Introduction: Motivation

PDR Algorithm: Preliminaries

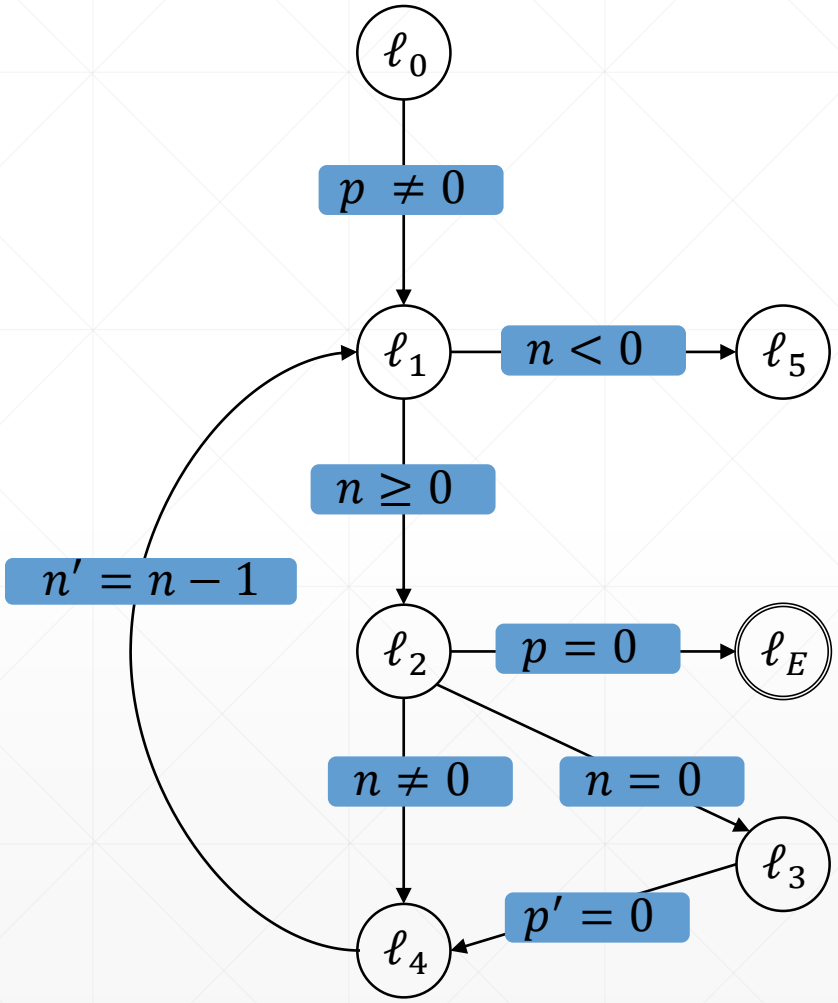
PDR Algorithm: Basic Notions

PDR Algorithm: Description

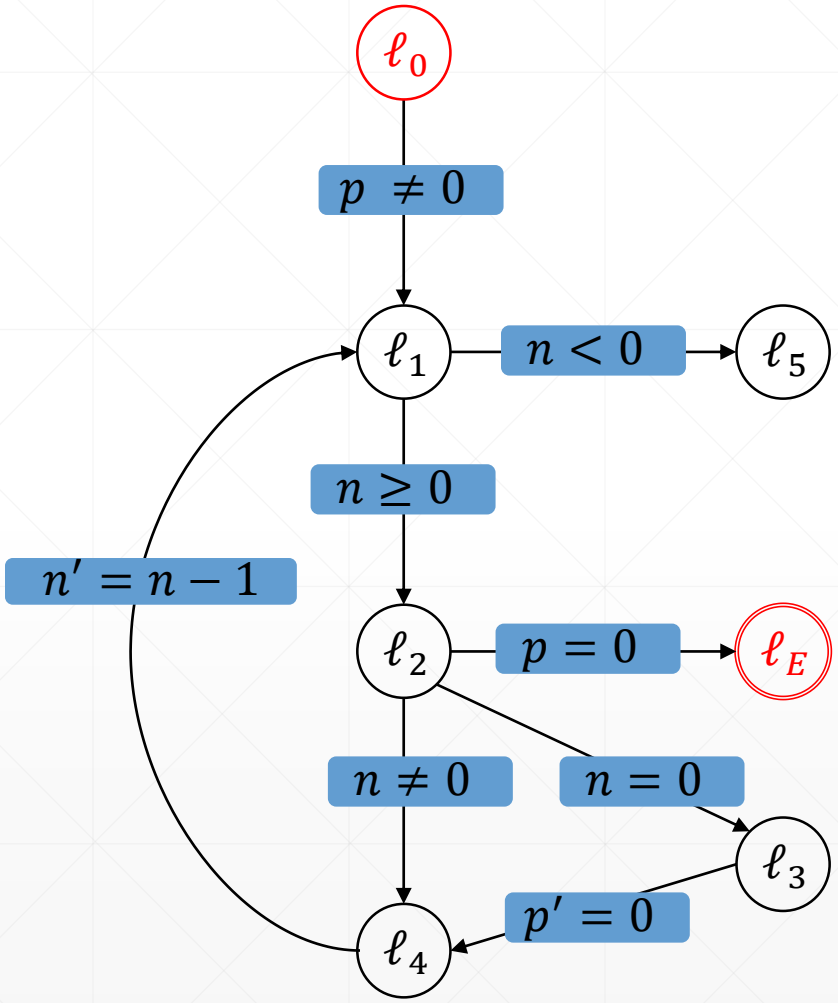
- Starts with checking for a 0-Counter-Example

- Repeats three phases until termination:
    1. Next Level Initialization Phase
    2. Blocking-Phase
    3. Propagation-Phase

Example: CFA


ℓ_0
$p \neq 0$
ℓ_1
$n < 0$
ℓ_5
$n \geq 0$
$n' = n - 1$
ℓ_2
$p = 0$
ℓ_E
$n \neq 0$
$n = 0$
ℓ_3
$p' = 0$
ℓ_4

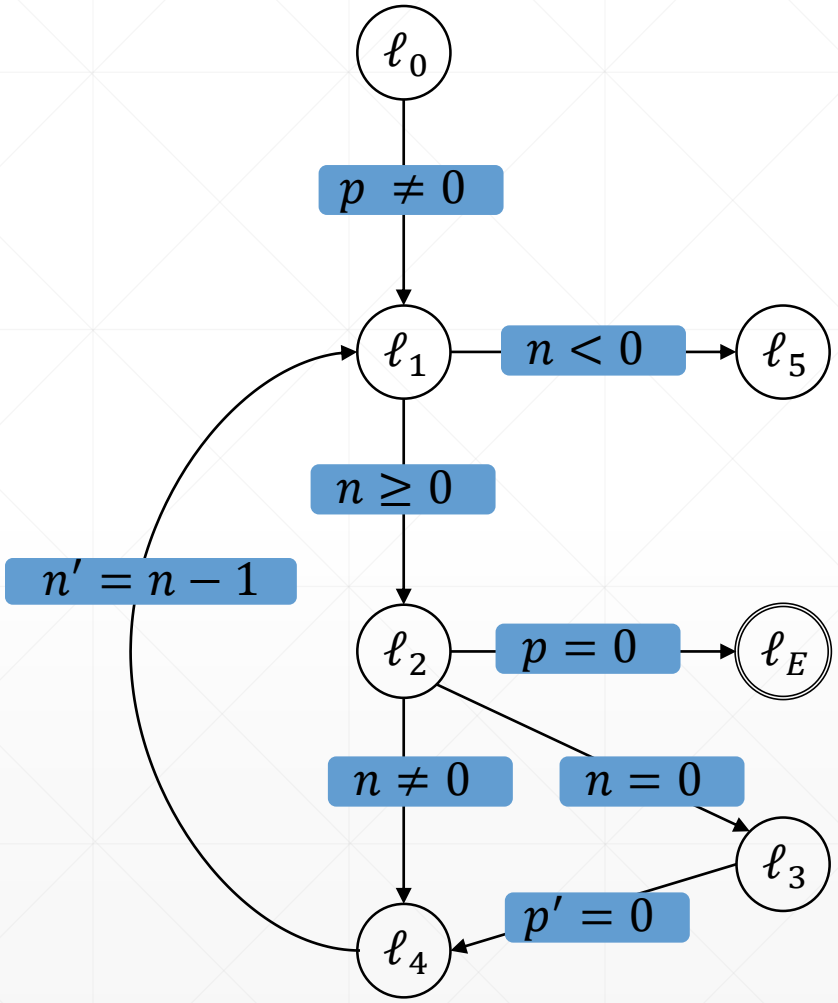
Example:



1. Step: Check for 0-Counter-Example

➢ Is $\ell_0 = \ell_E$?
➔ No, continue with initialization

Example:

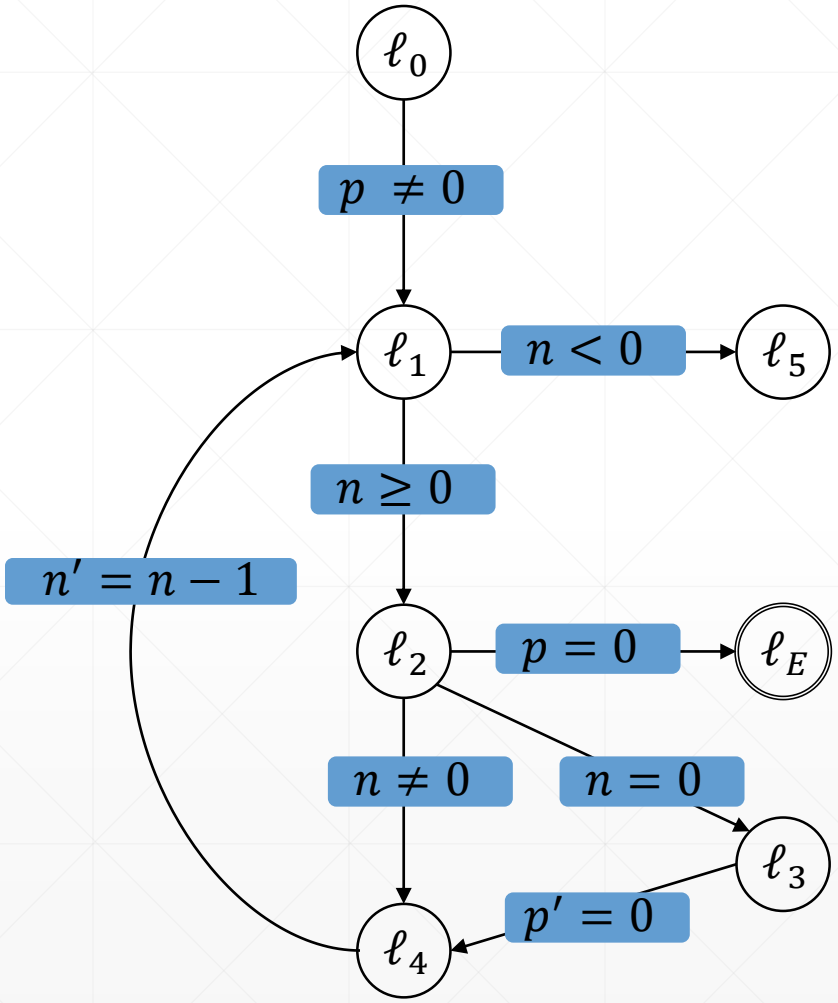


location	0
ℓ_0	
ℓ_1	
ℓ_2	
ℓ_3	
ℓ_4	

2. Step: Initialization of level 0

- $F_{0,\ell} = \begin{cases} \mathrm{T}, & \ell = \ell_0 \\ \mathrm{F}, & otherwise \end{cases}$

