1. eloadas

Merfoldko: SIMULA 67 programnyelv

- elotte: gepi kod, programozas kicsiben, szerializacio
- utana: nagymeretu programok, komplex rendszerek, osztott rendszerek

Objektumelvu programozasObjektumelvu programozast tamogato prog. nyelv tipusrendszere:

- egyszeru: integer | real | boolean | $\cdots$
- osszetett: vector | array | record | $\cdots$

Elvei:

- strukturaltsag leirasank fo egysege: osztaly
- objektumokhoz valo hozzaferes
- objektum: az osztaly egy peldanya
- adatbeburkolas
- adatabsztrakcio, informacio elrejtese
- objektumok azonositokkal valo megnevezese, elerese
- oroklodes es polimorfizmus

Absztrakcio:

- reszletek, eroforrasok elrejtese
- adatabsztrakcio
- funkcionalis absztrakcio
- elnevezesi absztrakcio
- viselkedesi absztrakcio
- modellabsztrakcio

Adatszerkezet: Adathalmaz, amely bizonyos strukturaban szervezetten letezik.
Adattipus: adattartomanyok halmaza es a hozzajuk tartozo muveletek veges halmaza
Adattipus informalis definicioja:

- adattartomanyok veges osszessege
- van egy kituntetett bazistartomany
- tartomanyokon ertelmezett muveletek, melyekkel a bazistartomany minden peldanya eloallithato
- az adattartomanyok megszamlalhatok

$\Rightarrow$ kulonbozo matematikai modelleket hozhatunk letre. Pl.: matematikai modell
Absztrakt adattipus:

- adattipusok olyan osztalya, amely zart az adattartomanyok, muveletek, a tartomayok peldanyainka es a muveletek elnevezese alapjan
- fuggetlen az adatok abrazolasatol es az adott abrazolasok mellett a muveletek megvalositasatol

Az algebra spcifikacioja: ⟨algebra neve⟩=
sorts: ⟨szortok azonositoi⟩
oprs: ⟨muveletek szimbolumai⟩
eqns: ⟨valtozok deklaracioja⟩
⟨muveletek jelenteset meghatarozo szimbolumok listaja⟩ end ⟨algebra neve⟩

Muveleti szimbolumok formai:

- prefix forma: Pl.: add: nat nat → nat
- infix forma: Pl.: +: N N → N [infix]
- kifejezes forma: Pl.: _ + _ : N N → N

Axiomak alatalanos formaja:

- $\alpha(a) \Rightarrow f_1(f_2(a)) = h(a)$
- egyenletek formajaban

Egyszeru oroklodes: algebra1=
sorts: szortok1
oprs: opszimbolumok1
eqns: deklaracio1; axiomak1
end algebra1;

algebra2 = algebra1 +
sorts: szortok
oprs: opszimbolumok
eqns: deklaracio; axiomak
end algebra2;
Vagyis:
algebra2=
sorts: szortok1, szortok
oprs: opszimbolumok1, opszimbolumok
eqns: deklaracio1; deklaracio; axiomak1; axiomak
end algebra2;

Parameterek szerepei az algebraban:

- objektum kiertekelese
- objektum felepitese
- korlatozas

2. eloadas:

Szignatura: $\Sigma = (S, OP)$

S: szortok halmaza;

OP: konstans es operacios szimbolumok halmaza;

$OP = K_s \cup OP_{w,s}; s \in S;$

K_S: konstans szimbolumok halmaza;

$OP_{w,s}$ operacios szimbolumok halmaza; w argument szort, $w \in S^+$; s eredmeny szort, $s \in S$;

$K_s; OP_{w,s}$ paronkent diszjunktak;

$K = \bigcup\limits_{s \in S} K_s; OP = K \cup (\bigcup\limits_{\substack{w \in S^+ \\ s \in S}} OP_{w,s}) \quad N \in K_s; \quad N :\rightarrow s;$

$N \in OP_{w,s}, w = s_1 \cdots s_n$; akkor $N = s_1 \cdots s_n \rightarrow s$;

Adott $\Sigma = (S, OP)$ szignaturahoz tartozo **Σ-algebra:**
$A = (S_A, OP_A)$, ahol $S_A = \{A_S | s \in S\}$ es $N = (N_A)(N \in OP)$;

1. A_S, A bazishalmaza $\forall s \in S$;
2. $N_A \in A_s$;
   $\forall N \in K_s : N \rightarrow s$ es $s \in S$ konstans szimbolumra;
   $\forall N : OP(s_1 \cdots s_n \rightarrow s)$ es $s_1 \cdots s_n \in S^+; s \in S$ muveleti szimbolumra;

Megjegyzes: Ha $\Sigma = (S_1 \cdots S_n, N_1, \cdots N_m)$; akkor $A = (A_{s_1}, \cdots, A_{s_n}, N_{1_A}, \cdots, N_{m_A})$; (megfeleltetesi sorrendben!)

Valtozo: Adott $SIG = (S, OP)$, es $X_s, s \in S$, az s szorthoz tartozo valtozok halmaza.
$X = \bigcup_{s \in S} X_s$, a SIG szignaturahoz tartozo valtozok halmaza.
Deklaracio: $x, y \in X_s$; Jelolesuk: **oprs**: $x, y \in S$;

Term szintaktikai definicioja:
Adott $\Sigma = (S, OP)$; X a szignaturahoz tartozo valtozo.
$T_{\Sigma(X)} = (T_{\Sigma(X),s}), s \in S$ definicioja:
Bazis termek: $X_s \in T_{\Sigma(X),s}$; $n :\rightarrow s \in OP$; akkor $n \in T_{\Sigma(X),s}$;
Osszetett termek: $n : s_1 \cdot s_k \rightarrow s, k \geq 1, n \in OP, t_i \in T_{\Sigma(X),s}, 1 \leq i \leq k$;
akkor $n(t_1, \cdots, t_k) \in T_{\Sigma(X),s}$;

Strukturalis indukcio: Adott $\Sigma = (S, OP)$; a szignaturahoz tartozo X valtozokkal.
Legyen p predikatum, amely a $t \in T_{op}(X)$ termekre van ertemezve, ha

1. $\forall t \in K$ es $\forall t \in X : p(t) =$"true";
2. $\forall N(t_1, \cdots, t_n) \in T_{op}(X) : p(N(t_1, \cdots, t_n) =$"true";

akkor $\forall t \in T_{op}(X) : p(t) =$"true".

A term kiertekelese: Adott $\Sigma = (S, OP)$; es a T_{op}. Legyen A egy Σ-algebra.
A kiertekeles $eval : T_{op} \rightarrow A$ definicioja:
$eval(N) = N_A$; ha $N_A \in K$;

$eval(N(t_1, \cdots, t_n)) = N_A(eval(t_1), \cdots, eval(t_n))$, ha $N(t_1, ..., t_n) \in T_{op}$.

Term (ertekadas) kiertekelese: Adott $\Sigma = (S, OP)$ a szignaturahoz tartozo X valtozokkal, es T_{op}. Legyen A egy Σ-algebra.

$ass : X \rightarrow A$, ahol $ass(x) \in A_s, x \in X_s, s \in S$;
$ass : T_{op}(x) \rightarrow A$ definicioja;
$ass(x) = ass(x), x \in X$ valtozo;
$ass(N) = N_A, N \in K$ konstans szimbolum;
$ass(N(t_1, \cdots, t_n)) = N_A(ass(t_1), \cdots, ass(t_n)); \quad N(t_1, \cdots, t_n) \in T_{op}(X)$;

Egyenletek: Adott $\Sigma = (S, OP)$ a szignaturahoz tartozo X valtozokkal.
Az $e = (X, L, R)$ harmast, $L, R \in T_{OP,s}(X), s \in S$ mellett egyenletnek nevezzuk.
Az $e = (X, L, R)$ egyenlet helyes az A Σ-algebraban, ha minden $ass : X \rightarrow A$ eseten $ass(L) = ass(R)$.

Specifikacio: $SPEC = (S, OP, E)$; $\Sigma = (S, OP)$; $E = \{e(X, L, R)\}$; $\forall x \in X, L = R$;
X valtozok halmaza, L, R, termek X-bol vett valtozokkal.

Tipus:
⟨tipus neve⟩ (⟨parameterek listaja⟩) is a type specification =
parameters = ⟨atvett aktualis tipusnev_1⟩ + ... + ⟨atvett aktualis tipusnev_k⟩ +
sorts: ⟨formalis parameterek nevei⟩;
oprs: ⟨muveletek formai⟩;
eqns: ⟨muveletek jelentesenek leirasa⟩;
export =
type sort: ⟨tipushalmaz neve⟩;
oprs: ⟨muveletek formai⟩;
eqns: ⟨muveletek jelentesenek leirasa⟩;
end ⟨tipus neve⟩;

Σ-algebrak kozti homomorfizmus:
Legyenek $A = (S_A, OP_A)$ es $B = (S_B, OP_B)$ azonos $\Sigma = (S, OP)$ szignaturaju algebrak.
A $h : A \rightarrow B$ homomorfizmus egy fuggvenycsalad, $h = (h_s)_{s \in S}$ ahol $h_s : S_A \rightarrow S_B$ ugy, hogy:

- $\forall N :\rightarrow s \in OP$ es $s \in S$ konstans szimbolumra teljesul: $h_s(N_A) = N_B$
- valamint $\forall N : s_1 \cdots s_k \rightarrow s_l \in OP$ es $\forall i = 1, \cdots, k$-ra es $a_i \in A$ eseten teljesul a homomorfikus feltetel, azaz $h_s(N_A(a_i, \cdots, a_k)) = N_B(h_{s_1}(a_1), \cdots, h_{s_k}(a_k))$.

A bijektiv homomorfizmust izomorfizmusnak nevezzuk.
Az A es B Σ-algebrakat izomorfikusnak nevezzuk, ha letezik az izomorfizmus $A \rightarrow B$ eseten es jelolese ekkor: $A \cong B$.
Homorfizmusok kompozicioja szinten homomorfizmus.
Ha h_s izomorfizmus, akkor h_s^{-1} is az.
Egy adott Σ szignaturahoz tartozo absztrakt adattipus a Σ-algebrak egy olyan osztalya, amely az izomorfizmusra zart: $C \subset Alg(\Sigma)$ es $A \in C$ es $A \cong B \Rightarrow B \in C$.

3. eloadas:

Specifikacio morfizmus spec. esetei:
1) Atnevezes
2) Benne foglaltatas, tartalmazas, bovites
3) Abrazolas, reprezentacio
4) Parameter atadas
Specialisan, formalis parameterek helyettesitese aktualis parameterekkel (parameter passing)

1. Standard parameteratadas: $spec(spec_1) \to spec(spec_2)$, ahol $spec_1$ formalis, $spec_2$ aktualis parameter ertekadassal torteno specifikacio

2. Ismetelt parameteratadas: $spec(spec_1(spec_A)) \to spec(spec_2(spec_B))$;

Szignaturamorfizmus: Adott: $\Sigma = (S, OP)$, $\Sigma' = (S', OP')$, mellett a $h_\Sigma : \Sigma \to \Sigma'$ lekepezest szignaturamorfizmusnak nevezzuk, ha $h_\Sigma = (h_S : S \to S', h_{OP} : OP \to OP')$ ugy, hogy $(\forall N : s_1 \cdot s_n \to s \in OP)(h_{OP}(N) : h_S(s_1) \cdots h_S(s_n) \to h_S(s) \in OP')$.
Kituntetett sortu szignaturamorfizmus: $h_s(pt(\Sigma)) = pt(\Sigma')$.

A h : $\boldsymbol{\Sigma \to \Sigma'}$ szignaturamorfizmus kiterjesztese valtozokra:
Legyenek X, X' rendre a Σ, Σ' valtozoi.
Tovabbiakban altalaban: $h = h_\Sigma$; $h(s) = h_s$; $h(N) = h_{OP}(N)$;
$h_X : (\bigcup_{s \in S} X_S) \to (\bigcup_{s' \in S'} X'_{S'})$ ha $x \in X_S, s \in S$, akkor $h_X(x) \in X'_{h(s)=s'}$;

A $h : \Sigma \to \Sigma'$ szignaturamorfizmus kiterjesztese termekre:
Adottak: $T_{\Sigma(X)}, T_{\Sigma'(X')}$ rendre a Σ, Σ' termeknek halmazai.
$\forall t \in T_{\Sigma(X)}$-hez tartozo $h_T(t) \in T_{\Sigma'(X')}$ definicoja:

- $(\forall x \in X)(h_T(x) = h_X(x))$
- $(\forall (N :\to s) \in OP)(h_T(N :\to s) = h_X(h(N) :\to s)$
- $(\forall N : s_1 \cdots s_n \to s) \in OP)(h_T(N(t_1, \cdots, t_n)) = h(N)(h_T(t_1), \cdots, h_T(t_n))$

A h : $\boldsymbol{\Sigma \to \Sigma'}$ szignaturamorfizmus kiterjesztese egyenletek formajaban adott axiomakra:
Legyen $e = (X, L, R) \in E$, akkor e helyettesitendo $h^*(e) = (X^*, h^*(L), h^*(R))$ egyenlettel $\in E'$, ahol $\forall x \in X_{s \in S}$ valtozo helyettesitendo $x^* \in X^*_{h(s)=s' \in S}$ valtozoval, L es R kepzesnel pedig $\forall N : s_1 \cdots s_n \to s \in OP$, eseten $N(t_1, \cdot, t_n) \in T_{OP}(X)$, helyettesitendo $h(N)(h^*(t_1), \cdots, h^*(t_n))$ operacioval.
Roviden:
- minden x valtozo helyere $h(s) = s'$-nek megfelelo valtozo;
- L, R term a $h(N) = N'$-nek helyere megfelelo operaciokkal kepezett $L' = R'$ lekepezes.

