Induced Operations

Fabian Schaub
Kamal Zakieldin

2019-06-13

Outline

- Motivation
- Inducing along the Abstraction function
  - Correctness
  - Fixed Points
  - Application to Data Flow Analysis
  - Example
- Inducing along the Concretisation function
  - Introduction
  - Concretisation process
  - Widening Operator
  - Correctness

Induced Operations

Key Idea

Use Galois connections to transform computations into more approximate computations with better time-, space-, or termination behavior.

Induced Operations

Two possible ways:

Inducing along the Abstraction function

- Replace a computation using L by a computation using M:

  Analysis using M is an upper approximation to the analysis *induced* by L (loss of precision).

Inducing along the Concretisation function

- Use M for approximating the fixed point computations in L:

  Ensure convergence of fixed points by using the more approximate complete lattice M while maintaining precision of the analysis.

Inducing along the Abstraction Function

Assumptions

- Galois connections $(L_1, \alpha_1, \gamma_1, M_1)$ and $(L_2, \alpha_2, \gamma_2, M_2)$
- Analysis $f_p\ :\ L_1 \to L_2$

Goal

Replace f_p by new more approximate analysis $g_p\ :\ M_1 \to M_2$.

- Candidate for g_p: $\alpha_2 \circ f_p \circ \gamma_1$

Inducing along the Abstraction Function

Example

Consider analysis $f_{plus}(\mathbb{ZZ}) = \{z_1 + z_2 \mid (z_1, z_2) \in \mathbb{ZZ}\}$ using complete lattices $(\mathscr{P}(\mathbb{Z}), \subseteq)$ and $(\mathscr{P}(\mathbb{Z} \times \mathbb{Z}), \subseteq)$.

Galois Connections

- $(\mathscr{P}(\mathbb{Z}), \alpha_{sign}, \gamma_{sign}, \mathscr{P}(\mathbf{Sign}))$
  - $\alpha_{sign}(Z) = \{sign(z) \mid z \in Z\}$
  - $\gamma_{sign}(S) = \{z \in Z \mid sign(z) \in S\}$
- $(\mathscr{P}(\mathbb{Z} \times \mathbb{Z}), \alpha_{SS'}, \gamma_{SS'}, \mathscr{P}(\mathbf{Sign} \times \mathbf{Sign}))$
  - $\alpha_{SS'}(ZZ) = \{(sign(z_1), sign(z_2)) \mid (z_1, z_2) \in ZZ\}$
  - $\gamma_{SS'}(SS) = \{(z_1, z_2) \mid (sign(z_1), sign(z_2)) \in SS\}$

Inducing along the Abstraction Function

Example (cont'd)

Construct analysis $g_{plus} : \mathscr{P}(\mathbf{Sign} \times \mathbf{Sign}) \to \mathscr{P}(\mathbf{Sign})$ from f_{plus}, using candidate $g_{plus} = \alpha_{sign} \circ f_{plus} \circ \gamma_{SS'}$.

$$
\begin{aligned}
g_{plus}(SS) &= \alpha_{sign}(f_{plus}(\gamma_{SS'}(SS))) \\
&= \alpha_{sign}(f_{plus}(\{(z_1, z_2) \mid (sign(z_1), sign(z_2)) \in SS\})) \\
&= \alpha_{sign}(\{z_1 + z_2 \mid (sign(z_1), sign(z_2)) \in SS\}) \\
&= \{sign(z_1 + z_2) \mid (sign(z_1), sign(z_2)) \in SS\} \\
&= \bigcup \{s_1 \oplus s_2 \mid (s_1, s_2) \in SS\}
\end{aligned}
$$

where $\oplus$ is the "addition" on signs.

Inducing along the Abstraction Function

Correctness

Recap

- Galois connections $(L_i, \alpha_i, \gamma_i, M_i),\ i \in \{1, 2\}$
- Analysis $f_p : L_1 \to L_2$
- Analysis $g_p : M_1 \to M_2$

Correctness relations

- Representation functions $\beta_i : V_i \to L_i$
- Correctness relation $R_i : V_i \times L_i \to \{true, false\}$ generated by $\beta_i : V_i \to L_i$
- Correctness relation $S_i : V_i \times M_i \to \{true, false\}$ generated by $\alpha_i \circ \beta_i : V_i \to M_i$

Inducing along the Abstraction Function

Correctness cont'd

Lemma 4.41

If $(L_i, \alpha_i, \gamma_i, M_i)$ are Galois connections and $\beta_i : V_i \to L_i$ are representation functions, then

$$((\alpha_1 \circ \beta_1) \twoheadrightarrow (\alpha_2 \circ \beta_2))(\rightsquigarrow) = \alpha_2 \circ ((\beta_1 \twoheadrightarrow \beta_2)(\rightsquigarrow)) \circ \gamma_1$$

holds for all $\rightsquigarrow$.

