Programazioaren Metodologia

Kudeaketaren eta Informazio Sistemen Informatikaren Ingeniaritzako Gradua
Bilboko Ingeniaritza Eskola (UPV/EHU)
Lengoaia eta Sistema Informatikoak Saila
1. maila
4. gaia: Programak era formalean eratortzeko metodoa
1,5 puntu

1. azterketa-eredua: 4g1e-∃

Ebazpidea

Eguneratze-data: 2020 - 04 - 11

Aurkibidea

Irudien zerrenda

Taulen zerrenda

****

1 Programa iteratibo bat egiaztatzea (*1,5 puntu*)

1.1 Enuntziatua

Osoa den x zenbakia eta 20ren berdinak edo handiagoak diren zenbaki osoz eratuta dagoen $A(1..n)$ bektore ez-hutsa sarrerako datu gisa hartuta, q aldagai boolearrean x balioa $A(1..n)$ bektoreko elementuren baten anizkoitza al den erabakiko duen programa eratorri behar da. Programa eratortzeko, emandako hasierako eta bukaerako baldintzak (φ eta ψ), INB inbariantea eta E espresioa hartu behar dira kontuan eta Hoare-ren kalkuluko While-aren Erregela eta Esleipenaren Axioma erabili behar dira. Lortutako programak eraginkorra izan beharko du, hau da, uneren batean erantzuna baiezkoa izango dela konturatuz gero, programak bukatu egin beharko du gainerako posizioak aztertu gabe.

1 irudian, eratorri beharreko programaren egitura, φ, ψ, INB eta E-ren definizioa eta φ eta INB formuletan erabilitako predikatuaren definizioa daude.

1 irudian, mod eragilea zatiketa osoaren hodarra adierazteko erabili da. Adibideak: $20\ mod\ 3 = 2$, $18\ mod\ 3 = 0$, $19\ mod\ 3 = 1$. Hiru adibide horietan, div eragilearen bidez adieraziko dugun zatiketa osoak 6 balioa itzuliko luke: $20\ div\ 3 = 6$, $18\ div\ 3 = 6$, $19\ div\ 3 = 6$. Zatiketa osoarentzat beste adibide batzuk: $19\ div\ 2 = 9$; $19\ div\ 3 = 6$; $19\ div\ 4 = 4$; $17\ div\ 3 = 5$; $8\ div\ 12 = 0$.

Eratortze-prozesuan, 3. orrialdean dagoen 1 taulan agertzen diren laburdurak erabiltzea komeniko litzateke. Bestalde, 4. orrialdean dagoen 2 taulan, enuntziatu honetan erabili diren letra grekoak jaso dira. Azkenik, 4. orrialdean dagoen 3 taulan, eratortze-prozesuan kontuan hartu beharreko urratsei edo atalei dagozkien puntuazioak ipini dira.

1 irudian eta 1 taulan agertzen diren zenbakizko elementuen bidez adierazitako balioak zenbaki osoak dira. Beraz, elementu horien bidez adierazitako balioak $\mathbb{Z}$ multzokoak dira. $\mathbb{Z}$ multzoa honako multzo hau da: $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$.

Formalki, $\mathbb{Z} = I\!N \cup \{-y \mid y \in I\!N \wedge y \geq 1\}$. Definizio horretan, $I\!N = \{0, 1, 2, 3, \ldots\}$ zenbaki arrunten multzoa da eta $\cup$ multzoen arteko bilketa adierazteko erabili da. Beraz, $\mathbb{Z}$ multzoa $I\!N$ eta $\{-y \mid y \in I\!N \wedge y \geq 1\}$ multzoen arteko bildura da.

Adibidea. (Eratorri beharreko programarentzat. Programa horren egitura, 1 irudian dago) *Har ditzagun $x = 500$ eta honako $A(1..8)$ bektorea:*

A(1..8)	*102*	*50*	*25*	*94*	*25*	*27*	*53*	*72*
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*

Eratorri behar den programak, x eta $A(1..8)$-ren balio horientzat $True$ balio boolearra laga beharko luke q aldagaian. Izan ere, x balioa gutxienez $A(1..8)$ bektoreko elementu baten anizkoitza da. Zehazki, x $A(1..8)$ bektoreko 2, 3 eta 5 posizioetako elementuen anizkoitza da. Eratorri behar den programaren egitura 1 irudian ikus daiteke.

Aldiz, $A(1..8)$ *bektorearen balioak beste hauek balira, orduan programak* $False$ *balio boolearra laga beharko luke* q *aldagaian. Izan ere,* $A(1..n)$ *bektoreko edozein elementu hartzen badugu,* x *ez da bere anizkoitza izango:*

A(1..8)	*102*	*28*	*21*	*136*	*74*	*27*	*62*	*71*
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*

Eratorri beharreko programaren egitura:

$\{\varphi\}$
Hasieraketak?
while $\{INB\}$ $\{E\}$ B? **loop**
    Aginduak?
end loop;
$\{\psi\}$

φ, INB, E eta ψ-ren definizioak:

$\varphi \equiv \quad n \geq 1 \;\wedge\; hogei(A(1..n))$

$INB \equiv \quad n \geq 1 \;\wedge\; hogei(A(1..n)) \;\wedge\; (1 \leq i \leq n+1) \;\wedge$
$\qquad (q \leftrightarrow \exists k(1 \leq k \leq i-1 \;\wedge\; x\ mod\ A(k) = 0))$

$E = \quad n + 1 - i$

$\psi \equiv \quad q \leftrightarrow \exists k(1 \leq k \leq n \;\wedge\; x\ mod\ A(k) = 0)$

Erabilitako predikatuaren definizioa:

$hogei(H(1..r)) \equiv \forall k(1 \leq k \leq r \;\rightarrow\; H(k) \geq 20)$

1 irudia: Eratorri beharreko programaren egitura, φ, INB, E eta ψ-ren definizioak eta erabilitako predikatuaren definizioa.

Honako laburdura hauek erabiltzea aholkatzen da:
$\lambda \equiv n \geq 1 \;\wedge\; hogei(A(1..n))$
$\gamma(\ell) \equiv x\ mod\ A(\ell) = 0$
$\mu(\ell) \equiv \exists k(1 \leq k \leq \ell \;\wedge\; x\ mod\ A(k) = 0)$

1 taula: Aholkatutako laburdurak.

1.2 Erantzuna

Ebazpen honetan erabili diren beste letra grekoak 17. orrialdean dagoen 5 taulan jaso dira.

Enuntziatuan erabili diren letra grekoak:
φ : fi ψ : psi γ : gamma μ : mu λ : lambda

2 taula: Enuntziatuan erabili diren letra grekoen izenak.

Puntuazioa:

(a) While-aren aurreko hasieraketak kalkulatzea: 0,250
(b) While-aren baldintza (B) kalkulatzea: 0,380
    (b.1) $\neg B$ eta B formulatzea: 0,150
    (b.2) While-aren erregelako (II) puntua egiaztatzea: 0,005
    (b.3) While-aren erregelako (IV) puntua egiaztatzea: 0,200
    (b.4) While-aren erregelako (V) puntua egiaztatzea: 0,025
(c) While-aren barruko aginduak kalkulatzea: 0,850
    (c.1) While-aren erregelako (III) puntuari lotutako garapena: 0,550
    (c.2) While-aren erregelako (VI) puntuari lotutako garapena: 0,300
(d) d) Bukaeran programa osoa idaztea: 0,020
 	
■ 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.
 	