Specifikaciomorfizmus: Adva: $SPEC = (\Sigma, S, OP, E)$, $SPEC' = (\Sigma', S', OP', E')$,
$h_{SPEC} : SPEC \to SPEC'$;
$h_{SPEC} = (h_\Sigma, h_E)$; $h_\Sigma : \Sigma \to \Sigma'$; $h_E : E \to E'$;
$E' = h_E(E) = \{h^*(e) | \forall e = (X, L, R) \in E\}$.

Definicio: Adva parameteres tipusspecifikacio:
$PSPEC = (SPEC, SPEC1)$; ahol $SPEC = (S, OP, E)$, $SPEC1 = SPEC \cup (S1, OP1, E1)$.

Adva tovabba $h : SPEC \to SPEC'$ specifikacio morfizmus, ahol $SPEC' = (S', OP', E')$.

Patameteratado morfizmus diagramja:

$$\begin{array}{ccc} SPEC & \xrightarrow{p:tartalmazas} & SPEC1 \\ \big\downarrow{\scriptstyle h:SPEC\to SPEC'} & & {\scriptstyle h_1}\big\downarrow \\ SPEC' & \xrightarrow{p':tartalmazas} & SPEC1' \end{array}$$

A parameteratadas jelentese:

- Ha p es p' tartalmazas az osszes reszspecifikacio eseten;
- h_1: $(\forall s \in S \cup S1)(h1(s) = \text{if } s \in S1 \text{ then } s \text{ else } h(s) \text{ fi})$

$(\forall (N : s_1 \cdot s_n) \in OP \cup OP', n \geq 0)(h1(N : s_1 \cdots s_n) =$

if $(N : s_1 \cdots s_n) \in OP$ then $n : h1(s_1) \cdots h1(s_n) \to h1(s)$ else $h(N) : h(s_1) \cdots h(s_n) \to h(s) fi$;

- $SPEC1' = SPEC' \cup (S', OP', E1')$, ahol $S1' = S1, OP1' = h1(OP1), E1' = h1^*(E1)$.

Adattipusosztaly specifikacioja:

PAR: formalis parameterek specifikacioja;

$EXP = PAR \cup (S1, OP1, E1)$: export felulet specifikacioja;

$IMP = PAR \cup (S2, OP2, E2)$: import felulet specifikacioja;

$BOD = IMP + eb(EXP)$: megvalositas specifikacioja;

$$\begin{array}{ccc} PAR & \xrightarrow{e} & EXP \\ \big\downarrow{\scriptstyle i} & & \big\downarrow{\scriptstyle eb} \\ IMP & \xrightarrow{ib} & BOD \end{array}$$

Specifikacio: PAR, IMP;

Kituntetett sortu specifikacio:

$EXP = (S_{EXP}, OP_{EXP}, E_{EXP}); pt(S_{EXP}) \in S_{EXP}$;

$BOD = (S_{BOD}, OP_{BOD}, E_{BOD}); pt(S_{BOD}) \in S_{BOD}$;

Tartalmazas: e, i, ib; (Ha az absztrakt es a konkret parameterek azonosak!)

eb: $EXP \to BOD$; kituntetett sortu morfizmus;

Jelolese a torzs reszben: oprs: rep: $pt(S_{BOD}) \to pt(S_{EXP})$

Absztrakt adattipus specifikacioja:

$PAR \xrightarrow{e} EXP$

Absztrakt adattipus az adattipusoknak egy olyan osztalya, amely zart az adattartomanyok, a muveletek, a tartomanyok peldanyainak es a muveleteknek az elnevezese alapjan. Igy az absztrakt adattipus fuggetlen az adatok abrazolasatol es az adott abrazolasok mellett a muveletek megvalositasatol.

$\langle$osztalynev$\rangle$ **is a class specification**=

parameters=

  sorts:

  oprs:

  eqns:

exports=

  class sort: $\langle$osztalynev$\rangle$

  oprs:

eqns:

imports=

sorts:

oprs:

eqns:

body= sorts:

oprs: rep: $pt(S_{BOD}) \to pt(S_{EXP})$;

eqns:

end $\langle$osztalynev$\rangle$;

Osztalyspecifikacio, specialis esetek:

$$\begin{tikzcd} SPEC \arrow[r] \arrow[d] & SPECEXP \arrow[r] \arrow[d] & SPEC\emptyset \arrow[d] \\ PSPEC \arrow[r] & PSPECEXP \arrow[r] & CLASS \end{tikzcd}$$

Kozepen nincs nyil (csak maskepp nem tudtam)!

$SPEC = (\emptyset, BOD, \emptyset, BOD)$;
$SPECEXP = (\emptyset, EXP, \emptyset, BOD)$;
$SPEC0 = (\emptyset, EXP, IMP, BOD)$;
$PSPEC = (PAR, BOD, \emptyset, BOD)$;
$PSPECEXP = (PAR, EXP, \emptyset, BOD)$;
$CLASS = (PAR, EXP, IMP, BOD)$;

Itt van meg 2 tablazat.

4. eloadas:

Definicio: termek szarmaztatasa
Adva $\Sigma = (S, OP)$ szignatura es a hozzatartozo E szemantikai egyenletek halmaza, rogzitett $X = X_e$ mellett, minden $e = (L, R) \in E$ eseten. Az egyenlet ket helyettesitesi szabalyt definial:
$L \to R$; $R \to L$;
Ha a $t1 \to t2$ szabaly alkalmazhato egy $t \in T_{OP}(X)$ termre, es t1 a t-nek egy resztermje, akkor t1 helyettesitese t2-vel a t termben egy ujabb t' termet eredmenyez.
Jeloles: $t' = t(t1/t2)$.
Ekkor azt mondjuk, hogy t' term kozvetlen szarmaztatasa t termnek E axiomai altal a $t1 \to t2$ szabaly felhasznalasaval.

A kozvetlen szarmaztatasok egy $t0 \to t1 \to \cdots \to tn$ sorozata eseten $t = t0$ es $t' = tn$ jeloles mellett az $e' = (t, t')$ egyenlet E-bol szarmaztatott egyenletnek nevezzuk az adott Σ szignaturahoz tartozo rogzitett X mellett.
A szarmaztatott egyenlet helyes, ha t kiertekelese megegyezik t' kiertekelesevel.

$\Sigma = (S, OP)$; Σ-algebra$=(S_A, OP_A)$;
$SPEC_A = (S_A, OP_A, E_A)$; $d_a = (A, F, E_a)$; $d_a = (\{A_0, A_1, \cdots, A_n\},$
$\{f_0 \to A_0, \cdots, f_m : A_i \cdots A_j \to A_k\}, \{\cdots, \alpha(a) \Rightarrow f_s(f_c(a)) = h(a), \cdots\},$
ahol $a \in A : (a_i, \cdots, a_k) \in (A_i x \cdots x A_i)$;
Jelolesek: $F = F_c \cup F_s$; $f_c \in F_c$; $f_s \in F_s$;

Egyenloseg axioma:
$a_1 = a_2 \equiv ([a_1 = f_0 \wedge a_2 = f_0] \vee [(\forall f_s \in F_s)(f_s(a_1) = f_s(a_2))]);$
A helyettesitesi szabaly:
$a_1 = a_2 \to ([a_1 = f_0 \wedge a_2 = f_0] \vee [(\forall f_s \in F_s)(f_s(a_1) = f_s(a_2))]);$

Strukturalis indukcio:
Adott $\Sigma = (S, OP)$ a szignaturahoz tartozo X valtozokkal.
Legyen p predikatum, amely $t \in T_{OP}(x)$ termekre van ertelmezve.
Ha

1. $(\forall t \in K \wedge \forall t \in X)(p(t) \equiv T)$;
2. $(\forall N(t1, \cdots, tn) \in T_{OP}(X))(p(N(t_1, \cdots, t_n) \equiv T)$;

akkor $(\forall t \in T_{OP}(X))(p(t) \equiv T)$.

Strukturalis indukcio atfogalmazasa:
Adott $\Sigma = (S, OP)$ a szignaturahoz tartozo X valtozokkal.
Legyen $p(t) : H_1(t) = H_2(t)$ predikatum, amely a $t \in T_{OP}(X)$ termekre van ertelmezve.
Ha

1. Alapeset: $(\forall t \in K \wedge \forall t \in X)(H_1(t) = H_2(t) \equiv T)$;
2. Indukcios lepes: $(\forall N(t_1, \cdots, t_n) \in T_{OP}(X))(H_1(N(t_1, ..., t_n)) = H_2(N(t_1, ..., t_n)) \equiv T)$;

akkor $(\forall t \in T_{OP}(X))(H_1(t) = H_2(t) \equiv T)$

Adott $\Sigma = (S, OP)$; $t \in T_{OP}(X)$; Legyen $t_1 = H_1(f_s(t))$; $t_2 = H_2(t)$;
Tekintsuk a $f_s(f_c(t)) = H_{sc}(t)$ axiomat.
Tetel: $H_1(f_s(t)) = H_2(t)$
Bizonyitas:

- Alapeset:
  Bizonyitsuk be f_0 konstans szimbolumra, hogy $t = f_0$ eseten: $H_1(f_s(f_0)) = H_2(f_0)$;
- Strukturalis indukcios lepes:
  Mutassuk ki, hogy minden $t = f_c(t') \in T_{OP}(X)$ konstrukcios muveletre, hogy ha
  $H_1(f_s(t')) = H_2(t') = T$, akkor $H_1(f_s(f_c(t'))) = H_2(f_c(t')) \equiv T$;
  azaz $H_1(H_{sc}(t')) = H_2(f_c(t')) \equiv T$;

A strukturalis indukcio ket helyettesitesi szabalya:

1. Alapeset: $H_1(f_s(t)) = H_2(t) \rightarrow H_1(f_s(f_0)) = H_2(f_0)$;
2. Indukcios lepes: $H_1(f_s(f_c(t'))) = H_2(f_c(t')) \rightarrow H_1(H_{sc}(t)) = H_2(f_c(t'))$;

Reprezentacios fuggveny: Adva egy adattipus absztrakt es konkret specifikacioja:
$d_a = (A, F, E_a)$; $\quad d_c = (C, G, E_c)$;
$A = A_0, ..., A_n$; $\quad C = C_0, ..., C_m$;
$F = \{f_0 :\rightarrow A_0, \cdots, f_i : A_i \cdots A_k \rightarrow A_l, \cdots\}; G = \{g_0 \rightarrow C_0, \cdots, g_i : C_i \cdots C_k \rightarrow C_l, \cdots\}$;
Az absztrakt es konkret objektumok egymashoz valo viszonya:
$\varphi : C \rightarrow A \quad \varphi = (\varphi_0, \cdots, \varphi_n)$, ahol $\varphi_0 : C_0 \rightarrow A_0; \cdots; \varphi_n : C_n \rightarrow A_n$;

Definicio: Adva d_a absztrakt es d_c konkret tipusspecifikaciok, amelyeknek szignaturajuk azonos.
Adva tovabba $\varphi : C \rightarrow A$ morfizmus.
A C objektumhalmazt az A egy reprezentaciojanak nevezzuk, ha $(\forall a \in A)((\exists c \in C)(a = \varphi(c))$;

Tetel: Adva d_a absztrakt es d_c konkret tipusspecifikaciok azonos szignaturaval.
$\varphi : C \rightarrow A$ morfizmus.
$F_c \subset F$ a konstrukcios muveletek halmaza.
Felteves: $\forall f_c \in F_c$ konstrukcios muveletre fennall:
$\quad a \in A \wedge f_c(a) \in A \wedge c \in C \wedge g_c(c) \in C \wedge a = \varphi(c)$.
Ha $(\forall c \in C \wedge \forall f_c \in F_c)(f_c(\varphi(c)) = \varphi(g_c(c)))$, akkor C objektumhalmaz az A egy reprezentacioja.
Bizonyitas: Strukturalis indukcioval:
a) alapeset: $a = f_0 . f_0 \in A_0, g_0 \in C_0$, feltevesunk szerint $f_0 = \varphi(g_0)$.
Tehat $a = f_0$ eseten letezik olyan $c \in C_0$, hogy $a = \varphi(c)$.
b) indukcio: $a' = f_c(a)$, ahol feltesszuk, hogy $a = \varphi(c)$ es $c \in C_0$.
Tehat $a' = f_c(\varphi(c))$ es muvelettartasra vonatkozo feltevesunk alapjan:
$a' = \varphi(g_c(c))$, es $c' = g_c(c)$ valasztas mellett $a' = \varphi(c')$ es $c' \in C_0$.

