$

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

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

$p \neq nil$ $\tau[[p+nil]] \neq \tau[[p]]$ /ha p elején nem ugyanolyan elem van, mint e elején./

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

(2') $\tau[[ap]] = a\,\tau[[p]] \cup \{\varepsilon\}$ esetén már $\tau[[p+nil]] = \tau[[p]]$

Köv.: $\forall$ p$\in$P: $\tau[[p]]$ 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.: $ab\underline{nil} + ac\underline{nil} \overset{mûv.}{=} (ab\underline{nil}+ac\underline{nil}) + a(b\underline{nil}+c\underline{nil})$ (E1-E4-bõl nem levezethetõ.)

<u>D.:</u> *Új mûveleti szemantika*

$L_1 = \langle C_1, A, \to_1 \rangle$, $L_2 = \langle C_2, A, \to_2 \rangle$, $p_1 \in C_1$, $p_2 \in C_2$:

$p_1 \approx_B p_2 \overset{def.}{::=} \exists\, R \subseteq C_1 \times C_2$ (1) $(p_1,p_2) \in R$

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

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

/<u>Mgj.:</u> Ha kitörlöm a közepét, akkor biszimuláció./

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

<u>Mgj.:</u> /- 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*

/<u>Mgj.:</u> - axiomatikus szemantika - verifikálás (helyességellenõrzés) miatt kell

- leíró szemantika - részprogramok viselkedésérõl tudnak következtetni az összetett programra (program szintézis)
- mûveleti szemantika - milyen lépéseket hajt végre a program (helyesség bizonyításra nem alkalmas)
- összehasonlításuk nehéz/

<u>Pl.:</u> Példanyelv TCSP

- szekvenciális folyamatok
- együttmûködés: aszinkron
- kommunikáció: szinkron, szimmetrikus /A szinkron, szimmetrikus miatt holtpontba vagy divergenciába juthat a rendszer./

  holtpont, divergencia /dolgozik a rendszer csak semmit nem csinál (abort)/

<u>Jel.:</u> Com - kommunikációs események,

Id - folyamatazonosítók

<u>D.:</u> P := stop - holtpont

| div - divergencia (abort)

| a $\to$ P - prefix

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

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

| P $\|_A$ Q - szinkronizált párhuzamos

| 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/,

Proc = $\{p \in Rec \mid FV(p) = \emptyset\}$ /FV(p) - p szabad változóinak halmaza (free variable)/

<u>Pl.:</u> P folyamat abc-je: $\alpha$P /néha A-val jelölik/

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

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

<u>Mgj.:</u> $\alpha(x \to P) = \alpha P$ $x \in \alpha P$ /kikötés/

(1) (coin $\to$ $STOP_{\alpha VMS}$) /- bevesz egy érmét és megáll/ (X1)

(2) (coin $\to$ choc $\to$ coin $\to$ choc $\to$ $STOP_{\alpha VMS}$) (X2)

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

CTR = (right $\to$ up $\to$ right $\to$ right $\to$ $STOP_{\alpha CTR}$)

<u>Mgj.:</u> $\left.\begin{matrix} x \to y \\ P \to Q \end{matrix}\right\}$ rossz, mert x $\to$ (y $\to$ STOP) jó

(4) $\alpha$CLOCK = {tick} **Rekurzió:** (tick $\to$ CLOCK) = CLOCK

$\uparrow$ /óraketyegés/

(tick $\to$ tick $\to$ CLOCK) = CLOCK

CLOCK = (tick $\to$ tick $\to$ tick $\to$ CLOCK)

<u>Mgj.:</u> 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) $CLOCK = \mu X{:}\{tick\}.(tick \to X)$

(2) $VMS = (coin \to choc \to VMS)$ $\quad VMS = \mu X{:}\{coin, choc\}.(coin \to choc \to X)$

(3) 5p váltó: $\alpha CH5A = \{in5p, out2p, out1p\}$

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

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

D.: /*Összetett folyamat abc-je*/ $\quad \alpha(x \to P \mid y \to Q) = \alpha P \quad \{x,y\} \subseteq \alpha P, \alpha P = \alpha Q$

Pl.: (1) $(up \to STOP \mid right \to right \to up \to STOP)$

(2) $CH5C = in5p \to (out1p \to out2p \to out1p \to out1p \to CH5C) \mid$
$(out2p \to out1p \to out2p \to CH5C)$

(3) $VMCT = \mu X.coin \to (choc \to X \mid toffee \to X)$ $\quad$ (X4)

$VMCT = coin \to (choc \to VMCT \mid toffee \to VMCT)$

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

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

(5) $VMCRED = \mu X.(coin \to choc \to X \mid choc \to coin \to X)$ - hitelezõ gép.

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

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

$COPYBIT = \mu X.(in.0 \to out.0 \to X \mid in.1 \to out.1 \to X)$

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

csak: $(x \to P \mid y \to Q \mid ... \mid z \to R)$ $\quad$ ($x \neq y$, $y \neq z$, $x \neq z$ determinisztikus)

$(x \to P \mid (y \to Q \mid z \to R))$ hibás!!! /a belsõ elágazást nem bírja az õrzés miatt/

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

Pl.: $B = \{x,y,z\}$ $\quad (s: B \to P(s)) = (x \to P(x) \mid y \to P(y) \mid z \to P(z))$

Pl.: (1) $\alpha RUN_A = A \quad A = \{x_1, ..., x_n\}$

$RUN_A = (x: A \to RUN_A) = (x_1 \to RUN_A \mid \ldots \mid x_n \to RUN_A)$ bármikor, bármelyik esemény kiválasztható

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

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

Mgj.: $\mid, \to, STOP$ mint speciális esetek megadhatók.

Pl.: (kölcsönös rekurzió)

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

$DD = (setorange \to G \mid setlemon \to W)$

$G = (coin \to orange \to G \mid setlemon \to W)$

$W = (coin \to lemon \to W \mid setorange \to G)$

(2) Mgj.: $\infty$ egyenlõséghalmaz is megadható

$CT_n$, ha n távolsára van a földtõl.

$CT_0 = (up \to CT_1 \mid around \to CT_0)$

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

Mgj.: gépi állapottal megjeleníthetõ

Pl.: Gépi állapot ezért $\square$-ok nincsenek.

Axiómák: /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)/

$(x\text{: } A \rightarrow P(x)) = (y\text{: } B \rightarrow Q(y)) \Leftrightarrow A=B \wedge \forall x \in A\text{: } P(x) = Q(x)$

(és az abc is "=")

**Alkalmazás /axiomatikus szemantikában/:**

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

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

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.: $R(x) = \left\{ \begin{smallmatrix} P\text{, ha } x = c \\ Q\text{, ha } x = d \end{smallmatrix} \right.$

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

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

Pl.: (1) (coin→choc→coin→choc→STOP) ≠ (coin→STOP)
Biz.: L1D, L1A
(2) $\mu$X.(coin→(choc→X|toffee→X)) = $\mu$X.(coin→(toffee→X|choc→X))
Biz.: L1C

$\boxed{\text{L2:}}$ Ha F(X) prefix, õrzött kifejezés, akkor Y=F(Y)-nak egyértelmûen létezik megoldása. ( Y=F(Y) ⇔ Y=$\mu$X.F(X) ) /Ez az egyenlõség azért jó, mert leíró szemantikában is igaz./

L2A: $\mu$X.F(X) = F($\mu$X.F(X))

Pl.: (3) VM1 = (coin→VM2)     VM2 = (choc→VM1)
Á.: VM1 = VMS
ui.: VM1 = (coin→VM2) = (coin→(choc→VM1))
VM1 ugyanannak a rekurzív egyenlõségnek a megoldása, mint a VMS. ◇

/Mgj.: rekurzív egyenleteknek nem mindig egyértelmû a megoldása ⇒ monotonitás kihasználható/

D.: *Kölcsönösen rekurzív egyenlõségek halmaza*

i ∈ S - indexhalmaz (S) eleme
X(i) - folyamat
F(i,X) - õrzött kifejezés
}⇒ X(i)=F(i,X)
X(i)=$F_i$(X)     X[1..n]

Axióma: Ha ∀i∈S: ( $X_i$=F(i,X) és $Y_i$=F(i,Y) ) ⇒ X=Y     /X,Y - megoldáshalmazok/
(∃! X(1) ... X(i) ... X(m) megoldáshalmaz)

Mgj.: - ∀ folyamat x:B→F(x) alakra hozható, /így/ $\mu$X.(x:B→F(x,X)) is:
(x:B→F(x,$\mu$X.(x:B→F(x,X)))) (L2A)     ↑ x=x:B→F(x,X) megoldása
- Az elsõ x∈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.: Összefûzés: sˆt.

