3. Gaia: Programen Egiaztapena

4. Ariketa-orria: Iterazioen egiaztapena

1. Hurrengo baieztapenetan aukeratu zuzena den inbariantea:

1.1. Programa honek x elementua $A(1..n)$ bektorean agertzen den ala ez erabakitzen du.

$\{ n \geq 1 \}$

```
i := 0; dago := false;
```

INB1 $\equiv \{ (\mathit{dago} \leftrightarrow \exists j \ (1 \leq j \leq i \ \wedge \ A(j) = x)) \ \wedge \ 0 \leq i \leq n \}$ [X]

INB2 $\equiv \{ (\mathit{dago} \ \wedge \ \exists j \ (1 \leq j \leq i \ \wedge \ A(j) = x)) \ \wedge \ 0 \leq i \leq n \}$ [ ]

```
while not dago and i < n loop
   i := i+1;
   if A(i) = x then
      dago := true;
   end if;
end loop;
```

$\{ \mathit{dago} \leftrightarrow \exists j \ (1 \leq j \leq n \ \wedge \ A(j) = x) \}$

1.2. Programa honek *lehen* aldagai boolearrean x zenbaki arrunta lehena den ala ez erabakitzen du.

$\{ x \geq 2 \}$

```
d := 2;
```

INB1 $\equiv \{ 1 < d \leq x \ \wedge \ \forall i \ (1 < i < d \ \rightarrow \ x \ \mathit{mod} \ i \neq 0) \}$ [X]

INB2 $\equiv \{ 1 < d \leq x \ \leftrightarrow \ \forall i \ (1 < i < d \ \rightarrow \ x \ \mathit{mod} \ i \neq 0) \}$ [ ]

```
while x mod d /= 0 loop
   d := d+1;
end loop;
lehen := (d = x);
```

$\{ \mathit{lehen} \leftrightarrow \forall i \ (1 < i < x \ \rightarrow \ x \ \mathit{mod} \ i \neq 0) \}$

1.3. Programa honek x zenbaki arruntaren faktoriala kalkulatzen du.

$\{ x \geq 0 \}$

```
f := 1; t := x;
```

$$\textbf{INB1} \equiv \{ f = \prod_{i=1}^{t-1} i \wedge t \geq 0 \} \qquad [\ \ ]$$

$$\textbf{INB2} \equiv \{ f = \prod_{i=t+1}^{x} i \wedge t \geq 0 \} \qquad [X]$$

$$\textbf{INB3} \equiv \{ f = \prod_{i=t-1}^{x} i \wedge t \geq 0 \} \qquad [\ \ ]$$

$$\textbf{INB4} \equiv \{ f = \prod_{i=t}^{x} i \wedge t \geq 0 \} \qquad [\ \ ]$$

```
while t >= 1 loop
   f := f*t;
   t := t-1;
end loop;
```

$\{ f = \prod_{i=1}^{x} i \}$

2. Hurrengo iterazioen inbariantea asmatu:

2.1. Honako programa honek $A(1..n)$ bektoreko minimoa kalkulatzen du m aldagaian.

$\{ n \geq 1 \}$

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

$\textbf{INB} \equiv \{ \ \underline{txikiena(A(1..k), m) \wedge 1 \leq k \leq n} \ \}$

$\textbf{E} \equiv \underline{n - k + 1}$

$\{ txikiena(A(1..n), m) \}$

non:

$$txikiena(A(1..n), m) \equiv \exists i \ (1 \leq i \leq n \wedge A(i) = m) \wedge \forall j \ (1 \leq j \leq n \rightarrow A(j) \geq m)$$

