PROGRAMAZIOAREN METODOLOGIA
Azterketa Partziala – 3. gaia – Egiaztapena
2013ko martxoaren 11

ARIKETA (Egiaztapena) – (2 puntu)

Honako programa hau guztiz zuzena al den egiaztatu Hoare-ren kalkulua erabiliz. Espezifikazioaren arabera programak, sarrerako datu bezala zenbaki osoz osatutako A(1..n) eta B(1..n) bektoreak emanda eta A(1..n) bektorean balio negatiborik ez dagoela jakinda, B(1..n) bektoreko osagai bakoitza posizio bereko A(1..n) bektoreko elementuaren erro karratuaren azpitik egindako hurbilketa osoa al den erabaki behar du *q* aldagai boolearrean.

$\{\varphi\} \equiv \{n \geq 1 \wedge q \wedge ezneg(A(1..n))\}$
i : = 1;
while {INB} {E} $i \neq n + 1$ **and** q **loop**
    q : = (ekaho(A(i)) = B(i));
    i : = i + 1;
end loop;
$\{\psi\} \equiv \{q \leftrightarrow denakerro(A(1..n), B(1..n), n)\}$

$\{INB\} \equiv \{ezneg(A(1..n)) \wedge (1 \leq i \leq n + 1) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), i - 1))\}$
$E = n + 1 - i$
$ezneg(H(1..r)) \equiv \forall k(1 \leq k \leq r \rightarrow H(k) \geq 0)$
$denakerro(F(1..r), G(1..r), pos) \equiv \forall k(1 \leq k \leq pos \rightarrow ekaho(F(k)) = G(k))$

Hor **ekaho** funtzioa, negatiboa ez den zenbaki oso bat emanda, zenbaki horren **e**rro **k**arratuaren **a**zpitik egindako **h**urbilketa **o**soa kalkulatzen duen funtzioa da (Adibideak: ekaho(9) = 3, ekaho(10) = 3, ekaho(8) = 2).

Egiaztapena egiterakoan, **ekaho** funtzioa inplementatuta dagoela suposatu behar da eta erabiltzeaz bakarrik arduratu beharko dugu, mod, div, eta antzeko beste funtzioekin egiten dugun bezala. Gainera, negatiboa den argumentu bat emanez gero, **ekaho** funtzioak errorea sortuko du. Hori dela eta, ekaho(x) erako dei batek errorerik ez sortzeko x balioak 0 edo handiagoa izan beharko luke.

Programa zuzena baldin bada, zuzentasunaren froga eman behar da.

Puntuazioa:

a) Hasierako zatiketa eta eskema: 0,200
b) Hasierako esleipenaren egiaztapena: 0,150 (Kalkulua: 0,050. Inplikazioa: 0,100)
c) While-aren erregelako (I) puntua: 0,010
d) While-aren erregelako (II) puntua: 0,040
e) While-aren erregelako (III) puntua: 0,700 (Kalkulua: 0,200. Inplikazioa: 0,500)
f) While-aren erregelako (IV) puntua: 0,350
    (Inplikazio erraza: 0,100. Inplikazio zaila: 0,250)
g) While-aren erregelako (V) puntua: 0,100
h) While-aren erregelako (VI) puntua: 0,200 (Kalkulua: 0,050. Inplikazioa: 0,150)
i) Zuzentasunaren froga: 0,250

Inplikazio bat zergatik betetzen den ez bada azaltzen, zero kontatuko da, hau da, inplikazio bat betetzen dela esateak zergatik betetzen den azaldu gabe, zero balio du.

PROGRAMAZIOAREN METODOLOGIA
2014ko martxoaren 11ko partzialaren soluzioa
3. gaia -- Egiaztapena
Kudeaketaren eta Informazio Sistemen Informatikaren Ingeniaritzako Gradua
Bilboko IITUE (UPV / EHU)
Lengoaia eta Sistema Informatikoak Saila

Ariketa (Egiaztapena)

Honako programa hau guztiz zuzena al den egiaztatu Hoare-ren kalkulua erabiliz. Espezifikazioaren arabera programak, sarrerako datu bezala zenbaki osoz osatutako A(1..n) eta B(1..n) bektoreak emanda eta A(1..n) bektorean balio negatiborik ez dagoela jakinda, B(1..n) bektoreko osagai bakoitza posizio bereko A(1..n) bektoreko elementuaren erro karratuaren azpitik egindako hurbilketa osoa al den erabaki behar du *q* aldagai boolearrean.