pl.: <coin, choc>ˆ<coin, toffee> = <coin, choc, coin, toffee>

L1: sˆ<> = <>ˆs =s /az üres sorozat (<>) az egységelem/

L2: sˆ(tˆu) = (sˆt)ˆu /asszociatív/

L3: sˆt = sˆu ⇔ t = u

L4: sˆt = uˆt ⇔ s = u

L5: sˆt = <> ⇔ s = <> és t = <>

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

D.: f disztributív, ha f(sˆt) = f(s)ˆf(t)     /elemenként alkalmazható/
/definiálható egyelemû 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.: Megosztás (vetítés) A-ra: $t\uparrow A$
Pl.: (<around, up, down, around>)↑{up, down} = <up, down>
L1: $<>\uparrow A = <>$ /szigorú/
L2: $(s\hat{}t)\uparrow A = (s\uparrow A)\hat{}(t\uparrow A)$ /disztr./
L3: $<x>\uparrow A = <x>$, ha $x\in A$ /disztr. miatt ∀ sorozatra def./
L4: $<x>\uparrow A = <>$, ha $x\notin A$ /disztr. miatt ∀ sorozatra def./
L5: $s\uparrow\{\} = <>$ /elõzõekbõl kijön/ (biz.: s hossza szerinti indukcióval)
L6: $(s\uparrow A)\uparrow B = s\uparrow(A\cap B)$ (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: $(<x>\hat{}s)' = x$
L3: $s = (<s_0>\hat{}s')$, ha $s\neq<>$
L4: $s = t \Leftrightarrow ((s = t = <>) \vee (s_0 = t_0 \wedge t' = s'))$
D.: A* - Az A elemeinek összes véges sorozata (<> is)
D.: $A^* = \{s \mid s\uparrow A = s\}$
L1: $<>\in A^*$
L2: $<x>\in A^* \Leftrightarrow x\in A$
L3: $(s\hat{}t)\in A^* \Leftrightarrow s\in A^* \wedge t\in A^*$
L4: $A^* = \{t \mid t = <> \vee (t_0 \in A \wedge t'\in A^*)\}$ A* rekurzív definíciója

## Rendezés (parciális)

D.: $(s \leq t)$ s prefixe t-nek, ha $\exists u$: $s\hat{}u = t$.
Mgj.: legkisebb elem: <>
L1: $<> \leq s$ $/<>\hat{}s = s/$ legkisebb
L2: $s \leq s$ $/s\hat{}<> = s/$ reflexív a rendezés
L3: $s \leq t \wedge t \leq s \Rightarrow s = t$ antiszimmetrikus
L4: $s \leq t \wedge t \leq u \Rightarrow s \leq u$ tranzitív
L5: $(<x>\hat{}s) \leq t \Leftrightarrow t \neq <> \wedge x = t_0 \wedge s \leq t'$ (prefix rekurzív)
L6: $s \leq u \wedge t \leq u \Rightarrow s \leq t \vee t \leq s$
D.: s in t = ($\exists$u,v: $t = u\hat{}s\hat{}v$)
L1: <> in t
L2: t in t
L3: t in s ∧ s in t ⇒ s = t
L4: s in t ∧ t in u ⇒ s in u /L1-L4 is parciális rendezés/
L5:(L7) $(<x>\hat{}s)$ in t ⇒ $t \neq <> \wedge ((t_0 = x \wedge s \leq t') \vee (<x>\hat{}s$ in $t'))$
L6:(L8) $s \leq t \Rightarrow (s\uparrow A) \leq (t\uparrow A)$
(↑ monoton a prefix parciális rendezésre nézve; a vetítés megtartja a rendezést)
Lemma: ∀disztributív (sorozatra elemenként feld.) fv.
monoton a prefix parciális rendezésre.
Biz.: $s \leq t$, $s\hat{}u = t$ → $f(t) = f(s\hat{}u) = f(s)\hat{}f(u)$ → $f(s) \leq f(t)$ ◇
Lemma: "^" monoton a második argumentumára nézve (kétváltozós)
Biz.: $t \leq u \Rightarrow s\hat{}t \leq s\hat{}u$ ◇

D.: Minden argumentumában monoton többváltozós függvényt monotonnak nevezünk.
D.: Hossz: #t $\qquad$ #<x,y,x> = 3
L1: #<> = 0
L2: #<x> = 1
L3: #<sˆt> = #s + #t
L4: $\#(t\uparrow(A\cup B)) = \#(t\uparrow A) + \#(t\uparrow B) - \#(t\uparrow(A\cap B))$
L5: $s \leq t \Rightarrow \#s \leq \#t$
L6: $\#(t^n) = n(\#t)$
D.: $s\downarrow x = \#(s\uparrow\{x\})$ /hányszor fordul elõ egy (x) esemény s-ben/

Folyamatok történethalmaza

Pl.: (1) traces(STOP) = {<>}
(2) traces(coin→STOP) = {<>, <coin>}
(3) traces($\mu$X.coin→choc→X) = {s | ∃n> s≤<coin,choc>$^n$} /rekurzív csokigép/
(4) traces($\mu$X.tick→X) = {tick}*
L1: traces(STOP) = {t | t = <>}
L2: traces(c→P)={t | t=<> ∨ ($t_0$=c ∧ t'∈traces(P))}={<>}∪{<c>ˆt | t∈traces(P)}
L3: traces(c→P|d→Q) = {t| t=<> ∨ ($t_0$=c ∧ t'∈traces(P)) ∨ ($t_0$=d ∧ t'∈traces(Q))}
L4: traces(x:B→P(x)) = {t | t = <> ∨ ( $t_0$ ∈B ∧ t'∈traces(P($t_0$)) ) }
L5: X = F(X) rekurzív folyamat esetén: $F^0(X) = X$ (*)
$F^{n+1}(X) = F(F^n(X))$ /$F^\omega$ - végtelen hatványa F-nek/
Ha F õresemény definiált, akkor traces($\mu$X:A.F(X)) = $\bigcup_{n\geq 0}$ traces($F^n(STOP_A)$)
/F monoton és folytonos legyen/
pl.: lf nem folytonos, mert Ha $Q_i \Rightarrow Q_{i+1}$, akkor lf(S,$Q_i$) ⇒ lf(S,$Q_{i+1}$) és
lf(S,∨$Q_i$) ≠ ∨lf(S,$Q_i$)
És nem is monoton, mert lf(S,lub($Q_i$)) = lub(lf(S,$Q_i$)) /lub≡sup/
Mgj.: - láncfolytonos F esetén elég véges n-re számolni $F^n$-t.
- monotonitás kell ahhoz, hogy számolni tudjam a rekurzív F-et.
- (*) jobboldalának kiszámítása egyszerû, mert n véges. (Folytonos F esetén)
Pl.: (1) $RUN_A$ = $\mu$X:A.F(X) ($RUN_A$ := x:A→$RUN_A$)
F(X) = (x:A→X) (∼)
Á.: Traces($RUN_A$) = A*
Biz.: L5 alapján elegendõ belátni, hogy
traces($F^n(STOP_A)$) = {s | s∈A* ∧ #s≤n} ∀n-re
$\boxed{n=0:}$ traces($STOP_A$) = {<>} = {s | s∈A* és #s≤0} (**)
mert: $F^0(STOP_A) = STOP_A$
$\boxed{n\to n+1:}$ traces($F^{n+1}(STOP_A)$) $\underset{(**)}{=}$ traces($F(F^n(STOP_A))$) $\underset{(\sim)}{=}$
traces(x:A→$F^n(STOP_A)$) $\underset{L4}{=}$ {t | t=<> ∨ ($t_0$ ∈A ∧ t'∈traces($F^n(STOP_A)$))}
$\underset{indukció}{=}$ {t | t = <> ∨ ( $t_0$ ∈A ∧ (t'∈A* ∧ #t'≤n) ) } $\underset{konkat.,\ \#}{=}$
{t|t=<> ∨ (($t_0$ ∈A ∧ t'∈A*) ∧ #t'≤n+1)}={t|t∈A* ∧ #t≤n+1)}⋄
(2) traces(VMS) = $\bigcup_{n\geq 0}${s|s≤<coin,choc>$^n$}; A={choc,coin}
Biz.: ind. felt.: traces($F^n_{VMS}(STOP_A)$)={t|t≤<coin,choc>$^n$}, ahol F(X)=(coin→choc→X)
$\boxed{n=0:}$ traces($STOP_A$) = {<>} = {s|s≤<coin,choc>$^0$}
$\boxed{n\to n+1:}$ traces(coin→choc→$F^n(STOP_A)$) $\underset{L2,L2}{=}$
{<>,<coin>}∪{<coin,choc>}∪{t|traces($F^n(STOP_A)$)} $\underset{ind.hip.}{=}$
{<>,<coin>}∪{<coin,choc>ˆt|t≤<coin,choc>$^n$} =

$\{s \mid s=\langle\rangle \vee s=\langle coin\rangle \vee \exists t\rangle\ s=\langle coin,choc\rangle\hat{\ }t \wedge t\leq\langle coin,choc\rangle^n\} =$
$\{s \mid s\leq\langle coin,choc\rangle^{n+1}\}$ $\diamond$

Prefix zárt: L6: $\langle\rangle\in$traces(P)
L7: $s\hat{\ }t\in$traces(P) $\Rightarrow$ $s\in$traces(P)

L8: traces(P) $\subseteq (\alpha P)^*$

További mûveletek

D.: • $f:A\to B$ $f^*:A^*\to B^*$ (f elemenként) $f^*(\langle\rangle) = \langle\rangle$
$f^*(\langle x\rangle) = \langle f(x)\rangle$
$f^*(s\hat{\ }t) = f^*(s)\hat{\ }f^*(t)$

