~~Metodologi:~~

Programazioaren Metodologia

Baldintzazko egiturak

$\{\phi\} \equiv \{ zenbatzero = N_k (1 \leq k \leq i \wedge A(k)=0) \wedge 1 \leq i \leq n \}$

$i := i+1;$

$\{\phi_1\} \equiv \{ zenbatzero = N_k (1 \leq k < i \wedge A(k)=0) \wedge 1 \leq i \leq n \}$

if $A(i)=0$ then $zenbatzero := zenbatzero + 1$; end if;

$\{\psi\} \equiv zenbatzero = N_k (1 \leq k \leq i \wedge A(k)=0) \wedge 1 < i \leq n$

Frogapenaren egitura:

$\{\phi\}$ $i := i+1$ $\{\phi_1\}$

$\{\phi_1\}$ if $A(i)=0$ then $zenbtzero := zenbatzero + 1$; end if; $\{\psi\}$

A

$\{\phi\}$ $i := i+1;$ $\{\phi_1\}$

B

B.1

$\{\phi_1 \wedge A(i)=0\}$ $zenbatzero := zenbatzero + 1;$ $\{\psi\}$

B.2

$(\phi_1 \wedge A(i) \neq 0) \rightarrow (\psi)$

B.3

$\phi_1 \rightarrow def(A(i)=0)$

Frogapena:

1. $\{ zenbatzero = N_k (1 \leq k \leq i+1 \wedge A(k)=0) \wedge 1 \leq i+1 \leq n \}$ $i := i+1;$ $\{\phi_1\}$ (AA)
2. $\phi \rightarrow (zenbatzero = N_k (1 \leq k < i+1 \wedge A(k)=0) \wedge 1 \leq i+1 < n)$
3. $\{\phi\}$ $i := i+1;$ $\{\phi_1\}$ 2,1 eta ODE

B.1 4. $\{ zenbatzero + 1 = N_k (1 \leq k < i \wedge A(k)=0) \wedge 1 \leq i < n \}$ $zenbatzero := zenbatzero + 1;$ $\{\psi\}$

5. $(\phi_1 \wedge A(i)=0) \rightarrow (zenbatzero + 1 = N_k (1 \leq k \leq i \wedge A(k)=0) \wedge 1 \leq i < n)$

6. $\{\Phi_1 \wedge A(i)=0\}$

~~be~~ zenbatzero := zenbatzero + 1;

$\{\Psi\}$

B.2

7. $(\Phi_1 \wedge A(i)=0) \rightarrow (zenbatzero = Nk(1 \leq k \leq i \wedge A(k)=0) \wedge 1 < i \leq n)$

B.3 8. $\Phi_1 \rightarrow (1 < i \leq n) \rightarrow def(A(i)=0)$

9. $\{\Phi_1\}$ if $A(i)=0$ then zenbatzero := zenbatzero + 1; end if; $\{\Psi\}$ ~~7~~, 6, 7, 8 (BDE)

10. $\{\Phi\}$ $i:=i+1$; if $A(i)=0$ then zenbatzero = zenbatzero + 1; end if; $\{\Psi\}$ 3, 9 (KPE)

Programazioaren Metodologia

1

$\{ 1 \le i \le n \wedge z = N_k (1 \le k < i \wedge A(k) > B(k) \}$

if $A(i) > B(i)$ then $z := z+1$; end if;

$\{ 1 \le i \le n \wedge z = N_k (1 \le k \le i \wedge A(k) > B(k)$

2

2. $\{ 1 \le i-1 < n \wedge \neg dago \wedge \neg badago (A(1..i-1, x)) \}$

4. $\{ 1 \le i \le n \wedge \neg dago \wedge \neg badago (A(1.. i-1), x))$

6. $\{ 1 \le i \le n \wedge ($ true $\rightarrow badago (A(1..i), x)$ $\}$ dago := true $\{ dago \rightarrow badago\, A(1...i), x\} \wedge 1 \le i \le n$

8. $\phi_i \wedge A(i) \ne x \rightarrow \{ 1 \le i \le n \wedge \neg dago \wedge \neg badago (A(1..i), x) \rightarrow$

9. $1 \le i \le n$

10. Bde 7,8,9

<u>Adibidea</u>

1. $x \ge y \rightarrow x-y = |x-y|$
2. $\{ x-y = |x-y| \}$ $z := x-y$; $\{ z = |\cancel{x-} z|$
3. $\{ x \ge y \}$ $z := x-y$; $\{ z = | x-y| \}$ 1,2 eta ODE
4. $\{ x < y \} \rightarrow y-x = |x-y|$
5. $\{ y-x = | x-y| \}$ $z := \cancel{x}-x$; $\{ \cancel{z = |z|} \} \{ z = |x-y| \}$ (AA)
6. $\{ x < y \}$ $z := y-x$ $\{ z = | x-y| \}$ $\cancel{3},4,5$ ODE
7. $\{ true \}$ if $x \ge y$ then $z := x-y$;
   else $z := \cancel{y}-x$;
   end if;

$\{ z := x-y \}$

4

A)

$\{ z = N_j (1 \leq j < i \wedge A(j) > B(j)) \wedge 1 \leq i < n \}$

if $A(i) > B(i)$ then

$z := z+1;$

end if;

$i := i+1;$

$\{ z = N_j (1 \leq j < i \wedge A(j) > B(j)) \wedge 1 \leq i \leq n \}$

$2 = N_j (1 \leq j < 3 \wedge A(j) > B(j)) \wedge 1 \leq 3 < 4$

$z := 3;$

$3 = N_j (1 \leq j < 4 \wedge A(j) > B(j) \wedge 1 \leq 4 \leq 4$

A1

$\{ \phi \wedge A(j) > B(j) \}$ $z := z+1;$ $\{ \phi_1 \}$

1. $\{ z+1 = N_j (1 \leq j < i \wedge A(j) > B(j)) \wedge 1 \leq i < n \}$ $z := z+1$ $\{ \phi_1 \}$
2. $(\phi \wedge A(j) > B(j)) \rightarrow (z+1 = N_j (1 \leq j < i+1 \wedge A(j) > B(j)) \wedge 1 \leq i \leq n \}$
3. $\{ \phi \wedge A(i) > B(i) \}$

$z := z+1;$

$\{ \phi_1 \}$

2, 1 et. ODE

4. $(\phi \wedge A(i) \leq B(i) \} \rightarrow (z = N_j (1 \leq j < i+1 \wedge A(j) > B(j)) \wedge 1 \leq i \leq n$
5. $\{ z = N_k (1 \leq j < i+1 \wedge A(j) > B(j)) \wedge 1 \leq i+1 \leq n \}$ $i := i+1$ $\{ \phi 4 \}$
6. 3, 5 et. KPE