■ Ariketa hau gainditzeko, *(a)*, *(b)* eta *(c)* ataletan, atal horietako puntuazioaren erdia lortu beharko da.

3 taula: Puntuazioa atalka.

1.2.1 *(a)* While-aren aurreko hasieraketen kalkulua

While-aren aurretik egin beharreko hasieraketei dagokien atala while-aren erregelako (I) puntuari lotuta dago.

- $\varphi \to INB$?

$$\underbrace{\lambda}_{\varphi} \to \underbrace{\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1))}_{INB}? \tag{1}$$

Inplikazioaren lehenengo zatian (φ formulan) informazioa dugu eta bigarren zatian (INB formulan) lau galdera ditugu: λ? $1 \leq i$? $i \leq n+1$? $q \leftrightarrow \mu(i-1)$?

Inplikazioa betetzen bada, ez da hasieraketarik behar. Aldiz, inplikazioa ez bada betetzen, orduan inplikazioaren bigarren zatiko formulak, hau da INB formulak dioena betearaziko duten esleipenak ipini beharko dira.

2 irudian, hasieraketak kalkulatzeko abiapuntuari dagokion eskema dugu.

- λ? Bai, φ formulan λ dugulako.
- $1 \leq i$? φ formulan dugun informaziotik ezin da $1 \leq i$ ondorioztatu. Ez dakigu $1 \leq i$ egiazkoa al den ala ez.
- $i \leq n+1$? Kasu honetan ere φ formulan dugun informaziotik ezin da $i \leq n+1$ ondorioztatu. Ezin dugu jakin $i \leq n+1$ egiazkoa al den ala ez.
- $q \leftrightarrow \mu(i-1)$? Hau ere ezin da ondorioztatu φ formulan dugun informaziotik. Informazio hori kontuan hartuz ezin dugu erabaki $q \leftrightarrow \mu(i-1)$ betetzen al den ala ez.

Hasieraketak kalkulatzeko, abiapuntuko eskema:	
$\{\varphi\}$	$\varphi \to INB?$
$\{INB\}$	

2 irudia: Hasieraketak kalkulatzeko, abiapuntuko eskema.

Beraz, $\varphi \to INB$ inplikazioa ez da betetzen. Izan ere, φ formulan ez dago ez i-ri eta ez q-ri buruzko informaziorik.

- **Helburua:** INB formulak dioena betearaztea.

  INB formulak dioena betearazteko, esleipen aginduak erabil ditzakegu. INB formulak dioena betearazi behar dugu esleipen aginduen bidez. Balio ezezaguna duten bi aldagai ditugunez, i eta q, bi aldagai horiek hasieratu beharko ditugu. Alde batetik, q aldagaiak $q \leftrightarrow \mu(i-1)$ betetzea nahi dugu, baina i-ren balioa ezagutu gabe ezinezkoa da q-ri zein balio eman behar zaion erabakitzea: $True$ ala $False$. Horregatik, lehenengo i-ren balioa kalkulatuko dugu. φ-gatik, badakigu $n \geq 1$ dela. Ondorioz, $n + 1 \geq 2$ izango da. Informazio hori kontuan hartuz, badakigu i-ri 1 balioa edo $n + 1$ balioa emanez gero, i aldagaiak $1 \leq i$ eta $i \leq n + 1$, propietate biak, beteko dituela. Bi balio horiek (1 eta $n + 1$), INB formulak i-rentzat zehazten duen tartearen mugak dira. Beraz, une honetan bi aukera ditugu: i-ri 1 balioa ematea edo i-ri $n + 1$ balioa ematea. Lehenengo aukera hautatzeak $A(1..n)$ bektorea ezkerretik eskuinera zeharkatzea ekarriko du berarekin. Aldiz, bigarren aukera hautatzen bada, $A(1..n)$ bektorea eskuinetik ezkerrera zeharkatuko da. Hautatuko den aukerak INB formularekin eta, zehazki E espresioarekin bat etorri beharko du.

  E espresioak $n + z - i$ egitura baldin badu, z zenbaki oso bat izanda, bektorea ezkerretik eskuinera zeharkatu behar dela esan nahiko du horrek. E espresioak $i - z$ egitura baldin badu, z zenbaki oso bat izanda, bektorea eskuinetik ezkerrera zeharkatu beharko da.

  Gure kasuan, E espresioak $n + z - i$ egitura du, $z = 1$ izanda. Beraz, $A(1..n)$ bektorea ezkerretik eskuinera zeharkatu behar da.

  Ondorioz, i aldagaia 1 balioarekin hasieratu behar da. Eratortzen edo eraikitzen ari garen programan $i := 1$; esleipena ipini ondoren, esleipen horri dagokion φ_1 formula kalkulatu behar da. Horretarako, INB formulatik abiatuko gara eta esleipenaren axioma (EA) erabiliko dugu.

  3 irudian, i hasieratu ondoren izango dugun egoera edo eskema ikus dezakegu.

Eskema i aldagaia hasieratu ondoren:		
	$\{\varphi\}$	$\varphi \to \varphi_1?$
$\nearrow$	$\{\varphi_1 \equiv def(1) \;\wedge\; INB_i^1\}$	
(EA)	i := 1;	
$\nwarrow$	$\{INB\}$	

3 irudia: i-ren hasieraketa.

- φ_1 formularen kalkulua INB formulatik abiatuta eta esleipenaren axioma (EA) erabilita.

$$
\begin{aligned}
\varphi_1 &\equiv def(1) \;\wedge\; INB_i^1 \\
&\equiv True \;\wedge\; \lambda \;\wedge\; (1 \le 1 \le n+1) \;\wedge\; (q \leftrightarrow \mu(1-1)) \\
&\equiv True \;\wedge\; \lambda \;\wedge\; (1 \le 1) \;\wedge\; (1 \le n+1) \;\wedge\; (q \leftrightarrow \mu(0)) \\
&\equiv True \;\wedge\; \lambda \;\wedge\; True \;\wedge\; (1 \le n+1) \;\wedge\; (q \leftrightarrow \mu(0)) \\
&\equiv \lambda \;\wedge\; (1 \le n+1) \;\wedge\; (q \leftrightarrow \mu(0)) \\
&\equiv \lambda \;\wedge\; (0 \le n) \;\wedge\; (q \leftrightarrow \mu(0))
\end{aligned}
$$

φ_1 sinplifikatzeko, alde batetik $(1 \le 1 \le n+1)$ espresioa deskonposatu da eta $(1 \le 1) \wedge (1 \le n+1)$ espresioa ipini da. Beste aldetik, z edozein zenbaki oso izanda ere, $z \le z$ beti beteko dela kontuan hartu da eta $(1 \le 1)$ espresioaren ordez $True$ ipini da. Gainera, δ logikako edozein formula izanda ere, $True \wedge \delta \equiv \delta$ beteko denez, $True$-ren agerpenak kendu egin dira. Bukatzeko, $1 \le n+1$ espresioaren ordez $0 \le n$ espresio baliokidea ipini da: $1 \le n+1$ espresioko osagai biei 1 kentzen badiegu, $0 \le n$ geldituko baita.

- $\varphi \rightarrow \varphi_1$?

$$
\underbrace{\lambda}_{\varphi} \rightarrow \underbrace{\lambda \;\wedge\; (0 \le n) \;\wedge\; (q \leftrightarrow \mu(0))}_{\varphi_1}? \tag{2}
$$

Inplikazioaren lehenengo zatian (φ formulan), informazioa daukagu eta inplikazioaren bigarren zatian (φ_1 formulan) hiru galdera ditugu: λ? $0 \le n$? $q \leftrightarrow \mu(0)$?

