

Comparing and Combining Widening Operators

Agostino Cortesi

Dipartimento di Informatica
Università Ca' Foscari
Venezia, Italy

Introduction

Motivations

Aim of this work

Widening Operators

Basic Definitions

Set- and Pair-Widenings

Comparing Set-Widening and Pair-Widening

Pair Widening and Cartesian Product

Strong Pair-Widening Operators

Widening Operators and Galois Insertions

Deriving Abstractions

Pair-Widening and Abstraction

Pair-Widening and Reduced Product

Conclusions

Conclusions and Future Work

Abstract Interpretation

Abstract Interpretation is a general theory of approximation of mathematical structures, in particular those involved in the semantic models of computer systems, that has been successfully applied for the static analysis of software systems.

It is based on two main key-concepts:

- the correspondence between concrete and abstract semantics through Galois connections/insertions, and
- the feasibility of a fixed point computation of the abstract semantics, through the fast convergence of widening operators.

Something is still missing

- ▶ Galois connections have been widely studied, yielding to a suite of general techniques to manage the combination of abstract domains, e.g. different kind of products, and more sophisticated notions like the quotient, the complement, and the powerset of abstract domains.
- ▶ Not much attention has been given to provide general results about widening operators, even though they play a crucial role in particular when infinite abstract domains are considered.
- ▶ This is mainly due to the fact that the definition of widening provides extremely weak algebraic properties, while it is extremely demanding with respect to convergence and termination.

Aim of the work

- ▶ We investigate which properties are necessary to support a systematic design of widening operators, by discussing and comparing different definitions in the literature, and by proposing various ways to combine them.
- ▶ In particular, we prove that, for Galois insertions, widening is preserved by abstraction, and we show how widening operators can be combined for the cartesian and reduced product of abstract domains.

Partial Orders and Posets

Definition (partial order)

If P is a non-empty set, then by a *partial order* on P we mean a binary relation \leq on P which is reflexive, anti-symmetric, and transitive.

Definition (poset)

By a *poset* (P, \leq) we shall mean a set P on which there is defined a partial order \leq .

lub and glb

Definition (upper and lower bounds)

Let P be a poset, and let S be a subset of P .

- ▶ An element $x \in P$ is an *upper bound* of S if $s \leq x$ for all $s \in S$.
- ▶ If the set of the upper bounds of S has a least element z , then z is called the *least upper bound (lub)* of S , and will be denoted by $z = \sqcup S$.
- ▶ By duality, an element $x \in P$ is a *lower bound* of S if $x \leq s$ for all $s \in S$.
- ▶ If the set of the lower bounds of S has a maximum element z , then z is called the *greatest lower bound (glb)* of S , and will be denoted by $z = \sqcap S$.

(Complete) Lattices

Definition (lattice)

Let P be a non empty poset. If $x \sqcup y$ and $x \sqcap y$ exist for all $x, y \in P$, then P is a *lattice*.

Definition (complete lattice)

Let P be a non empty poset. If $\sqcup S$ and $\sqcap S$ exist for all $S \subseteq P$, then P is a *complete lattice*.

Galois connections/insertions

Definition (Galois connection and insertion)

Let C and D be complete lattices, and consider two functions:

$\gamma_{DC} : D \rightarrow C$ and $\alpha_{CD} : C \rightarrow D$.

- ▶ The tuple $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ is a *Galois connection* if

$$\forall c \in C \text{ and } \forall d \in D : \alpha_{CD}(c) \leq_D d \Leftrightarrow c \leq_C \gamma_{DC}(d).$$

- ▶ G_{CD} is a *Galois insertion* when γ_{DC} is injective or, equivalently, when α_{CD} is onto.

In a Galois connection or insertion G_{CD} , the functions γ_{DC} and α_{CD} are called the concretization and the abstraction function, respectively.

Properties of Galois connections/insertions

Lemma

Let C and D be complete lattices, and consider two order-preserving functions $\gamma_{DC} : D \rightarrow C$ and $\alpha_{CD} : C \rightarrow D$. Then, G_{CD} is a Galois connection if and only if

- $\gamma_{DC} \circ \alpha_{CD}$ is extensive, i.e., $\forall c \in C, c \leq_C \gamma_{DC}(\alpha_{CD}(c))$;
- $\alpha_{CD} \circ \gamma_{DC}$ is reductive, i.e., $\forall d \in D, \alpha_{CD}(\gamma_{DC}(d)) \leq_D d$;

Moreover, G_{CD} is a Galois insertion if it is a Galois connection and $\alpha_{CD} \circ \gamma_{DC}$ is the identity function.