A reprezentacios fuggveny implicit definicioja:
$f_0 = \varphi(g_0)$;
$(\forall f_c \in F_c)(f_c(\varphi(c)) = \varphi(g_c(C))$;

A reprezentacios fuggveny rekurziv (explicit) definicioja:
Tegyuk fel, hogy $c = g_c(g_s(c))$.
Ennek alapjan a reprezentacios fuggveny rekurziv definicioja:
$\varphi(c) =$if $c = g_0$ then f_0 else $f_c(\varphi(g_s(c)))$.

A reprezentacios fuggveny definicioja nem egyertelmu!

5. eloadas

Interfesz lekepezesek:
    Megvalositas: interfesz $\rightarrow BOD_M$
    Kiterjesztes: interfesz $\rightarrow BOD_M$
    Finomitas: interfesz $\rightarrow$ interfesz'

$$\begin{tikzcd} formpar \arrow[r, "p"] \arrow[d, "b"] & SPEC(formpar) \arrow[d, "h_1"] \\ aktpar \arrow[r, "p'"] & SPEC(aktpar) \end{tikzcd}$$

Egzakt megvalositas:
Adott a modulspecifkacio: MOD=(PAR, EXP, IMP, BOD, e, eb, i, ib),
ahol a MOD modul interfesz specifikacioja: I(MOD)=(PAR, EXP, IMP, e, i).
Az INT interfesz specifikaciot a MOD modulspecifikacio egzakt megvalositasanak nevezzuk, ha I(MOD)=INT.

Megvalositas: Adott egy INT=(PAR, EXP, IMP, e, i); interfesz specifikacio.
A MOD'=(PAR', EXP', IMP', BOD', e', eb', i', ib') modulspecifikaciot az INT interfesz specifikacio megvalositasanak nevezzuk, ha letezik olyan $r = (r_P, r_E, r_I)$ specifikacio morfizmus harmas, amelyikre $i' \circ r_P = r_I \circ i$; es $e' \circ r_P = r_P \circ e$;
A megvalositas az alabbi diagram kommutaciojat fejezi ki: $\cdots$

Ha $r_P = r_E = r_I =$ identitas, akkor egzakt megvalositas.

Legyen SPEC'=(S', OP', E') a SPEC=(S, OP, E) specifikaciobol morfizmussal szarmaztatott specifikacio:
- Tartalmazas
- Atnevezes. a Specifikaciot atnevezzuk ugy, hogy a sortok, az operaciok uj nevet kapnak, de ugy, hogy a szemantika valtozatlan marad
- Abrazolas, amely az atnevezes egy formaja

A sort atnevezesenek jelolese: sorts: $\langle$uj sort neve$\rangle$ = $\langle$¡regi sort neve$\rangle$
Az operacios szimbolum atnevezesenek jelolese: oprs: $\langle$uj op neve$\rangle$ = $\langle$regi op neve$\rangle$
Deklaracios resz atnevezese: (a sortok atnevezesei alapjan automatikus)
eqns: $a1, a2, ..., ak \in$ $\langle$regi sort neve$\rangle$;
Atnevezes: eqns: $c1, c2, ..., ck \in$ $\langle$ uj sort neve $\rangle$;

Szemantikai egyenletek atnevezese:
(A sortok es operacios szimbolumok atnevezesei alapjan automatikus.)
regi axioma: $e : L = R$;   regi op neve: $f_0, ..., f_n$;
$L : f_s(f_c(a))$; $R : f_i(...(f_j(a))...)$;
uj op nevek rendre: $g_0, ..., g_n$; akkor
uj axioma: $e' = L' = R'$; ahol $L' : g_s(g_c(a))$; $R' : g_i(...(g_j(a))...)$;

Tetel: Adva d_a absztrakt es d_c konkret tipusspecifikaciok azonos szignaturaval.
$\varphi : C \to A$ morfizmus.
$F_c \subset F$ a konstrukcios muveletek halmaza.
Felteves: $\forall f_c \in F_c$ konstrukcios muveletre fennall:
$a \in A \wedge f_c(a) \in A \wedge c \in C \wedge g_c(c) \in C \wedge a = \varphi(c)$.
Ha $(\forall c \in C \wedge \forall f_c \in F_c)(f_c(\varphi(c)) = \varphi(g_c(c)))$, akkor C objektumhalmaz az A egy reprezentacioja.
Bizonyitas: Strukturalis indukcioval:
a) alapeset: $a = f_0 . f_0 \in A_0, g_0 \in C_0$, feltevesunk szerint $f_0 = \varphi(g_0)$.
Tehat $a = f_0$ eseten letezik olyan $c \in C_0$, hogy $a = \varphi(c)$.
b) indukcio: $a' = f_c(a)$, ahol feltesszuk, hogy $a = \varphi(c)$ es $c \in C_0$.
Tehat $a' = f_c(\varphi(c))$ es muvelettartasra vonatkozo feltevesunk alapjan:
$a' = \varphi(g_c(c))$, es $c' = g_c(c)$ valasztas mellett $a' = \varphi(c')$ es $c' \in C_0$.

A reprezentacios fuggveny implicit definicioja:
$f_0 = \varphi(g_0)$;
$(\forall f_c \in F_c)(f_c(\varphi(c)) = \varphi(g_c(C))$;
A reprezentacios fuggveny rekurziv (explicit) definicioja:
Tegyuk fel, hogy $c = g_c(g_s(c))$.
Ennek alapjan a reprezentacios fuggveny rekurziv definicioja:
$\varphi(c) =$if $c = g_0$ then f_0 else $f_c(\varphi(g_s(c)))$.

A reprezentacios fuggveny definicioja nem egyertelmu!

Reprezentacio jelolese:
body =
oprs: rep: vector nat data $\to$ stack
eqns: $v \in$ vector, $n \in$ nat, $d \in$ data
create = (nil, zerus)
push(v, n, d) = (put(v, n+1, d), n+1)
body =
oprs: rep: $C_0 C_1 \cdots C_i \to A_0$
eqns: $c_0 \in C_0$; $c_1 \in C_1$; $\cdots ; c_i \in C_i$
$f_0 = g_0(c)$
$f_c(c_0, c_1, \cdots, c_i) = g_c(c)$

A BOD spedcifikacio reprezentacios formaja:
(az ib, eb morfizmusok alapjan automatikus kiegeszitessel egyutt)
body = imports +
class sort: C0
oprs: rep: $C_0 C_1 \cdots C_i \to A_0$ $(\forall f_i : A^+ \to A \in F)(g : C^+ \to C)$
eqns: $c_0 \in C_0; c_1 \in C_1 \cdots c_2 \in C_2$
$f_0 = g_0(c)$
$f_c(c_0, c_1, \cdots, c_i) = g_c(c)$
$\forall (f_s(f_c(a)) = f_i(...(f_j(a))...) \in exports \wedge a = rep(c))$

$g_s(g_c(c)) = g_i(\cdots(g_j(c))\cdots);$

Reprezentacio elemzes:
- $\varphi_1(c) = \varphi_2(c)$?
- $attr_c(c) = attr_s(\varphi(c))$?
- $c_1 = c_2 \Rightarrow \varphi(c_1) = \varphi(c_2)$?
- $I_c(c) \Rightarrow I_a(\varphi(c))$?
(Ha $attr_c(c) = attr_a(\varphi(c))$ es $I_c(c) : 0 \leq attr_c(c) \leq n$ es $I_a(\varphi(c)) : 0 \leq attr_a(\varphi(c)) \leq n$, akkor az $I_c(c) \Rightarrow I_a(\varphi(c))$ allitas trivialis.)

$\varphi_1(c) = \varphi_2(c) \equiv (\varphi_1(c) = f_0 \wedge \varphi_2(c) = f_0) \vee (\forall f_s \in F_s)(f_s(\varphi_1(c)) = f_s(\varphi_2(c)));$
Bizonyitas:
a.) alapeset: $c = g_0$; $(\varphi_1(g_0) = f_0 \wedge \varphi_2(g_0) = f_0)$
b.) indukcios lepes: $c = g_{c1}(c')$, ahol c'-re $\varphi_1(c') = \varphi_2(c')$.
$\varphi_1(g_{c1}(c')) = \varphi_2(g_{c1}(c')) = (\forall f_s \in F_s)(f_s(\varphi_1(g_{c1}(c'))) = f_s(\varphi(g_{c1}(c')))) = (\forall f_s \in F_s)(f_s(f_{c1}(\varphi_1(c'))) = f_s(f_{c2}(\varphi_2(c'))))$

Allitas: $attr_c(c) = attr_s(\varphi(c))$ Bizonyitas indukcioval:
a.) alapeset: $c = g_0 \Rightarrow \varphi(g_0) = f_0$; $attr_c(g_0) = attr_a(\varphi(g_0))$?
b.) indukcios lepes: Felteves $c = g_c(c')$ mellett $attr_c(c') = attr_a(\varphi(c'))$
$attr_c(c) = attr_c(g_c(c'))$
$attr_a(\varphi(c)) = attr_a(\varphi(g_c(c')) = attr_a(f_c(\varphi(c'))$
$attr_c(g_c(c')) = attr_a(f_c(\varphi(c'))$

$c_1 = c_2 \Rightarrow \varphi(c_1) = \varphi(c_2)$?
$c_1 = c_2 \equiv (c_1 = g_0 \wedge c_2 = g_0) \vee (\forall g_0 \in G_s)(g_s(c_1) = g_s(c_2)) \Rightarrow \varphi_1(c) = \varphi_2(c)$
$\equiv (\varphi_1(c) = f_0 \wedge \varphi_2(c) = f_0) \vee (\forall f_s \in F_s \cdots$

6. eloadas

Kettos specifikacio: Adott $d_a = (A, F, E_a)$; $d_c = (C, G, E_c)$; $a_0 = \{c|I_a(c)\}$; $C_0 = \{c|I_c(c)\}$;
abrazolas: $\varphi : C_0 \to A_0$;
$E_a = \{\cdots, \alpha(a) \Rightarrow f_s(f_c(a)) = h(a); \cdots), (\neg I_a(f_c(a)) \wedge I_a(a)) \Rightarrow f_c(a) = \text{"undefined"}\}$;
$h(a) = f_i(\cdots(f_j(a)))$,
$E_c = \{\cdots, \alpha_c(c) \Rightarrow g_s(g_c(c)) = h_c(c); (\neg I_c(g_c(c)) \wedge I_c(c)) \Rightarrow g_c(c) = \text{"undefined"}\}$; (algebrai leiras)
$h_c(c) = (g_i(\cdots(g_j(c))), \cdots)$,
$E_c = \{\cdots, \{pre_i(c)\}c' = g_i(c, c')\{post_i(c, c')\}, \cdots, \}$ (elo-utofelteteles leiras)
$\{I_c(g_c(c)) \wedge I_c(c)\}c' = g_c(c, c')\{I_c(c') \wedge c' = f_c(c)\}$;
$E_c = \{\cdots, Q_i(c, c'), \cdots\}$;

Minden algebrai axioma elo- utofelteteles formara hozhato.
$\alpha(a) \Rightarrow f_s(f_c(a)) = h(a)$;
$\{\alpha(a) \wedge b = f_c(a)\}b' = f_s(b)\{b' = h(a)\}$
$(\neg I_a(f_c(a)) \wedge I_a(a)) \Rightarrow f_c(a) = \text{"undefined"}$;
$\{I_a(a) \wedge I_a(f_c(a))\}\ a' = f_c(a)\ \{I_a(a') \wedge a' = f_c(a)\}$

Definicio: (Az implementacio helyessege)
Adva $d_a = (A, F, E_a)$ absztrakt specifikacio, $d_c = (C, G, E_c)$ konkret specifikacio, amelynek szignaturaja azonos.
$\varphi : C \to A$ morfizmus.
Ha

1. C az A egy reprezentacioja az adott φ mellett;
2. $(\forall f_i \in F)(c \in C \wedge \varphi(c) \in A \wedge f_i(\varphi(c))$ ertelmezve van, akkor $g_i(c)$ is ertelmezve van;
3. $(\forall f_i \in F)(c \in C \wedge c' = g_i(c) \wedge c' \in C \wedge \varphi(c) \in A \wedge \varphi(c') \in A$, akkor $f_i(\varphi(c)) = \varphi(g_i(c))$;

akkor d_c a d_a szerint helyes.
Ld. 92. o. abra.

Allitas: Adva $d_a = (A, F, E_a)$, $d_c = (C, G, E_c)$, $\varphi : C \to A$; es d_c a d_a szerint helyes.
P_a (absztrakt program), $p_a(a)$: P_a programfuggvenye.
Allitsuk elo a P_c konkret programot a P_a absztrakt programbol ugy, hogy
$\forall a \in A$ helyere a megfelelo $c \in C$-t
$\forall f_i \in F$ helyere a megfelelo $g_i \in G$-t tesszuk.
Ha a konkret program programfuggvenye a $p_c(c)$ es a programok indulasakor $a_0 = \varphi(c_0)$,
akkor $p_a(\varphi(c_0)) = \varphi(p_c(c_0))$.
Bizonyitas: Az adattipus programban szereplo muveleteinek szama szerinti teljes indukcioval.
a.) Alapeset: Felteves: indulaskor $a_0 = \varphi(c_0)$.
b.) Indukcios lepes:
k a muveletek szama, $k > 0$. A k-ik muvelet eredmenye:
$a_k = f(a_{k-1})$, $c_k = g(c_{k-1})$;
Indukcios felteves: $a_{k-1} = \varphi(c_{k-1})$
A k-ik muvelet eredmenye: $(f(a_{k-1}), g(c_{k-1}))$,
$a_k = f(a_{k-1}) = f(\varphi(c_{k-1})) = \varphi(g(c_{k-1})) = \varphi(c_k)$.

