3. PROGRAMEN EGIAZTAPENA

3.1. Hoare-ren sistema formala.
3.2. Asignazioa.
3.3. Konposaketa sekuentziala.
3.4. Baldintzazko sententziak.
3.5. Iterazioak: inbarianteak.
3.6. Iterazioen bukaera.
3.7. Programa errekurtsiboak.

3.1. Hoare-ren sistema formala.

▪Programen zuzentasun partziala eta totala

▪$\{\phi\}P\{\psi\}$ ≡ P <u>partzialki zuzena</u> da (ϕ , ψ) espezifikazioarekiko

≡ ϕ *betetzen den egoera batean hasten den Pren edozein konputazio, bukatzen bada,* ψ *betetzen den egoera batean bukatzen da.*

▪Buka(ϕ , P) ≡ ϕ *betetzen den egoera batean hasten den Pren edozein konputazio pauso kopuru finituan <u>bukatzen da</u>.*

▪$\{\phi\}[P]\{\psi\}$ ≡ P <u>osoki zuzena</u> da (φ, ψ) espezifikazioarekiko

≡ φ *betetzen den egoera batean hasten den Pren edozein konputazio,* ψ *betetzen den egoera batean bukatzen da.*

$$\boxed{\{\varphi\}[P]\{\psi\} \equiv \{\varphi\}P\{\psi\} + \text{Buka}(\varphi, P)}$$

SISTEMA FORMALAK

Sistema formala:

- Axiomak: *Egiazkoak diren oinarrizko propietateak*
- Inferentzi erregelak: *Nola deduzitu propietate batzuk besteetatik*

$$\frac{P_1, P_2, \ldots, P_n}{P}$$

Frogapena sistema formal batean:

- $P_1, P_2, \ldots, P_{i-1}, P_i, \ldots, P_k$ non:

  P_k den frogatzen den propietatea

  eta P_i $(1 \leq i \leq k)$ bakoitza den:

  - axioma bat edo
  - aurreko $P_1, P_2, \ldots, P_{i-1}$ propietateetatik deduzitzen den propietatea inferentzi erregela baten bitartez

HOARE-REN SISTEMA FORMALA

- Propietateak $\{\varphi\}P\{\psi\}$ motako baieztapenak dira, hau da, zuzentasun partzialari buruzko baieztapenak.

$\{x=a \land y=b\}$
lag:= x;
x:= y;
y:= lag;
$\{x=b \land y=a\}$
frogagarria da

$\{true\}$
lag:= x;
x:= y;
y:= lag;
$\{x = y\}$
<u>*ez*</u> *da frogagarria*

HOARE-REN SISTEMA FORMALA (II)

- Osaera:
  - axiomak: $\{\varphi\}P\{\psi\}$

    oinarrizko propietateak,

    esate baterako, P asignazioa denean

  - honelako inferentzi erregelak

$$\frac{\{\ldots\}\ P_1\ \{\ldots\}\ \ ,\ \ \{\ldots\}\ P_2\ \{\ldots\}}{\{\ldots\}\ P_1 \times P_2\ \{\ldots\}}$$

programak konposatzeko dauden moduetarako

- Programazio-lengoaien semantika axiomatikoa

3.2.- ASIGNAZIOA

- Asignazioaren axioma. (Hoare-ren kalkulua)

(AA) $\boxed{\{\mathbf{def\ (t)} \wedge \psi_x^{\,t}\}\ \ \mathbf{x := t;}\ \ \{\ \psi\ \}}$

<u>Adibidea</u> A(1..n) osokoen bektorea

$$\{\underbrace{1 \le i \le n}_{\text{def (A(i)) =def (t)}} \wedge \underbrace{A(i) > 0}_{\psi_x^{\,t}}\}\ \ x := \underbrace{A(i)}_{t};\ \ \{\ \underbrace{x > 0}_{\psi}\}$$

Beste adibide bat:

$$\{ z \neq 0 \ \wedge \ y/z \neq 1\} \ x:= y/z; \ \{ x \neq 1 \}$$

Def(y/z)?

Frogatu al daiteke honako hau?

$$\{ z \neq 0 \ \wedge \ y = 0\} \ x:= y/z; \ \{ x \neq 1 \}$$

Bai. ODE erabiliz. Izan ere,

$$(z \neq 0 \ \wedge \ y = 0) \rightarrow (z \neq 0 \ \wedge \ y/z \neq 1)$$

Hoare-ren kalkulua

Aurreko adibidea tratatzeko inferentzi erregela bat behar dugu:

Ondorioaren erregela

(ODE)

$$\frac{\varphi \to \varphi_1\ ,\ \{\varphi_1\}\ P\ \{\psi_1\},\ \psi_1 \to \psi}{\{\varphi\}\ P\ \{\psi\}}$$

Eta bere bi aldaera:

$$\frac{\varphi \to \varphi_1\ ,\ \{\varphi_1\}\ P\ \{\psi\}}{\{\varphi\}\ P\ \{\psi\}}$$

$$\frac{\{\varphi\}\ P\ \{\psi_1\},\ \psi_1 \to \psi}{\{\varphi\}\ P\ \{\psi\}}$$

Adibidea:

A(1..n) osokoen arraya izanik,

$$posit(A(1..n)) \equiv \forall i\ (1 \le i \le n \rightarrow A(i) > 0)$$

Frogatu al daiteke honako hau:

$\{1 \le j \le n \wedge posit(A(1..n))\}$ $x := A(j);$ $\{x > 0\}$?

