At start, we have $D_T = \{ x \mapsto T \mid x \in \text{Vars} \}$.

Example:

The abstract effects of edges $[k]^2 \mid \pi$ are again composed to the effects of paths $\pi = k_1 \ldots k_r$ by:

$$[\pi]^2 = [k_r]^2 \circ \ldots \circ [k_1]^2 : D \rightarrow D$$

Idea for Correctness:

Abstract Interpretation
Cousot, Cousot 1977

Establish a description relation $\Delta$ between the concrete values and their descriptions with:

$$x \Delta a_1 \land a_1 \subseteq a_2 \implies x \Delta a_2$$

Concretization:

$$\gamma a = \{ x \mid x \Delta a \}$$

// returns the set of described values :-)}
The abstract effects of edges $[k]^i$ are again composed to the effects of paths $\pi = k_1 \ldots k_p$ by:

$$[\pi]^i = [k_1]^i \circ \ldots \circ [k_i]^i : D \to D$$

**Idea for Correctness:** Abstract Interpretation

Cousot, Cousot 1977

Establish a description relation $\Delta$ between the concrete values and their descriptions with:

$$x \Delta a_1 \land a_1 \subseteq a_2 \implies x \Delta a_2$$

Concretization:

$$\gamma a = \{ x \mid x \Delta a \}$$

// returns the set of described values :-)

(1) Values:

$$\Delta \subseteq \mathbb{Z} \times \mathbb{Z}^\top$$

$$z \Delta a \iff z = a \lor a = \top$$

Concretization:

$$\gamma a = \begin{cases} \{ a \} & \text{if } a \in \top \\ \mathbb{Z} & \text{if } a = \top \end{cases}$$

$$\varnothing \neq \{ 5 \} = \{ 5 \}$$

$$\top = \mathbb{Z}$$

(2) Variable Assignments:

$$\Delta \subseteq (\text{Vars} \to \mathbb{Z}) \times (\text{Vars} \to \mathbb{Z}^\top)$$

$$\forall D \quad \text{iff } D \neq \bot \land \rho x \subseteq D x \quad (x \in \text{Vars})$$

Concretization:

$$\gamma D = \begin{cases} \emptyset & \text{if } D = \bot \\ \{ \forall x : (\rho x) \Delta (D x) \} & \text{otherwise} \end{cases}$$
Example: \[ \{ x \mapsto 1, y \mapsto -7 \} \Delta \{ x \mapsto \top, y \mapsto -7 \} \]

(3) States:
\[ \Delta \subseteq ((\text{Vars} \rightarrow \mathbb{Z}) \times (\mathbb{N} \rightarrow \mathbb{Z})) \times (\text{Vars} \rightarrow \mathbb{Z}^+) \]
\[ (\rho, \mu) \Delta D \iff \rho \Delta D \]

Concretization:
\[ \gamma D = \begin{cases} \emptyset & \text{if } D = \perp \\ \{ (\rho, \mu) \mid \forall x : (\rho x) \Delta (D x) \} & \text{otherwise} \end{cases} \]

We show:

\[ (* ) \text{ If } s \Delta D \text{ and } [\pi] s \text{ is defined, then:} \]
\[ ([\pi] s) \Delta ([\pi]^2 D) \]

\[ \begin{array}{c}
\begin{array}{c}
 s \quad [\pi] \\
\Delta \\
 D \quad [\pi]^2 \\
\Delta \\
 s_1 \end{array}
\end{array} \]

Example: \[ \{ x \mapsto 1, y \mapsto -7 \} \Delta \{ x \mapsto \top, y \mapsto -7 \} \]

(3) States:
\[ \Delta \subseteq ((\text{Vars} \rightarrow \mathbb{Z}) \times (\mathbb{N} \rightarrow \mathbb{Z})) \times (\text{Vars} \rightarrow \mathbb{Z}^+) \]
\[ (\rho, \mu) \Delta D \iff \rho \Delta D \]

Concretization:
\[ \gamma D = \begin{cases} \emptyset & \text{if } D = \perp \\ \{ (\rho, \mu) \mid \forall x : (\rho x) \Delta (D x) \} & \text{otherwise} \end{cases} \]

We show:

\[ (* ) \text{ If } s \Delta D \text{ and } [\pi] s \text{ is defined, then:} \]
\[ ([\pi] s) \Delta ([\pi]^2 D) \]

\[ \begin{array}{c}
\begin{array}{c}
 s \quad [\pi] \\
\Delta \\
 D \quad [\pi]^2 \\
\Delta \\
 s_1 \end{array}
\end{array} \]
The abstract semantics simulates the concrete semantics.