- $\hat{\ }/\langle\langle 1,3\rangle,\langle\rangle,\langle 7\rangle\rangle = \langle 1,3\rangle\hat{\ }\langle\rangle\hat{\ }\langle 7\rangle = \langle 1,3,7\rangle$; $\hat{\ }/s$
- összefésülés $s\in$interleaving(t,u) /az összes lehetséges módon összefésüli/
  pl.: $t = \langle 1,6,5,2,7\rangle$ $u = \langle 3,1,4\rangle$ $\Rightarrow$ $s = \langle 1,6,3,1,5,4,2,7\rangle$
- s[i] - az s i. eleme /0-val kezdõdik az indexelés/
- megfordítás: $\overline{\langle 3,5,37\rangle} = \langle 37,5,3\rangle$
- kiválasztás: $s = \langle\underbrace{a.7}_{\text{rendezett pár}}, b.9, a.8, c.0\rangle$ $\left.\begin{array}{l} s\downarrow a=\langle 7,8\rangle \\ s\downarrow d=\langle\rangle \end{array}\right\}$ ha párok sorozatára értelmezzük "$\downarrow$"-ot
- kompozíció: "$\surd$" - sikeres terminálás, a történet utolsó eleme

L1: $s;t = s$ , ha $\neg(\langle\surd\rangle$ in s) szigorú konkatenáció: ";" /ha nincs $\surd$, akkor nem tudom folytatni/

L2: $(s\hat{\ }\langle\surd\rangle);t = s\hat{\ }t$ , ha $\neg(\langle\surd\rangle$ in s)

L2A: $(s\hat{\ }\langle\surd\rangle\hat{\ }u);t = s\hat{\ }t$ , ha $\neg(\langle\surd\rangle$ in s)

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

(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 = NOLOSS$\wedge$FAIR1 = $(0\leq((tr\downarrow coin)-(tr\downarrow choc))\leq 1)$
(4) VMCFIX = $(\neg(\langle in1p\rangle^3$ in tr)) /- 3 db. 1 penny-s nincs egymás után/
(5) MENDVMC = ($tr\in$traces(VMC)$\wedge$VMCFIX) /a (4)-es javítása/
(6) $0\leq((tr\downarrow coin)-(tr\downarrow choc))\leq 2$ /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 $\langle\rangle$ 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 ($tr = \langle\rangle$)

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

L4C: P sat S(tr) "$\Rightarrow$" $c\to d\to P$ sat ($tr\leq\langle c,d\rangle \vee (tr\geq\langle c,d\rangle \wedge S(tr''))$)
/ha $tr\leq\langle c,d\rangle$ $\Rightarrow$ $tr\in\{\langle\rangle,\langle c\rangle,\langle c,d\rangle\}$/

L4D: P sat S(tr) és Q sat T(tr) "$\Rightarrow$"
$(c\to P|d\to Q)$ 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(tr,x)) "$\Rightarrow$"
$(x:B\to P(x))$ sat ( $tr=\langle\rangle \vee (tr_0 \in B \wedge S(tr',tr_0))$ ) /elágazás lev. szabálya/

D.: P/s ::= P az s-beli események után. /P folytatása s után/ pl.: $(d\to Q)/d = Q$

*/Rekurzió lev. szabályai:/*

L5: P sat $S(tr_1)$ és $s\in$traces(P) "$\Rightarrow$" (P/s) sat $S(s\hat{\ }tr_2)$

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

VMS = (coin→(choc→VMS)) F(X) = (coin→(choc→X))

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

VMSPEC = (0≤((tr↓coin)-(tr↓choc))≤1)

Biz.: $\left.\begin{array}{l}(tr=<>) \Rightarrow VMSPEC\\ STOP\ sat\ (tr=<>)\end{array}\right\} \underset{LS}{\Rightarrow}$ STOP sat VMSPEC

Tfh. X sat (0≤((tr↓coin)-(tr↓choc))≤1) $\overset{L4C}{\Rightarrow}$

F(X)=(coin→choc→X) sat

(tr≤<coin,choc> ∨ (tr≥<coin,choc> ∧ 0≤((tr"↓coin)-(tr"↓choc))≤1))

$\overset{(*)}{\Rightarrow}$ VMSPEC

(*) (1) <>↓coin = <>↓choc = 0

(<coin>↓coin)=(<coin,choc>↓coin)=(<coin,choc>↓choc)=1; <coin>↓choc=0

(2) tr≥<coin,choc> ⇒ tr↓coin=tr"↓coin+1 ∧ tr↓choc=tr"↓choc+1. ◇

Párhuzamosság /folyamatokat (+ környezeteket) rakunk össze zárt rendszerré/

**Egyenlõre:** $\alpha$P = $\alpha$Q (spec. eset) /$\alpha$ - az abc/

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

Pl.: (1) GRCUST = (toffee→GRCUST|choc→GRCUST|coin→choc→GRCUST)

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

VMCT = $\mu$X.coin→(choc→X|toffee→X)

(GRCUST || VMCT) = $\mu$X.(coin→choc→X) (Így karamellát sosem ad.)

(2) FOOLCUST = (in2p→large→FOOLCUST|in1p→large→FOOLCUST)

(FOOLCUST || VMC) = $\mu$X.(in2p→large→X|in1p→STOP) /in1p esetén holtpontba kerül a gép/

L1: P || Q = Q || P /azonos abc-k mellett/

L2: P || (Q || R) = (P || Q) || R

L3A: P || $STOP_{\alpha P}$ = $STOP_{\alpha P}$ /P minden eseménye közös a STOP-pal/

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

L4A: (c→P) || (c→Q) = (c→(P || Q))

L4B: (c→P) || (d→Q) = STOP , ha c≠d (holtpont)

L4: (x:A→P(x)) || (y:B→Q(y)) = (z:(A∩B)→(P(z) || Q(z)))

/Mgj.: Ez még mindig Hoar féle axiómarendszer./

Pl.: $\left.\begin{array}{l}P = (a\to b\to P|b\to P)\\ Q = (a\to(b\to Q|c\to Q))\end{array}\right\}$ ⇒ P||Q = (a→((b→P)||(b→Q|c→Q)) = a→(b→(P||Q)) =

= $\mu$X.(a→b→X)

*Történetekre vonatkozó szabályok:*

L1: traces(P||Q) = traces(P)∩traces(Q)

L2: (P||Q)/s = (P/s)||(Q/s) (Q/s - Q mûködése s eseménysorozat után)

**Általánosítás:** $\alpha$P ≠ $\alpha$Q, $\alpha$(P||Q) = $\alpha$P∪$\alpha$Q

Pl.: (1) $\alpha$NOISYVM = {coin,choc,toffee,clink,clunk}

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

$\alpha$CUST = {coin,choc,curse,toffe} /curse - szidalmaz/

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

(NOISYVM||CUST) =

$\mu$X.(coin→(clink→curse→choc→clink→X|curse→clink→choc→clink→X)

(2) $\alpha$P = {up,down} P = (up→down→P)

$\alpha$Q = {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: $(c\to P) \parallel (c\to Q) = (c\to(P \parallel Q))$

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

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

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

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

L7: $\left.\begin{matrix} P = (x{:}A\to P(x)),\ A\subseteq\alpha P \\ Q = (y{:}B\to Q(y)),\ B\subseteq\alpha Q \end{matrix}\right\}\Rightarrow (P||Q) = (z{:}C\to P'||Q')$, ahol

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

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

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

Pl.: $\alpha P=\{a,c\}$, $\alpha Q=\{b,c\}$,   $P=(a\to c\to P)$, $Q=(c\to b\to Q)$

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

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

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

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

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

*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>

$\left.\begin{matrix} t1\uparrow\alpha NOISYVM = \langle coin,clink\rangle\in traces(NOISYVM) \\ t1\uparrow\alpha CUST = \langle coin,curse\rangle\in traces(CUST)\end{matrix}\right\}\Rightarrow t1\in traces(NOISYVM \parallel CUST)$

t2 = <coin,curse,clink>$\in$traces(NOISYVM || CUST)

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

L3B: Ha $\alpha P = \alpha Q \Rightarrow traces(P||Q) = traces(P)\cap traces(Q)$

Ábrák:

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

$\alpha PHIL_i$ = {i.sits down, i.gets up, i.picks up fork.i, i.picks up fork.($i\oplus1$), i.puts down fork.i, i.puts down fork.($i\oplus1$)}

$PHIL_i$ = (i.sits down$\to$i.picks up fork.i$\to$i.picks up fork.($i\oplus1$)$\to$ i.puts down fork.i$\to$i.puts down fork.($i\oplus1$)$\to$i.gets up$\to PHIL_i$)

$\alpha FORK_i$ = {i.picks up fork.i, ($i\ominus1$).picks up fork.i, i.puts down fork.i, ($i\ominus1$).puts down fork.i}

$FORK_i$ = (i.picks up fork.i$\to$i.puts down fork.i$\to FORK_i$ | ($i\ominus1$).picks up fork.i$\to$($i\ominus1$).puts down fork.i$\to FORK_i$)