Example:

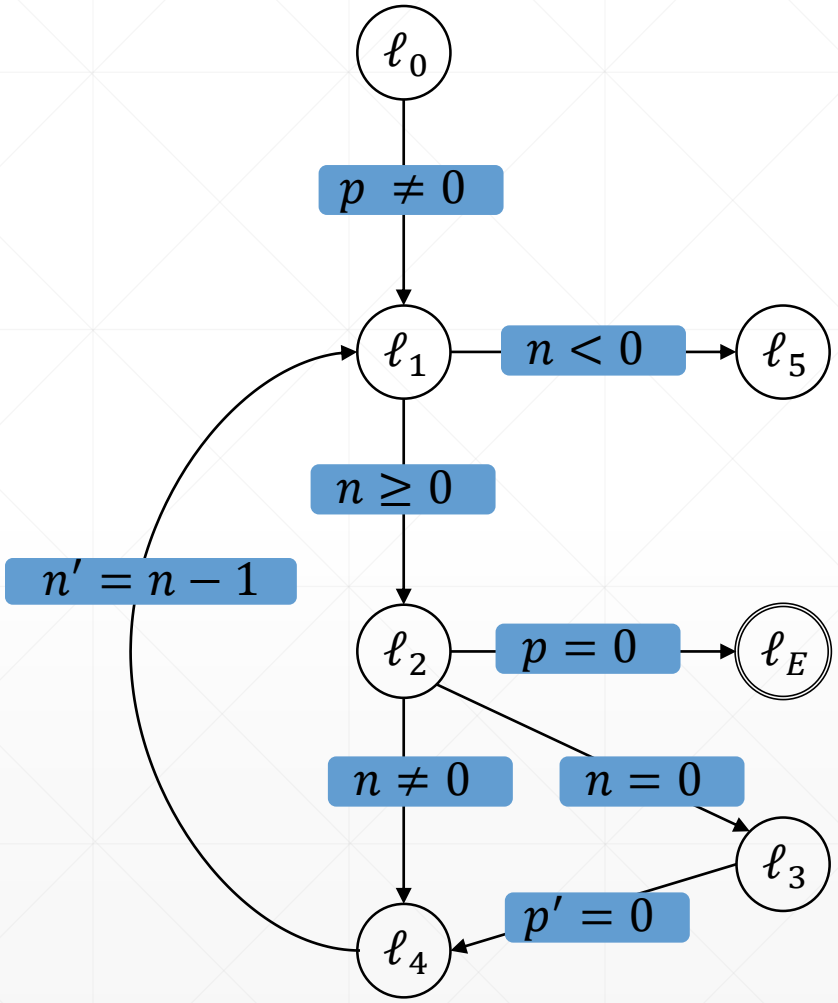


location	0
ℓ_0	t
ℓ_1	f
ℓ_2	f
ℓ_3	f
ℓ_4	f

2. Step: Initialization of level 0

- $F_{0,\ell} = \begin{cases} \mathrm{T}, & \ell = \ell_0 \\ \mathrm{F}, & otherwise \end{cases}$

Example:

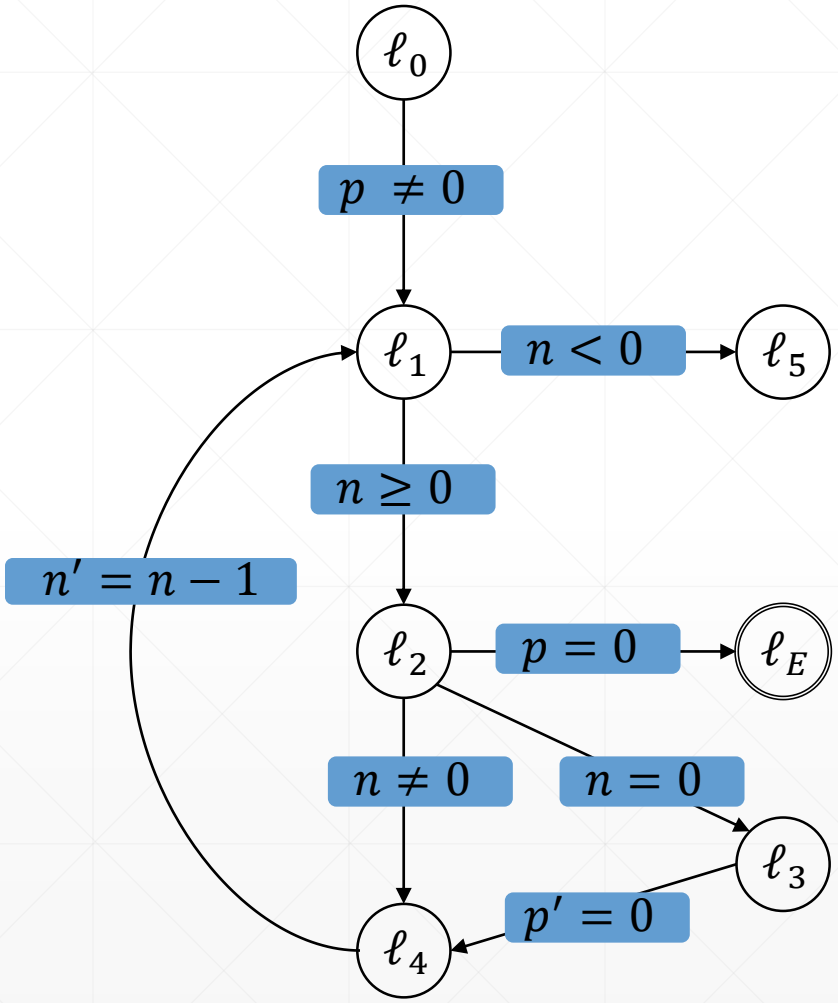


location	0	1
ℓ_0	t	
ℓ_1	f	
ℓ_2	f	
ℓ_3	f	
ℓ_4	f	

3. Step: Level 1

- Initialize level 1 frames as true

Example:

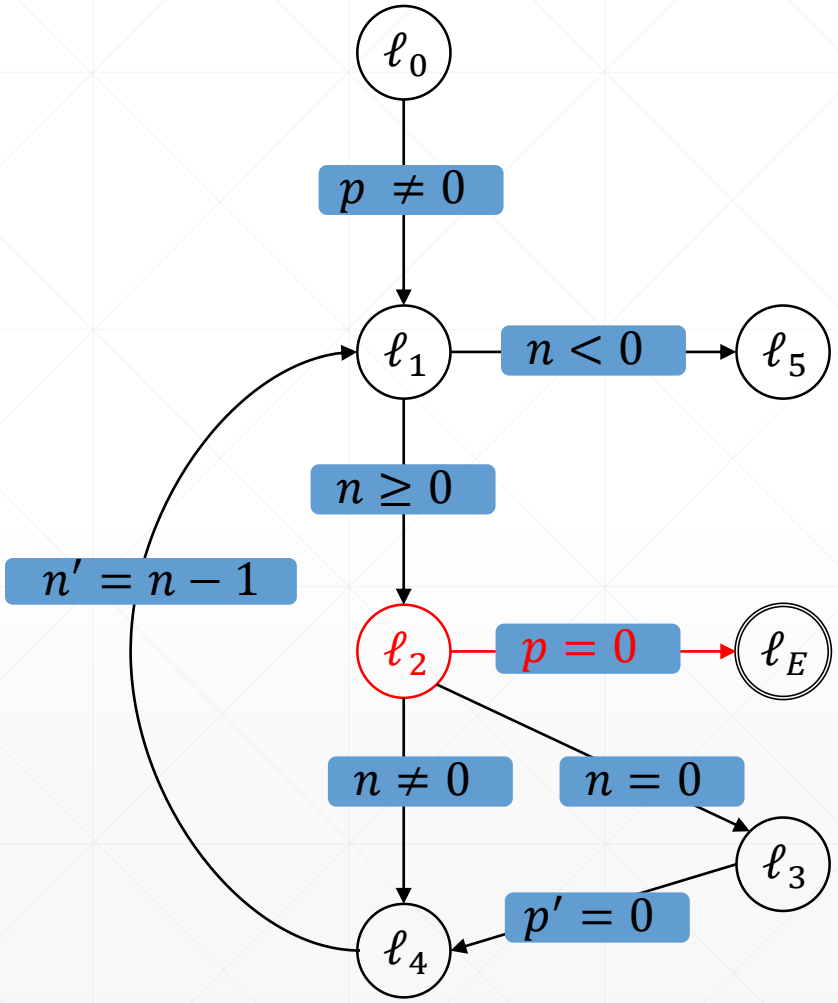


location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

3. Step: Level 1

- Initialize level 1 frames as true

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

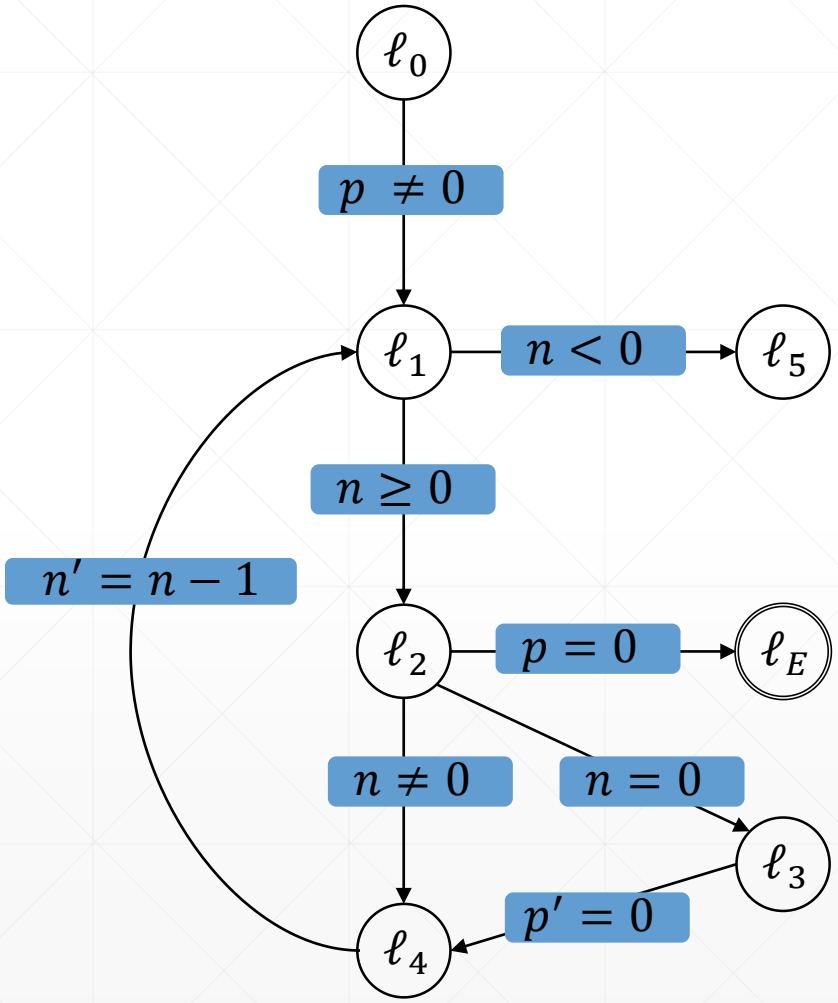
3. Step: Level 1

➢ Get initial proof-obligation

Proof-Obligations:

- $(p = 0, \ell_2, 1)$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

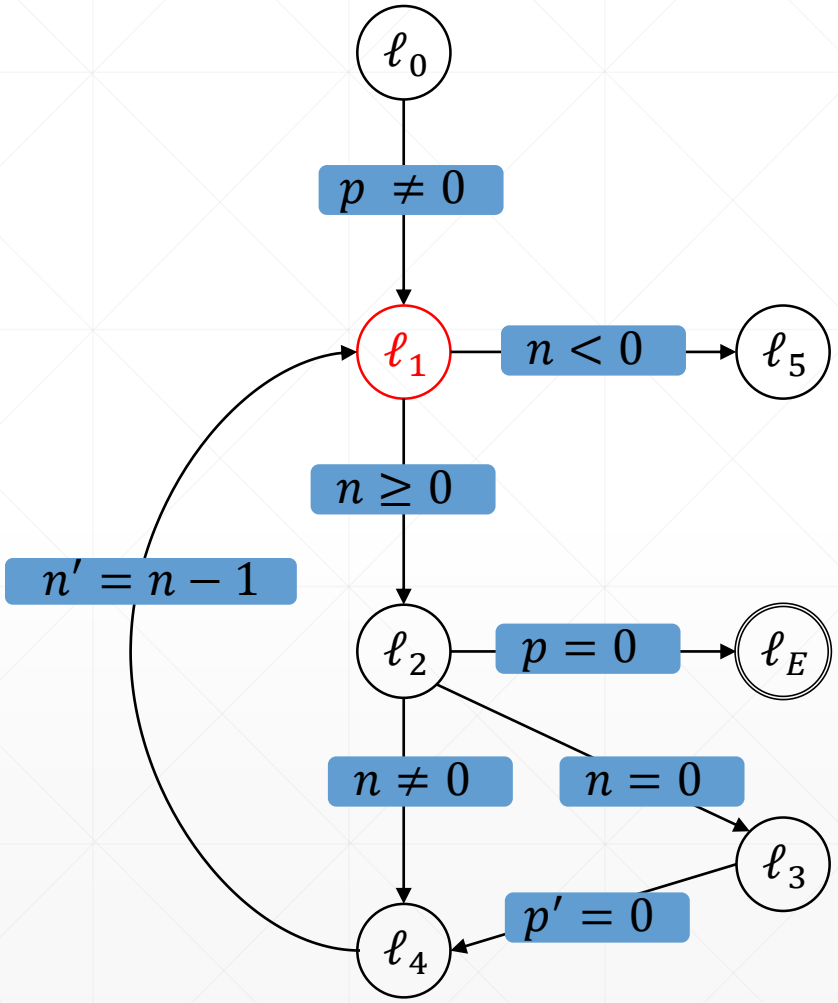
4. Step: Level 1 Blocking-Phase:

➢ Try to block $(p = 0, \ell_2, 1)$

Proof-Obligations:

- $(p = 0, \ell_2, 1)$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

4. Step: Level 1 Blocking-Phase:

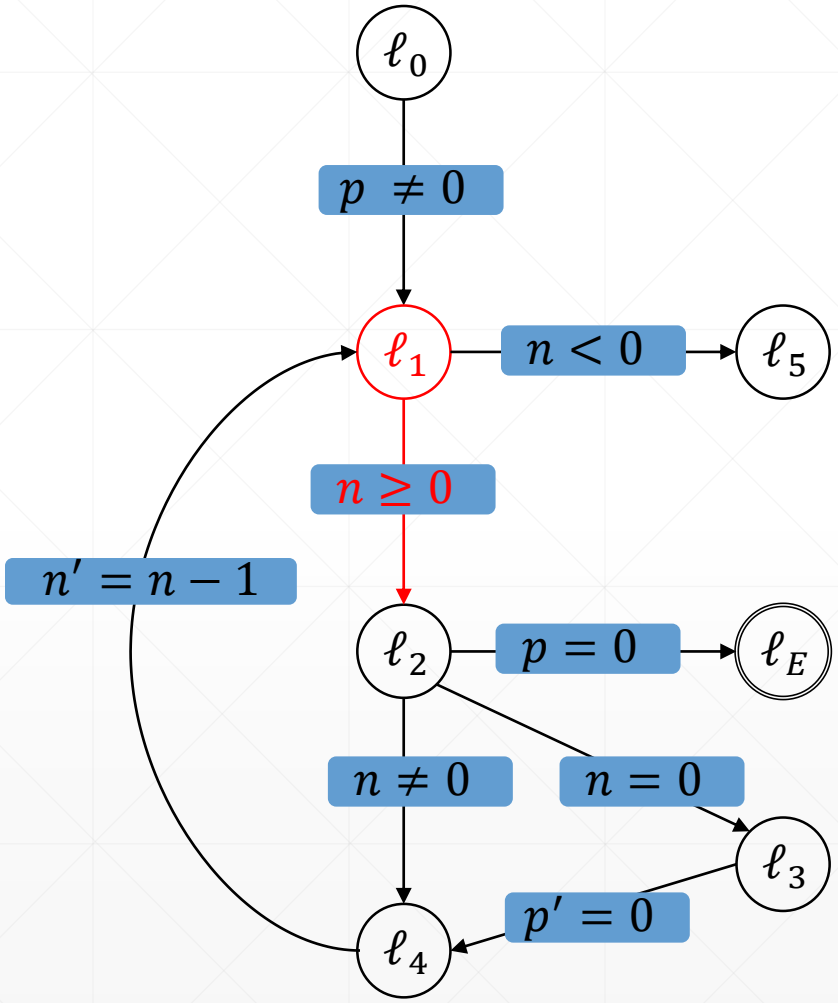
➢ Try to block $(p = 0, \ell_2, 1)$

- Predecessor ℓ_1:
  - $F_{0,\ell_1} \wedge T_{\ell_1 \to \ell_2} \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 1)$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

4. Step: Level 1 Blocking-Phase:

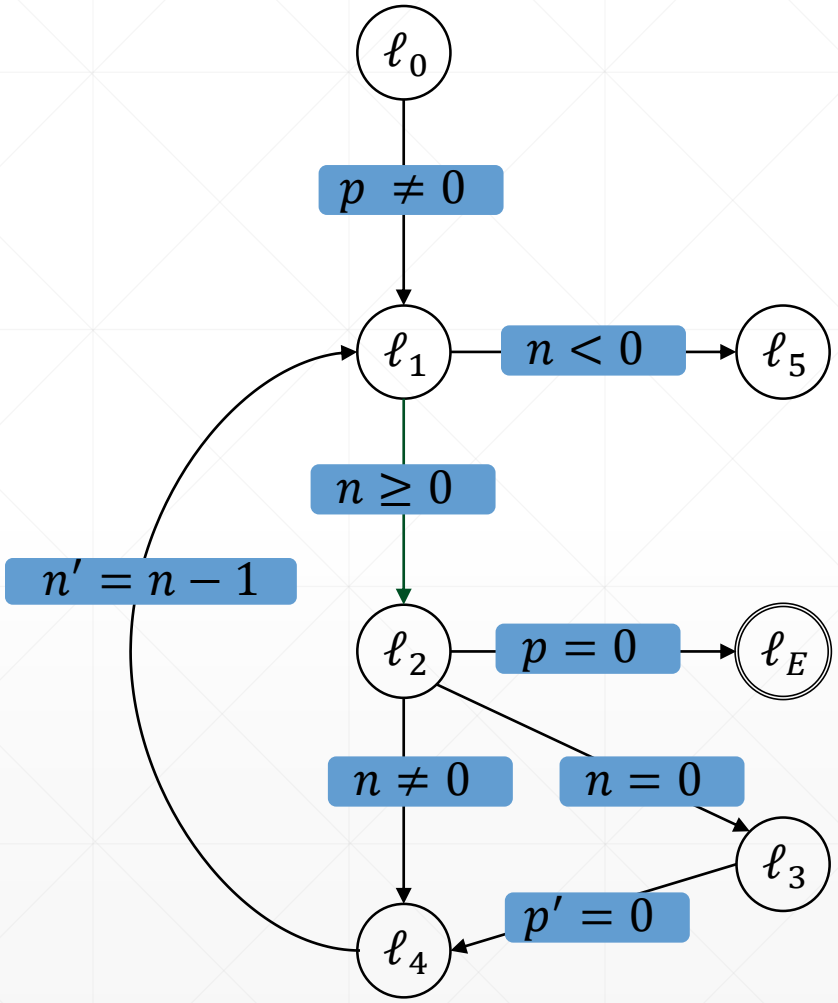
➢ Try to block $(p = 0, \ell_2, 1)$

- Predecessor ℓ_1:
  - $f \wedge n \geq 0 \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 1)$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	f	t
ℓ_3	f	t
ℓ_4	f	t