In particular:

\[ [\pi] s \in \gamma([\pi]^D) \]

In practice, this means, e.g., that \( D x = -7 \) implies:

\[ \rho' x = -7 \quad \text{for all} \quad \rho' \in \gamma D \]

\[ \rho_1 x = -7 \quad \text{for} \quad (\rho_1, \_ ) = [\pi] s \]

To prove \((\ast)\), we show for every edge \( k \):

\[ (\ast\ast) \]

Then \((\ast)\) follows by induction.
To prove (**), we show for every expression $e$:

$$([e] \rho) \Delta ([e]^2 D) \text { whenever } \rho \Delta D$$

We show:

1. If $s \Delta D$ and $[\pi] s$ is defined, then:
   $$([\pi] s) \Delta ([\pi]^2 D)$$

2. To prove (**), we show for every edge $k$:
   $$([e] \rho) \Delta ([e]^2 D) \text { whenever } \rho \Delta D$$

Then (+) follows by induction :-}
To prove (**) we show for every expression $e$:

$(* *) \quad ([e] \rho) \Delta ([e]^2 D) \quad \text{whenever} \quad \rho \Delta D$

To prove (**) we show for every operator $\square$:

$(x \boxdot y) \Delta (x^2 \boxdot_1 y^2) \quad \text{whenever} \quad x \Delta x^2 \land y \Delta y^2$

This precisely was how we defined the operators $\square^2$.

Now, (**) is proved by case distinction on the edge labels $lab$.

Let $s = (\rho, \mu) \Delta D$. In particular, $\perp \neq D$.

In particular, $\perp \neq D$.

Case $x = c$:

$\rho_1 = \rho \oplus \{ x \mapsto [e] \rho \}$ \quad $\mu_1 = \mu$

$D_1 = D \oplus \{ x \mapsto [e]^2 D \}$

$\Rightarrow (\rho_1, \mu_1) \Delta D_1$
Now, \((**\)\) is proved by case distinction on the edge labels \(lab\).

Let \(s = (\rho, \mu) \Delta D\). In particular, \(\bot \neq D : \text{Vars} \rightarrow \mathbb{Z}^T\)

**Case** \(x = c\):

\[
\begin{align*}
\rho' & = \rho \oplus \{ x \mapsto [x] \rho \} \\
D' & = D \oplus \{ x \mapsto [x] D \}
\end{align*}
\]

\(\mu_1 = \mu\)

\[
\implies (\rho_1, \mu_1) \Delta D_1
\]

**Case** \(x = M[e]\):

\[
\begin{align*}
\rho_1 & = \rho \oplus \{ x \mapsto \mu([e] D) \} \\
D_1 & = D \oplus \{ x \mapsto \top \}
\end{align*}
\]

\(\mu_1 = \mu\)

\[
\implies (\rho_1, \mu_1) \Delta D_1
\]

**Case** \(M[e_1] = e_2\):

\[
\begin{align*}
\rho_1 & = \rho \\
D_1 & = D \\
\mu_1 & = \mu \oplus \{ [e_1] D \mapsto [e_2] D \}
\end{align*}
\]

\[
\implies (\rho_1, \mu_1) \Delta D_1
\]

**Case** \(\text{Neg}(e)\):

\(\rho_1, \mu_1 = s\) where:

\[
\begin{align*}
0 & = [e] \rho \\
\Delta & \{ [e] D \} \\
\implies 0 & \subset [e] D \\
\implies \bot & \neq D_1 = D \\
\implies (\rho_1, \mu_1) & \Delta D_1
\end{align*}
\]
Case $\text{Pos}(e)$ : 

$(\rho_1, \mu_1) = s$ where:

$0 \neq [\epsilon^* \rho \Delta [\epsilon^* D]$

$\implies 0 \neq [\epsilon^* D]$

$\implies \bot \neq D_1 = D$

$\implies (\rho_1, \mu_1) \Delta D_1$

::)

---

We conclude: The assertion $(\ast)$ is true ::)}

The MOP-Solution:

$$D^*[v] = \bigcup \{ [\pi]^1 D_{\pi} \mid \pi : \text{start} \rightarrow^* v \}$$

where $D_{\pi} x = \top \quad (x \in \text{Vars})$.

---

Case $\text{Pos}(e)$ : 

$(\rho_1, \mu_1) = s$ where:

$0 \neq [\epsilon^* \rho \Delta [\epsilon^* D]$

$\implies 0 \neq [\epsilon^* D]$

$\implies \bot \neq D_1 = D$

$\implies (\rho_1, \mu_1) \Delta D_1$

::)

---

We conclude: The assertion $(\ast)$ is true ::)}

The MOP-Solution:

$$D^*[v] = \bigcup \{ [\pi]^1 D_{\pi} \mid \pi : \text{start} \rightarrow^* v \}$$

where $D_{\pi} x = \top \quad (x \in \text{Vars})$.