3. Gaia: Programen egiaztapena

2. Ariketa-orria (A): Asignazioak eta konposaketa sekuentziala

1. Ondoko baieztapena zuzena egiten duten post-baldintzak aukeratu, $A(1..n)$ zenbaki osoez osatutako bektorea izanik:

$\{ 1 \leq n \wedge \forall i\, (1 \leq i < n \rightarrow A(i) = A(n)) \}$

```
y := 1;
```

i) $\{ \forall i\, (1 \leq i \leq n \rightarrow A(i) = y) \}$ [ ]

ii) $\{ \forall i\, (2 \leq i \leq n \rightarrow A(i) = y * A(i-1)) \}$ [X]

iii) $\{ \forall i\, (1 \leq i \leq n \rightarrow y * A(i) = y) \}$ [ ]

2. Ondoko hirukoteetarako post-baldintza egokienak ({ ___ }) osatu:

2.1. $\{ \exists i\, (txiki \leq i \leq txiki + 5 \wedge A(i) > 0) \}$

```
txiki := txiki+2;
```

$\{ \underline{\exists i\, (txiki-2 \leq i \leq txiki+3 \wedge A(i) > 0} \}$

2.2. $\{ bikoitia(k) \wedge y \times z^k = p \}$

```
k := k/2;
z := z*z;
```

$\{ \underline{bikoitia(2k) \wedge y \times z^{2k} = p} \}$

3. Hurrengo frogapenean hutsuneak bete (___):

$\{ bikoitia(k) \wedge y \times z^k = p \}$

```
k := k/2;
```

$\{ y \times z^{2 \times k} = p \}$

Frogapena:

1. $(bikoitia(k) \wedge y \times z^k = p) \rightarrow (\underline{y \cdot z^k = p})$

2. $\{ \underline{y \cdot z^{2k/2} = p} \}$

```
k := k/2;
```

$\{ y \times z^{k \times 2} = p \}$ **(AA)**

3. $\{ bikoitia(k) \wedge y \times z^k = p \}$

```
k := k/2;
```

$\{ y \times z^{k \times 2} = p \}$ 1, 2 eta **(ODE)**

4. Egiaztatu hurrengo baieztapenak:

4.1.

$\{ n \geq 1 \wedge i = 0 \}$

```
zerorik_ez := true;
```

$\{ 0 \leq i \leq n \wedge (zerorik\_ez \leftrightarrow \forall k (1 \leq k \leq i \rightarrow A(k) \neq 0)) \}$

4.2.

$\{ i = j^k \wedge i < w \}$

```
i := i*j;
```

$\{ i = j^{k+1} \}$

5. Hurrengo frogapenean hutsuneak bete (___):

$\{ batura = g \}$

```
g := g+1;
batura := batura+g;
```

$\{ batura = 2 \times g - 1 \}$

Frogapena:

1. $(batura = g) \rightarrow ($ $\underline{batura = g+1-1}$ $)$

2. $\{ \underline{batura = g + 1 - 1} \}$
   `g := g+1;`
   $\{ batura = g - 1 \}$ **(AA)**

3. $\{ batura = g \}$
   `g := g + 1;`
   $\{ batura = g - 1 \}$ 1, 2 eta **(ODE)**

4. $(batura = g - 1) \rightarrow (batura + g - g = g - 1) \rightarrow$
   $($ $\underline{batura + g = 2g-1}$ $)$

5. $\{ \underline{batura + g = 2g-1} \}$
   `batura := batura+g;`
   $\{ batura = 2 \times g - 1 \}$ **(AA)**

6. $\{ batura = g - 1 \}$
   `batura := batura+g;`
   $\{ batura = 2 \times g - 1 \}$ 4, 5 eta **(ODE)**

7. $\{ batura = g \}$
   `g := g+1;`
   `batura := batura+g;`
   $\{ batura = 2 \times g - 1 \}$ 3, 6 eta **(KPE)**

6. Kontradibide baten bidez froga ezazu ondoko baieztapena ez dela zuzena:

$\{ y * z^k = p \}$

```
k := k/2;
z := z*z;
```

$\{ y * z^k = p \}$

3. gaia: Programen egiaztapena

(A) Arilketa-orria

2

2.2

$\{ billoitia(K) \wedge y \times z^K = p \}$

$K := K/2;$

$z := z * z;$

$\{ billoitia(2K) \wedge y \times (z z)^{(2K/2)} = p \} \Rightarrow \{ billoitia(2K) \wedge y \cdot z^{2K}$

Frogapena:

1. $\{ billoitia(2K) \wedge y \cdot (z * z)^{(2K/2)} = p \}$ $z := z * z$ $\{ billoitia(2K) \wedge y \cdot (z z)^{(2K/2)} = p \}$

Ψ_z^{z*z}

2. $\{ billoitia(2K/2) \wedge y \cdot (z)^{\frac{2 \cdot 2K/2}{2}} = p \}$ $K := K/2$ $\{ billoitia(2K) \wedge y \cdot (z * z)^{(2K/2)} = p \}$

$\Psi_K^{K/2}$

3. $\{ billoitia(K) \wedge y \cdot z^K = p \} \longrightarrow \{ billoitia(2K/2) \wedge y \cdot z^{\frac{2 \cdot 2K}{2 \cdot 2}} = p \}$

4.

4.1)

$\{n \geq 1 \wedge i = 0\}$

zerorik_ez := true

$\{0 \leq i \leq n \wedge (zerorik\_ez \leftrightarrow \forall k(1 \leq k \leq i \rightarrow A(k) \neq 0)$

Frogapena:

1. $(n \geq 1 \wedge i = 0) \rightarrow (0 \leq i \leq n)$

2. $(0 \leq i \leq n)$

   zerorik_ez := true;

3. $(0 \leq i \leq n \wedge zerorik\_ez) \rightarrow (0 \leq i \leq n \wedge zerorik\_ez \leftrightarrow \forall k(1 \leq i \leq k \rightarrow A(k) \neq 0))$

Adibidea:

a) $\{x = a \wedge y = b\}\ x := x + y\ \{x + y = a \wedge y = b\} \rightarrow \{x = a+b \wedge y = b\}$

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

c) $\{x = a+b \wedge y = a\}\ x = x - y\ \{x = b \wedge y = \cancel{a}b\}$

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

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

φ_x^{x-y} $\qquad \{\varphi\}$

$\{x - (x-y) = b \wedge y - x = a\}\ y := \cancel{x-y}\ \{x - y = b \wedge y = a\}$

φ_y^{y-x} $\qquad \varphi$

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

φ_x^{x+y}

$\{y \cdot x = 5^{k+1} - 1\}$

$k := k+1$

$x := x + 5^k$

$\{y \cdot x = 5^{k+1} - 1\}$

$\{y \cdot (x+5^k) = 5^{k+1} - 1\}$ $x := x+5^k$ $\{y \cdot x = 5^{k+1} - 1\}$

$\varphi_x^{x+5^k}$ $\qquad \varphi$

$\{y(x+5^{k+1}) = 5^{k+2} - 1\}$ $k := k+1$ $\{y(x+5^k) = 5^{k+1} - 1\}$

φ_k^{k+1} $\qquad \varphi$

$\{yx + y5^{k+1} = 5^{k+2} - 1\} \rightarrow \{yx = \cancel{y}5^{k+2} - y5^{k+1} - 1\}$

