Widening and Narrowing Operators for Abstract Interpretation *

Agostino Cortesi and Matteo Zanioli
Università Ca' Foscari di Venezia
I-30170 Venezia (Italy)
cortesi@unive.it zanioli@dsi.unive.it

Abstract

Abstract Interpretation, one of the most applied techniques for semantics based static analysis of software, 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. The latter point is crucial to ensure the scalability of the analysis to large software systems. The aim of this paper is to set the ground for a systematic design of widening and narrowing operators, by comparing the different definitions introduced in the literature and by discussing how to tune them in case of domain abstraction and domains' combination through cartesian and reduced products.

Keywords: Static Analysis, Abstract Interpretation, Abstract Domains, Widening Operators, Narrowing Operators.

1 Introduction

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. This theory 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 combination of widening operators (to get fast convergence) and narrowing operators (to improve the accuracy of the resulting analysis).

While 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 [13, 24, 8], and more sophisticated notions like the quotient [10], the complement [9], and the powerset [22] of abstract domains, not much attention has been given to provide general results about widening and narrowing operators.

Nevertheless, widening and narrowing operators play a crucial role in particular when infinite abstract domains are considered to ensure the scalability of the analysis to large software systems, as it has been shown in the case of the Astrée project for analysis of absence of run-time error of avionic critical software [11].

The first infinite abstract domain (that of intervals) was introduced in [12]. This abstract domain was later used to prove that, thanks to widening and narrowing operators, infinite abstract domains can lead to effective static analyses for a given programming language that are strictly more precise and equally efficient than any other one using a finite abstract domain or an abstract domain satisfying chain conditions [16].

Specific widening and narrowing operators have been also designed not only for numerical domains but also for type graphs [25], in domains for reordering CLP(RLin) programs [32], and in the analysis of programs containing digital filters [21], just to name a few. More recently, widenings have been used also to infer loop invariants inside an STM solver [26], in trace partitioning abstract domains [33] and in string analysis for string-generating programs [6].

*Extended version of A. Cortesi, "Widening Operators for Abstract Interpretation" [7].

The main challenge for widening and narrowing operators is when considering numerical domains. For instance, the original widening operator proposed by Cousot and Halbwachs [17] for the domain of convex polyhedra, has been improved by recent works by Bagnara et al [1], and further refined for the domain of pentagons by Logozzo et.al. in [27]. In [2], the authors define three generic widening methodologies for a finite powerset abstract domain. The widening operators are obtained by lifting any widening operator defined on the base-level abstract domain. The proposed techniques are instantiated on powersets of convex polyhedra, a domain for which no non-trivial widening operator was previously known.

We observed that, with the noticeable exception of [16, 2], there is still a lack of general techniques that support the systematic construction of widening or narrowing operators. 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.

The aim of the paper is to fill this gap, and to set the ground for a systematic design of widening and narrowing operators either when they are defined on sets and when they are refined on pairs.
The main contributions can be summarized as follows:

1. the formal definitions of the widening and narrowing operations already introduced in the literature;
2. the proof that the widening and narrowing operators are preserved by abstraction;
3. an indication as how to construct widening operators for a product domain such as the reduced and cartesian products.

Moreover we prove that, for Galois Insertions, widening and narrowing operators are preserved by abstraction and we show how the operators can be combined in the cartesian and reduced product of abstract domains.
The advantages of suitable combinations of widening and narrowing operators are illustrated on a suite of examples, ranging from interval to powerset domains.

The rest of this paper is organized as follows. The next section reports some preliminary notions. In Section 3 we analyze different notions of widening and narrowing operators and we show their weakness points and their mutual relations. In the Section 4 we show how widening and narrowing behave with respect to the combination of domains through Galois insertions. Finally, Section 5 concludes.

2 Basic Definitions

Let us briefly recall some basic definitions on orders and lattices [4, 18].

Definition 1 (poset) *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. By a* poset *$(P, \leq)$ we shall mean a set P on which there is defined a partial order $\leq$.*

Definition 2 (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 $z = \sqcap S$.*

Looking ahead, we shall often adopt the neater notation $x \sqcup y$ in place of $\sqcup\{x, y\}$, and $x \sqcap y$ in place of $\sqcap\{x, y\}$.

Definition 3 (directed set, cpo) *Let S be a subset of a poset $(P, \leq)$. Then S is said to be* directed *if for each pair of elements $x, y \in S$, there exists $z \in S$ such that $x \leq z$ and $y \leq z$.*

We say that a poset $(P, \leq)$ is a cpo *(complete partially ordered set) if P has a bottom element $\bot$, and $\sqcup D$ exists for each directed subset D of P.*

Definition 4 (chain) *A chain of a poset $(P, \leq)$ is a subset $C \subseteq P$ such that $\forall x, y \in C : (x \leq y) \vee (y \leq x)$.*

Definition 5 (ACC and DCC) *A poset $(P, \leq)$ is said to satisfy the ascending chain condition (ACC) if every ascending chain $x_1 \leq x_2 \leq \ldots$ of elements of P is eventually stationary, that is, there is some positive integer n such that $x_m = x_n$ for all $m > n$. By duality, a poset $(P, \leq)$ satisfies the descending chain condition (DCC) if every descending chain $x_1 \geq x_2 \geq \ldots$ of elements of P is strictly decreasing that is $\exists k \geq 0 : \forall j \geq k : x_k = x_j$.*

Definition 6 (join and meet semi lattice) *A join semi lattice and a meet semi lattice are poset $(P, \leq)$ such that each pair of elements $x, y \in P$ has, respectively, least upper bound $(x \sqcup y)$ and great lower bound $(x \sqcap y)$.*

Definition 7 (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. *Moreover, if $\sqcup S$ and $\sqcap S$ exist for every $S \subseteq P$, then P is a* complete lattice.

In what follows a function's domain and range are indicated by subscripts: ε_{XY} is a function from X to Y. The ordering and the least upper bound operator defined in X are denoted by $\sqsubseteq_X$ and $\sqcup_X$, respectively.

Definition 8 (Galois connection and insertion) *Let C and D be complete lattices, and consider two functions: $\gamma_{DC} : D \to C$ and $\alpha_{CD} : C \to D$. 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. The following are well-known properties of these functions, see [15].

