

4. gaia: Programek era formalean eratorreko metodoa.

(*) White-aren emeela:

I. $\gamma \rightarrow INB$

II. $\{INB \rightarrow \text{df}(B)\}$

III. $\{INB \wedge B\} \gamma$

Ajenduak

$\{INB\} \gamma$

IV. $\{INB \wedge B\} \rightarrow \gamma$

V. $\{INB \wedge B\} \rightarrow E > 0$

VI. $\{INB \wedge B \wedge E = v\} \gamma$

Ajenduak

$\{E < v\} \gamma$

PROGRAMAREN EGITURA

$\{E\}$

Hameraketa?

while $\{INB\} \{E\} B$ loop

Ajenduak?

and loop;

$\{\gamma\}$

- Hameraketa
- White-aren boldintza
- Ajenduak

Lohaketa

$$\lambda \equiv n \geq 2 \wedge \text{pasa}(\text{A}(1..n))$$

$$Y(l) \equiv (\text{A}(l) \bmod l) = 0$$

$$\mu(l) \equiv \forall k ((2 \leq k \leq l) \rightarrow ((\text{A}(k) \bmod k) \neq 0))$$

Definizioak:

$$\{\gamma\} \equiv \lambda$$

$$\{INB\} \equiv \lambda \wedge (2 \leq i \leq n) \wedge (q \leftrightarrow Y(i)) \wedge \mu(i-1)$$

$$\{E\} \equiv n - i$$

$$\{\gamma\} \equiv q \leftrightarrow \exists k ((2 \leq k \leq n) \wedge Y(k))$$

(a) HASIERAKETAK

$E = n - i$ erakoa denet ("galkomuga"-indizoa) beldorea eskemelik estunera zeharratuko da.

I. $\gamma \rightarrow INB ?$

$$\begin{array}{c} \lambda \\ \downarrow \\ \lambda \wedge (2 \leq i \leq n) \wedge (q \leftrightarrow Y(i)) \wedge \mu(i-1) \\ \hookrightarrow \text{a-fatik bai. } B \end{array}$$

Implikazioa ez da betetzen, lehengo zatiak ^(a)ez baitago B , d eta θ formulaek betetzen direla zientzako erabili ditzagun informazioak.

Inplikazioa betetzea nahi dugunet da beldorea eskemelik estunera zeharratuko denet i-n 2. balioa esleituko diot.

$\{\gamma\}$

$$\{\gamma\} \equiv \{ \text{df}(2) \wedge (INB); \gamma \equiv \{ \text{True} \wedge \lambda \wedge (2 \leq 2 \leq n) \wedge (q \leftrightarrow \gamma(2)) \wedge \mu(2-1) \} \equiv$$

$$= \{ \lambda \wedge (2 \leq n) \wedge (q \leftrightarrow \gamma(2)) \wedge \mu(1) \} \equiv$$

$$= \{ \lambda \wedge q \leftrightarrow \gamma(2) \wedge \text{True} \} \equiv$$

$$= \{ \lambda \wedge q \leftrightarrow \gamma(2) \}$$

$\hookrightarrow \forall k ((2 \leq k \leq 1) \rightarrow (\text{A}(k) \bmod k) \neq 0)$

multzoa nula
denet True

$$\frac{\lambda}{\alpha} \wedge \underbrace{q \leftrightarrow Y(2)}_{\beta}$$

α betetzen da λ -patik baina β ea da betetzen. β betetzenko q -ni fare esleku beharko dio gu, $Y(2)$ beltzaren arabera harkoa denez, esei dugulako berria $Y(2) \equiv 4 \cdot (2) \bmod 2 = 0$ natea (BETI).

$$\begin{aligned} \{ & \varphi_1 \\ \{ & \varphi_2 \\ q := & Y(2) \\ \{ & \varphi_1 \\ i := & 2; \\ \{ & INB \end{aligned}$$

$$\begin{aligned} \{ & \varphi_2 \equiv \{ \text{def}(Y(2)) \wedge (Y(1) \neq 1) \} \equiv \\ & \{ (1 \leq i \leq n) \wedge i \neq 0 \wedge \lambda \wedge Y(i) \leftrightarrow (Y(2) \neq 1) \equiv \\ & \{ \varphi_2 \equiv \{ \text{In} \} \equiv \delta \equiv \{ \lambda \} \end{aligned}$$

$(\varphi \rightarrow \varphi_2)$ han da $\rightarrow \lambda \rightarrow \lambda$? Bai, aplikazioa bete egin da, eta ondorioz hanera telekui auraitu dugu.

b) Balduriaz

④ While noiz geldituko da?

$$\neg B \equiv \{ i=n \vee q \}$$

\hookrightarrow orduan, $B = \{ i \neq n \wedge \neg q \}$

II. $INB \rightarrow \text{def}(B)$?

$$INB \rightarrow \text{def}(i \neq n \wedge \neg q) ?$$

$INB \rightarrow \text{True}$? Bai, bisaren zatia tree delako.