4. Step: Level 1 Blocking-Phase:

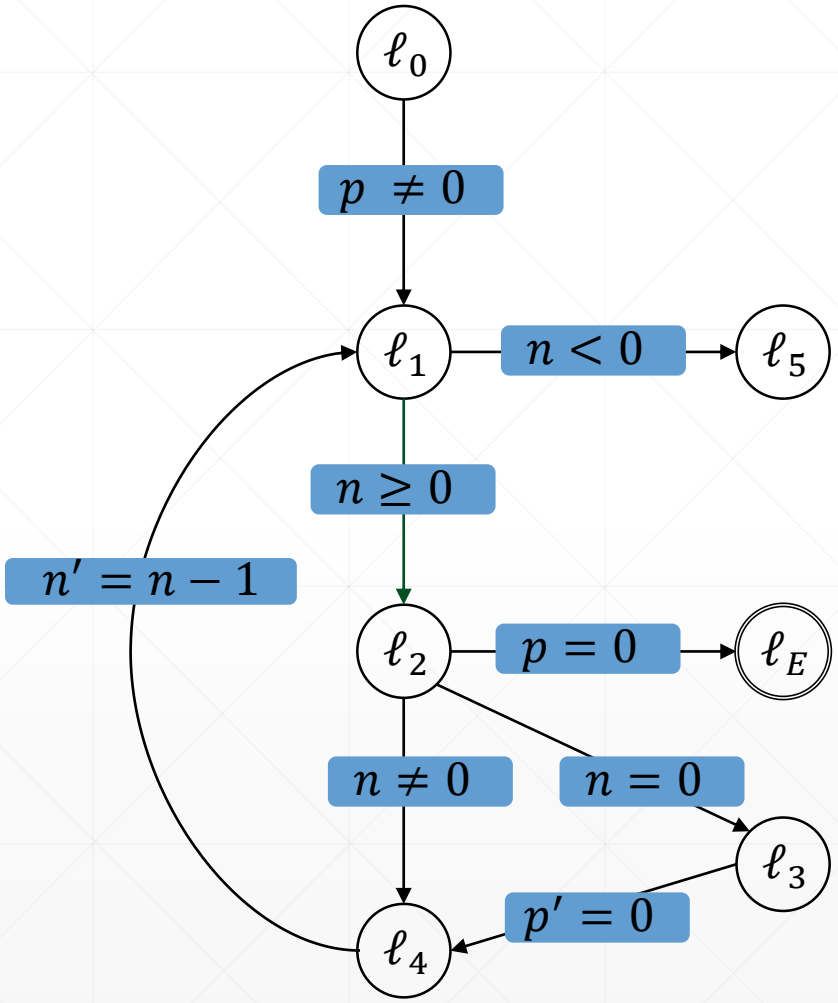
➢ Try to block $(p = 0, \ell_2, 1)$

- Predecessor ℓ_1:
  - $f \wedge n \geq 0 \wedge p' = 0$
  - ➔ Unsatisfiable
  - ➔ Strengthen frames $F_{0,\ell_2}, F_{1,\ell_2}$

Proof-Obligations:

- ∅

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t
ℓ_4	f	t

4. Step: Level 1 Blocking-Phase:

➢ Try to block $(p = 0, \ell_2, 1)$

- Predecessor ℓ_1:
  - $f \wedge n \geq 0 \wedge p' = 0$

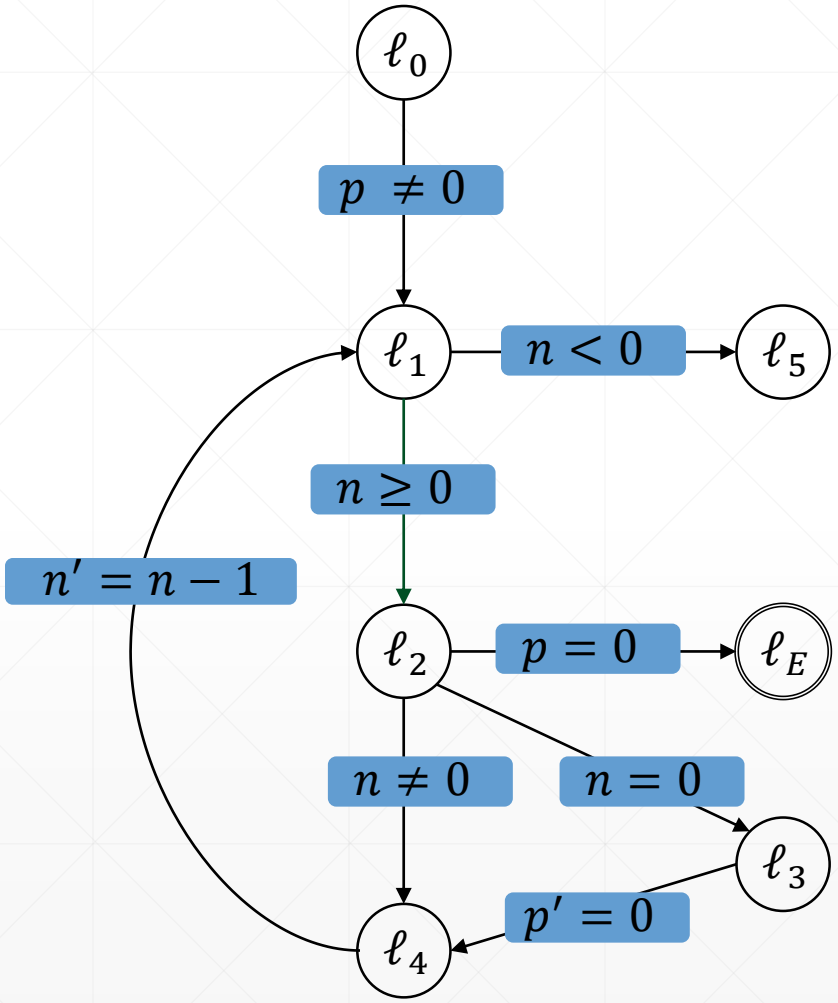
➔ Unsatisfiable

➔ Strengthen frames $F_{0,\ell_2}, F_{1,\ell_2}$

Proof-Obligations:

- $\emptyset$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t
ℓ_4	f	t

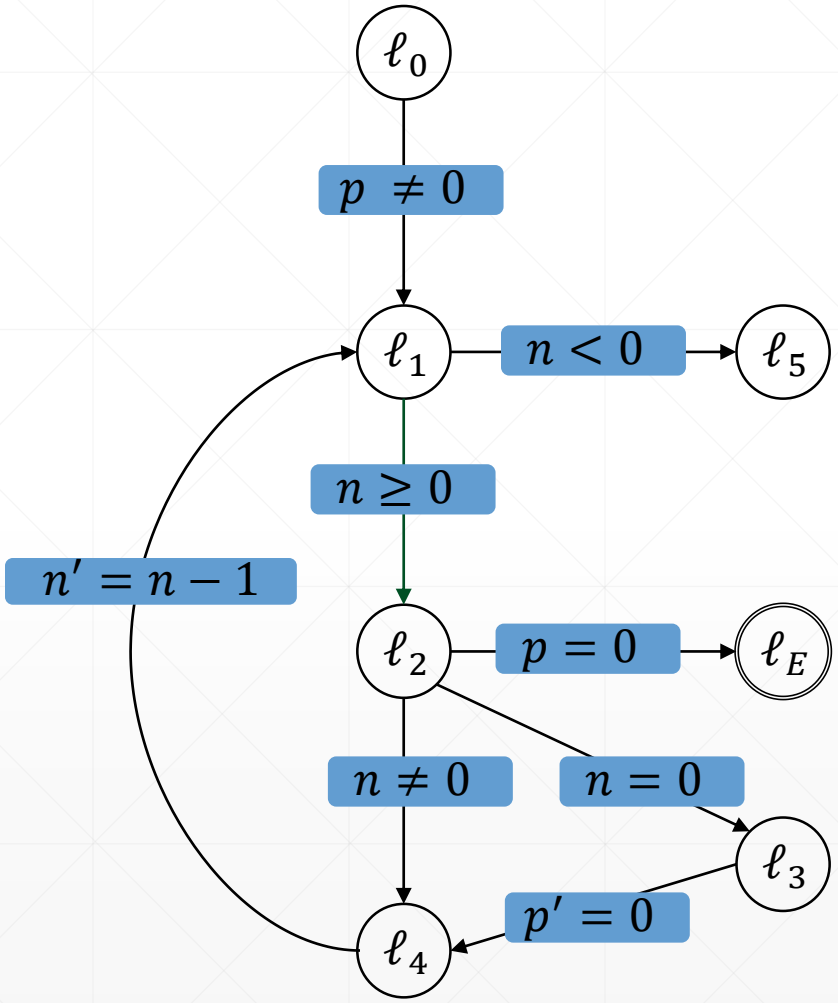
5. Step: Level 1 Propagation-Phase

➢ Is there a global fixpoint?