Lemma 1 *Let C and D be complete lattices, and consider two monotone functions $\gamma_{DC} : D \to C$ and $\alpha_{CD} : C \to D$. Then, G_{CD} is a Galois connection if and only if*

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

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

Lemma 2 *Let G_{CD} be a Galois connection/insertion,*

- *if α_{CD} and γ_{DC} form a Galois connection, then one of the two functions determines the other one. More precisely, for $d \in D$, $\gamma_{DC}(d) = \sqcup_C \{c \in C \mid \alpha_{CD}(c) \sqsubseteq_D d\}$, and similarly, for $c \in C, \alpha_{CD}(c) = \sqcap_D \{d \in D \mid c \sqsubseteq_C \gamma_{DC}(d)\}$. Each function is called the* adjoint *of the other one.*
- *$\alpha_{CD} \circ \gamma_{DC} \circ \alpha_{CD} = \alpha_{CD}$, and $\gamma_{DC} \circ \alpha_{CD} \gamma_{DC} = \gamma_{DC}$.*

3 Widening and Narrowing Operators

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, abstract interpretation theory provides very powerful tools, the widening operators, that attempt to predict the fix-point based on the sequence of approximations computed on earlier iterations of the analysis on a cpo or on a (complete) lattice. The degradation of precision of the solution obtained by widening can be partly restored by further applying a narrowing operator [16].

3.1 Set- and Pair-Widening Operators

In the Abstract Interpretation literature, two different general definitions of widening operator have been introduced. The first one defines a widening operator as a partial function on the powerset of a poset P, while the second one defines it as a binary (total) function on a poset P. In both cases, two main requirements are given: first, the widening has to be an extrapolation operator, second, it has to guarantee termination when applied to increasing sequences.

Definition 9 (set-widening [13, 15]) *Let $(P, \leq)$ be a poset. A set-widening operator is a partial function $\nabla_\star : \wp(P) \nrightarrow P$ such that*

(i) Covering: Let S be an element of $\wp(P)$. If $\nabla_\star(S)$ is defined, then $\forall x \in S$, $x \leq \nabla_\star(S)$.

(ii) Termination: For every ascending chain $\{x_i\}_{i\geq 0}$, the chain defined as

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

is ascending too, and it stabilizes after a finite number of terms.

The definition above has been used recently in [19, 20], for fix-point computations over sets represented as automata, in a model checking approach.

Example 1 *Consider the lattice of intervals $L = \{\bot\} \cup \{[\ell, u] \mid \ell \in \mathbb{Z} \cup \{-\infty\},\ u \in \mathbb{Z} \cup \{+\infty\},\ \ell \leq u\}$, ordered by: $\forall x \in L, \bot \leq x$ and $[\ell_0, u_0] \leq [\ell_1, u_1]$ if $\ell_1 \leq \ell_0$ and $u_0 \leq u_1$. Let k be a fixed positive integer constant, and I be any set of indices. Consider the threshold widening operator defined on L by:*

$$\nabla^k_\star(\{\bot\}) = \bot$$
$$\nabla^k_\star(\{\bot\} \cup S) = \nabla^k_\star(S)$$
$$\nabla^k_\star(\{[\ell_i, u_i] : i \in I\}) = [h_1, h_2]$$

where

$$h_1 = min\{\ell_i : i \in I\} \text{ if } min\{\ell_i : i \in I\} > -k, \text{ else } -\infty$$
$$h_2 = max\{u_i : i \in I\} \text{ if } max\{u_i : i \in I\}) < k, \text{ else } +\infty.$$

Observe that for all k, $\nabla^k_\star$ is associative, and monotone. Observe that ∇^k_* may widen also the singletons. For instance, we get $\nabla^7_\star(\{[-8, 4]\}) = [-\infty, 4]$.

Definition 10 (pair-widening [16], [31]) *Let $(P, \leq)$ be a poset. A pair-widening operator is a binary operator $\nabla : P \times P \to P$ such that*

(i) Covering: $\forall x, y \in P : x \leq x\nabla y$, and $y \leq x\nabla y$.

(ii) Termination: For every ascending chain $\{x_i\}_{i\geq 0}$, the ascending chain defined as

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

stabilizes after a finite number of terms.

Definition 11 (extrapolator) *Let $(P, \leq)$ be a poset. A binary operator $\bullet : P \times P \to P$ is called* extrapolator *if it satisfies the covering property, i.e. $\forall x, y \in P : x \leq x \bullet y$, and $y \leq x \bullet y$.*

Observe that pair-widening operators are not necessarily neither commutative neither monotone, nor associative, while these properties are crucial for chaotic iteration fixpoint algorithms [31].

Example 2 *Consider the binary operator introduced in [12] on the same lattice of Intervals of Example 1:*

$$\begin{aligned} \bot\nabla x &= x \\ x\nabla\bot &= x \\ [\ell_0, u_0]\nabla[\ell_1, u_1] &= [\text{if } \ell_1 < \ell_0 \text{ then } -\infty \text{ else } \ell_0, \\ &\quad \text{if } u_0 < u_1 \text{ then } +\infty \text{ else } u_0]. \end{aligned}$$

∇ is a pair-widening operator, as it satisfies both covering and termination requirements of Def.10. Observe that the operator is not commutative, as for instance

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

Moreover, in order to see that it is not monotone, consider $[0,1] \leq [0,3]$. We have:

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

and of course $[0,+\infty]$ is not smaller or equal to $[0,3]$. Finally, observe that associativity does not hold either:

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

Let us come back to the two definitions of widening operators introduced before. As a first contribution, we see how to build a set-widening out of a pair-widening operator.

Theorem 1 *Let $(P,\leq)$ be a poset, and let $\nabla : P \times P \to P$ be a pair-widening operator on P. Define $\nabla_\star : \wp(P) \nrightarrow P$ such that:*

- *$dom(\nabla_\star) = R_1 \cup R_2$, where*
  $R_1 = \{\{x,y\} \mid x,y \in P\}$, and
  $R_2 = \{S \subseteq P \mid S$ is a finite ascending chain$\}$.
- *$\forall \{x,y\} \in R_1$,*
  $\nabla_\star(\{x,y\}) =_{def} \begin{cases} x\nabla y & \text{if } x \leq y \\ z \in \{x\nabla y, y\nabla x\} & \text{randomly, otherwise.} \end{cases}$
- *$\forall S = \{x_i \mid x_0 \leq x_1 \leq \cdots \leq x_j\} \in R_2$,*
  $\nabla_\star(S) =_{def} (((x_0\nabla x_1)\nabla x_2 \ldots)\nabla x_j)$.

Then $\nabla_\star$ is a set-widening operator.

Proof: We have to show that both covering and termination requirements hold for $\nabla_\star$.

- *Covering.* Let $S \subseteq P$ such that $\nabla_\star(S)$ is defined. We have to show that $\forall s \in S : s \leq \nabla_\star(S)$.
  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.
- *Termination.* Consider the ascending chain $\{x_i\}_{i\geq 0}$. Consider the corresponding ascending chain $\{\hat{y}_i\}_{i\geq 0}$ obtained by ∇ (see Def. 10), and the ascending chain $\{y_i\}_{i\geq 0}$ obtained using $\nabla_\star$ (see Def. 9). We can 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:

$$\begin{array}{rcll} y_{i+1} & = & \nabla_\star(\{x_j \mid 0 \leq j \leq i+1\}) & \text{by (ii) of Def. 9} \\ & = & (((x_0\nabla x_1)\nabla x_2 \ldots)\nabla x_{i+1}) & \text{by definition of } \nabla_\star \\ & = & \nabla_\star(\{x_j \mid 0 \leq j \leq i\})\nabla x_{i+1} & \text{again by definition of } \nabla_\star \\ & = & \hat{y}_i\nabla x_{i+1} & \text{by inductive hypotesis} \\ & = & \hat{y}_{i+1} & \text{by (ii) of Def. 10} \end{array}$$

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

□

The notion of set-widening is weaker than the notion of pair-widening. This is why, in general, there is no way to prove the dual of Theorem 1, which can be stated only under restricted conditions.