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

$$\lambda \wedge \{ 2 \leq i \leq n \} \wedge \underbrace{(q \leftrightarrow Y(i))}_{\alpha} \wedge \underbrace{\mu(i-1)}_{\delta} \wedge \underbrace{(i=n \vee q)}_{\neg B}$$

$$q \leftrightarrow \exists k (2 \leq k \leq n) \wedge Y(k)$$

B desputazio bat denez
 $\neg B$ ega (zaleko 3aikora daude de hura) astertze behar dira.

$i=n$	q
True	True
True	False
False	True

⑧ Behenengo bi-kasuelau ($i=n$) denez:

$$\alpha \equiv q \leftrightarrow Y(i) \equiv q \leftrightarrow Y(n) \wedge \underbrace{\mu(i-1)}_{\alpha} \equiv \underbrace{\mu(n-1)}_{\beta} \quad \text{dira, orduan:}$$

$$\lambda \wedge (2 \leq i \leq n) \wedge \underbrace{(q \leftrightarrow Y(n))}_{\alpha} \wedge \underbrace{\mu(n-1)}_{\beta} \wedge (i=n \vee q)$$

$$\downarrow$$

$$q \leftrightarrow \exists k ((2 \leq k \leq n) \wedge Y(k))$$

λ ete α formulakoa badakigu $n-1$ norroko arte, honi barne, asertioa ez dela betetzen, beraz asertio hori eta α baldintza berdus dute; orduan implikazioa beteko da.

⑨ $i \neq n$ eta $q = \text{True}$ karna

$$\lambda \wedge \underbrace{(2 \leq i \leq n)}_{\alpha} \wedge \underbrace{(q \leftrightarrow Y(i))}_{\alpha} \wedge \underbrace{\mu(i-1)}_{\beta} \wedge (i=n \vee q)$$

$$\downarrow$$

$$q \leftrightarrow \exists k ((2 \leq k \leq n) \wedge Y(k))$$

$i \neq n$ denez α -tako badakigu $i \leq n$ dela eta $q = \text{True}$ denez badakigu $Y(i)$ betetzen dela eta behoko asertioak tantean betetzen dela:

$$q \leftrightarrow \exists k ((2 \leq k \leq n) \wedge Y(k)) \Rightarrow$$

$$\text{True} \leftrightarrow \underbrace{Y(2) \vee Y(3) \vee \dots \vee Y(i) \vee \dots \vee Y(n)}_{\text{True}} \Rightarrow \text{True} \leftrightarrow Y(2) \vee Y(3) \vee \dots \vee Y(n) \Rightarrow$$

$$\boxed{\delta \vee \text{True} \equiv \text{True}}$$

$\Rightarrow \text{True} \leftrightarrow \text{True}$? BAI, implikazioa betetzen da.

$\forall ((INB \wedge B) \rightarrow E > 0)$

INB

B

$$\lambda \wedge \underbrace{(2 \leq i \leq n)}_{\alpha} \wedge (q \leftrightarrow \delta(i)) \wedge \mu(i-1) \wedge i \neq n \wedge \neg q$$



$$n-i > 0$$

$i \neq n$ denez B patik ete α gatik $i < n$ dela dahu, beraz
 $n-i > 0$ beteko da.

② aginduak

Prop. 1

III. $\exists INB \wedge B \wedge E = v$

Aginduak

$\exists INB \wedge$

$$INB \wedge B \rightarrow INB ?$$

Bai, $INB \wedge B$ era
 baina INB ere era
 izango da.

Prop 2.

VI. $\exists INB \wedge B \wedge E = v$

Aginduak

$\exists E < v$

$(INB \wedge B \wedge E = v) \rightarrow E < v$, et de beteko $E = v$
 egia baldun bada. erau debilo izan ere $E < v$.
 Implikazioa et denez betetzen $E < v$ betetzen
 agindu bat egia bezeroa duzu programa honetan.
 Beltzera eskeinetik eskuineko zehorkatzaren aniz
 E-ren balioa txikitako i aldagaiaari $i+1$ balioa
 esleituko dioque, ete esleitzen non azkuna
 erabiltz φ'_3 formula kalkulatuko ditz.