Inducing along the Abstraction Function

Correctness cont'd

Proof (Lemma 4.41)

Simply calculate:

$$
\begin{aligned}
&((\alpha_1 \circ \beta_1) \twoheadrightarrow (\alpha_2 \circ \beta_2))(\rightsquigarrow)(m_1) \\
&\quad = \bigsqcup \{\alpha_2(\beta_2(v_2)) \mid \alpha_1(\beta_1(v_1)) \sqsubseteq m_1 \wedge v_1 \rightsquigarrow v_2\} \\
&\quad = \alpha_2 \left(\bigsqcup \{\beta_2(v_2)) \mid \beta_1(v_1) \sqsubseteq \gamma_1(m_1) \wedge v_1 \rightsquigarrow v_2\} \right) \\
&\quad = \alpha_2((\beta_1 \twoheadrightarrow \beta_2)(\rightsquigarrow)(\gamma_1(m_1)) \\
&\quad = (\alpha_2 \circ ((\beta_1 \twoheadrightarrow \beta_2)(\rightsquigarrow)) \circ \gamma_1)(m_1)
\end{aligned}
$$

∎

Inducing along the Abstraction Function

Correctness cont'd

Lemma 4.41 yields:

$$(p \vdash \cdot \rightsquigarrow \cdot)(R_1 \twoheadrightarrow R_2) f_p \wedge \alpha_2 \circ f_p \circ \gamma_1 \sqsubseteq g_p$$
$$\Rightarrow (p \vdash \cdot \rightsquigarrow \cdot)(S_1 \twoheadrightarrow S_2) g_p$$

In words: if f_p is correct and g_p is an upper approximation to the induced analysis $\alpha_2 \circ f_p \circ \gamma_1$ then also g_p is correct.

Inducing along the Abstraction Function

Correctness cont'd

Proof

1. Suppose $(p \vdash \cdot \rightsquigarrow \cdot)(R_1 \twoheadrightarrow R_2)f_p$ and $\alpha_2 \circ f_p \circ \gamma_1 \sqsubseteq g_p$.
2. Since $(L_i, \alpha_i, \gamma_i, M_i)$ are Galois connections and f_p and g_p are monotone we get $f_p \sqsubseteq \gamma_2 \circ g_p \circ \alpha_1$.
3. Using the first assumption and Lemma 4.8:

$$
\begin{aligned}
&(p \vdash \cdot \rightsquigarrow \cdot)(R_1 \twoheadrightarrow R_2)f_p \wedge f_p \sqsubseteq \gamma_2 \circ g_p \circ \alpha_1 \\
&\qquad \Rightarrow (\beta_1 \twoheadrightarrow \beta_2)(p \vdash \cdot \rightsquigarrow \cdot) \sqsubseteq f_p \wedge f_p \sqsubseteq \gamma_2 \circ g_p \circ \alpha_1 \\
&\qquad \Rightarrow (\beta_1 \twoheadrightarrow \beta_2)(p \vdash \cdot \rightsquigarrow \cdot) \sqsubseteq \gamma_2 \circ g_p \circ \alpha_1 \\
&\qquad \Rightarrow \alpha_2 \circ (\beta_1 \twoheadrightarrow \beta_2)(p \vdash \cdot \rightsquigarrow \cdot) \circ \gamma_1 \sqsubseteq g_p \\
&\qquad \Rightarrow (\alpha_1 \circ \beta_1 \twoheadrightarrow \alpha_2 \circ \beta_2)(p \vdash \cdot \rightsquigarrow \cdot) \sqsubseteq g_p \\
&\qquad \Rightarrow (p \vdash \cdot \rightsquigarrow \cdot)(S_1 \twoheadrightarrow S_2)g_p
\end{aligned}
$$

Inducing along the Abstraction Function

Optimality

Definition

A function $f_p : L_1 \to L_2$ is *optimal* for the program p if and only if correctness of a function $f' : L_1 \to L_2$ amounts to $f_p \sqsubseteq f'$

Equivalently, f_p is *optimal* if and only if $(\beta_1 \twoheadrightarrow \beta_2)(p \vdash \cdot \rightsquigarrow \cdot) = f_p$

Lemma 4.41 may then be read as saying that if $f_p : L_1 \to L_2$ is optimal then so is $\alpha_2 \circ f_p \circ \gamma_1 : M_1 \to M_2$.