By $(\ast)$, we have for all initial states $s$ and all program executions $\pi$ which reach $v$:

$([\pi] s) \Delta (D^*[v])$
We conclude: The assertion (*)& is true :))

The MOP-Solution
\[
D^*[v] = \{ [[\pi]] \uparrow D_T \mid \pi: \text{start} \rightarrow^* v \}
\]
where \( D_T x = \top \quad (x \in \text{Vars}) \).

By (*)& we have for all initial states \( s \) and all program executions \( \pi \) which reach \( v \):
\[
([[\pi]] s) \Delta (D^*[v])
\]

In order to approximate the MOP, we use our constraint system :})

Example:

\[
\begin{array}{c}
0 \quad x = 10; \\
1 \quad y = 1; \\
2 \quad \text{Pos}(x > 1) \\
3 \quad \text{Neg}(x > 1) \\
\text{M}[R] = y; \\
4 \quad y = x \ast y; \\
5 \quad x = x - 1; \\
7 \quad \downarrow
\end{array}
\]

Example:

\[
\begin{array}{c}
0 \quad x = 10; \\
1 \quad y = 1; \\
2 \quad \text{Pos}(x > 1) \\
3 \quad \text{Neg}(x > 1) \\
\text{M}[R] = y; \\
4 \quad y = x \ast y; \\
5 \quad x = x - 1; \\
7 \quad \downarrow
\end{array}
\]
Conclusion:

Although we compute with concrete values, we fail to compute everything :-(

The fixpoint iteration, at least, is guaranteed to terminate:
For $n$ program points and $m$ variables, we maximally need:

$$n \cdot (m + 1) \text{ rounds}$$

Caveat:

The effects of edge are not distributive !!!
Counter Example: \( f = [x = x + y]^1 \)

Let \( D_1 = \{x \mapsto 2, y \mapsto 3\} \)
\( D_2 = \{x \mapsto 3, y \mapsto 2\} \)

\[ f D_1 \sqcup f D_2 = \{x \mapsto 5, y \mapsto 3\} \sqcup \{x \mapsto 5, y \mapsto 2\} \]
\[ = \{x \mapsto 5, y \mapsto 3\} \]
\[ \neq \{x \mapsto 5, y \mapsto 2\} \]
\[ = f \{x \mapsto 5, y \mapsto 2\} \]
\[ = f(D_1 \sqcup D_2) \]

We conclude:

The least solution \( D \) of the constraint system in general yields only an upper approximation of the MOP, i.e.,

\[ D^* \subseteq D \]

We conclude:

As an upper approximation, \( D[v] \) nonetheless describes the result of every program execution \( \pi \) which reaches \( v \):

\( ([\pi] (\rho, \mu)) \Delta (D[v]) \)

whenever \( [\pi] (\rho, \mu) \) is defined. :-)

Transformation 4:

Removal of Dead Code

\( D[u] = \perp \)
Transformation 4 (cont.): Removal of Dead Code

\[ \bot \neq D[u] = D \]
\[ [c]^{T} D = 0 \]

\begin{align*}
\text{Neg} (c) & \quad \Rightarrow \\
\text{Pos} (c) & \quad \Rightarrow \\
\end{align*}

Transformation 4 (cont.): Simplified Expressions

\[ \bot \neq D[u] = D \]
\[ [c]^{T} D = c \]

\[
x = c;
\]

Extensions:

- Instead of complete right-hand sides, also subexpressions could be simplified:

\[
x + (3 * y) \quad \Rightarrow \quad (x + 3) \cdot y \quad \Rightarrow \quad x + 15
\]

... and further simplifications be applied, e.g.:

\[
x * 0 \quad \Rightarrow \quad 0
\]
\[
x + 1 \quad \Rightarrow \quad x
\]
\[
x + 0 \quad \Rightarrow \quad x
\]
\[
x - 0 \quad \Rightarrow \quad x
\]

... 

So far, the information of conditions has not yet be optimally exploited:

\[
\text{if } (x == 7) \quad y = x + 3;
\]

Even if the value of \( x \) before the if statement is unknown, we at least know that \( x \) definitely has the value 7 — whenever the then-part is entered.

