**Script** generated by TTT

Title: Seidl: Programmoptimierung (13.11.2013)

Date: Wed Nov 13 08:32:31 CET 2013

Duration: 88:07 min

Pages: 43

---

Caveat: $\mathbb{Z}^\top$ is not a complete lattice in itself :-(

(2) $\mathbb{D} = (\mathit{Vars} \to \mathbb{Z}^\top)_\perp = (\mathit{Vars} \to \mathbb{Z}^\top) \cup \{\perp\}$

// $\perp$ denotes: "not reachable" :-))

with $D_1 \sqsubseteq D_2$ iff $\perp = D_1$ or

$D_1\, x \sqsubseteq D_2\, x \quad (x \in \mathit{Vars})$

Remark: $\mathbb{D}$ is a complete lattice :-)

Consider $X \subseteq \mathbb{D}$ . W.l.o.g., $\perp \notin X$ .

Then $X \subseteq \mathit{Vars} \to \mathbb{Z}^\top$ .

If $X = \emptyset$ , then $\bigsqcup X = \perp \in \mathbb{D}$ :-)



---

If $X \neq \emptyset$ , then $\bigsqcup X = D$ with

$$D\, x = \bigsqcup\{f\, x \mid f \in X\} = \begin{cases} z & \text{if } \cancel{f\, x} = z \quad (f \in X) \\ \top & \text{otherwise} \end{cases}$$

:-))



---

If $X \neq \emptyset$ , then $\bigsqcup X = D$ with

$$D\, x = \bigsqcup\{f\, x \mid f \in X\} = \begin{cases} z & \text{if } f\, x = z \quad (f \in X) \\ \top & \text{otherwise} \end{cases}$$

:-))

For every edge $k = (\_, \mathit{lab}, \_)$ , construct an effect function $[\![k]\!]^\sharp = [\![\mathit{lab}]\!]^\sharp : \mathbb{D} \to \mathbb{D}$ which simulates the concrete computation.

Obviously, $[\![\mathit{lab}]\!]^\sharp \perp = \perp$ for all $\mathit{lab}$ :-)

Now let $\perp \neq D \in \mathit{Vars} \to \mathbb{Z}^\top$.

## Idea:

- We use $D$ to determine the values of expressions.

$$[\![x = x+y]\!]\ \{x \mapsto 5, y \mapsto \top\}$$



## Idea:

- We use $D$ to determine the values of expressions.
- For some sub-expressions, we obtain $\top$ :-)

$\Longrightarrow$

We must replace the concrete operators $\square$ by abstract operators $\square^\sharp$ which can handle $\top$:

$$a \,\square^\sharp\, b = \begin{cases} \top & \text{if} \quad a = \top \text{ or } b = \top \\ a \,\square\, b & \text{otherwise} \end{cases}$$



## Idea:

- We use $D$ to determine the values of expressions.
- For some sub-expressions, we obtain $\top$ :-)

$\Longrightarrow$

We must replace the concrete operators $\square$ by abstract operators $\square^\sharp$ which can handle $\top$:

$$a \,\square^\sharp\, b = \begin{cases} \top & \text{if} \quad a = \top \text{ or } b = \top \\ a \,\square\, b & \text{otherwise} \end{cases}$$

- The abstract operators allow to define an abstract evaluation of expressions:

$$[\![e]\!]^\sharp \;:\; (\mathit{Vars} \to \mathbb{Z}^\top) \to \mathbb{Z}^\top$$



## Idea:

- We use $D$ to determine the values of expressions.
- For some sub-expressions, we obtain $\top$ :-)

$\Longrightarrow$

We must replace the concrete operators $\square$ by abstract operators $\square^\sharp$ which can handle $\top$:

$$a \,\square^\sharp\, b = \begin{cases} \top & \text{if} \quad a = \top \text{ or } b = \top \\ a \,\square\, b & \text{otherwise} \end{cases}$$

