4. gaia: Programak era formalean eratorzeko metodoa.

⊛ While-aren emaitza:

I. $\varphi \to INB$

II. $\{INB \to dif(B)\}$

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

Apunduak

$\{INB\}$

IV. $((INB \wedge \neg B) \to \psi$

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

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

Apunduak

$\{E < v\}$

Hasieraketak
While-aren bolditza
Apunduak

Laburdurak

$\lambda \equiv n \geq 2 \wedge posiB(A(..n))$

$\gamma(\ell) \equiv (A(\ell) \bmod \ell) = 0$

$\mu(\ell) \equiv \forall k((2 \leq k \leq \ell) \to ((A(k) \bmod k) \neq 0))$

Definizioak:

$\{\varphi\} \equiv \lambda$

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

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

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

PROGRAMAREN EGITURA

$\{\varphi\}$

Hasieraketak?

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

Apunduak?

end loop;

$\{\psi\}$

⊛ HASIERAKETAK

$E = n - i$ eraiko denez ("gako-muga" - indizea) beltzaren ekeretik eskumera zehartzeko de

I. $\varphi \to INB$?

$$\underbrace{\lambda}_{\alpha} \wedge \underbrace{(2 \leq i \leq n)}_{\beta} \wedge \underbrace{(q \leftrightarrow \gamma(i))}_{\partial} \wedge \underbrace{\mu(i-1)}_{\theta}$$

↳ α-gatik bai. β

Implikazioa ez da betetzen, lehenengo zatian(α) ez baitago β, ∂ eta θ formulak betetzen direla ziurtatzeko erabili dezakegun informazioik.

Implikazioa betetzea nahi dugunez eta bektorea ekeretik eskumera zehartzeko denez i-ri 2 balioa esleitzeko diot.

$\{\varphi\}$

$i := 2;$

$\{INB\}$

$\{\varphi_1\} \equiv \{dif(2) \wedge (INB)_i^2\} \equiv \{True \wedge \lambda \wedge (2 \leq 2 \leq n) \wedge (q \leftrightarrow \gamma(2)) \wedge \mu(2-1)\} \equiv$

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

↳ $\forall k((2 \leq k \leq 1) \to ((A(k) \bmod k) \neq 0))$

↳ multzo hutsa denez True

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

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

$(\varphi \to \varphi_1)$?

$$\overbrace{\lambda}^{\partial} \downarrow$$

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

α betetzen da ∂-patik baina β ez da betetzen. β betetzeko q-ri false esleitu behar diogu, $\gamma(2)$ bektorearen arabera dena, ezin dugulako bermatu $\gamma(2) \equiv A(2) \bmod 2 = 0$ izatea (BETI).

$\{\varphi\}$

$\{\varphi_2\}$

$q := \gamma(2)$

$\{\varphi_1\}$

$i := 2;$

$\{INB\}$

$$\{\varphi_2\} \equiv \{def(\gamma(2)) \wedge (\varphi_1)_q^{\gamma(2)}\} \equiv$$

$$\{\varphi_2\} \equiv \{True \wedge \lambda \wedge \gamma(2) \leftrightarrow \gamma(2)\} \equiv \Big\| \gamma(2) \overset{?}{\leftrightarrow} \gamma(2) \text{ bai, beraz True da} \Big\| \equiv$$

$$\{\varphi_2\} \equiv \| True \wedge \partial \equiv \partial \| \equiv \{\lambda\}$$

$\varphi \to \varphi_2$? hau da $\lambda \to \lambda$? Bai, implikazioa betetzen da, eta ondorioz hasieratzeko aukaitu dugu.

b) Balduitza

(*) Zenbat noiz gelditzen da?

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

↳ ordezkatu, $B \equiv \{i \neq n \wedge \neg q\}$

II. $INB \to def(B)$?

$INB \to def(i \neq n \wedge \neg q)$?

$INB \to True$? Bai, bigarren zatia true delako.

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

$$\lambda \wedge (2 \leq i \leq n) \wedge \underbrace{(q \leftrightarrow \gamma(i))}_{\alpha} \wedge \underbrace{\mu(i-1)}_{\partial} \wedge \overbrace{\underbrace{(i = n \vee q)}_{B \text{ desjuntzio bat denez}}}^{\neg B}$$

$$\downarrow$$

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

$\neg B$ egia izateko 3 aukera daude ele hurrenak osterte behar dira.

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

(*) Lehenengo bi kasuetan $(i=n)$ denez:

$\alpha \equiv q \leftrightarrow Y(i) \equiv q \leftrightarrow Y(n)$ eta $\theta \equiv \mu(i-1) \equiv \mu(n-1)$ dira, ordezkatu

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

$$\downarrow$$

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

α eta θ formulekin badakigu $n-1$ posizioa arte, hori baino, asertzioa ez dela betetzen, beraz asertzio hau eta α baldintza berdina dute; ordezkatu implikazioa betiko da.