2.2. Programa honek $A(1..n)$ taulako elementuak atzekoz aurrera jartzen ditu.

$\{ \; n \geq 1 \; \wedge \; A = (a_1, \ldots, a_n) \; \}$

```
k := 1;
```

$\textbf{INB} \equiv \{ \; \underline{\forall i \; (\; 1 \leq i < k \; \rightarrow \; A(i) = a_{n-i+1} \;)}$
$\underline{\wedge \; \forall i \; (\; k \leq i \leq n - k + 1 \; \rightarrow \; A(i) = a_i \;)}$
$\underline{\wedge \; \forall i \; (\; n - k + 1 < i \leq n \; \rightarrow \; A(i) = a_{n-i+1} \;)}$
$\underline{\wedge \; 1 \leq k \leq \frac{n}{2} + 1} \; \}$

$\textbf{E} \equiv \; \underline{\frac{n}{2} - k + 1}$

```
while k <= n/2 loop
   lag := A(k);
   A(k) := A(n-k+1);
   A(n-k+1) := lag;
   k := k+1;
end loop;
```

$\{ \; \forall i \; (\; 1 \leq i \leq n \; \rightarrow \; A(i) = a_{n-i+1} \;) \; \}$

2.3. A taulako elementuen erdiak baino gehiago, B taulan posizio berean daudenak baino handiagoak diren ala ez adieraziko du b aldagai boolearrak.

$\{ \; n \geq 1 \; \}$

```
i := 1; z := 0;
```

$\textbf{INB} \equiv \{ \; \underline{z = \mathcal{N} j \; (\; 1 \leq j < i \; \wedge \; A(j) > B(j) \;) \; \wedge \; 1 \leq i \leq n + 1} \; \}$

$\textbf{E} \equiv \; \underline{n - i + 1}$

```
while i <= n loop
   if A(i) > B(i) then
      z := z+1;
   end if;
   i := i+1;
end loop;
b := (z > n/2);
```

$\{ \; b \; \leftrightarrow \; \mathcal{N} j \; (\; 1 \leq j \leq n \; \wedge \; A(j) > B(j) \;) > \frac{n}{2} \; \}$

3. Dokumentatu markatzen diren asertzioekin honako programa iteratibo hauek:

3.1. Honako programa honek $|x - y|$ adierazpenaren balioa uzten du d aldagaian.

Aurre $\equiv \{ \; true \; \}$

```
d := 0;
if x <= y then
   u := x;
   z := y;
else
   u := y;
   z := x;
end if;
```

$\phi_1 \equiv \{ \; d = 0 \; \wedge \; u = min(x, y) \; \wedge \; z = max(x, y) \; \}$

INB $\equiv \{ \; d = max(x, y) - z \; \wedge \; u = min(x, y) \; \wedge \; u \leq z \; \}$

E $\equiv z - min(x, y) \equiv z - u$

```
while u /= z loop
```

$\phi_2 \equiv \{ \; d = max(x, y) - z \; \wedge \; u = min(x, y) \; \wedge \; u < z \; \}$

```
   z := z-1;
```

$\phi_3 \equiv \{ \; d = max(x, y) - (z + 1) \; \wedge \; u = min(x, y) \; \wedge \; u < z + 1 \; \}$

```
   d := d+1;
end loop;
```

Post $\equiv \{ \; d = |x - y| \; \}$

3.2. Programak $A(1..n)$ bektorean bakoitiak diren osagaien kopurua eta bikoitiak direnena berdina den ala ez erabakitzen du.

Aurre $\equiv \{ \; n \geq 1 \; \}$

```
i := 0; w := 0; z := 0;
```

INB $\equiv \{ \; 0 \leq i \leq n \; \wedge \; w = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; \wedge$
$v = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 \neq 0 \;) \; \}$

```
while ( i < n ) loop
```

E $\equiv n - i$

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

$\phi_1 \equiv \{ \; 0 \leq i \leq n \; \wedge \; w = \mathcal{N}j \; (\; 1 \leq j < i \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; \wedge$
$v = \mathcal{N}j \; (\; 1 \leq j < i \; \wedge \; A(j) \; mod \; 2 \neq 0 \;) \; \}$

```
   if ( A(i) mod 2 = 0 ) then
```

