# JOIN OVER PATHS

- Recall: Given a program as a LTS $\Gamma_c \equiv (V, L, l_0, l_e, T)$, the assertion map $\mu : L \to \mathbb{P}(State)$ associates a set of states with every location.
    - $\mu(l)$ is the set of states reachable at $l$ during any execution.
    - $\mu$ is also called the Concrete Join Over Paths (JOP) or the collecting semantics.
- Instead of operating over concrete states, we can also consider JOP over abstract states.

# ABSTRACT TRANSFER FUNCTION

- Given a Galois Connection $(\mathbb{P}(State), \subseteq) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} (D, \leq)$, for every program command $p$, we can define the abstract transfer function $\hat{f}_p$ (previously called the abstract strongest post-condition operator)
  - $\hat{f}_p : D \rightarrow D$.
- We can define the concrete transfer function as follows: $f_p(\sigma) = \{\sigma' \,|\, (\sigma, p) \hookrightarrow (\sigma', skip)\}$.
  - $f_p(c) = \bigcup_{\sigma \in c} f_p(\sigma)$
- Then, the abstract transfer function must be a consistent abstraction of the concrete transfer function:
  - $\forall d \in D \,.\, f_p(\gamma(d)) \subseteq \gamma(\hat{f}_p(d))$
  - Equivalently, $\forall c \in \mathbb{P}(State) \,.\, \hat{f}_p(\alpha(c)) \leq \alpha(f(c))$

# ABSTRACT TRANSFER FUNCTION

## EXAMPLE

- Consider the sign abstract domain, and the program command $p$ : x := x+1.
  - $\hat{f}_p(+) = ???$

# ABSTRACT TRANSFER FUNCTION

## EXAMPLE

- Consider the sign abstract domain, and the program command $p$ : x := x+1.
  - $\hat{f}_p(+) = +$

# ABSTRACT TRANSFER FUNCTION

## EXAMPLE

- Consider the sign abstract domain, and the program command $p$ : x := x+1.
  - $\hat{f}_p(+) = +$
  - $\hat{f}_p(-) = ???$

# ABSTRACT TRANSFER FUNCTION

## EXAMPLE

- Consider the sign abstract domain, and the program command $p$ : x := x+1.
  - $\hat{f}_p( + ) = +$
  - $\hat{f}_p( - ) = + -$