Prop 2

$$\left\{ \begin{array}{l} \{ INB \wedge B \wedge E = v \} \\ \{ \varphi'_3 \equiv \{ \text{def}(i+1) \wedge (E < v) \}^{i+1} \} \end{array} \right\} \equiv // E = n - c // \equiv$$

$$\begin{aligned} \varphi'_3 &\equiv \\ i &:= i+1 \\ &\equiv \{ \text{true} \wedge n - (i+1) < v \} \equiv \\ &\equiv n - c - 1 < v \end{aligned}$$

$$\{ E < v \}$$

Oraintxe $(INB \wedge B \wedge E = v) \rightarrow \varphi'_3$ betetzen den epartuta

$$\lambda \wedge (2 \leq i \leq n) \wedge (q \leftrightarrow \gamma(i)) \wedge \mu(i-1) \wedge i \neq n \wedge \neg q \wedge \underbrace{(n-i) = v}_{\alpha}$$



$$\underbrace{n-i-1 < v}_{B}$$

Implikazioa bete epten da β erakhoa delako a patile:

$n-i = v$ era dela dalguruz - Δ epten badugu bi aldeetan 3-

ere era itzaga da $n-i-1 = v-1$, eta $v-1$ batioa v batioa baino txikagoa da.

Oraintz Prog 2 zutene da, baina bi programetan berdina izan behar dugu, beraz, Prog 1-n $i := i + \Delta$ agindua ipini beharko dut.

Eta ipu ψ_3 formula kalkulatu eta $(INB \wedge B) \rightarrow \psi_3$ betetzen al den astertu beharko dut.

Prog 1

$$\begin{aligned} & \exists INB \wedge B \quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} \psi_3 \\ i := i + \Delta; \\ \exists INB \end{array} \right\} \end{array} \right\} \text{def}(i + \Delta) \wedge (INB)^{i + \Delta} \equiv \\ & \equiv \text{time} \wedge \lambda \wedge (2 \leq i + \Delta \leq n) \wedge (q \leftrightarrow \gamma(i + \Delta)) \wedge \mu(i + \Delta - 1) \equiv \\ & \equiv \lambda \wedge (\overset{-\Delta}{2 \leq} \overset{-\Delta}{i + \Delta} \overset{-\Delta}{\leq n}) \wedge (q \leftrightarrow \gamma(i + \Delta)) \wedge \mu(i) \equiv \\ & \equiv \lambda \wedge (1 \leq i \leq n - 1) \wedge (q \leftrightarrow \gamma(i + \Delta)) \wedge \mu(i) \end{aligned}$$

Oraintz $(INB \wedge B) \rightarrow \psi_3$ muplikazioa. betetzen al den astertu beharko dugu.

$$\lambda \wedge \underbrace{(2 \leq i \leq n)}_{\alpha_1} \wedge \underbrace{(q \leftrightarrow \gamma(i))}_{\beta} \wedge \underbrace{\mu(i - 1)}_{\alpha_2} \wedge \underbrace{i \neq n}_{\alpha_3} \wedge \underbrace{\neg q}_{\beta}$$

$$\lambda \wedge (1 \leq i \leq n - 1) \wedge (q \leftrightarrow \gamma(i + \Delta)) \wedge \mu(i)$$

Betetzen da β_1 dalgulako $i - 1$ patulu eta β_2 patulu eta β_3 patulu. Betetzen delako eta β patulu eta β_2 patulu eta β_3 patulu. β el β patulu badalagu i posizioan. $\gamma(i) = \text{False}$ dela, baina $i + \Delta$ posizioan es dalguruz $\gamma(i + \Delta)$ ren batioa.

Beraz, muplikazioa \rightarrow deitez betetzen, agindu bat gehituko dugu implikazioa beteteko, hometorako $i + \Delta$ posizioa astertu behar da, hometorako hanako agindua behar da:

$$q := \gamma(i + \Delta);$$

Eslepena jasotzen du kalkulatutako dut eta $(INB \wedge B) \rightarrow \psi_4$ muplikazioa betetzen al den astertuko dut.