- The abstract operators allow to define an abstract evaluation of expressions:

$$[\![e]\!]^\sharp \;:\; (\mathit{Vars} \to \mathbb{Z}^\top) \to \mathbb{Z}^\top$$

Abstract evaluation of expressions is like the concrete evaluation — but with abstract values and operators. Here:

$$
\begin{array}{lll}
[\![c]\!]^\sharp\, D & = & c \\
[\![e_1 \,\square\, e_2]\!]^\sharp\, D & = & [\![e_1]\!]^\sharp\, D \,\square^\sharp\, [\![e_2]\!]^\sharp\, D
\end{array}
$$

... analogously for unary operators :-)



Abstract evaluation of expressions is like the concrete evaluation — but with abstract values and operators. Here:

$$
\begin{array}{lll}
[\![c]\!]^\sharp\, D & = & c \\
[\![e_1 \,\square\, e_2]\!]^\sharp\, D & = & [\![e_1]\!]^\sharp\, D \,\square^\sharp\, [\![e_2]\!]^\sharp\, D
\end{array}
$$

... analogously for unary operators :-)

**Example:** $D = \{x \mapsto 2, y \mapsto \top\}$

$$
\begin{array}{lll}
[\![x + 7]\!]^\sharp\, D & = & [\![x]\!]^\sharp\, D +^\sharp [\![7]\!]^\sharp\, D \\
& = & 2 +^\sharp 7 \\
& = & 9 \\
[\![x - y]\!]^\sharp\, D & = & 2 -^\sharp \top \\
& = & \top
\end{array}
$$



Thus, we obtain the following effects of edges $[\![lab]\!]^\sharp$ :

$$
\begin{array}{lll}
[\![;]\!]^\sharp\, D & = & D \\
[\![\mathrm{Pos}\,(e)]\!]^\sharp\, D & = & \begin{cases} \bot & \text{if } 0 = [\![e]\!]^\sharp\, D \\ D & \text{otherwise} \end{cases} \\
[\![\mathrm{Neg}\,(e)]\!]^\sharp\, D & = & \begin{cases} D & \text{if } 0 \sqsubseteq [\![e]\!]^\sharp\, D \\ \bot & \text{otherwise} \end{cases} \\
[\![x = e;]\!]^\sharp\, D & = & D \oplus \{x \mapsto [\![e]\!]^\sharp\, D\} \\
[\![x = M[e];]\!]^\sharp\, D & = & D \oplus \{x \mapsto \top\} \\
[\![M[e_1] = e_2;]\!]^\sharp\, D & = & D
\end{array}
$$

$0, \top$

$1, 7, -3, 5, \ldots$

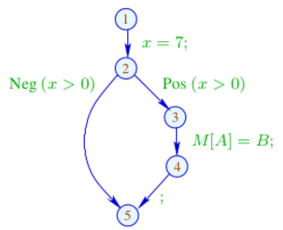
... whenever $D \neq \bot$ :-)



At *start*, we have $D_\top = \{x \mapsto \top \mid x \in \mathit{Vars}\}$ .

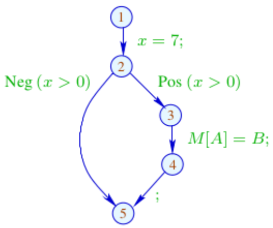
**Example:**

$\bot$



At *start*, we have $D_\top = \{x \mapsto \top \mid x \in \mathit{Vars}\}$ .

## Example:




| | |
|---|---|
| 1 | $\{x \mapsto \top\}$ |
| 2 | $\{x \mapsto 7\}$ |
| 3 | $\{x \mapsto 7\}$ |
| 4 | $\{x \mapsto 7\}$ |
| 5 | $\bot \sqcup \{x \mapsto 7\} = \{x \mapsto 7\}$ |



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

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977



Patrick Cousot, ENS, Paris



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

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977

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

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977

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

$$x \,\Delta\, a_1 \;\wedge\; a_1 \sqsubseteq a_2 \;\Longrightarrow\; x \,\Delta\, a_2$$