Proof-Obligations:

- ∅

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t
ℓ_4	f	t

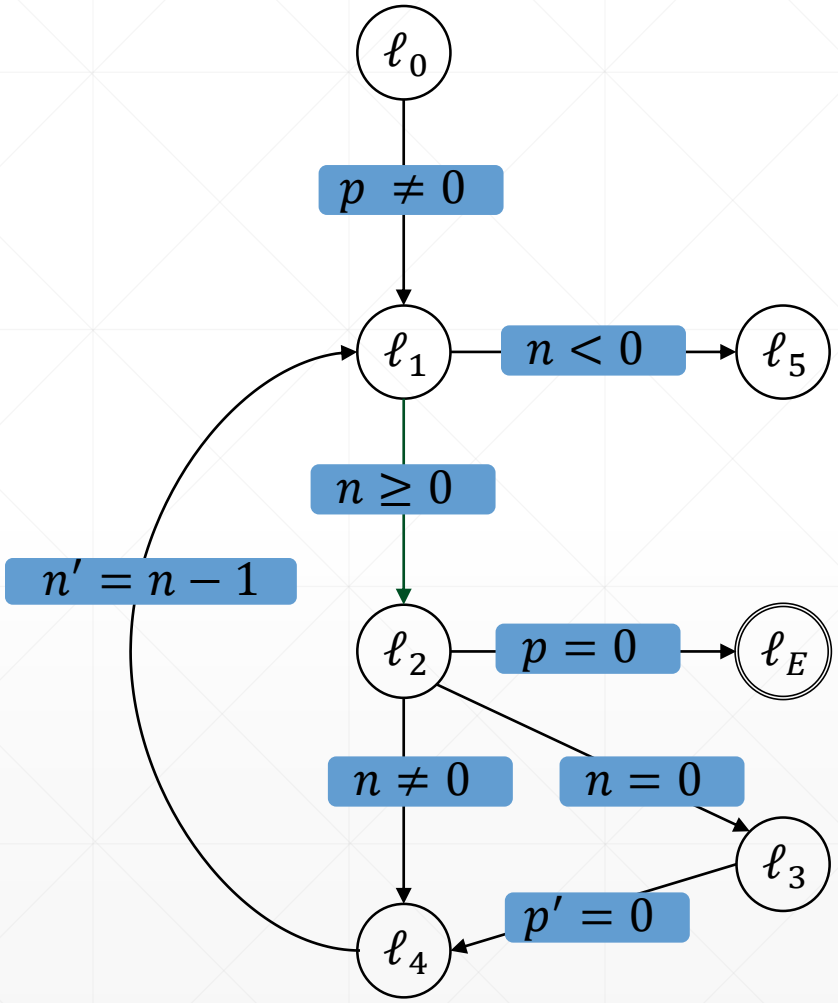
5. Step: Level 1 Propagation-Phase

➢ Is there an i where $F_{i-1,\ell} = F_{i,\ell}$ for $\ell \in L \setminus \{\ell_E\}$?

Proof-Obligations:

- $\emptyset$

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t
ℓ_4	f	t

5. Step: Level 1 Propagation-Phase

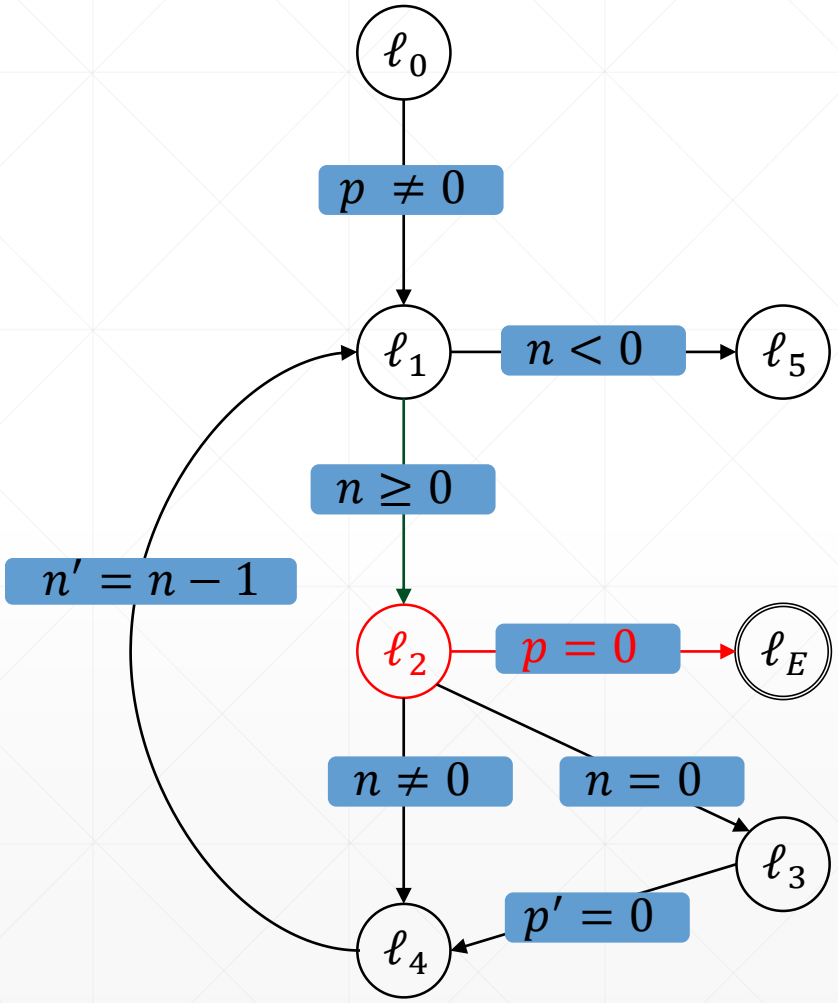
➢ Is there an i where $F_{i-1,\ell} = F_{i,\ell}$ for $\ell \in L \setminus \{\ell_E\}$?

➔ No. Continue with next level.

Proof-Obligations:

- ∅

Example:



location	0	1
ℓ_0	t	t
ℓ_1	f	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t
ℓ_4	f	t

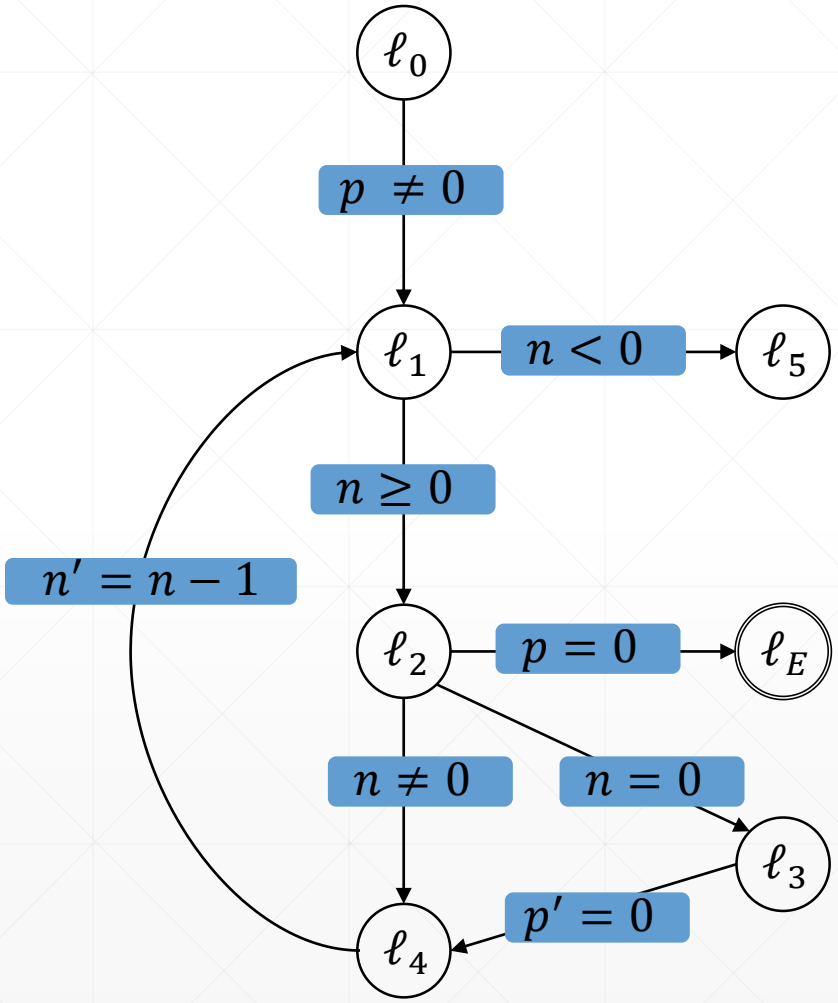
6. Step: Level 2

- Initzialize new frames
- Add initial proof-obligation $(p = 0, \ell_2, 2)$

Proof-Obligations:

- $\emptyset$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	f	t	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

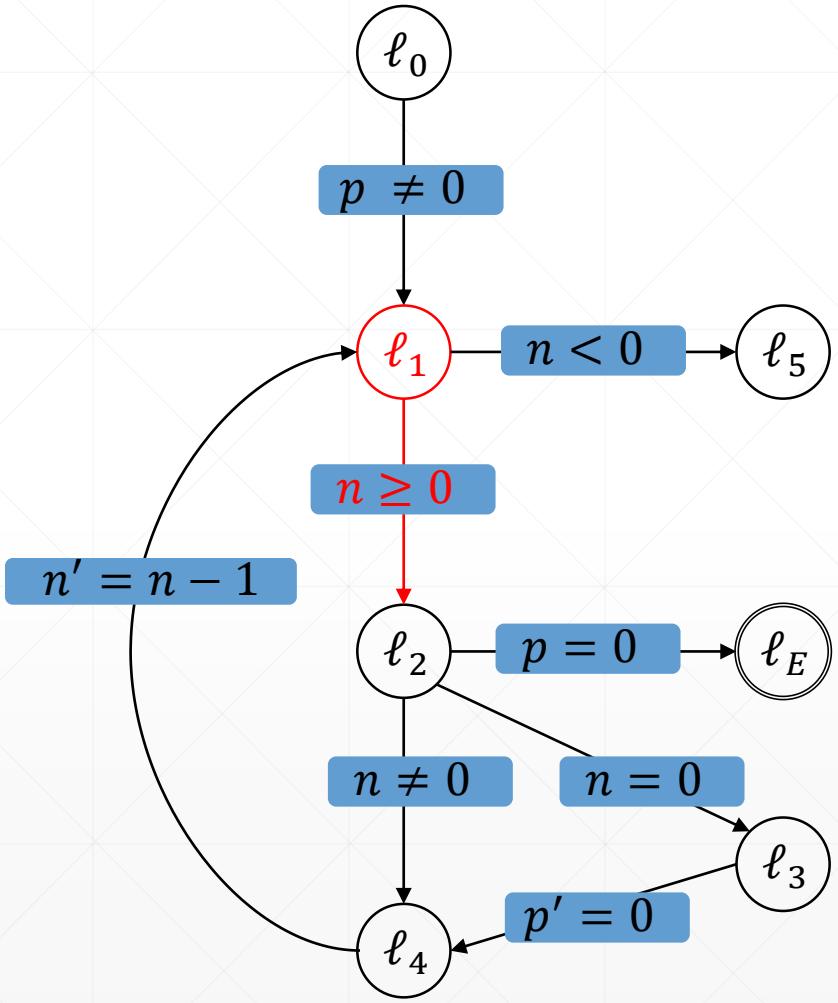
6. Step: Level 2

- Initzialize new frames
- Add initial proof-obligation $(p = 0, \ell_2, 2)$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	f	t	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