Theorem 2 *Let $(P, \leq)$ be a poset, and let $\nabla_\star : \wp(P) \nrightarrow P$ be a set-widening operator on P such that*

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

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

Proof: First, observe that ∇ is well defined. The covering requirement follows immediately from the definition of ∇ and the covering property of $\nabla_\star$. Now, consider an ascending chain $\{x_i\}_{i \geq 0}$ in P, and the ascending chain $y_0 = x_0, y_{i+1} = y_i \nabla x_i$. As $\nabla_\star$ is a set-widening, we know that the sequence $y'_0 = x_0, y'_i = \nabla_\star(\{x_j \mid 0 \leq j \leq i\}$ stabilizes finitely. We show by induction that for each i, $y_i = y'_i$. The basis is true, as $y_0 = x_0 = y'_0$. On the induction step,

$$\begin{array}{rcll} y'_{i+1} & = & \nabla_\star(\{x_j \mid 0 \leq j \leq i+1\} & \text{by point (ii) of Def. 9} \\ & = & \nabla_\star(\{\nabla_\star(\{x_j \mid 0 \leq j \leq i\}), x_{i+1}\}) & \text{by hypothesis on } \nabla_\star \\ & = & \nabla_\star(\{y'_i, x_{i+1}\}) & \text{by point (ii) of Def. 9} \\ & = & \nabla_\star(\{y_i, x_{i+1}\}) & \text{by inductive hypothesis} \\ & = & y_i \nabla x_{i+1} & \text{by definition of } \nabla \\ & = & y_{i+1} & \text{by point (ii) of Def. 10.} \end{array}$$

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

Observe that the set-widening operator $\nabla^k_\star$ of Example 1 satisfies the conditions of Theorem 2 above, yielding to a corresponding pair-widening operator.

3.2 Set- and Pair-Narrowing Operators

Similarly, two different general definitions of narrowing operator have been introduced. The first one defines a narrowing operator as a partial function on the powerset of a poset P, while the second one defines it as a binary (total) function on a poset P.

Definition 12 (set-narrowing [15, 19]) *Let $(P, \leq)$ be a poset. A set-narrowing operator is a partial function $\Delta_\star : \wp(P) \nrightarrow P$ such that*

(i) Bounding: Let S be an element of $\wp(P)$. If $\Delta_\star(S)$ is defined, then $glb(S)$ exists and there exists $s \in S$ such that $glb(S) \leq \Delta_\star(S) \leq s$.

(ii) Termination: For every decreasing chain $x_0 \geq x_1 \geq \ldots$, the chain defined as

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

is descending too, and it stabilizes after a finite number of terms.

Example 3 *Let L be the lattice of intervals introduced in Example 1. We can define $\Delta_\star$, a narrowing operator, on L as follows.*

$$\begin{array}{c} \Delta_\star(\{\bot\}) = \bot \\ \Delta_\star(\{\bot\} \cup S) = \Delta_\star(S) \\ \Delta_\star(\{[\ell_i, u_i] : i \in I\}) = [h_1, h_2] \end{array}$$

where

$$\begin{array}{c} h_1 = max\{\ell_i : i \in I\} \\ h_2 = min\{u_i : i \in I\} \end{array}$$

It is easy to verify that it satisfy the termination condition, as it converges immediately on decreasing chains. Observe that $\Delta_\star$ is associative, and monotone. Observe that $\Delta_\star$ may narrow also the singletons. For instance, we get $\Delta_\star(\{[-8, 4]\}) = [-8, 4]$ and $\Delta_\star(\{[-8, 6], [1, 5], [-9, 11]\}) = [1, 5]$.

Example 4 *Observe that both conditions (bounding and termination) are required in order to get a narrowing operator. For instance, on the lattice of intervals on $\mathbb{R}$ instead of $\mathbb{Z}$, the operator Δ_* defined in Example 3 fulfills the bounding condition but it does not satisfy the termination one. Therefore, it is a not narrowing operator.*

Definition 13 (pair-narrowing [14, 16]) *Let $(P, \leq)$ be a poset. A pair-narrowng operator is a binary operator $\Delta : P \times P \to P$ such that*

(i) Bounding: $\forall x, y \in P : (x \leq y) \Longrightarrow (x \leq (y \Delta x) \leq y)$.

(ii) Termination: For every decreasing chain $x_0 \geq x_1 \geq \ldots$, the decreasing chain defined as

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

stabilizes after a finite number of terms.

Observe that pair-narrowing operators are not necessarily neither commutative neither monotone, nor associative. Moreover observe also that if P is a meet-semi-lattice (the greatest lower bound $x \sqcap y$ exists for all $x, y \in P$) satisfying the decreasing chain condition (no strictly decreasing chain in P can be infinite), then $\sqcap$ is a narrowing.

Example 5 *Consider the binary operator introduced in [16] on the same lattice of intervals on $\mathbb{Z}$ of Example 1:*

$$\begin{array}{rcl} \bot \Delta x & = & \bot \\ x \Delta \bot & = & \bot \\ [\ell_0, u_0] \Delta [\ell_1, u_1] & = & [\textit{if } \ell_0 = -\infty \textit{ then } \ell_1 \textit{ else } \ell_0, \\ & & \textit{if } u_0 = +\infty \textit{ then } u_1 \textit{ else } u_0] \end{array}$$

Δ is a pair-widening operator, as it satisfies both bounding and termination requirements of Def.13.

$$\begin{array}{rcl} [-\infty, +\infty] \Delta [-\infty, 101] & = & [-\infty, 101] \\ [1, +\infty] \Delta [50, 100] & = & [1, 100] \\ [1, 4] \Delta [2, 3] & = & [1, 3] \end{array}$$

Let us come back to the two definitions of narrowing operators introduced above. Like in the case of widening, we study how we can build a set-narrowing operator out of a pair-narrowing operator, and viceversa.

Theorem 3 *Let $(P, \leq)$ be a poset, and let $\Delta : P \times P \to P$ be a pair-narrowing operator on P. Define $\Delta_\star : \wp(P) \nrightarrow P$ such that:*

- *$dom(\Delta_\star) = R_1 \cup R_2$, where*
  $R_1 = \{\{x, y\} \mid x, y \in P\ : \exists\ glb(x, y)\}$, and
  $R_2 = \{S \subseteq P \mid S$ is a finite descending chain$\}$.