Concretization: $\gamma\, a = \{x \mid x \,\Delta\, a\}$

// returns the set of described values :-)



Patrick Cousot, ENS, Paris



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

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977

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

$$x \,\Delta\, a_1 \;\wedge\; a_1 \sqsubseteq a_2 \;\Longrightarrow\; x \,\Delta\, a_2$$

$\gamma(a_1) \leq \gamma(a_2)$

Concretization: $\gamma\, a = \{x \mid x \,\Delta\, a\}$

// returns the set of described values :-)



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

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977

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

$$x \,\Delta\, a_1 \;\wedge\; a_1 \sqsubseteq a_2 \;\Longrightarrow\; x \,\Delta\, a_2$$

Concretization: $\gamma\, a = \{x \mid x \,\Delta\, a\}$

// returns the set of described values :-)

(1) Values: $\Delta \subseteq \mathbb{Z} \times \mathbb{Z}^{\top}$

$$z \,\Delta\, a \quad \text{iff} \quad z = a \vee a = \top$$

Concretization:

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



(1) Values: $\Delta \subseteq \mathbb{Z} \times \mathbb{Z}^{\top}$

$$z \,\Delta\, a \quad \text{iff} \quad z = a \vee a = \top$$

Concretization:

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

(2) Variable Assignments: $\Delta \subseteq (\mathit{Vars} \to \mathbb{Z}) \times (\mathit{Vars} \to \mathbb{Z}^{\top})_{\perp}$

$$\rho \,\Delta\, D \quad \text{iff} \quad D \neq \perp \wedge \rho\, x \sqsubseteq D\, x \quad (x \in \mathit{Vars})$$

Concretization:

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



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

(3) States:

$$\Delta \subseteq ((\mathit{Vars} \to \mathbb{Z}) \times (\mathbb{N} \to \mathbb{Z})) \times (\mathit{Vars} \to \mathbb{Z}^{\top})_{\perp}$$

$$(\rho, \mu) \,\Delta\, D \qquad \text{iff} \qquad \rho \,\Delta\, D$$

Concretization:

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



## We show:

$(*)$ If $s \,\Delta\, D$ and $[\![\pi]\!]\, s$ is defined, then:

$$([\![\pi]\!]\, s) \ \Delta \ ([\![\pi]\!]^{\sharp}\, D)$$

$$\begin{tikzcd} s \arrow[r, "{[\![\pi]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\ D \arrow[r, "{[\![\pi]\!]^{\sharp}}"'] & D_1 \end{tikzcd}$$

The abstract semantics simulates the concrete semantics :-)

In particular:

$$[\![\pi]\!]\, s \in \gamma\,([\![\pi]\!]^\sharp\, D)$$



The abstract semantics simulates the concrete semantics :-)

In particular:

$$[\![\pi]\!]\, s \in \gamma\,([\![\pi]\!]^\sharp\, D)$$

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

$$\begin{array}{lrcll} & \rho'\, x & = & -7 & \text{for all} \quad \rho' \in \gamma\, D \\ \Longrightarrow & \rho_1\, x & = & -7 & \text{for} \quad (\rho_1, \_) = [\![\pi]\!]\, s \end{array}$$



We show:

$(*)$ If $s \,\Delta\, D$ and $[\![\pi]\!]\, s$ is defined, then:

$$([\![\pi]\!]\, s) \;\; \Delta \;\; ([\![\pi]\!]^\sharp\, D)$$

$$\begin{tikzcd} \boxed{s} \arrow[r, "{[\![\pi]\!]}"] \arrow[d, dash, "\Delta"'] & \boxed{s_1} \arrow[d, dash, dotted, "\Delta"] \\ \boxed{D} \arrow[r, "{[\![\pi]\!]^\sharp}"'] & \boxed{D_1} \end{tikzcd}$$



The abstract semantics simulates the concrete semantics :-)