1.-$\{ 1 \le j \le n \wedge A(j) > 0\}$ $x := A(j);$ $\{ x > 0\}$ (AA)

2.-$(1 \le j \le n \wedge posit(A(1..n))) \rightarrow (1 \le j \le n \wedge A(j) > 0)$

3.-$\{1 \le j \le n \wedge posit(A(1..n))\}$

$x := A(j);$

$\{x > 0\}$ 1,2 eta (ODE)

Egiaztapen-adibideak

$\{1 \le i < n\}$ i:= i+1; $\{1 \le i \le n\}$

Hoare-ren kalkulua:

1.- $1 \le i < n \rightarrow 1 \le i+1 \le n$

2.- $\{1 \le i+1 \le n\}$ i:= i+1; $\{1 \le i \le n\}$ (AA)

3.- $\{1 \le i < n\}$ i:= i+1; $\{1 \le i \le n\}$ 1, 2, eta (ODE)

Egiaztapen-adibideak (II)

$\{z=1 \wedge x > 0\}$ y:= 0; $\{z = x^y \wedge y \geq 0\}$

Hoare-ren kalkulua

1.- $z = 1 \wedge x > 0 \rightarrow z = x^0$

2.- $\{z = x^0\}$ y:= 0; $\{z = x^y \wedge y = 0\}$ (AA)

3.- $(z = x^y \wedge y = 0) \rightarrow (z = x^y \wedge y \geq 0)$

4.- $\{z=1 \wedge x > 0\}$ y:= 0; $\{z = x^y \wedge y \geq 0\}$ 1, 2, 3, eta (ODE)

Egiaztapen-adibideak (III)

$\{b \wedge \text{Posit}(A(1..i)) \wedge 1 \leq i < n \wedge A(i+1) < 0\}$

b:= False;

$\{b \leftrightarrow \text{Posit}(A(1..i+1))\}$

Hoare-ren kalkulua

1.- $(b \wedge \text{Posit}(A(1..i)) \wedge 1 \leq i < n \wedge A(i+1) < 0)$

$\rightarrow (1 \leq i < n \wedge A(i+1) < 0)$

2.- $\{1 \leq i < n \wedge A(i+1) < 0\}$ b:= False;

$\{\neg b \wedge 1 \leq i < n \wedge A(i+1) < 0\}$ (AA)

3.- $(\neg b \wedge 1 \leq i < n \wedge A(i+1) < 0)$

$\rightarrow (\neg b \wedge \neg \text{Posit}(A(1..i+1)))$

$\rightarrow (b \leftrightarrow \text{Posit}(A(1..i+1)))$

4.- 1, 2, 3 eta (ODE)

Frogapen desberdin bat:

1.- $(b \wedge \text{Posit}(A(1..i)) \wedge 1 \leq i < n \wedge A(i+1) < 0)$

$\rightarrow (1 \leq i < n \wedge A(i+1) < 0)$

$\rightarrow (\neg\text{Posit}(A(1..i+1)))$

$\rightarrow (\text{false} \leftrightarrow \text{Posit}(A(1..i+1)))$

2.- $\{ \text{false} \leftrightarrow \text{Posit}(A(1..i+1))\}$

b:= false;

$\{b \leftrightarrow \text{Posit}(A(1..i+1))\}$ (AA)

3.- $\{b \wedge \text{Posit}(A(1..i)) \wedge 1 \leq i < n \wedge A(i+1) < 0\}$

b:= false;

$\{b \leftrightarrow \text{Posit}(A(1..i+1))\}$ 1, 2 eta (ODE)

3.3. Konposaketa sekuentziala.

• **Konposaketaren erregela**

(KPE)

$$\frac{\{\varphi\}\ P_1\ \{\varphi_1\}\ ,\ \{\varphi_1\}\ P_2\ \{\psi\}}{\{\varphi\}\ P_1\ ;\ P_2\ \{\psi\}}$$

• Orokorrean: φ_i-ak tarteko asertzioak dira

$$\frac{\{\varphi\}\ P_1\ \{\varphi_1\}\ ,\ \{\varphi_1\}\ P_2\ \{\varphi_2\ \}\ldots\{\varphi_{n-1}\}\ P_n\{\psi\}}{\{\varphi\}\ P_1\ ;\ P_2\ ;\ \ldots;\ P_n\ \{\psi\}}$$

Adibidea

$\{ x = a \wedge y = b \}$

$x := x+y;$

$y := x-y;$

$x := x-y;$

$\{ x = b \wedge y = a \}$

"beheranzko" tarteko asertzioak:	*"goranzko" tarteko asertzioak:*
$\{x = a+b \ \wedge \ y = b\}$	$\{y=b \wedge x-y=a\}$
$\{x = a+b \ \wedge \ y = a\}$	$\{x-y=b \wedge y=a\}$