$\{\varphi\} \equiv \{n \geq 1 \wedge q \wedge ezneg(A(1..n))\}$
i : = 1;
while {INB} {E} i ≠ n + 1 **and** q **loop**
    q : = (ekaho(A(i)) = B(i));
    i : = i + 1;
end loop;
$\{\psi\} \equiv \{q \leftrightarrow denakerro(A(1..n), B(1..n), n)\}$

$\{INB\} \equiv \{ezneg(A(1..n)) \wedge (1 \leq i \leq n + 1) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), i - 1))\}$ $E = n + 1 - i$ $ezneg(H(1..r)) \equiv \forall k(1 \leq k \leq r \rightarrow H(k) \geq 0)$ $denakerro(F(1..r), G(1..r), pos) \equiv \forall k(1 \leq k \leq pos \rightarrow ekaho(F(k)) = G(k))$

Hor **ekaho** funtzioa, negatiboa ez den zenbaki oso bat emanda, zenbaki horren **e**rro **k**arratuaren **a**zpitik egindako **h**urbilketa **o**soa kalkulatzen duen funtzioa da (Adibideak: ekaho(9) = 3, ekaho(10) = 3, ekaho(8) = 2).

Egiaztapena egiterakoan, **ekaho** funtzioa inplementatuta dagoela suposatu behar da eta erabiltzeaz bakarrik arduratu beharko dugu, mod, div, eta antzeko beste funtzioekin egiten dugun bezala. Gainera, negatiboa den argumentu bat emanez gero, **ekaho** funtzioak errorea sortuko du. Hori dela eta, ekaho(x) erako dei batek errorerik ez sortzeko x balioak 0 edo handiagoa izan beharko luke.

Hasierako zatiketa eta eskema:

- While aginduaren aurretik esleipen bat dagoenez, while-aren aurrebaldintza edo hasierako baldintza bezala {INB} ipini behar da.

$\{\varphi\}$
i : = 1;
{INB}
while {INB} {E} i ≠ n + 1 **and** q **loop**
    q : = (ekaho(A(i)) = B(i));
    i : = i + 1;
end loop;
$\{\psi\}$

- Bi azpiprograma bereiztu behar dira:

```
{φ}
i : = 1;
{INB}
```

eta

```
{INB}
while {INB} {E} i ≠ n + 1 and q loop
   q : = (ekaho(A(i)) = B(i));
   i : = i + 1;
end loop;
{ψ}
```

➢ Hasteko lehenengo azpiprograma zuzena dela egiaztatuko da

```
{φ}                         φ → φ1?
          {φ1}
          i : = 1;
(EA)
          {INB}
```

- $\{\varphi_1\} \equiv \{def(1) \wedge (INB)_i^{\,1}\} \equiv$

$\equiv \{true \wedge ezneg(A(1..n)) \wedge (1 \le 1 \le n + 1) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), 1 - 1))\} \equiv$ sinplifikazioa

$\equiv \{ezneg(A(1..n)) \wedge (1 \le n + 1) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), 0))\} \equiv$ sinplifikazioa

$\equiv \{ezneg(A(1..n)) \wedge (0 \le n) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), 0))\} \equiv$ formula

$\equiv \{ezneg(A(1..n)) \wedge (0 \le n) \wedge (q \leftrightarrow \forall k(1 \le k \le 0 \rightarrow ekaho(A(k)) = B(k)))\} \equiv$ eremu hutsa

$\equiv \{ezneg(A(1..n)) \wedge (0 \le n) \wedge (q \leftrightarrow true)\} \equiv$ sinplifikazioa

$\equiv \{ezneg(A(1..n)) \wedge (0 \le n) \wedge q\}$

- Lehenengo sinplifikazioan, alde batetik δ edozein formula izanda ere, *true* $\wedge\ \delta \equiv \delta$ betetzen dela hartu da kontuan. Beste aldetik, $1 \le 1$ beti betetzen denez, $(1 \le 1 \le n + 1)$ ipintzea $(1 \le n + 1)$ ipintzearen berdina da.