- *$\forall \{x, y\} \in R_1$,*
  $\Delta_\star(\{x, y\}) =_{def} \begin{cases} y \Delta x & \textit{if } x \leq y \\ glb(\{x, y\}) & \textit{otherwise.} \end{cases}$

- *$\forall S = \{x_i \mid x_0 \geq x_1 \geq \cdots \geq x_j\} \in R_2$,*
  $\Delta_\star(S) =_{def} ((((x_0 \Delta x_1) \Delta x_2) \Delta) \ldots \Delta x_j)$.

Then $\Delta_\star$ is a set-narrowing operator.

Proof: We have to show that both bounding and termination requirements hold for $\Delta_\star$.

- *Bounding.* Let $S \subseteq P$ such that $\Delta_\star(S)$ is defined. We have to show that $glb(S) \leq \Delta_\star(S) \leq s$.
  Case $S \in R_1$: it follows from the definition of Δ.
  Case $S \in R_2$: it follows by induction on the length of the decreasing chain $(x_0 \geq x_1 \geq \ldots \geq x_j)$, and by the transitivity of the partial order.

- *Termination.* Consider the decreasing chain $\{x_i\}_{i\geq 0}$. Consider the corresponding decreasing chain $\{\hat{y}_i\}_{i\geq 0}$ obtained by Δ (see Def. 13), and the decreasing chain $\{y_i\}_{i\geq 0}$ obtained using $\Delta_\star$ (see Def. 12). We can 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:

$$\begin{array}{rcll} y_{i+1} & = & \Delta_\star(\{x_j \mid 0 \leq j \leq i+1\}) & \text{by definition of the sequence } \{y_j\}_{j\geq 0} \\ & = & (((((x_0 \Delta x_1)\Delta x_2)\Delta) \ldots \Delta x_i)\Delta x_{i+1}) & \text{by definition of } \Delta_\star \\ & = & \Delta_\star(\{x_j \mid 0 \leq j \leq i\})\Delta x_{i+1} & \text{again by definition of } \Delta_\star \\ & = & \hat{y}_i \Delta x_{i+1} & \text{by inductive hypothesis} \\ & = & \hat{y}_{i+1} & \text{by (ii) of pair-narrowing definition} \end{array}$$

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

□

Theorem 4 *Let $(P, \leq)$ be a poset, and let $\Delta_\star : \wp(P) \nrightarrow P$ be a set-narrowing operator on P such that*

1. *$dom(\Delta_\star) \supseteq \{\{x, y\} \mid x, y \in P\}$, and*
2. *$\forall S \subseteq P,\ \forall x \in P,$ if $S \cup \{x\} \subseteq dom(\Delta_\star)$ then also $S \subseteq dom(\Delta_\star)$*
3. *$\forall S \subseteq P,\ \forall x \in P,\ \Delta_\star(S \cup \{x\}) = \Delta_\star(\{\Delta_\star(S), x\})$.*

Then, the binary operator $\Delta : P \times P \to P$ defined $x\Delta y = \Delta_\star(\{x, y\})$ is a pair-narrowing operator.

Proof: First, observe that Δ is well defined. The bounding requirement follows immediately from the definition of Δ and the bounding property of $\Delta_\star$. Now, consider an descending chain $\{x_i\}_{i\geq 0}$ in P, and the descending chain $y_0 = x_0, y_{i+1} = y_i \Delta x_{i+1}$. As $\Delta_\star$ is a set-narrowing, we know that the sequence $y'_0 = x_0, y'_i = \Delta_\star(\{x_j \mid 0 \leq j \leq i\})$ stabilizes finitely. We show by induction that for each i, $y_i = y'_i$. The basis is true, as $y_0 = x_0 = y'_0$. On the induction step,

$$\begin{array}{rcll} y_{i+1} & = & y_i \Delta x_{i+1} & \text{by definition of the sequence } \{y_j\}_{j\geq 0} \\ & = & \Delta_\star(\{y_i, x_{i+1}\}) & \text{by } \Delta \text{ definition} \\ & = & \Delta_\star(\{\Delta_\star(\{x_j \mid 0 \leq j \leq i\}), x_{i+1}\}) & \text{by induction hypothesis} \\ & = & \Delta_\star(\{x_j \mid 0 \leq j \leq i+1\}) & \text{by the property 3} \\ & = & y'_{i+1} & \text{by (ii) of set-narrowing definition} \end{array}$$

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

3.3 Combination of Widening and Narrowing Operators

In order to better understand how widening and a narrowing operators can be combined in an effective way, consider the following example on the finite powerset domain of intervals.

The design of a successful widening is a very delicate task that is not only dependent on the considered abstract domain but also on the particular analysis or verification application. An important contribution in such context is [2], which introduces three methodologies for the design of widening operators. All of these methodologies are based on the same extrapolator, while they differ on the termination property: the first one poses constraints on the cardinality of the arguments, the second one uses connectors (as, for example, Egli-Milner Connectors), and the last one is certificate-based.
Notice that these generic widening constructions are applicable to any finite powerset abstract domain, encoding either numerical or symbolic information.

Example 6 *Let L be the lattice of intervals introduced in Example 1, and let $\wp_f(L)$ be its finite powerset. For $A, B \in \wp_f(L)$, we say $A \trianglelefteq B$ if and only if $\forall x \in A, \exists y \in B$ such that $x \leq y$. Consider the function reduce : $\wp_f(L) \to \wp_f(L)$ defined as $\forall A \subseteq L$, reduce(A) is the maximal subset of A such that $\forall x, y \in A : x < y \Rightarrow x \notin reduce(A)$. Observe that reduce$(A) \trianglelefteq A$ and $A \trianglelefteq$ reduce(A).*

The closure of $A \subseteq L$, denoted by $\overline{A}$, is the superset of A such that $\forall x, y \in A$, such that $x \cap y \neq \emptyset$, the least upper bound $x \sqcup y \in \overline{A}$.
For $X \subseteq L$, we denote by $min(X)$ the minimal value, and by $max(X)$ the maximal value, e.g. $min(\{[3,8],[2,5],[1,4]\}) = 1$ and $max(\{[3,8],[2,5],[1,4]\}) = 8$.
By $minInt(X)$ we denote the interval which have $min(X)$ as bottom value and, analogously, by $maxInt(X)$ the interval having $max(X)$ as top value, e.g. $minInt(\{[3,8],[2,5],[1,4]\}) = [1,4]$ and $maxInt(\{[3,8],[2,5],[1,4]\}) = [3,8]$.
For any positive constant k, we can define the pair-widening $\nabla^k : \wp_f(L) \times \wp_f(L) \rightarrow \wp_f(L)$ as follows.
Let A, B be elements of $\wp_f(L)$.