# ABSTRACT TRANSFER FUNCTION

## EXAMPLE

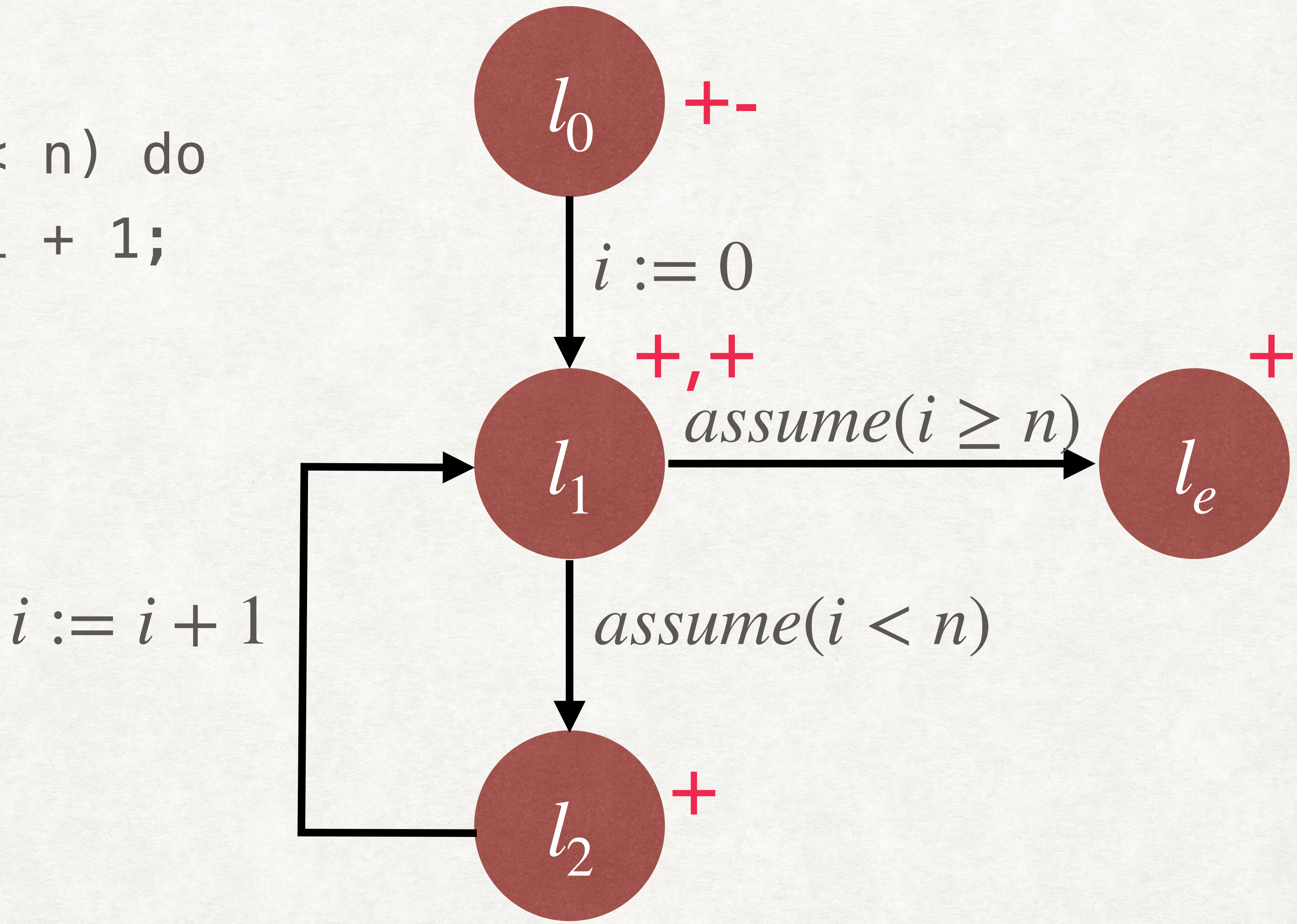
- Consider the sign abstract domain, and the program command $p$ : x := x+1.
    - $\hat{f}_p( + ) = +$
    - $\hat{f}_p( - ) = + -$
    - $\hat{f}_p( + - ) = + -$
    - $\hat{f}_p( \bot ) = \bot$
- See whether the condition $\forall d \in D \,.\, f_p(\gamma(d)) \subseteq \gamma(\hat{f}_p(d))$ is satisfied.