$\phi_2 \equiv \{ \; 0 \leq i \leq n \; \wedge \; w + 1 = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; \wedge$
$v = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 \neq 0 \;) \; \}$

```
      w := w+1;
   else
```

$\phi_3 \equiv \{ \; 0 \leq i \leq n \; \wedge \; w = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; \wedge$
$v + 1 = \mathcal{N}j \; (\; 1 \leq j \leq i \; \wedge \; A(j) \; mod \; 2 \neq 0 \;) \; \}$

```
      v := v+1;
   end if;
end loop;
```

$\phi_4 \equiv \{ \; w = \mathcal{N}j \; (\; 1 \leq j \leq n \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; \wedge \; v = \mathcal{N}j \; (\; 1 \leq j \leq n \; \wedge$
$A(j) \; mod \; 2 \neq 0 \;) \; \}$

```
e := (w=v);
```

Post $\equiv \{ \; e \leftrightarrow \mathcal{N}j \; (\; 1 \leq j \leq n \; \wedge \; A(j) \; mod \; 2 = 0 \;) \; = \; \mathcal{N}j \; (\; 1 \leq j \leq n \; \wedge$
$A(j) \; mod \; 2 \neq 0 \;)\}$

3.3. Programak 2ren 0 eta n-ren arteko berreduren batura kalkulatzen du b aldagaian; alegia, $2^0, 2^1, \ldots, 2^n$ segidaren batura kalkulatzen du.

Aurre $\equiv \{\ n \geq 0\ \}$
```
   i := 0; p := 1; b := 1;
   while i < n loop
```
INB $\equiv \{\ 0 \leq i \leq n\ \wedge\ b = \sum_{k=0}^{i} 2^k\ \wedge\ p = 2^i\ \}$
E $\equiv n - i$

$\phi_1 \equiv \{\ 0 \leq i < n\ \wedge\ b = \sum_{k=0}^{i} 2^k\ \wedge\ p = 2^i\ \}$
```
      i := i + 1;
```
$\phi_2 \equiv \{\ 0 \leq i \leq n\ \wedge\ b = \sum_{k=0}^{i-1} 2^k\ \wedge\ p = 2^{i-1}\ \}$
```
      p := p * 2;
```
$\phi_3 \equiv \{\ 0 \leq i \leq n\ \wedge\ b = \sum_{k=0}^{i-1} 2^k\ \wedge\ p = 2^i\ \}$
```
      b := b + p;
   end loop;
```
Aurre $\equiv \{\ b = \sum_{k=0}^{n} 2^k\ \}$

3.4. $A(1..n)$ taula batura berdineko bi sekziotan bana daitekeen ala ez erabakiko du programa honek. Hala bada, i aldagaia izango da banaketa adierazten duen indizea.

Aurre $\equiv \{\ n \geq 1\ \}$
```
   x := A(1); y := 0; k:= 2;
```
INB $\equiv \{\ y = \sum_{j=2}^{k-1} A(j)\ \wedge\ 2 \leq k \leq n+1\ \wedge\ x = A(1)\ \}$
E $\equiv n - k + 1$
```
   while k <= n loop
      y := y+A(k);
      k := k+1;
   end loop;
   i := 1;
```
INB $\equiv \{\ \forall j\ (\ 1 \leq j < i\ \rightarrow\ \sum_{k=1}^{j} A(k) \neq \sum_{k=j+1}^{n} A(k)\ )$
$\wedge\ y = \sum_{k=i+1}^{n} A(k)\ \wedge\ x = \sum_{k=1}^{i} A(k)\ \wedge\ 1 \leq i \leq n\ \}$
E $\equiv n - i$
```
   while x /= y and i < n loop
      i := i+1;
      x := x+A(i);
      y := y-A(i);
   end loop;
   eqsum := (not i = n);
```
Post $\equiv \{\ eqsum\ \leftrightarrow\ \exists j\ (\ 1 \leq j < n\ \wedge\ \sum_{k=1}^{j} A(k) = \sum_{k=j+1}^{n} A(k)\ )\ \}$