- *If the cardinality of $reduce(A \cup B)$ is smaller or equal to k, then $A \nabla^k B = reduce(A \cup B)$.*
- *Otherwise, let $R = reduce(\overline{W})$ where W is obtained by:*
  - *$W = A \cup B$*
  - *If the cardinality of $reduce(W)$ is greater than k and $\exists s' \in B$ such that $max(s') > max(A)$ then: let $r \in A$ be the interval such that $max(r) = max(A)$ then $W = W \cup [min(r), +\infty]$.*
  - *And if the cardinality of $reduce(W)$ is greater than k and $\exists s' \in B$ such that $min(s') < min(A)$ then: let $r \in A$ be the interval such that $min(r) = min(A)$ then $W = W \cup [-\infty, max(r)]$.*
- *While the cardinality of R is greater than k:*
  let $s, s' \in R$ such that $|min(s') - max(s)|$ is minimal in R, then $R = (R \setminus \{s, s'\}) \cup \{(s \sqcup s')\}$.
- *$A \nabla^k B = R$.*

Observe that if $Y = A \nabla^k B$, then the cardinality of Y is always smaller or equal to k.
For instance, if

$$A = \{[-5,2],[1,6],[11,23],[27,33],[30,35],[36,40]\}$$

and

$$B = \{[-2,3],[9,15],[32,35],[37,42]\}$$

then

$$A \nabla^3 B = \{[-5,6],[9,23],[27,+\infty]\}.$$

In fact , as the cardinality of $reduce(A \cup B)$ is 4, which is greater than $k = 3$, and there exists an interval s in B (namely $[37,42]$) such that $min(s) > max(A)$, the set $W = A \cup B \cup \{[36,+\infty]\}$ is computed. Then, its closure $\overline{W} = W \cup \{[-5,6],[-5,3],[-2,3],[9,23],[27,35],[36,42]\}$ is computed. Finally, the reduce operator is applied, yielding to $reduce(\overline{W}) = \{[-5,6],[9,23],[27,+\infty]\}$.

Notice that this widening operator satisfies the constraints in [2], as it merges an extrapolation heuristics "∇-covered" and a "k-collapsor", as requested to obtain a "cardinality-based" widening. In addition, our operator can be applied also on not comparable elements, whereas the generic construction provided by Bagnara et.al. requires that the first element is less than second one.

Similarly, we can define a corresponding pair-narrowing operator $\Delta^k : \wp_f(L) \rightarrow \wp(L)$. Let $A, B \in \wp_f(L)$ such that $A \trianglelefteq B$, $B \Delta^k A$ is defined as follows.

- *Let $A' = reduce(A) = \{s_1, \ldots, s_n\}$, $B' = reduce(B) = \{q_1, \ldots, q_m\}$ and $R = A'$.*
- *If $min(A') = -\infty$ then $R = R \setminus \{minInt(A')\} \cup \{minInt(B')\}$, and if $max(A') = +\infty$ then $R = R \setminus \{maxInt(A')\} \cup \{maxInt(B')\}$.*
- *For each $q_i \in B'$.*
  - *Let $H_i = \{s_j \in R | s_j \leq q_i\}$*
  - *If cardinality of H_i is greater than 1.*

- *Let $a, b \in H_i$ such that $|min(b) - max(a)|$ is minimal in H_i.*
- *$R = reduce(R \setminus \{a, b\} \cup \{lub(a, b)\})$.*

– *If the cardinality of R is smaller than k then break.*

- *$B\Delta^k A = R$.*

Observe that Δ^k is a pair-narrowing operator, as it satisfies both bounding and termination properties. For instance, if

$$A = \{[-10, -6], [-5, -2], [-1, 0], [1, 3], [9, 13], [18, 20], [23, 27], [29, +\infty]\}$$

and

$$B = \{[-10, 3], [7, 13], [16, +\infty]\}$$

then we have

$$B\Delta^3 A = \{[-10, 3], [9, 13], [16, +\infty]\}$$

As an example on how the widening and narrowing operators just introduced can be combined in order to accelerate the fixpoint computation without loosing too much accuracy, consider the function $F : \wp_f(L) \to \wp_f(L)$ defined by

$$F \equiv \lambda X.((((X \sqcup \{[1, 2]\}) \cup \{(maxInt(X) \oplus [2, 2])\}) \setminus \{\bot\}) \sqcap \{[100, 100]\})$$

where $\oplus : L \times L \to L$ such that $\bot \oplus X = X \oplus \bot = \bot$ and $[\ell_0, u_0] \oplus [\ell_1, u_1] = [\ell_0 + \ell_1, u_0 + u_1]$. The computation of the fixpoint of F starting from the $\bot$ element, would require at least 50 steps, getting to the fixpoint element $\{[1, 2], [3, 4], \ldots, [100, 100]\}$. In order to accelerate the fixpoint computation of F, first we use the widening operator ∇^3 defined above.

$$\begin{array}{lcl} X_0 & = & \{\bot\} \\ X_1 & = & X_0\nabla^3((((X_0 \sqcup \{[1, 2]\}) \cup \{(maxInt(X_0) \oplus [2, 2])\}) \setminus \{\bot\}) \sqcap \{[100, 100]\}) \\ & = & \{[1, 2]\} \\ X_2 & = & \{[1, 2], [3, 5]\} \\ & \vdots & \\ X_4 & = & \{[1, 2], [3, 4], [5, +\infty]\} = X_5 \end{array}$$

The fixpoint is obtained in 5 steps, but the accuracy of the result is not satisfactory as it completely looses the rightmost bound. Nevertheless, this lack of precision can be recovered by applying the narrowing operator Δ^3.

$$\begin{array}{lcl} Y_0 & = & X_4 \\ Y_1 & = & Y_0\Delta^3((((Y_0 \sqcup \{[1, 2]\}) \cup \{(maxInt(Y_0) \oplus [2, 2])\}) \setminus \{\bot\}) \sqcap \{[100, 100]\}) \\ & = & \{[1, 2], [3, 4], [5, 100]\} \\ Y_2 & = & \{[1, 2], [3, 4], [5, 100]\} = Y_1 \end{array}$$

Observe that Δ^3 requires only 3 steps to converge. We obtain as a final result the set $\{[1, 2], [3, 4], [5, 100]\}$, which is not as precise as the least fixpoint computation mentioned above, but that has the advantage of being reached dramatically quicker, and of preserving accuracy about the rightmost bound of the possible values of F.

3.4 Widening, Narrowing and Cartesian Product

The next theorems show how pair-widening and pair-narrowing operators can be combined when considering the cartesian product of posets.