Properties of Galois connections/insertions

Lemma

- ▶ if α_{CD} and γ_{DC} form a Galois connection/insertion, then one of the two functions determines the other one.

$$\begin{aligned}\forall d \in D, \gamma_{DC}(d) &= \sqcup_C \{c \in C \mid \alpha_{CD}(c) \sqsubseteq_D d\} \\ \forall c \in C, \alpha_{CD}(c) &= \sqcap_D \{d \in D \mid c \sqsubseteq_C \gamma_{DC}(d)\}.\end{aligned}$$

Each function is called the adjoint of the other one.

- ▶ $\alpha_{CD} \circ \gamma_{DC} \circ \alpha_{CD} = \alpha_{CD}$ and similarly, $\gamma_{DC} \circ \alpha_{CD} \circ \gamma_{DC} = \gamma_{DC}$.

The need for a widening

- ▶ In Abstract Interpretation, the collecting semantics of a program is expressed as a least fix-point of a set of equations. The equations are solved over some abstract domain that captures the property of interest to be analyzed.
- ▶ Typically, the equations are solved iteratively; that is, successive approximations of the solution is computed until a fix-point is reached. However, for many useful abstract domains, such chains can be either infinite or too long to let the analysis be efficient.
- ▶ To make use of these domains, the widening operators, predict the fix-point based on the sequence of approximations computed on earlier iterations of the analysis.

Set-Widening

Definition (set-widening)

Let (P, \leq) be a poset. A set-widening operator is a partial function $\nabla_* : \wp(P) \rightarrow P$ such that

- (i) Covering: Let S be an element of $\wp(P)$. If $\nabla_*(S)$ is defined, then $\forall x \in S, x \leq \nabla_*(S)$.
- (ii) Termination: For every increasing chain $x_0 \leq x_1 \leq \dots$, the increasing chain defined as

$$y_0 = x_0, y_i = \nabla_*({x_j \mid 0 \leq j \leq i})$$

stabilizes after a finite number of terms.

Pair-widening

Definition (pair-widening)

Let (P, \leq) be a poset. A pair-widening operator is a binary operator $\nabla : P \times P \rightarrow P$ such that

- (i) Covering: $\forall x, y \in P : x \leq x \nabla y$, and $y \leq x \nabla y$.
- (ii) Termination: For every increasing chain $x_0 \leq x_1 \leq \dots$, the increasing chain defined as

$$y_0 = x_0, y_{i+1} = y_i \nabla x_{i+1}$$

stabilizes after a finite number of terms.

Example 1

A pair-widening operator for the lattice of intervals

$L = \{\perp\} \cup \{[l, u] \mid l \in \mathbb{Z} \cup \{-\infty\}, u \in \mathbb{Z} \cup \{+\infty\}, l \leq u\}$ can be defined as:

$$\begin{aligned} \perp \nabla x &= x \\ x \nabla \perp &= x \\ [l_0, u_0] \nabla [l_1, u_1] &= \begin{cases} -\infty & \text{if } l_1 < l_0 \\ l_0 & \text{else} \end{cases} \\ &\quad \begin{cases} +\infty & \text{if } u_0 < u_1 \\ u_0 & \text{else} \end{cases} \end{aligned}$$

Observe that the operator is not commutative, as for instance

$$\begin{aligned} [2, 3] \nabla [1, 4] &= [-\infty, +\infty] \\ [1, 4] \nabla [2, 3] &= [1, 4] \end{aligned}$$

Example 1 (ctd.)

- ▶ Observe that it is not even order preserving. In fact, consider $[0, 1] \leq [0, 3]$. We have:

$$\begin{aligned} [0, 1] \nabla [0, 2] &= [0 + \infty] \\ [0, 3] \nabla [0, 2] &= [0, 3]. \end{aligned}$$

and of course $[0, 3]$ is not smaller or equal to $[0, +\infty]$.

- ▶ Observe that associativity does not hold either:

$$\begin{aligned} [0, 2] \nabla ([0, 1] \nabla [0, 2]) &= [0 + \infty] \\ ([0, 2] \nabla [0, 1]) \nabla [0, 2] &= [0, 2]. \end{aligned}$$

Example 2

The pair widening of Example 1 is a reflexive operator. This is not the case in general, as you can see by considering another widening operator on the same lattice of Intervals.