4. Programa honek batura eta biderkadura berdina duen $A(1..j)$ sekziorik luzeena mugatzen duen j indizea k aldagaian uzten du. Zuzentasun osoaren frogapenaren eskema asmatu.

```
m := 1; k := 1; bat := A(1); bider := A(1);
while m < n loop
   m := m+1; bat := bat+A(m); bider := bider*A(m);
   if bat = bider then
      k := m;
   end if;
end loop;
```

Soluzioa: Frogatu behar ditugu hurrengo baieztapenak:

- $\{ \phi \}$ `m := 1; k := 1; bat := A(1); bider := A(1);` $\{ \textbf{INB} \}$
- $\textbf{INB} \rightarrow def(m < n)$
- $\{ \textbf{INB} \wedge m < n \}$ `S` $\{ \textbf{INB} \}$

  Baieztapen hau frogatzeko, beste baieztapen hauek frogatu behar dira:

  - $\{ \textbf{INB} \wedge m < n \}$ `m:=m+1; bat:=bat+A(m); bider:=bider*A(m);` $\{ \phi_1 \}$
  - $\{ \phi_1 \wedge bat = bider \}$ `k := m;` $\{ \textbf{INB} \}$
  - $(\phi_1 \wedge \neg(bat = bider)) \rightarrow \textbf{INB}$
  - $\phi_1 \rightarrow def(bat = bider)$

- $(\textbf{INB} \wedge \neg(m < n)) \rightarrow \psi$

5. Hurrengo programako iterazioak inbariantea konserbatzen duela frogatu. Programak x elementua $A(1..n)$ bektorean agertzen den ala ez erabakitzen du.

$\{ n \geq 1 \}$

```
i := 0; dago := false;
while not dago and i < n loop
   i := i+1;
   if A(i) = x then
      dago := true;
   end if;
end loop;
```

$\{ dago \leftrightarrow \exists j \ (1 \leq j \leq n \wedge A(j) = x) \}$

Soluzioa:

Inbariantea honako hau da:

$$\{ (dago \leftrightarrow \exists j \ (1 \leq j \leq i \wedge A(j) = x)) \wedge 0 \leq i \leq n \}$$

Frogapena:

1. $(\, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \wedge \, i < n \,)$
$\rightarrow \, (\, \neg\exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i < n \, \wedge \, \neg dago \,)$

2. $\{ \, \neg\exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i < n \, \wedge \, \neg dago \, \}$
```
i := i+1;
```
$\{ \, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \}$ **(AA)**

3. $\{ \, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \wedge \, i < n \, \}$
```
i := i+1;
```
1, 2 eta **(ODE)**
$\{ \, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \}$

4. $(\, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \wedge \, A(i) = x \,)$
$\rightarrow \, (\, \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \,)$

5. $\{ \, \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \}$
```
dago := true;
```
$\{ \, \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, dago \, \}$ **(AA)**

6. $(\, \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, dago \,)$
$\rightarrow \, (\, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \,)$

7. $\{ \, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \neg dago \, \wedge \, A(i) = x \, \}$
```
dago := true;
```
4, 5, 6 eta **(ODE)**
$\{ \, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \}$

8. $(\, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \wedge \, A(i) \neq x \,)$
$\rightarrow \, (\, \neg\exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \,)$
$\rightarrow \, (\, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \,)$

9. $(\, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \,)$
$\rightarrow \, (\, 0 \leq i \leq n \,) \, \rightarrow \, def(A(i) = x)$

10. $\{ \, \neg\exists j \, (\, 1 \leq j < i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \neg dago \, \}$
```
if A(i) = x then
   dago := true;
end if;
```
7, 8, 9 eta **(ODE)**
$\{ \, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \}$