$PHILOS = (PHIL_0||PHIL_1||PHIL_2||PHIL_3||PHIL_4)$

FORKS = $(\mathrm{FORK}_0||\mathrm{FORK}_1||\mathrm{FORK}_2||\mathrm{FORK}_3||\mathrm{FORK}_4)$
COLLEGE = (PHILOS||FORKS)

$\mathrm{LEFT}_i = (\text{i.sits down}\rightarrow \mu X.(\text{i.picks up fork.i}\rightarrow\text{i.puts down fork.i}\rightarrow X|\text{i.gets up}\rightarrow \mathrm{LEFT}_i))$
$\alpha\mathrm{LEFT}_i = \{\text{i.sits down, i.picks up fork.i, i.puts down fork.i, i.gets up}\}$
$\mathrm{LEFT}_i = (\text{i.sits down}\rightarrow\text{i.picks up fork.i}\rightarrow\text{i.puts down fork.i}\rightarrow\text{i.gets up}\rightarrow\mathrm{LEFT}_i)$
$\alpha\mathrm{RIGHT}_i = \{\text{i.sits down, i.picks up fork.}(i\oplus 1)\text{, i.puts down fork.}(i\oplus 1)\text{, i.gets up}\}$
$\mathrm{RIGHT}_i = (\text{i.sits down}\rightarrow\text{i.picks up fork.}(i\oplus 1)\rightarrow\text{i.puts down fork.}(i\oplus 1)\rightarrow$
$\text{i.gets up}\rightarrow\mathrm{RIGHT}_i)$
$\mathrm{PHIL}_i = \mathrm{LEFT}_i||\mathrm{RIGHT}_i$
$\alpha\mathrm{FOOT} = \bigcup_{i=0}^{4}\{\text{i.sits down, i.gets up}\},\quad U = \bigcup_{i=0}^{4}\{\text{i.gets up}\},\quad D = \bigcup_{i=0}^{4}\{\text{i.sits down}\}$
$\mathrm{FOOT}_0 = (x{:}D\rightarrow\mathrm{FOOT}_1)$
$\mathrm{FOOT}_j = (x{:}D\rightarrow\mathrm{FOOT}_{j+1} \mid y{:}U\rightarrow\mathrm{FOOT}_{j-1})\qquad j\in\{1,2,3\}$
$\mathrm{FOOT}_4 = (y{:}U\rightarrow\mathrm{FOOT}_3)$
NEWCOLLEGE = (COLLEGE || $\mathrm{FOOT}_0$)
Á.: (NEWCOLLEGE/s) $\neq$ STOP $\quad\forall s\in$traces(NEWCOLLEGE) /Holtpont?/
/Mgj.: Ha nem több, mint 4-en ülnek az asztalnál, akkor nincs holtpont./
Biz.: D.: seated(s) = $\#(s\uparrow D)$ - $\#(s\uparrow U)$ /- most hányan ülnek; s - történet/
SÁ.: Mivel $s\uparrow(U\cup D)\in$traces($\mathrm{FOOT}_0$) $\Rightarrow$ seated(s)$\leq 4$ /biz. kell/
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.$\diamond$

Géppel: Állapotok száma: PHIL: 6
FORK: 3
COLLEGE: $6^5\times 3^5 \approx 18$ millió $\rightarrow$ 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)
$f{:}\alpha P\rightarrow A$ (eseménynévcsere)
f(P) — f(c)-t hajt végre, amikor P c-t hajt végre $\}\Rightarrow \alpha(f(P)) = f(\alpha(P))$
traces(f(P)) = $\{f^*(s) \mid s\in$traces(P)$\}$ /f* - elemenként/

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)
$\mathrm{LR}_0 = f(\mathrm{CT}_0)$ $/\mathrm{CT}_0||\mathrm{CT}_0 = \mathrm{CT}_0$ átcimkézés nélkül/
(3) a sarokban around LRUD = $\mathrm{LR}_0||\mathrm{CT}_0$

(4) copybit-ek összekapcsolása

$f(out.0) = g(in.0) = mid.0$

$f(out.1) = g(in.1) = mid.1$

$f(in.0) = in.0 \quad f(in.1) = in.1$

$g(out.0) = out.0 \quad g(out.1) = out.1$

$CHAIN2 = f(COPYBIT)||g(COPYBIT)$ /szinkronizált kommunikáció a mid eseményekre/

(5) Logikai vált. (0,1)

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

fetch.0 fetch.1 $\quad$ $fetch \leftrightarrow \binom{coin\to lemon}{coin\to orange}$

$BOOL = f(DD) \quad DD = (setorange\to G \mid setlemon\to W)$

$G = (coin\to orange\to G \mid setlemon\to W)$

$W = (coin\to lemon\to W \mid setorange\to G)$

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

(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.: Cimkézés: $\quad P \quad l{:}P \overset{def.}{::=} f_l(P)$

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

Pl.: (1) $(left{:}VMS) \mid\mid (right{:}VMS) \neq (VMS||VMS) = VMS$

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

$b{:}=false; \quad P\rightsquigarrow b.assign.0\to P$

$\underset{\uparrow}{b{:}=\neg c}; \quad P\rightsquigarrow\underset{\uparrow}{(c.fetch.0}\to b.assign.1\to P|c.fetch.1\to b.assign.0\to P)$

ennek az értelmezése ez

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

Kérdés: 0-e: l.around, m.around

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

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

ha $l=0 \Rightarrow P \rightsquigarrow l.around\to P \mid$

kül. $\Rightarrow Q \rightsquigarrow l.down\to l.up\to Q$

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

$ADD = DOWN_0$

$DOWN_i = (l.down\to DOWN_{i+1}|l.around\to UP_i)$

$UP_0 = P$

$UP_{i+1} = l.up\to m.up\to UP_i$

Pl.: Kis egészek halmaza

$\alpha EL = \{in, no, yes\}$ $\quad$ csak berakni lehet

$EL = in\to no\to \mu X.(in\to yes\to X)$ $\quad$ /volt-e már in esemény/

$SET3 = (0{:}EL) \mid\mid (1{:}EL) \mid\mid (2{:}EL) \mid\mid (3{:}EL)$

$m{:}SET3 \mid\mid USER$

$\alpha(m{:}SET3) = \{m.2.in, ...\}$

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

$m.2.in\to(m.2.yes\to P \mid m.2.no\to Q)$

[[

Halmazzal cimkézés

/D.:/ L : P c helyett l.c $l \in L$ minden alkalommal más l választható (környezet) /több folyamat nem jön létre/

/Pl.:/ $\alpha$LACKEY = {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 $5 \cdot 2 = 10$ esemény

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

/Mindig más lehet a cimke./

LACKEY: {0,1}:LACKEY

Specifikációk

/Á.:/ Tfh. P sat S(tr) $\forall$tr $\in$ traces(P): S(tr)

Q sat T(tr) tr $\in$ traces(P||Q)

S(tr $\uparrow \alpha$P) (tr $\uparrow \alpha$P) $\in$ trace(P)

T(tr $\uparrow \alpha$Q) (tr $\uparrow \alpha$Q) $\in$ trace(Q)

$\Rightarrow$ (P||Q) sat (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$\rightarrow$c$\rightarrow$P)

$\alpha$Q = {b,c} Q = (c$\rightarrow$b$\rightarrow$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.:/ P sat ($0 \leq$tr$\downarrow$a - tr$\downarrow$c$\leq 1$)

Q sat ($0 \leq$tr$\downarrow$c - tr$\downarrow$b$\leq 1$)

(*), (**) $\Rightarrow$ (P||Q) sat ($0 \leq$tr$\downarrow$a - tr$\downarrow$c$\leq 1$ $\wedge$ $0 \leq$tr$\downarrow$c - tr$\downarrow$b$\leq 1$) $\diamond$

/D.:/ $\forall$s: P/s$\neq$STOP Ekkor nem áll le.

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

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

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

Determinisztikus folyamatok elmélet (Leíró szemantika)

**traces(P) prefix-zárt:** L6: <>$\in$traces(P)

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

L8: traces(P) $\subseteq$ ($\alpha$P)*

/Mgj.:/ ($\alpha$P, traces(P)) megfelel L6, L7, L8-nak.