Inplikazio hori betetzen bada, ez dugu beste hasieraketarik beharko. Baina inplikazioa ez bada betetzen, inplikazioa betearaziko duten, eta era zehatzagoan esanda, φ_1 formulak dioena betearaziko duten hasieraketak ipini beharko dira.

  - λ? Bai, φ formulan λ dugulako.
  - $0 \le n$? φ formulak dioenez, $n \ge 1$ betetzen da. n balioa 1 baino handiagoa edo berdina baldin bada, orduan nahitaez, 0 baino handiagoa izango da eta $0 \le n$ beteko da. Ezinezkoa da zenbaki bat 1 baino handiagoa edo berdina izatea eta 0 baino handiagoa edo berdina ez izatea.
  - $q \leftrightarrow \mu(0)$? φ formulan dugun informazioa kontuan hartuz, ezin da $q \leftrightarrow \mu(0)$ ondorioztatu. Beraz, ez dakigu $q \leftrightarrow \mu(0)$ betetzen al den ala ez.

Laburbilduta, $\varphi \rightarrow \varphi_1$ inplikazioa ez da betetzen. φ formulan ez dago q-ri buruzko informaziorik.

- **Helburua:** φ_1 formulak dioena betearaztea.

φ_1 formulak dioena egiazkoa izan dadin, esleipena erabili behar dugu. Era zehatzagoan ipinita, q aldagaiak $q \leftrightarrow \mu(0)$ propietatea betetzea nahi dugu. Propietate horretan, $\mu(0)$-ren esanahia honako hau da:

$$
\exists k (1 \le k \le 0 \;\wedge\; x \; mod \; A(k) = 0) \tag{3}
$$

Formula existentzial horren definizio-eremua, $1 \le k \le 0$, hutsa da. Ondorioz, (3) formula osoaren balioa $False$ da. Hau da, $\mu(0)$-ren balioa $False$ da. Beraz, helburua $q \leftrightarrow False$ betetzea da. Helburu hori lortzeko, q-ri $False$ balioa esleitu beharko diogu.

Eratortzen edo eraikitzen ari garen programan, φ_1 formularen gainean, $q := False$; esleipena ipini ondoren, φ_1 formula, esleipen hori eta esleipenaren axioma (EA) kontuan hartu eta hiru elementu horiei dagokien formula, φ_2 formula, kalkulatu beharko da.

4 irudian, q hasieratu ondoren izango dugun egoera edo eskema ikus dezakegu.

- φ_2 formularen kalkulua φ_1-etik abiatuta eta esleipenaren axioma (EA) erabilita.

Eskema q aldagaia hasieratu ondoren:		
	$\{\varphi\}$	$\varphi \to \varphi_2?$
$\nearrow$	$\{\varphi_2 \equiv def(False) \ \wedge \ (\varphi_1)_q^{False}\}$	
(EA)	q := False;	
$\nearrow$	$\{\varphi_1 \equiv def(1) \ \wedge \ INB_i^1\}$	
(EA)	i := 1;	
$\nwarrow$	$\{INB\}$	

4 irudia: q-ren hasieraketa.

$$\begin{aligned}\varphi_2 \quad &\equiv def(False) \ \wedge \ (\varphi_1)_q^{False} \\ &\equiv True \ \wedge \ \lambda \ \wedge \ (0 \leq n) \ \wedge \ (False \leftrightarrow \mu(0)) \\ &\equiv \lambda \ \wedge \ (0 \leq n) \ \wedge \ (False \leftrightarrow \mu(0))\end{aligned}$$

δ logikako edozein formula izanda ere, $True \wedge \delta \equiv \delta$ beteko denez, $True$-ren agerpena kendu egin da. Horrela, φ_2 sinplifikatu egin da.

- $\varphi \to \varphi_2?$

$$\underbrace{\lambda}_{\varphi} \to \underbrace{\lambda \ \wedge \ (0 \leq n) \ \wedge \ (False \leftrightarrow \mu(0))}_{\varphi_2}? \tag{4}$$

Inplikazio horretako lehenengo zatian (φ formulan) informazioa daukagu eta bigarren zatian (φ_2 formulan), hiru galdera ditugu: λ? $0 \leq n$? $False \leftrightarrow \mu(0)$?

Inplikazioa betetzen bada, hasieraketekin bukatu dugula esan nahiko du horrek. Baina inplikazioa ez bada betetzen, φ_2 formulak dioena betearaziko duten esleipenak beharko dira.

  - λ? Bai, φ formulan λ dugulako.
  - $0 \leq n$? φ formulan, hau da, λ formulan, $n \geq 1$ betetzen dela esaten zaigunez, $0 \leq n$ beteko dela baiezta dezakegu.
  - $False \leftrightarrow \mu(0)$? 6. orrialdeko (3) formulan ikusten den bezala, $\mu(0)$ laburdurak definizio-eremu hutsa duen formula existencial bat adierazten du. Ondorioz, formula horren balioa —eta $\mu(0)$-ren balioa— $False$ da. Beraz, galdera honako hau da: $False \leftrightarrow False$? Erantzuna baiezkoa da. Izan ere, δ edozein formula izanda, $\delta \leftrightarrow \delta \equiv True$ beteko da.

$\varphi \to \varphi_2$ inplikazioa bete egiten dela ikusi dugu: φ formulak φ_2 formula inplikatzen du. Inplikazio hori bete denez, hasieraketekin bukatu dugu.

1.2.2 *(b)* B **baldintzaren kalkulua**

Inbariantetik ateratako informaziotik eraiki edo eratorri behar da $while$-aren B baldintza. Baldintza hori formulatu ondoren, benetan zuzena dela egiaztatu beharko dugu. Horretarako, $while$-aren erregelako (II), (IV) eta (V) puntuei dagozkien inplikazioak aztertu beharko dira.

1.2.2.1 *(b.1)* $\neg B$ **eta** B**-ren formulazioa**

$while$ aginduko B baldintza kalkulatzeko, hasteko $\neg B$ formulatuko da. $\neg B$ espresioak, $while$-a bukatzeko edo $while$-a gelditzeko bete beharreko baldintza adieraziko du. $\neg B$ formulatzeko, *$while$-a noiz geldituko da?* galderari erantzun beharko zaio, edo, bestela, baliokidea den *$while$-etik noiz aterako gara?* galderari erantzun beharko zaio.

Gainetik ikusita, hau da, xehetasunetan sartu gabe, erantzuna honako hau izango da: behin betiko erantzuna ezagutzen denean gelditu beharko dugu $while$-a. Azken batean, q aldagaian itzuli beharreko balioa $True$ ala $False$ den dakigunean.

x zenbakia zatitzen duen $A(1..n)$ bektoreko elementu bat aurkitzen bada, hau da, x balioa $A(1..n)$ bektoreko elementuren baten anizkoitza dela ikusten bada, orduan q aldagaian $True$ balioa itzuli beharko da. Era zehatzagoan adierazita, q aldagaian $True$ balioa itzuli beharko da honako hau betetzen bada: 1 posizioa eta une honetako posizioaren arteko bektore zatiko elementuren batentzat, x anizkoitza baldin bada. Beraz, inbariantean agertzen den $\exists k(1 \leq k \leq i-1 \;\wedge\; x \; mod \; A(k) = 0)$ formularen balioa $True$ baldin bada, $while$-ak gelditu egin beharko du. Gainera, inbariantean ikus daitekeenez, $while$-aren edozein bueltatan, inbariantea betetzen den puntuan gaudenean, formula existentzial horren balioa eta q-ren balioa bat etorriko dira. $\exists k(1 \leq k \leq i-1 \;\wedge\; x \; mod \; A(k) = 0)$ formula existentziala ezin da zuzenean B baldintzan ipini, ez baitago erabiltzen ari garen programazio-lengoaian idatzita. Baina q-ren balioa formula existentzial horren balioarekin bat datorrela jakinda, q erabil daiteke. Ondorioz, programak itzuli beharreko behin betiko balioa $True$ dela jakingo dugu q aldagaiak $True$ balioa hartu bezain laster.