- Bigarren sinplifikazioan $1 \le n + 1$ propietatean alde bietan 1 kenduz ere esanahi bereko propietatea gelditzen denez, hori egin da eta $0 \le n$ geratu da.

- Jarraian denakerro(A(1..n), B(1..n), 0) predikatua dagokion formulaz ordezkatu da, hau da, $\forall k(1 \le k \le 0 \rightarrow ekaho(A(k)) = B(k))$ formulaz. Hor eremu hutsa duen formula unibertsal bat geratzen zaigunez, badakigu bere balioa true dela.

- Azkeneko sinplifikazioa δ edozein formula izanda ere, $\delta \leftrightarrow$ *true* $\equiv \delta$ betetzen delako egin da.

- $\varphi \rightarrow \varphi_1$?

$$\{\underbrace{n \geq 1}_{\alpha} \wedge \underbrace{q}_{\beta} \wedge \underbrace{ezneg(A(1..n))}_{\gamma}\}$$

$$\downarrow ?$$

$$\{\underbrace{ezneg(A(1..n))}_{\gamma\text{-gatik}} \wedge \underbrace{0 \leq n}_{\alpha\text{-gatik}} \wedge \underbrace{q}_{\beta\text{-gatik}}\}$$

$n \geq 1$ betetzen denez, $n \geq 0$ ere beteko da, hau da, $0 \leq n$ beteko da. Bestalde, φ formulan $q \wedge ezneg(A(1..n))$ true dela esaten zaigunez, badakigu φ_1 formulako $q \wedge ezneg(A(1..n))$ zatia true dela.

➢ Orain bigarren azpiprograma hartu eta While-aren erregela (WE) aplikatuko dugu, aurrebaldintza {INB} dela eta bukaerako baldintza $\{\psi\}$ dela kontsideratuz. Erregela hori kontuan hartuz azpiprograma hau zuzena dela erabakitzeko jarraian zehazten diren kalkuluak eta egiaztapenak burutu beharko dira.

Eskema:

I. $INB \rightarrow INB$?
II. $INB \rightarrow def(B)$?

III. $\{INB \wedge B\}$ $(INB \wedge B) \rightarrow \varphi_3$?
$\{\varphi_3\}$
q : = (ekaho(A(i)) = B(i));
(EA)
$\{\varphi_2\}$
i : = i + 1;
(EA)
{INB}

IV. $(INB \wedge \neg B) \rightarrow \psi$?
V. $(INB \wedge B) \rightarrow E > 0$?
VI. $\{INB \wedge B \wedge E = v\}$ $(INB \wedge B \wedge E = v) \rightarrow \varphi_5$?
$\{\varphi_5\}$
q : = (ekaho(A(i)) = B(i));
(EA)
$\{\varphi_4\}$
i : = i + 1;
(EA)
$\{E < v\}$

I. $INB \rightarrow INB$? Bai, alde bietan gauza bera daukagulako.

II. INB → def(B)?
INB → def(i ≠ n + 1 **and** q)?
INB → true? Bai, inplikazioaren bigarren zatian true daukagulako.

III.

- $\{\varphi_2\} \equiv \{def(i + 1) \wedge (INB)_i^{\,i+1}\} \equiv$
  $\equiv \{true \wedge ezneg(A(1..n)) \wedge (1 \le i + 1 \le n + 1) \wedge$
  $(q \leftrightarrow denakerro(A(1..n), B(1..n), i + 1 - 1)) \equiv^{\text{sinplifikazioa}}$
  $\equiv \{ezneg(A(1..n)) \wedge (0 \le i \le n) \wedge$
  $(q \leftrightarrow denakerro(A(1..n), B(1..n), i))\}$

  Sinplifikazio urratsean alde batetik δ edozein formula izanda ere, *true* ∧ δ ≡ δ betetzen dela hartu da kontuan. Beste aldetik, (1 ≤ i + 1 ≤ n) eraldatu da, erdian i geldi dadin i + 1 balioaren ordez. Horretarako hiru osagaiei 1 kendu zaie: (1 – 1 ≤ i + 1 – 1 ≤ n + 1 – 1). Eragiketak burutu ondoren (0 ≤ i ≤ n) gelditu da. Gainera denakerro(A(1..n), B(1..n), i + 1 – 1) espresioan kenketa burutu da eta denakerro(A(1..n), B(1..n), i) geratu da.