Az utolso lepes eredmenye:
(a', c'), $a' = \varphi(c')$, $a' = p_a(a_0)$ es $c' = p_c(c_0)$,
ezert $a' = \varphi(c')$, azaz $p_a(a_0) = \varphi(p_c(c_0))$, $p_a(\varphi(c_0)) = \varphi(p_c(c_0))$

Allitas: (A kulso felulet specifikaciojaval adott konkret specifikacio absztrakt specifikacio szerinti helyessegenek egy elegseges feltetele.)
Adva $d_a = (A, F, E_a)$, $d_c = (C, G, E_c)$,
$E_a = \{\{\text{"}true\text{"}\}\ a = f_0\ \{post_{f_0}(a)\}, \cdots, \{pre_{f_i}(a)\}\ a' = f_i(a)\ \{post_{f_i}(a, a')\}, \cdots\}$,
$E_c = \{\{\text{"}true\text{"}\}\ c = g_0\ \{post_{g_0}(c)\}, \cdots, \{pre_{g_i}(c)\}\ c' = g_i(c)\ \{post_{g_i}(c, c')\}, \cdots\}$.
$A_0 = \{a | I_a(a)\}$, $C_0 = \{c | I_c(c)\}$, $\varphi : C \to A$.
Ha bebizonyitjuk, hogy

1. $I_c(c) \Rightarrow I_a(\varphi(c)$;
2. $post_{g_0}(c) \Rightarrow I_c(c)$;
3. $post_{g_0}(c) \Rightarrow post_{f_0}(\varphi(c))$;
4. $I_c(c) \wedge pre_{f_i}(\varphi(c)) \Rightarrow pre_{g_i}(c)$;
5. $I_c(c) \wedge pre_{f_i}(\varphi(c)) \wedge post_{g_i}(c, c') \wedge I_c(c') \Rightarrow post_{f_i}(\varphi(c), \varphi(c'))$;

akkor a d_c konkret specifikacio a d_a absztrakt specifikacio szerint helyes.
Bizonyitas:
a) C az A egy reprezentacioja
- $a = f_0$. 2. es 1. szerint: $g_0 \in C \wedge \varphi(g_0) \in A$. 3. szerint: $\varphi(g_0) = f_0$.
- 4. szerint: ha $f_c \in F_c$, $f_c(\varphi(c))$ ertelmezve van, akkor $g_c(c)$ is ertelmezve van.
- 5. szerint: $\varphi(c') = f_c(\varphi(c)) \wedge c' = g_c(c)$, azaz $f_c(\varphi(c)) = \varphi(g_c(c))$

b) Morfizmusdiagram szerinti kapcsolat
- 3. szerint: ha $\forall f_i \in F, f_i(\varphi(c))$ ertelmezve van, akkor $g_i(c)$ is ertelmezve van.
- 5. es 1. szerint $c' = g_i(c) \wedge I_c(c') \wedge I_a(\varphi(c')) \wedge \varphi(c') = f_i(\varphi(c)), (\forall f \in F)(\varphi(g(c)) = f(\varphi(g(c)))$.

Megj.: Ha $p = f_i(a)$ es $q = g_i(c)$, ahol p, q parameterek, akkor $f_i(\varphi(c)) = \varphi(g_i(c))$ helyebe p=q lep.

Reprezentacio elemzes:
$\varphi_1(c) = \varphi_2(c)$?
$length_c() = length_a(\varphi(c))$?
$c_1 = c_2 \Rightarrow \varphi(c_1) = \varphi(c_2)$?
$I_c(c) \Rightarrow I_a(\varphi(c))$?

Implementacio elemzes:
$post_{g_0}(c) \Rightarrow post_{f_0}(\varphi(c))$?
$I_c(c) \wedge pre_{f_i}(\varphi(c)) \Rightarrow pre_{g_i}(c)$?
$I_c(c) \wedge pre_{f_i}(\varphi(c)) \wedge post_{g_i}(c, c') \wedge I_c(c') \Rightarrow post_{f_i}(\varphi(c), \varphi(c'))$?

Formalis parameterek aktualizalasaval torteno abrazolas:
Definicio: Adott egy INT = (PAR, EXP, IMP, e, i) interfesz specifikacio.
Adott annak MOD'=(PAR', EXP', IMP', BOD', e', eb', i', ib'); megvalositasa.
Ekkor a $r = (r_P, r_E, r_I)$ specifikacio morfizmus harmasra: $i' \circ r_P = r_I \circ i$; es $e' \circ r_P = r_E \circ e$;

7. eloadas

Interfesz realizaciok:
INT = (PAR, EXP, IMP, e, i); interfesz specifikacio.
$r : INT \to MOD$;
1.) incialis realizacio; Jeloles: IR(INT);
2.) Vegleges realizacio; Jeloles: FR(INT);
Legyen I(IR(INT)) = INT, I(FR(INT)) = INT, akkor mindket modulspecifikacio egzakt realizacio.
Inicialis realizacio: $IR(INT) = (PAR, EXP, IMP, BOD, e, i, eb_1, ib_1)$;
Vegleges realizacio: $FR(INT) = (PAR, EXP, IMP, FINAL, e, i, eb_2, ib_2)$;

Szarmaztatas: (Derivation):
$t_0 \to t_1 \to \cdots \to t_n$, $e = (t_0, t_n)$, $t_1 \in T_{OP,X}$;
$e_i \in E : e_i = e(X, L_i, R_i)$; $e_0 \to e_1 \to \cdots \to e_n$; $e_i \equiv T$; $\quad i = 1, \cdots, n$;
Jeloles:
$d_a = (A, F, E_a)$: a $PAR \cup EXP$ export felulet specifikacioja.
$d_c = (C, G, E_c)$: a BOD torzsresz specifikacioja, realizacio.
Adva $\varphi(c)$ reprenzentacios fuggveny.

Definicio: Legyen $E_a = \{L_{ai}(a) = R_{ai}(a) | 1 \le i \le k\}, E_c = \{L_{ci}(c) = R_{ci}(c) | 1 \le i \le k\}$;
Ha $(\forall i, 1 \le i \le n)(e_{ai}(a) \to \cdots \to e_{ai}(a); e_{ci}(c) \to \cdots \to e_{ck}(c))$
es $(\forall i, 1 \le i \le n)(e_{ai}(\varphi(c)) = e_{ck}(c) \equiv T)$, akkor d_c specifikaciot a d_a specifikacio szerinti korrekt realizacionak nevezzuk az adott $\varphi(c)$ reprezentacio mellett.

Tetel:
$d_a = (A, F, E_a)$: az export felulet specifikacioja, $d_c = (C, G, E_c)$: a torzsresz specifikacioja.
Adva $\varphi(c)$ reprezentacios fuggveny. Ha
- $(\varphi(t_{c1} = \varphi(t_{c2})) \equiv (t_{c1} = t_{c2})$,
- barmely (t_a, t_c) par, ahol $t_a \in T_{\Sigma_a}, t_c \in T_{\Sigma_c}$, $t_a = \varphi(t_c)$;

akkor d_c a d_a szerinti korrekt realizacio a $\varphi(c)$ reprezentacio mellett.
Bizonyitas:
$L_{ai}(a) = R_{ai}(a)$;
$l_{ai}(a) \to L_{ai}(\varphi(c)) \to \varphi(L_{ci}(c))$;
$R_{ai}(a) \to R_{ai}(\varphi(c)) \to \varphi(R_{ci}(c))$;
Tehat $\varphi(L_{ci}(c)) = \varphi(R_{ci}(c)) \equiv L_{ci}(c) = R_{ci}(c)$;

Adott $L_{ai}(\varphi(c)) = R_{ai}(\varphi(c))$;
Peldaul: $f_s(f_c(\varphi(c))) = f_c(f_s(\varphi(c)))$
Vegleges realizacio:
- $\{pre_g(c)\}\ c' = g(c)\ \{post_g(c, c')\}$;
- $Q_g(c)$;

Proceduralisan adott konkret specifikacio elo- es utofeltetelekkel adott absztrakt specifikacio szerinti helyessege:
Tetel:
Adottak a d_a es a d_c specifikaciok kozos szignaturaval:

$d_a = (A, F, E_a)$; $A = \{A_0, A_1, \cdots, A_n\}$; $F = \{f_0 :\to A_0, f_1 : A^+ \to A, \cdots, f_m : A^+ \to A\}$;
$\{"true"\}$ $a = f_0$ $\{post_{f_0}(a)\} \in E_a$,
$\{pre_{f_i}(a)\}$ $a' = f_i(a)$ $\{post_{f_i}(a, a')\} \in E_a$, $f_i \in F$;
$d_c = (C, G, E_c)$; $C = \{C_0, C_1, \cdots, C_n\}$; $G = \{g_0 :\to C_0, g_1 : C^+ \to C, \cdots, g_m : C^+ \to C\}$;
$(\forall i, i \in \{0, 1, \cdots, m\})$ $(Q_{g_i} \in E_c, g_i \in G)$, ahol Q_{g_i} az f_i kiszamitasara szolgalo eljaras, azaz:
procedure g_0 begin Q_0 end;
precedure g_i begin Q_i end; $i = 1, \cdots, n$;

absztrakt invarians: $A_0 = \{a | I_a(a)\}$,
konkret invarians: $C_0 = \{c | I_c(c)\}$,
A reprezentacios fuggveny: $\varphi : C \to A$

Ha a kovetkezo tetelek teljesulnek:
1. $(\forall c \in C)(I_c(c) \Rightarrow I_a(\varphi(c))$;
2. $\{"true"\}$ Q_0 $\{post_{f_0}(\varphi(c) \wedge I_c(c)\}$;
3. $(\forall f_i \in F)$: $\{pre_{f_i}(\varphi(c)) \wedge I_c(c)\}$ Q_i $\{post_{f_i}(\varphi(c), \varphi(c')) \wedge I_c(c')\}$;
ahol 2. es 3. teljes helyessegi tetelek, akkor a d_c konkret specifikacio a d_a absztrakt specifikacio szerint helyes.
Bizonyitas:
- C az A egy reprezentacioja.
Minden $g_i(c)$ konstrukctios muvelet szimulalja $f_i(\varphi(c))$-t.
$(\{"true"\}$ Q_0 $\{post_{f_0}(\varphi(c)) \wedge I_c(c)\} \equiv "true") \Rightarrow f_0 = \varphi(g_0) \wedge g_0 \in C)$.
$((\forall f_i \in F_c)$: $\{pre_{f_i}(\varphi(c)) \wedge I_c(c)\}$ Q_i $\{post_{f_i}(\varphi(c), \varphi(c')) \wedge I_c(c')\}) \Rightarrow$
1.) ha $f_i(\varphi(c))$ ertelmezve van, akkor $g_i(c)$ is.
2.) $(c \in C \wedge c' = g_i(c) \wedge c' \in C \wedge a = \varphi(c) \wedge a \in A \wedge a' = f_i(a) \wedge a' \in A) \Rightarrow a' = \varphi(c')$.
- minden $g_i(c)$ nem konstrukcios muvelet is szimulalja $f_i(\varphi(c))$-t.
$((\forall f_i \in F)$: $\{pre_{f_i}(\varphi(c)) \wedge I_c(c)\}$ Q_i $\{post_{f_i}(\varphi(c), \varphi(c')) \wedge I_c(c)\}) \Rightarrow$
3.) ha $f_i(\varphi(c))$ ertelmezve van akkor $g_i(c)$ is.
4.) $(c \in C \wedge c' = g_i(c) \wedge c' \in C \wedge a = \varphi(c) \wedge a \in A \wedge a' = f_i(a) \wedge a' \in A) \Rightarrow a' = \varphi(c')$

Determinisztikus program:
$S ::= skip | u \leftarrow t | S1; S2 |$ if B then S_1 else S_2 fi | while B do S_1 od
$u \leftarrow t$ ertekadas; u valtozo, t kifejezes; u es t azonos tipusuak.
B kvantorfuggetlen logikai kifejezes;

8. eloadas

Tipus:
Alaptipusok: integer; bool; $\cdots$
Osszetett tipusok: $T_1 T_2 \cdots T_n \to T$; $n \geq 1$, ahol $T_1, T_2, \cdots T_n, T$ alap tipusok.

Valtozo es konstans:
- valtozo:
  - egyszeru valtozo: (integer, bool, $\cdots$);
  - tomb valtozo: egy dimenzios, tobb dimenzios;
- konstans:
  - alap tipusu: integer, bool, $\cdots$;
  - osszetett tipusu: $T_1 T_2 \cdots T_n \to T$;
    T bool: akkor relacio szimbolum,
    T nem bool: fuggveny szimbolum.

Tipusos kifejezesek:

1. T alaptipusu konstans.
2. Egyszeru T tipusu valtozo.
3. Ha $s_1, \cdots, s_n$ rendre $T_1, \cdots, T_n$ tipusu kifejzesek es op: $T_1 \cdots T_n \to T$, akkor $op(s_1, \cdots s_n)$ T tipusu kifejezes.
4. Ha $s_1, \cdots, s_n$ rendre $T_1, \cdots, T_n$ tipusu kifejezesek, A egy $T_1 \cdots T_n \to T$ tomb, akkor $A[s_1, ..., s_n]$ T tipusu kifejezes.
5. Ha α Boolean kifejezes es s_1, s_2 T tipusu kifejzesek, akkor if α then s_1 else s_2 fi T tipusu kifejzes.