$\{y * z^k = p\}$

$k := k/2;$

$z := z * z;$

$\{y * z^k = p\}$

$\{y * z * z^k = p\}$ $z := z * z$ $\{y * z^k = p\}$

φ_z^{z*z} $\qquad \varphi$

$\{y * z^{2k/2} = p\}$ $k := k/2$ $\{y * z^{2k} = p\}$

$\varphi_k^{k/2}$

Frogapenaren eskema:

(a) $\{y * z^k = p\}$ $k := k/2$ $\{y * z^{k/2} = p\}$

(b) $\{y * (z*z)^{k/2} = p\}$ $z := z*z$ $\{y * z^k = p\}$

Frogapena

1. ~~$\{y*(z*z)^k = p\}$~~ $z := z*z$ $\{y * z^k = p\}$ (b)
2. ~~$\{y * z^k = p\}$ $k :=$~~ $k := k/2$ $\{y*(z*z)^k = p\}$ (a)
3. $\{y * (z*z)^{k/2}$ $\{y * z^{2k/2} = p\}$ $\longrightarrow$ $\{y*(z*z)^{k/2} = p\}$
4. $\{y * z^k = p\}$ $\longrightarrow$ $\{y * z^{2k/2} = p\}$

K ez dakigu bikoitia den edo ez beraz,

$\{y * z^k = p\} \xrightarrow{?} \{y*(z*z)^{k/2} = p\}$

$\{y = 2 \wedge z = 3 \wedge k = 3 \wedge p = 54\}$ Ez da betetzen

$\{y = 2 \wedge z = 9 \wedge k = 1 \wedge p = 18\}$ postbaldintza

7)

(A)

$x = 6$, $k = 1$

$k := k+1 \Rightarrow k := 2$

$x := 6 + 5^2 \Rightarrow x := 31$

$4 \times 31 = 5^3 - 1$

(B)

$k = 0 \quad x = 5$

$k := k+1 \Rightarrow k = 1$

$x := x + 5^k \Rightarrow x := 5 + 5^1$

$\{ x = 5^{k+1} \} \Rightarrow 10 = 5^1 \} \Rightarrow \boxed{5 \neq 10}$

A-sen fragapene:

1. $\{ 4 \times x = 5^{k+1} - 1 \}$

$k := k+1$

$\{ 4 \times x = 5^k - 1 \}$

2. $\{ 4 \cdot (x + 5^k) = 5^{k+1} - 1 \}$

$x := x + 5^k$

$\{ 4 \cdot x = 5^{k+1} - 1 \}$

3. $\{ 4 \times x = 5^k - 1 \} \rightarrow \{ \cancel{4 \times +}$

7. Ondoko baieztapena egiaztatu zuzena bada, eta, bestela, justifikatu kontradibide baten bidez zuzena ez dela:

(A) $\{\, 4 \times x = 5^{k+1} - 1 \,\}$
```
k := k+1;
x := x+5^k;
```
$\{\, 4 \times x = 5^{k+1} - 1 \,\}$

(B) $\{\, x = 5^{k+1} \,\}$
```
k := k+1;
x := x+5^k;
```
$\{\, x = 5^{k+1} \,\}$

(A) baieztapena zuzena da eta (B) ez da zuzena [X]

(B) baieztapena zuzena da eta (A) ez da zuzena [ ]

$\{\phi\}\ P\ \{A \leftrightarrow B\}$

1)

$\{\emptyset\}\ P\ \{A \wedge B\}$

$(A \wedge B) \rightarrow \underbrace{(A \wedge B) \vee (\neg B \wedge \neg A)}_{A \leftrightarrow B}$

2)

$\{\phi\}\ P\ \{A \wedge \neg B\}$

$(\neg A \wedge \neg B) \rightarrow (\neg A \wedge \neg B) \vee (A \wedge B) \equiv A \leftrightarrow B$

2. Gaia: Programen Espezifikazioa

1. Ariketa-orria. (A)

1. Ondoko aukeren artean identifikatu zuzenak diren formulak edo baieztapenak (bat baino gehiago izan daitezke zuzenak). Horretaz gain, formula bakoitzak dituen aldagai libreak kontuan izanik predikatu bat egokitu (1.1 ariketan adierazten den bezala)

1.1. $handiena(A(1..n), x) \equiv x$ da $A(1..n)$ bektoreko elementurik handiena.

a) $\exists i\ (\ 1 \leq i \leq n\ \wedge\ A(i) = x)\ \wedge\ \forall j\ (\ 1 \leq j \leq n\ \rightarrow\ x \geq A(j)\ )$ [X]

b) $1 \leq i \leq n\ \wedge\ A(i) = x\ \wedge\ \forall j\ (\ 1 \leq j \leq n\ \rightarrow\ x \geq A(j)\ )$ [ ]

c) $\exists i\ (\ 1 \leq i \leq n\ \wedge\ A(i) = x)\ \wedge\ \forall j\ (\ 1 \leq j \leq n\ \rightarrow\ A(i) \geq A(j)\ )$ [X]

1.2. ______________________________ $\equiv A(1..n)$ bektorean ez dago elementu errepikaturik.

a) $\forall i\ (\ 1 \leq i \leq n\ \rightarrow\ \forall j\ (\ i < j \leq n\ \rightarrow\ A(i) \neq A(j)\ )\ )$ [X]

b) $\forall i\ (\ 1 \leq i \leq n\ \rightarrow\ \mathcal{N} j\ (\ 1 \leq j \leq n\ \wedge\ A(i) = A(j)\ ) = 1\ )$ [X]

c) $\forall i\, \forall j\ (\ 1 \leq i \leq n\ \wedge 1\ \leq j \leq n\ \wedge\ i \neq j\ \rightarrow\ A(i) \neq A(j)\ )$ [X]

1.3. ______________________________ $\equiv A(1..n)$ osoko bektorean lehenengo elementua baino handiagoak diren elementuen kopurua k da.

a) $k = \mathcal{N} i\ (\ 1 < i \leq n\ \wedge\ A(i) > A(1)\ )$ [X]

b) $k = \mathcal{N} i\ (\ 1 \leq i \leq n\ \wedge\ A(i) > A(1)\ )$ [X]

c) $A(1) < \mathcal{N} i\ (\ 1 \leq i \leq n\ \wedge\ A(i) = k\ )$ [ ]

1.4. ______________________________ $\equiv A(1..n)$ bektoreko elementuak gorantz ordenatuta daude.

a) $\forall i\ (\ 1 \leq i \leq n\ \rightarrow\ A(i) < A(i+1)\ )$ [X]

b) $\forall i\ (\ 1 \leq i < n\ \rightarrow\ A(i) < A(i+1)\ )$ [X]

c) $\forall i\ (\ 1 \leq i \leq n\ \rightarrow\ A(i-1) < A(i)\ )$ [ ]

Programazioaren Metodologia Ariketak

②

2.1

A(1..n) osoko bektorean ez daude bi zero jarraian

$$\forall i (1 \leq i \leq n \rightarrow (A(i) \neq 0 \vee A(i+1) \neq 0)$$

2.2

x A(1..n) bektorean i posizioa baino lehenago agertzen den ala ez itzultzen du Dago izeneko aldagaian.