Let k be a fixed positive integer constant:

$$\begin{aligned} \perp \nabla_k x &= x \\ x \nabla_k \perp &= x \\ [l_0, u_0] \nabla_k [l_1, u_1] &= [\min(l_0, l_1) \text{ if } \min(l_0, l_1) > -k, \text{ else } -\infty \\ &\quad \max(u_0, u_1) \text{ if } \max(u_0, u_1) < k, \text{ else } +\infty] \end{aligned}$$

Observe that for all k , ∇_k is commutative, associative, and order-preserving. However, it is not reflexive. For instance, if $k = 7$ we get:

$$[-8, 4] \nabla [-8, 4] = [-\infty, 4]$$

Set-widening from pair-widening

Lemma

Let (P, \leq) be a poset, and let $\nabla : P \times P \rightarrow P$ be a pair-widening operator on P . Define $\nabla_* : \wp(P) \rightarrow P$ such that:

- $\text{dom}(\nabla_*) = R_1 \cup R_2$, where

$$R_1 = \{\{x, y\} \mid x, y \in P\}, \text{ and}$$

$$R_2 = \{S \subseteq P \mid S \text{ is a finite ascending chain}\}.$$

- $\forall \{x, y\} \in R_1$,

$$\nabla_*(\{x, y\}) =_{\text{def}} \begin{cases} x \nabla y & \text{if } x \leq y \\ z \in \{x \nabla y, y \nabla x\} & \text{randomly, otherwise.} \end{cases}$$

- $\forall S = \{x_i \mid x_0 \leq x_1 \leq \dots \leq x_j\} \in R_2$,

$$\nabla_*(S) =_{\text{def}} (((x_0 \nabla x_1) \nabla x_2 \dots) \nabla x_j).$$

Then ∇_* is a set-widening operator.

Proof (Covering)

Let $S \subseteq P$ such that $\nabla_*(S)$ is defined. We have to show that $\forall s \in S : s \leq \nabla_*(S)$.

- ▶ Case $S \in R_1$: it follows from the definition of ∇ .
- ▶ Case $S \in R_2$: it follows by induction on the length of the ascending chain, and by the transitivity of the partial order.

Proof (Termination)

- ▶ Consider the ascending chain $x_0 \leq x_1 \leq \dots$. Consider the corresponding ascending chain $\hat{y}_0 \leq \hat{y}_1 \leq \dots$ obtained by ∇ , and the ascending chain $y_0 \leq y_1 \leq \dots$ obtained using ∇_* . We prove by induction that for each index i , $y_i = \hat{y}_i$.
- ▶ The basis is true, as $y_0 = x_0 = \hat{y}_0$.
- ▶ Consider the inductive step:

$$\begin{aligned}
 y_{i+1} &= \nabla_*(\{x_j \mid 0 \leq j \leq i+1\}) && \text{by (ii) of Def. set-w} \\
 &= (((x_0 \nabla x_1) \nabla x_2 \dots) \nabla x_{i+1}) && \text{by definition of } \nabla_* \\
 &= \nabla_*(\{x_j \mid 0 \leq j \leq i\}) \nabla x_{i+1} && \text{again by definition of } \nabla_* \\
 &= \hat{y}_i \nabla x_{i+1} && \text{by inductive hypothesis} \\
 &= \hat{y}_{i+1} && \text{by (ii) of Def. of pair-w}
 \end{aligned}$$

As the sequence $\{\hat{y}_i\}_{0 \leq i}$ stabilizes after a finite number of terms, so does $\{y_i\}_{0 \leq i}$. □

Pair-widening from set-widening

Lemma

Let (P, \leq) be a poset, and let $\nabla_* : \wp(P) \rightarrow P$ be a set-widening operator on P such that

- $\text{dom}(\nabla_*) \supseteq \{\{x, y\} \mid x, y \in P\}$, and
- $\forall S \subseteq P, \forall x \in P, \nabla_*(S \cup \{x\}) = \nabla_*({\nabla_*(S), x})$.

Then, the binary operator $\nabla : P \times P \rightarrow P$ defined by $x \nabla y = \nabla_*({\nabla_*(x, y)})$ is a pair-widening operator.

Proof

- ▶ The covering requirement follows immediately from the definition of ∇ and the covering property of ∇_* .
- ▶ Consider $x_0 \leq x_1 \leq \dots$ in P , and the increasing chain $y_0 = x_0, y_{i+1} = y_i \nabla x_i$.
- ▶ As ∇_* is a set-widening, we know that the sequence $y'_0 = x_0, y'_i = \nabla_*(\{x_j \mid 0 \leq j \leq i\})$ stabilizes finitely.
- ▶ We show by induction that for each i , $y_i = y'_i$.

Proof (ctd.)