/Mgj.:/ (A,S) - (kölcsönösen egyértelmûen) azonosít egy folyamatot (P)

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

$\forall x \in P^0$: P(x) = {t|<x>^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 ...)
(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.: $(x: B \to (A, S(x))) = (A, \{<>\} \cup \{<x>\hat{}s \mid x \in B \land s \in S(x)\})$
Def.: (D5) $\mu X.A.F(X) = (A, \bigcup_{n \geq 0} traces(F^n(STOP_A)))$, ha F õreseménnyel ellátott.
Def.: $f(A,S)/s = (A, \{t, (s\hat{}t) \in S\})$, ha $s \in S$
Mgj.: a jobb oldali párok megfelelnek a prefix-zártság követelményének.
Def.: $(A,S) \mid\mid (B,T) = (A \cup B, \{s \mid s \in (A \cup B)^* \land (s \uparrow A) \in S \land (s \uparrow B) \in T\})$

Mûveleti szemantika
/D.:/ $<Proc, Act, \to>$, ahol $Act = Com \cup \{\tau\}$ ($\tau$ - nem lehet rá szinkronizálni)
$\to$: /konfiguráció átmenet/
(1) $div \xrightarrow{\tau} div$ div: divergáló folyamat
(2) $P \xrightarrow{\tau} div$
(3) $(a \to P) \xrightarrow{a} P$ /a két $\to$ nem ugyanaz/
(4a) $P \sqcap Q \xrightarrow{\tau} P$ belsõ nemdeterminisztikusság
(4b) $P \sqcap Q \xrightarrow{\tau} Q$
(5a) $\dfrac{P \xrightarrow{a} P'}{P \square Q \xrightarrow{a} P' \quad Q \square P \xrightarrow{a} P'}$ Külsõ nemdeterminisztikusság
(5b) $\dfrac{P \xrightarrow{\tau} P'}{P \square Q \xrightarrow{\tau} P' \square Q \quad Q \square P \xrightarrow{\tau} Q \square P'}$
(6) $\dfrac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P \mid\mid_A Q \xrightarrow{a} P' \mid\mid_A Q'}$ $a \in A$
szinkronizálni kell
$\dfrac{P \mid\mid_A Q \xrightarrow{\alpha} P' \mid\mid_A Q'}{P \mid\mid_A Q \xrightarrow{\alpha} P' \mid\mid_A Q \quad Q \mid\mid_A P \xrightarrow{\alpha} Q \mid\mid_A P'}$ $\alpha \notin A$
nem kell szinkronizálni
(7) átnevezés $\dfrac{P \xrightarrow{a} P'}{P[b/a] \xrightarrow{b} P'[b/a]}$ $\dfrac{P \xrightarrow{\alpha} P'}{P[b/a] \xrightarrow{\alpha} P'[b/a]}$ $\alpha \neq a$
(8) $\dfrac{P \xrightarrow{a} P'}{P \backslash a \xrightarrow{\tau} P' \backslash a}$ $\dfrac{P \xrightarrow{\alpha} P'}{P \backslash a \xrightarrow{\alpha} P' \backslash a}$ $\alpha \neq a$
(9) $\dfrac{P[rec\ x.P/x] \xrightarrow{\alpha} Q}{rec\ x.P \xrightarrow{\alpha} Q}$
Mgj.: A három szemantika ugyanazt jelenti.
Vajon tényleg ugyanaz-e? Be kell bizonyítani!
Felépítünk egy algebrai nyelvet. Ezzel az ilyen kérdés bizonyítható.
Def.: (egyetlen típusú szignatúra - one-sorted signature)
$\sum = <F, \alpha>$ F - fv szimbólumok halmaza.
$\alpha: F \to IN_0$ aritás fv., /ahol/ $f \in F$ /esetén/, $\alpha(f)$ az f változóinak száma
$\forall k \in IN$: $\sum_k = \{f \in F \mid \alpha(f) = k\}$
Példa.: Act (akciók nyelve), p::= nil | ap | p+q $\sum 1$
$\sum 1_0 = \{nil\}$ $\sum 1_1 = Act$ $\sum 1_2 = \{+\}$
Def.: $\sum$ - kifejezés (szintaxis)
$T_\Sigma$ a legkisebb olyan kT stringhalmaz, hogy:
(1) $\sum_0 \subseteq T$
(2) ha $t_i \in T$, $1 \leq i \leq k$, akkor $f(t_1, ..., t_k) \in T$ $\forall f \in \sum_k$ $1 \leq k$-ra

Mgj.: $\sum_0=\emptyset \Rightarrow T_\Sigma = \emptyset$

Mgj.: f$\in \sum_2$, $\_f\_$:S,S$\to$S

f($t_1$,$t_2$) ($t_1 f t_2$)

Példa.: $\sum_1$ szign. S típuson műveletek: nil: $\to$S

a_: S$\to$S a$\in$Act

_+_: S,S$\to$S

Mgj.: M1 ::= nil | aM1 | M1+M1 nyelvtan

$T_{\Sigma_1} = \mathcal{L}$(M1)

Def.: $\sum$-algebra = <A,$\sum_A$> (szemantika)

- A (hordozó halmaz, szemantikus tartomány)
- $\sum_A = \{f_A | f\in F\}$ műveletek halmaza, $f_A$:$A^n \to$A, n = $\alpha$(f)

$f_A$:$A^0 \to$A egy konstans

Def.: A $\sum$ algebrák osztálya: ALG($\sum$)

Példa.: <PS,{$nil_{PS}$,$+_{PS}$}$\cup$\{$a_{PS}$|a$\in$Act\}> Ez a $\sum_1$ algebra.

PS = \{T$\subseteq$Act* | T$\neq \emptyset$ és prefix zárt\}

$nil_{PS} = \{\mathcal{E}\}$

$a_{PS}(T) = \{\mathcal{E}\}\cup\{at|\ t\in T\}$, ahol T a P folyamat történethalmaza, nem üres és prefix-zárt

$T_1 +_{PS} T_2 = T_1 \cup T_2$

Jelölés.: néha A jelöli (A,$\sum_A$)-t.

$f(\vec{a}) = f(a_1, ..., a_k)$

f:A$\to$B $\vec{a}\in A^k$, $\vec{b}\in B^k$ $f(\vec{a})$

$\vec{a} R \vec{b}$

Def.: Kifejezés-algebra $\in$ ALG($\sum$)

$0\leq k$, f$\in \sum_k$ ::= \{ $f_{T_\Sigma}$: $T_\Sigma^k \to T_\Sigma$, $f_{T_\Sigma}(\vec{t})$ = "f($t_1$, ..., $t_k$)" \}, ahol

$T_\Sigma^k$ - k darab string, $T_\Sigma$ - 1 darab string, $\vec{t} = (t_1, ..., t_k)$, $t_i \in T_\Sigma$

<$T_\Sigma$,\{$f_{T_\Sigma}$|f$\in \sum$ \}>

Mgj.: $T_\Sigma$ "anil"

"anil+b" $\sum$ kifejezések halmaza

($T_\Sigma$,$\sum_{T_\Sigma}$) , ahol $\sum_{T_\Sigma}$ fv-ek halmaza; ÉT-a a $T_\Sigma$; stringekből csinál stringet

/Mgj.:/ - Így igaz, hogy $\forall\sum$-hoz adható $\sum$-algebra. Pl. a hozzá tartozó kifejezés-alg.

- Számunkra értelmes szemantikát adó alg-kat keresünk. (A kif. alg. nem az!)

Példa.: $T_{\Sigma_1}$ is egy $\sum_1$ algebra.

Ez bármely két szintaktikusan különböző folyamat között különbséget tesz.

Def.: $\sum$-homomorfizmus ($\sum$-algebrák közötti leképezés)

$\sum$ szignatúra; <A,$\sum_A$>, <B,$\sum_B$> $\sum$-algebrák;

$\varphi$:A$\to$B $\sum$-homomorfizmus, ha $\varphi(f_A(\vec{a})) = f_B(\varphi(\vec{a}))$ $\forall f_i \in \sum_i$ i=A,B

/azaz művelettartó/ kommutatív diagram:

$$\begin{array}{lccc} A: & \vec{a} & \to & f_A(\vec{a}) \\ & \varphi\downarrow & & \varphi\downarrow \\ B: & \vec{b} & \to & f_B(\vec{b}) \end{array}$$

Mgj.: bijektív homomorfizmus $\to$ izomorf. A$\simeq$B

kompozícionális

Példa.: $\alpha$:$T_{\Sigma_1} \to$PS $\alpha(p) = \{s\in Act^* \mid p\xrightarrow{s}\}$ $\sum_1$-homomorfizmus $T_{\Sigma_1}$-ről PS-re.

Biz.: Kell: $\alpha(ap) = a_{PS}(\alpha(p)) = \{at \mid t\in \alpha(p)\}$

$\alpha(nil) = \{\mathcal{E}\}$

$\alpha(p+q) = \alpha(p)\cup\alpha(q)$

Ig.: $\alpha(ap) \underset{\text{def } \alpha}{=} \{s\in Act^* \mid ap\xrightarrow{s}\} =$ /$\xrightarrow{}$def/ -p-ből induló t sorozatok

$= \{\mathcal{E}\}\cup\{at \mid t\in Act^* \wedge p\xrightarrow{t}\} \underset{\alpha \text{ def.}}{=} \{\mathcal{E}\}\cup\{at \mid t\in \alpha(p)\} \underset{a_{PS} \text{ def.}}{=} a_{PS}(\alpha(p))$ $\diamond$

Mgj.: - $\alpha$(anil+nil) = $\alpha$(anil) $\rightarrow$ $\alpha$ nem bijektív
- PS absztraktabb $T_{\Sigma_1}$ -nél (több folyamatot azonosít)

Lemma.: Két $\sum$-homomorfizmus kompozíciója is $\sum$-homomorfizmus.

Lemma.: $\sum$-algebra felett adott identitás fv. $\sum$-homomorfizmus.