$$Dago = true \leftrightarrow \exists j (1 \leq j \leq i \wedge A(j) = x)$$

2.3

Osoko elementuz osatutako A(1..n) bektorean A(i..j) sekzioko elementuen batura x aldagaian itzultzen du

$$x = \sum_{k=i}^{j} A(k)$$

2.4

B(1..n) bektorea lortzen da A(1..n) bektorearen osagaiak zirkularki eskuinerantz errotatuz.

$$\forall i (2 \leq i \leq n \rightarrow B(i) = A(i-1)) \wedge B(1) = A(n)$$

③

3.1

$\forall i (2 \leq i \leq n \rightarrow A(1) \neq A(i)) \Rightarrow$ Ez da existitzen A(2..n) bektorean A(1) zenbakiaren berdinik

3.2

$\exists i \, (i > 0 \wedge x \times i = 8)$

3.3

$1 \leq ind \leq 6 \leq n \wedge \forall j \, (6 < j < n \rightarrow A(ind) \geq A(j))$

1 etik 6 rako posizioko zenbakiak hortik aurrerakoak baino handiago edo berdinak dira.

3.4

$\forall j \, \forall k \, (1 \leq j \leq n \wedge 1 \leq k \leq m \wedge j \neq k \rightarrow A(j) \neq B(k))$

j eta ka ezberdinak badira ez dago A eta B bektoreetan zenbaki berdinik

4

4.1

Aldagai libreak, x, k, A(1..n)

$(1 \leq k \leq n \wedge A(k) = x \wedge \forall i \, (1 \leq i < k \wedge A(i) \neq x)$

4.2

Aldagai libreak, z, i, k

$z = \sum_{i=1}^{k} i$ $\quad \exists i \, (1 \leq i \wedge z = \sum_{j=1}^{i} j) \checkmark$

4.3

x y ~~z~~ dira Aldagai libreak.

~~$\exists x ($ ... $y < n \wedge A$~~

$\exists x$

$x > y \wedge \exists i \, (i \geq 0 \wedge x = 2^i \wedge 2^{i-1} \leq y) \checkmark$

4.4

Aldagai libreak x, A(1..n), i

$\forall i \, (1 \leq i \leq n \rightarrow A(i) > x) \checkmark$

4.5

Aldagai librea A(1..n), k, i

$k = N i \, (1 \leq i \leq n \wedge (A(i) = 0))$ Eskuin ondoren

$k = N i \, (1 \leq i \leq n \wedge A(i) = 0)$

5.6

$\{\varphi\} \equiv$

$\{\psi\} \equiv$ ~~$\forall i(1 \le i < n \to A\ Lehena(A(i))) \land A(i)\ Lehena(A(i)) \to Lehena(A(i+1)))$~~

~~nonLehena x ≡~~

~~x eta z~~ ~~etterren~~, ~~Elkar Segidako Zenbaki lehenak (i, n, A(i)))~~

~~$\forall i(1 \le i < n)$~~ → ~~A(i) Lehena(A(i))~~ → $\forall i(1 \le i \le n \to$ Elkar Zenbaki lehenak$(i, i+1, A(i), \ldots, A(i+1))$ ~~Lehena(A(i))~~

7.1

a)

$A(1..n) = a(1..n)$

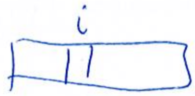
$\{\Phi\} \equiv$ luz A ~~$(a_1, a_2, a_3 \ldots a_n) = (a_n, a_{n-1}, a_{n-2}, \ldots, a_1)$~~

$\{\Psi\} \equiv$ ~~$\forall i(1 \le i \le n \to A_i$~~
~~$\forall k(1 \le k \le n \to A(i) = A(k))$~~

$\equiv$ ~~n~~ $A(i)$

$\equiv \forall i(1 \le i \le n \to A(i) = A(n-i))$

$A(i)$



a_i

b)

$\{\Phi\} \equiv$ ~~$A(1..n) = A$~~ $B(1..n)\ (n \ge 1)$

$\{\Psi\} \equiv \forall i(1 \le i \le n \to$ ~~$A(i) = B(n-i)$~~$)$
$B(i) = A(n-i+1)$

Adibidea

```
begin
  r := x;  q := 0;
  while r ≥ y loop
     r := r-y;
     q := q+1;
  end loop
end
```

$\{\Psi\} \equiv x = q * y + r\}$

Programazioaren Metodologia. Ariketak

5

5.1

$x<z \wedge lehena(x) \wedge lehena(z) \wedge \neg\exists y(x<y<z \wedge \cancel{y\ mod}\ lehena(y)) \equiv elkarsegida(x,z)$

non $lehena(x) \equiv x>1 \wedge \exists i(1<i<x \wedge x \bmod i \neq 0)$

5.2

~~handiena (t(k))~~ $handiena(t(1..n), t(k))$

non $handiena(x) \equiv \forall i(1\leq i\leq n \rightarrow A(i)<\cancel{A}(k))$

5.3

$Permutazioa(B(1..n), A(1..n)) \wedge Gorantz(A(1..n))$

non $permutazioa(B(1..n), A(1..n)) \equiv \forall i(1\leq i\leq n \rightarrow N_j(1\leq j\leq n \wedge A(i)=A(j)) =$

$= N_k(1\leq k\leq n \wedge A(i)=A(k))$

non $Gorantz(A(1..n)) \equiv \forall i(1\leq i\leq n \cancel{\rightarrow} \wedge A(i)\leq A(i+1))$

5.4

$\forall i(1\leq i\leq n \rightarrow Agerpenkopurua(A(i), A(1..n), 1, n, B(i)))$

5.5

~~Agerpen kopurua~~

$\forall i(1\leq i\leq n \rightarrow Agerpenkopurua(A(i), A(1..n), 1, n, y)) \wedge Agerpenkopurua(x, A(1..n), 1, n, z) \wedge$
$y\leq z$

non $Agerpenkopurua(x, A(1,n), i, j, y) \equiv (2.1)$

6.1

p zenbakia n-ren faktore lehena da.

$n \bmod p = 0 \wedge \text{lehena}(p)$

6.2

x eta y zenbakiek ez dute faktore lehenik konpartitzen.

$\neg\exists z(\text{lehena}(z) \wedge x \bmod z = 0 \wedge y \bmod z = 0)$

6.3

A(1..n) bektoreak x zenbakiaren faktorizazioa errepresentatzen du

(x = 100' bada, A = [2, 2, 5, 5] izan daiteke.

$\prod_{i=1}^{n} A(i) = x \wedge \forall i(1 \leq i \leq n \rightarrow A(i) \leq A(i+1))$

6.4

A(1..n) bektorean A(1..k) zenbakiaren faktore lehen guztiak agertu eta

B(1..k) faktore lehenen anizkoiztasun balioak.