11. $\{ \, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \wedge \, \neg dago \, \wedge \, i < n \, \}$
```
i := i+1;
if A(i) = x then
   dago := true;
end if;
```
$\{ \, dago \leftrightarrow \exists j \, (\, 1 \leq j \leq i \, \wedge \, A(j) = x \,) \, \wedge \, 0 \leq i \leq n \, \}$ 3, 10 eta **(KPE)**

6. Hurrengo programen zuzentasun osoa frogatu.

6.1. Honako programa honek x eta y zenbaki osokoen biderkadura kalkulatzen du.

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

Soluzioa:

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

```
   z := 0;
   while x /= 0 loop        INB ≡ { z + x × y = a × b ∧ x ≥ 0 }
      z := z+y;
      x := x-1;
   end loop;
```

$\{ \ z = a \times b \ \}$

Zuzentasun partzialaren frogapena:

1. $\{ \ x = a \ \wedge \ a \geq 0 \ \wedge \ y = b \ \}$
   `z := 0;`
   $\{ \ x = a \geq 0 \ \wedge \ y = b \ \wedge \ z = 0 \ \}$ **(AA)**

2. $(\ x = a \ \wedge \ a \geq 0 \ \wedge \ y = b \ \wedge \ z = 0 \ ) \ \rightarrow$
   $(\ x \times y = a \times b \ \wedge \ x \geq 0 \ \wedge \ z = 0 \ )$
   $\rightarrow \ (\ z + x \times y = a \times b \ \wedge \ x \geq 0 \ )$

3. $(\ z + x \times y = a \times b \ \wedge \ x \geq 0 \ \wedge \ x \neq 0 \ ) \ \rightarrow$
   $(\ z + x \times y = a \times b \ \wedge \ x > 0 \ )$

4. $\{ \ z + x \times y = a \times b \ \wedge \ x > 0 \ \}$
   `z := z+y;`
   $\{ \ z - y + x \times y = a \times b \ \wedge \ x > 0 \ \}$ **(AA)**

5. $\{ \ z - y + x \times y = a \times b \ \wedge \ x > 0 \ \}$
   `x := x-1;`
   $\{ \ z - y + (x+1) \times y = a \times b \ \wedge \ x + 1 > 0 \ \}$ **(AA)**

6. $\{ \ z + x \times y = a \times b \ \wedge \ x > 0 \ \}$
   `z := z+y;`
   `x := x-1;`
   $\{ \ z - y + (x+1) \times y = a \times b \ \wedge \ x + 1 > 0 \ \}$ 4, 5 eta **(KPE)**

7. $(\ z - y + (x+1) \times y = a \times b \ \wedge \ x + 1 > 0 \ )$
   $\rightarrow \ (\ z - y + x \times y + y = a \times b \ \wedge \ x \geq 0 \ )$
   $\rightarrow \ (\ z + x \times y = a \times b \ \wedge \ x \geq 0 \ )$

8. $\{ \ z + x \times y = a \times b \ \wedge \ x \geq 0 \ \wedge \ x \neq 0 \ \}$
   `z := z+y;`
   `x := x-1;`
   $\{ \ z + x \times y = a \times b \ \wedge \ x \geq 0 \ \}$ 3, 6, 7 eta **(ODE)**

9. $(\ z + x \times y = a \times b \ \wedge \ x \geq 0 \ \wedge \ x = 0 \ )$
   $\rightarrow \ (\ z + 0 \times y = a \times b \ ) \ \rightarrow \ (\ z = a \times b \ )$

10. $(\ z + x \times y = a \times b \ \wedge \ x \geq 0 \ ) \ \rightarrow \ def(x \neq 0)$

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

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

$\{ z = a \times b \}$ 2, 8, 9, 10 eta **(WHE)**

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

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

$\{ z = a \times b \}$ 1, 11 eta **(KPE)**

Balidazioa:

- Borne adierazpena: $E \equiv x$
- $(z + x \times y = a \times b \wedge x \geq 0 \wedge x \neq 0) \rightarrow (x > 0) \rightarrow E \in \mathbb{N}$
- 1. $(z + x \times y = a \times b \wedge x \geq 0 \wedge x \neq 0 \wedge x = k) \rightarrow (x = k)$