Inducing along the Abstraction Function

Fixed Points

Consider analysis $f_p : L_1 \to L_2$ requires computation of the least fixed point of a monotone function $F : (L_1 \to L_2) \to (L_1 \to L_2)$ so that $f_p = \mathit{lfp}(F)$.

- $(L_i, \alpha_i, \gamma_i, M_i)$ give rise to $(L_1 \to L_2, \alpha, \gamma, M_1 \to M_2)$
- Let $G : (M_1 \to M_2) \to (M_1 \to M_2)$ be an upper approximation to $\alpha \circ F \circ \gamma$
- Take $g_p : M_1 \to M_2$ to be $g_p = \mathit{lfp}(G)$

Fact

Correctness of f_p carries over to g_p.

Inducing along the Abstraction Function

Fixed Points - Correctness

Lemma 4.42

Assume

- (L, α, γ, M) is a Galois connection
- $f : L \to L$ and $g : M \to M$ are monotone functions
- g is an upper approximation to f (i.e. $\alpha \circ f \circ \gamma \sqsubseteq g$)

Then follows

- $\forall m \in M : g(m) \sqsubseteq m \Rightarrow f(\gamma(m)) \sqsubseteq \gamma(m)$
- and furthermore $\mathit{lfp}(f) \sqsubseteq \gamma(\mathit{lfp}(g))$ and $\alpha(\mathit{lfp}(f)) \sqsubseteq \mathit{lfp}(g)$

Inducing along the Abstraction Function

Fixed Points - Correctness

Proof

Show $\forall m \in M : g(m) \sqsubseteq m \Rightarrow f(\gamma(m)) \sqsubseteq \gamma(m)$

$$\begin{aligned} & g(m) \sqsubseteq m \wedge \alpha(f(\gamma(m))) \sqsubseteq g(m) \\ \Rightarrow\ & \alpha(f(\gamma(m))) \sqsubseteq m \\ \Rightarrow\ & f(\gamma(m)) \sqsubseteq \gamma(m) \end{aligned}$$

$\blacksquare$

Inducing along the Abstraction Function

Fixed Points - Correctness

Proof cont'd

From the previous result follows $\{\gamma(m) \mid g(m) \sqsubseteq m\} \subseteq \{l \mid f(l) \sqsubseteq l\}$ and hence (using Lemma 4.22)

$$\gamma\left(\bigsqcap\{m \mid g(m) \sqsubseteq m\}\right) = \bigsqcap\{\gamma(m) \mid g(m) \sqsubseteq m\} \sqsupseteq \bigsqcap\{l \mid f(l) \sqsubseteq l\}$$

Using Tarski's theorem and that a Galois connection is an adjunction:

$$\begin{aligned}
&\gamma(\bigsqcap\{m \mid g(m) \sqsubseteq m\}) \sqsupseteq \bigsqcap\{l \mid f(l) \sqsubseteq l\} \\
&\Rightarrow \gamma(Red(g)) \sqsupseteq Red(f) \\
&\Rightarrow lfp(f) \sqsubseteq \gamma(lfp(g)) \\
&\Rightarrow \alpha(lfp(f)) \sqsubseteq lfp(g)
\end{aligned}$$