Az alap tipus-halazokon ertelmezett szokasos kifejezesek rekurziv definicioja:
kifejezes $e ::= c \mid x \mid (e_1 + e_2) \mid (e_1 - e_2) \mid (e_1 \cdot e_2)$;
bool kifejezes $b ::= (e_1 = e_2) \mid (e_1 < e_2) \mid \neg b \mid (e_1 \wedge e_2)$.
Szemantika: $\langle$szintaktikai tartomany$\rangle \to \langle$szemantikai tartomany$\rangle$;

Allapot: Egy T tipusu konstans allapota annak konkret erteke.
Egy T tipusu v valtozo allapota $\sigma(v)$.
A T tipusu lehetseges allapotainak halmazat jelolje: D_T.
A T tipusu v valtozo megfelelo allapota egy lekepezes D_T-re: $\sigma(v) \in D_T$.

Kifejezes jelentese:
Jeloles. Adott D_T mellett a megfelelo allapotok halmazat jelolje Σ.
Definicio: Egy T tipusu s kifejezes jelenetese: $\sigma(s)$: $\Sigma \to D_T$;
Definicio:

1. Ha az e kifejezes egy T tipusu d konstans: $\sigma(e) = d$;
2. Ha az e kifejezes egy T tipusu v egyszeru valtozo: $\sigma(e) = \sigma(v)$;
3. Ha az e kifejezes egy T tipusu muvelet: $e = op(s_1, \cdots, s_n)$, amelyhez az $f(s_1, \cdots, s_n)$ lekepezes tartozik: $\sigma(e) = f(\sigma(s_1), \cdots, \sigma(s_n))$;

4. Ha az e kifejezes egy T tipusu tomb: $e = A[s_1, \cdots, s_n]$, $\sigma(e) = \sigma(A)(\sigma(s_1), \cdots, \sigma(s_n))$;
5. Ha e if α then s_1 else s_2 fi formaju bool kifejezes:
   $\sigma(\alpha) = "true" \rightarrow \sigma(e) = \sigma(s_1)$;
   $\sigma(\alpha) = "false" \rightarrow \sigma(e) = \sigma(s_2)$.

Egy p allitas jelentese: $S(p)$: $\Sigma \rightarrow \{"true", "false"\}$;
A program jelentese: $M[S]$; Denotacios szemantika; Operacios szemantika.

Az allapot-atmenet: $\langle S, \sigma\rangle \rightarrow \langle S', \sigma'\rangle$.
S program, σ kiindulasi allapottal
. S' maradek program, σ' eredmeny allapottal.
$S' = E$: programon beluli ures program.

Determinisztikus program jelentese:
$\langle \text{skip}, \sigma\rangle \rightarrow \langle E, \sigma\rangle$;
$\langle u \leftarrow t, \sigma\rangle \rightarrow \langle E, \sigma[u \leftarrow t]\rangle$;
$\sigma(\alpha) \Rightarrow \langle$ if α then S_1 else S_2 fi, $\sigma\rangle \rightarrow \langle S_1, \sigma\rangle$;
$\sigma(\neg\alpha) \Rightarrow \langle$ if α then S_1 else S_2 fi, $\sigma\rangle \rightarrow \langle S_2, \sigma\rangle$;
$\sigma(\alpha) \Rightarrow \langle$ while α do S od, $\sigma\rangle \rightarrow \langle S$; while α do S od,$\sigma\rangle$;
$\sigma(\neg\alpha) \Rightarrow \langle$ while α do S od, $\sigma\rangle \rightarrow \langle E, \sigma\rangle$;
Az S program allapotainak halmaza: Σ. Egy allapot: $\sigma \in \Sigma$.

Az $\mathbf{S_0}$ program vegrehajtasa:
$\tau : \langle S_0, \sigma_0\rangle \rightarrow \langle S_1, \sigma_1\rangle \rightarrow \cdots \rightarrow \langle S_{n-1}, \sigma_{n-1}\rangle \rightarrow \langle S_n, \sigma_n\rangle$;
$\langle S_i, \sigma_i\rangle \rightarrow \langle S_{i+1}, \sigma_{i+1}\rangle$ atmenethez tartozik egy tranzakcio:
$(S_i, \alpha_i \rightarrow r_i, S_{i+1})$ ugy, hogy $\alpha(\sigma_1) = "true"$ es $\sigma_{i+1} = r_i(\sigma_i)$;
Az S_0 program vegrehajtasa befejezodik σ_n allapotban, ha τ veges,
es az utolso konfiguracio: $\langle E, \sigma_n\rangle$; $\langle S_0, \sigma_0\rangle \rightarrow^* \langle E, \sigma_n\rangle$;
Jeloles: $val(\tau) = \sigma_n$.
A τ vegrehajtas lehet vegtelen (divergens). Virtualis vegrehajtas:
$\langle S, \sigma\rangle \rightarrow^* \langle E, \perp\rangle$;
$val(\tau) = \perp$. $\perp \notin \Sigma$.

$comp(S)(\sigma)$: az S program osszes kiszamitasanak eredmenye, amely σ kezdesi allapotahoz tartozik.
Determinisztikus program eseten $comp(S)(\sigma)$ egyelemu.

Az S program input output szemantikaja: $M[S]$: $\Sigma \rightarrow \Sigma$.
Az S program jelentese adott σ eseten:
- $M[S](\sigma) = \{\sigma' | \sigma' \in comp(S)(\sigma)\}$,
- Ha az S vegrehajtasa sikertelen: $fail \in M[S](\sigma)$.
- Ha az S vegrehajtasa divergens: $\perp \in M[S](\sigma)$.

Az S program parcialis helyessegi szemantikaja:
$M[S] : \Sigma \rightarrow P(\Sigma), M[S](\sigma) : \{\sigma' | \langle S, \sigma\rangle \rightarrow^* \langle E, \sigma'\rangle\}$

Az S program teljes helyessegi szemantikaja:
$M_{tot}[S] : \Sigma \to (P(\Sigma \cup \{\perp\}),$
$M_{tot}[S](\sigma) = M[S](\sigma) \cup \{\perp\}.$
Az S program specifikacioja egy (φ, ψ) kettos, ahol φ a program elofeltetele es ψ az utofeltetele, azaz $\varphi(\sigma) =$ "$true$" es $\forall \sigma' \in M[s](\sigma)$ eseten $\psi(\sigma') =$ "$true$".

Programhelyessegi kerdesek
Parcialis helyesseg: Az S programot a (φ, ψ) specifikacio szerint parcialisan helyesnek mondjuk, ha minden $\sigma \in \Sigma$ kezdo ertekhez tarotozo allapot mellett, amelyre $\varphi(\sigma) =$ "$true$", felteve, hogy a vegrehajtas befejezodik $\sigma' \in \Sigma$ es $\psi(\sigma') =$ "$true$" allapot mellett,
akkor: $[(\varphi(\sigma) = \text{"}true\text{"}) \wedge (\sigma' \in M[S](\sigma)) \Rightarrow \psi(\sigma') = \text{"}true\text{"}.$
Jeloles: $\{\varphi\}$ P $\{\psi\}$.
Eredmenyesseg: $\varphi(\sigma) = (fail \notin M[S](\sigma));$
Befejezodes: $\varphi(\sigma) = (\perp \notin M[S](\sigma));$
Teljes helyesseg: Az S programot a (φ, ψ) specifikacio szerint teljesen helyesnek mondjuk, ha $\forall \sigma \in \Sigma$ kezdo ertekre, ha $\varphi(\sigma) =$ "$true$", a tranzakcio befejezodik es $\sigma' \in \Sigma$ eseten, amelyre $\psi(\sigma') =$ "$true$":
- $\varphi(\sigma) \to (\{\perp, fail\} \cap M[S](\sigma) = \{\});$
- $[(\varphi(\sigma) = \text{"}true\text{"}) \wedge (\sigma' \in M[S](\sigma))] \Rightarrow \psi(\sigma') = \text{"}true\text{"}.$
Jeloles: $\{\{\varphi\}\}$ P $\{\{\psi\}\}$.

Induktiv allitasok (Floyd) modszere programok parcialis helyessegenek a bizonyitasara
Tranzakcio:
Szintaxis:
A tranzakcio egy $(l, \alpha \to r, l')$ harmas. l,l': cimke; α: logikai kifejezes; f: lekepezes;
Szemantika:
l cimketol k' cimkeig az f lekepezes valosul meg, ha $\alpha =$ "$true$".

$$l \xrightarrow{\alpha \to f} l'$$

Tranzakcios diagram: (L, T, s, t) negyes, ahol L az $l \in L$ cimek egy veges halmaza. T a tranzakciok veges halmaza. $s \in L$, egy kituntetett cim, az entry cim. $t \in L$, egy kituntetett cim, az exit cim.
Σ allapotok halmaza; $l, l' \in L$. $\alpha : \Sigma \to bool$. $f : \Sigma \to \Sigma$, ahol egy allapot $\sigma \in \Sigma$.
t cim, amelyre $\neg\exists(l \in L, \alpha \to f \in T)(t, \alpha \to f, l)$.

Q-diagam:
Adva: PT = (L, T, s, t) tranzakcios diagram.
A Q-diagram a PT tranzakcios diagramnak egy olyan allitasokkal kiegeszitett formaja, amelyben egy Q fuggveny minden $l \in L$ cimkehez hozzarendel egy Q_l allitast.

Adva Q diagram a PT tranzakcios diagramhoz. Egy $\pi = (l, \alpha \to r, l')$ tranzakcio verifikacios feltetele:
$V_\pi = Q_l \wedge \alpha \Rightarrow Q_{l'} \circ r.$
A PT tranzakcios diagramhoz tartozo Q diagram osszes verifikacios feltetelenek a halmazat jelolje $V(PT, Q)$.
A PT tranzakcios diagramhoz tartozo Q-diagramrol azt mondjuk, hogy az induktiv, ha

$(\forall V_\pi \in V(PT, Q))(V_\pi = "true")$.
A PT tranzakcios diagramhoz rendelt Q-diagramrol azt mondjuk, hogy az invarians, ha
$(\forall l_i \in PT)(Q_S(\sigma_0) = "true" \Rightarrow Q_{l_i}(\sigma_i) = "true")$.
Az induktiv Q-diagramot az adott (φ, ψ) specifikacio szerint konzisztens-nek mondjuk,
ha $\varphi(\sigma_0) \Rightarrow Q_s(\sigma_0)$ es $Q_t(\sigma_n) \Rightarrow \psi(\sigma_s)$.

Floyd-fele induktiv allitasok modszere programok parcialis helyessegenek bizonyitasara

1. Az adott P programhoz keszitsuk el a PT tranzakcios diagramot.
2. PT tranzakcios diagramhoz keszitsuk el a Q allitasokkal kiegeszitett Q-diagramot.
3. Bizonyitsuk be, hogy a Q-diagram induktiv es invarians.
4. Bizonyitsuk be, hogy a Q-diagram konzisztens a (φ, ψ) speifikacio szerint.

9. eloadas

Kettos specifikacio: Adott $d_a = (A, F, E_a)$; $d_c = (C, G, E_)$; $A_0 = \{a|I_a(a)\}$; $C_0 = \{c|I_c(c)\}$;
abrazolas: $\varphi : C_0 \to A_0$;
$E_a = \{\cdots, f_s(f_c(a)) = h(a), \cdots, I_a(f_c(a)) =$"false"$\Rightarrow f_c(a) =$ "undefined"$\}$;
$E'_a = \{\cdots, \{y = f_c(a)\}\ z = f_s(y)\ \{z = h(a)\}, \cdots, \{I_a(f_c(a))\}\ z = f_c(a)\ \{I_a(z) \wedge z = f_c(a)\}\}$
$E'_a = \{\cdots, \{y = f_c(a) \wedge I_a(a)\}\ z = f_s(y)\ \{z = h(a) \wedge I_a(a)\}, \cdots, \{I_a(f_c(a)) \wedge I_a(a)\}\ z = f_c(a)$ $\{I_a(z) \wedge z = f_c(a) \wedge I_a(a)\}\}$; azaz $E'_a = \{\cdots, \{pre_{f_i}(a)\}a' = f_i(a)\{post_{f_i}(a, a')\}, \cdots\}$;
$a = \varphi(c)$;
$E_c = \{\cdots, g_s(g_c(c)) = h_c(c), \cdots, I_c(g_c(c)) =$"false"$\Rightarrow g_c(c) =$ "undefined"$\}$;
$E_c = \{\cdots, pre_{g_i}(c)\}\ c' = g_i(c)\ \{post_{g_i}(c, c')\}, \cdots\}$;
$E_c = \{\cdots, Q_{g_i}, \cdots\}$;

Ha bebizonyitjuk, hogy
1) $I_c(c) \Rightarrow I_a(\varphi(c))$;
2) $post_{g_0}(c) \Rightarrow I_c(c)$;
3) $post_{g_0}(c) \Rightarrow post_{f_0}(\varphi(c))$;
4) $I_c(c) \wedge pre_{f_i}(\varphi(c)) \Rightarrow pre_{g_i}(c)$;
5) $I_c(c) \wedge pre_{f_i}(\varphi(c)) \wedge post_{g_i}(c, c') \wedge I_c(c') \Rightarrow post_{f_i}(\varphi(c), \varphi(c'))$;
akkor a d_c konkret specifikacio a d_a absztrakt specifikacio szerint helyes.