# ABSTRACT JOP

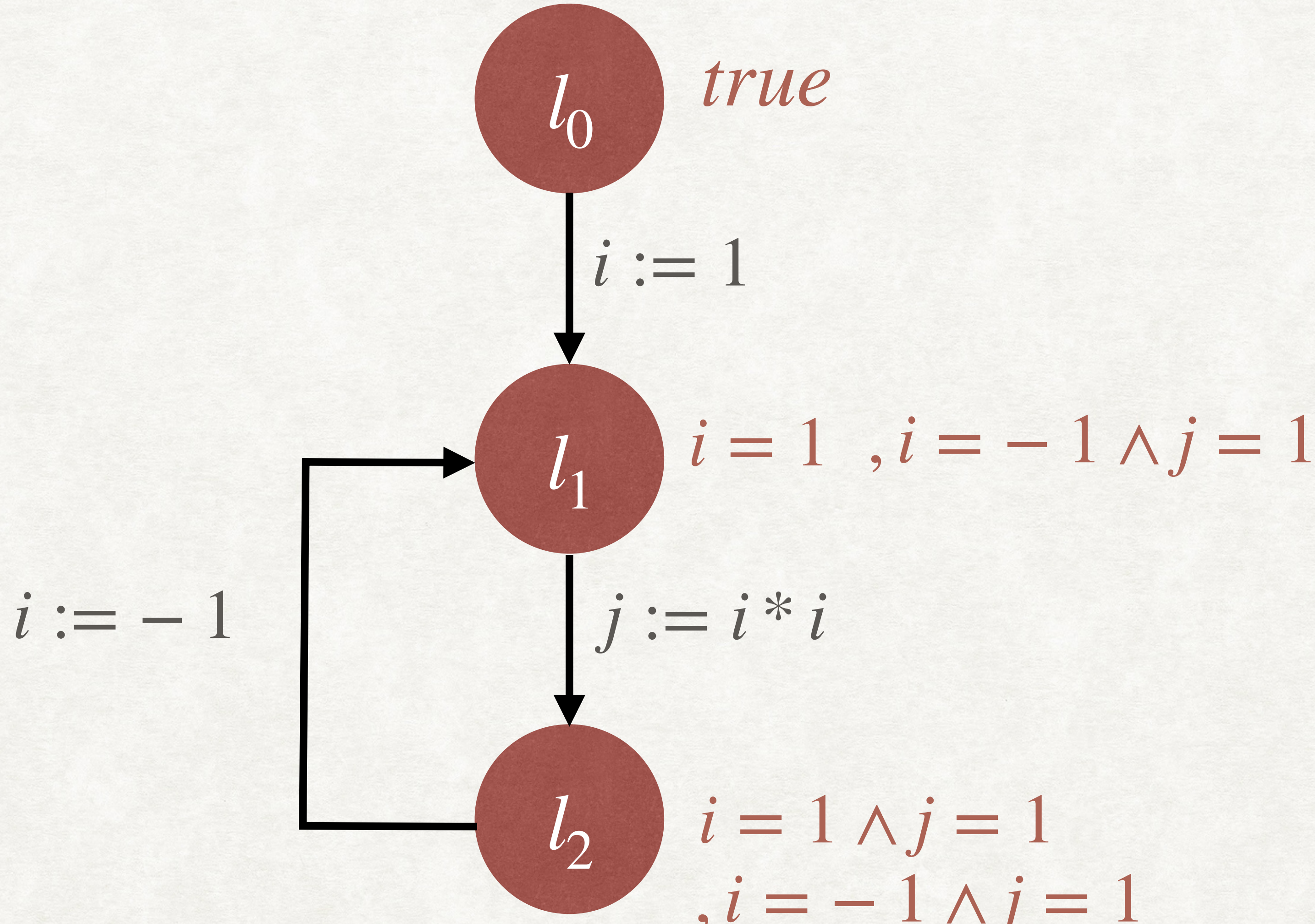
- Instead of executing the program with concrete states, we execute the program with abstract state, and the abstract transfer function for each program command.
- Collect all the abstract states at each location, for every possible execution
    - Their join is the abstract JOP map, $\hat{\mu} : L \to D$.