Bestalde, q aldagaiak $False$ balioari eusten badio denbora guztian, baina bektorea bukatzen bada (eskuineko ertzera iritsi garelako), orduan programak itzuli beharreko behin betiko balioa $False$ izango da. Bektorea bukatu dela jakingo dugu i aldagaiak, inbariantearen arabera, har dezakeen azkeneko balioa hartzen duenean.

Laburbilduta, q aldagaiak $True$ balioa hartzen badu edo bektorea bukatu egiten bada (eskuineko ertzera iritsi garelako eta posizio guztiak aztertu direlako eta, beraz, i aldagaiak har dezakeen azken balioa hartu duelako), orduan behin betiko erantzuna edukiko dugu. Behin betiko erantzuna q-ren balioa izango da:

$$\neg B \equiv (q = True) \vee (i = n+1)$$

$\neg B$ lortu ondoren, espresio horri ukapena aplikatu beharko diogu B lortzeko:

$$\begin{aligned} B \;&\equiv \neg(\neg B) \\ &\equiv \neg((q = True) \vee (i = n+1)) \\ &\equiv (\neg(q = True)) \wedge (\neg(i = n+1)) \\ &\equiv (q = False) \wedge (i \neq n+1) \end{aligned}$$

1.2.2.2 *(b.2)* While-aren erregelako (II) puntuaren egiaztapena

B baldintza egokia izateko, $while$-aren erregelako (II) puntuko inplikazioak egiazkoa izan beharko du.

$$\begin{aligned} &INB \rightarrow def(B)? \\ &INB \rightarrow def((q = False) \wedge (i \neq n+1))? \\ &INB \rightarrow True? \end{aligned}$$

Inplikazio horretako lehenengo zatian, INB betetzen dela esaten zaigu eta, bigarren zatian, $True$ betetzen al den galdetzen zaigu. Erantzuna baiezkoa da. Izan ere, $True$ beti betetzen da, hau da $True$ beti $True$ da, eta hori erakitzeko ez dago INB formulan dagoen informazioaren beharrik. Inplikazio hori bete egiten dela justifikatzeko beste bide bat honako hau da: δ edozein formula izanda, $\delta \rightarrow True \equiv True$.

1.2.2.3 *(b.3)* While-aren erregelako (IV) puntuaren egiaztapena

$(INB \;\wedge\; \neg B) \rightarrow \psi?$

$$\underbrace{\lambda \;\wedge\; (1 \leq i \leq n+1) \;\wedge\; (q \leftrightarrow \mu(i-1)) \;\wedge\; ((q = True) \;\vee\; (i = n+1))}_{INB \;\wedge\; \neg B} \rightarrow \underbrace{(q \leftrightarrow \mu(n))}_{\psi}?$$

Inplikazio horretako lehenengo zatian (ezkerreko aldean), informazioa dugu:

$$\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1)) \ \wedge \ ((q = True) \ \vee \ (i = n+1))$$

$(1 \leq i \leq n+1)$ espresioa deskonposatzen badugu, honako hau geldituko zaigu:

$$\underbrace{\lambda}_{\alpha_1} \wedge \underbrace{(1 \leq i)}_{\alpha_2} \wedge \underbrace{(i \leq n+1)}_{\alpha_3} \wedge \underbrace{(q \leftrightarrow \mu(i-1))}_{\alpha_4} \wedge (\underbrace{(q = True)}_{\alpha_5} \vee \underbrace{(i = n+1)}_{\alpha_6})$$

Inplikazio horretako bigarren zatian (eskuineko aldean), galdera bakar bat dugu:

$$q \leftrightarrow \mu(n)?$$

Informazio gehiago edukitzeko, $\alpha_5 \vee \alpha_6$ disjuntziora jo beharko dugu. $\alpha_5 \vee \alpha_6$ disjuntzioa denez, egiazkoa izateko hiru aukera daude: bai α_5 eta bai α_6, biak egiazkoak izatea; edo bakarrik α_5 izatea egiazkoa; edo bakarrik α_6 izatea egiazkoa. Hiru aukera horiek 9. orrialdeko 4 taulan jaso dira.

	α_5	α_6
	$q = True$	$i = n+1$
1	True	True
2	True	False
3	False	True

4 taula: $((q = True) \ \vee \ (i = n+1))$ espresioa egiazkoa izateko dauden hiru aukerak.

- 1 eta 3 kasuak: $i = n+1$

  $i = n+1$ betetzen bada, orduan $i-1 = n$ beteko da eta, ondorioz, α_4 eta ψ formulak formula bera dira. α_4 bete egiten denez, ψ ere bete egingo da.

  Egin dugun dedukzio edo arrazoibide horretan, ez da beharrezkoa q-ren balioa ezagutzea. Berdin zaigu q-ren balioa $True$ edo $False$ izan. Horregatik hain zuzen ere, 9. orrialdeko 4 taulako 1 eta 3 kasuak batera azter daitezke.

- 2 kasua: $q = True$ eta $i \neq n+1$

  $i \neq n+1$ betetzen bada, orduan α_3-gatik $i < n+1$ beteko da, eta baita $i-1 < n$ ere. Ondorioz, α_4 eta ψ ez dira formula bera.

  Gogora dezagun zein den galdera:

  $$q \leftrightarrow \mu(n)? \tag{5}$$

  $\mu(n)$-ren esanahia berreskuratzen badugu, galdera honako hau izango da:

  $$q \leftrightarrow \exists k(1 \leq k \leq n \ \wedge \ x \ mod \ A(k) = 0)? \tag{6}$$

  Formula existentziala disjuntzioaren bidez adierazten badugu, galdera honela geldituko da:

  $$q \leftrightarrow \gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(n)? \tag{7}$$

  α_4-gatik badakigu honako hau egiazkoa dela:

  $$q \leftrightarrow \exists k(1 \leq k \leq i-1 \ \wedge \ x \ mod \ A(k) = 0)$$

Baliokidetasun horretan, formula existentziala disjuntzioaren bidez adierazten badugu, honako espresio hau izango dugu:

$$q \leftrightarrow \gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1) \tag{8}$$

α_3-gatik eta $i \neq n+1$ kasuan egoteagatik, $i-1 \leq n-1$ betetzen dela ziurta dezakegu. Beraz, (8) espresioko gamma kopurua (7) espresioko gamma kopurua baino txikiagoa da.

Hori jakinda, 9. orrialdeko (7) galdera honela berridatz daiteke:

$$q \leftrightarrow \gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1) \ \vee \ \gamma(i) \ \vee \ldots \vee \ \gamma(n)? \tag{9}$$

(9) espresioan 10. orrialdeko (8) espresioan baino gamma gehiago dagoela ikus dezakegu.