  2. $\{ x = k \}$
  ```
  z := z+y;
  ```
  $\{ x = k \}$ **(AA)**

  3. $\{ x = k \}$
  ```
  x := x-1;
  ```
  $\{ x + 1 = k \}$ **(AA)**

  4. $\{ x = k \}$
  ```
  z := z+y;
  x := x-1;
  ```
  $\{ x + 1 = k \}$ 2, 3 eta **(KPE)**

  5. $(x + 1 = k) \rightarrow (x = k - 1) \rightarrow (x < k)$

  6. $\{ z + x \times y = a \times b \wedge x \geq 0 \wedge x \neq 0 \wedge x = k \}$
  ```
  z := z+y;
  x := x-1;
  ```
  $\{ x < k \}$ 1, 4, 5 eta **(ODE)**

6.2. Programa honek x elementua $A(1..n)$ bektorean zenbat aldiz agertzen den kontatzen du.

```
i := 1; z := 0;
while i <= n loop
   if A(i) = x then
      z := z+1;
   end if;
   i := i+1;
end loop;
```

Soluzioa:

$\{\ n \geq 1\ \}$

```
i := 1; z := 0;
```

INB $\equiv \{\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ i \leq n+1\ \}$

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

$\{\ z = \mathcal{N}j\ (\ 1 \leq j \leq n\ \wedge\ A(j) = x\ )\ \}$

Zuzentasun partzialaren frogapena:

1. $\{\ n \geq 1\ \}$
   `i := 1;`
   $\{\ n \geq i\ \wedge\ n \geq 1\ \wedge\ i = 1\ \}$ **(AA)**

2. $\{\ n \geq i\ \}$
   `z := 0;`
   $\{\ n \geq i\ \wedge\ z = 0\ \wedge\ n \geq 1\ \wedge\ i = 1\ \}$ **(AA)**

3. $\{\ n \geq 1\ \}$
   `i := 1;`
   `z := 0;`
   $\{\ n \geq i\ \wedge\ z = 0\ \wedge\ n \geq 1\ \wedge\ i = 1\ \}$ 1, 2 eta **(KPE)**

4. $(\ n \geq i\ \wedge\ z = 0\ \wedge\ n \geq 1\ \wedge\ i = 1\ ) \rightarrow$
   $(\ 1 \leq i \leq n+1\ \wedge\ z = 0\ \wedge\ 0 = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ )$
   $\rightarrow\ (\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n+1\ )$

5. $(\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ i \leq n+1\ \wedge\ 1 \leq i \leq n\ )$
   $\rightarrow\ (\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ )$

6. $(\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \wedge\ A(i) = x\ )$
   $\rightarrow\ (\ z+1 = \mathcal{N}j\ (\ 1 \leq j \leq i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ )$

7. $\{\ z+1 = \mathcal{N}j\ (\ 1 \leq j \leq i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \}$
   `z := z+1;`
   $\{\ z = \mathcal{N}j\ (\ 1 \leq j \leq i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \}$ **(AA)**

8. $\{\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \wedge\ A(i) = x\ \}$
   `z := z+1;`
   $\{\ z = \mathcal{N}j\ (\ 1 \leq j \leq i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \}$ 6, 7 eta **(ODE)**

9. $(\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ \wedge\ A(i) \neq x\ )$
   $\rightarrow\ (\ z = \mathcal{N}j\ (\ 1 \leq j \leq i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ )$

10. $(\ z = \mathcal{N}j\ (\ 1 \leq j < i\ \wedge\ A(j) = x\ )\ \wedge\ 1 \leq i \leq n\ ) \rightarrow\ def(A(i) = x)$

11. $\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

```
    if A(i) = x then
       z := z+1;
    end if;
```

8, 9, 10 eta **(BDE)**

$\{ z = \mathcal{N}j \; (1 \leq j \leq i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