Therefore, we can define:

\[
[\text{Pos} (x == c)]^{T} D = \begin{cases} 
D & \text{if } [x == c]^{T} D = 1 \\
\bot & \text{if } [x == c]^{T} D = 0 \\
D_1 & \text{otherwise}
\end{cases}
\]

where

\[
D_1 = D \oplus \{ x \rightarrow (D \cap [c]^{T} D) \}.
\]
Extensions:
- Instead of complete right-hand sides, also subexpressions could be simplified:

\[ x + (3 \times y) \quad \xrightarrow{(x+7, y=5)} \quad x + 15 \]

... and further simplifications be applied. For instance:
- \( x * 1 \Rightarrow 0 \)
- \( x * 1 \Rightarrow x \)
- \( x + 0 \Rightarrow x \)
- \( x - 0 \Rightarrow x \)

\[ x \Rightarrow T \land \neg T \]

The effect of an edge labeled \( \text{Neg} (x \neq e) \) is analogous. 

Our Example:

\[ \begin{align*}
\text{Neg} (x == 7) & \quad \text{Pos} (x == 7) \\
\text{Neg} (x == 7) & \quad \text{Pos} (x == 7)
\end{align*} \]

\[ y = x + 3; \]

\[ y = 10; \]

The effect of an edge labeled \( \text{Neg} (x \neq e) \) is analogous.

Our Example:
The effect of an edge labeled $\text{Neg}(x \neq e)$ is analogous $\because$

Our Example:

![Diagram of a graph with edges labeled Neg(x == 7) and Pos(x == 7).]

1.5 Interval Analysis

Observation:

- Programmers often use global constants for switching debugging code on/off.
  
  $\rightarrow$

  Constant propagation is useful $\because$

- In general, precise values of variables will be unknown — perhaps, however, a tight interval $!!!$

Example:

```plaintext
for (i = 0; i < 42; i++)
  if (0 ≤ i ∧ i < 42)
    $A_i = A + i$;
    $M[A_i] = i$;

// A start address of an array
// if the array-bound check

Obviously, the inner check is superfluous $\because$
```
Idea 1:

Determine for every variable $x$ an (as tight as possible :) interval of possible values:

$$I = \{[l, u] \mid l \in \mathbb{Z} \cup \{-\infty\}, u \in \mathbb{Z} \cup \{+\infty\}, l \leq u\}$$

Partial Ordering:

$$[l_1, u_1] \subseteq [l_2, u_2] \iff l_2 \leq l_1 \land u_1 \leq u_2$$

Thus:

$$[l_1, u_1] \cup [l_2, u_2] = [l_1 \cap l_2, u_1 \cup u_2]$$

Caveat:

$\rightarrow$ II is not a complete lattice :-(

$\rightarrow$ II has infinite ascending chains, e.g.,

$$[0, 0] \subset [0, 1] \subset [-1, 1] \subset [-1, 2] \subset \ldots$$
Caveat:

→ \( \mathbb{I} \) is not a complete lattice \( \therefore \)

→ \( \mathbb{I} \) has infinite ascending chains, e.g.,

\[ [0, 0] \subset [0, 1] \subset [-1, 1] \subset [-1, 2] \subset \ldots \]

\[
\text{While (true)} \\
\text{X = X + 1;}
\]

\[
[0, \phi] \quad [0, \phi] \quad [0, \phi]
\]

322

Example:

\[
\gamma [0, 7] = \{0, \ldots, 7\} \\
\gamma [0, \infty] = \{0, 1, 2, \ldots, \}
\]

Computing with intervals: Interval Arithmetic \( \because \)

Addition:

\[
[l_1, u_1] \cdot [l_2, u_2] = [l_1 + l_2, u_1 + u_2] \quad \text{where} \\
-\infty + - = -\infty \\
+\infty + - = +\infty \\
// -\infty + +\infty \quad \text{cannot occur} \quad \therefore
\]

324

Caveat:

→ \( \mathbb{I} \) is not a complete lattice \( \therefore \)

→ \( \mathbb{I} \) has infinite ascending chains, e.g.,

\[ [0, 0] \subset [0, 1] \subset [-1, 1] \subset [-1, 2] \subset \ldots \]

Description Relation:

\[
z \Delta \frac{l}{u} \quad \text{iff} \\
l \leq z \leq u
\]

Concretization:

\[
\gamma[l, u] = \{z \in \mathbb{Z} \mid l \leq z \leq u\}
\]

323

Caveat:

→ \( \mathbb{I} \) is not a complete lattice \( \therefore \)

→ \( \mathbb{I} \) has infinite ascending chains, e.g.,

\[ [0, 0] \subset [0, 1] \subset [-1, 1] \subset [-1, 2] \subset \ldots \]

Description Relation:

\[
z \Delta \frac{l}{u} \quad \text{iff} \\
l \leq z \leq u
\]

Concretization:

\[
\gamma[l, u] = \{z \in \mathbb{Z} \mid l \leq z \leq u\}
\]

323