Ha a kovetkezo tetelek teljesulnek:
1. $(\forall c \in C)(I_c(c) \Rightarrow I_a(\varphi(c))$;
2. $\{$"true"$\}\ Q_0\ \{post_{f_0}(\varphi(c)) \wedge I_c(c)\}$;
3. $(\forall f_i \in F) : \{pre_{f_i}(\varphi(c)) \wedge I_c(c)\}\ Q_i\ post_{f_i}(\varphi(c), \varphi(c')) \wedge I_c(c')\}$;
ahol 2. es 3. teljes helyessegi tetelek, akkor a d_c konkret specifikacio a d_a absztrakt specifikacio szerint helyes.

Adott S determinisztikus program:
Tranzakcios diagram: (L, R, s, t);
$s : u \leftarrow f$; $(\{s, t\}, P(s,$"true"$\to (u \leftarrow f), t)\}, s, t)$;

Adott $\{\varphi\}\ S\{\psi\}$ parcialis helyessegi tetel.
Adott az S program ST = (L, T, s, t) tranzakcios diagramja, es Q diagramja, amelyrol bebozonyitottuk, hogy induktiv.
Ha bebizonyitjuk, hogy a Q-diagram a (φ, ψ) specifikacio szerint konzisztens, azaz
$\varphi \Rightarrow Q_s$; $Q_t \Rightarrow \psi$;
akkor az S program a (φ, ψ) specifikacio szerint parcialisan helyes.
A program befejezodesenek (konvergens tulajdonsaganak) bizonyitasa. φ - konvergencia bizonyitasa.

Alapfogalom: **Jol rendezett halmaz:**
Legyen W egy halomaz es $<: W \times W$ binaris relacio. A $<$ relaciot rendezonek mondjuk, ha tetszoleges $a, b, c \in W$ -re:
- irreflexiv: $a < a =$"false".
- asszimetrikus: $a < b =$"true" $\Rightarrow b < a=$"false".
- tranzitiv: $(a < b =$ "true"$) \wedge (b < c=$"true"$) \Rightarrow a < c=$"true".

A parcialisan rendezett $(W, <)$ halmazt jol rendezettnek nevezzuk, ha nem letezik vegtelen $\cdots < w_2 < w_1 < w_0$, sorozat, $w_i \in W$, eseten.

φ - konvergencia bizonyitasanak Floyd-fele modszere:
Allitas:
Adott a P program PT =(L, R, s, t) tranzakcios diagramja es φ.
1) Keszitsuk el PT alapjan a kovergencia bizonyitasahoz szukseges Q-diagramot.
2) Bizonyitsuk be, hogy Q-diagram induktiv es $\varphi \Rightarrow Q_s$.
3) Valasszunk meg egy (W, <) jol rendezett halmazt es a $\rho = \{\rho_l | l \in L\}$, fuggvenyhalmazt, ahol $p_l : \Sigma \rightarrow W$, minden $l \in L$ eseten.
4) Bizonyitsuk be, hogy ρ_l definialva van: $Q_l(\sigma) \Rightarrow \rho_l \in W$.
5) Mutassuk ki, hogy $(\forall (l, \alpha \rightarrow f, l') \in R)(Q_l(\sigma) \wedge \alpha(\sigma) \Rightarrow \rho_{l'}(f(\sigma)) < \rho_l(\sigma)$.
Ha ezeket bebizonyitottuk, akkor a P program φ-konvergens.
Bizonyitas:
$\nu : \langle s, \sigma_0 \rangle \rightarrow \langle l_1, \sigma_1 \rangle \rightarrow \cdots;$
Q induktivitasabol kovetkezik, hogy Q invarians. Ha $\varphi \Rightarrow Q_s$, akkor
$\rho_s(\sigma_0), \rho_{l_1}(\sigma_1), \cdots$ definialva van es minden $\langle l, \sigma \rangle \rightarrow \langle l', \sigma' \rangle$ tranzakciora $\rho_{l'}(f(\sigma)) < \rho_l(\sigma)$.
Igy W jol-rendezettsegebol kovetkezik, hogy a vegrehajtas veges.

Vegrehajtasi (runtime) hibamentesseg:
Tekintsuk az S programnak azokat a vegrehajtasait:
$\nu : \langle s, \sigma_0 \rangle \rightarrow \langle l_1, \sigma_1 \rangle \rightarrow \cdots$, amelyekre $\varphi(\sigma_0) =$"true".
Ha nincs olyan vegrehajtas, amelynek soran valamely cimkenel a szoba joheto tranzakciok kozott letezik olyan, amely nincsen definialva, akkor azt mondjuk, hogy az S program a φ input specifikacio mellett mentes a vegrehajtasi hibatol.

Vegrehajtasi hibamentesseg bizonyitasa:
Adott a P program PT=(L, R, s, t) tranzakcios diagramja es φ.
Keszitsuk el annak Q-diagramjat. Ha minden $l \in L$ eseten az osszes $(l, \alpha \rightarrow f, l')$ tranzakcional $Q_l(\sigma) \wedge (\alpha(\sigma) \Rightarrow pre_f(\sigma)$, akkor a P program mentes a vegrehajtasi hibatol.

P program tejes-helyessegenek bizonyitasa:
Adott a P program es annak (φ, ψ) specifikacioja.
- Konstrualjuk meg a P programhoz a vele szemantikailag ekvivalens PT diagramot.
- Keszitsuk el a Q diagramot.
- Bizonyitsuk be, hogy a P program parcialisan helyes az adott specifikacio szerint.
- Bizonyitsuk be, hogy a P program kovergens.
- Bizonyitsuk be, hogy a P program mentes a vegrehajtasi hibatol.
Akkor a P program a (φ, ψ) specifikacio szerint teljesen helyes.

10. eloadas

Realizacio:
r : INT $\rightarrow$ MOD;
$r = (r_P, r_E, r_I)$;
Kettos specifikacio:
$E_c = \{\cdots, g_s(g_c(c)) = h_c(c), \cdots, I_c(g_c(c)) =$"false" $\Rightarrow g_c(c) =$"undefined"$\}$;
$E_c = \{\cdots, Q_{g_i}, \cdots\}$;

Program helyesseg: $\{\varphi\}S\{\psi\}$

Program vegrehajtasa:
$\langle S, \sigma\rangle \rightarrow \langle S_1, \sigma_1\rangle \rightarrow \cdots \rightarrow \langle S_{n-1}, \sigma_{n-1}\rangle \rightarrow \langle S_n, \sigma_n\rangle$;
$\langle s, \sigma\rangle \rightarrow \langle l_1, \sigma_1\rangle \rightarrow \cdots \rightarrow \langle l_{n-1}, \sigma_{n-1}\rangle \rightarrow \langle l_n, \sigma_n\rangle$;

Determinisztikus programok helyessegenek bizonyitasa Hoare modszerrel:
Hoare fele harmas: $\{p\}S\{q\}$.
Definicio: A $\{p\}S\{q\}$ formulat parcialis helyessegi ertelemben, helyesnek mondjuk, ha $M[S]([\{p\}]) \subset \{q\}$.
Jeloles: $\{p\}S\{q\}$="true".
Definicio: A $\{\{p\}\}S\{\{q\}\}$ formulat teljes helyessegi ertelemben, helyesnek mondjuk, ha $M_{tot}[S]([\{p\}]) \subset \{q\}$.
Jeloles: $\{\{p\}\}S\{\{q\}\}$="true".

Hoare fele bizonyitasi rendszer (BR): axiomak + kovetkeztetesi szabalyok.
Dedukcio: axioma + kovetkeztetesi szabalyok $\Rightarrow$ tetel.
BD: Determinisztikus programok bizonyitasi rendszere.

Determinisztikus program:
S ::= skip | $u \leftarrow t$ | $S_1; S_2$ | if α then S_1 else S_2 fi | while α do S od
Axiomak:
$\{P(x,y)\}$ skip $\{P(x,y)\}$
$\{P(x, g(x,y))\} y \leftarrow g(x,y)\ \{P(x,y)\}$
Kovetkeztetesi szabalyok:
- Szekvencia:

$$\frac{\{P\}S_1\{Q_1\} \text{ es } \{Q_1\}S_2\{Q\}}{\{P\}S_1; S_2\{Q\}}$$

- Felteteles elagazas:

$$\frac{\{P \wedge \alpha\}S_1\{Q\} \text{ es } \{P \wedge \neg\alpha\}S_2\{Q\}}{\{P\} \text{ if } \alpha \text{ then } S_1 \text{ else } S_2 \text{ fi } \{Q\}}$$

- Iteracio:

$$\frac{\{P \wedge \alpha\}S\{P\} \text{ es } P \wedge \neg\alpha \Rightarrow Q}{\{P\} \text{ while } \alpha \text{ do } S \text{ od } \{Q\}}$$

A kovetkezmeny szabalya:

$$\frac{P \Rightarrow P_1 \text{ es } \{P_1\}S\{Q_1\} \text{ es } Q_1 \Rightarrow Q}{\{P\}S\{Q\}}$$

Ertekadas kovetkeztetesi szabalya:

$$\frac{P(x, f(x,y)) \Rightarrow Q(x,y)}{\{P(x,y)\}y \leftarrow f(x,y)\{Q(x,y)\}}$$

Iteracio kovetkeztetesi szabalyanak altalanos formaja:

$$\frac{P \Rightarrow I \text{ es } \{I \wedge \alpha\}S\{I\} \text{ es } I \wedge \neg\alpha \Rightarrow Q}{\{P\} \text{ while } \alpha \text{ do } S \text{ od } \{Q\}}$$

A felsorolt axiomak es kovetkeztetesi szabalyok alkotjak a determinisztikus programok parcialis helyessegenek bizonyitasara szolgalo bizonyitasi rendszert.
Jeloles: PD.

A teljes helyesseg bizonyitasanak kovetkeztetesi szabalya:

$$\frac{\begin{array}{c} P(x,y) \Rightarrow I(x,y) \text{ es } I(x,y) \Rightarrow E(x,y) \in W_< \text{ es} \\ \{\{I(x,y) \wedge \alpha(x,y) \wedge E = E(x,y)\}\}S\{\{I(x,y) \wedge E < E(x,y)\}\} \text{ es} \\ I(x,y) \wedge \neg\alpha(x,y) \Rightarrow Q(x,y) \end{array}}{\{\{P(x,y)\} \text{ while } \alpha(x,y) \text{ do } S \text{ od } \{\{Q(x,y)\}\}}$$

Az iteracio kovetkeztetesi szabalya a ciklusszamlaloval:

$$\frac{\begin{array}{c} P(x,y) \Rightarrow I(x,y,0) \text{ es } I(x,y,i) \Rightarrow i < k(x) \text{ es } \{\{I(x,y,i) \wedge \alpha(x,y)\}\}S\{\{I(x,y,i+1)\}\} \text{ es} \\ I(x,y,i) \wedge \neg\alpha(x,y) \Rightarrow Q(x,y) \end{array}}{\{\{P(x,y)\} \text{ while } \alpha(x,y) \text{ do } S \text{ od } \{\{Q(x,y)\}\}}$$

A felsorolt axiomak es kovetkeztetesi szabalyok alkotjak a determinisztikus programok teljes helyessegenek bizonyitasara szolgalo bizonyitasi rendszert.
Jeloles: TD.

Adott a bizonyitasi rendszer: BR.
Jeloles: $\{P\}S\{Q\}/BR_{seq}$="true" amelynek jelentese, hogy a $\{P\}S\{Q\}$ formula parcialis helyessegi ertelemben, levezetheto, bizonyithato a BR rendszerben.

Adott a bizonyitasi rendszer: BR.
Jeloles: $\{\{P\}\}S\{\{Q\}\}/BR_{seq}$="true", amelynek jelentese, hogy a $\{\{P\}\}S\{\{Q\}\}$ formula teljes helyessegi ertelemben, levezetheto, bizonyithato a BR rendszerben.

Definicio: Adott a BR bizonyitasi rendszer, es a programoknak egy C osztalya.
A BR bizonyitasi rendszert megbizhatonak mondjuk a C osztaly programjainak parcialis helyessegere

vonatkozoan, ha minden $S \in C$ programra vonatkozo $\{P\}S\{Q\}$ formulara
$\{P\}S\{Q\}/BR_{seq}$="true" $\Rightarrow$ $\{P\}S\{Q\}$="true".
A BR bizonyitasi rendszert megbizhatonak mondjuk a C osztaly programjainak teljes helyessegere vonatkozoan, ha minden $S \in C$ programra vonatkozo $\{\{P\}\}S\{\{Q\}\}$ formulara
$\{\{P\}\}S\{\{Q\}\}/BR_{seq}$="true" $\Rightarrow$ $\{\{P\}\}S\{\{Q\}\}$="true".