Theorem 5 *Let ∇_A and ∇_D be pair-widening operators defined on the posets A and D, respectively. The binary operator $\nabla : (A \times D) \times (A \times D) \to (A \times D)$ 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*

$$\begin{array}{lll} & a \leq a\nabla_{A} a' \text{ and } d \leq d\nabla_{D} d' & \text{by covering of } \nabla_{A}, \nabla_{D} \\ \Rightarrow & \langle a,d\rangle \leq \langle a\nabla_{A} a', d\nabla_{D} d'\rangle & \text{by definition of } \leq \text{ on } A \times D \\ \Rightarrow & \langle a,d\rangle \leq \langle a,d\rangle \nabla \langle a',d'\rangle & \text{by definition of } \nabla. \end{array}$$

- *Termination* Let $\{\langle a_i, d_i\rangle\}_{i\geq 0}$ be an ascending chain 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. □

Theorem 6 *Let Δ_{A} and Δ_{D} be pair-narrowing operators defined on the posets A and D, respectively. The binary operator $\Delta : (A \times D) \times (A \times D) \to (A \times D)$ defined by $\forall \langle a,d\rangle, \langle a',d'\rangle \in A \times D : \langle a,d\rangle \Delta \langle a',d'\rangle = \langle a\Delta_{A} a', d\Delta_{D} d'\rangle$ is a pair-narrowing operator.*

Proof:

- *Bounding*

$$\begin{array}{ll} & \forall a, a' \in A : (a \leq a') \Longrightarrow (a \leq a' \Delta a \leq a') \text{ and} \\ & \forall d, d' \in D : (d \leq d') \Longrightarrow (d \leq d' \Delta d \leq d') \\ & \quad \text{by bounding of } \Delta_A \text{ and } \Delta_B \\ \Rightarrow & \langle a,d\rangle \leq \langle a' \Delta_A a, d' \Delta_D d\rangle \leq \langle a',d'\rangle \\ & \quad \text{by definition of } \leq \text{ on } A \times D \\ \Rightarrow & \langle a,d\rangle \leq \langle a',d'\rangle \Delta \langle a,d\rangle \leq \langle a',d'\rangle \\ & \quad \text{by definition of } \Delta \end{array}$$

- *Termination* Let $\{\langle a_i, d_i\rangle\}_{i\geq 0}$ be a descending chain in the cartesian product $A \times D$. We have to show that the sequence $\langle u_0, v_0\rangle = \langle a_0, d_0\rangle,\ \langle u_{i+1}, v_{i+1}\rangle = \langle u_i, v_i\rangle \Delta \langle a_i, d_i\rangle$ stabilizes after a finite number of terms.

  By the termination property of Δ_{A} and Δ_{D}, both the sequence $\hat{a}_0 = a_0,\ \hat{a}_{i+1} = \hat{a}_i \Delta_{A} a_i$, and the sequence $\hat{d}_0 = d_0,\ \hat{d}_{i+1} = \hat{d}_i \Delta_{D} d_i$ stabilize finitely.

  By induction we prove that for each i, $\langle u_i, v_i\rangle = \langle \hat{a}_i, \hat{d}_i\rangle$.
  The basis is true: $\langle u_0, v_0\rangle = \langle a_0, d_0\rangle = \langle \hat{a}_0 \hat{d}_0\rangle$. On the induction step,

$$\begin{array}{lcll} \langle u_{i+1}, v_{i+1}\rangle & = & \langle u_i, v_i\rangle \Delta \langle a_{i+1}, d_{i+1}\rangle & \text{by definition of } \rangle u_{i+1}, v_{i+1}\rangle \\ & = & \langle \hat{a}_i, \hat{d}_i\rangle \Delta \langle a_{i+1}, d_{i+1}\rangle & \text{by induction hypothesis} \\ & = & \langle \hat{a}_i \Delta_A a_{i+1}, \hat{d}_i \Delta_D d_{i+1}\rangle & \text{by definition of } \Delta \\ & = & \langle \hat{a}_{i+1}, \hat{d}_{i+1}\rangle & \text{by definition of } \hat{a}_{i+1} \text{ and } \hat{d}_{i+1} \end{array}$$

  Therefore, the sequence $\{\langle u_j, v_j\rangle\}_{j\geq 0}$ stabilizes finitely too.

□

A corresponding result can be obtained also for set-widening and set-narrowing operators.

3.5 Combination of widening and narrowing operators on the same poset

What happens when more than one widening (or narrowing) operators are defined on a poset P? Is it possible to get a more precise and/or a more efficient operator by combining them in a suitable way? Unfortunately, in general the answer is negative. And the reason relies on the fact that the possibly non monotonic behavior of the widening (or narrowing) operators becomes an issue when trying to prove termination of their combination on an ascending (and descending for narrowing) chain. However, as soon as stronger termination conditions are guaranteed on the poset P, some positive results can be easily derived.

Theorem 7 *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 $\nabla_\sqcap, \nabla_\sqcup$ defined by*

$$\begin{aligned} x \nabla_\sqcap y &= (x \nabla_1 y) \sqcap (x \nabla_2 y) \\ x \nabla_\sqcup y &= (x \nabla_1 y) \sqcup (x \nabla_2 y) \end{aligned}$$

are pair-widening operators.

Proof: It follows by properties of $\sqcup$ and $\sqcap$. □

This result may apply for instance to widening operators defined on the (infinite) domain of congruences [23], where prime factorization is an issue, in order to tune performance vs. accuracy of the analysis. In fact, $\nabla_\sqcup$ may gain in efficiency with respect to both ∇_1 and ∇_2, while $\nabla_\sqcap$ may better keep accuracy, thus returning a more accurate result.

A corresponding result can be obtained with narrowing operators.

Theorem 8 *Let $(P, \leq)$ be a lattice satisfying the descending chain property. Let Δ_1, Δ_2 be two pair-narrowing operators on P. Then, the binary operators $\Delta_\sqcap, \Delta_\sqcup$ defined by*

$$\begin{aligned} x \Delta_\sqcap y &= (x \Delta_1 y) \sqcap (x \Delta_2 y) \\ x \Delta_\sqcup y &= (x \Delta_1 y) \sqcup (x \Delta_2 y) \end{aligned}$$

are pair-narrowing operators.

Proof: It follows by properties of $\sqcup$ and $\sqcap$, as for the widening operators. □

Similar results can be easily derived by similar proofs also for set-widening and set-narrowing operators.

Theorem 9 *Let $(P, \leq)$ be a lattice satisfying the ascending chain property. Let ∇_{*1}, ∇_{*2} be two set-widening operators on P. Then, the operators $\nabla_{*\sqcap}, \nabla_{*\sqcup}$ defined by*

$$\begin{aligned} \nabla_{*\sqcap}(\{S\}) &= (\nabla_{*1}(\{S\})) \sqcap (\nabla_{*2}(\{S\})) \\ \nabla_{*\sqcup}(\{S\}) &= (\nabla_{*1}(\{S\})) \sqcup (\nabla_{*2}(\{S\})) \end{aligned}$$

are set-widening operators.