In particular:

$$[\![\pi]\!]\, s \in \gamma\,([\![\pi]\!]^\sharp\, D)$$

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

$$\begin{array}{lrcll} & \rho'\, x & = & -7 & \text{for all} \quad \rho' \in \gamma\, D \\ \Longrightarrow & \rho_1\, x & = & -7 & \text{for} \quad (\rho_1, \_) = [\![\pi]\!]\, s \end{array}$$

We show:

$(*)$ If $s \,\Delta\, D$ and $[\![\pi]\!]\, s$ is defined, then:

$$([\![\pi]\!]\, s) \;\;\Delta\;\; ([\![\pi]\!]^\sharp\, D)$$

$$\begin{tikzcd} s \arrow[r, "{[\![\pi]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\ D \arrow[r, "{[\![\pi]\!]^\sharp}"'] & D_1 \end{tikzcd}$$



To prove $(*)$, we show for every edge $k$ :

$$(**) \quad \begin{tikzcd} s \arrow[r, "{[\![k]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\ D \arrow[r, "{[\![k]\!]^\sharp}"'] & D_1 \end{tikzcd}$$

Then $(*)$ follows by induction :-)



To prove $(*)$, we show for every edge $k$ :

$$(**) \quad \begin{tikzcd} s \arrow[r, "{[\![k]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\ D \arrow[r, "{[\![k]\!]^\sharp}"'] & D_1 \end{tikzcd}$$

Then $(*)$ follows by induction :-)

290

To prove $(**)$, we show for every expression $e$ :

$(*\!*\!*)$ $\quad ([\![e]\!]\, \rho) \;\;\Delta\;\; ([\![e]\!]^\sharp\, D)$ whenever $\rho \,\Delta\, D$

To prove $(**)$, we show for every expression $e$ :

$(***)$ $\quad ([\![e]\!]\,\rho) \;\Delta\; ([\![e]\!]^\sharp\, D)$ whenever $\rho \;\Delta\; D$

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

$$(x \,\square\, y) \;\Delta\; (x^\sharp \,\square^\sharp\, y^\sharp) \qquad \text{whenever} \quad x \;\Delta\; x^\sharp \wedge y \;\Delta\; y^\sharp$$



To prove $(**)$, we show for every expression $e$ :

$(***)$ $\quad ([\![e]\!]\,\rho) \;\Delta\; ([\![e]\!]^\sharp\, D)$ whenever $\rho \;\Delta\; D$

Induction

Base Case

$[\![x]\!]\,\rho \;\Delta\; [\![x]\!]^\sharp\, D$

$\rho(x) \;\Delta\; D(x)^\sharp$



To prove $(**)$, we show for every expression $e$ :

$(***)$ $\quad ([\![e]\!]\,\rho) \;\Delta\; ([\![e]\!]^\sharp\, D)$ whenever $\rho \;\Delta\; D$

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

$$\boxed{(x \,\square\, y) \;\Delta\; (x^\sharp \,\square^\sharp\, y^\sharp) \qquad \text{whenever} \quad x \;\Delta\; x^\sharp \wedge y \;\Delta\; y^\sharp}$$



To prove $(**)$, we show for every expression $e$ :

$(***)$ $\quad ([\![e]\!]\,\rho) \;\Delta\; ([\![e]\!]^\sharp\, D)$ whenever $\rho \;\Delta\; D$

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

$$(x \,\square\, y) \;\Delta\; (x^\sharp \,\square^\sharp\, y^\sharp) \qquad \text{whenever} \quad x \;\Delta\; x^\sharp \wedge y \;\Delta\; y^\sharp$$

This precisely was how we have defined the operators $\square^\sharp$ :-)

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

Let $s = (\rho, \mu) \, \Delta \, D$ . In particular, $\bot \neq D \;\; : \;\; \textit{Vars} \to \mathbb{Z}^\top$