Inducing along the Abstraction Function

Application to Data Flow Analysis

Generalized Monotone Framework A

- complete lattice L
- finite flow $F \subseteq \mathbf{Lab} \times \mathbf{Lab}$
- finite set of extremal labels $E \subseteq \mathbf{Lab}$
- extremal value $i \in L$
- a mapping f from the labels of F and E to monotone transfer functions $L \to L$
- Constraints $A^{\sqsupseteq}$

$$A_\circ(l) \;\sqsupseteq\; \bigsqcup\{A_\bullet(l') \mid (l',l) \in F\} \sqcup i_E^l \text{ where } i_E^l = \begin{cases} i & l \in E \\ \bot & l \notin E \end{cases}$$

$$A_\bullet(l) \;\sqsupseteq\; f_l(A_\circ(l))$$

Inducing along the Abstraction Function

Application to Data Flow Analysis

Generalized Monotone Framework A

- $(A_\circ, A_\bullet) \models A^\sqsupseteq$ whenever $A_\circ, A_\bullet$ is a solution to the constraints $A^\sqsupseteq$
- consider the associated monotone function $\vec{f}(A_\circ, A_\bullet) = (\lambda l.A_\circ(l)\ ,\ \lambda l.A_\bullet(l))$
- $(A_\circ, A_\bullet) \sqsupseteq \vec{f}(A_\circ, A_\bullet)$ is equivalent to $(A_\circ, A_\bullet) \models A^\sqsupseteq$

Inducing along the Abstraction Function

Application to Data Flow Analysis

Generalized Monotone Framework B

- let (L, α, γ, M) be a Galois Connection
- B is as A, but has
  - the mapping g from labels of F and E to monotone transfer functions $M \to M$, that satisfies $g_l \sqsupseteq \alpha \circ f_l \circ \gamma$
  - the extremal value $j \sqsupseteq \alpha(i)$
- As in A we get the constraints $B^{\sqsupseteq}$ for B and the associated monotone function $\vec{g}$

Fact

$$(B_\circ, B_\bullet) \models B^{\sqsupseteq} \implies (\gamma \circ B_\circ, \gamma \circ B_\bullet) \models A^{\sqsupseteq}$$

Inducing along the Abstraction Function

A Worked Example

Sets of States Analysis SS

- complete lattice $(\mathscr{P}(\textbf{State}), \subseteq)$
- flow $F = \mathit{flow}(S_*)$
- set $E = \{\mathit{init}(S_*)\}$ of extremal labels
- extremal value $i = \textbf{State}$
- transfer functions given by $f_\cdot^{SS}$:

$$f_l^{SS}(\Sigma) = \begin{cases} \{\sigma[x \mapsto \mathscr{A}[\![a]\!]\sigma] \mid \sigma \in \Sigma\} & \text{if } [x := a]^l \text{ is in } S_* \\ \Sigma & \text{if } [\mathit{skip}]^l \text{ is in } S_* \\ \Sigma & \text{if } [b]^l \text{ is in } S_* \end{cases}$$

where $\Sigma \subseteq \textbf{State}$

Inducing along the Abstraction Function

A Worked Example

Fact

The *SS* analysis is correct

Inducing along the Abstraction Function

A Worked Example

Constant Propagation Analysis

- complete lattice $\mathbf{State_{CP}} = ((\mathbf{Var} \to \mathbf{Z}^{\top})_{\perp}, \sqsubseteq)$
- flow $F = \mathit{flow}(S_*)$
- extremal labels $E = \{\mathit{init}(S_*)\}$
- extremal value $i = \lambda x.\top$
- transfer functions of the constant propagation analysis [1] given by $f_{\cdot}^{CP}$

[1] Principles of Program Analysis, page 71, Table 2.7

Inducing along the Abstraction Function

A Worked Example

The relationship between the two analyses is established by the representation function

$$\beta_{CP} : \mathbf{State} \to \mathbf{\widehat{State}_{CP}}$$
$$\beta_{CP}(\sigma) = \sigma$$

Galois Connection

β_{CP} gives rise to a Galois connection $(\mathscr{P}(\mathbf{State}), \alpha_{CP}, \gamma_{CP}, \mathbf{\widehat{State}_{CP}})$

$$\alpha_{CP}(\Sigma) = \bigsqcup\{\beta_{CP}(\sigma) \mid \sigma \in \Sigma\}$$
$$\gamma_{CP}(\hat{\sigma}) = \{\sigma \mid \beta_{CP}(\sigma) \sqsubseteq \hat{\sigma}\}$$

Inducing along the Abstraction Function

A Worked Example

Conclusion

one can now show

$$\forall l \in \mathbf{Lab} : f_l^{CP} \sqsupseteq \alpha_{CP} \circ f_l^{SS} \circ \gamma_{CP}$$
$$\gamma_{CP}(\lambda x.\top) = \mathbf{State}$$

and hence *CP* is an upper approximation to the analysis induced from *SS* by the Galois connection and therefore correct.