Ariketa: Frogatu formalki Hoare-ren kalkuluaren bidez:

$\{x = a \wedge y = b\}$ x:=x+y; y:=x-y; x:=x-y; $\{x = b \wedge y = a\}$

3.4. Baldintzazko sententziak.

Baldintzaren erregela:

$$\textbf{(BDE)}\quad \boxed{\dfrac{\{\varphi \wedge B\}P_1\{\psi\},\ \{\varphi \wedge \neg B\}P_2\{\psi\},\ \varphi \rightarrow def\ (B)}{\{\varphi\}\ \underline{if}\ B\ \underline{then}\ P_1\ \underline{else}\ P_2\ \underline{end\ if};\ \{\psi\}}}$$

Adibidea: def $(x \geq y) \equiv$ True

$$\dfrac{\{x \geq y\}\ z:=x\text{-}y;\ \{z=|x\text{-}y|\}\ ,\ \{x<y\}\ z:=y\text{-}x\ \{z=|x\text{-}y|\}}{\{true\}\ \underline{if}\ x \geq y\ \underline{then}\ z:=x\text{-}y;\ \underline{else}\ z:=y\text{-}x;\ \underline{end\ if};\ \{z=|x\text{-}y|\}}$$

Baldintzaren erregela. Frogapen formala.

1.- $x \geq y \rightarrow x - y = |x - y|$

2.- $\{x - y = |x - y|\}$ `z:=x-y;` $\{z = |x - y|\}$ (AA)

3.- $\{x \geq y\}$ `z:=x-y;` $\{z = |x - y|\}$ 1, 2, (ODE)

4.- $x < y \rightarrow y - x = |x - y|$

5.- $\{y - x = |x - y|\}$ `z:=y-x;` $\{z = |x - y|\}$ (AA)

6.- $\{x < y\}$ `z:=y-x;` $\{z = |x - y|\}$ 4, 5, (ODE)

7.- $\{true\}$
```
if x ≥ y then z:= x-y;
    else z:= y-x;
end if;
```
$\{z = |x - y|\}$ 3, 6, (BDE)

Beste baldintzazko agindu bat

- Hoare-ren kalkulua:

(BDE)
$$\frac{\{\varphi \wedge B\}\ P_1\ \{\psi\},\ (\varphi \wedge \neg B) \rightarrow \psi\ ,\ \varphi \rightarrow \mathrm{def}\,(B)}{\{\varphi\}\ \underline{\text{if}}\ B\ \underline{\text{then}}\ P_1\ \underline{\text{end}}\ \underline{\text{if}};\ \{\psi\}}$$

Ariketa:

$\{x=a\}$ <u>if</u> $x < 0$ <u>then</u> $x := -x;$ <u>end if</u>; $\{x=|a|\}$

Beste baldintzazko agindu bat. Adibidea.

$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \wedge A(k) = 0) \wedge 1 \le i < n\}$

```
i:= i + 1;
 {                                                  }
if A(i) = 0
then                                             P
      Zenbatzero:= Zenbatzero + 1;
end if;
```

$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \wedge A(k) = 0) \wedge 1 \le i \le n\}$

Adibidea. Frogapen formalaren eskema

$\{Zenbatzero = \mathcal{N}k\ (1 \leq k \leq i\ \wedge A(k) = 0)\ \wedge\ 1 \leq i < n\}$

```
i:= i + 1;
```

$\{Zenbatzero = \mathcal{N}k\ (1 \leq k \leq i-1 \wedge A(k) = 0) \wedge\ 1 \leq i \leq n\}$

$\equiv \varphi_1$

```
if A(i) = 0
then
```

$\{Zenbatzero + 1 = \mathcal{N}k\ (1 \leq k \leq i \wedge A(k) = 0) \wedge\ 1 \leq i \leq n\}$

```
      Zenbatzero:= Zenbatzero + 1;
```

$[\ \varphi_1 \wedge\ A(i) \neq 0 \rightarrow \underline{Zenbatzero = \mathcal{N}k\ (1 \leq k \leq i \wedge A(k) = 0)}\ ]$

```
end if;
```

$\{Zenbatzero = \mathcal{N}k\ (1 \leq k \leq i\ \wedge A(k) = 0)\ \wedge\ 1 \leq i \leq n\}$

Adibidea. Frogapen formala Hoare-ren kalkuluan

1.- $(Zenbatzero = \mathcal{N}k\ (1 \le k \le i \ \wedge A(k)=0) \ \wedge \ 1 \le i < n) \rightarrow$
$(Zenbatzero = \mathcal{N}k\ (1 \le k \le i \ \wedge A(k)=0) \ \wedge \ 1 \le i+1 \le n)$

2.- $\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \wedge A(k) = 0) \ \wedge \ 1 \le i+1 \le n\}$

```
i:= i + 1;
```