Mgj.: - Olyan $\sum$-algebrát keresünk (leíró szemantika), amely a mûveleti szemantika szerint azonosított folyamatokat tekinti azonosnak.
$T_\Sigma$ belül vannak (a mûv. szem. alapján) "ekvivalens" kifejezések
$\equiv_{T_\Sigma}$ekvivalenciareláció.
- $T_\Sigma/\equiv$ hányadosalgebra

Def.: $\sum$-kongruencia
$\sum$ - szignatúra, $<A,\sum_A>$ $\sum$-algebra,
$R \subseteq A\times A$ $\sum$-kongruencia, ha - R ekvivalencia reláció (refl., szimm., tranz.)
- $\vec{a} R \vec{a}' \Rightarrow f_A(\vec{a}) R f_A(\vec{a}')$ $\forall f \in \sum$
/Elég most nekünk $\vec{a}$ helyett $a$, $\vec{a}'$ helyett $a'$/

Példa.: p equ q $\Leftrightarrow$ $\alpha(p) = \alpha(q)$; $T_{\Sigma_1}$ -en equ kongruencia
(Biz. késõbb) $\rightsquigarrow$ algebra

Tétel.: Minden $\sum$-homomorfizmus magja $\sum$-kongruencia.

Def.: $\sum$-szignatúra; $<A,\sum_A>$, $<B,\sum_B>$ $\sum$-algebrák; $\varphi$:A$\rightarrow$B $\sum$-homomorfizmus
$\varphi$ magja A-n ($=_\varphi$), ha $a =_\varphi a' \Leftrightarrow \varphi(a)=\varphi(a')$
/amiket egybevisz. A mag a reláció/

Def.: Hányadosalgebra
$<A,\sum_A>$ $\sum$-algebra; R - kongruencia
$A/R = <Q,\sum_Q>$, ahol $Q = A/R = \{[a]_R \mid a \in A\}$ ekvivalenciaosztály
$\sum_Q = \{f_Q | f \in \sum\}$, $f_Q: A^k \rightarrow A$
$f_Q([a_1]_R, ..., [a_k]_R) = [f_A(a_1, ..., a_k)]_R$

Mgj.: R kongruencia, így $f_Q$ definíciója jó.

Def.: $nat_R$: A$\rightarrow$A/R $nat_R(a) = [a]_R$
$nat_R$ természetes $\sum$-homomorfizmus az R kongruenciára nézve.

Tétel: Homomorfizmus tétel
$\sum$ /szignatúra/, $<A,\sum_A>$, $<B,\sum_B>$ /$\sum$-algebra/; $\varphi$:A$\rightarrow$B /$\sum$-homomorfizmus/
R $\sum$-kongruencia A-n, $R \subseteq =_\varphi$ /$\Rightarrow$ $\varphi$ absztraktabb mint R / $(a,b)\in R \Rightarrow (a,b)\in\varphi$
/$\Rightarrow$/ $\exists!$ $\varphi^*$ $\sum$-homomorfizmus úgy, hogy $\varphi^* \circ nat_R = \varphi$

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "nat_R"'] & & B \\ & A/R \arrow[ur, "\exists!\varphi^*"'] & \end{tikzcd}$$

Tétel: (Izomorfia tétel) - $\varphi^*$ szürjektív $\Leftrightarrow$ ha $\varphi$ szürjektív
- $\varphi^*$ injektív $\Leftrightarrow$ ha $=_\varphi \subseteq R$

Def.: Kezdeti algebra
K: $\sum$-algebrák osztálya.
I kezdeti algebra K-ban, ha $\forall A \in K$: pontosan egy homomorfizmus van I-rõl A-ra.

Lemma: • Ha $I_1$ és $I_2$ is kezdeti algebrák K-ban, akkor $I_1 \simeq I_2$
• Ha $I_1$ kezdeti K-ban és $I_2 \simeq I_1$, akkor $I_2$ is kezdeti K-ban.

$$\begin{tikzcd} I_1 \arrow[rr, "\varphi"] \arrow[dr] & & A \\ & I_2 \arrow[ur] & \end{tikzcd}$$

Tétel: $\sum$-szignatúrára $T_\Sigma$ kezdeti algebra az ALG($\sum$)-ban.

Biz.: késõbb. (soha)

Jelölés: $T_\Sigma \xrightarrow{\imath_A} A$ $\imath_A$ kezdeti-homomorfizmus, ı - pont nélküli "i"

Példa: $\sum_1$ $\imath_{PS}$: $T_{\Sigma_1} \rightarrow PS$
$\imath_{PS}(t) = \alpha(t)$

Mgj.: $\sum$ /szignatúra/, R,S kongruenciák $T_\Sigma/R \cong T_\Sigma/S$ $\Leftrightarrow$ R=S

Def.: $I \xrightarrow{\imath_A} A \qquad \mathcal{R}_{\imath_A} \subseteq A$

$A \setminus \mathcal{R}_{\imath_A}$ lom /nem képe semminek

Def.: Elérhetõ $\sum$-algebra

$\sum$-szignatúra, $<A,\sum_A>$ elérhetõ, ha a $\imath_A$: $T_\Sigma \to A$ homomorfizmus szürjektív.

(nincs lom a szemantikai tartományban)

Példa: $\sum_1$- algebrák között PS elérhetõ.

Biz.: Elegendõ: $\exists\Pi$:$PS \xrightarrow{\Pi} T_{\Sigma_1}$: $\imath_{PS} \circ \Pi = id_{PS}$

$T = \{t_i \mid 0 \leq i \leq N\}$ történethalmaz$\in$PS

$\Pi(T) = (\ t_i\!: 0 \leq i \leq N\!: \mathcal{P}(t_i)\ )$, ahol $\quad \mathcal{P}$: $Act^* \to T_{\Sigma_1}$, $\quad \mathcal{P}(as) = a(\mathcal{P}(s))$

Mgj.: $\Pi$ függ T elemeinek felsorolási sorrendjétõl (különbözõ kifejezés lesz az eredmény),

nem homomorfizmus. $\qquad T_{\Sigma_1} \underset{\imath_{PS}}{\overset{\Pi}{\leftrightarrows}} PS$

Def.: Az algebra megfelel R kongruenciának

$\sum$ szignatúra; $<A,\sum_A>$ $\sum$-algebra; R kongruencia $T_\Sigma$-n.

A megfelel R-nek ($A \models R$), ha $R \subseteq =_{\imath_A}$. (A - az R-nek megfelelõ leíró modell.)

Az ALG($\sum$,R) az R-nek megfelelõ $\sum$ algebrák osztálya.

Példa: Ha p $equ_{PS}$ q $\Leftrightarrow$ $\alpha(p) = \alpha(q)$ ($\Leftrightarrow$ (equ $=_{PS}$ $\alpha$ és $\imath_{PS}(p) = \alpha(p)$) )

$\Rightarrow$ PS$\models$equ, azaz PS leíró modell equ-ra nézve.

Mgj.: ALG($\sum$,R) elemei között vannak túl absztraktak.

Def.: $<A,\sum_A>$ "teljesen" absztrakt (fully absztract) az R-re nézve, ha $R = =_{\imath_A}$.

Példa: elõzõ.

Tétel: $\sum$ szignatúra, R kongruencia $T_\Sigma$-n.

A $T_\Sigma/R$ hányadosalgebra kezdeti algebra ALG($\sum$,R)-ben.

Biz.: Legyen $<A,\sum_A>\in$ALG($\sum$,R) tetszõleges

$(A \models R) \Rightarrow (R \subseteq =_{\imath_A})$

$$\begin{tikzcd} T_\Sigma \arrow[rr, "\imath_A"] \arrow[dr, "nat_R"'] & & A \\ & T_\Sigma/R \arrow[ur, "\exists!\imath_A^*"'] & \end{tikzcd}$$

a hom. tétel szerint

Tehát $T_\Sigma/R$ kezdeti algebra. $\diamond$

Tétel: $\sum$ szignatúra, $<A,\sum_A>$, R kongruencia $T_\Sigma$-n.

(i) $<A,\sum_A>$ elérhetõ és teljesen absztrakt R szerint.

$\Updownarrow$

(ii) $<A,\sum_A>$ kezdeti algebra ALG($\sum$,R)-ben.

]]

1998. dec. 7. Párhuzamos folyamatok II. Kiselõadó, Informatika 3. (12)

T.: $\sum$ szignatúra, $<A,\sum_A>$ $\sum$-algebra, R kongruencia $T_\Sigma$-n.

(1) $<A,\sum_A>$ elérhetõ és teljesen absztrakt R szerint.

$\Updownarrow$

(2) $<A,\sum_A>$ kezdeti algebra ALG($\sum$,R)-ben.

Biz.: $T_\Sigma/R$ kezdeti ALG($\sum$,R)-ben, így:

(2)-ben $<A,\sum_A> \simeq T_\Sigma/R$

$$\begin{tikzcd} T_\Sigma \arrow[rr, "\imath_A"] \arrow[dr, "nat_R"'] & & A \\ & T_\Sigma/R \arrow[ur, "="'] & \end{tikzcd}$$

izomorfizmus tétel szerint $\diamond$

Pl.: PS elérhetõ és teljesen absztrakt $equ_A$-ra, így PS kezdeti ALG($\sum_1$,$equ_A$)-ban.

$PS \simeq T_{\Sigma_1}/equ_A$.