- $\{\varphi_3\} \equiv \{def(ekaho(A(i)) = B(i)) \wedge (\varphi_2)_q^{\,ekaho(A(i)) = B(i)}\} \equiv$
  $\equiv \{(1 \le i \le n) \wedge (1 \le i \le n) \wedge A(i) \ge 0 \wedge$
  $ezneg(A(1..n)) \wedge (0 \le i \le n) \wedge$
  $(ekaho(A(i)) = B(i)) \leftrightarrow denakerro(A(1..n), B(1..n), i))\} \equiv^{\text{sinplifikazioa}}$
  $\equiv \{(1 \le i \le n) \wedge A(i) \ge 0 \wedge$
  $ezneg(A(1..n)) \wedge (0 \le i \le n) \wedge$
  $(ekaho(A(i)) = B(i)) \leftrightarrow denakerro(A(1..n), B(1..n), i))\} \equiv^{\text{sinplifikazioa}}$
  $\equiv \{(1 \le i \le n) \wedge A(i) \ge 0 \wedge$
  $ezneg(A(1..n)) \wedge$
  $(ekaho(A(i)) = B(i)) \leftrightarrow denakerro(A(1..n), B(1..n), i))\}$

def(ekaho(A(i)) = B(i)) espresioak i-rentzat bi eremu sortzen ditu (bata A(i)-gatik eta bestea B(i)-gatik) eta gainera A(i) ≥ 0 espresioa ere sortzen du, ekaho funtzioak errorea ez sortzeko baldintza hain zuzen ere. Hor (1 ≤ i ≤ n) espresioa bi aldiz agertzen denez (bata A(i)-ren definizioagatik eta bestea B(i)-ren definizioagatik) bietako bat kendu egin da lehenengo sinplifikazioan.

Hala ere bi eremu geratzen dira i-rentzat. Horregatik bigarren sinplifikazioan i aldagaiari dagokion eremua zein den erabakitzeko, beheko mugetatik handiena (1 eta 0ren arteko handiena) eta goiko mugetatik txikiena (n eta n-ren arteko txikiena) hartu behar dira, beraz 1 eta n.

- $(INB \wedge B) \rightarrow \varphi_3$?

$$\underbrace{\text{ezneg}(A(1..n))}_{\delta} \wedge (\underbrace{1 \le i}_{\alpha_1} \underbrace{\le n + 1}_{\alpha_2}) \wedge \underbrace{(\underbrace{q}_{\beta_1} \leftrightarrow \underbrace{\text{denakerro}(A(1..n), B(1..n), i - 1)}_{\beta_2})}_{\beta} \wedge \underbrace{i \ne n + 1}_{\alpha_3} \textbf{ and } \underbrace{q}_{\gamma}$$

$$\downarrow ?$$

$$(\underbrace{1 \le i}_{\alpha_1\text{-gatik}} \underbrace{\le n}_{\alpha_2 \text{ eta } \alpha_3\text{-gatik}}) \wedge \underbrace{A(i) \ge 0}_{\alpha_1,\, \alpha_2, \text{ eta } \delta\text{-gatik}} \wedge \underbrace{\text{ezneg}(A(1..n))}_{\delta\text{-gatik}} \wedge \underbrace{(\underbrace{\text{ekaho}(A(i)) = B(i)}_{\lambda_1} \leftrightarrow \underbrace{\text{denakerro}(A(1..n), B(1..n), i)}_{\lambda_2})}_{\beta \text{ eta } \gamma\text{-gatik}})$$

$INB \wedge B$ betetzen dela jakinda, φ_3 betetzen al den jakin nahi da.

α_1-gatik $0 \le i$ betetzen da.

α_2 eta α_3-gatik $i \le n$ betetzen da.

α_1, α_2 eta α_3-gatik i-ren balioa 1 eta n-ren artean dagoela ziurta dezakegu eta, ondorioz, A(i) elementuan A(1..n) bektorearen osagai bat da. Hori jakinda, δ-gatik $A(i) \ge 0$ dela ziurta dezakegu.