$\forall i(1 \leq i \leq k \rightarrow \text{faktore lehena}(A(i), x) \wedge \neg\exists j(i \leq j \leq k \rightarrow A(i) = A(j) \wedge i \neq j) \wedge$

$\wedge$ anizkoiztasun balioa da$(B(i), A(i)))$

non anizkoiztasunBalioaDa$(x, y) \equiv$ faktore lehena$(x, y) \wedge \exists b(x^b \bmod y = 0)$

6.

Aurre:

Post: $B(i) = $ faktore lehena$(A(i), x) \rightarrow A(j)^{B(j)} \bmod x = 0 \wedge$

Aurre: $\{n \geq 1 \wedge x \geq 1\}$

Post: $\{z = N i(1 \leq i \leq n \rightarrow A(i) \bmod x = 0 \wedge \text{lehena}(A(i))\}$

4) Predikatuen bideoa

4.1

Agerpen_pos $(A(1..n), x, k)$

$\equiv$

4.2

Batura_ondoz_ondoko(z)

$\equiv$

4.3

Berredura_txikiena(x,y)

$\equiv$

4.4

Bigarren Ariketa Orria

2.1

$\text{agerpenkopurua}(x, A(1..n), i, j, y) \equiv$

$1 \le i \le j \le n \land y = Nk(i \le k \le j \land A(k) = x)$

2.3

$\forall i (1 \le i \le n \rightarrow \text{agerpenkopurua}(A(i), A(1..n), 1, n, 2))$

2.4 $\forall i (1 \le i \le n \rightarrow \text{agerpenkopurua}(A(i), A(1..n), 1, n, 0))$

5

5.1

A beltorello osagaiak permutatzen ditu

$\{\Phi\} \equiv \{A(1..n) \,/\, n \geq 1\}$

$\{\Psi\} \equiv \{\prod_{i=1}^{n} A(i)\}$

5.2

A beltorello osagaiak gorantz ordenatu.

$\{\Phi\} \equiv \{A \; n \geq 1\}$

$\{\Psi\} \equiv \{\forall i (1 \leq i \leq n \wedge A(i) < A(i+1)\}$

5.3

$\{\Phi\} \equiv \{n > 1\}$

$\{\Psi\} \equiv$ Zerra_forma $\leftrightarrow \forall i (1 \leq i \leq n \rightarrow ((A(i) > A(i-1) \wedge A(i) < A(i+1)) \vee (A(i) < A(i-1) \wedge A(i) > A(i$

6

6.1

a) $\{\Phi\} \equiv \{true\}$

$\{\Psi\} \equiv \{biderr = x * y\}$

b)

$\{\Phi\} \equiv \{x = a\}$

$\{\Psi\} \equiv \{x = a * y\}$

6.2

a)

Programazioaren Metodologia

Procedure Eguneratu (A : in out)

```
begin
   i := 0;
   while i < n loop
      i := i + 1;
      A(i) := A(i) + 10;
   end loop;
end;
```

$\{\Phi\} \equiv \{ n \geq 1 \wedge A(1..n) = (a_1, a_2, \ldots a_n) \}$

$\{\Psi\} \equiv \{ \forall j (1 \leq j \leq n \rightarrow A(j) = a_i + 10 \}$

Programazioaren Metodologia

1. Gaia. Programen Espezifikazioa

Asertzioak: egoera-multzoak adierazteko formulak

Programa baten konputazio-egoera: exekuzioaren une batetako aldagai guztien balioak. Programa funtzio bezala ikus daiteke,

Programa: hasierako egoera → amaierako egoera

Expresio logikoak programetan txertatzen direnak iruzkin modura.

Asertzio bakoitzak puntu batean gerta daitezkeen egoeren multzoa (infinitu izan daiteke) errepresentatzen du.

Adibidea

$\{n >= 1\}$ = Aurre

```
begin
i:=0; b:=0;
while i<n loop
      i:=i+1;
      b:=b+A(i);
end loop;
end;
```

$$\left\{ b = \sum_{j=1}^{i} A(j) \right\}$$

A | 3 | 8 | 4 | ... | 15 |

iterazioa	i	b
1	0	0
	1	3
	2	11
	3	15
	4	⋮
	⋮	

$\left\{ b = \sum_{j=1}^{n} A(j) \right\}$ = Post

Adibideak. Lehen mailako logika

	True	False
$\forall i (1 \le i \le n \rightarrow A(i) = B(i)+1)$	A: 1, 2, 3, 4, 5 B: 0, 1, 2, 3, 4	A: 0, 2, 4, 3 B: 1, 2, 3, 4
$\exists i (1 \le i \le n \cancel{\rightarrow} \wedge A(i) = 0)$	A: 3, 2, 1, 0	A: 5, 4, 5, 2, 1

Programazioaren Metodologia

$\{\phi\} \equiv \{\forall i (1 \le i \le n \rightarrow A(i) \ne 0\}$ $\{\psi\} \equiv \{kont = N i (1 \le i \le n \wedge x \bmod A(i) = 0)\}$

Aurrebaldintza Postbaldintza

```
k := 0;
      ← {n ≥ 1 ∧ k = 0}
kont := 0;
      ← {n ≥ 1 ∧ kont = 0}
while k < n loop
      ← {n ≥ 1 ∧ kont = N i (1 ≤ i ≤ k ∧ x mod A(i) = 0}
   k := k+1;
      ← ~~{n ≥ 1 ∧ kont = N i (1 ≤ i ≤ j+1~~
   if x mod A(i) = 0 then kont := kont+1; end if;
      ← {n ≥ 1 ∧ kont = N i (1 ≤ i ≤ k ∧ x mod A(i) = 0)}
end loop;
```

Ordezpenaren Adibideak:

$$(x^3 \ge 0 \wedge x+z<5)^{A(i)}_{x} = (A(i)^3 \ge 0 \wedge A(i)+z<5)$$

$$\left(\prod_{i=1}^{k} A(i) = x\right)^{8}_{k} = \left(\prod_{i=1}^{8} (A(i) = x\right)$$

$$\forall i (1 \le i \le n \rightarrow A(i) = x)^{i-1}_{x}$$

$$(\forall k (1 \le k \le n \rightarrow A(k) = x)^{i-1}_{x} = (\forall k (1 \le k \le n \rightarrow A(k) = i-1)$$

$$k = 0 \rightarrow \forall j (1 \le j \le k \rightarrow A(j) = 0)$$

Formulak idazteko pausuak:

1) Esaldia ulertu eta anbiguotasuna badago erabakia hartu
2) Identifikatu zeintzuk izango diren aldagai libreak.
3) Pentsatu zein kuantifikatzaile behar dugun.

3. Gaia. Programen egiaztapena

Programa baten adibidea:

1. agindua [$z := x;$ $\{\phi\} \equiv \{y \geq 1\}$

2. agindua [$kont := 1;$ $\{y \geq 1 \land z = x\}$

$\{y \geq 1 \land z = x \land kont = 1\}$

3. agindua [while $kont < y$ loop

$\{kont < y \land$

3.1. agindua [$z := z + x;$

$\{kont < y \land$

3.2. agindua [$kont := kont + 1;$

end loop; $\{kont \leq y \land$

$\{\psi\} \equiv \{z = x * y\}$

Aginduen bitarteren ~~asertzioa~~ asignazio berriak egongo dira beti.