- ▶ The basis is true, as $y_0 = x_0 = y'_0$.
- ▶ On the induction step,

$$\begin{aligned}
 y'_{i+1} &= \nabla_*(\{x_j \mid 0 \leq j \leq i + 1\}) && \text{by def. of set-w.} \\
 &= \nabla_*(\{\nabla_*(\{x_j \mid 0 \leq j \leq i\}), x_{i+1}\}) && \text{by hyp. on } \nabla_* \\
 &= \nabla_*(\{y'_i, x_{i+1}\}) && \text{by def. of set-w.} \\
 &= \nabla_*(\{y_i, x_{i+1}\}) && \text{by inductive hyp.} \\
 &= y_i \nabla x_{i+1} && \text{by def. of } \nabla \\
 &= y_{i+1} && \text{by def. of pair-w.}
 \end{aligned}$$

- ▶ As the sequence $\{y'_i\}_{i \geq 0}$ stabilizes after a finite number of terms, so does $\{y_i\}_{i \geq 0}$. □

Pair-widening and cartesian product

Theorem

Let ∇_A and ∇_D be pair-widening operators defined on the posets A and D , respectively.

The binary operator $\nabla : (A \times D) \times (A \times D) \rightarrow (A \times D)$ defined by

$$\forall \langle a, d \rangle, \langle a', d' \rangle \in A \times D : \langle a, d \rangle \nabla \langle a', d' \rangle = \langle a \nabla_A a', d \nabla_D d' \rangle$$

is a pair-widening operator.

Proof (Covering)

$$\begin{aligned}
 & a \leq a \nabla_A a' \quad \text{and} \quad d \leq d \nabla_D d' && \text{by covering of } \nabla_A, \nabla_D \\
 \Rightarrow & \langle a, d \rangle \leq \langle a \nabla_A a', d \nabla_D d' \rangle && \text{by def. of } \leq \text{ on } A \times D \\
 \Rightarrow & \langle a, d \rangle \leq \langle a, d \rangle \nabla \langle a', d' \rangle && \text{by definition of } \nabla.
 \end{aligned}$$

Proof (Termination)

Let $\langle a_0, d_0 \rangle \leq \langle a_1, d_1 \rangle \leq \dots$ be an increasing sequence in the cartesian product $A \times D$. We have to show that the sequence $\langle u_0, v_0 \rangle = \langle a_0, d_0 \rangle$, $\langle u_{i+1}, v_{i+1} \rangle = \langle u_i, v_i \rangle \nabla \langle a_i, d_i \rangle$ stabilizes after a finite number of terms.

By the termination property of ∇_A and ∇_D , both the sequence $\hat{a}_0 = a_0$, $\hat{a}_{i+1} = \hat{a}_i \nabla_A a_i$, and the sequence $\hat{d}_0 = d_0$, $\hat{d}_{i+1} = \hat{d}_i \nabla_D d_i$ stabilize finitely.

It can be easily proved by induction that for each i , $\langle u_i, v_i \rangle = \langle \hat{a}_i, \hat{d}_i \rangle$. Therefore, the sequence $\{\langle u_j, v_j \rangle\}_{j \geq 0}$ stabilizes finitely too. □

Pair-widening operators on the same poset

Lemma

Let (P, \leq) be a lattice satisfying the ascending chain property. Let ∇_1, ∇_2 be two pair-widening operators on P . Then the binary operators

$\nabla_{\sqcup} : P \times P \rightarrow P$ defined by: $\forall x, y \in P : x \nabla y = (x \nabla_1 y) \sqcup (x \nabla_2 y)$

$\nabla_{\sqcap} : P \times P \rightarrow P$ defined by: $\forall x, y \in P : x \nabla y = (x \nabla_1 y) \sqcap (x \nabla_2 y)$

are pair-widening operators.

Observe that the two operators of this Lemma are such that ∇_{\sqcup} may gain in efficiency with respect to both ∇_1 and ∇_2 , while ∇_{\sqcap} may return a more accurate result.

Strong Pair-widening

For numerical domains like polyhedra, where the abstract elements computed at each iteration of the analysis are not necessarily ordered, a stronger notion of widening is needed.

Definition (strong pair-widening)

Let (P, \leq) be a poset. A strong pair-widening operator is a binary operator $\nabla : P \times P \rightarrow P$ such that

- (i) Covering: $\forall x, y \in P : x \leq x \nabla y$, and $y \leq x \nabla y$.
- (ii) Termination: For every sequence $\{x_i\}_{i \geq 0}$, the increasing chain defined as

$$y_0 = x_0, y_{i+1} = y_i \nabla x_{i+1}$$

stabilizes after a finite number of terms.