δ-gatik ezneg(A(1..n)) beteko dela ere ziurta dezakegu.

φ_3 formulako $\lambda_1 \leftrightarrow \lambda_2$ inplikazio bikoitzari dagokionez, honako inplikazio hau egiaztatu behar da: $(INB \wedge B) \rightarrow (\lambda_1 \leftrightarrow \lambda_2)$?

β bezala izendatu dugun $q \leftrightarrow$ denakerro(A(1..n), B(1..n), i – 1) formularen esanahia honako hau da:

$q \leftrightarrow \forall k(1 \le k \le i - 1 \rightarrow \text{ekaho}(A(k)) = B(k))$

Konjuntzioa erabiliz, honela ere adieraz daiteke:

$q = (\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i - 1)) = B(i - 1))$

Bestetik $\lambda_1 \leftrightarrow \lambda_2$ bezala izendatu dugun
$(\text{ekaho}(A(i)) = B(i)) \leftrightarrow \text{denakerro}(A(1..n), B(1..n), i)))$
formularen esanahia honako hau da:

$(\text{ekaho}(A(i)) = B(i)) \leftrightarrow \forall k(1 \le k \le i \rightarrow \text{ekaho}(A(k)) = B(k))$

Konjuntzioa erabiliz, honela ere adieraz daiteke:

$$(\text{ekaho}(A(i)) = B(i)) = (\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1)) \wedge (\text{ekaho}(A(i)) = B(i))$$

Galdera honako hau da:

$$q = (\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1))$$

betetzen dela jakinda,

$$(\text{ekaho}(A(i)) = B(i)) = (\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1)) \wedge (\text{ekaho}(A(i)) = B(i))$$

ere btetzen al da?

γ-gatik badakigu q-ren balioa true dela. Beraz, q eta $(\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1))$ formularen balioak berdinak direnez, $(\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1))$ formularen balioa ere true dela ondorioztа dezakegu.

Beraz,

$$(\text{ekaho}(A(i)) = B(i)) = \underbrace{(\text{ekaho}(A(1)) = B(1)) \wedge \ldots \wedge (\text{ekaho}(A(i-1)) = B(i-1))}_{\text{true}} \wedge (\text{ekaho}(A(i)) = B(i))$$

formulan true den zatia sinplifika daiteke eta galdera honako hau da

$$(\text{ekaho}(A(i)) = B(i)) = (\text{ekaho}(A(i)) = B(i))?$$

Eta erantzuna baiezkoa da alde bietan gauza bera daukagulako.

Ondorioz, $INB \wedge B$ formulak $\lambda_1 \leftrightarrow \lambda_2$ formula inplikatzen duela frogatu da, β eta γ zatietan zegoen informazioa erabiliz.

IV. $(INB \wedge \neg B) \rightarrow \psi$?

$$\underbrace{ezneg(A(1..n))}_{\delta} \wedge (\underbrace{1 \le i}_{\alpha_1} \le \underbrace{i \le n+1}_{\alpha_2}) \wedge \underbrace{(\underbrace{q}_{\beta_1} \leftrightarrow \underbrace{denakerro(A(1..n), B(1..n), i-1)}_{\beta_2})}_{\beta} \wedge (\underbrace{i = n+1}_{\alpha_3} \vee \underbrace{\neg q}_{\gamma})$$

$$\downarrow ?$$

$$\underbrace{\underbrace{q}_{\psi_1} \leftrightarrow \underbrace{denakerro(A(1..n), B(1..n), n)}_{\psi_2}}_{\psi}$$

Helburua δ, α_1, α_2, β eta $\alpha_3 \vee \gamma$ egiazkoak direla jakinda, ψ egiazkoa al den erabakitzea da. Kasu honetan $\alpha_3 \vee \gamma$ disjuntzioa, hau da, $(i = n + 1 \vee \neg q)$ disjuntzioa daukagunez, disjuntzio hori egia izateko dauden hiru aukerak hartu beharko dira kontuan:

i = n + 1	**¬q**
True	True
True	False
False	True

- ✓ Lehenengo bi kasuetan **$i = n + 1$** denez, β eta ψ formula bera dira. β betetzen dela dakigunez, ψ formula ere bete egiten da. Ondorioz inplikazioa ere bete egiten da.
- ✓ Hirugarren kasuan **$i = n + 1$** false da eta **$\neg q$ = True** betetzen da. Ondorioz, α_2 kontuan hartuz, $i \le n$ eta **q = False** betetzen dira. Orain $i \le n$ betetzen denez, β eta ψ ez dira formula bera eta arrazonamendu desberdina jarraitu behar da. Gure helburua ψ betetzen al den erabakitzea da. β formularen esanahia honako hau da:

  $$q \leftrightarrow \forall k(1 \le k \le i-1 \rightarrow ekaho(A(k)) = B(k))$$

  Konjuntzioa erabiliz, honela ere adieraz daiteke:

  $$q = (ekaho(A(1)) = B(1)) \wedge \ldots \wedge (ekaho(A(i-1)) = B(i-1))$$

  q false denez badakigu

  $$(ekaho(A(1)) = B(1)) \wedge \ldots \wedge (ekaho(A(i-1)) = B(i-1))$$

  ere false dela.

  ψ formularen esanahia honako hau da:

  $$q \leftrightarrow \forall k(1 \le k \le n \rightarrow ekaho(A(k)) = B(k))$$

Konjuntzioa erabiliz, honela ere adieraz daiteke:

$$q = \underbrace{(ekaho(A(1)) = B(1)) \wedge \dots \wedge (ekaho(A(i-1)) = B(i-1))}_{\text{false}} \wedge \dots \wedge (ekaho(A(n)) = B(n))$$

β formula eta q = false informazioa erabiliz
$(ekaho(A(1)) = B(1)) \wedge \dots \wedge (ekaho(A(i-1)) = B(i-1))$

formularen balioa false dela ikusi dugu. Gainera π edozein formula izanda ere $false \wedge \pi \equiv false$ betetzen denez,

$(ekaho(A(1)) = B(1)) \wedge \dots \wedge (ekaho(A(i-1)) = B(i-1)) \wedge \dots \wedge ekaho(A(n)) = B(n)$

formularen balioa ere false izango da eta, ondorioz, q-ren balioaren berdina da eta beraz, inplikazioa bete egiten da.

V. $(INB \wedge B) \rightarrow E > 0?$

$$ezneg(A(1..n)) \wedge (1 \le \underbrace{i \le n + 1}_{\alpha}) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), i-1)) \wedge \underbrace{i \ne n + 1}_{\beta} \textbf{ and } q$$

$$\downarrow ?$$

$$\underbrace{n + 1 - i > 0}_{\alpha \text{ eta } \beta\text{-gatik}}$$

Helburua $n + 1 - i > 0$ betetzen al den erabakitzea da.
α-gatik $i \le n + 1$ betetzen da, hau da, $n + 1 \ge i$ betetzen da. β-gatik $i \ne n + 1$ dela ere badakigu. Beraz, $n + 1 > i$ betetzen da. Gure helburua $n + 1 - i$ espresioarekin zer gertatzen den jakitea denez, espresio horretako alde bietan i kenduko dugu: $n + 1 - i > i - i$. Sinplifikatuz $n + 1 - i > 0$ geratzen da, eta hori zen frogatu nahi genuena.

VI.

- $\{\varphi_4\} \equiv \{def(i + 1) \wedge (E < v)_i^{i+1}\} \equiv$
  $\equiv \{true \wedge n + 1 - (i + 1) < v\} \equiv^{\text{sinplifikazioa}}$
  $\equiv \{n + 1 - i - 1 < v\} \equiv^{\text{sinplifikazioa}}$
  $\equiv \{n - i < v\}$

  δ edozein formula izanda ere *true* $\wedge\ \delta \equiv \delta$ betetzen denez, sinplifikazioko lehenengo urratsean true ezabatu da. Gainera, $n + 1 - (i + 1)$ espresioa eraldatu da $n + 1 - i - 1 < v$ espresioa lortuz.
  Bigarren sinplifikazioan batekoak ezabatu dira.