$q = True$ eta $i \neq n+1$ kasuan gaudenez, 10. orrialdeko (8) baliokidetasunetik $\gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1)$ disjuntzioaren balioa $True$ dela ondoriozta dezakegu. Beraz, 10. orrialdeko (9) galdera honela berridatz daiteke:

$$True \leftrightarrow True \ \vee \ \gamma(i) \ \vee \ldots \vee \ \gamma(n)? \tag{10}$$

$\gamma(i) \ \vee \ldots \vee \ \gamma(n)$ disjuntzioari buruzko informaziorik ez dugu, baina $True \vee \delta \equiv True$ baliokidetasun logikoa erabiliz, 10. orrialdeko (10) galdera honela geldituko litzateke:

$$True \leftrightarrow True?$$

Galdera horrentzat erantzuna baiezkoa da. Izan ere, δ edozein formula izanda, $\delta \leftrightarrow \delta \equiv True$ betetzen da.

$q = True$ eta $i \neq n+1$ kasuari dagokion dedukzio-prozesuan q aldagaiaren balioa ezagutzea beharrezkoa zaigu.

Guztira, $(INB \ \wedge \ \neg B) \rightarrow \psi$ inplikazioa bete egiten dela ikusi dugu.

1.2.2.4 *(b.4)* **While-aren erregelako** (V) **puntuaren egiaztapena**

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

$$\underbrace{\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1)) \ \wedge \ (q = False) \ \wedge \ (i \neq n+1)}_{INB \ \wedge \ B} \rightarrow \underbrace{(n+1-i > 0)}_{E>0}?$$

Inplikazio horretako lehenengo zatian (ezkerreko aldean, beraz) informazioa dugu:

$$\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1)) \ \wedge \ (q = False) \ \wedge \ (i \neq n+1)$$

$(1 \leq i \leq n+1)$ espresioa deskonposatzen badugu, honako hau geldituko zaigu:

$$\underbrace{\lambda}_{\beta_1} \ \wedge \ \underbrace{(1 \leq i)}_{\beta_2} \ \wedge \ \underbrace{(i \leq n+1)}_{\beta_3} \ \wedge \ \underbrace{(q \leftrightarrow \mu(i-1))}_{\beta_4} \ \wedge \ \underbrace{(q = False)}_{\beta_5} \ \wedge \ \underbrace{(i \neq n+1)}_{\beta_6}$$

Bestalde, inplikazio horretako bigarren zatian (eskuineko aldean, beraz) galdera bakarra dugu:

$$n+1-i > 0?$$

β_3 eta β_6-gatik, $n+1 > i$ egiazkoa dela ondoriozta dezakegu. Alde bietan kenketaren bidez i kentzen badugu, $n+1-i > i-i$ geldituko zaigu. Hor eragiketak eginda, $n+1-i > 0$ geldituko da. Eta hori da lortu nahi genuena. Beraz, inplikazioa bete egiten da.

1.2.3 *(c)* While-aren barruko aginduen kalkulua

Atal honetan, hasieraketen atalean azaldutako ideia bera erabili behar da: beharrezkoak diren inplikazioak aztertutakoan jakingo da esleipen gehiago ipini behar al den ala ez eta, gainera, prozesu horretan parte hartuko duten formulek adieraziko digute zein esleipen ipini behar diren. (III) eta (VI) puntuak aldi berean eraman behar dira, paraleloan. Izan ere, puntu horietan kontsideratu beharreko formulak desberdinak izan arren, kasu bietan esleipen berdinak ipini beharko dira eta esleipen horiek kasu bietarako egokiak izan beharko dute.

1.2.3.1 *(c.1)* eta *(c.2)* While-aren erregelako (III) eta (VI) puntuei lotutako garapenak

1. $(INB \wedge B) \rightarrow INB$? $(INB \wedge B \wedge E = v) \rightarrow E < v$?

   $While$-aren barruan joan behar duten aginduak kalkulatzen hasteko abiapuntua 11. orrialdeko 5 irudian ikus daiteke. $(INB \wedge B) \rightarrow INB$ eta $(INB \wedge B \wedge E = v) \rightarrow E < v$ inplikazioak betetzen badira, orduan ez da egongo esleipenik ipini beharrik. Baina inplikazio horietakoren bat ez bada betetzen, orduan gutxienez esleipen bat ipini beharko da, beti ere inplikazioko bigarren zatiak dioena betearazteko helburuarekin.

(III) puntuari dagokion abiapuntuko eskema:	
$\{INB \wedge B\}$	$(INB \wedge B) \rightarrow INB$?
$\{INB\}$	

(VI) puntuari dagokion abiapuntuko eskema:	
$\{INB \wedge B \wedge E = v\}$	$(INB \wedge B \wedge E = v) \rightarrow E < v$?
$\{E < v\}$	

   5 irudia: (III) eta (VI) puntuei dagozkien abiapuntuko eskemak.

   - $(INB \wedge B) \rightarrow INB$?
     Inplikazio horretan INB eta B betetzen direla esaten zaigu, eta INB betetzen al den galdetzen zaigu. Erantzuna baiezkoa da.
   - $(INB \wedge B \wedge E = v) \rightarrow E < v$? Inplikazio horretan, INB, B eta $E = v$ betetzen direla esaten zaigu eta $E < v$ betetzen al den galdetzen zaigu. Erantzuna ezezkoa da: E-ren balioa v baldin bada, orduan E-ren balioa ezin daiteke izan aldi berean v baino txikiagoa.

   $(INB \wedge B) \rightarrow INB$ inplikazioa betetzen denez, (III) puntuari dagokionez ez da esleipenik behar. Baina $(INB \wedge B \wedge E = v) \rightarrow E < v$ inplikazioa ez denez betetzen, (VI) puntuari dagokionez esleipen baten beharra dago $E < v$ bete dadin.

2. **Helburua:** $E < v$ betearaztea:
   $E = v$ betetzen dela jakinda, hau da, $n + 1 - i = v$ betetzen dela jakinda, helburua $n + 1 - i < v$ betearaztea da.

   $n + 1 - i$ espresioak, une honetako posizioa (i aldagaiak adierazten duen posizioa) eta helmugaren ($n + 1$ balioaren) arteko distantzia adierazten du. Hasieraketen atalean ikusi dugu bektorea ezkerretik eskuinera zeharkatu behar dela eta, horrek esan nahi du i-ren balioa handituz joango dela. Une honetan i-ren balioari 1 balioa gehitzen badiogu, helmuga den $n + 1$ balioa eta i-ren arteko distantzia txikiagoa izatea lortuko dugu.

Beraz, $i := i + 1$; esleipena ipini behar dela ondorioztatu dugu.

Esleipen hori, bai (III) puntuan eta baita (VI) puntuan ere, bietan, ipini behar da. Izan ere, (III) eta (VI) puntuetan agindu berdinak eduki behar ditugu. Esleipena ipini ondoren, bai (III) puntuan eta bai (VI) puntuan, bietan, esleipenaren axioma (EA) erabili beharko da formula berriak kalkulatzeko.

3. φ_3 eta φ_4-ren kalkulua:

   - φ_3 formularen kalkulua INB formulatik abiatuta eta esleipenaren axioma (EA) erabilita.

     $$\begin{aligned} \varphi_3 &\equiv def(i+1) \ \wedge \ INB_i^{i+1} \\ &\equiv True \ \wedge \ \lambda \ \wedge \ (1 \leq i+1 \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i+1-1)) \\ &\equiv \lambda \ \wedge \ (0 \leq i \leq n) \ \wedge \ (q \leftrightarrow \mu(i)) \end{aligned}$$

     φ_3 formula sinplifikatzeko, δ edozein formula izanda ere, $True \wedge \delta \equiv \delta$ beteko dela kontuan hartu da eta $True$ ezabatu da. Bestalde, $(1 \leq i+1 \leq n+1)$ espresioko hiru osagaietan kenketa aplikatu da (ken 1) eta $(0 \leq i \leq n)$ espresioa gelditu da.