(*) $i \neq n$ eta $q = True$ kasua

$$\lambda \wedge \underbrace{(2 \le i \le n)}_{\alpha_1} \wedge \underbrace{(q \leftrightarrow Y(i))}_{\alpha} \wedge \underbrace{\mu(i-1)}_{\theta} \wedge \overbrace{(i=n \vee q)}^{\beta}$$

$$\downarrow$$

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

$i \neq n$ denez α_1-ren badakigu $i < n$ dela eta $q = True$ denez badakigu $Y(i)$ betetzen dela eta beheko asertzioko tontoan betetzen dela:
[$q \leftrightarrow Y(i)$ dela dakigu eta $q = True$]

$$q \overset{?}{\leftrightarrow} \exists k\big((2 \le k \le n) \wedge Y(k)\big) \Rightarrow$$

$$True \overset{?}{\leftrightarrow} \underbrace{\gamma(2) \vee \gamma(3) \vee \dots \vee \gamma(i) \vee \dots \vee \gamma(n)}_{True} \Rightarrow True \overset{?}{\leftrightarrow} \gamma(2) \vee \gamma(3) \vee \dots \vee True \vee \dots \vee \gamma(n) \Rightarrow$$

$$\boxed{\gamma \vee True \equiv True}$$

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

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

$$\overbrace{\lambda \wedge \underbrace{(2 \leq i \leq n)}_{\alpha} \wedge (q \leftrightarrow \gamma(i)) \wedge \mu(i-1)}^{INB} \wedge \overbrace{i \neq n \wedge \neg q}^{B}$$

$$\downarrow$$

$$n - i > 0$$

$i \neq n$ denez B. gatik ete α gatik $i < n$ dela dakigu, beraz $n - i > 0$ betiko da.

E agindua k

Prog. 1

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

Agindua k

$\{INB\}$

$INB \wedge B \rightarrow INB$?

Bai, $INB \wedge B$ egia badira INB ere egia izango da.

Prog 2.

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

Agindua k

$\{E < v\}$

$(INB \wedge B \wedge E = v) \rightarrow E < v$, ez da betiko $E = v$ egia baldin bada. ezin dateke izan ere $E < v$.

Implikazioa ez denez betetzen $E < v$ betetzeko aginduba t egin behar dugu programa honetan. Beltorica eskemetik estimera zehatzatzen ari gorenez E-ren balioa txikitzeko i aldagaiari i+1 balioa esleituko diogu, ete esleitzen ari gara φ_3' formula kalkulatuko dut.

$\boxed{\text{Pros 2}}$

$\{INB \wedge B \wedge E \neq v\}$

$\{\varphi_3'\} \equiv$

$i := i+1$

$\{E < v\}$

$$\{\varphi_3'\} \equiv \{def(i+1) \wedge (E < v)_i^{i+1}\} \equiv \quad // \quad E = n - i \quad // \equiv$$

$$\equiv \{True \wedge n - (i+1) < v\} \equiv$$

$$\equiv \quad n - i - 1 < v$$

Orain $(INB \wedge B \wedge E = v) \rightarrow \varphi_3'$ betetzen den egiartatu

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

$$\downarrow$$

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

Implikazioa betetzen da β epaskoa delako α patik:
$n-i=v$ epea dela dakigunez -1 egiten badugu bi aldeetan ere epea izango da $n-i-1=v-1$, eta $v-1$ balioa v balioa baino txikiagoa da.

Orain Prog 2 zuzena da, baina bi programetan berdina izan behar dugu, beraz, Prog 1-n $i:=i+1$ agindua ipini behar du dut.
EA egin φ_3 formula kalkulatu eta $(INB \wedge B) \to \varphi_3$ betetzen al den aztertu behar du dut.

Prog 1

$\{INB \wedge B\}$
$\{\varphi_3\}$
$i:=i+1;$
EA
$\{INB\}$

$$\{\varphi_3\} \equiv \{def(i+1) \wedge (INB)^{i+1}_{i}\} \equiv$$
$$\equiv \{time \wedge \lambda \wedge (2 \le i+1 \le n) \wedge (q \leftrightarrow \gamma(i+1)) \wedge \mu(i+1-1)\} \equiv$$
$$\equiv \lambda \wedge (2 \overset{-1}{\le} i+1 \overset{-1}{\le} n \overset{-1}{}) \wedge (q \leftrightarrow \gamma(i+1)) \wedge \mu(i)\} \equiv$$
$$\equiv \lambda \wedge (1 \le i \le n-1) \wedge (q \leftrightarrow \gamma(i+1)) \wedge \mu(i)\}$$

Orain $(INB \wedge B) \to \varphi_3$ implikazioa betetzen al den aztertu behar du dugu.

$$\underbrace{\lambda}_{\alpha} \wedge \underbrace{(2 \le i \le n)}_{\alpha_1} \wedge \underbrace{(q \leftrightarrow \gamma(i))}_{\beta} \wedge \underbrace{\mu(i-1)}_{\beta_1} \wedge \underbrace{i \ne n}_{\alpha_2} \wedge \underbrace{\neg q}_{\theta}$$

$$\downarrow$$

$$\underbrace{\lambda}_{\alpha \text{ patik epea}} \wedge \underbrace{(1 \le i \le n-1)}_{\alpha_1 \text{ eta } \alpha_2 \text{ patik epea}} \wedge \underbrace{(q \leftrightarrow \gamma(i+1))} \wedge \underbrace{\mu(i)}$$

β eta θ patik badaukagu i posizioan $\gamma(i)=$ False dela, baina $i+1$ posizioan ez daukagu $\gamma(i+1)$ ren balioa beraz ez da betetzen.