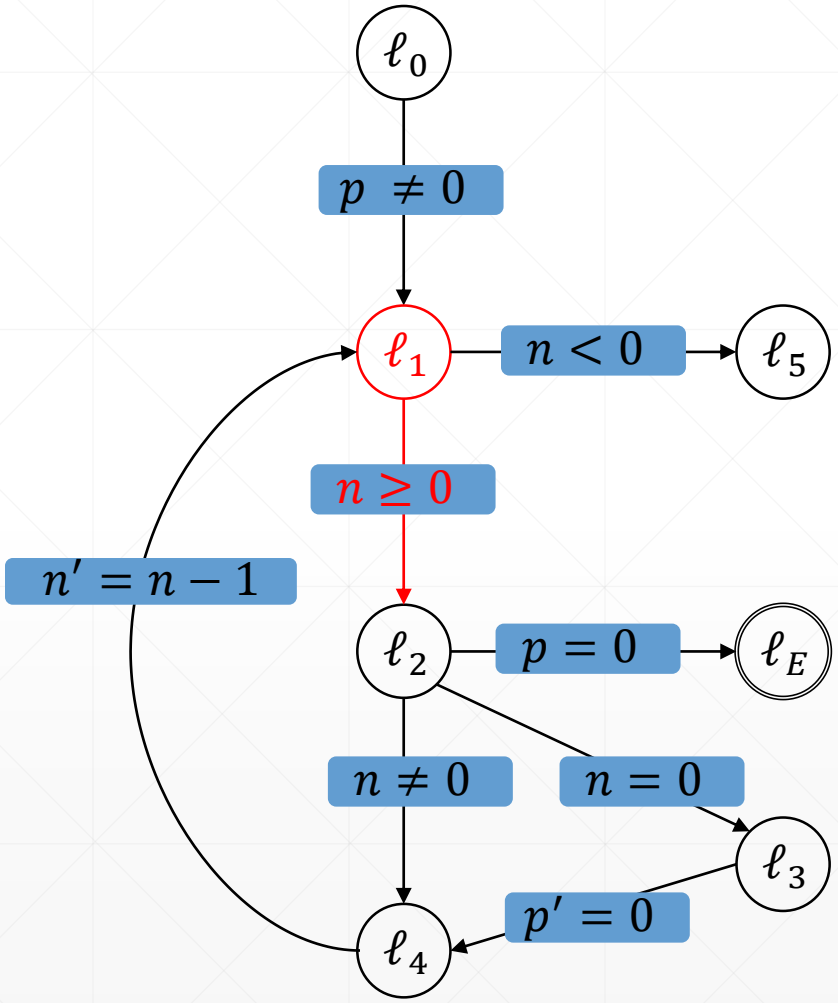
➢ Try to block $(p = 0, \ell_2, 2)$

- Predecessor ℓ_1:
  - $t \wedge n \geq 0 \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	f	t	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

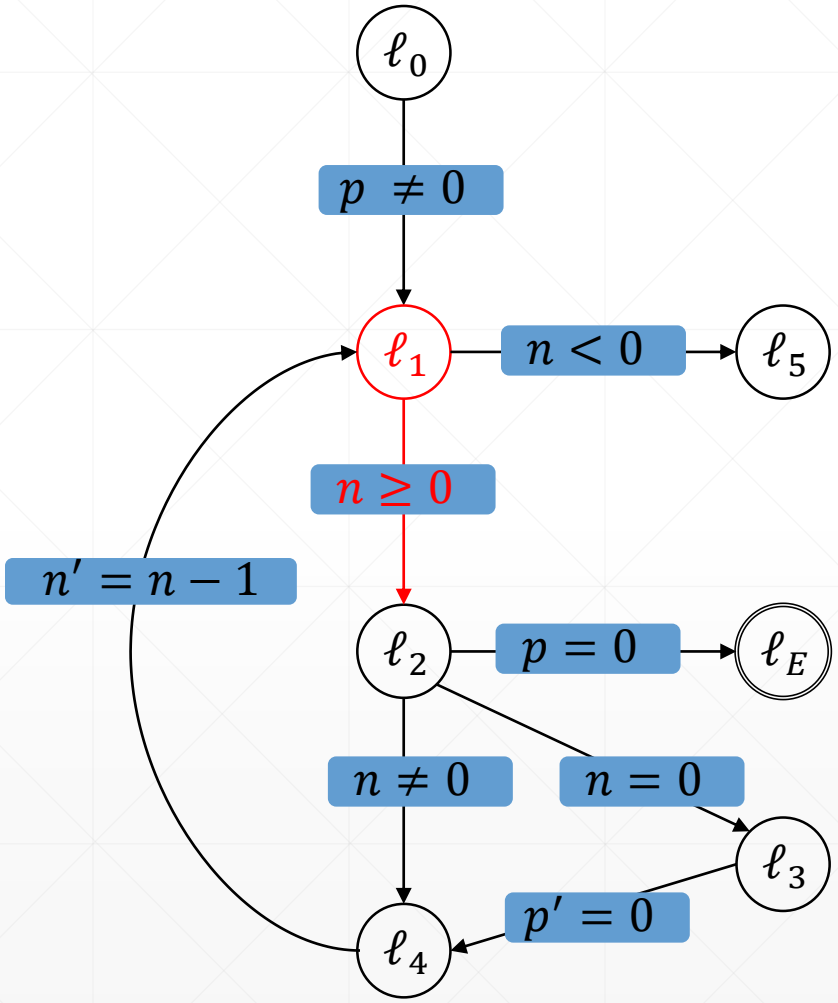
➢ Try to block $(p = 0, \ell_2, 2)$

- Predecessor ℓ_1:
  - $t \wedge n \geq 0 \wedge p' = 0$
    - ➔ Satisfiable!
    - ➔ $wp(n \geq 0, p' = 0) = (p = 0)$
  - ➔ New proof-obligation $(p = 0, \ell_1, 1)$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	f	t	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

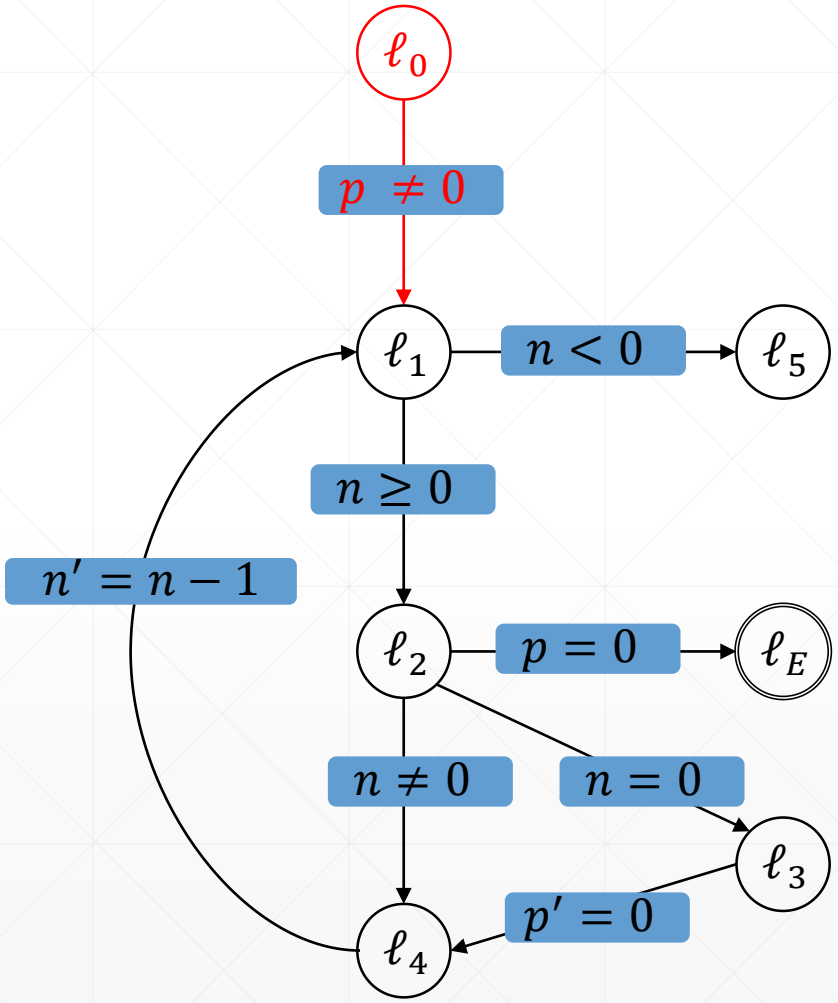
➢ Try to block $(p = 0, \ell_2, 2)$

- Predecessor ℓ_1:
  - $t \wedge n \geq 0 \wedge p' = 0$
    - ➔ Satisfiable!
    - ➔ $wp(n \geq 0, p' = 0) = (p = 0)$
  - ➔ New proof-obligation $(p = 0, \ell_1, 1)$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$
- $(p = 0, \ell_1, 1)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	f	t	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