- $\{\varphi_5\} \equiv \{def(ekaho(A(i)) = B(i)) \wedge (\varphi_4)_q^{ekaho(A(i)) = B(i)}\} \equiv$
  $\equiv \{(1 \le i \le n) \wedge (1 \le i \le n) \wedge A(i) \ge 0 \wedge (n - i < v)\} \equiv^{\text{sinplifikazioa}}$
  $\equiv \{(1 \le i \le n) \wedge A(i) \ge 0 \wedge (n - i < v)\}$

  def(ekaho(A(i)) = B(i)) espresioak i-rentzat bi eremu sortzen ditu (bata A(i)-gatik eta bestea B(i)-gatik) eta gainera $A(i) \ge 0$ espresioa ere sortzen du, ekaho funtzioak errorea ez sortzeko baldintza hain zuzen ere. Hor i aldagaiaren eremu biak berdinak direnez, bat zuzenean ken daiteke.

- $(INB \wedge B \wedge E = v) \to \varphi_5$?

$$\underbrace{ezneg(A(1..n))}_{\delta} \wedge (\underbrace{1 \le i}_{\alpha_1} \underbrace{\le n + 1}_{\alpha_2}) \wedge (q \leftrightarrow denakerro(A(1..n), B(1..n), i - 1)) \wedge \underbrace{i \ne n + 1}_{\alpha_3} \textbf{ and } q \wedge \underbrace{n + 1 - i = v}_{\beta}$$

$$\downarrow ?$$

$$(\underbrace{1 \le i}_{\alpha_1\text{-gatik}} \underbrace{\le n}_{\alpha_2 \text{ eta } \alpha_3\text{-gatik}}) \wedge \underbrace{A(i) \ge 0}_{\alpha_1,\ \alpha_2,\ \alpha_3 \text{ eta } \delta\text{-gatik}} \wedge \underbrace{(n - i < v)}_{\beta\text{-gatik}}$$

$1 \le i$ espresioa α_1-gatik betetzen da.
$i \le n$ espresioa α_2 eta α_3-gatik betetzen da.
α_1, α_2 eta α_3-gatik i-ren balioa 1 eta n-ren artean dagoela ziurta dezakegu eta, ondorioz, A(i) elementuan A(1..n) bektorearen osagai bat da. Hori jakinda, δ-gatik $A(i) \ge 0$ dela ziurta dezakegu.
β-gatik badakigu $n + 1 - i = v$ betetzen dela. Orain $n - i < v$ betetzen al den jakin nahi da. Hori dela eta, $n + 1 - i = v$ espresioan alde bietan 1 kenduz espresioa eraldatu egingo dugu, hau da, $n + 1 - i - 1 = v - 1$, eta sinplifikatu ondoren $n - i = v - 1$ geratzen da. Beraz orain badakigu $n - i$ espresioaren balioa $v - 1$ dela eta galdera $n - i$ espresioaren balioa v baino txikiagoa al den da. $v - 1$ beti v baino txikiagoa izaten denez, $n - i$ espresioaren balioa v baino txikiagoa dela ziurta dezakegu.

Beraz $(INB \wedge B \wedge E < v) \to \varphi_5$ inplikazioa bete egiten da.

- **Zuzentasunaren froga:**

1. $\varphi \rightarrow \varphi_1$
2. $\{\varphi_1\}$ i : = 1; {INB} (EA)
3. $\{\varphi\}$ i : = 1; {INB} (OE 1, 2)

I 4. INB → INB

II 5. INB → def(B)

III 6. (INB ∧ B) → φ_3
7. $\{\varphi_3\}$ q : = (ekaho(A(i)) = B(i)); $\{\varphi_2\}$ (EA)
8. {INB ∧ B} q : = (ekaho(A(i)) = B(i)); $\{\varphi_2\}$ (OE 6, 7)
9. $\{\varphi_2\}$ i : = i + 1; {INB} (EA)
10. {INB ∧ B}
    q : = (ekaho(A(i)) = B(i));
    i : = i + 1;
    {INB} (KE 8, 9)

IV 11. (INB ∧ ¬B) → ψ

V 12. (INB ∧ B) → E > 0

VI 13. (INB ∧ B ∧ E = v) → φ_5
14. $\{\varphi_5\}$ q : = (ekaho(A(i)) = B(i)); $\{\varphi_4\}$ (EA)
15. {INB ∧ B ∧ E = v} q : = (ekaho(A(i)) = B(i)); $\{\varphi_4\}$ (OE 13, 14)
16. $\{\varphi_4\}$ i : = i + 1; {E < v} (EA)
17. {INB ∧ B ∧ E = v}
    q : = (ekaho(A(i)) = B(i));
    i : = i + 1;
    {E < v} (KE 15, 16)