Pair-widening vs. Strong pair-widening

Lemma

Let ∇ be a pair-widening operator on a lattice (P, \leq, \sqcup) , such that for every finite set $\{x_i\}_{0 \leq i \leq n}$ and for every $y \in P$,

$$(((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla (x_0 \sqcup x_1 \sqcup \dots \sqcup x_n \sqcup y) = (((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla y$$

then ∇ is a strong pair-widening operator.

Proof

- ▶ We need to focus only on the termination property.
- ▶ Consider the sequence $\{x_i\}_{0 \leq i \leq n}$, and the increasing sequence

$$z_0 = x_0, z_{i+1} = x_0 \sqcup \dots \sqcup x_{i+1}$$

We show by induction that the two increasing sequences $y_0 = x_0$, $y_{i+1} = y_i \nabla x_{i+1}$ and $h_0 = z_0$, $h_{i+1} = h_i \nabla z_{i+1}$ are such that $\forall i : y_i = h_i$.

- ▶ The basis is trivial, as $y_0 = x_0 = z_0 = h_0$.

Proof (ctd.)

The induction step:

$$\begin{aligned}
 h_{i+1} &= h_i \nabla z_{i+1} && \text{by def. of } \{h_j\}_{j \geq 0} \\
 &= y_i \nabla z_{i+1} && \text{by inductive hyp.} \\
 &= (((x_0 \nabla x_1) \nabla \dots) \nabla x_i) \nabla z_{i+1} && \text{by def. of } \{y_j\}_{j \geq 0} \\
 &= (((x_0 \nabla x_1) \nabla \dots) \nabla x_i) \nabla (x_0 \sqcup \dots \sqcup x_{i+1}) && \text{by def. of } \{z_j\}_{j \geq 0} \\
 &= ((x_0 \nabla x_1) \nabla \dots) \nabla x_i \nabla x_{i+1} && \text{by hyp. on } \nabla \\
 &= y_{i+1} && \text{by def. of } \{y_j\}_{j \geq 0}
 \end{aligned}$$

As the increasing sequence $\{h_j\}_{j \geq 0}$ stabilizes after a finite number of terms, so does $\{y_j\}_{j \geq 0}$. □

Strong-Widening vs. Pair-Widening (2)

Lemma

Let ∇ be an associative pair-widening operator on a lattice (P, \leq, \sqcup) , such that for $\forall x, y \in P : x \nabla y = x \nabla (x \sqcup y)$, then ∇ is a strong pair-widening operator.

Proof: By the previous Lemma, it is sufficient to prove by induction that for every finite set $\{x_i\}_{0 \leq i \leq n}$ and for every $y \in P$,

$$(((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla (x_0 \sqcup x_1 \sqcup \dots \sqcup x_n \sqcup y) =$$

$$(((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla y.$$

Proof (ctd.)

The basis ($n = 1$) follows immediately from the hypothesis.

Induction step:

$$(((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla (x_0 \sqcup x_2 \sqcup \dots \sqcup x_n \sqcup y) =$$

by inductive hypothesis

$$(((x_0 \nabla x_1) \nabla \dots) \nabla (x_0 \sqcup x_2 \sqcup \dots \sqcup x_n)) \nabla (x_0 \sqcup x_2 \sqcup \dots \sqcup x_n \sqcup y) =$$

by associativity of ∇ and of \sqcup

$$(((x_0 \nabla x_1) \nabla \dots) \nabla ((x_0 \sqcup x_2 \sqcup \dots \sqcup x_n) \nabla ((x_0 \sqcup x_2 \sqcup \dots \sqcup x_n) \sqcup y)) =$$

by applying the hypothesis

$$(((x_0 \nabla x_1) \nabla \dots) \nabla ((x_0 \sqcup x_2 \sqcup \dots \sqcup x_n) \nabla y)) =$$

by associativity of ∇

$$(((x_0 \nabla x_1) \nabla \dots) \nabla x_n) \nabla y.$$



Deriving abstractions from widening

- ▶ Widening operators have already been used in order to derive abstract domains, e.g for cofibered domains (Venet).
- ▶ The next results show how to derive Galois insertions by introducing an abstraction function built on top of a widening operator. In order to do that, additional requirements have to be assumed on the widening operator, like idempotence and order-preservation on pairs/singletons.

Deriving Abstraction from widening

Theorem

Let ∇ be a pair-widening operator on a complete lattice (L, \leq) such that:

- ▶ ∇ is idempotent
- ▶ $\forall x, y \in L : x \leq y \Rightarrow x\nabla x \leq y\nabla y$.

Let A be the set $\{x\nabla x \mid x \in L\}$.

Then $\alpha_{LA}(x) = x\nabla x$ is the lower adjoint of a Galois insertion between L and A , with the upper adjoint being the identity function.