$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i\text{-}1 \wedge A(k)=0) \ \wedge \ 1 \le i \le n\}$

φ_1 tarteko asertzioa (AA)

3.- $(A(i) = 0 \wedge \varphi_1) \rightarrow$
$(Zenbatzero + 1 = \mathcal{N}k\ (1 \le k \le i \wedge A(k)=0) \ \wedge \ 1 \le i \le n)$

4.- $\{Zenbatzero + 1 = \mathcal{N}k\ (1 \le k \le i \wedge A(k)=0) \ \wedge \ 1 \le i \le n)\}$

```
Zenbatzero:= Zenbatzero + 1;
```

$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \wedge A(k)=0) \ \wedge \ 1 \le i \le n)\}$ (AA)

Adibidea. Frogapen formala Hoare-ren kalkuluan (II)

$\psi \equiv Zenbatzero = \mathcal{N}k\ (1 \le k \le i \land A(k)=0)\ \land\ 1 \le i \le n)$

5.- $\{A(i)=0 \land \varphi_1\}$ `Zenbatzero:=Zenbatzero+1;` $\{\psi\}$

3, 4, (ODE)

6.- $(A(i) \neq 0 \land \varphi_1) \rightarrow \psi$

7.- $\varphi_1 \rightarrow 1 \le i \le n \equiv def(A(i)=0)$

8.- $\{\varphi_1\}$ `if A(i) = 0`

```
then Zenbatzero:=Zenbatzero+1;
end if;
```

$\{\psi\}$ 5, 6, 7, (BDE)

9.- $\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \land A(k)=0)\ \land\ 1 \le i < n)\}$

P

$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \land A(k)=0)\ \land\ 1 \le i \le n)\}$

1, 2, 8, (ODE), (KPE)

Ariketa: dokumentatu eta frogatu formalki:

$$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \land A(k) = 0) \land 1 \le i < n\}$$

```
if A(i+1) = 0
then                                          P
    Zenbatzero:= Zenbatzero + 1;
end if;
{                                                }
i:= i + 1;
```

$$\{Zenbatzero = \mathcal{N}k\ (1 \le k \le i \land A(k) = 0) \land 1 \le i \le n\}$$

3.5. Iterazioak: Inbarianteak.

Iterazio batek agindu-multzo bat errepikatuz gauzatzen du bere egitekoa. Alabaina, egindakoa islatzen duen <u>propietate bat kontserbatu</u> egiten du prozesuan zehar.

<u>Adibideak:</u>

$P_1 \equiv$ **<u>while</u>** `y` $\neq$ `0` **<u>loop</u>** `x:=x+1; y:=y-1;`**<u>end loop</u>**;

eginkizuna: $\{x = a \wedge y = b \geq 0\}$ P_1 $\{x = a+b\}$

propietatea: $x+y = a+b \wedge b \geq y \geq 0$

Iterazioen adibideak

$P_2 \equiv$ **while** `2*z` $\leq$ x **loop** `z:=2*z;` **end loop**;

eginkizuna:

$\{x \geq 1 \wedge z = 1\}\ P_2\ \{z = \max \{k \mid \mathrm{ber2}(k) \wedge k \leq x\}\}$

propietatea: $\mathrm{ber2}(z) \wedge z \leq x$

$P_3 \equiv$ **while** `i` $\neq$ n **loop** `i:=i+1; s:=s+A(i);` **end loop**;

eginkizuna: $\{i = 0 \wedge s = 0\}\ P_3\ \{s = \sum_{j=1}^{n} A(j)\}$

propietatea: $\{s = \sum_{j=1}^{i} A(j) \wedge 0 \leq i \leq n\}$

Iterazioen inbariantea

{ φ }
<u>while</u> B **<u>loop</u>** {INB}
P
<u>end</u> <u>loop</u>;
{ ψ }

INB *propietatea*

- *P-k aldatzen dituen aldagaiei dagokie,*
- *P-k kontserbatu egiten du, eta*
- *iterazioaren semantika zehazten du.*

Iterazioen egiaztapena, Hoare-ren kalkuluan

- While-ren erregela: (WHE)

$$\frac{\varphi \rightarrow INB,\ INB \rightarrow def(B),\{INB \wedge B\}\ P\ \{INB\},(INB \wedge \neg B) \rightarrow \psi}{\{\varphi\}\ \underline{\textbf{while}}\ B\ \underline{\textbf{loop}}\ P;\ \underline{\textbf{end}}\ \underline{\textbf{loop}};\ \{\psi\}}$$

Aski litzateke:

$$\frac{\{INB \wedge B\}\ P\ \{INB\}}{\{INB\}\ \underline{\textbf{while}}\ B\ \underline{\textbf{loop}}\ P;\ \underline{\textbf{end}}\ \underline{\textbf{loop}};\ \{INB \wedge \neg B\}}$$

eta (ODE) *erabiltzea*

$$\frac{\varphi \rightarrow INB,\ INB \rightarrow def(B),\qquad\qquad ,\ INB \wedge \neg B \rightarrow \psi}{\{\varphi\}\ \underline{\textbf{while}}\ B\ \underline{\textbf{loop}}\ P;\ \underline{end}\ \underline{loop};\ \{\psi\}}$$

Inbarianteen adibideak. Iterazioen egiaztapena.