Hoare-ren sistema formala

Programen zuzentasun partziala eta totala:

Axiomak: Egiazkoak diren oinarrizko propietateak

Inferentzia erregelak: nola deduzitu zerbait beste objektu batetatik.

Zuzentasun partzialari buruzko baieztapena:

$\{\phi\} \equiv \{x = a \land y = b\}$

$lag := x;$

$x := \cancel{x};$

$\cancel{x} := lag;$

$\{\psi\} \equiv \{x = b \land y = a\}$

Asignazioaren Axioma:

$\{def(t) \land \psi_x^t\}\ x := t\ \{\psi\}$

adibidea:

① $\{kont+1 \leq y\}\ kont := kont+1\ \{kont \leq y\}$
$\{\varphi\}$ $\{\psi\}$

② $\{kont < y \rightarrow kont+1 \leq y$
$\{\phi\}$ $\{\psi\}$

③ $\{kont < y\}\ kont := kont+1\ \{kont \leq y\}$
$\{\phi\}$ $\{\psi\}$

OBE (1,2)

Ondorioen erregela:

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

Bere bi aldeak:

$$\frac{\varphi \rightarrow \varphi_1,\ \{\varphi_1\}\ P\ \{\psi\}}{\{\varphi\}\ P\ \{\psi\}} \qquad \frac{\{\varphi\}\ P\ \{\psi_1\},\ \psi_1 \rightarrow \psi}{\{\varphi\}\ P\ \{\psi\}}$$

Bigarren adibidea:

① $\{y/z \neq 1\}\ x = y/z\ \{x \neq 1\}$

② $z \neq 0 \wedge \cancel{z} = 0 \rightarrow y/z \neq 1$

③ $\{z \neq 0 \wedge y = 0\}\ x = \frac{y}{z}\ \{x \neq 1\}$

```
function Badago_x (B: in ~~~x) return Booleen

begin
   Dago := False;
   I := 1;
   while I <= B'Last and Dago := False loop
      If B(I) = x then
         Dago := true
      else
         I := I+1;
      end if;
   end loop;
   return Dago;
```

1.1 Berredura := 1 ; I := 1   Aurre: pos ≥ 0

```
while i < pos loop
   berredura := berredura * 2 ;
   I := I+1;
end loop
```

Post: 2^{pos-1} eragiketa egingo du

1.3

```
berredura := 1;
while (berredura <= x) loop
berredura := berredura * 2;
end loop;
```

Aurre: x >= 0

Post: $2^n >= x$, n txikiena

2011-ko azterketa

①

1)

P zenbakia n-ren faktore lehena da.

$lehena(p) \wedge n \bmod p = 0 \equiv faktorelehena(n,p)$

2)

$\neg \exists z \{ \exists t (faktorelehena(x,z) \wedge faktorelehena(y,t) \wedge z = t)$

3)

$A(1..n)$ eta x

$\cancel{\forall i (1 \leq i \leq n \rightarrow x \bmod A(i) = 0 \wedge \ldots)}$

$\forall i (1 \leq i \leq n \rightarrow faktorelehena(n, A(i)) \wedge \prod_{i=0}^{n} A(i) \equiv faktorelehengustiak(A(1..n))$

4)

$A(1..n)$ bektoreko $A(1..k)$ sekzioan x zenbakiaren faktore lehen guztiak

~~faktorelehengustiak(A(1..n), x)~~

$1 \leq k \leq n \wedge \forall i (1 \leq i \leq k \rightarrow lehena(A(i)) \wedge x = \prod_{i=0}^{k} A(i)^{B(i)}$

②

1)

Aurre: $x \geq 0 \wedge n \geq 1$

Post: $\forall i (1 \leq i \leq n \rightarrow faktoreLehena(A(i), x) \rightarrow x \bmod A(i)^{B(i)} = 0 \wedge$

$\cancel{x \bmod (A(i)) \neq 0 \rightarrow B(i) = 0}$

$\forall j (B(i) < j \leq x \rightarrow x \bmod B(i)^{j} \neq 0 \wedge$

$(\neg faktoreLehena(A(i), x) \rightarrow B(i) = 0$

2)

Aurre: $\{n \geq 1 \land x > 0\}$

Post: $\{z = N i (1 \leq i \leq n \rightarrow$ faktore lehena $(x, A(i))\}$

3

1)

$\{1 \leq i \leq n \land A(i) \neq 0\}$ $k := x \bmod A(i)$ $\{(k = 0) \leftrightarrow$ faktore-lehena $(A(i), x)\}$

$A(1, 2, 3, 4, 5)$

$\{1 \leq 4 \leq 5 \land 4 \neq 0\}$ $k := 8 \bmod 4$ $\{(k=0) \leftrightarrow$ faktore lehena $(A(i), x)$

$A(i) = 4$ izanda $k = 0$ izango da, baina 4 ez da x-en faktore lehena,

2)

$\{1 \leq i \leq n \land$ lehena $(A(i))\}$

$k := x \bmod A(i)$

$\{(k=0) \leftrightarrow$ faktore lehena $(A(i), x)$

Bagoaz:

~~$\{1 \leq i \leq n \land$ lehena $(A(i))\}$~~

$\rightarrow$

~~$k := x \bmod A(i)$ $\{1 \leq i \leq n \land$ lehena $(A(i))\}$~~

$(1 \leq i \leq n \land$ lehena $(A(i)) \rightarrow (1 \leq i \leq n \land A(i) \neq 0 \land x \bmod (A(i)) = 0) \leftrightarrow$ faktore lehena $(A(i), x)$

$k := x \bmod A(i)$

$\{$ ~~$1 \leq i \leq n \land A(i) \neq 0$~~ $\land (k = 0) \leftrightarrow$ faktore lehena $(A(i), x)$ ~~AA~~

4 3) $\{1 \leq i \leq n \land$ lehena $(A(i))\}$

$k := x \bmod A(i)$

$\{k = 0 \leftrightarrow$ faktore lehena $(A(i), x)$ 1,2 eta ODE

4.6

$\forall j (i \le j \le i+y \rightarrow A(j)=1) \wedge \forall j (1 \le j < n+y \wedge j \ne i \rightarrow$

$\not\exists k (j \le k \le j+y \wedge A(k)=1) < y)$

4.9

$\forall i (1 \le i \le m-n+1 \wedge \forall j (1 \le j \le n \rightarrow A(j) = B(i+j-1)$

5.5

A(1..n) bektorean gehien agertzen den elementua x da.