   - φ_4 formularen kalkulua $E < v$ formulatik abiatuta eta esleipenaren axioma (EA) erabilita.

     $$\begin{aligned} \varphi_4 &\equiv def(i+1) \ \wedge \ (E < v)_i^{i+1} \\ &\equiv True \ \wedge \ (n+1-(i+1) < v) \\ &\equiv True \ \wedge \ (n+1-i-1 < v) \\ &\equiv (n-i < v) \end{aligned}$$

     φ_4 formula sinplifikatzeko, δ edozein formula izanda ere, $True \wedge \delta \equiv \delta$ beteko dela kontuan hartu da eta $True$ ezabatu da. Gainera, $(n+1-(i+1) < v)$ espresioa eraldatu da eta $(n-i < v)$ espresioa lortu da. Horretarako, $(i+1)$ espresioari zeinu negatiboa aplikatu zaio eta, gero, 1-1 kenketa egin da.

12. orrialdeko 6 irudian, i eguneratu ondoren (III) eta (VI) puntuei dagozkien eskemak erakusten dira. φ_3 eta φ_4 kalkulatu ondoren, $(INB \wedge B) \rightarrow \varphi_3$ eta $(INB \wedge B \wedge E = v) \rightarrow \varphi_4$ inplikazioak aztertu behar dira.

(III) puntuari dagokion eskema i eguneratu ondoren:

$\{INB \ \wedge \ B\}$ $\qquad$ $(INB \ \wedge \ B) \rightarrow \varphi_3?$

$\nearrow$ $\quad \{\varphi_3 \equiv def(i+1) \ \wedge \ INB_i^{i+1}\}$
(EA) $\quad$ i := i + 1;
$\nwarrow$ $\quad \{INB\}$

(VI) puntuari dagokion eskema i eguneratu ondoren:

$\{INB \ \wedge \ B \ \wedge \ E = v\}$ $\qquad$ $(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_4?$

$\nearrow$ $\quad \{\varphi_4 \equiv def(i+1) \ \wedge \ (E < v)_i^{i+1}\}$
(EA) $\quad$ i := i + 1;
$\nwarrow$ $\quad \{E < v\}$

6 irudia: (III) eta (VI) puntuei dagozkien eskemak i eguneratu ondoren.

4. $(INB \wedge B) \rightarrow \varphi_3$? $(INB \wedge B \wedge E = v) \rightarrow \varphi_4$?

- Inplikazioa egiaztatu: $(INB \wedge B) \rightarrow \varphi_3$?
  $\lambda \wedge (1 \leq i \leq n+1) \wedge (q \leftrightarrow \mu(i-1)) \wedge (q = False) \wedge (i \neq n+1) \rightarrow$
  $\lambda \wedge (0 \leq i \leq n) \wedge (q \leftrightarrow \mu(i))$?

  Inplikazio horretako lehenengo zatian (ezkerreko aldean edo lehenengo lerroan), informazioa daukagu:

  $$\lambda \wedge (1 \leq i \leq n+1) \wedge (q \leftrightarrow \mu(i-1)) \wedge (q = False) \wedge (i \neq n+1)$$

  $(1 \leq i \leq n+1)$ deskonposatzen badugu, honako hau geldituko zaigu:

  $$\underbrace{\lambda}_{\alpha_1} \wedge \underbrace{(1 \leq i)}_{\alpha_2} \wedge \underbrace{(i \leq n+1)}_{\alpha_3} \wedge \underbrace{(q \leftrightarrow \mu(i-1))}_{\alpha_4} \wedge \underbrace{(q = False)}_{\alpha_5} \wedge \underbrace{(i \neq n+1)}_{\alpha_6}$$

  Inplikazio horretako bigarren zatian (eskuineko aldean edo bigarren lerroan), lau galdera ditugu: λ? $0 \leq i$? $i \leq n$? $q \leftrightarrow \mu(i)$?

  – λ? Bai, α_1-gatik.
  – $0 \leq i$? Bai, α_2-gatik.
  – $i \leq n$? Bai, α_3 eta α_6-gatik.
  – $q \leftrightarrow \mu(i)$? $\mu(i)$-ren esanahia kontuan hartzen badugu, galdera honela geldituko zaigu:

  $$q \leftrightarrow \exists k(1 \leq k \leq i \wedge x \; mod \; A(k) = 0)?$$

  Horko formula existentzial hori disjuntzio gisa adierazten badugu, galdera honako era honetan geldituko zaigu:

  $$q \leftrightarrow (\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1) \vee \gamma(i))? \tag{11}$$

  α_4-gatik, badakigu honako hau betetzen dela:

  $$q \leftrightarrow \exists k(1 \leq k \leq i-1 \wedge x \; mod \; A(k) = 0)$$

  Horko formula existentziala disjuntzioaren bidez adierazten badugu, honako hau geldituko zaigu:

  $$q \leftrightarrow (\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1))$$

  α_5-gatik, badakigu q-ren balioa $False$ dela. Beraz, $\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1)$ ere $False$ izango da.

  Bukaeran, (11) galdera honela gelditu da:

  $$False \leftrightarrow (False \vee \gamma(i))? \tag{12}$$

  δ edozein formula izanda ere, $False \vee \delta \equiv \delta$ denez, (12) galdera honela geldituko da:

  $$False \leftrightarrow \gamma(i)? \tag{13}$$

  $\gamma(i)$ laburdurak $(x \; mod \; A(i) = 0)$ adierazten duenez:

  $$False \leftrightarrow (x \; mod \; A(i) = 0)? \tag{14}$$

  $INB \wedge B$ formulan ez dugu galdera horri erantzuteko erabil dezakegun informaziorik. Ondorioz, $(INB \wedge B) \rightarrow \varphi_3$ inplikazioa ez da betetzen.

$(INB \ \wedge \ B) \rightarrow \varphi_3$ ez dela betetzen frogatu dugu.

- Inplikazioa egiaztatu: $(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_4$?
$$\underbrace{\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1))}_{INB} \wedge \underbrace{(q = False) \ \wedge \ (i \neq n+1)}_{B} \wedge$$
$$\underbrace{(n+1-i = v)}_{E=v} \rightarrow \underbrace{(n-i < v)}_{\varphi_4}?$$

Inplikazioko lehenengo zatian informazioa dugu:
$$\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1)) \ \wedge \ (q = False) \ \wedge \ (i \neq n+1) \wedge$$
$$(n+1-i = v)$$

$(1 \leq i \leq n+1)$ deskonposatzen badugu, honako hau izango dugu:
$$\underbrace{\lambda}_{\alpha_1} \wedge \underbrace{(1 \leq i)}_{\alpha_2} \wedge \underbrace{(i \leq n+1)}_{\alpha_3} \wedge \underbrace{(q \leftrightarrow \mu(i-1))}_{\alpha_4} \wedge \underbrace{(q = False)}_{\alpha_5} \wedge \underbrace{(i \neq n+1)}_{\alpha_6}$$
$$\wedge \underbrace{(n+1-i = v)}_{\alpha_7}$$

Inplikazioko bigarren zatian galdera bakarra daukadu: $n - i < v$?

– $n - i < v$? α_7-gatik, badakigu $(n + 1 - i = v)$ betetzen dela. Berdintza horren alde bietan kenketaren bidez 1 kentzen badugu, $(n+1-i-1 = v-1)$ geldituko zaigu, hau da, $(n - i = v - 1)$. z edozein zenbaki oso izanda ere, $z - 1 < z$ beteko denez, $v - 1 < v$ ere beteko da. Beraz, $(n - i < v)$ betetzen dela ondoriozta dezakegu.