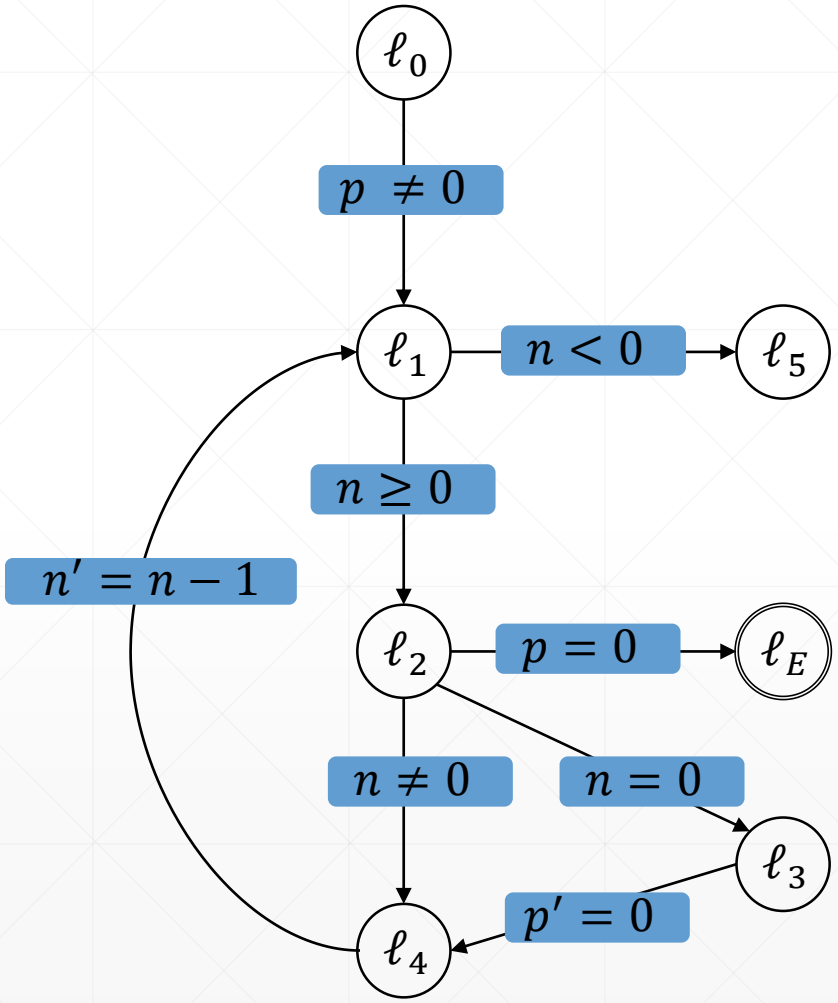
7. Step: Level 2 Blocking-Phase:

- Try to block $(p = 0, \ell_1, 1)$
- Predecessor ℓ_0:
  - $t \wedge p \neq 0 \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$
- $(p = 0, \ell_1, 1)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

- Try to block $(p = 0, \ell_1, 1)$
- Predecessor ℓ_0:
  - $t \wedge p \neq 0 \wedge p' = 0$

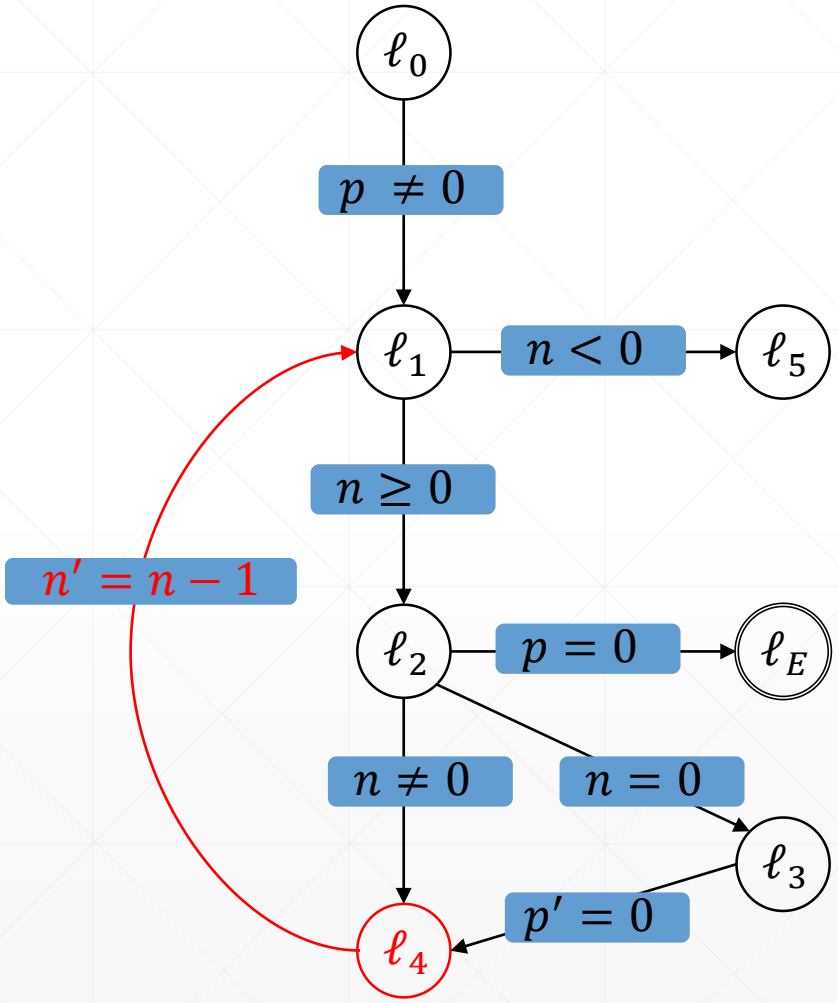
  ➔ Unsatisfiable!

  ➔ Strengthen frames $F_{0,\ell_1}, F_{1,\ell_1}$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$
- $(p = 0, \ell_1, 1)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

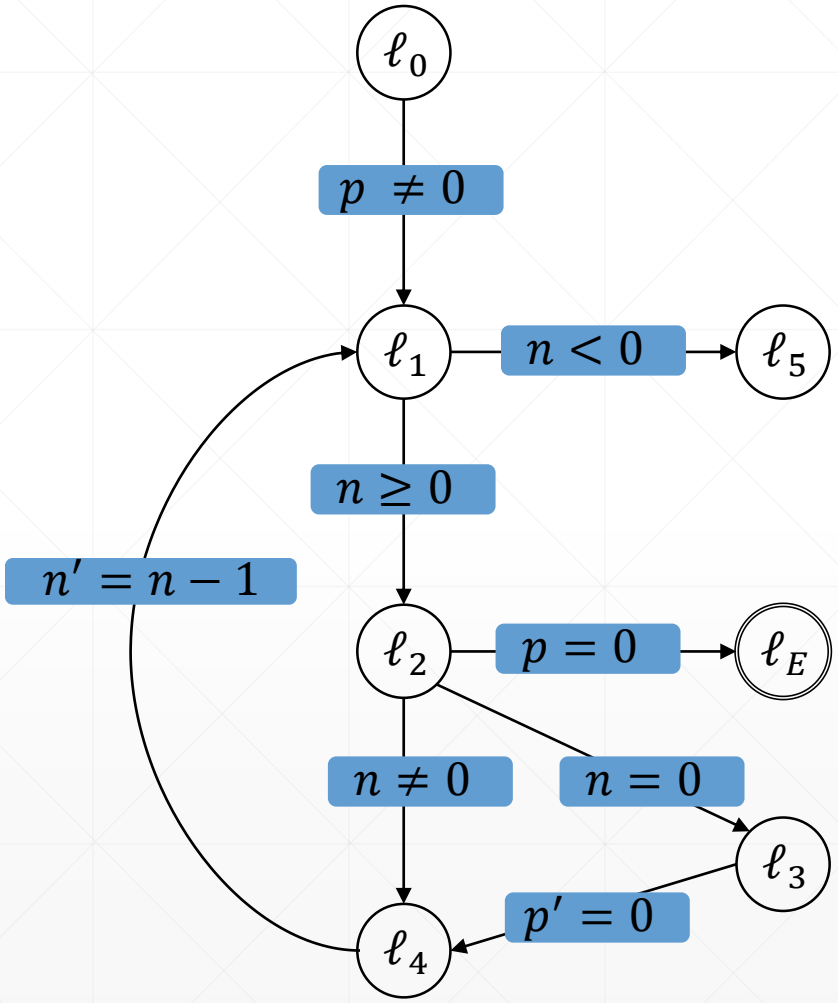
7. Step: Level 2 Blocking-Phase:

- Try to block $(p = 0, \ell_1, 1)$
- Predecessor ℓ_4:
  - $f \wedge n' = n - 1 \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$
- $(p = 0, \ell_1, 1)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

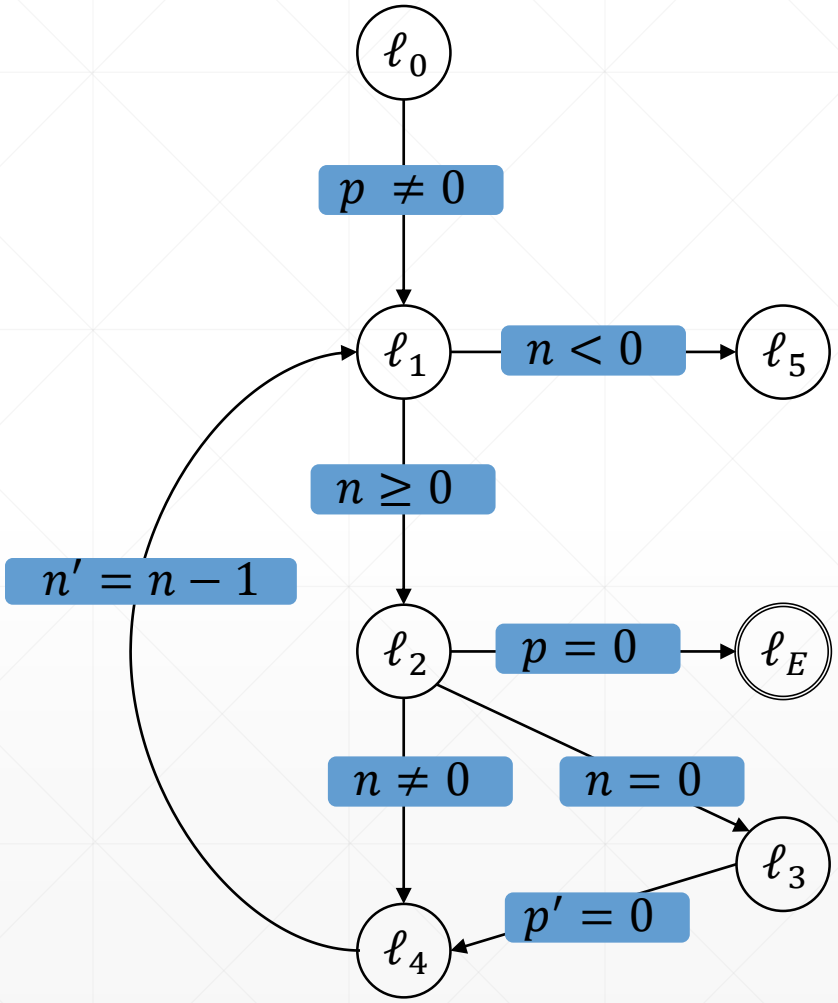
- Try to block $(p = 0, \ell_1, 1)$
- Predecessor ℓ_4:
  - $f \wedge n' = n - 1 \wedge p' = 0$

  ➔ Unsatisfiable!