$\forall t (Agerpenkopurua(A(i), A(1..n), 1, n, t) \wedge Agerpenkopurua(x, A(1..n), 1, n, y) \wedge t < y$

$\forall i (1 \le i \le n \wedge A(i) \ne x)$

3)

$\{ bikoitia(k) \wedge y * z^k = p \}$

$k := k/2$

$\{ y * z^{2k} = p \}$

$\{ bikoitia(k) \wedge y * z^k = p\} \rightarrow (y * z^k = p)$

$(y * z^k = p)$

4.1

$\{n \geq 1 \wedge i = 0\}$

zeronik_ez := true

$\{0 \leq i \leq n \wedge (zeronik\_ez \leftrightarrow \forall k(1 \leq k \leq i \rightarrow A(k) \neq 0)\}$

$(n \geq 1 \wedge i = 0) \rightarrow (0 \leq i \leq n \wedge true \leftrightarrow \forall k(1 \leq k \leq i \; A(k) \neq 0)$

$\{(0 \leq i \leq n \wedge true \leftrightarrow \forall k(1 \leq k \leq i \rightarrow A(k) \neq 0$

zeronik_ez := true

$\{0 \leq i \leq n \wedge zeronik\_ez \leftrightarrow \forall k(1 \leq k \leq i \rightarrow A(k) \neq 0\}$

$\{n \geq 1 \wedge i = 0\}$

zeronik_ez := true

$\{0 \leq i \leq n \wedge zeronik\_ez \leftrightarrow \forall k(1 \leq k \leq i \rightarrow A(k) \neq 0)$

4.2

$\{i = j^k \wedge i < w\}$

$i := i * j;$

$\{i = j^{k+1}\}$

1. $(i = j^k \wedge i < w) \rightarrow (ij = j^{k+1}) \cancel{\wedge \; i < w)}$

2. $\{ij = j^{k+1}\}$

$i := ij$

$\{i = j^{k+1}\}$

3. $\{i = j^k \wedge i < w)$

$i := ij$

$\{i = j^{k+1}\}$

1,2ek OBE 4

5)

$\{batura = g\}$

$g := g+1;$

$batura := batura + g;$

$\{batura = 2*g - 1\}$

1. $(batura = g) \rightarrow (batura = g+1-1)$

2. $\{batura = g+1-1\}$

$g := g+1;$

$\{batura = g-1\}$ AA

3. ~~$(\{batura = g-1\} \rightarrow (batura + g = g + g - 1)$~~

~~batura~~

3. $\{batura = g\}$

$g := g+1;$

$\{batura = g-1\}$ 1,2 eta ODE

4. $(batura = g-1) \rightarrow (batura + g = 2*g-1)$ AA

5. $\{batura + g = 2*g-1\}$

$batura := batura + g;$

$\{batura = 2*g-1\}$ AA

6. $\{batura = g-1\}$

$batura := batura + g;$

$\{batura = 2*g-1\}$ 4, 5 eta ODE

7. $\{batura = g\}$

$g := g+1$

$batura := batura + g;$

$\{batura = 2*g-1\}$ 3, 6 eta KPE

7.

A)

$\{4 * 6 = 5^{3+1} - 1\}$

$i := i+1;$

$31 := 6 + 5^{*2}$

$\{4 \times 31 = 5^2 - 1\}$ Kontra Adibidea $4 \times 31 \neq 5^2 - 1$

B)

~~$\{x = 5^{k+1}\}$~~

~~$k := k+1;$~~

~~$x := x + 5^k$~~

~~$\{x = 5^{k+1}\}$~~

~~1. $\{x = 5^{k+1}\}$~~

~~$k := k+1;$~~

~~$\{x = 5^k\}$~~

~~2. $\{x = 5^k\} \rightarrow (x + x = x + 5^k)$~~

$\{4 \times x = 5^{k+1} - 1\}$

$k := k+1$

$x := x + 5^k$

$\{4 \times x = 5^k - 1\}$

1. $(4 \times x = 5^{k+1} - 1\} \rightarrow$

$k := k+1$

$\{4 * x = 5^k - 1\}$ AA

2. $(4 * x = 5k - 1) \rightarrow (4 * x + 4 \times 5^k = 5^k - 1 + 4 \times 5^k) \rightarrow$

$\rightarrow 4 * (x + 5^k) = 5^k - 1 + 4 \times 5^k$

$\{4 * x = 5^{k+1} - 1\}$

1. $\{1 \le k \le n \wedge \cancel{x = 2 \times (k+1)} \; x + 2k(k+1) = \sum_{k=1}^{n} (2 \times k - 1) \quad \{1 \le k \le n \wedge x = k^2\}$

2. $\{1 \le k \le n \wedge x + 2k = \sum_{k=1}^{k+1} (2k+1)\} \quad \{1 \le k \le n \wedge x = 2k-1\}$

3. $\{1 \le k \le n \wedge x + 2k = \sum_{i=1}^{k+1} (2k+1) \quad \{1 \le k \le n \wedge x = k^2$

$(1 \le k \le n \wedge x = k^2) \rightarrow (1 \le k \le n \wedge x = \sum_{i=1}^{k+1} (2k+1)) \rightarrow$

$k \mathrel{+}=$

$\rightarrow (1 \le k+1 \le n \wedge x + 2(k+1) = \sum_{i=1}^{k} (2k-1) + 2k \rightarrow$

$\rightarrow (1 \le k+1 \le n \wedge x + 2k = \sum_{i=1}^{k+1} 2k+1$

$\{\cancel{1 \le i \le n \wedge A(i) \ne 0}\}$

$k := \cancel{x \bmod}$

a)

$\{1 \le i \le n \wedge \text{lehere}(A(i))\}$

$k := x \bmod A(i)$

$\{(k=0) \leftrightarrow \text{fattore-lehere}(A(i), x)\}$

1. $(1 \le i \le n \wedge \text{lehere}(A(i))) \rightarrow (1 \le i \le n \wedge A(i) \ne 0 \wedge x \bmod A(i) = 0) \rightarrow$

2. $\{1 \le i \le n \wedge A(i) \ne 0 \wedge x \bmod A(i) = 0\}$

$k := x \bmod A(i)$

$\{1 \le i \le n \wedge A(i) \ne 0 \wedge (k=0)\}$

3. $(1 \le i \le n \wedge A(i) \ne 0 \wedge (k=0)) \rightarrow ((k=0) \leftrightarrow \text{fattore-lehere}(A(i), x))$

4. $\{1 \le i \le n \wedge \text{lehere}(A(i))\}$

$k := x \bmod A(i)$

$\{(k=0) \leftrightarrow \text{fattore-lehere}(A(i), x)$

5/

$\{1 \le k \le n \wedge x = k^2\}$

$k := k+1;$

$x := x + 2*k - 1;$

$\{1 \le k \le n \wedge x = k^2\}$

$x + k+1-1 = k(k+1)^2$

1. $(1 \le k < n \wedge x = k^2\} \rightarrow (1 \le k \le n \wedge \cancel{x + k+1-1 = (k+1)^2})$

$\{1 \le k+1 \le n \wedge x + k+1-1 = k(k+1)^2\}$

$k := k+1$

$\{1 \le k \le n \wedge \cancel{x + k - 1 = k^2}$
$x + k - 1 = (k-1)k\}$

a)

~~∃∃∃(Adig(x, z) ∧ Adig(x, u))~~

$\exists z \exists u \, (Adig(x,z) \wedge Adig(x,u) \wedge \rightarrow \exists t = z \circ u)$

b)