Inducing along the Concretisation Function

Why?

Inducing by abstraction function has a critical disadvantage. It lose precision along the analysis.

Inducing by Concretisation Function

instead of replacing the analysis using L with analysis using M;

- We perform normally on L (to not lose precision).
- but we only use M to approximate the fixed point computations done in L (to ensure convergence of the fixed points).

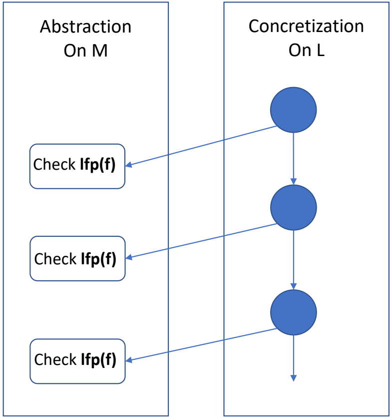
Inducing by Concretisation Function

Inducing by Concretisation Function

Using widening operator $\nabla_M : M \times M \to M$

- to define $\nabla_L : L \times L \to L$
  by using the formula $l_1 \nabla_L l_2 = \gamma(\alpha(l_1) \nabla_M \alpha(l_2))$
- we can approximate $\mathbf{lfp}(\mathbf{f})$ over L.

Concretisation process



Inducing along the concretization function

Widening Operator

Why Widening Operator?

- We can’t guarantee reaching stability eventually.
- or reaching least upper bound that equals **lfp(f)**.

Widening Operator

- used to obtain approximations of the least fixed points.
- used to limit the number of computation steps needed.

lemma 4.45

If $(\mathbf{L}, \alpha, \gamma, \mathbf{M})$ is a Galois insertion such that $\gamma(\perp_\mathbf{M}) = \perp_\mathbf{L}$ and if $\nabla_\mathbf{M} : \mathbf{M} \times \mathbf{M} \to \mathbf{M}$ is a widening operator.

Then $\nabla_\mathbf{L} : \mathbf{L} \times \mathbf{L} \to \mathbf{L}$ is a widening operator defined by the formula $\mathbf{l_1} \nabla_\mathbf{L} \mathbf{l_2} = \gamma(\alpha(\mathbf{l_1} \nabla_\mathbf{M} \alpha(\mathbf{l_2}))$.

this satisfies $\mathbf{lfp}_{\nabla_\mathbf{L}}(\mathbf{f}) = \gamma(\mathbf{lfp}_{\nabla_\mathbf{M}}(\alpha \circ \mathbf{f} \circ \gamma))$ for all monotone functions $\mathbf{f} : \mathbf{L} \to \mathbf{L}$.

Proof

- given $\nabla_\mathbf{L}$ is a widening operator, $\exists n_f \geq 0, \mathbf{lfp}_{\nabla_\mathbf{L}}(\mathbf{f}) = \mathbf{f}^{\mathbf{n_f}}_{\nabla_\mathbf{L}} = \mathbf{f}^{\mathbf{n}}_{\nabla_\mathbf{L}}$
- given $\nabla_\mathbf{M}$ is a widening operator, $\exists n_g \geq 0, \mathbf{lfp}_{\nabla_\mathbf{M}}(\mathbf{g}) = \mathbf{g}^{\mathbf{n_g}}_{\nabla_\mathbf{M}} = \mathbf{g}^{\mathbf{n}}_{\nabla_\mathbf{M}}$
- if we can prove that: $\mathbf{f}^{\mathbf{n}}_{\nabla_\mathbf{L}} = \gamma(\mathbf{g}^{\mathbf{n}}_{\nabla_\mathbf{M}})$
- we can obtain that: $\mathbf{lfp}_{\nabla_\mathbf{L}}(\mathbf{f}) = \gamma(\mathbf{lfp}_{\nabla_\mathbf{M}}(\mathbf{g}))$

The Proof

by induction on **n:**

- base case: $n = 0$.

