VMCAI 2015

Abstracting Induction by Extrapolation and Interpolation

Mumbai, India January 12th, 2015

Patrick Cousot

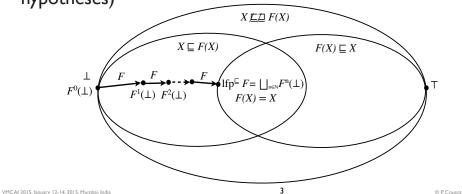
pcousot@cs.nyu.edu cs.nyu.edu/~pcousot

VMCAI 2015, January 12-14, 2015, Mumbai, India

© P. Cousot

Fixpoints

- Poset (or pre-order) < D, ⊑, ⊥, ⊥>
- Transformer: $F \in D \mapsto D$
- Least fixpoint: Ifp $F = \bigsqcup_{n \in \mathbb{N}} F^n(\bot)$ (under appropriate hypotheses)



Abstract Interpreters

- Transitional abstract interpreters: proceed by induction on program steps
- Structural abstract interpreters: proceed by induction on the program syntax
- Common main problem: over/under-approximate fixpoints in non-Noetherian^(*) abstract domains ^(**)

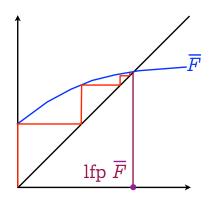
(*) Iterative fixpoint computations may not converge in finitely many steps (**) Or convergence may be guaranteed but to slow.

VMCAI 2015, January 12-14, 2015, Mumbai, India

2

© P. Cousot

Convergence acceleration with widening

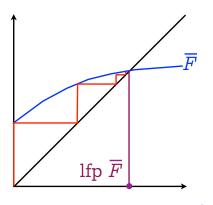


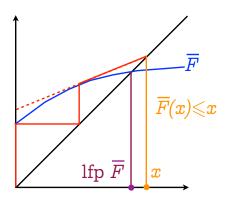
Infinite iteration

VMCAI 2015, January 12-14, 2015, Mumbai, India

© P. Cousot

Convergence acceleration with widening





Infinite iteration

Accelerated iteration with widening

(e.g. with a widening based on the derivative as in Newton-Raphson method(*))

(*) Javier Esparza, Stefan Kiefer, Michael Luttenberger: Newtonian program analysis. J. ACM 57(6): 33 (2010)

VMCAI 2015, January 12-14, 2015, Mumbai, India **5** © P.

Extrapolation by Widening

• $X^0 = \bot$ (increasing iterates with widening)

$$X^{n+1} = X^n \nabla F(X^n)$$
 when $F(X^n) \not\subseteq X^n$

$$X^{n+1} = X^n$$
 when $F(X^n) \subseteq X^n$

Widening ∇:

 \bullet $Y \sqsubseteq X \nabla Y$

(extrapolation)

• Enforces convergence of increasing iterates with widening (to a limit X*)

VMCAI 2015, January 12-14, 2015, Mumbai, India 6 © P. Cousot

The oldest widenings

• Primitive widening [1,2]

$$[a_1, b_1] \overline{V} [a_2, b_2] =$$

$$[\underline{if} a_2 < a_1 \underline{then} -\infty \underline{else} a_1 \underline{fi},$$

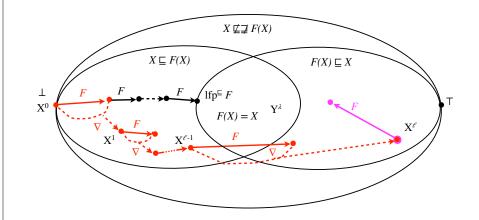
$$\underline{if} b_2 > b_1 \underline{then} +\infty \underline{else} b_1 \underline{fi}]$$

Widening with thresholds [3]

$$\begin{aligned} \forall x \in \bar{L}_2, \pm \nabla_2(j) & x = x \nabla_2(j) \pm x \\ [l_1, u_1] \nabla_2(j) & [l_2, u_2] \\ &= [if \ 0 \leq l_2 < l_1 \ then \ 0 \ elsif \ l_2 < l_1 \ then \ -b - 1 \ else \ l_1 \ fi, \\ & if \ u_1 < u_2 \leq 0 \ then \ 0 \ elsif \ u_1 < u_2 \ then \ b \ else \ u_1 \ fi] \end{aligned}$$

[1] Patrick Cousot, Radhia Cousot: Vérification statique de la cohérence dynamique des programmes, Rapport du contrat IRIA-SESORI No 75-032, 23 septembre 1975. [2] Patrick Cousot, Radhia Cousot: Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. POPL 1977: 238-252 [3] Patrick Cousot, Semantic foundations of program analysis, Ch. 10 of Program flow analysis: theory and practice, N. Jones & S., Muchnich (eds.), Prentice Hall, 1981.