- Adibide 1:

$\{x = a \wedge y = b \geq 0\}$

$\{x+y = a+b \wedge 0 \leq y \leq b\} \equiv INB$

```
while y≠0 loop
   x:=x+1;
   y:=y-1;
end loop;
```

$\{x = a+b\}$

Inbarianteen adibideak. Iterazioen egiaztapena (II).

Frogapen formala:

1.- $(x=a \wedge y=b \geq 0) \rightarrow (x+y=a+b \wedge 0 \leq y \leq b)$

2.- $(\underbrace{x+y = a+b \wedge 0 \leq y \leq b}_{INB} \wedge \underbrace{y \neq 0}_{B}) \rightarrow$

$$((x+1) + (y-1) = a+b \wedge 0 \leq y-1 \leq b)$$

3.- $\{(x+1) + (y-1) = a+b \wedge 0 \leq y-1 \leq b\}$

```
x:=x+1;  y:=y-1;
```

$\{x+y = a+b \wedge 0 \leq y \leq b\}$ (AA) eta (KPE)

4.- $(x+y = a+b \wedge 0 \leq y \leq b \wedge y \neq 0)$

```
x:=x+1;  y:=y-1;
```

$\{x+y = a+b \wedge 0 \leq y \leq b\}$ 2, 3, (ODE)

Inbarianteen adibideak. Iterazioen egiaztapena (III).

5.- $(\underbrace{x+y = a+b \wedge 0 \leq y \leq b}_{\text{INB}} \wedge \underbrace{y=0}_{\neg B}) \rightarrow (x=a+b)$

6.- $\{x = a \wedge y = b \geq 0\}$

```
while y≠0 loop x:=x+1; y:=y-1; end loop;
```

$\{x = a+b\}$ 1, 4, 5, (WHE)

$\boxed{\phi \rightarrow \text{INB}}$

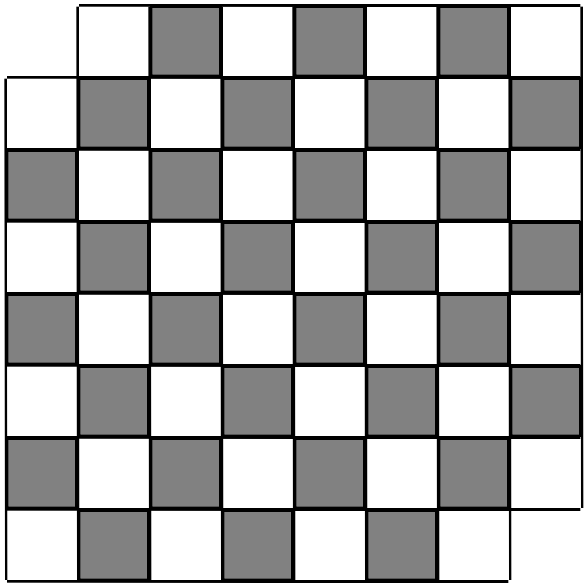
$\boxed{(\text{INB} \wedge \neg B) \rightarrow \psi}$

$\boxed{\{\text{INB} \wedge B\}\ P\ \{\text{INB}\}}$

(2 eta 3 direla-eta frogatzen da)

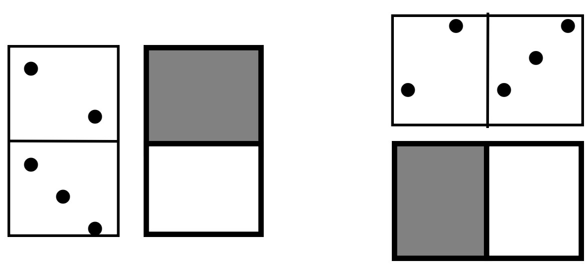
Inbarianteen erabilgarritasuna

Jo dezagun xakeko taulatu bati ezkerreko goi-laukia eta eskuineko behe-laukia kendu egiten dizkiogula:



<u>Galdera</u>:
Litekeena al da taulatua erabat estaltzea dominoko fitxekin?

Dominoko fitxek bi laukitxo estaltzen dituzte.



(fitxak modu horizontalean nahiz bertikalean jar daitezke taulatuan)

Inbarianteen adibideak. Iterazioen egiaztapena (IV).

- Adibide 2:

$\{x \geq 1\}$

P

```
z:=1;
while 2*z≤x loop          {ber2(z) ∧z ≤ x}
      z:=2*z;
end loop;
```

$\{z = \max \{k \mid ber2(k) \wedge k \leq x\} \}$

Frogapen formala:

1.- $x \geq 1 \rightarrow (ber2(1) \wedge 1 \leq x)$

2.- $\{ber2(1) \wedge 1 \leq x\}$ `z:=1;` $\{ber2(z) \wedge z \leq x\}$ (AA)

3.- $\{x \geq 1\}$ `z:=1;` $\{ber2(z) \wedge z \leq x\}$ 1, 2, (ODE)

Inbarianteen adibideak. Iterazioen egiaztapena (V).