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Rightarrow \alpha(f(f^n_{\nabla_L})) \sqsubseteq \alpha(f^n_{\nabla_L})$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Rightarrow \alpha(f(f^n_{\nabla_L})) \sqsubseteq \alpha(f^n_{\nabla_L})$

  $\Rightarrow \alpha(f(\gamma(g^n_{\nabla_M}))) \sqsubseteq \alpha(\gamma(g^n_{\nabla_M}))$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $$\begin{aligned} f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} &\Rightarrow \alpha(f(f^n_{\nabla_L})) \sqsubseteq \alpha(f^n_{\nabla_L}) \\ &\Rightarrow \alpha(f(\gamma(g^n_{\nabla_M}))) \sqsubseteq \alpha(\gamma(g^n_{\nabla_M})) \\ &\Rightarrow g(g^n_{\nabla_M}) \sqsubseteq \alpha(\gamma(g^n_{\nabla_M})) \end{aligned}$$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $$\begin{aligned} f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} &\Rightarrow \alpha(f(f^n_{\nabla_L})) \sqsubseteq \alpha(f^n_{\nabla_L}) \\ &\Rightarrow \alpha(f(\gamma(g^n_{\nabla_M}))) \sqsubseteq \alpha(\gamma(g^n_{\nabla_M})) \\ &\Rightarrow g(g^n_{\nabla_M}) \sqsubseteq \alpha(\gamma(g^n_{\nabla_M})) \\ &\Rightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M} \end{aligned}$$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M} \Rightarrow \gamma(g(g^n_{\nabla_M})) \sqsubseteq \gamma(g^n_{\nabla_M})$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M} \Rightarrow \gamma(g(g^n_{\nabla_M})) \sqsubseteq \gamma(g^n_{\nabla_M})$

  $\Rightarrow \gamma(\alpha(f(\gamma(g^n_{\nabla_M})))) \sqsubseteq \gamma(g^n_{\nabla_M})$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $$f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$$

  $$\begin{aligned} g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M} &\Rightarrow \gamma(g(g^n_{\nabla_M})) \sqsubseteq \gamma(g^n_{\nabla_M}) \\ &\Rightarrow \gamma(\alpha(f(\gamma(g^n_{\nabla_M})))) \sqsubseteq \gamma(g^n_{\nabla_M}) \\ &\Rightarrow \gamma(\alpha(f(f^n_{\nabla_L}))) \sqsubseteq f^n_{\nabla_L} \end{aligned}$$

The Proof

by induction on **n:**

- base case: n = 0.

  $f^0_{\nabla_L} = \perp_L$ and $g^0_{\nabla_M} = \perp_M$

  assume $\perp_L = \gamma(\perp_M)$

  $\Rightarrow f^0_{\nabla_L} = \gamma(g^0_{\nabla_M})$

- for induction step over n.

  $f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \Leftrightarrow g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M}$

  $$\begin{aligned} g(g^n_{\nabla_M}) \sqsubseteq g^n_{\nabla_M} &\Rightarrow \gamma(g(g^n_{\nabla_M})) \sqsubseteq \gamma(g^n_{\nabla_M}) \\ &\Rightarrow \gamma(\alpha(f(\gamma(g^n_{\nabla_M})))) \sqsubseteq \gamma(g^n_{\nabla_M}) \\ &\Rightarrow \gamma(\alpha(f(f^n_{\nabla_L}))) \sqsubseteq f^n_{\nabla_L} \\ &\Rightarrow f(f^n_{\nabla_L}) \sqsubseteq f^n_{\nabla_L} \end{aligned}$$

The Proof

- induction step: $n > 0$.

The Proof

- induction step: n > 0.

$$f^n_{\nabla_L} = \begin{cases} f^{n-1}_{\nabla_L} & \text{if } f(f^{n-1}_{\nabla_L}) \sqsubseteq f^{n-1}_{\nabla_L} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \text{otherwise} \end{cases}$$

The Proof

- induction step: n > 0.

$$f^{n}_{\nabla_L} = \begin{cases} f^{n-1}_{\nabla_L} & \textit{if} \;\; f(f^{n-1}_{\nabla_L}) \sqsubseteq f^{n-1}_{\nabla_L} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \textit{otherwise} \end{cases}$$

$$= \begin{cases} f^{n-1}_{\nabla_L} & \textit{if} \;\; g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \textit{otherwise} \end{cases}$$

The Proof

- induction step: n > 0.