Theorem 10 *Let $(P, \leq)$ be a lattice satisfying the descending chain property. Let Δ_{*1}, Δ_{*2} be two set-widening operators on P. Then, the operators $\Delta_{*\sqcap}, \Delta_{*\sqcup}$ defined by*

$$\begin{aligned} \Delta_{*\sqcap}(\{S\}) &= (\Delta_{*1}(\{S\})) \sqcap (\Delta_{*2}(\{S\})) \\ \Delta_{*\sqcup}(\{S\}) &= (\Delta_{*1}(\{S\})) \sqcup (\Delta_{*2}(\{S\})) \end{aligned}$$

are set-narrowing operators.

3.6 Strong Widening and Narrowing Operators

For numerical domains like polyhedra, where the abstract elements computed at each iteration of the analysis are not necessarily ordered, stronger notions of widening and narrowing are used for forcing the termination of the analysis. This is the case, for instance, of the trace partitioning abstract domain of Astrée, an abstract interpretation-based analyzer aiming at proving automatically the absence of run time errors in programs written in the C programming language, which has been applied with success to large safety critical real-time software for avionics [5, 11].

Definition 14 (strong pair-widening [33]) *Let $(P, \leq)$ be a poset. A strong pair-widening operator is a binary operator $\nabla : P \times P \to P$ 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 ascending chain defined as $y_0 = x_0,\ y_{i+1} = y_i \nabla x_{i+1}$ stabilizes after a finite number of terms.

Observe that this definition is strictly stronger than Definition 10, as termination is required starting from every (not necessarily increasing) sequence.

Example 7 *The octagon domain [28, 30] is based on invariants of the form $\pm x \pm y \leq c$, where x and y are numerical variables and c is a numeric constant. Sets described by such invariants are special kind of polyhedra called octagons because they feature at most eight edges in dimension 2. These constraints are expressed through Difference Bound Matrices, which are adjacency matrices of weighted graphs. The widening operator defined on this domain consists on removing unstable constraints. In this case, termination has to be guaranteed for the chain of widened elements starting from a sequence of elements possibly incomparable. This is why the strongest notion of pair widening has to be used.*
Notice however that as an alternative to the strong pair-widening, Bagnara et.al. [3] introduced a different representation of the octagons to ensure that the standard pair-widening can be applied. This approach is applied in [3] to several weakly-relational domains, but it can be generalized to other domains.

The two notions of Pair-widening and Strong pair-widening are equivalent for a lattice P, under associativity conditions, as shown in Theorem 11. In order to prove it, we introduce the following auxiliary Lemma.

Lemma 3 *Let ∇ be a pair-widening operator on a lattice $(P, \leq)$, 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 $y_0 = x_0 = z_0 = h_0$.
The induction step:

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

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

Theorem 11 *Let ∇ be an associative pair-widening operator on a lattice $(P, \leq)$, 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 Lemma 3, it is sufficient to prove by induction that for every finite set $\{x_i\}_{0\leq i\leq n}$ and for every $y \in P$, $(((x_0 \nabla x_1)\nabla \dots)\nabla x_n)\ \nabla\ (x_0 \sqcup x_1 \sqcup \dots \sqcup x_n \sqcup y) = (((x_0 \nabla x_1)\nabla \dots)\nabla x_n)\nabla y$.
The basis ($n = 1$) follows immediately from the hypothesis.
Induction step:

$$\begin{array}{ll}
(((x_0 \nabla x_1)\nabla \dots)\nabla x_n)\ \nabla\ (x_0 \sqcup \dots \sqcup x_n \sqcup y)\ = & \text{by inductive hypothesis} \\
(((x_0 \nabla x_1)\nabla \dots)\nabla (x_0 \sqcup \dots \sqcup x_n))\ \nabla\ (x_0 \sqcup \dots \sqcup x_n \sqcup y)\ = & \text{by associativity of } \nabla \text{ and of } \sqcup \\
((x_0 \nabla x_1)\nabla \dots)\nabla ((x_0 \sqcup \dots \sqcup x_n)\nabla ((x_0 \sqcup \dots \sqcup x_n) \sqcup y))\ = & \text{by applying the hypothesis} \\
((x_0 \nabla x_1)\nabla \dots)\nabla ((x_0 \sqcup \dots \sqcup x_n)\nabla y)\ = & \text{by associativity of } \nabla \\
(((x_0 \nabla x_1)\nabla \dots)\nabla x_n)\nabla y. &
\end{array}$$

□

Example 8 *The pair-widening operator on intervals obtained from the set-widening of Example 1 following the construction of Theorem 2, satisfies the condition of Theorem 11, and it is in fact a strong pair widening operator. However, not every pair-widening operator is also a strong one. On the same lattice of intervals, consider for instance the pair-widening* ∇ *defined by:*

$$\bot \nabla x = x \qquad and \qquad x \nabla \bot = x$$

$$[\ell_0, u_0] \nabla [\ell_1, u_1] = \qquad = \begin{cases} [-\infty, +\infty] \\ \qquad if\ [\ell_0, u_0] \leq [\ell_1, u_1]\ or\ [\ell_1, u_1] \leq [\ell_0, u_0] \\ \\ [min(\ell_0, \ell_1), max(u_0, u_1)] \\ \qquad otherwise \end{cases}$$

On increasing sequences, the widened sequence terminates immediately, whereas if we consider for instance the sequence $\{[i, i+1]\}_{i \geq 0}$, ∇ *yields to the ascending sequence* $\{[0, i]\}_{i \geq 1}$, *which does not terminate.*

Definition 15 (strong pair-narrowing) *Let* $(P, \leq)$ *be a poset. A strong pair-narrowing operator is a binary operator* $\Delta : P \times P \to P$ *such that*

(i) Bounding: $\forall x, y \in P : (x \leq y) \Longrightarrow (x \leq (y \Delta x) \leq y)$.

(ii) Termination: For every sequence $\{x_i\}_{i \geq 0}$, *the decreasing chain defined as*

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

stabilizes after a finite number of terms.

Example 9 *The following strong narrowing operator has been introduced in [12].*

$$\begin{array}{rcl} x \Delta \bot & = & \bot \\ [\ell_0, u_0] \Delta [\ell_1, u_1] & = & [if\ \ell_0 = -\infty\ then\ \ell_1\ else\ min(\ell_0, \ell_1), \\ & & \quad if\ u_0 = +\infty\ then\ u_1\ else\ max(u_0, u_1)] \end{array}$$

Δ *is a pair-narrowing operator, as it satisfies both bounding and termination requirements of Def.15. For instance:*

$$\begin{array}{rcrcl} [-\infty, +\infty] & \Delta & [-\infty, 101] & = & [-\infty, 101] \\ [-\infty, 101] & \Delta & [0, 100] & = & [0, 101] \\ [0, 100] & \Delta & [0, 99] & = & [0, 100] \end{array}$$

The two notions of pair-narrowing (Def. 13) and strong pair-narrowing (Def. 15) are equivalent for a lattice P, under associativity conditions, as shown in Theorem 12. In order to prove it, we introduce the following auxiliary Lemma.