Leíró szemantika - összefoglalás

- Ha adott a mûveleti szem. és keresem a definíciós szemantikát /mûveletit equ def./,

$\Rightarrow$ kell, hogy a definíciós szem. mûvelet szerint elérhetõ, teljesen absztrakt alg. legyen.

- Létezik ilyen, pl.: a kifejezés-alg. equ szerinti hányados alg /-ája/.

- Létezik több is, amely izomorf vele /a hányados alg-val/ ( $\underset{\text{kezdeti hom. magja}}{=_{\imath_A}}$ = $\underline{\text{equ}}$ )

Lényeges, hogy az $\imath_A$ homomorfizmus kiszámításának mi a módja.

(A hányados alg. ugyanolyan nehezen számolható, mint az $\underline{\text{equ}}$ maga.)

<u>Mgj.:</u> $=_{\imath_A}$ nem mindegy, hogy milyen, mert

pl.: $S \xrightarrow{=_{\imath_A}}$ /lf(S,...) $\Rightarrow$ S-hez valójában $p(S)^{-1}$-et rendelem/

$\lceil lf(S,R)\rceil = \lceil p(S)^{-1}(R)\rceil$

$lf(DO,R) = (\mu X{:}lf(S_0,X))$

<u>Továbbiakban:</u> $=_{\imath_A}$ axiomatikus jellemzése /$P_1$ - feladat, $P_2$ - új feladat, és levezetési szabályokkal próbáljuk igazolni ekvivalenciájukat/

(mi ekvivalens)

<u>Mgj.:</u> Köv. szabályokkal hat. meg, hogy melyik két folyamat ekvivalens ($\rightarrow$ CSP szabályai)

egyenlõségek $\rightarrow$ kongruenciát indukálnak.

<u>D.:</u> $\sum$ kifejezés változókkal: $\sum$ szignatúra, X változók halmaza.

$T_\Sigma(X)$ az X feletti $\sum$ kifejezések azon legkisebb halmaza:

(1) $X \subseteq T$

(2) $\sum_0 \subseteq T$

(3) ha $t_i \in T$, $1 \le i \le k$, akkor $f(t_1, ..., t_k) \in T$ $\quad \forall f \in \sum_k$, $1 \le k$

<u>Mgj.:</u> $T_\Sigma(\emptyset) = T_\Sigma$ /$T_\Sigma$ - zárt alapkifejezések halmaza/

<u>D.:</u> Szabad (kif.) algebra: ($T_\Sigma(X)$ + mûveletek)

Legyen K a $\sum$-algebrák egy osztálya.

$F \in K$ szabad algebra az X felett, ha $\exists$ univerzális leképezés u: $X \rightarrow F$, hogy

$\forall \langle A, \sum_A \rangle \in K \wedge \forall p{:}X \rightarrow A$ (A értékelésre): $\exists!\ \overline{p}{:}F \rightarrow A$: $\overline{p} \circ u = p$

$$\begin{array}{ccc} X & \xrightarrow{u} & F \\ & p\searrow \ \swarrow \exists!\overline{p} & \\ & A & \end{array}$$

<u>Lemma.:</u> (1) I kezdeti K-ban $\Leftrightarrow$ I szabad K-ban $\emptyset$ felett (hom. tétel)

(2) Ha $F_1$ is és $F_2$ is szabad alg. K-ban X felett, $\Rightarrow$ $F_1 \simeq F_2$.

(3) Ha $F_1$ szabad alg. K-ban X felett, és $F_1 \simeq F_2$ $\Rightarrow$ $F_2$ is az.

<u>T.:</u> (egyértemû kiterjesztés tétele - uniq. ext. theo.)

$\sum$ szignatúra, X halmaz. $T_\Sigma(X)$ szabad alg. ALG($\sum$)-ban, X felett.

<u>Biz.:</u> <u>$\exists$u konstruktív:</u> /ilyet kell mutatni/

(0) u(x) = x

Legyen $p{:}X \rightarrow A$ tetsz.. A értékelés

Ekkor $\overline{p}{:}T_\Sigma(X) \rightarrow A$ induktívan definiálható.

$$\begin{array}{ccc} X & \xrightarrow{u} & T_\Sigma(X) \\ & p\searrow \ \swarrow \exists!\overline{p} & \\ & A & \end{array}$$

(1) $\overline{p}(x) = p(x)$

(2) $\overline{p}(f) = f_A$ /(2)-(3) -

(3) $\overline{p}(f(t_1, ..., t_k)) = f_A(\overline{p}(t_1), ..., \overline{p}(t_k))$ $\quad f \in \sum_k$, $k \ge 1$ $\quad \sum$-homomorfizmus/

(0)(1) $\rightarrow \overline{p} \circ u = p$.

<u>Egyértelmûség:</u> Legyen $\varphi{:}T_\Sigma(X) \rightarrow A$ $\sum$-homomorfizmus $\varphi \circ u = p$.

$\sum$ kif. feletti struktúra indukcióval: $\varphi = \overline{p}$. $\diamond$

<u>Mgj.:</u> kif. értéke egyértelmûen meghatározott a benne elõforduló vált-k értéke szerint.

<u>Jelölés:</u> $p{:}X \rightarrow A$, $t \in T_\Sigma(X)$

$A[[t]]p ::= \overline{p}(t)$ /p értékét keresem A fölött/ /$\overline{p}$ - kifejezéshez rendel értéket/

/$\overline{p}$("a+b") $\quad$ p:a$\rightarrow$5, b$\rightarrow$3/

$$\begin{array}{ccc} X & \xrightarrow{u} & T_\Sigma(X) \\ & p\searrow \ \swarrow \exists!\overline{p} & \\ & A & \end{array}$$

<u>D.:</u> helyettesítés (pl. változók kiküszöbölésére)

$\sum$ szignatúra, X halmaz. $\sigma{:}X \rightarrow T_\Sigma(X)$ helyettesítés. /$\sigma$:a$\rightarrow$"1", b$\rightarrow$"2+3" $\Rightarrow$ $\sigma$("a+b")= "1+2+3" /

<u>Jelölés:</u> szimultán helyettesítés $\overline{\sigma}(t) = t^{x_1, x_2 \leftarrow \sigma(x_1)\sigma(x_2)}$

$t\sigma ::= \overline{\sigma}(t)$, ahol $[t_0,...,t_n/x_0,...,x_n]$

Lemma: (helyettesítés és értékelés)

(1) $A[[t_1]](\overline{p}\circ\sigma) = A[[t_1\sigma]]p$ kiszámításának két módja:

(a) x-et helyettesít, kifejezést értékel

(b)/ $\underset{\overline{p}\circ\sigma}{\overset{\sigma}{\text{x értékek,}}}$ ért./

(2) $\sum$ szignatúra, $<A,\sum_A>$ alg., X halmaz, p:X$\rightarrow$A A-értékelés, $\sigma$:X$\rightarrow T_\Sigma$(X) helyettesítés. Ekkor $\underset{(a)}{\overline{(\overline{p}\circ\sigma)}} = \underset{(b)}{\overline{p}\circ\overline{\sigma}} = (*)$

(1) $\equiv$ (2)

Biz.: $T_\Sigma$(X) szabad alg. X felett, így: (*)

(a)

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & T_\Sigma \in \overline{\sigma}(t) \\ u\searrow & & \swarrow \exists!\overline{\sigma} \\ & T_\Sigma(X) & \end{array}$$

(b) /x helyettesített $\swarrow$ étéke/

$$\begin{array}{ccc} X & \xrightarrow{\sigma}\ \xrightarrow{\overline{p}} & A \\ u\searrow & & \nearrow \exists!\overline{(\overline{p}\circ\sigma)} \\ & T_\Sigma(X) & \end{array}$$

$$\begin{array}{ccccc} & & X & & \\ & u\swarrow & & \searrow p & \\ X & \xrightarrow{\sigma} & T_\Sigma(X) & \xrightarrow{\overline{p}} & A \\ & u\searrow & \downarrow\overline{\sigma} & \nearrow(*) & \\ & & T_\Sigma(X) & & \end{array}$$

$\diamond$

Pl.: $X=\left\{\begin{smallmatrix}a\\b\end{smallmatrix}\right\} \xrightarrow{\sigma} \begin{smallmatrix}\text{"1"}\\\text{"2+3"}\end{smallmatrix}$

$$\overline{p}\searrow \quad \swarrow\overline{p}$$
$$\begin{smallmatrix}1\\5\end{smallmatrix} = 6$$

D.: (egyenlõségi axióma)

$\sum$ szignatúdra, $t_1,t_2 \in T_\Sigma$(X). $t_1 = t_2$ egy $\sum$ egyenlõségi axióma.