4.- $(\underbrace{ber2(z) \wedge z \leq x}_{INB} \wedge \underbrace{2*z \leq x}_{B}) \rightarrow (ber2(2*z) \wedge 2*z \leq x)$

5.- $\{ber2(2*z) \wedge 2*z \leq x\}$ `z:=2*z;` $\{ber2(z) \wedge z \leq x\}$ (AA)

6.- $\{ber2(z) \wedge z \leq x \wedge 2*z \leq x\}$ `z:=2*z;` $\{ber2(z) \wedge z \leq x\}$

4, 5, (ODE)

7.- $(\underbrace{ber2(z) \wedge z \leq x}_{INB} \wedge \underbrace{2*z > x}_{\neg B}) \rightarrow (z = \max\{k \mid ber2(k) \wedge k \leq x\})$

8.-$\{ber2(z) \wedge z \leq x\}$

while 2*z ≤ x **loop** z:=2*z;**end** **loop**;

$\{z = \max\{k \mid ber2(k) \wedge k \leq x\}\}$ 6, 7, (WHE)

9.- $\{x \geq 1\}$ P $\{z = \max\{k \mid ber2(k) \wedge k \leq x\}\}$ 3, 8, (KPE)

3.6. Iterazioen bukaera.

- $\{\varphi\}[P]\ \{\psi\} \equiv \{\varphi\}\ P\ \{\psi\} + \underline{\text{Buka}\ (P, \varphi)}$

  P iteratiboa
  edo errekurtsiboa bada

- *Litekeena da iterazio bat hasierako egoera batzuetarako bukatzea eta beste batzuetarako ez*

  $\Rightarrow$ ***Aurrebaldintzaren araberako bukaera.***

  $\Rightarrow$ ***Inbariantearen araberako bukaera.***

Adibide1

$P \equiv$ `while i ≠ 0 loop i:=i-1; end loop;`

- *Betetzen da* {true} P {i = 0}

  EZ ordea Buka (P, true)

  $\Rightarrow$ *EZ* {true} [P] {i = 0}

- *Betetzen da* {i ≥ 0} P {i = 0}

  baita ere Buka (P, i ≥ 0)

  $\Rightarrow$ {i ≥ 0} [P] {i = 0}

- *Aurrebaldintza* i ≥ 0 bada

  i ≥ 0 *kontserbatzen da (inbariantea da),*

  baina aurrebaldintza true bada, ez.

Adibide2

$P \equiv$ **<u>while</u>** `i` $\neq$ `0` **<u>loop</u>** `i:=i-2;` **<u>end</u>** **<u>loop</u>**;

- *Betetzen da* {true} P $\{i = 0\}$

  <u>*EZ*</u> *ordea* Buka (P, true)

  $\Rightarrow$ <u>*EZ*</u> {true} [P] $\{i = 0\}$

- *Betetzen da* $\{i \geq 0 \wedge \text{bikoiti}(i)\}$ P $\{i = 0\}$

  baita ere Buka $(P, i \geq 0 \wedge \text{bikoiti}(i))$

  $\Rightarrow$ $\{i \geq 0 \wedge \text{bikoiti}(i)\}$ [P] $\{i = 0\}$

- *Aurrebaldintza* $i \geq 0 \wedge \text{bikoiti}(i)$ bada

  $i \geq 0 \wedge \text{bikoiti}(i)$ *kontserbatzen da (inbariantea da),*

  baina aurrebaldintza true bada, ez.

Bukaeraren azterketa

while B **loop** {INB}
P
end loop;

pauso kopuru finituan bukatuko da, baldin

- *P-k B-ko aldagairen bat aldatzen badu,*
- *eta aldaketa horren aplikazioak,* INB $\wedge$ B *betetzen den egoera batean hasita, B faltsu egiten badu denbora finituan.*

Iterazioen bukaera frogatzeko metodoa: oinarria

- *E espresio batek balio arruntak har baditzake, pauso kopuru finitu batean baizik ezin daiteke txikiagotu.*

- 80 > … > 23 > ...> 14 > …> 3 >…0 (ez dago besterik)

- ($\mathbb{N}$, ≤) **ondo oinarritutako ordena** da

EZ dauka kate beherakor infiniturik

Iterazioen bukaera frogatzeko metodoa

Izan bedi E zenbakizko espresio bat (P-ko aldagaiez osatua) <u>borne-adierazpena</u> deituko duguna; honako bi propietate hauek betetzen badira:

(a) $(\mathrm{INB} \wedge \mathrm{B}) \rightarrow \mathrm{E} \in \mathbf{N}$ (*hau da*, $\mathrm{E} \geq 0$)

(b) $\{\mathrm{INB} \wedge \mathrm{B} \wedge \mathrm{E} = \mathrm{z}\}\ \mathrm{P}\ \{\mathrm{E} < \mathrm{z}\}$

($\mathrm{z} \notin$ Aldagaiak(INB, B, P))

orduan

<u>**while**</u> B <u>**loop**</u> P <u>**end**</u> <u>**loop**</u>; (INB inbariantea)

pauso kopuru finituan amaitzen da.