Deriving Abstraction from Pair-Widening

It is sufficient to prove that $\forall x \in L : x \leq \gamma_{\mathcal{A}L}(\alpha_{LA}(x))$, and that $\forall a \in A : a = \alpha_{LA}(\gamma_{\mathcal{A}L}(a))$.

$$\begin{array}{ll} \forall x \in L : x \leq x \nabla x & \text{by def. of pair-w.} \\ \Rightarrow x \leq \alpha_{LA}(x) & \text{by definition of } \alpha_{LA} \\ \Rightarrow x \leq \gamma_{\mathcal{A}L}(\alpha_{LA}(x)) & \text{as } \gamma_{\mathcal{A}L} \text{ is the identity} \end{array}$$

$$\begin{array}{ll} \forall a \in A : a = a \nabla a & \text{by definition of } A \\ \Rightarrow a = (\gamma_{\mathcal{A}L}(a)) \nabla (\gamma_{\mathcal{A}L}(a)) & \text{as } \gamma_{\mathcal{A}L} \text{ is the identity} \\ \Rightarrow a = \alpha_{LA}(\gamma_{\mathcal{A}L}(a)) & \text{by definition of } \alpha_{LA} \end{array}$$



Deriving Abstraction from Set-Widening

Lemma

Let ∇_* be a set-widening operator on a complete lattice (L, \leq) such that

- ▶ $\nabla_*(\{x\})$ is defined for each x in L
- ▶ $\forall x, y \in L : x \leq y \Rightarrow \nabla_*(\{x\}) \leq \nabla_*(\{y\})$.

Let A be the set $\{\nabla_*(\{x\}) \mid x \in L\}$.

Consider the function $\alpha_{LA} : L \rightarrow A$ defined by $\alpha_{LA}(x) = \nabla_*(\{x\})$.

Then, α_{LA} is the lower adjoint of a Galois insertion between L and A , with the upper adjoint being the identity function.

Pair-widening is preserved by abstraction

Theorem

Let C and D be two complete lattices, s.t. $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ is a Galois insertion. Let ∇_C be a pair-widening on C . The binary operator ∇_D defined by

$$\forall d_1, d_2 \in D, d_1 \nabla_D d_2 = \alpha_{CD}(\gamma_{DC}(d_1) \nabla_C \gamma_{DC}(d_2))$$

is a pair-widening operator on D .

Proof (Covering)

Let us show that $\forall d_1, d_2 \in D : d_1 \leq d_1 \nabla_D d_2$.

$$\begin{array}{ll}
 \gamma_{DC}(d_1) & \leq \gamma_{DC}(d_1) \nabla_C \gamma_{DC}(d_2) & \text{by def. of pair-w.} \\
 \alpha_{CD}(\gamma_{DC}(d_1)) & \leq \alpha_{CD}(\gamma_{DC}(d_1) \nabla_C \gamma_{DC}(d_2)) & \text{by monoton. of } \alpha_{CD} \\
 \alpha_{CD}(\gamma_{DC}(d_1)) & \leq d_1 \nabla_D d_2 & \text{by def. of } \nabla_D \\
 d_1 & \leq d_1 \nabla_D d_2 & \text{by Galois insertion.}
 \end{array}$$

The same way, we can also prove that $\forall d_1, d_2 \in D : d_2 \leq d_1 \nabla_D d_2$.

Proof (Termination)

- ▶ Consider the ascending chain $d_0 \leq d_1 \leq \dots$ in D .
- ▶ Consider the corresponding ascending chain $\gamma_{DC}(d_0) \leq \gamma_{DC}(d_1) \leq \dots$ in C .
- ▶ And consider the sequence $y_0 = \gamma_{DC}(d_0)$, $y_{i+1} = y_i \nabla_C \gamma_{DC}(d_{i+1})$.
As ∇_C is a pair-widening operator, this ascending sequence stabilizes after a finite number of terms.
- ▶ We have to show that also the sequence

$$\hat{y}_0 = d_0, \hat{y}_{i+1} = \hat{y}_i \nabla_D d_{i+1}$$

stabilizes after a finite number of terms.

- ▶ By induction, we prove that for each i , $\hat{y}_i = \alpha_{CD}(y_i)$.

Proof (Termination, ctd.)