12. $\{ z = \mathcal{N}j \; (1 \leq j \leq i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

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

$\{ z = \mathcal{N}j \; (1 \leq j \leq i-1 \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i-1 \leq n \; \}$ **(AA)**

13. $(z = \mathcal{N}j \; (1 \leq j \leq i-1 \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i-1 \leq n \;)$
$\quad \rightarrow \; (z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \;)$

14. $\{ z = \mathcal{N}j \; (1 \leq j \leq i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

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

12, 13 eta **(ODE)**

$\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \; \}$

15. $\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

```
    if A(i) = x then
       z := z+1;
    end if;
    i := i+1;
```

11, 14 eta **(KPE)**

$\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \; \}$

16. $\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n \; \}$

```
    if A(i) = x then
       z := z+1;
    end if;
    i := i+1;
```

5, 15 eta **(ODE)**

$\{ z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \; \}$

17. $(z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \; \wedge \; i > n \;)$
$\quad \rightarrow \; (z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; i = n+1 \;)$
$\quad \rightarrow \; (z = \mathcal{N}j \; (1 \leq j < n+1 \; \wedge \; A(j) = x \;) \;)$
$\quad \rightarrow \; (z = \mathcal{N}j \; (1 \leq j \leq n \; \wedge \; A(j) = x \;) \;)$

18. $(z = \mathcal{N}j \; (1 \leq j < i \; \wedge \; A(j) = x \;) \; \wedge \; 1 \leq i \leq n+1 \;) \; \rightarrow \; def(i \leq n)$

19. $\{ n \geq i \; \wedge \; z = 0 \; \}$

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

$\{ z = \mathcal{N}j \; (1 \leq j \leq n \; \wedge \; A(j) = x \;) \; \}$ 4, 16, 17, 18 eta **(WHE)**

20. $\{ n \geq 1 \}$

```
i := 1;
z := 0;
while i <= n loop
   if A(i) = x then
      z := z+1;
   end if;
   i := i+1;
end loop;
```

$\{ z = \mathcal{N} j \ (1 \leq j \leq n \ \wedge \ A(j) = x \ ) \}$ 3, 19 eta **(KPE)**

Balidazioa:

- Borne adierazpena: $E \equiv n - i$
- $(z = \mathcal{N} j \ (1 \leq j < i \ \wedge \ A(j) = x \ ) \ \wedge \ i \leq n \ ) \ \rightarrow \ (\ i \leq n \ ) \ \rightarrow \ (\ 0 \leq n - i \ ) \ \rightarrow \ E \in \mathbb{N}$
-
  1. $(z = \mathcal{N} j \ (1 \leq j < i \ \wedge \ A(j) = x \ ) \ \wedge \ i \leq n \ \wedge n - i = k \ ) \ \rightarrow \ (\ n - i = k \ )$

  2. $\{ n - i = k \}$
     ```
     if A(i) = x then
        z := z+1;
     end if;
     ```
     $\{ n - i = k \}$ **(BDE)**

  3. $\{ n - i = k \}$
     ```
     i := i+1;
     ```
     $\{ n - (i - 1) = k \}$ **(AA)**

  4. $\{ n - i = k \}$
     ```
     if A(i) = x then
        z := z+1;
     end if;
     i := i+1;
     ```
     $\{ n - (i - 1) = k \}$ 2, 3 eta **(KPE)**

  5. $(\ n - (i - 1) = k \ ) \ \rightarrow \ (\ n - i + 1 = k \ ) \ \rightarrow \ (\ n - i < k \ )$

  6. $\{ z = \mathcal{N} j \ (1 \leq j < i \ \wedge \ A(j) = x \ ) \ \wedge \ i \leq n \ \wedge n - i = k \}$
     ```
     if A(i) = x then
        z := z+1;
     end if;
     i := i+1;
     ```
     $\{ n - i < k \}$ 1, 4, 5 eta **(ODE)**