18. {INB}
    while {INB} i ≠ n + 1 **and** q **loop**
        q : = (ekaho(A(i)) = B(i));
        i : = i + 1;
    end loop;
    {ψ} (WE 4, 5, 10, 11, 12, 17)

19. {φ}
    i : = 1;
    while {INB} i ≠ n + 1 **and** q **loop**
        q : = (ekaho(A(i)) = B(i));
        i : = i + 1;
    end loop;
    {ψ} (KE 3, 18)

Zuzentasunaren froga ematerakoan, While-aren aurreko esleipenari dagozkion hiru puntuak (1-3), while-aren erregelako III puntuari dagozkion bost puntuak (6-10) eta while-aren erregelako VI puntuari dagozkion bost puntuak (13-17) lortzeko, formulatik formulara doazen zatiak edo blokeak hartuz eta elkartuz joatea da onena, kasuan kasuko programa osatu arte.

While-aren aurretik dagoen esleipenaren kasuan, hasteko 1 eta 2 oinarrizko blokeak hartuko genituzke eta bi bloke horiek elkartzerakoan 3 blokea lortuko genuke. Oinarrizko blokeak (kasu honetan 1 eta 2) formulatik formulara joaten dira eta erdian gehienez esleipen bat izaten dute. Oinarrizko blokeak erdian esleipenik ez badu (1 oinarrizko blokeak bezala), orduan inplikazio bezala ipini beharko da. Oinarrizko blokeak esleipen bat badu (2 blokeak bezala), orduan oinarrizko bloke hori Esleipenaren Axiomagatik (EA) zuzena dela adierazi beharko da. Kasu honetan 1 blokeak esleipenik ez duenez, 1 eta 2 blokeak elkartzeko ondorioaren erregela (OE) erabili behar da.

3 | 1 | $\{\varphi\}$

2 | $\{\varphi_1\}$

(EA) $i := 1;$

$\{INB\}$

While-aren erregelako III puntuari dagokion programan, hasteko 6 eta 7 oinarrizko blokeak hartuko genituzke eta bloke horiek elkartzean 8 blokea lortuko genuke. Oinarrizko blokeak (kasu honetan 6 eta 7) formulatik formulara joaten dira eta erdian gehienez esleipen bat izaten dute. Oinarrizko blokeak erdian esleipenik ez badu (6 oinarrizko blokeak bezala), orduan inplikazio bezala ipini beharko da. Oinarrizko blokeak esleipen bat badu (7 blokeak bezala), orduan oinarrizko bloke hori Esleipenaren Axiomagatik (EA) zuzena dela adierazi beharko da. Kasu honetan 6 blokeak esleipenik ez duenez, 6 eta 7 blokeak elkartzeko ondorioaren erregela (OE) erabili behar da. Jarraian 9 oinarrizko blokea hartuko genuke. 9 oinarrizko blokeak esleipen bat du eta oinarrizko bloke hori Esleipenaren Axiomagatik (EA) zuzena dela adierazi beharko da. Gero 8 eta 9 oinarrizko blokeak elkartu beharko dira. Bloke biek gutxienez esleipen bat dutenez, konposizioaren erregelaren bidez (KE) elkartuko dira. 8 eta 9 blokeak elkartzean 10 blokea lortzen da eta hori III puntuari dagokion programa da.

10 | 8 | 6 | **III.** $\{INB \wedge B\}$

7 | $\{\varphi_3\}$

(EA) $q := (ekaho(A(i)) = B(i));$

9 | $\{\varphi_2\}$

(EA) $i := i + 1;$

$\{INB\}$

While-aren erregelako VI puntuari dagokion zatian planteamendua III puntuko planteamenduaren berdina da.

17 15 13 **VI.** $\{INB \wedge B \wedge E = v\}$

14

$\{\varphi_5\}$

q : = (ekaho(A(i)) = B(i));

(EA)

16

$\{\varphi_4\}$

i : = i + 1;

(EA)

$\{E < v\}$