$$\begin{array}{l}
 \left\{ \begin{array}{l} \text{Prog 1} \\ \{ \text{INB} \wedge B \} \end{array} \right. \\
 \left\{ \begin{array}{l} \{ \varphi_4 \equiv \} \text{ def } (\gamma_{(i+1)} \wedge (\varphi'_3)^{\gamma_{(i+1)}}) \varphi = \\
 q := \gamma_{(i+1)}; \\
 \{ \varphi_3 \} \\
 i = i+1 \\
 \{ \text{INB} \} \end{array} \right. \\
 \left. \begin{array}{l} \equiv \{ (\underbrace{1 \leq i \leq n}_{\alpha_1}) \wedge (\underbrace{i+1 \neq 0}_{\text{true}}) \wedge \lambda \wedge (1 \leq i \leq n-1) \wedge (\gamma_{(i+1)} \Rightarrow \gamma_{(i+1)}) \wedge \mu_{(i)} \varphi = \\
 \equiv \{ (0 \leq i \leq n-1) \wedge \lambda \wedge (1 \leq i \leq n-1) \wedge \mu_{(i)} \varphi = \\
 \{ \varphi_4 \} \equiv \{ (1 \leq i \leq n-1) \wedge \lambda \wedge \mu_{(i)} \varphi \end{array} \right. \\
 \end{array}$$

$$(\text{INB} \wedge B) \rightarrow \varphi_4 ?$$

$$\begin{array}{c}
 \lambda \wedge \underbrace{(2 \leq i \leq n)}_{\alpha_1} \wedge \underbrace{(q \leftrightarrow \gamma_{(i)})}_{\text{true}} \wedge \underbrace{\mu_{(i-1)}}_{\alpha_3} \wedge \underbrace{i \neq n}_{\alpha_2} \wedge \underbrace{\varphi}_{\alpha_4} \\
 \downarrow
 \end{array}$$

$$\begin{array}{c}
 \lambda \wedge \underbrace{(1 \leq i \leq n-1)}_{\substack{\alpha_1 \text{-gate} \\ \hookrightarrow \alpha_1 \text{ and } \alpha_2 \text{ gate}}} \wedge \underbrace{\mu_{(i)}}_{\alpha_2} \\
 \downarrow
 \end{array}$$

lehen esan ditzguret α_3 -gateko badago artekide $i-1$ posizora arte
 α_1 eta α_2 -gateko badalagu i posizian ero artekide degtar da betetzen dela.

Bera, inplikazioe bai betetzen da. Orain Prog 1 zuen da, baina
Prog 2-n ayndi berak izan behar ditzguret, eslepen bera jomia beter dugu
ite φ_4 kalkulatzeko behar da EA. erabiliz eta amaitzeko $(\text{INB} \wedge B \wedge E = r) \rightarrow \varphi_4$
ite φ_4 kalkulatzeko behar da.

Prog 2

$$\begin{array}{l}
 \left\{ \begin{array}{l} \text{INB} \wedge B \wedge E = r \varphi \\
 \{ \varphi'_4 \} \\
 q := \gamma_{(i+1)}; \\
 \{ \varphi'_3 \} \\
 i = i+1; \\
 \{ E < v \} \end{array} \right. \\
 \left. \begin{array}{l} \{ \varphi'_4 \} \equiv \{ \text{def } (\gamma_{(i+1)} \wedge (\varphi'_3)^{\gamma_{(i+1)}}) \varphi = \\
 \equiv \{ (\underbrace{1 \leq i \leq n}_{\alpha_1}) \wedge (\underbrace{i+1 \neq 0}_{\text{true}}) \wedge \underbrace{(n-i-1 < v)}_{\varphi} \varphi = \\
 \{ \varphi'_3 \} \equiv \{ (0 \leq i \leq n-1) \wedge (n-i-1 < v) \varphi = \end{array} \right. \\
 \end{array}$$

$$\text{INB} \wedge B \wedge E = r \rightarrow \varphi'_4 ?$$

$\text{INB} \wedge \text{P} \wedge \text{E} = r \rightarrow T_4 ?$

- 7 -

$$\lambda \ 1 \underbrace{(2 \leq i \leq n)}_{\alpha_3} \wedge (q \leftrightarrow \tau(i)) \wedge \mu (i-1) \wedge \underbrace{i \neq n \wedge q \in \text{en}}_{\alpha} \wedge \underbrace{i = n-i = v}_{\alpha_1}$$

\downarrow

$\underbrace{0 \leq i \leq n-1}_{\alpha \text{ patik } i < n} \wedge \underbrace{n-i-1 < v}_{\alpha \text{ eti } \alpha_1 \text{ patik beteben da:}}$

da epa dela deluguet $n-i = v$ epa da
 eti \rightarrow epa in aldeialdi $n-i-1 = v-1$ ere
 epa da, ondorioz $v-1$ baina v baino txikiagoa
 da.

d) Programa osoa ideari

{44

{424

$q := Y(2);$

{414

$i := 2;$

while {INB4} {E4} $i \neq n$ and not q loop

{444} {444}

$q := Y(i+1);$

{434} {434}

$i := i + 1;$

end loop

{44}