D.: (egyenlõségi érvelés, DED(E))

E - $\sum$ egyenlõségek halmaza (reláció $T_\Sigma$(X) felett)

DED(E):

(1) $\dfrac{}{t = t}$ (reflexív)

(2) $\dfrac{t_1 = t_2}{t_2 = t_1}$ (szimmetrikus)

(3) $\dfrac{t_1 = t_2 \ \wedge\ t_2 = t_3}{t_1 = t_3}$ (tranzitív)

(4) $\dfrac{t_1 = u_1 \ \ldots\ t_k = u_k}{f(t_1,\ldots,t_k) = f(u_1,\ldots,u_k)}$ (helyettesíthetõség)

(5) $\dfrac{t_1 = t_2}{t_1\sigma = t_2\sigma}$ (példányosíthatóság) /$\sigma$(x) = "a+b", "a+x" = "x+a" $\Rightarrow$ "a+a+b" = "a+b+a"/

(6) $\dfrac{}{e}$ (e$\in$E) (axióma)

Jelölés: Ha $t_1 = t_2$ levezethetõ (1)...(6) véges sokszori alkalmazásával, akkor DED(E) $\vdash t_1 = t_2$.

Mgj.: - Véges sok szabály van véges sok feltétellel.
- E $\sum$ egyenlõségek halmaza DED(E)-n keresztül (1-4 miatt) kongruencia retlációt definiál.

D.: $[=_E]$ $\sum$ szignatúra, E $\sum$-egyenlõségek halmaza. $=_E$ reláció $T_\Sigma$(X) felett, azaz $=_E \subseteq T_\Sigma(X)\times T_\Sigma(X)$ és $t_1 =_E t_2 \ \Leftrightarrow\ $ DED(E) $\vdash t_1 = t_2$.

Ha $t_1 =_E t_2 \ \Rightarrow$ bizonyítható DED(E)-ben $t_1 = t_2$.

Jelölés: $\doteq_E$ az $=_E$ megszorítása $T_\Sigma$-ra. /Nincs benne változó. $=_{\imath_A}$-t $\doteq_E$-vel kell összehasonlítani/

Mgj.: Legyen equ mûveleti szemantikával def. $T_\Sigma$ felett. Keressük az E egyenlõséghalmazt, amelyre $\doteq_E$ = equ. (Esetleg ismert A algebra (modell), amelyre $=_{\imath_A}$ = equ).

Pl.: PS modellje volt (nil | ap | p+q)-nak. Így segít $E_1$ megtalálásában:

/$E_1$:/ (1) x+(y+z) = (x+y)+z (unió asszoc.)
(2) x+y = y+x (szimm.)
(3) x+x = x (idempontens)
(4) x+nil = x (prefix-zárt)
(5) a(x+y) = ax+ay $\forall$a$\in$Act (prefix és unió disztr.) /lineáris idõ axiómája/

kell: $\doteq_{E_1} =_{\imath_{PS}}$.

D.: $[=_A]$ /reláció/ $T_\Sigma(X)$ felett és $\quad t_1 =_A t_2 \;\Leftrightarrow\; A[[t_1]]p = A[[t_2]]p \quad \forall p \in X \to A$.

Ha $t_1 =_A t_2 \;\Rightarrow\; t_1 = t_2$ érvényes A felett. $\qquad A \models t_1 = t_2$.

$\doteq_A$ az $=_A$ megszorítása $T_\Sigma$-ra. $\;(\doteq_A \,=\, =_{\imath_A})$

Mgj.: $\doteq_E \,=\, =_{\imath_A}$ /mûv. - leíró/

$=_E \,=\, =_A$ -ból következne, de ezt nehéz biz., ezért helyett:

$=_E \,\subseteq\, =_A$ /amit levezetünk az helyes/ és

$\doteq_E \,\supseteq\, =_{\imath_A}$ /zárt kifejezésekre teljes/

D.: $\sum$ szignatúra, $<A,\sum_A>$ $\sum$-algebra, E $\sum$-egyenletek halmaza.

A megfelel E-nek ($A\models E$), ha $E \subseteq =_A$. /Minden elemére A-beli./

Jel.: ALG($\sum$,E) azon algebrák osztálya, amelyek megfelelnek E-nek (A az E modellje).

Mgj.: $A\models E \;\Leftrightarrow\; A\models e \;\; \forall e\in E$-re

Pl.: $PS\models E_1$

(1) $PS\models LT$ $\qquad$ /LT - lineáris idõ axiómája/

$a\in Act$, $x,y\in X$, $p\in X\to PS$

$PS[[a(x+y)]]p = \{\mathcal{E}\}\cup\{at \mid t\in PS[[x+y]]p\} = \{\mathcal{E}\}\cup\{at \mid t\in PS[[x]]p\cup PS[[y]]p\}$

$= \{\mathcal{E}\}\cup\{at \mid t\in PS[[x]]p\}\cup\{at \mid t\in PS[[y]]p\} = PS[[ax]]p\cup PS[[ay]]p = PS[[ax+ay]]p$.

T.: $\sum$ szignatúra, E egyelõséghalmaz, $<A,\sum_A>$ algebra, és $A\models E$. Ekkor $=_E \,\subseteq\, =_A$.

Biz.: Struktúrális indukció.

$E \underset{\text{ezt tudjuk}}{\subseteq} =_E \underset{\text{ezt kell biz.}}{\subseteq} =_A$ $\qquad$ /elõbb $E \subseteq =_A$-t bizonyítjuk/

$t_1 = t_2$ levezetés hossza szerinti indukcióval, azaz $\forall R\in DED(E)$ következtetési szabályra be kell látni, hogy $P^{=\leftarrow =_A} \;\Rightarrow\; C^{=\leftarrow =_A}$, ahol $R{:}P\Rightarrow C$.

1..4, $\surd$ ($=_A$ kongruencia)

6, $\surd$ ($E \subseteq =_A$ (felt. és def. $A\models E$))

5, $t_1 =_A t_2$, $\sigma{:}X\to T_\Sigma(X)$ helyettesítés tetsz. $p{:}X\to A$ értékelésre:

$A[[t_1\sigma]]p \underset{\substack{\text{helyettesítési}\\ \text{lemma}}}{=} A[[t_1]](\overline{p}\circ\sigma) \underset{t_1 =_A t_2}{=} A[[t_2]](\overline{p}\circ\sigma) \underset{\substack{\text{helyettesítési}\\ \text{lemma}}}{=} A[[t_2\sigma]]p \quad \diamond$

Mgj.: $PS\models E_1$ miatt $=_{E_1} \subseteq =_{PS}$.

T.: (normál forma) $\quad \sum$ szignatúra, $<A,\sum_A>$ $\sum$-algebra, $A\models E$.

Ha $\exists\alpha{:}A\to T_\Sigma$: $nat_{\doteq_E} \circ \alpha \circ \imath_A = nat_{\doteq_E} \;\Rightarrow\; =_{\imath_A} = \doteq_E$.

Biz.:

$$\begin{array}{ccl} T_\Sigma \underset{\imath_A}{\overset{\alpha}{\leftrightarrows}} A & & /T_\Sigma \text{ - reprezentáns}/ \\ nat_{\doteq_E} \searrow \; \swarrow \imath_A^* & & /\imath_A^* \text{ - izomorfia (ezt biz.)}/ \\ T_\Sigma/\doteq_E & & /T_\Sigma/\doteq_E \text{ - ekv. oszt.}/ \quad \diamond \end{array}$$

Mgj.: $\alpha\circ\imath_A$ $\;T_\Sigma \underset{\imath_A}{\overset{\alpha}{\leftrightarrows}} A\;$ normalizáló fv., elemhez a repr-ót rendeli (normál formát).

Pl.: (korábban volt) $\qquad T = \{t_i \mid 0\le i<N\}$

$$\begin{array}{ccl} T_{\Sigma_1} \underset{\imath_{PS}}{\overset{\Pi}{\leftrightarrows}} PS & \Pi(T) = (\; t_i{:}\; 0\le i\le N{:}\; \mathcal{P}(t_i) \;) & \mathcal{P}{:}Act^*\to T_{\Sigma_1} \\ \searrow \; \swarrow & & \mathcal{P}(as) = a\mathcal{P}(s) \\ T_\Sigma/\doteq_E & & \imath_{PS}\circ\Pi = id_{PS} \end{array}$$

kell: $nat_{\doteq_{E_1}} \circ \Pi \circ \imath_{PS} = nat_{\doteq_{E_1}}$

$p\in T_{\Sigma_1}$
$\imath_{PS}(p) = \{t_i \mid 0\le i<N_p\}$
$\imath_{PS}(ap) = \{t_j \mid 0\le j<N_{ap}\}$
$\imath_{PS}$ hom. $\Rightarrow \imath_{PS}(ap) = a(\imath_{PS}(p))$
(*) $\{\varepsilon\}\cup\{at_i \mid 0\le i<N\} = \{t_j \mid 0\le t_j<N_{ap}\}$

biz.: struktúrális ind.

(a) $t = ap$

$(\Pi\circ\imath_{PS})(ap) = \Pi(\{t_j \mid 0\le j<N_{ap}\}) = (t_j{:}\; 0\le j<N_{ap}{:}\mathcal{P}(t_j))$

$\underset{(*)}{\doteq_E} nil+(t_i{:}\; 0\le i<N_p{:}a\mathcal{P}(t_i)) \underset{\text{axiómák}}{\doteq_E} a(t_i{:}\; 0\le i<N_p{:}\mathcal{P}(t_i))$

$\underset{\text{axiómák és 4., LT}}{\doteq_E} a((\Pi\circ\imath_{PS})(p)) \underset{\Pi \text{ és } \imath_{PS} \text{ def.}}{\doteq_E} ap$