The basis is trivial, as $\hat{y}_0 = d_0 = \alpha_{CD}(\gamma_{DC}(d_0)) = \alpha_{CD}(y_0)$.
 Looking at the inductive step,

$$\begin{aligned}
 \hat{y}_{i+1} &= \hat{y}_i \nabla_D d_{i+1} && \text{by def. of } \{\hat{y}_j\}_{j \geq 0}. \\
 &= \alpha_{CD}(y_i) \nabla_D d_{i+1} && \text{by inductive hyp.} \\
 &= \alpha_{CD}(y_i) \nabla_D \alpha_{CD}(\gamma_{DC}(d_{i+1})) && \text{by Galois insertion} \\
 &= \alpha_{CD}(y_i \nabla_C \gamma_{DC}(d_{i+1})) && \text{by def. of } \nabla_D \\
 &= \alpha_{CD}(y_{i+1}) && \text{by def. of } \{y_j\}_{j \geq 0}.
 \end{aligned}$$



Pair-widening is preserved by projection

Corollary

Let A and D be complete lattices, and let ∇ be a pair-widening operator over the cartesian product $A \times D$. Let π_1 be the projection on the first argument. The binary operators $\nabla_A : A \times A \rightarrow A$ defined by

$$a \nabla_A a' = \pi_1(\langle a, \top \rangle \nabla \langle a', \top \rangle)$$

is a pair-widening operator.

Reduced Product

Definition

Let C, A, D be complete lattices, and let $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ and $G_{CA} = (\gamma_{AC}, C, A, \alpha_{CA})$ be Galois insertions.

Consider the function $reduce: A \times D \rightarrow A \times D$ defined by

$$reduce(\langle a, d \rangle) = \sqcap \{ \langle a', d' \rangle \mid \gamma_{AC}(a) \sqcap \gamma_{DC}(d) = \gamma_{AC}(a') \sqcap \gamma_{DC}(d') \}$$

The reduced product $A \sqcap D$ is defined as follows:

$$A \sqcap D = \{ reduce(\langle a, d \rangle) \mid a \in A, d \in D \}.$$

Moreover, the function $\gamma : A \sqcap D \rightarrow C$ defined by $\gamma(\langle a, d \rangle) = \gamma_{AC}(a) \sqcap \gamma_{DC}(d)$ is the lower adjoint of a Galois insertion between $A \sqcap D$ and the domain C .

Lemma

Let C, A, D be complete lattices, and let $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ and $G_{CA} = (\gamma_{AC}, C, A, \alpha_{CA})$ be Galois insertions.

$\forall \hat{a} \in A, \hat{d} \in D, \langle a, d \rangle \in A \sqcap D,$

$$a \leq \hat{a} \text{ and } d \leq \hat{d} \Rightarrow \langle a, d \rangle \leq \text{reduce}(\langle \hat{a}, \hat{d} \rangle)$$

Proof

By glb properties and monotonicity of gamma functions,
 $\gamma_{AC}(a) \sqcap \gamma_{DC}(d) \leq \gamma_{AC}(\hat{a}) \sqcap \gamma_{DC}(\hat{d})$. Therefore, $reduce(\langle \hat{a}, \hat{d} \rangle)$ is
 such that

$$\gamma(\langle a, d \rangle) \leq \gamma(reduce(\langle \hat{a}, \hat{d} \rangle))$$

where γ is the lower adjoint of the Galois insertion $(\gamma, C, A \sqcap D, \alpha)$
 as in Def. 22.

By applying α to both expressions, by monotonicity of α we get

$$\alpha(\gamma(\langle a, d \rangle)) \leq \alpha(\gamma(reduce(\langle \hat{a}, \hat{d} \rangle)))$$

and by Galois insertion properties, as $\alpha \circ \gamma$ is the identity function,
 we get

$$\langle a, d \rangle \leq reduce(\langle \hat{a}, \hat{d} \rangle)$$



Extrapolation is preserved by reduced product

Lemma

Let C, A, D be complete lattices, and let $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ and $G_{CA} = (\gamma_{AC}, C, A, \alpha_{CA})$ be Galois insertions.

Let ∇_A and ∇_D be pair-widening operators defined on the lattice A and D , respectively.

The binary operator $\bullet : (A \sqcap D) \times (A \sqcap D) \rightarrow (A \sqcap D)$ defined by

$$\forall \langle a, d \rangle, \langle a', d' \rangle \in A \sqcap D : \langle a, d \rangle \bullet \langle a', d' \rangle = \text{reduce}(\langle a \nabla_A a', d \nabla_D d' \rangle)$$

is an extrapolator operator (i.e. the Covering property holds).