# EXAMPLE

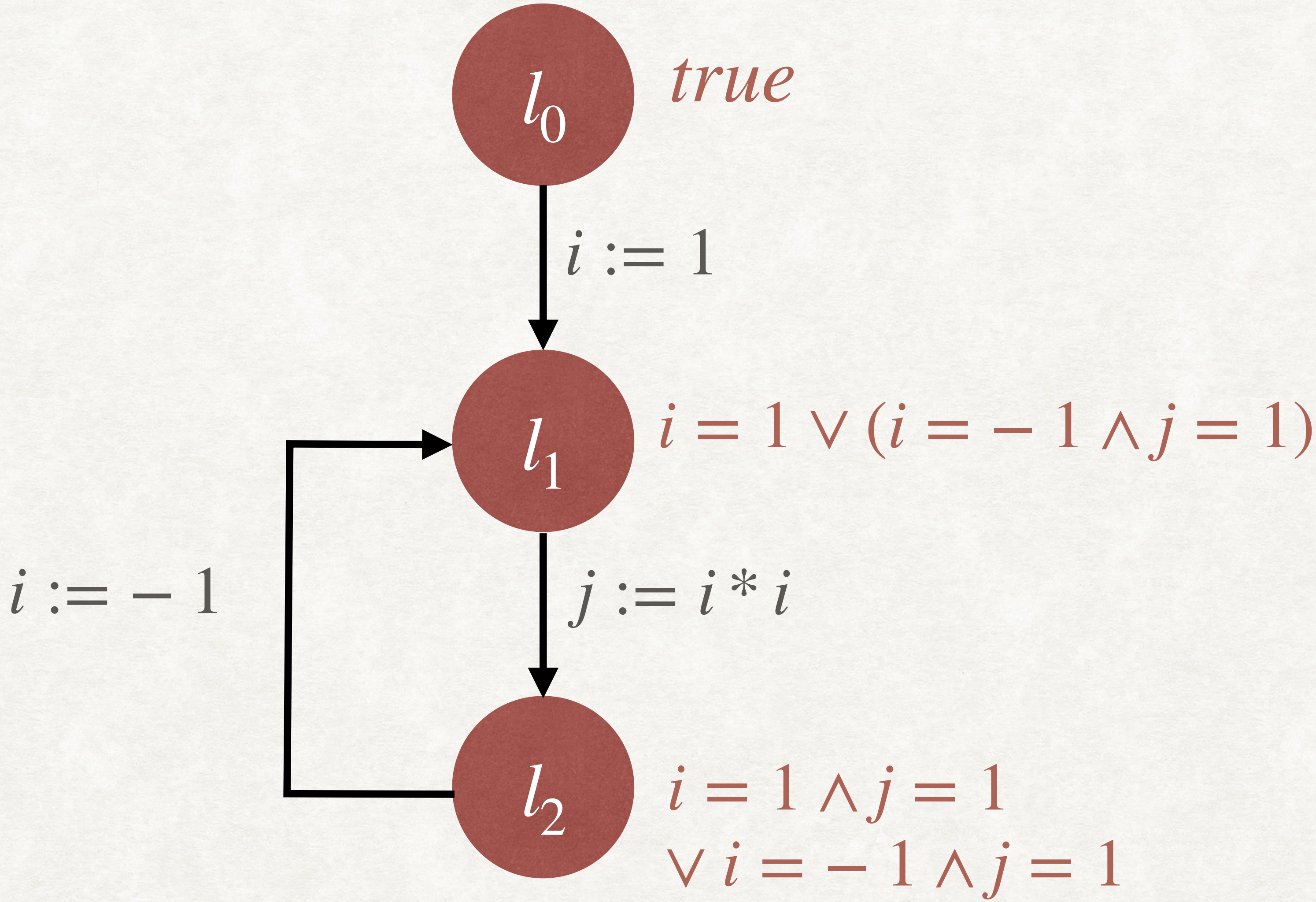
```
i := 0;
while(i < n) do
    i := i + 1;
```