Proof-Obligations:

- $(p = 0, \ell_2, 2)$
- $(p = 0, \ell_1, 1)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

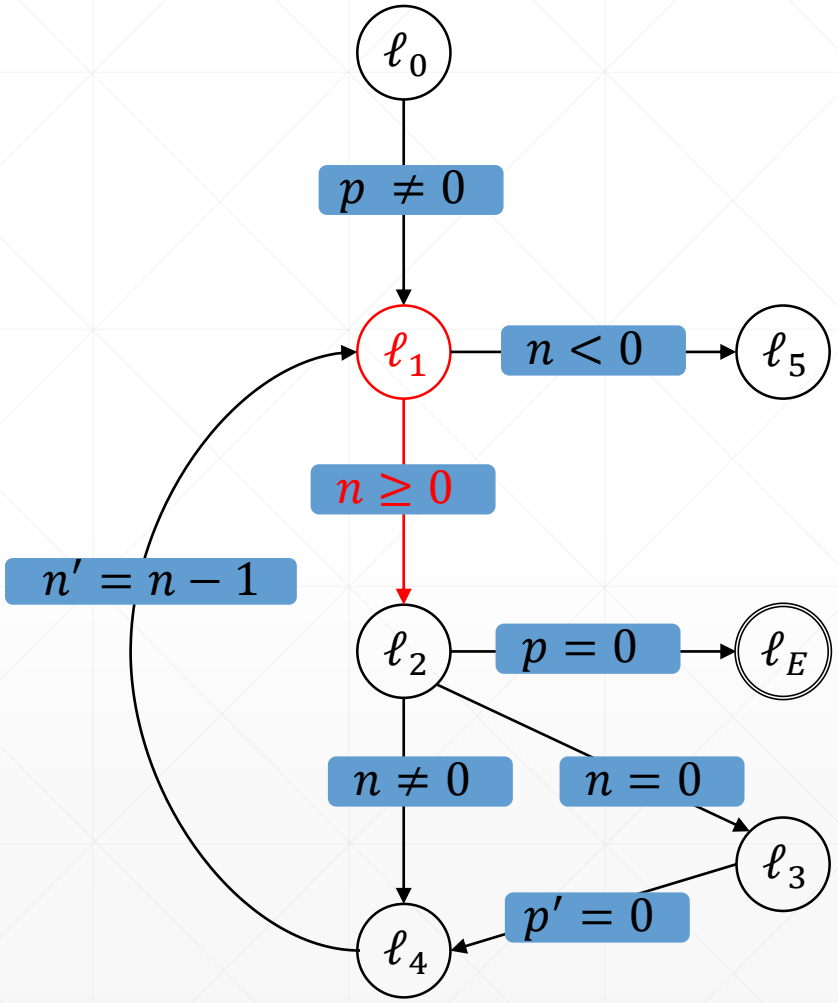
- Try to block $(p = 0, \ell_1, 1)$
- Predecessor ℓ_4:
  - $f \wedge n' = n - 1 \wedge p' = 0$

  ➔ Unsatisfiable!

Proof-Obligations:

- $(p = 0, \ell_2, 2)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_3	f	t	t
ℓ_4	f	t	t

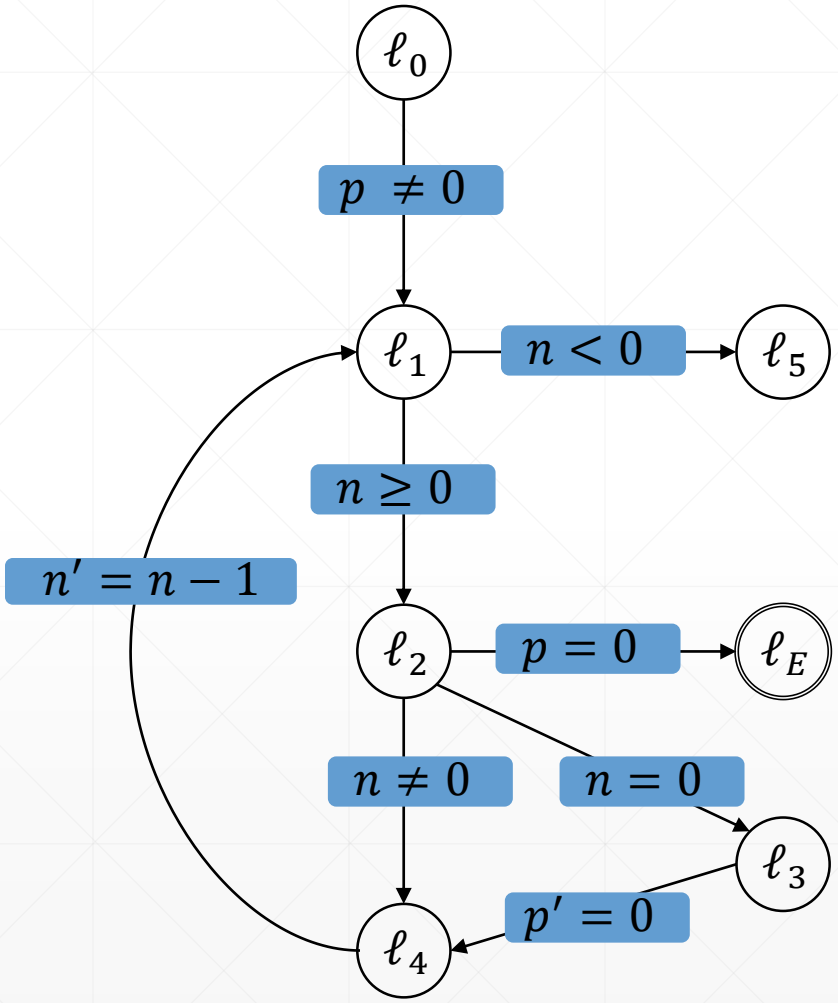
7. Step: Level 2 Blocking-Phase:

- Try to block $(p = 0, \ell_2, 2)$ again
- Predecessor ℓ_1:
  - $t \wedge p \neq 0 \wedge n \geq 0 \wedge p' = 0$

Proof-Obligations:

- $(p = 0, \ell_2, 2)$

Example:



location	0	1	2
ℓ_0	t	t	t
ℓ_1	$f \wedge p \neq 0$	$t \wedge p \neq 0$	t
ℓ_2	$f \wedge p \neq 0$	$t \wedge p \neq 0$	$t \wedge p \neq 0$
ℓ_3	f	t	t
ℓ_4	f	t	t

7. Step: Level 2 Blocking-Phase:

- Try to block $(p = 0, \ell_2, 2)$ again
- Predecessor ℓ_1:
  - $t \wedge p \neq 0 \wedge n \geq 0 \wedge p' = 0$

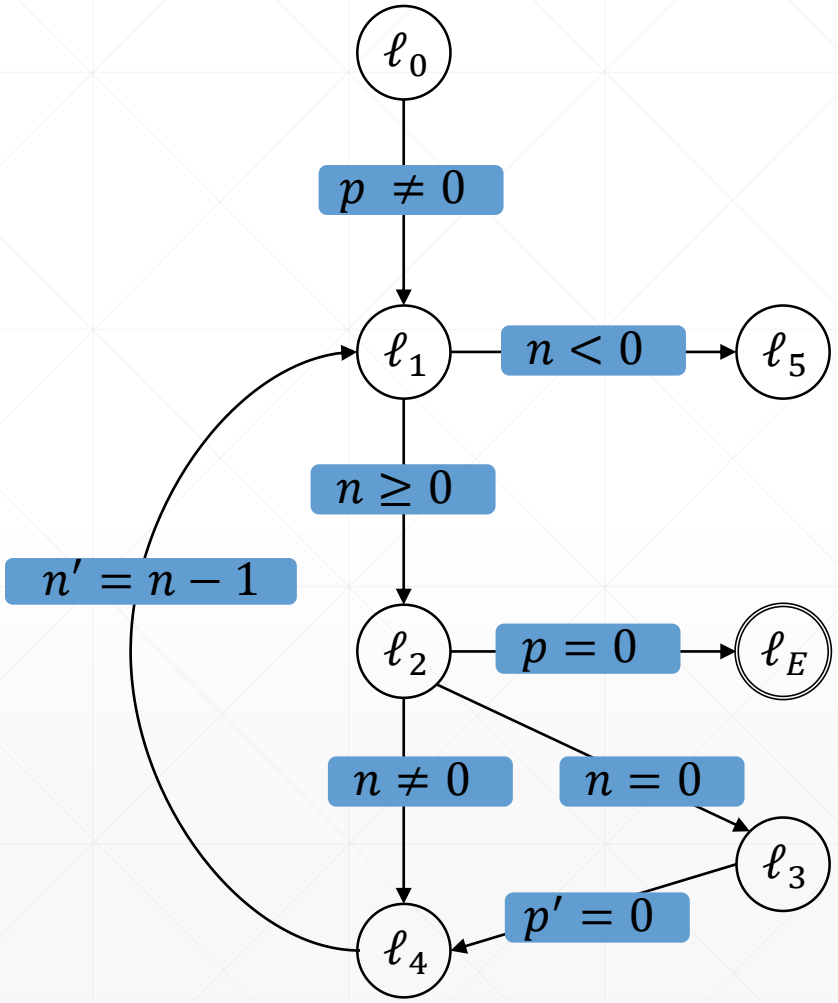
  ➔ Unsatisfiable!

  ➔ Strengthen frames F_{2,ℓ_2}

Proof-Obligations:

- Ø

Example:



location	0	1	2	3	4	5
ℓ_0						
ℓ_1						
ℓ_2						
ℓ_3						
ℓ_4						

Text

Proof-Obligations:

6. Related Work

Implementation in Ultimate: Traceabstraction with PDR

Implemented Improvements

Evaluation: Data Comparison

Evaluation: Discussion

Future Work: Implementing Further Improvements

Conclusion