Extrapolation with widening



VMCAI 2015. Ianuary 12-14. 2015. Mumbai, India 8 © P. Cousot

Interpolation with narrowing

• $Y^0 = X^{\ell}$ (decreasing iterates with narrowing)

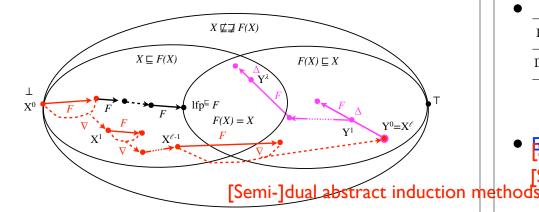
$$Y^{n+1} = Y^n \triangle F(Y^n)$$
 when $F(Y^n) \sqsubset Y^n$

$$Y^{n+1} = Y^n$$
 when $F(Y^n) = Y^n$

- Narrowing Δ :
 - $\bullet \ \ Y \sqsubseteq X \implies Y \sqsubseteq X \ \Delta \ Y \sqsubseteq X$ (interpolation)
 - Enforces convergence of decreasing iterates with narrowing (to a limit Y^{λ})

VMCAI 2015, January 12-14, 2015, Mumbai, India

Interpolation with narrowing



Could stop when $F(X) \not\subseteq X \land F(F(X)) \subseteq F(X)$ but not the current practice.

VMCAI 2015, January 12-14, 2015, Mumbai, India

The oldest narrowing

• [2]

$$\begin{bmatrix} a_1,b_1 \end{bmatrix} \bar{\Delta} \begin{bmatrix} a_2,b_2 \end{bmatrix} =$$

$$\begin{bmatrix} \underline{if} \ a_1 = -\infty \ \underline{then} \ a_2 \ \underline{else} \ MIN \ (a_1,a_2), \\ \underline{if} \ b_1 = +\infty \ \underline{then} \ b_2 \ \underline{else} \ MAX \ (b_1,b_2) \end{bmatrix}$$

[2] Patrick Cousot, Radhia Cousot: Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. POPL 1977: 238-252
VMCAI 2015, January 12-14, 2015, Mumbai, India

© P. Cousot

[Semi-]dual abstract inductifsemie]dualsabstract induetion in place [Semi-]dual abstract induction methods-]dual abstract induction methods-]dual abstract induction methods [Semi-]dual abstract induction methods widenabstract induction methods widenabstract induction methods between his labstract induction methods between hi

•		Convergence above the limit	Convergence below the limit
	Increasing iteration	Widening ∇	Dual-narrowing \(\widetilde{\Delta} \)
	Decreasing iteration	Narrowing △	Dual widening $\widetilde{\overline{V}}$ a narrowing
			• • • • • • • • • • • • • • • • • • • •

Extrapolators $(\nabla, \widetilde{\nabla})$ and interpolators $(\Delta, \widetilde{\Delta})$

• Semi-Idual abstract induction methods
[Semi-Idual abstract induction methods

• Abstr<mark>tetanapet</mark>

• a narrowi

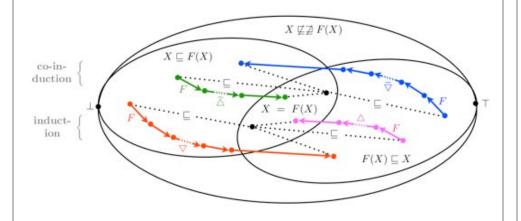
Example

[Semi-]dual abstract induction methodstrade induction and strade induction methods and strade induction are the companied which is the companied with the companied which is the companied with th

widening/narrowing/duals can be structurening of the wing duals can be structurening of the wing duals can be structurening of the wing duals can be structurently duals can be structurently duals can be structurently duals and the wing duals contained to the wing duals contained to the wing duals and the wing duals contained to the wing duals and the wing duals contained to the wing duals and the wing duals contained to the wing duals and the wing duals are an another wing duals and the wing duals and the wing duals are an another wing duals and the wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals and the wing duals are an another wing duals are another wing duals are an another wing duals are an another wing du