$$f^{n}_{\nabla_L} = \begin{cases} f^{n-1}_{\nabla_L} & \text{if } f(f^{n-1}_{\nabla_L}) \sqsubseteq f^{n-1}_{\nabla_L} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \text{otherwise} \end{cases}$$

$$= \begin{cases} f^{n-1}_{\nabla_L} & \text{if } g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \text{otherwise} \end{cases}$$

$$= \begin{cases} \gamma(g^{n-1}_{\nabla_M}) & \text{if } g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ \gamma(\alpha\boldsymbol{(}\gamma(g^{n-1}_{\nabla_M}) \nabla_M f(\gamma(g^{n-1}_{\nabla_M}))\boldsymbol{)}) & \text{otherwise} \end{cases}$$

The Proof

- induction step: n > 0.

$$f^n_{\nabla_L} = \begin{cases} f^{n-1}_{\nabla_L} & \text{if } f(f^{n-1}_{\nabla_L}) \sqsubseteq f^{n-1}_{\nabla_L} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \text{otherwise} \end{cases}$$

$$= \begin{cases} f^{n-1}_{\nabla_L} & \text{if } g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \text{otherwise} \end{cases}$$

$$= \begin{cases} \gamma(g^{n-1}_{\nabla_M}) & \text{if } g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ \gamma(\alpha(\gamma(g^{n-1}_{\nabla_M}) \nabla_M f(\gamma(g^{n-1}_{\nabla_M})))) & \text{otherwise} \end{cases}$$

$$= \gamma\left(\begin{cases} (g^{n-1}_{\nabla_M}) & \text{if } g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ g^{n-1}_{\nabla_M} \nabla_M g(g^{n-1}_{\nabla_M}) & \text{otherwise} \end{cases} \right)$$

The Proof

- induction step: n > 0.

$$f^n_{\nabla_L} = \begin{cases} f^{n-1}_{\nabla_L} & \textit{if} \;\; f(f^{n-1}_{\nabla_L}) \sqsubseteq f^{n-1}_{\nabla_L} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \textit{otherwise} \end{cases}$$

$$= \begin{cases} f^{n-1}_{\nabla_L} & \textit{if} \;\; g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ f^{n-1}_{\nabla_L} \nabla_L f(f^{n-1}_{\nabla_L}) & \textit{otherwise} \end{cases}$$

$$= \begin{cases} \gamma(g^{n-1}_{\nabla_M}) & \textit{if} \;\; g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ \gamma(\alpha\boldsymbol{(}\gamma(g^{n-1}_{\nabla_M}) \nabla_M f(\gamma(g^{n-1}_{\nabla_M}))\boldsymbol{)}) & \textit{otherwise} \end{cases}$$

$$= \gamma\left(\begin{cases} (g^{n-1}_{\nabla_M}) & \textit{if} \;\; g(g^{n-1}_{\nabla_M}) \sqsubseteq g^{n-1}_{\nabla_M} \\ g^{n-1}_{\nabla_M} \nabla_M g(g^{n-1}_{\nabla_M}) & \textit{otherwise} \end{cases} \right)$$

$$= \gamma(g^n_{\nabla_M})$$

Proof

- given $\nabla_{\mathbf{L}}$ is a widening operator, $\exists n_f \geq 0, \mathbf{lfp}_{\nabla_{\mathbf{L}}}(\mathbf{f}) = \mathbf{f}_{\nabla_{\mathbf{L}}}^{\mathbf{n_f}} = \mathbf{f}_{\nabla_{\mathbf{L}}}^{\mathbf{n}}$
- given $\nabla_{\mathbf{M}}$ is a widening operator, $\exists n_g \geq 0, \mathbf{lfp}_{\nabla_{\mathbf{M}}}(\mathbf{g}) = \mathbf{g}_{\nabla_{\mathbf{M}}}^{\mathbf{n_g}} = \mathbf{g}_{\nabla_{\mathbf{M}}}^{\mathbf{n}}$
- We have proven that: $\mathbf{f}_{\nabla_{\mathbf{L}}}^{\mathbf{n}} = \gamma(\mathbf{g}_{\nabla_{\mathbf{M}}}^{\mathbf{n}})$
- which prove that: $\mathbf{lfp}_{\nabla_{\mathbf{L}}}(\mathbf{f}) = \gamma(\mathbf{lfp}_{\nabla_{\mathbf{M}}}(\mathbf{g}))$

So, we can perform our analysis over **L** without lossing precision.

Thank you for your attention!

Fabian Schaub
Kamal Zakieldin