Metodoaren justifikazioa

Izan bedi

$E = z_1$ *iterazioaren sarreran,*

$E = z_2$ *hurrengo iterazioan, …*

orduan

(a) $z_1, z_2, \ldots, z_i, \ldots \in \mathbf{N}$

(b) $z_1 > z_2 > \ldots > z_i > \ldots$

$\Rightarrow$

Ezinezkoa da pauso kopuru infinitua egotea

$E = z_i \in \mathbf{N}$ *delarik*

$\Rightarrow$ INB $\wedge$ B *ezin daiteke bete mugagabeki*

$\Rightarrow$ *pauso kopuru finituan* $\neg$B *beteko da*

Adibideak (I)

- Adibide 1 (x,y: Integer)

$\{x=a \wedge y=b\geq 0\}$

while $y\neq 0$ **loop** $\{x+y=a+b \wedge 0\leq y\leq b\}\equiv INB$

```
    x:=x+1;
    y:=y-1;
```

$\boxed{E \equiv y}$

end loop;

$\{x=a+b\}$

Frogatu behar dugu:

(a) $(x+y=a+b \wedge 0\leq y\leq b \wedge y\neq 0) \rightarrow y\in \mathbf{N}$

(b) $\{x+y=a+b \wedge 0<y\leq b \wedge y=z\}$

$x:=x+1;\ y:=y-1;\ \{y < z\}$

Adibideak (II)

(b) atalaren froga formala:

1.- $(x+y=a+b \wedge 0<y\leq b \wedge y=z) \rightarrow (y-1< z)$

2.- $\{y-1< z\}$ x:= x+1; $\{y-1< z\}$ (AA)

3.- $\{y-1< z\}$ y:= y-1; $\{y< z\}$ (AA)

4.- $\{x+y = a+b \wedge 0<y\leq b \wedge y = z\}$

`x:=x+1; y:=y-1;` $\{y < z\}$

1, 2, 3, (KPE), (ODE)

Adibideak (III)

- Adibide 2 (x,z: Integer)

$\{ber2(z) \wedge 1 \leq z \leq x\}$

```
while 2*z≤x loop
      z:=2*z;
end loop;
```

$\boxed{E \equiv x\text{-}z}$

Frogatu behar dugu:

(a) $(ber2(z) \wedge 1 \leq z \leq x \wedge 2*z \leq x) \rightarrow x-z \in \mathbf{N}$

(b) $\{ber2(z) \wedge 1 \leq z \leq x \wedge 2*z \leq x \wedge x-z=b\}$

z:=2*z; $\{x-z<b\}$

Adibideak (IV)

(b) atalaren froga formala:

1.- $(\text{ber2}(z) \wedge 1 \le z \le x \wedge 2*z \le x \wedge x\text{-}z=b)$

$\rightarrow (1 \le z \wedge x\text{-}z=b \ge 0 \wedge x\text{-}(2*z) \ge 0)$

$\rightarrow (x\text{-}(2*z) < b)$

2.- $\{x\text{-}(2*z) < b\}$ `z:=2*z;` $\{x\text{-}z < b\}$ (AA)

3.- $\{\text{ber2}(z) \wedge 1 \le z \le x \wedge 2*z \le x \wedge x\text{-}z=b\}$

`z:=2*z;` $\{x\text{-}z<b\}$ 1, 2, (ODE)

Adibidea:

$\{ n \geq 1 \}$

```
  i:=0; neg:=0;
```

$\{ 0 \leq i \leq n \wedge neg = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j) < 0) \} \equiv INB$

```
[ while i<n loop                    E ≡ n-i
        i:=i+1;
        if A(i)<0 then neg:=neg+1; end
  if;
  end loop; ]
```

$\{neg = \mathcal{N} j \ (1 \leq j \leq n \wedge A(j) < 0)\}$

Adibidea (jarraipena):

- $\{ n \geq 1 \}$ `i:=0; neg:=0;` $\{ 0 \leq i \leq n \wedge neg = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j)<0) \}$
- def(`i<n`) $\equiv$ True
- $\{0 \leq \underline{i < n} \wedge neg = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j)<0)\}$

`i:=i+1;`

$\{0 \leq i \leq n \wedge neg = \mathcal{N} j \ (1 \leq j \leq i-1 \wedge A(j)<0)\}$

__if__ `A(i)<0` **__then__** $\{0 \leq i \leq n \wedge neg+1 = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j)<0)\}$

`neg:=neg+1;`

$[(neg = \mathcal{N} j \ (1 \leq j \leq i-1 \wedge A(j)<0) \wedge A(i) \geq 0)$

$\rightarrow neg = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j)<0)]$

__end__ **__if__**;,

$\{ 0 \leq i \leq n \wedge neg = \mathcal{N} j \ (1 \leq j \leq i \wedge A(j)<0))\}$