Definicio: Adott a kovetkezo formaju bizonyitasi szabaly:

$$\frac{\varphi_1, \cdots, \varphi_k}{\varphi_{k+1}}$$

A bizonyitasi szabalyt megbizhatonak nevezzuk parcialis (totalis) helyessegi ertelemben az adott C osztalyban, ha
φ_1="true" $\wedge \cdots \wedge$ φ_k="true" $\Rightarrow$ φ_{k+1}="true" parcialis ill. totalis helyessegi ertelemben.

Tetel: A PD bizonyitasi rendszer determinisztikus programok parcialis helyessegenek a bizonyitasara megbizhato.
Tetel: A TD bizonyitasi rendszer determinisztikus programok teljes helyessegenek a bizonyitasara megbizhato.

Definicio: Adott a BR bizonyitasi rendszer, es a programoknak egy C osztalya.
A BR bizonyitasi rendszert teljesnek mondjuk a C osztaly programjainak parcialis helyessegere vonatkozoan, ha minden $S \in C$ programra vonatkozo helyessegi $\{P\}S\{Q\}$ formulara
$\{P\}S\{Q\}$="true" $\Rightarrow$ $\{P\}S\{Q\}/BR_{seq}$= "true".
A BR bizonyitasi rendszert teljesnek mondjuk a C osztaly programjainak teljes helyessegere vonatkozoan, ha minden $S \in C$ programra vonatkozo helyessegi $\{\{P\}\}S\{\{Q\}\}$ formulara
$\{\{P\}\}S\{\{Q\}\}$="true" $\Rightarrow$ $\{\{P\}\}S\{\{Q\}\}/BR_{seq}$="true".

Tetel: A PD bizonyitasi rendszer determinisztikus programok parcialis helyessegenek bizonyitasara teljes.
Tetel: A TD bizonyitasi rendszer determinisztikus programok teljes helyessegenek bizonyitasara teljes. (Az iteraciok szamara tett bizonyos megszoritasok eseten.)

A nem teljesseg okai lehetnek:

1. A bizonyitasi rendszer nem teljes az allitasok kovetkezmenyeinek meghatarozasanal. (Godel Incompleteness Theorem)

2. Az allitasok leirasara hasznalt nyelv nem eleg teljes a helyessegi bizonyitas soran az allapotok es korlatozo fuggvenyek leirasara. (Megjavitom, de mindig lehet talalni olyan allitast, amit nem tudok bizonyitani.)

3. A bizonyitasi szabalyok az adott C osztalyra nezve nem teljesek.

Definicio: Egy P determinsiztikus program es p,q predikatum eseten $\{p\}P\{q\}$ helyessegi formulat igaznak mondjuk, ha $\{p\}PT\{q\}$ igaz.
Definicio: Adott egy S determinisztikus program, amelynek programfuggvenye $f_s(x, y), p(x, y), q(x, y)$ predikatum eseten a $\{p(x, y)\}S\{q(x, y)\}$ helyessegi formulat igaznak mondjuk,

ha $P(x, f_s(x,y)) \Rightarrow q(x,y)$.

Annotalt program:
div*:
quo $\leftarrow$ 0; rem $\leftarrow x$;
$\{I\}$ while rem$\geq y$ do rem $\leftarrow$rem$-y$; quo$\leftarrow$ quo+1 od;

Teljes helyesseg bizonyitasas:
E: rem;
I': $I \wedge y > 0$;
$\{x \geq 0 \wedge y \geq 0\}$ quo=0; rem=x $\{I'\}$;
$\{I' \wedge$ rem$\geq y\}$ rem$\leftarrow$ rem$-y$; quo $\leftarrow$quo+1$\{I'\}$;

$\{I' \wedge$ rem$\geq y \wedge$ rem$= z\}$
rem $\leftarrow$ rem$-y$; quo$\leftarrow$ quo+1
$\{$rem$< z\}$;

$I' \Rightarrow$ rem≥ 0;

11. eloadas

Az iteraciorol: while α do S od;
Ures iteracio: while "true" do skip od;
$k = 0 \Rightarrow$ (while α do S od)^k = while "true" do skip od;
$k \geq 0 \Rightarrow$ (while α do S od)$^{k+1}$= if α the S; (while α do S od)^k else skip fi;

A szemantikarol: $M[S](H)$; H = allapotok halmaza.
- Monoton: $H_1 \subset H_2 \Rightarrow M[S](H_1) \subset M[S](H_2)$;
- $M[S_1; S_2](H) = M[S_1](M[S_1](H))$;
- M[begin $S_1; S_2$ end; $S_3](H) = M[S_1$; begin $S_2; S_3$ end$](H)$;
- M[if α then S_1 else S_2 fi]$(H) = M[S_1](H \cap \{\alpha\}) \cup M[S_2](H \cap \{\neg\alpha\})$;
- M[while α do S od] $= \bigcup_{k=0}^{\infty}$(while α do S od)^k;

Bizonyitas:
- Mutassuk meg, hogy minden axioma a PD ill. TD rendszerben igaz, azaz megbizhatoak.
- Mutassuk meg, hogy minden kovetkeztetesi szabaly a PD ill. TD rendszerben igaz, azaz megbizhatoak.
- A fentiakbol ezekutan teljes indukcioval kovetkeznek az allitasaink.

Mit jelent az, hogy egy axioma igaz?
Definicio:
Axioma: $\{\sigma | p(\sigma)\}\langle S, \sigma\rangle \to \langle E, \tau\rangle\{\tau | q(\tau)\}$;
$\{p(\sigma)\}\langle S, \sigma\rangle \to \langle E, \tau\rangle\{q(\tau)]; \{p\}\langle s, \sigma\rangle \to \langle E, \tau\rangle\{q\}$;
Ha $M[S](\{p\}) \subset \{q\}$, akkor az axioma igaz.

S =skip; $\langle$skip,$\sigma\rangle \to \langle E, \sigma\rangle$;
Axioma: $\{p\}$ skip $\{p\}$;
M[skip]$(\{p\}) = \{p\} \Rightarrow \{p\}S\{p\}$ ="true";

$S = y \leftarrow f(x, y); \langle y \leftarrow f(x, y), \sigma\rangle \to \langle E, \tau\rangle; \tau = \sigma[y \leftarrow f(x, y)]$;
$M[y \leftarrow f(x, y)](\sigma) = \{\tau\}$;
$M[y \leftarrow f(x, y)](\sigma) = \{\sigma[y \leftarrow f(x, y)]\}$;
Axioma: $\{p(x, f(x, y))\}y \leftarrow f(x, y)\{p(x, y)\}$;
$(\forall\sigma \in \{p\})(\sigma[y \leftarrow f(x, y)] \in \{p\})$
$M[y \leftarrow f(x, y)](\{p\}) \subset \{p\} \Rightarrow \{p\}S\{p\}$ = "true";

Mit jelent az, hogy a $\varphi_1, \cdots, \varphi_k \Longrightarrow \varphi_{k+1}$ kovetkeztetesi szabaly igaz?
Definicio: Ha $((\varphi_l =$ "true"$) \wedge \cdots \wedge (\varphi_k =$"true"$)) \Rightarrow (\varphi_{k+1} =$"true"), akkor a kovetkeztetesi szabaly igaz, azaz megbizhato.

$S : S_1; S_2$;
Felteves:
- $M[S_1](\{p\}) \subset \{r\}$;
- $M[S_2](\{r\}) \subset \{q\}$;

$M[S_2](M[S_1](\{p\}) \subset M[S_2](\{r\}) \subset \{q\} \Rightarrow M[S_1; S_2](\{p\}) \subset \{q\} \Rightarrow$
$\Rightarrow \{p\}S_1, S_2\{q\}$ ="true"$\equiv \{p\}S\{q\}$="true";

A

$$\frac{\{p\}S_1\{r\},\{r\}S_2\{q\}}{\{p\}S_1;S_2\{q\}}$$

kompozicio szabalya tehat parcialis helyessegi ertelemben megbizhato.

S : if α then S_1 else S_2 fi;
Felteves:
- $M[S_1](\{p \wedge \alpha\}) \subset \{q\}$;
- $M[S_2](\{p \wedge \neg\alpha\}) \subset \{q\}$;

M[if α S_1 else S_2 fi]$(\{p\})$=
$((M[S_1](\{p\wedge\alpha\})\cup(M[S_2](\{p\wedge \not\alpha\}) \subset \{q\}) \Rightarrow \{p\}$ if α then S_1 else S_s fi $\{q\}$="true" $\equiv \{p\}S\{q\}$="true";
A felteteles elagazas:

$$\frac{\{p \wedge \alpha\}S_1\{q\},\{p \wedge \neg\alpha\}S_2\{q\}}{\{p\} \text{ if } \alpha \text{ then } S_1 \text{ else } S_2 \text{ fi } \{q\}}$$

kovetkeztetesi szabalya parcialis helyessegi ertelemben megbizhato.

$S =$ while α do S_1 od;
Felteves: $M[S_1](\{p \wedge \alpha\}) \subset \{p\}$;
$(\forall k, k \geq 0)(M[(\text{while } \alpha \text{ do } S_1 \text{ od})^k](\{p\}) \subset \{p \wedge\ \alpha\})$;
$k = 0$;
Felteves $k \geq 0$ eseten igaz, bizonyitsuk
$M[(\text{while } \alpha \text{ do } S_1 \text{ od})^{k+1}](\{p\}) \subset \{p \wedge \neg\alpha\}$;
$M[(\text{while } \alpha \text{ do } S_1 \text{ od})^{k+1}](\{p\}) = M[\text{if } \alpha \text{ then } S_1;\ (\text{while } \alpha \text{ do } S_1 \text{ od})^k \text{ else skip fi}](\{p\})$=
$M[S_1;\ (\text{while } \alpha \text{ do } S_2 \text{ od})^k](\{p \wedge \alpha\}) \cup M[skip](\{p \wedge \neg\alpha\})$=
$M[(\text{while } \alpha \text{ do } S_1 \text{ od})^k](M[S_1](\{p \wedge \alpha\}) \cup \{p \wedge \neg\alpha\{\subset M[(\text{while } \alpha \text{ do } S_1 \text{ od})^k](\{p\}) \cup \{p \wedge \neg\alpha\}) \subset \{p \wedge \neg\alpha\}$.
$\bigcup_{k=0}^{\infty} M[(\text{while } \alpha \text{ do } S_1 \text{ od})^k](\{p\}) \subset \{p \wedge \neg\alpha\}$.
$M[\text{while } \alpha \text{ do } S_1 \text{ od}](\{p\}) = \bigcup_{k=0}^{\infty} M[(\text{while } \alpha \text{ do } S_1 \text{ od})^k](\{p\}) \subset \{p \wedge \neg\alpha\}$.
$M[\text{while } \alpha \text{ do } S_1 \text{ od}](\{p\}) \subset \{p \wedge \neg\alpha\} \Rightarrow \{p\}$ while α do S_1 od $\{p \wedge \neg\alpha\} \equiv \{p\}S\{p \wedge \neg\alpha\}$="true".
Az iteracio

$$\frac{\{p \wedge \alpha\}S_1\{p\}}{\{p\} \text{ while } \alpha \text{ do } S_1 \text{ od } \{p \wedge \neg\alpha\}}$$

kovetkeztetesi szabalya parcialis helyessegi ertelemben helyes.

Kovetkezmeny szabalya:
Felteves:
$p \Rightarrow p_1, M[S](\{p_1\}) \subset \{q_1\}; q_1 \Rightarrow q$;
$\{\sigma | p(\sigma)\} \subset \{\sigma | p_1(\sigma)\}$; azaz $\{p\} \subset \{p_1\}$;
$\{\sigma | q_1(\sigma)\} \subset \{\sigma | q(\sigma)\}$; azaz $\{q_1\} \subset \{q\}$;
$M[S](\{p\}) \subset M[S](\{p_1\}) \subset \{q_1\} \subset \{q\}$;

Teljes helyesseg:
S =while α do S_1 od;

Felteves:
- $M_{tot}[S](\{p \wedge \alpha\}) \subset \{p\}$;
- $M_{tot}[S](\{p \wedge \alpha \wedge t = z\}) \subset \{t < z\}$;
- $p \Rightarrow t \geq 0$;
- z integer valtozo es nem fordul elo p, α, t, S formulakban;
Allitas: $\perp \notin M_{tot}[S](\{p\})$.

Adott:
- $S(x, y)$: while $\alpha(x, y)$ do $A(x, y)$ od, iteracio, a $f_s(x, y)$ =if $\neg\alpha(x, y)$ then y else $f_s(x, f_s(x, y))$ fi programfuggvenyel, $\alpha(x, y)$ kvantorfuggetlen logikai kifejezes
- $\{P(x, y)\}S(x, y)\{R(x, y)\}$;
- $I(x, y, i)$: ciklus invarians,
- $k(x)$: a ciklusszamlalo felso korlatja,
- $f_A(x, y)$: a ciklusmag programfuggvenye.