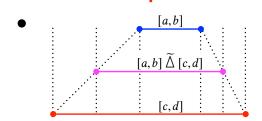
E.g. widening with thresholds is at 50 E.g. widening wan intesholds in adults car E.g. widening with diserted to best widening). It is alleging with diserted to be to be standard or the standard of the sta

Extrapolators, Interpolators, and Duals



VMCAI 2015, January 12-14, 2015, Mumbai, India 13

Example of dual-narrowing



- $\bullet \qquad [a,b] \widetilde{\Delta} [c,d] \triangleq [(c = -\infty \ \widehat{s} \ a \ \epsilon \ \lfloor (a+c)/2 \rfloor), (d = \infty \ \widehat{s} \ b \ \epsilon \ \lceil (b+d)/2 \rceil)]$
- The first method we tried in the late 70's with Radhia
 - Slow
 - Does not easily generalize (e.g. to polyhedra)

Interpolation with dual narrowing

• $Z^0 = \bot$ (increasing iterates with dual-narrowing)

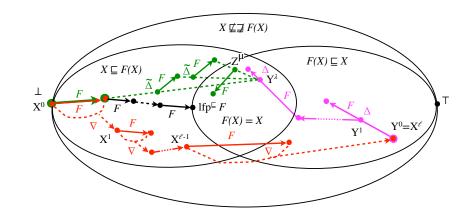
$$Z^{n+1} = F(Z^n) \tilde{\Delta} Y^{\lambda}$$
 when $F(Z^n) \not\sqsubseteq Z^n$

$$Z^{n+1} = Z^n$$
 when $F(Z^n) \sqsubseteq Z^n$

- Dual-narrowing $\tilde{\Delta}$:
 - $X \sqsubseteq Y \implies X \sqsubseteq X \tilde{\Delta} Y \sqsubseteq Y$ (interpolation)
 - Enforces convergence of increasing iterates with dual-narrowing

VMCAI 2015, January 12-14, 2015, Mumbai, India 14 © P. Cousot

Interpolation with dual-narrowing



VMCAI 2015, January 12-14, 2015, Mumbai, India 16 © P. Cousot

© P. Cousot

Relationship between narrowing and dual-narrowing

$$\bullet \quad \widetilde{\Delta} = \Delta^{-1}$$

$$\bullet \ Y \sqsubseteq X \implies Y \sqsubseteq X \ \Delta \ Y \sqsubseteq X$$

(narrowing)

 $\bullet \ Y \sqsubseteq X \implies Y \sqsubseteq Y \widetilde{\Delta} \ X \sqsubseteq X$

(dual-narrowing)

- Example: Craig interpolation
- Why not use a bounded widening (bounded by B)?
 - $F(X) \sqsubseteq B \Longrightarrow F(X) \sqsubseteq F(X) \widetilde{\Delta} B \sqsubseteq B$ (dual-narrowing)
 - $\bullet \ \ X \sqsubseteq F(X) \sqsubseteq B \Longrightarrow F(X) \sqsubseteq X \ \nabla_B \ F(X) \sqsubseteq B$

(bounded widening)

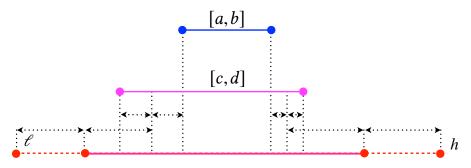
VMCAI 2015, January 12-14, 2015, Mumbai, India

17

© P. Cousot

Example of widenings (cont'd)

• Bounded widening (in $[\ell, h]$):



$$[a,b] \nabla_{[\ell,h]} [c,d] \triangleq [\underbrace{c+a-2\ell}_{2}, \underbrace{b+d+2h}_{2}]$$

VMCAI 2015, January 12-14, 2015, Mumbai, India

18

© P. Cousot

More in the paper...