$\exists k \{ 1 \leq k \leq n \wedge \forall i (1 \leq i \leq k) \rightarrow A(k) \geq 0 \wedge Adig(A(k), z)$

c)

$\forall i ((1 \leq i \leq n \rightarrow A(i) \geq 0) \wedge Adig(A(i), z)) \equiv Azkendigitua(A(1..n), z)$

$rc \; \forall i (1 \leq i \leq n \rightarrow Adig(A(i), z)$

2

Aurre: $A\{n \geq 1 \wedge \forall i (1 \leq i \leq n \rightarrow A(i) \geq 0)\}$

Post: $\{Digitu\_Berdina \leftrightarrow Azkendigitua(A(1..n), z)\}$

6.1

$\{1 \le v \le z \wedge x^z \times y^v = w\}$

$z := z+1;$

$w := w * x * y;$

$v := v+1;$

$\{1 < v \le z \wedge x^z \cdot y^v = w\}$

1. $(1 \le v \le z \wedge x^z * y^v = w) \to (1 \le v \le z \wedge x^z \cdot x \cdot y^v = w \cdot x)$ (A.A)

2. $\{1 \le v \le z-1 \wedge x^{z+1} \cdot y^v = w \cdot x\}$

$z := z+1;$

$\{1 \le v \le z \wedge x^z \cdot y^v = w \cdot x\}$

3. $\{1 \le v \le z \wedge x^z \cdot y^v = w\}$

$z := z+1;$

$\{1 \le v \le z \wedge x^z \cdot y^v = w \cdot x\}$ 1, 2 etc ODE

4. $(1 \le v \le z \wedge x^z \cdot y^v = w \cdot x) \to (1 \le v \le z \wedge x^z \cdot y^v \cdot y = w \cdot x \cdot y) \to$

$\to (1 \le v \le z \wedge x^z \cdot y^{v+1} = w x y)$ AA

5. $\{1 \le v \le z \wedge x^z \cdot y^{v+1} = w x y\}$

$w := w \cdot y \cdot x;$

$\{1 \le v \le z \wedge x^z \cdot y^{v+1} = w\}$

6. $\{1 \le v \le z \wedge x^z \cdot y^v = w \cdot x\}$

$w := w \cdot y \cdot x;$

$\{1 \le v \le z \wedge x^z \cdot y^{v+1} = w\}$ 4, 5, ODE

7. $\to 1 < v+1 \le z \wedge x^z \cdot y^{v+1} = w$

8. $\{1 \le v+1 \le z \wedge x^z \cdot y^{v+1} = w\}$

$v := v+1$

$\{1 < v \le z \wedge x^z \cdot y^v = w\}$

$\{1 \le v \le z \wedge x^z \cdot y^v = w\}$

$z := z+1$

$w := w \cdot y x$

$v := v+1$

$\{1 < v \le z \wedge x^z \cdot y^v = w\}$

2.1

$\{\phi\} \equiv \{n \geq 1\}$

$\{\psi\} \equiv \{$dago $\leftrightarrow$ badago $(A(1..n), x)$

```
Am := A(1)
                 {n ≥ m = A(1)}
I := 1;
                 {n ≥ 1 ∧ m = A(1) ∧ I = 1}
while i ≤ n ∧ ~~Badago~~ dago = false loop
                 {n ≥ 1 ∧ 1 ≤ i ≤ n ∧ dago = false}
    if A(i) = x then
                 {n ≥ 1 ∧ 1 ≤ i ≤ n ∧ dago = false ∧ A(i) = x
        Dago := true
    else
        ~~Dago := false~~
        I := i+1
    end if;
end loop;
    if Dago = true then
        Badago := true; ~~then~~
    else
        Badago := false;
    end if;
```

$\{\phi\} \equiv \{n \geq 1\}$

$\{\psi\} \equiv \{$handiena $(A(1...n), m)\}$

```
m := A(1)
i := 2;      {n ≥ 1 ∧ m = A(1)}
while i ≤ n loop     {n ≥ 1 ∧ m = A(1) ∧ i := 2}
             {n ≥ 1 ∧ i ≤ n ∧ handiena(A(1..i-1), m)}
    if m < A(i) then
             {n ≥ 1 ∧ handiena(A(1..i-1), m) ∧ 2 ≤ i ≤ n
        m := A(i);
             {n ≥ 1 ∧ handiena (A(1..i-1), m) ∧ 2 ≤ i ≤ n}
    end if;
    i := i+1;    {n ≥ 1
end loop;    {n ≥ 1
```

```
i := 1;
while i < n
    i := i+1
    if m < A(i) then
        m := A(i);
    end if;
end loop;
```

①

{true}
if x>y then
  z:= x;
else
  z:= y;
end if;
{(x ≥ y ∧ z:= x) ∨ (x < y ∧ z = y)}

2.1

{ i = n ∧ ¬ badago (A(1..n-1), x)}
if A(i) = x then
  badago := true;
else
  badago := false;
end if;
{ dago ⟺ badago (A(1.. n-1), x)

2.2

{1 ≤ i < n ∧ handiena (A(1..i), m)}
  i := i+1;
  if m < A(i) then
    m := A(i)
  end if
{ 1 ≤ i ≤ n ∧ handiena (A(1..i), m)}

5.3

$\{\neg berdin\}$

if $x = y$ then

berdin := true;

end if;

$\{berdin \Leftrightarrow x = y\}$

Eskema

(A)

$\{\neg berdin \land x = y\}$ berdin := true $\{berdin \Leftrightarrow x = y\}$

(B) $\{\neg berdin \land x \neq y\} \rightarrow (berdin \Leftrightarrow x = y$

(C) $\neg berdin \rightarrow def(x=y)$

Frogapena

(A)

1. $\{true \Leftrightarrow x = y\}$ berdin := true $\{berdin \Leftrightarrow x = y\}$

2. $(\neg berdin \land x = y) \rightarrow (x = y) \rightarrow (x = y \land true) \rightarrow (x = y \land true) \lor (\neg true \land x \neq y) \rightarrow true \Leftrightarrow (x = y)$

3. $\{\neg berdin \land x = y\}$ berdin := tru $\{berdin \Leftrightarrow true\}$ 2,1 (ODE)

(B) 4. $(\neg berdin \land x \neq y) \rightarrow (\neg berdin \neq y) \lor (berdin \land x = y) \rightarrow (berdin \Leftrightarrow x = y$

5. $def(x=y)$

6. $\{\neg berdin\}$ if $x = y$ then berdin := true; end if; $\{berdin \Leftrightarrow x = y$ 3,4,5 (ODE)

4.1

$\{\emptyset \land B\}\ I_1; \{\varphi\}, \{\emptyset \land \neg B_1 \land B_2\}\ I_2; \{\varphi\} \ldots \{\emptyset \land \neg B1 \land \neg B2 \land \ldots \land B_n\}\ I_n; \{\varphi\}, \{\emptyset \land \ldots \land \neg B_n\}\ I_{n+1} \{\varphi\};$