Betetzen da β_1 daukagulako $i-1$ posizioa arte betetzen dela eta θ patik eta β patik badaukagu i posizioan ere betetzen dela.

Beraz, implikazioa ez dutenez betetzen, agindu bat gehituko dugu implikazioa betetzeko, hometarako $i+1$ posizioa azterku behar da, hometorako hasako agindua behar da:

$$q := \gamma(i+1);$$

Esleipena jarri ondoren φ_4 kalkulatuko dut eta $(INB \wedge B) \to \varphi_4$ implikazioa betetzen al den aztertuko dut.

Prog 1

$\{INB \wedge B\}$

EA → $\{\varphi_4\}$

$q := \gamma(i+1);$

$\{\varphi_3\}$

EA → $i = i+1$

$\{INB\}$

$\{\varphi_4\} \equiv \{def(\gamma(i+1)) \wedge (\varphi_3)_q^{\gamma(i+1)}\} \equiv$

$\equiv \{(1 \le i+1 \le n) \wedge \lambda \wedge (1 \le i \le n-1) \wedge \overbrace{(\gamma(i-1) \leftrightarrow \gamma(i+1))}^{True} \wedge \mu(i)\} \equiv$

$\equiv \{(0 \le i \le n-1) \wedge \lambda \wedge (1 \le i \le n-1) \wedge \mu(i)\} \equiv$

$\{\varphi_4\} \equiv \{(1 \le i \le n-1) \wedge \lambda \wedge \mu(i)\}$

$(INB \wedge B) \rightarrow \varphi_4$?

$$\underbrace{\lambda}_{\alpha} \wedge \underbrace{(2 \le i \le n)}_{\alpha_1} \wedge \underbrace{(q \leftrightarrow \gamma(i))}_{\alpha_5} \wedge \underbrace{\mu(i-1)}_{\alpha_3} \wedge \underbrace{i \ne n}_{\alpha_2} \wedge \underbrace{\neg q}_{\alpha_4}$$

$$\downarrow$$

$$\underbrace{\lambda}_{\alpha\text{-gatek}} \wedge \underbrace{(1 \le i \le n-1)}_{\alpha_1 \text{ eta } \alpha_2 \text{ gatek}} \wedge \underbrace{\mu(i)}$$

Lehen esan dugunez α_3-gatek badago aztertuko $i-1$ posizioa ere eta α_4 eta α_5-gatek badaukagu i posizioan ere aztertuko dugula eta betetzen dela.

Beraz, implikazioa bai betetzen da. Orain Prog 1 zuzena da, baina Prog 2-n ere berak izan behar dituguna, eskuepen bera jarri behar dugu eta φ_4' kalkulatu behar da EA. erabiliz eta amaitzeko $(INB \wedge B \wedge E = v) \rightarrow \varphi_4'$ implikazioa betetzen den aztertu behar da.

Prog 2

$\{INB \wedge B \wedge E = v\}$

EA → $\{\varphi_4'\}$

$q := \gamma(i+1);$

EA → $\{\varphi_3'\}$

$i := i+1;$

$\{E < v\}$

$\{\varphi_4'\} \equiv \{def(\gamma(i+1)) \wedge (\varphi_3')_q^{\gamma(i+1)}\} \equiv$

$\equiv \{(1 \le i+1 \le n) \wedge (n-i-1 < v)\} \equiv$

$\{\varphi_4'\} \equiv \{(0 \le i \le n-1) \wedge (n-i-1 < v)\}$

$INB \wedge B \wedge E = v \rightarrow \varphi_4$?

$$\lambda \wedge \underbrace{(2 \le i \le n)}_{\alpha_3} \wedge (q \leftrightarrow \gamma(i)) \wedge \mu(i-1) \wedge \underbrace{i \ne n}_{\alpha} \wedge \neg q \wedge \underbrace{(n-i = v)}_{\alpha_1}$$

$$\downarrow$$

$$\underbrace{0 \le i \le n-1}_{} \wedge \underbrace{n-i-1 < v}_{}$$

α patik $i<n$ dela dakiqe eta α_3 patik

α eta α_1 patik betetzen dira:
α_1 egia dela definiturik $n-i=v$ egia da eta -1 egiaz ere aldatzen $n-i-1 = v-1$ ere egia da, orduan $v-1$ baino v baino txikiagoa da.

ⓓ Programa osoa idatzi

```
{φ}
{φ2}
q := γ(2);
{φ1}
i := 2;
while {INB}{E} i≠n and not q loop
  {φ4}{φ'4}
  q := γ(i+1);
  {φ3}{φ'3}
  i := i+1;
end loop
{ψ}
```