Widenings

VMCAI 2015. Ianuary 12-14. 2015. Mumbai. India

VMCAI 2015, January 12-14, 2015, Mumbai, India

© P. Cousot

Widenings are not increasing

A well-known fact

 $[1,1] \subseteq [1,2]$ but $[1,1]\nabla[1,2]=[1,\infty]\subseteq [1,2]\nabla[1,2]=[1,2]$

- A widening cannot both:
 - Be increasing in its first parameter
 - Enforce termination of the iterates
 - Avoid useless over-approximations as soon as a solution is found^(*)

 $^{(*)}\, \mbox{A}$ counter-example is $\ x \ \nabla \ y = \top$

VMCAI 2015, January 12-14, 2015, Mumbai, India

21

@ P. Couso

Soundness

- In the paper, the fixpoint approximation soundness theorems are expressed with minimalist hypotheses:
 - No need for complete lattices, complete partial orders (CPO's):
 - The concrete domain is a poset
 - The abstract domain is a pre-order
 - The concretization is defined for the abstract iterates only.

Soundness

VMCAI 2015, January 12-14, 2015, Mumbai, India

22

@ P Couset

Soundness (cont'd)

- No need for increasingness/monotony hypotheses for fixpoint theorems (Tarski, Kleene, etc)
 - The concrete transformer is increasing and the limit of the iterations does exist in the concrete domain
 - No hypotheses on the abstract transformer (no need for fixpoints in the abstract)
 - Soundness hypotheses on the extrapolators/ interpolators with respect to the concrete
- In addition, termination hypotheses on the extrapolators/interpolators ensure convergence in finitely many steps

VMCAI 2015, January 12-14, 2015, Mumbai, India 23 © P. Cousot VMCAI 2015, January 12-14, 2015, Mumbai, India 24 © P. Cousot

Soundness (cont'd)

- No need for increasingness/monotony hypotheses for fixpoint theorems (Tarski, Kleene, etc)
 - The concrete transformer is increasing and the limit of the iterations does exist in the concrete domain
 - No hypotheses on the abstract transformer (no need for fixpoints in the abstract)
 - Soundness hypotheses on the extrapolators/ interpolators with respect to the concrete

Examples of interpolators

VMCAI 2015, January 12-14, 2015, Mumbai, India 25 © P. Cousot

Craig interpolation

Craig interpolation:

Given $P \Longrightarrow Q$ find I such that $P \Longrightarrow I \Longrightarrow Q$ with $var(I) \subseteq var(P) \cap var(Q)$

is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)

VMCAI 2015, January 12-14, 2015, Mumbai, India **26** © P. Cousot

Craig interpolation

• Craig interpolation:

Given $P \Longrightarrow Q$ find I such that $P \Longrightarrow I \Longrightarrow Q$ with $var(I) \subseteq var(P) \cap var(Q)$

is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)

 This evidence looked very controversial to some reviewers

VMCAI 2015, January 12-14, 2015, Mumbai, India 27 © P. Cousot VMCAI 2015, January 12-14, 2015, Mumbai, India 28 © P. Cousot

Craig interpolation

• Craig interpolation:

Given $P \Longrightarrow Q$ find I such that $P \Longrightarrow I \Longrightarrow Q$ with $var(I) \subseteq var(P) \cap var(Q)$

is a dual narrowing (already observed by Vijay D'Silva and Leopold Haller as an inversed narrowing)

- This evidence looked very controversial to some reviewers
- The generalization of an idea does not diminish in any way the merits and originality of this idea

VMCAI 2015, January 12-14, 2015, Mumbai, India

29

© P. Cousot

Conclusion

VMCAI 2015, January 12-14, 2015, Mumbai, India

© P. Cousot

Conclusion

- Abstract interpretation in infinite domains is traditionally by iteration with widening/narrowing.
- We have shown how to use iteration with dualnarrowing (alone or after widening/narrowing).
- These ideas of the 70's generalize Craig interpolation from logic to arbitrary abstract domains.

The End, Thank You

VMCAI 2015, January 12-14, 2015, Mumbai, India 31 © P. Cousot VMCAI 2015, January 12-14, 2015, Mumbai, India 32 © P. Cousot