$(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_4$ bete egiten dela egiaztatu dugu.

$(INB \ \wedge \ B) \rightarrow \varphi_3$ inplikazioa ez denez betetzen, (III) puntuan beste esleipen baten beharra dugu, φ_3 formulak dioena bete dadin. Bestalde, $(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow E < v$ inplikazioa betetzen denez, (VI) puntuan ez dago beste esleipenen beharrik.

5. **Helburua:** φ_3 betearaztea:
$INB \ \wedge \ B$ formulak φ_3 ez duela inplikatzen ikusi dugu. Era zehatzagoan esanda, φ_3 formularen barruan betetzen ez den osagaia $q \leftrightarrow \mu(i)$ da. $\mu(i)$-ren esanahia kontuan hartzen badugu, betetzen ez dena honako baliokidetasun hau da:
$$q \leftrightarrow (\gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1) \vee \ \gamma(i))?$$
α_4-gatik, badakigu honako hau betetzen dela:
$$q \leftrightarrow (\gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1))$$
q-ren balioa eta $\gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1)$ disjuntzioaren balioa bat datozela jakinda eta helburua q-ren balioa eta $\gamma(1) \ \vee \ \gamma(2) \ \vee \ldots \vee \ \gamma(i-1) \vee \ \gamma(i)$ disjuntzioaren balioa bat etortzea dela jakinda, q-ri falta zaiona $\vee \ \gamma(i)$ da.

Beraz, honako esleipen hau behar dugu $q := q \vee \gamma(i)$;.

Esleipen hori (III) puntuan —φ_3-ren gainean— eta (VI) puntuan —φ_4-ren gainean— ipini behar da, (III) eta (VI) puntuetan agindu berdinak eduki behar direlako. Esleipen hori ipini ondoren, esleipenaren axioma (EA) erabili behar da (III) eta (VI) puntuetan formula berriak kalkulatzeko.

α_5-gatik q-ren balioa $False$ dela badakigunez, eta δ edozein formula izanda ere, $False \vee \delta \ \equiv \ \delta$ beteko dela kontuan hartuta, esleipena honela ipin daiteke: $q := \gamma(i)$;. Hala ere, hurrengo ataletan $q := q \vee \gamma(i)$; erabiliko da eta ez $q := \gamma(i)$; esleipena.

6. φ_5 eta φ_6 kalkulatu:

   - φ_5 formularen kalkulua φ_3-tik abiatuta eta esleipenaren axioma (EA) erabilita.

$$\begin{aligned}\varphi_5 &\equiv def(q \vee \gamma(i)) \;\wedge\; (\varphi_3)_q^{q\vee\gamma(i)}\\ &\equiv def(q \vee (x \; mod \; A(i) = 0)) \;\wedge\; \lambda \;\wedge\; (0 \le i \le n) \;\wedge\; ((q \vee \gamma(i)) \leftrightarrow \mu(i))\\ &\equiv (1 \le i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; \lambda \;\wedge\; (0 \le i \le n) \;\wedge\; ((q \vee \gamma(i)) \leftrightarrow \mu(i))\\ &\equiv (1 \le i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; \lambda \;\wedge\; ((q \vee \gamma(i)) \leftrightarrow \mu(i))\\ &\equiv (1 \le i) \;\wedge\; (i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; \lambda \;\wedge\; ((q \vee \gamma(i)) \leftrightarrow \mu(i))\end{aligned}$$

   i-rentzat bi tarte sortu dira φ_5 kalkulatzean: $(1 \le i \le n)$ eta $(0 \le i \le n)$. φ_5 sinplifikatzeko, i-rentzat tarte bakarra laga da. Tarte bakarra finkatzeko, beheko mugetatik handiena (1) eta goiko mugetatik txikiena (n) hartu behar dira. Bukatzeko, $(1 \le i \le n)$ espresioa bi zatitan banandu da: $(1 \le i)$ eta $(i \le n)$.

   - φ_6 formularen kalkulua φ_4-tik abiatuta eta esleipenaren axioma (EA) erabilita.

$$\begin{aligned}\varphi_6 &\equiv def(q \vee \gamma(i)) \;\wedge\; (\varphi_4)_q^{q\vee\gamma(i)}\\ &\equiv def(q \vee (x \; mod \; A(i) = 0)) \;\wedge\; (n - i < v)_q^{q\vee\gamma(i)}\\ &\equiv (1 \le i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; (n - i < v)\\ &\equiv (1 \le i) \;\wedge\; (i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; (n - i < v)\end{aligned}$$

   φ_6-ren azkeneko bertsioa lortzeko, $(1 \le i \le n)$ espresioa bi zatitan deskonposatu da: $(1 \le i)$ eta $(i \le n)$.

   16. orrialdeko 7 irudian, q eguneratu ondoren (III) eta (VI) puntuei dagozkien eskemak erakusten dira. φ_5 eta φ_6 kalkulatu ondoren, $(INB \wedge B) \rightarrow \varphi_5$ eta $(INB \wedge B \wedge E = v) \rightarrow \varphi_6$ inplikazioak aztertu behar dira.

7. $(INB \wedge B) \rightarrow \varphi_5$? $(INB \wedge B \wedge E = v) \rightarrow \varphi_6$?

   - Inplikazioa egiaztatu: $(INB \wedge B) \rightarrow \varphi_5$?

$$\underbrace{\lambda \;\wedge\; (1 \le i \le n+1) \;\wedge\; (q \leftrightarrow \mu(i-1))}_{INB} \wedge \underbrace{(q = False) \;\wedge\; (i \ne n+1)}_{B} \rightarrow$$
$$\underbrace{(1 \le i) \;\wedge\; (i \le n) \;\wedge\; (A(i) \ne 0) \;\wedge\; \lambda \;\wedge\; ((q \vee \gamma(i)) \leftrightarrow \mu(i))}_{\varphi_5}?$$

   Inplikazio horretako lehenengo zatian (ezkerreko aldean edo lehenengo lerroan), informazioa dugu:

$$\lambda \;\wedge\; (1 \le i \le n+1) \;\wedge\; (q \leftrightarrow \mu(i-1)) \;\wedge\; (q = False) \;\wedge\; (i \ne n+1)$$

   $(1 \le i \le n+1)$ deskonposatzen badugu, honako hau izango dugu:

$$\underbrace{\lambda}_{\alpha_1} \wedge \underbrace{(1 \le i)}_{\alpha_2} \wedge \underbrace{(i \le n+1)}_{\alpha_3} \wedge \underbrace{(q \leftrightarrow \mu(i-1))}_{\alpha_4} \wedge \underbrace{(q = False)}_{\alpha_5} \wedge \underbrace{(i \ne n+1)}_{\alpha_6}$$

   Bestalde, inplikazioko bigarren zatian (eskuineko aldean edo bigarren lerroan), bost galdera ditugu: $0 \le i$? $i \le n$? $(A(i) \ne 0)$? λ? $(q \vee \gamma(i)) \leftrightarrow \mu(i)$?

     – $0 \le i$? Bai, α_2-gatik.
     – $i \le n$? Bai, α_3 eta α_6-gatik.
     – $A(i) \ne 0$? α_1-en, hau da, λ-ren barruan, $A(1..n)$ bektoreak $hogei(A(1..n))$ betetzen duela esaten zaigu. Beraz, $A(1..n)$ bektoreko elementu guztiak 20ren berdinak edo handiagoak dira. Ondorioz, $A(1..n)$ bektoreko elementu guztiak zeroren desberdinak dira. Hori jakinda, $A(i)$ zeroren desberdina dela ziurta dezakegu.