Adibidea (jarraipena):

- $(0 \le i \le n \wedge neg = \mathcal{N} j\ (1 \le j \le i \wedge A(j) < 0) \wedge i \ge n)$
  $\rightarrow neg = \mathcal{N} j\ (1 \le j \le n \wedge A(j) < 0)$

- $(0 \le \underline{i < n} \wedge neg = \mathcal{N} j\ (1 \le j \le i \wedge A(j) < 0)) \rightarrow n - i \in \mathbf{N}$

- $\{0 \le i < n \wedge neg = \mathcal{N} j\ (1 \le j \le i \wedge A(j) < 0) \wedge n - i = v\}$

```
i:=i+1
```

$\{n - i < v\}$

3.7. Programa errekurtsiboak.

- Edozein programa errekurtsibok baditu gutxienez bi adar (baldintzazko):
  - Kasu nabaria (ez-errekurtsiboa): 1 edo gehiago
  - Kasu induktiboa (errekurtsiboa): 1 edo gehiago
- *Kasu nabarietan* dei errekurtsiborik gabe ebazten diren datuen azpimultzoak tratatzen dira.
- *Kasu induktiboak* ebazteko, kasu nabarietatik gertuago (zentzuren batean) dauden beste datu batzuen ebazpenean hartzen da oinarri.

Programa errekurtsiboetarako notazioa

- Programa errekurtsibo batek bere buruari deitu ahal izateko (kasu induktiboetako azpiproblemak), honakoa behar da:
  - Programa izendatzea, eta
  - Datuak eta emaitzak ondo parametrizatuta edukitzea

- <u>*function*</u> $f(x_1{:}T_1;\ldots;\ x_n{:}T_n)$ <u>*return*</u> $y_1{:}S_1,\ldots,y_m{:}S_m$

  modu honetan T_i motetako x_i datuak eta S_i motetako y_i emaitzak dituen f izeneko programa adieraziko dugu.

Adibidea

```
function fakt(n:integer) return f:integer
  is
  {n≥0}
  if n=0 then f:=1;
  else f:=fakt(n-1); f:=n*f; end if;
  {f=n!}
```

edo bestela

```
g:integer;
{n≥0}
if n=0 then f:=1;
else g:=fakt(n-1); f:=n*g; end if;
{f=n!}
```

Programa errekurtsiboen egiaztapena

- Indukzio bidezko *frogapena egiten da:*
  - Lehenbizi frogatu kasu nabariek *espezifikazioa betetzen dutela*
  - Gero, dei errekurtsiboek espezifikazioa betetzen dutela suposatuz (indukzio-hipotesia), kasu induktiboek ere *espezifikazioa betetzen dutela* frogatu .
- Errekurtsioa bukatzen dela ere frogatu behar da (indukzioaren balidazioa)*:*
  - E borne-adierazpena definitu *errekurtsioaren parametroen arabera (dei errekurtsiboen datuak).*
  - Frogatu E zenbaki arrunta dela kasu nabari bakoitzean
  - Frogatu E gutxitzen doala (**N**-ren barne) dei errekurtsibo bakoitzean

Adibidea: Faktoriala

```
function fakt(n:integer) return f:integer is
```

$\{n \geq 0\}$

```
if n=0 then f:=1;
else f:=fakt(n-1); f:=n*f; end if;
```

$\{f=n!\}$

- *Frogatu behar da* $\{n \geq 0\}$ [`f:=fakt(n)`] $\{f=n!\}$
  - Kasu nabaria: $\{n \geq 0 \wedge n=0\}$ `f:=1;` $\{f=n!\}$

    $(n \geq 0 \wedge n=0) \rightarrow (n=0) \rightarrow \{n!=1\}$

    `f:=1;`

    $\{f=n!\}$

Adibidea: Faktoriala (jarraipena)

- <u>Kasu induktiboa</u>:

$\{n \geq 0 \wedge n \neq 0\}$ `f:=fakt(n-1); f:=n*f;` $\{f=n!\}$

> Indukzio-hipotesia:
>
> $\{n-1 \geq 0\}$ `f:=fakt(n-1);` $\{f=(n-1)!\}$

$(n \geq 0 \wedge n \neq 0) \rightarrow \{n-1 \geq 0\}$

`f:=fakt(n-1);` $\{f=(n-1)!\}$

$\rightarrow \{n * f = n!\}$

`f:=n*f;` $\{f=n!\}$

Indukzio-hipotesiaren aplikazioa

Adibidea: Faktoriala (jarraipena)

- Indukzioaren balidazioa:

  Borne-adierazpena: n

  Kasu nabarian: $n=0\in\mathbf{N}$

  Kasu induktiboan $n>0$ eta

  `fakt(n)`-k `fakt(n-1)`-i *deitzen dio*;

  beraz, betetzen da:

  $$n>0 \rightarrow (n-1\in\mathbf{N} \wedge n-1<n)$$

- Ariketa: g aldagai laguntzailea erabiltzen duen kasurako egiaztapena egin.