Proof

Let $\langle a, d \rangle, \langle a', d' \rangle \in A \sqcap D$. We have to prove that
 $\langle a, d \rangle \leq \langle a, d \rangle \bullet \langle a', d' \rangle$.

$$\begin{aligned} \langle a, d \rangle &\leq \langle a \nabla_A a', d \nabla_D d' \rangle && \text{by covering of } \nabla_A, \nabla_D \\ \Rightarrow \langle a, d \rangle &\leq \text{reduce}(\langle a \nabla_A a', d \nabla_D d' \rangle) && \text{by previous Lemma} \\ \Rightarrow \langle a, d \rangle &\leq \langle a, d \rangle \bullet \langle a', d' \rangle && \text{by def. of } \nabla \end{aligned}$$

In the same way, we can also prove that
 $\langle a', d' \rangle \leq \langle a, d \rangle \bullet \langle a', d' \rangle$. □

Widening is preserved through reduced product

Theorem

Let C, A, D be complete lattices, and let $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ and $G_{CA} = (\gamma_{AC}, C, A, \alpha_{CA})$ be Galois insertions.

Let ∇_A and ∇_D be pair-widening operators defined on the lattice A and D , respectively, such that

$$\forall \langle a, d \rangle \in A \sqcap D, \forall a' \in A, \forall d' \in D : \langle a \nabla_A a', d \nabla_D d' \rangle \in A \sqcap D.$$

Then the binary operator $\nabla : (A \sqcap D) \times (A \sqcap D) \rightarrow (A \sqcap D)$ defined by

$$\forall \langle a, d \rangle, \langle a', d' \rangle \in A \sqcap D : \langle a, d \rangle \nabla \langle a', d' \rangle = \text{reduce}(\langle a \nabla_A a', d \nabla_D d' \rangle)$$

is a pair-widening operator.

Proof

- ▶ We may focus only on termination. Consider the increasing sequence $\langle a_0, d_0 \rangle \leq \langle a_1, d_1 \rangle \dots$ in $A \sqcap D$.
- ▶ As the ordering \leq in $A \sqcap D$ is the same as in the cartesian product $A \times D$, we may consider the increasing sequence $a_0 \leq a_1 \leq \dots$ in A , and the increasing sequence $d_0 \leq d_1 \leq \dots$ in D .
- ▶ By the termination property of ∇_A and ∇_D , we know that the corresponding sequences $\hat{a}_0 = a_0$, $\hat{a}_{i+1} = \hat{a}_i \nabla_A a_{i+1}$, and $\hat{d}_0 = d_0$, $\hat{d}_{i+1} = \hat{d}_i \nabla_D d_{i+1}$ stabilize after a finite number of terms.
- ▶ We show by induction that the increasing sequence $\langle a'_0, d'_0 \rangle = \langle a_0, d_0 \rangle$, $\langle a'_{i+1}, d'_{i+1} \rangle = \langle a'_i, d'_i \rangle \nabla \langle a_{i+1}, d_{i+1} \rangle$ is such that $\forall i : \langle a'_i, d'_i \rangle = \langle \hat{a}_i, \hat{d}_i \rangle$.

Proof (ctd.)

The basis is trivial, as $\langle a'_0, d'_0 \rangle = \langle a_0, d_0 \rangle = \langle \hat{a}_0, \hat{d}_0 \rangle$.

Induction step:

$$\begin{aligned}
 \langle a'_{i+1}, d'_{i+1} \rangle &= \langle a'_i, d'_i \rangle \nabla \langle a_{i+1}, d_{i+1} \rangle && \text{by def. of } \{\langle a'_j, d'_j \rangle\}_{j \geq 0} \\
 &= \text{reduce}(a'_i \nabla_A a_{i+1}, d'_i \nabla_D d_{i+1}) && \text{by def. of } \nabla \\
 &= \langle a'_i \nabla_A a_{i+1}, d'_i \nabla_D d_{i+1} \rangle && \text{by hypothesis} \\
 &= \langle \hat{a}_{i+1}, \hat{d}_{i+1} \rangle && \text{by def. of } \{\hat{a}_j\}_{j \geq 0}, \{\hat{d}_j\}_{j \geq 0}
 \end{aligned}$$

It follows that $\{\langle a'_j, d'_j \rangle\}_{j \geq 0}$ converges in a finite number of steps, namely the maximum between the termination indexes of $\{\hat{a}_j\}_{j \geq 0}$ and $\{\hat{d}_j\}_{j \geq 0}$. □

Conclusions and Future Work

- ▶ We investigated which properties are necessary to support a systematic design of widening operators.
- ▶ As far as we know, this is the first attempt to provide a general comparison of the different notions of widening used in the literature and a first comprehensive discussion of their main features.
- ▶ More work deserves to be done in order to support a broader range of widening operators when only the concretization function is available or when the lub operator is not always defined.
- ▶ We are currently investigating how to enhance domains and widening operators with suitable metrics that allow to get a quantitative comparison of their precision and/or of their speed to reach a fixed-point.

THANKS!