(III) puntuari dagokion eskema q eguneratu ondoren:		
	$\{INB \wedge B\}$	$(INB \wedge B) \rightarrow \varphi_5?$
$\nearrow$	$\{\varphi_5 \equiv def(q \vee \gamma(i)) \wedge (\varphi_3)_q^{q\vee\gamma(i)}\}$	
(EA)	q := $q \vee \gamma(i)$;	
$\nearrow$	$\{\varphi_3 \equiv def(i+1) \wedge INB_i^{i+1}\}$	
(EA)	i := i + 1;	
$\nwarrow$	$\{INB\}$	

(VI) puntuari dagokion eskema q eguneratu ondoren:		
	$\{INB \wedge B \wedge E = v\}$	$(INB \wedge B \wedge E = v) \rightarrow \varphi_6?$
$\nearrow$	$\{\varphi_6 \equiv def(q \vee \gamma(i)) \wedge (\varphi_4)_q^{q\vee\gamma(i)}\}$	
(EA)	q := $q \vee \gamma(i)$;	
$\nearrow$	$\{\varphi_4 \equiv def(i+1) \wedge (E < v)_i^{i+1}\}$	
(EA)	i := i + 1;	
$\nwarrow$	$\{E < v\}$	

$\gamma(i)$ laburdura erabili da $(x \ mod \ A(i) = 0)$ adierazteko.

7 irudia: (III) eta (VI) puntuei dagozkien eskemak q eguneratu ondoren.

- λ? Bai, α_1-gatik.
- $(q \vee \gamma(i)) \leftrightarrow \mu(i)$? $\mu(i)$-ren esanahia kontuan hartzen badugu, galdera hori honela adieraz daiteke:

$$(q \vee \gamma(i)) \leftrightarrow \exists k(1 \leq k \leq i \wedge x \ mod \ A(k) = 0)?$$

Hor, formula existentziala disjuntzioaren bidez adierazten badugu, galdera honako era honetara idatz dezakegu:

$$(q \vee \gamma(i)) \leftrightarrow (\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1) \vee \gamma(i))? \tag{15}$$

α_4-gatik, honako hau betetzen dela badakigu:

$$q \leftrightarrow \exists k(1 \leq k \leq i-1 \wedge x \ mod \ A(k) = 0)$$

Baliokidetasun horretako formula existentziala disjuntzioen bidez adierazten badugu, honako hau geldituko zaigu:

$$q \leftrightarrow (\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1))$$

α_5-gatik, badakigu q-ren balioa $False$ dela. Beraz, $\gamma(1) \vee \gamma(2) \vee \ldots \vee \gamma(i-1)$ ere $False$ da.

Azkenean, (15) galdera honela gelditu zaigu:

$$(False \vee \gamma(i)) \leftrightarrow (False \vee \gamma(i))? \tag{16}$$

δ edozein formula izanda ere, $False \vee \delta \equiv \delta$ betetzen denez, (16) galdera honako hau da:

$$\gamma(i) \leftrightarrow \gamma(i)? \tag{17}$$

Erantzuna baiezkoa da. Izan ere, δ edozein formula izanda ere, $\delta \leftrightarrow \delta \equiv True$ beteko da.

$(INB \ \wedge \ B) \rightarrow \varphi_5$ inplikazioa bete egiten dela egiaztatu dugu.

- Inplikazioa egiaztatu: $(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_6$?

$$\underbrace{\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1))}_{INB} \wedge \underbrace{(q = False) \ \wedge \ (i \neq n+1)}_{B} \wedge$$
$$\underbrace{(n+1-i=v)}_{E=v} \rightarrow \underbrace{(1 \leq i) \ \wedge \ (i \leq n) \ \wedge \ (A(i) \neq 0) \ \wedge \ (n-i<v)}_{\varphi_6}?$$

Inplikazio horretako lehenengo zatian informazioa dugu:

$$\lambda \ \wedge \ (1 \leq i \leq n+1) \ \wedge \ (q \leftrightarrow \mu(i-1)) \ \wedge \ (q = False) \ \wedge \ (i \neq n+1) \wedge$$
$$(n+1-i=v)$$

$(1 \leq i \leq n+1)$ deskonposatzen badugu, honako hau izango dugu:

$$\underbrace{\lambda}_{\alpha_1} \ \wedge \ \underbrace{(1 \leq i)}_{\alpha_2} \ \wedge \ \underbrace{(i \leq n+1)}_{\alpha_3} \ \wedge \ \underbrace{(q \leftrightarrow \mu(i-1))}_{\alpha_4} \ \wedge \ \underbrace{(q = False)}_{\alpha_5} \ \wedge \ \underbrace{(i \neq n+1)}_{\alpha_6}$$
$$\wedge \ \underbrace{(n+1-i=v)}_{\alpha_7}$$

Bestalde, inplikazioko bigarren zatian lau galdera ditugu: $0 \leq i$? $i \leq n$? $(A(i) \neq 0)$? $n-i<v$?

- $0 \leq i$? Bai, α_2-gatik.
- $i \leq n$? Bai, α_3 eta α_6-gatik.
- $A(i) \neq 0$? α_1-en, hau da, λ-ren barruan, $A(1..n)$ bektoreak $hogei(A(1..n))$ betetzen duela esaten zaigu. Beraz, $A(1..n)$ bektoreko elementu bakoitza 20ren berdina edo handiagoa da. Ondorioz, $A(1..n)$ bektoreko elementu guztiak zeroren desberdinak dira. Hori jakinda, $A(i)$ zeroren desberdina izango da.
- $n-i<v$? α_7-gatik, badakigu $(n+1-i=v)$ betetzen dela. Berdintza horren alde bietan kenketaren bidez 1 kentzen badugu, $(n+1-i-1=v-1)$ geldituko zaigu, hau da, $(n-i=v-1)$. z edozein zenbaki oso izanda ere, $z-1<z$ beteko denez, $v-1<v$ ere beteko da. Beraz, $(n-i<v)$ betetzen dela ondoriozta dezakegu.

$(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_6$ inplikazioa bete egiten dela egiaztatu dugu.

$(INB \ \wedge \ B) \ \rightarrow \varphi_5$ eta $(INB \ \wedge \ B \ \wedge \ E = v) \rightarrow \varphi_6$ inplikazioak betetzen direnez, ez da beste esleipenik behar. Beraz, eratortze-prozesua bukatu da.

1.2.4 *(d)* Eratorritako programa

Eratorri den programa 8 irudian dugu. Eratortze-prozesuan kalkulatu diren formulak ere irudi horretan ikus daitezke.

Erantzunen atalean erabili diren beste letra grekoak:
α : alfa β : beta δ : delta

5 taula: Erantzunen atalean erabili diren beste letra grekoen izenak.

Eratorritako programa:

$\{\varphi\}$
$\{\varphi_2\}$
q := False;
$\{\varphi_1\}$
i := 1;
while $\{INB\}$ $\{E\}$ **not** q **and** i $\neq$ n + 1 **loop**
$\{\varphi_5\}$ $\{\varphi_6\}$
    q := (q **or** (x mod A(i) = 0));
$\{\varphi_3\}$ $\{\varphi_4\}$
    i := i + 1;
end loop;
$\{\psi\}$

8 irudia: Eratorritako programa.