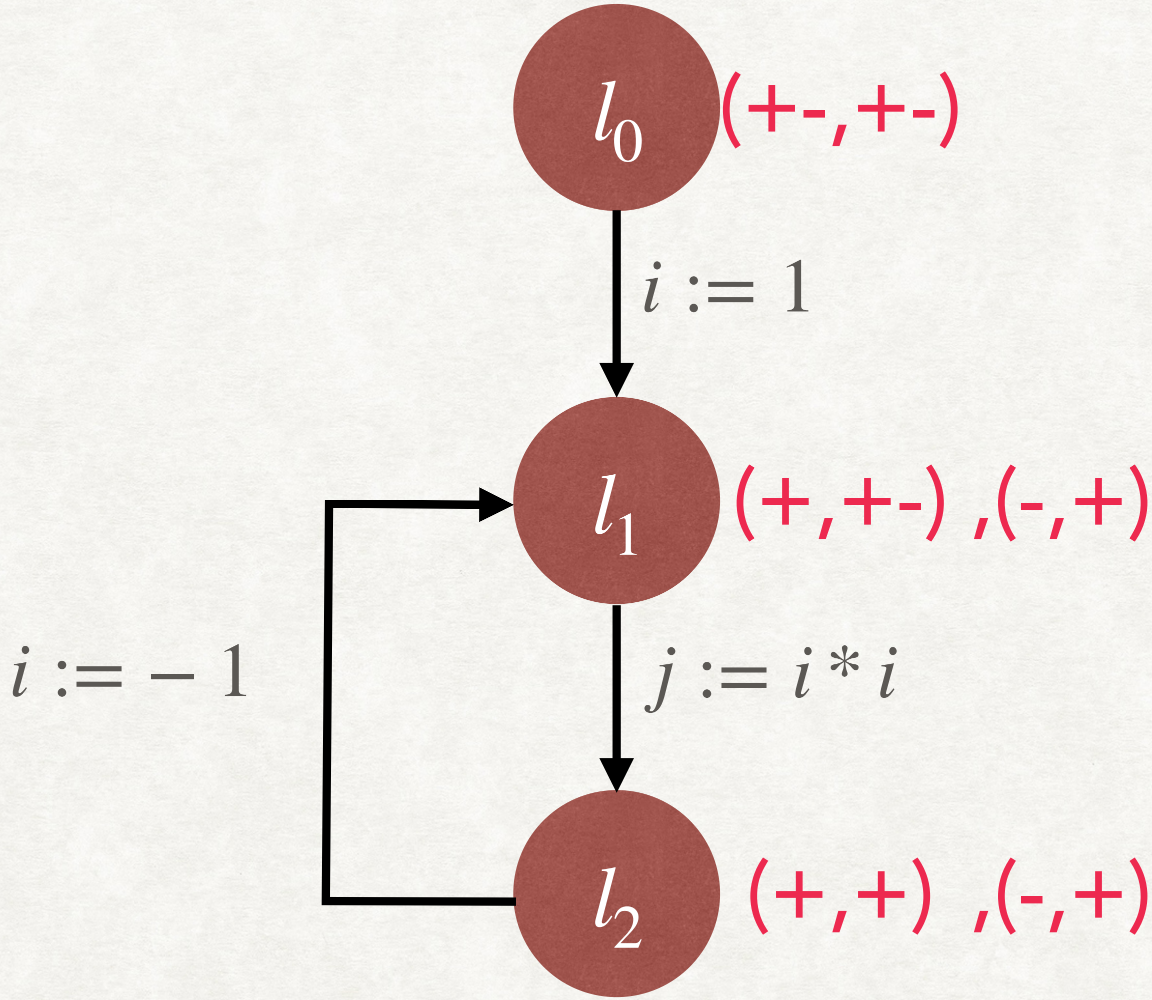
# EXAMPLE - COLLECTING SEMANTICS



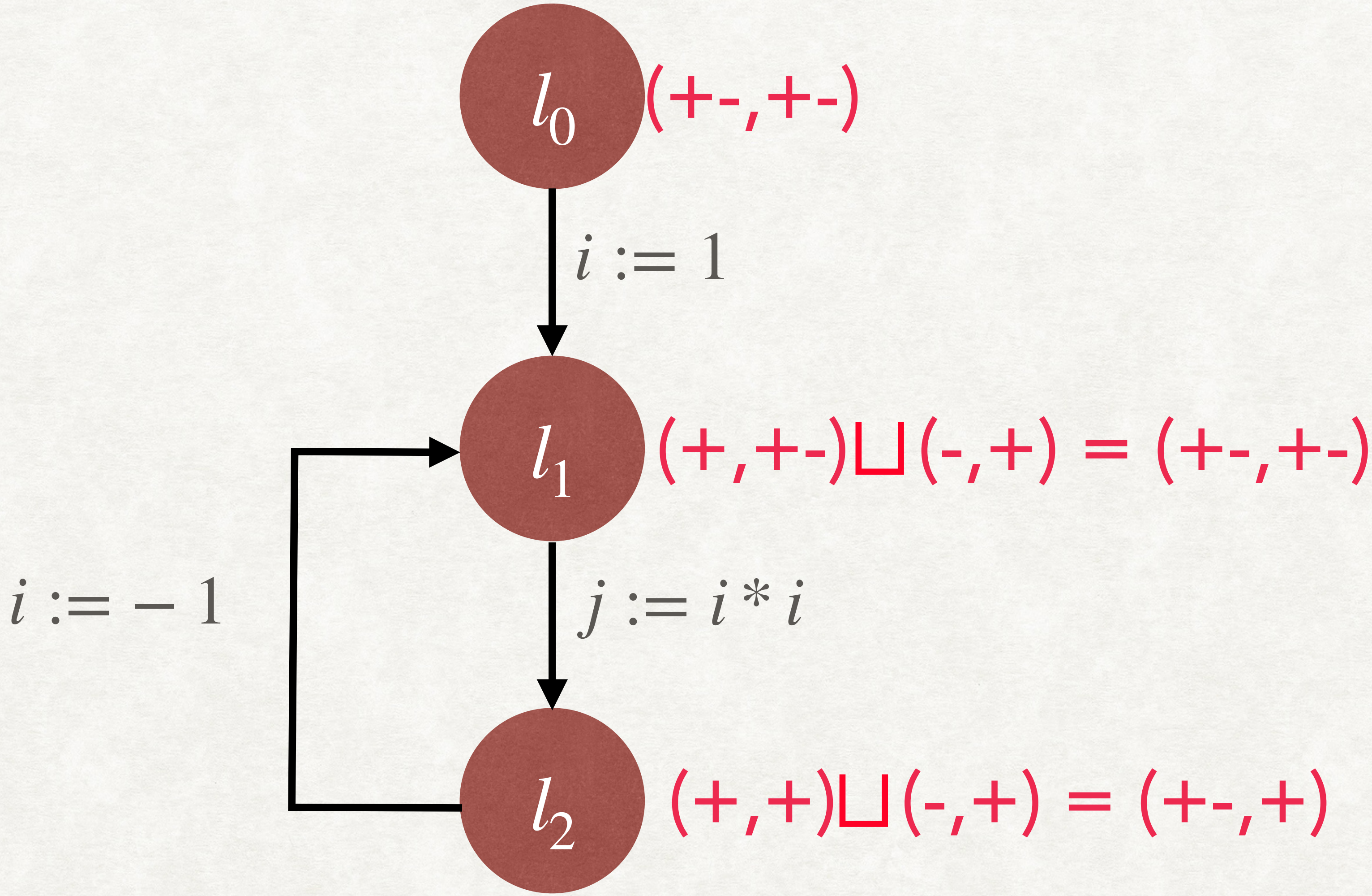
# EXAMPLE - COLLECTING SEMANTICS



# EXAMPLE - ABSTRACT JOP



# EXAMPLE - ABSTRACT JOP



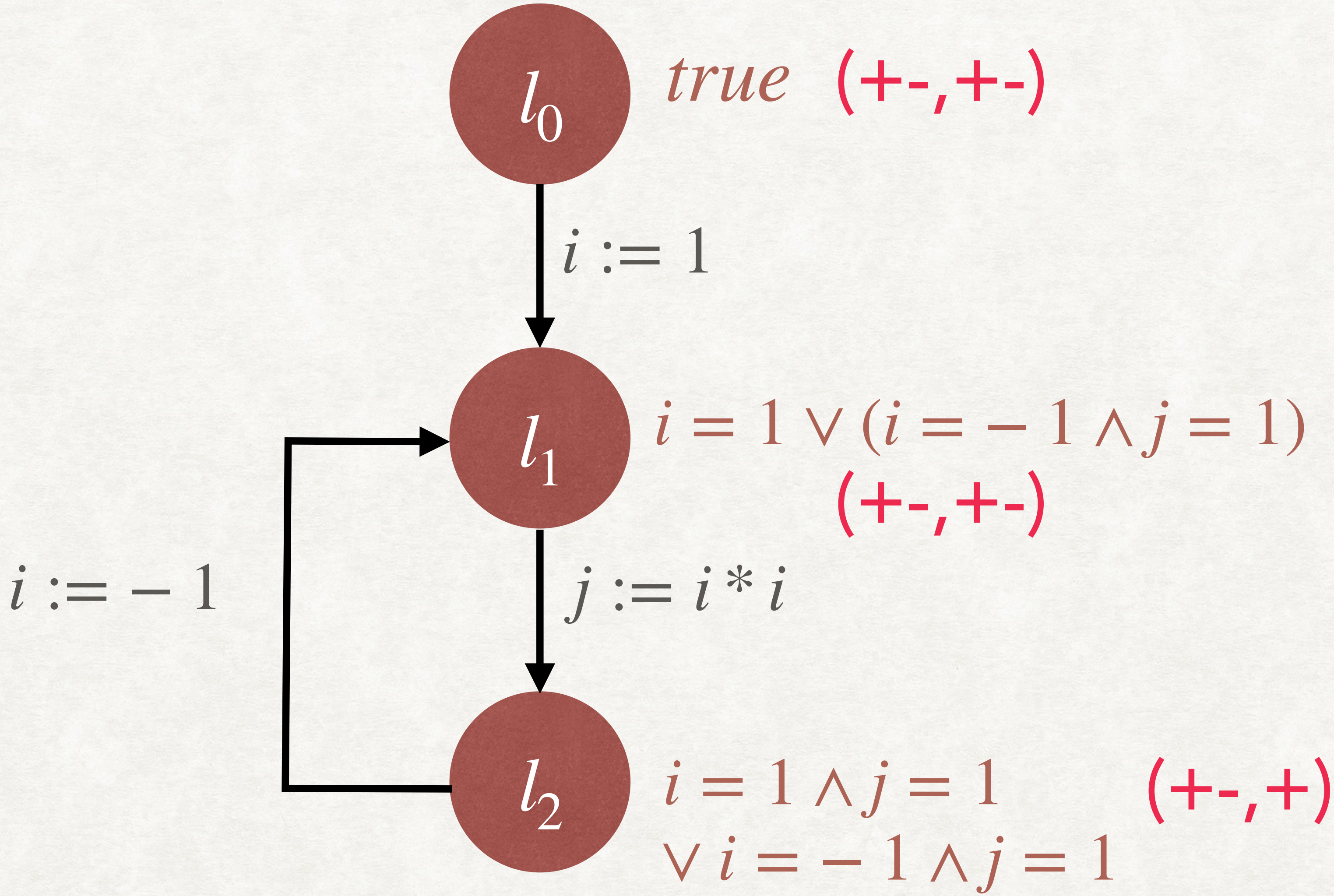
# SOUNDNESS OF ABSTRACT INTERPRETATION

## DEFINITION

- A given abstract interpretation (consisting of the abstract domain $(D, \leq)$, $(\alpha, \gamma)$, and abstract transfer functions $\hat{F}_D$) is sound, if for all $d_0 \in D$, assuming that $\hat{\mu}(l_0) = d_0$, the $\gamma$ image of the abstract JOP $\hat{\mu}$ at all locations over approximates the collecting semantics $\mu$, assuming that $\mu(l_0) = \gamma(d_0)$.
  - For all locations $l$, $\gamma(\hat{\mu}(l)) \supseteq \mu(l)$.

# SOUNDNESS OF ABSTRACT INTERPRETATION

## EXAMPLE



# SOUNDNESS OF ABSTRACT INTERPRETATION

## SUFFICIENT CONDITIONS

- An abstract interpretation $(D, \leq, \alpha, \gamma, \hat{F}_D)$ is sound if:
  - $(D, \leq)$ is complete lattice.
  - $(\mathbb{P}(State), \subseteq) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} (D, \leq)$
  - All abstract transfer functions in $\hat{F}_D$ are monotonic.
  - Every abstract transfer function in $\hat{F}_D$ is a consistent abstraction of the corresponding concrete transfer function.