**Case** $\boxed{x = e;}$ :

$$\rho_1 = \rho \oplus \{x \mapsto [\![e]\!]\,\rho\} \qquad \mu_1 = \mu$$
$$D_1 = D \oplus \{x \mapsto [\![e]\!]^\sharp\,D\}$$
$$\Longrightarrow \qquad (\rho_1, \mu_1) \, \Delta \, D_1$$



**Case** $\boxed{x = M[e];}$ :

$$\rho_1 = \rho \oplus \{x \mapsto \mu\,([\![e]\!]^\sharp \rho)\} \qquad \mu_1 = \mu$$
$$D_1 = D \oplus \{x \mapsto \top\}$$
$$\Longrightarrow \qquad (\rho_1, \mu_1) \, \Delta \, D_1$$

**Case** $\boxed{M[e_1] = e_2;}$ :

$$\rho_1 = \rho \qquad \mu_1 = \mu \oplus \{[\![e_1]\!]^\sharp \rho \mapsto [\![e_2]\!]^\sharp \rho\}$$
$$D_1 = D$$
$$\Longrightarrow \qquad (\rho_1, \mu_1) \, \Delta \, D_1$$



**Case** $\boxed{\mathrm{Neg}(e)}$ : $\qquad (\rho_1, \mu_1) = s$ where:

$$0 = [\![e]\!]\,\rho$$
$$\Delta \;\; [\![e]\!]^\sharp\,D$$
$$\Longrightarrow \quad 0 \sqsubseteq [\![e]\!]^\sharp\,D$$
$$\Longrightarrow \quad \bot \neq D_1 = D$$
$$\Longrightarrow \quad (\rho_1, \mu_1) \, \Delta \, D_1$$

s ?



**Case** $\boxed{\mathrm{Neg}(e)}$ : $\qquad (\rho_1, \mu_1) = s$ where:

$$0 = [\![e]\!]\,\rho$$
$$\Delta \;\; [\![e]\!]^\sharp\,D$$
$$\Longrightarrow \quad 0 \sqsubseteq [\![e]\!]^\sharp\,D$$
$$\Longrightarrow \quad \bot \neq D_1 = D$$
$$\Longrightarrow \quad (\rho_1, \mu_1) \, \Delta \, D_1$$

$S_1$

$\shortparallel$

Case $\boxed{\text{Pos}(e)}$ : $(\rho_1, \mu_1) = s$ where:

$$
\begin{array}{rll}
 & 0 & \neq \ [\![e]\!]\,\rho \\
 & & \Delta \ [\![e]\!]^\sharp\,D \\
\Longrightarrow & 0 & \neq \ [\![e]\!]^\sharp\,D \\
\Longrightarrow & \bot & \neq \ D_1 \ = \ D \\
\Longrightarrow & (\rho_1, \mu_1) & \Delta \ D_1
\end{array}
$$

$\shortparallel \qquad \shortparallel$

$s \qquad D$ :-)



We conclude: The assertion $(*)$ is true :-))

The MOP-Solution:

$$\mathcal{D}^*[v] \ = \ \bigsqcup \{ [\![\pi]\!]^\sharp\, D_\top \mid \pi : start \rightarrow^* v \}$$

where $D_\top\, x = \top \qquad (x \in Vars)$ .



We conclude: The assertion $(*)$ is true :-))

The MOP-Solution:

$$\mathcal{D}^*[v] \ = \ \bigsqcup \{ [\![\pi]\!]^\sharp\, D_\top \mid \pi : start \rightarrow^* v \}$$

where $D_\top\, x = \top \qquad (x \in Vars)$ .

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

$$([\![\pi]\!]\, s) \ \Delta \ (\mathcal{D}^*[v])$$



We conclude: The assertion $(*)$ is true :-))

The MOP-Solution

$$\mathcal{D}^*[v] \ = \ \bigsqcup \{ [\![\pi]\!]^\sharp\, D_\top \mid \pi : start \rightarrow^* v \}$$

where $D_\top\, x = \top \qquad (x \in Vars)$ .

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

$$([\![\pi]\!]\, s) \ \Delta \ (\mathcal{D}^*[v])$$

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