Ha bebizonyitjuk, hogy:
- $P(x, y) \Rightarrow I(x, y, 0)$,
- $I(x, y, i) \Rightarrow i \leq k(x)$,
- $I(x, y, i) \wedge \alpha(x, y) \Rightarrow I(x, f(x, y), i + 1)$,
- $I(x, y, i) \wedge \neg\alpha(x, y) \Rightarrow R(x, y)$,

akkor minden olyan y_0-ra, amelyre $P(x, y_0)$="true", $\exists f_s(x, x_0)$ es $R(x, f_s(x, y_0))$= "true".
Bizonyitas: A bizonyitas $k(x)$ szerinti teljes indukcioval:
Alapeset: $k(x) = 0$
$k(x) = 0 \Rightarrow \alpha(x, y_0)$="false"
Tegyuk fel ugyanis: $\alpha(x, y_0)$="true", akkor $I(x, f_A(x, y_0), 1)$="true", es $1 \leq k(x)$, ami ellentmondas.
Igy $I(x, y_0, 0) \wedge \neg\alpha(x, y_0) \Rightarrow R(x, y_0)$, amde most $f_s(x, y_0) = y_0$.
Indukcio: $k(x) > 0$ es felteves $k'(x) \leq k(x) - 1$-re az allitas igaz.
- $\alpha(x, y_0)$="false". Ekkor ugyanugy, mint fent belathato, hogy igaz az allitas.
- $\alpha(x, y_0)$="true". Ekkor $I(x, f_A(x, y_0), 1)$="true".

Legyen tehat $\quad y_1 = f_A(x, y_0)$,
$I_1(x, y_1, i) = I(x, f_A(x, y_0), i + 1)$.
Ekkor az uj ciklusszamlalo korlatja: $I_1(x, y_1, i) \Rightarrow i \leq k(x) - 1$.
y_1-re tehat letezik $f_s(x, y_1)$, es erre $R(x, f_s(x, y_1))$="true", azaz
$R(x, f_s(x, f_A(x, y_0))$="true"$=f_s(x, y_0)$.
Ezzel az iteracio kovetkeztetesi szabalyanak helyesseget bebizonyitottuk.

12. eloadas

Adott BR bizonyitasi rendszer es BR_{sec} a bizonyitasi rendszerben levezetheto formulak halmaza.
- A BR bizonyitasi rendszer megbizhato, ha $(\forall\varphi : \varphi \in BR_{sec}) \Rightarrow \varphi =$"true".
- A BR bizonyitasi rendszer teljes, ha $(\forall\varphi : \varphi \in BR \wedge \varphi =$"true"$) \Rightarrow \varphi \in BR_{sec}$.

A Hoare modszer teljessegi tetele:
Adva $S(x, y)$ strukturalt program, $S(x, y)$ tetszoleges reszprogramja: $s(x, y)$. Felteves:
$\{Q(x) \wedge y = I_S(x)\}s(x, y)\{Q(x) \wedge y = O_S(x)\} =$"true", ahol $f_s(x, I_S(x)) = O_S(x)$.
Allitas: Minden ilyen tulajdonsagu $s(x, y)$ resz - programra vonatkozo fenti tetel a Hoare-modszer segitsegevel levezetheto.
Megjegyzes: Nyilvan:
$\{Q(x) \wedge y = x\}S(x, y)\{Q(x) \wedge y = O_s(x)\} =$"true",
azaz $P(x) : Q(x) \wedge y = x; R(x, y) : Q(x) \wedge y = O_s(x)$;
$\{P(x)\}S(x, y)\{R(x, y)\} =$"true".
Bizonyitas: (parcialis helyesseg) Az alapstrukturak egymasba skatulyazasanak szama szerinti teljes indukcioval.
Alapeset: $s(x, y) = y \leftarrow g(x, y)$
A tetel: $\{Q(x) \wedge y = I_s(x)\}y \leftarrow g(x, y)\{Q(x) \wedge y = O_s(x)\}=$ "true",

$$\frac{Q(x) \wedge y = I_s(x) \Rightarrow Q(x) \wedge g(x, y) = O_s(x)}{\{Q(x) \wedge y = I_s(x)\}y \leftarrow g(x, y)\{Q(x) \wedge y = O_s(x)\}}$$

Indukcio: Tegyuk fel, hogy "k" melysegu egymasva skatulyazas eseten a tetel igaz es bizonyitsuk "k+1"-re is.
Harom eset:
- a k+1. struktura egy szekvencia;
- a k+1. struktura egy felteteles elagazas;
- a k+1. struktura egy iteracio.

1. A k+1. struktura egy szekvencia: $s(x, y) = s_1(x, y); s_2(x, y)$;
   A program fuggvenyek: $f_{s_1}(x, y), f_{s_2}(x, y)$.
   Indukcios feltevesunk:
   - $\{Q(x) \wedge y = I_{s_1}(x)\}s_1(x, y)\{Q(x) \wedge y = O_{s_1}(x)\}$,
   - $\{Q(x) \wedge y = I_{s_2}(x)\}s_2(x, y)\{Q(x) \wedge y = O_{s_2}(x)\}$,

   tetelek helyessege Hoare modszerrel bebizonyithatoak, azaz
   $O_{s_1}(x) = f_{s_1}(x, I_{s_1}(x))$, es $O_{s_2}(x) = f_{s_2}(x, I_{s_2}(x))$.
   A szekvencia szemantikaja alapjan:
   $I_s(x) = I_{s_1}(x)$, es $O_{s_1}(x) = I_{s_2}(x) es O_{s_2}(x) = O_s(x)$;
   ezert $f_s(x, I_s(x)) = f_{s_2}(x, f_{s_1}(x, I_{s_1}(x)))$.

$$\frac{\begin{array}{c}\{Q(x) \wedge y = I_{s_1}(x)\}S_1(x, y)\{Q(x) \wedge y = O_{s_1}(x)\}\\ \{Q(x) \wedge y = I_{s_2}(x)\}S_2(x, y)\{Q(x) \wedge y = O_{s_2}(x)\}\end{array}}{\{Q(x) \wedge y = I_s(x)\}S_1(x, y); S_2(x, y)\{Q(x) \wedge y = O_s(x)\}}$$

2. a k+1. struktura egy felteteles elagazas:
   $s(x, y)$= if $\alpha(x, y)$ then $S_1(x, y)$ else $S_2(x, y)$ fi
   Indukcios feltevesunk szerint:
   $\{Q(x) \wedge y = I_{s_1}(x)\}S_1(x, y)\{Q(x) \wedge y = O_{s_1}(x)\}$,
   $\{Q(x) \wedge y = I_{s_2}(x)\}S_2(x, y)\{Q(x) \wedge y = O_{s_2}(x)\}$,
   tetelek helyessege Hoare modszerrel bebizonyithatok.
   $(Q(x) \wedge y = I_s(x, y) \wedge \alpha(x, y)) \Rightarrow (Q(x) \wedge y = I_{s_1}(x, y))$,
   $(Q(x) \wedge y = I_s(x, y) \wedge \neg\alpha(x, y)) \Rightarrow (Q(x) \wedge y = I_{s_2}(x, y))$,
   masreszt
   $(Q(x) \wedge y = I_s(x, y) \wedge \alpha(x, y)) \Rightarrow O_s(x) = O_{s_1}(x)$,
   $(Q(x) \wedge y = I_s(x, y) \wedge \neg\alpha(x, y)) \Rightarrow O_s(x) = O_{s_2}(x)$,
   $Q(x) \wedge y = I_s(x, y) \wedge \alpha(x, y)) \Rightarrow (Q(x) \wedge y = I_{s_1}(x, y))$,
   $(Q(x) \wedge y = I_s(x, y) \wedge \neg\alpha(x, y)) \Rightarrow (Q(x) \wedge y = I_{s_2}(x, y))$,
   $\{Q(x) \wedge y = I_{s_1}(x))\}S_1(x, y)\{Q(x) \wedge y = O_{s_1}(x)\}$,
   $\{Q(x) \wedge y = I_{s_2}(x))\}S_2(x, y)\{Q(x) \wedge y = O_{s_2}(x)\}$,
   $(Q(x) \wedge y = O_{s_1}(x)) \Rightarrow y = O_s(x)$,
   $(Q(x) \wedge y = O_{s_2}(x)) \Rightarrow y = O_s(x)$,
   $\{Q(x) \wedge y = I_s(x)\}$ if $\alpha(x, y))$ then $S_1(x, y)$ else $S_2(x, y)$ fi $\{Q(x) \wedge y = O_s(x)\}$.

3. k+1. struktura egy iteracio:
   $s(x, y)$ = while $\alpha(x, y)$ do $A(x, y)$ od.
   $\{Q(x) \wedge y = I_A(x)\}A(x, y)\{Q(x) \wedge y = O_A(x)\}$ mar bizonyithato a Hoare modszerrel.
   Legyen $A(x, y)$ programfuggvenye: $f_A(x, y)$.
   A tetel, amely bizonyithato: $\{Q(x) \wedge y = I_A(x)\}y \leftarrow f_A(x, y)\{Q(x) \wedge y = O_A(x)\}$.
   Jeloles:
   $k = 0 \Rightarrow h(x, y, k) = y$
   $k > 0 \Rightarrow h(x, y, k) = \underbrace{f_A}_{1}(x, \underbrace{f_A}_{2}(x, \cdots \underbrace{(f_A(x, y))}_{k}));$
   Az iteracio szemantikajat leiro invarians: $I(x, y, k) : Q(x) \wedge y = h(x, I_A(x), k) \wedge f_s(x, y) = f_s(x, I_s(x))$.
   A bizonyitando tetelek:

   - $(Q(x) \wedge y = I_s(x)) \Rightarrow I(x, y, 0)$;
   - $\{I(x, y, k) \wedge \alpha(x, y)\}A(x, y)\{I(x, y, k + 1)\}$;
   - $(I(x, y, k) \wedge \neg\alpha(x, y)) \Rightarrow (Q(x) \wedge y = O_s(x))$.

   (a) 1. tetel: $(Q(x) \wedge y = I_s(x)) \Rightarrow I(x, y, 0)$,
   $(Q(x) \wedge y = I_s(x)) \Rightarrow (Q(x) \wedge y = I_A(x) \wedge f_s(x, y) = f_s(x, I_s(x)))$, ami trivialis.

   (b) 2. tetel. $\{I(x, y, k) \wedge \alpha(x, y)\}A(x, y)\{I(x, y, k + 1)\}$, az ertekadas kovetkeztetesi szabalya alapjan:
   $I(x, y, k) \wedge \alpha(x, y)) \Rightarrow I(x, f_A(x, y), k + 1)$,
   $(Q(x) \wedge y = h(x, I_A(x), k) \wedge f_s(x, y) = f_s(x, I_s(x)) \wedge \alpha(x, y)) \Rightarrow$
   $(Q(x) \wedge f_A(x, y) = h(x, I_A(x), k + 1) \wedge f_s(x, f_A(x, y)) = f_s(x, I_s(X))$.

   (c) 3. tetel. $(I(x, y, k) \wedge \neg\alpha(x, y)) \Rightarrow (Q(x) \wedge y = O_s(X))$, azaz
   $(Q(x) \wedge y = h(x, I_A(x), k) \wedge f_s(x, y) = f_s(x, I_S(x)) \wedge \neg\alpha(x, y)) \Rightarrow (Q(x) \wedge y = O_S(x))$.

Mivel $\neg\alpha(x,y)$ eseten $f_s(x,y) = y$, masreszt a definicio alapjan $f_s(x, I_s(x)) = O_s(x)$.

$$Q(x) \wedge y = I_s(x) \Rightarrow I(x,y,0)$$

$$\frac{\{I(x,y,k) \wedge \alpha(x,y)\}A(x,y)\{I(x,y,k+1)\} \quad I(x,y,k) \wedge \neg\alpha(x,y) \Rightarrow Q(x) \wedge y = O_s(x)}{\{Q(x) \wedge y = I_s(x)\} \text{ while } \alpha(x,y) \text{ do } A(x,y) \text{ od } \{Q(x) \wedge y = O_s(x)\}}$$

Adva $d_s = (A, F, E_a)$ absztrakt specifikacio, $d_c = (C, G, E_c)$ konkret specifikacio.
$A = \{A_0, A_1, \cdots, A_n\}$; $F = \{f_0, f_1, \cdots, f_m\}$;
$C = \{C_0, C_1, \cdots, C_n\}$; $G = \{g_0, g_1, \cdots, g_m\}$;
$E_a = \{\cdots, e_{a_i}(\cdots, f_j(a), \cdots; a), \cdots\}$;
$E_c = \{\cdots, e_{c_i}(\cdots, g_j(c), \cdots; c), \cdots\}$;
A reprezentacios fuggveny:
$\varphi : C \to a = A,\ f_0 = \varphi(g_0), (\forall f_c \in F_c)(\forall c \in C)((f_c(\varphi(c)) = \varphi(g_c(c))$.
Altalanos formaban az azonos jelentes:
$e_{a_i}(\cdots, f_j(\varphi(c)), \cdots; \varphi(c)) = e_{c_i}(\cdots, g_j(c), \cdots; c)$.
A helyesseg definiciojat szimulacio alapjan definialtuk:
$(\forall f_s \in F_s)(\forall c \in C)(f_s(\varphi(c)) = \varphi(g_s(c)))$.
Az azonos jelentes:

- Algebrai - algebrai" eset:
  $f_s(f_c(\varphi(c)) = f_c(f_s(\varphi(c))) \equiv g_s(g_c(c)) = g_c(g_s(c))$.
- "Kulso felulet - kulso felulet" eset:
  $(pre_{f_i}(\varphi(c)) \wedge postf_i(\varphi(c), \varphi(c'))) \equiv (pre_{g_i}(c) \wedge post_{g_i}(c, c'))$.