Lemma 4 *Let* Δ *be a pair-narrowing operator on a lattice* $(P, \leq)$, *such that for every finite set* $\{x_i\}_{0 \leq i \leq n}$ *and for every* $y \in P$, $(((x_0 \Delta x_1) \Delta \ldots) \Delta x_n)\ \Delta\ (x_0 \sqcap x_1 \sqcap \cdots \sqcap x_n \sqcap y) = (((x_0 \Delta x_1) \Delta \ldots) \Delta x_n) \Delta y$, *then* Δ *is a strong pair-narrowing operator.*

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

$$z_0 = x_0,\ z_{i+1} = x_0 \sqcap \ldots \sqcap x_{i+1}$$

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

The induction step:

$$\begin{array}{rcll} h_{i+1} & = & h_i \Delta z_{i+1} & \text{by Def. of } \{h_j\}_{j\geq 0} \\ & = & y_i \Delta z_{i+1} & \text{by inductive hypothesis} \\ & = & (((x_0 \Delta x_1)\Delta \ldots)\Delta x_i)\Delta z_{i+1} & \text{by Def. of } \{y_j\}_{j\geq 0} \\ & = & (((x_0 \Delta x_1)\Delta \ldots)\Delta x_i)\Delta (x_0 \sqcap \ldots \sqcap x_{i+1}) & \text{by Def. of } \{z_j\}_{j\geq 0} \\ & = & (((x_0 \Delta x_1)\Delta \ldots)\Delta x_i)\Delta x_{i+1} & \text{by hypothesis on } \Delta \\ & = & y_{i+1} & \text{by Def. of } \{y_j\}_{j\geq 0} \end{array}$$

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

Theorem 12 *Let Δ be an associative pair-narrowing operator on a lattice $(P, \leq)$, such that for $\forall x, y \in P : x\Delta y = x\Delta(x \sqcap y)$, then Δ is a strong pair-narrowing operator.*

Proof: By Lemma 4, it is sufficient to prove by induction that for every finite set $\{x_i\}_{0\leq i\leq n}$ and for every $y \in P$, $(((x_0\Delta x_1)\Delta \ldots)\Delta x_n) \ \Delta \ (x_0 \sqcap x_1 \sqcap \cdots \sqcap x_n \sqcap y) = (((x_0\Delta x_1)\Delta \ldots)\Delta x_n)\Delta y$.
The basis ($n = 1$) follows immediately from the hypothesis.
Induction step:

$$\begin{array}{ll} (((x_0\Delta x_1)\Delta \ldots)\Delta x_n) \ \Delta \ (x_0 \sqcap \cdots \sqcap x_n \sqcap y) \ = & \text{by inductive hypothesis} \\ (((x_0\Delta x_1)\Delta \ldots)\Delta (x_0 \sqcap \cdots \sqcap x_n)) \ \Delta \ (x_0 \sqcap \ldots \sqcap x_n \sqcap y) \ = & \text{by associativity of } \Delta \text{ and of } \sqcap \\ ((x_0\Delta x_1)\Delta \ldots)\Delta((x_0 \sqcap \cdots \sqcap x_n)\Delta((x_0 \sqcap \cdots \sqcap x_n) \sqcap y)) \ = & \text{by applying the hypothesis} \\ ((x_0\Delta x_1)\Delta \ldots)\Delta((x_0 \sqcap \cdots \sqcap x_n)\Delta y) \ = & \text{by associativity of } \Delta \\ (((x_0\Delta x_1)\Delta \ldots)\Delta x_n)\Delta y. & \end{array}$$

□

3.7 Lower Bound Pair-Narrowing

When considering narrowing operators for numerical domains other slightly different notions of narrowing have been introduced in the literature, where different bounding constraints are considered: $x\Delta y$ is bound to be greater than $x \sqcap y$ and lower than x.

Definition 16 (lower-bound pair-narrowing [29]) *Let $(P, \leq)$ be a meet-semi-lattice. A lower-bound pair-narrowing operator is a binary operator $\Delta : P \times P \to P$ such that*

(i) Bounding: $\forall x, y \in P : (x \sqcap y) \leq (x\Delta y) \leq x$.

(ii) Termination: For every decreasing chain $x_0 \geq x_1 \geq \ldots$, the decreasing chain defined as

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

stabilizes after a finite number of terms.

Observe that not every pair-narrowing operator is also a lower-bound pair-narrowing. For example, the pair-narrowing of Example 5 doesn't satisfy the above condition.
When modifying the termination constraints in Definition 16, we get:

Definition 17 (strong lower-bound pair-narrowing [29]) *Let $(P, \leq)$ be a poset. A strong lower-bound pair narrowing operator is a binary operator $\Delta : P \times P \to P$ such that*

(i) Bounding: $\forall x, y \in P : (x \sqcap y) \leq (x\Delta y) \leq x$.

(ii) Termination: For every sequence $x_0 \geq x_1 \geq \ldots$, the decreasing chain defined as

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

stabilizes after a finite number of terms.

Example 10 *This notion of narrowing operator is introduced, for the octagon domain, in [28, 30], with the strong widening operator defined in Definition 14.*

Under particular conditions, the two notions of *pair-narrowing* and *strong lower-bound pair-narrowing* are equivalent.

Theorem 13 *Let $(P, \leq)$ be a meet-semi-lattice (the greatest lower bound $x \sqcap y$ exist for all $x.y \in L$) satisfying the descending chain condition (no strictly decreasing chain in L can be infinite). Let $\Delta : P \times P \to P$ be a pair-narrowing operator such that $x \Delta y = x \sqcap y$. Then Δ is a strong lower-bound pair-narrowing.*

Proof:

- *Bounding*: Consider $y \leq x$:

$$\begin{array}{lll} & x \geq x\Delta y \geq y & \text{by bounding property in Def. 13} \\ \Rightarrow & x \geq x\Delta y \geq x \sqcap y & \text{by the relation between } x \text{ and } y \end{array}$$

  This result is true for each $x,\ y \in P : x \leq y$, as request by bounding property in Def. 17.

- *Termination*: Consider the sequence $\{x_i\}_{0 \leq i \leq n}$ and the decreasing sequence

$$z_0 = x_0,\ z_{i+1} = x_0 \sqcap \ldots \sqcap x_{i+1}$$

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

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

  The induction step:

$$\begin{array}{rcll} h_{i+1} & = & h_i \Delta z_{i+1} & \text{by Def. of } \{h_j\}_{j \geq 0} \\ & = & y_i \Delta z_{i+1} & \text{by inductive hypothesis} \\ & = & (((x_0 \Delta x_1) \Delta \ldots) \Delta x_i) \Delta z_{i+1} & \text{by Def. of } \{y_j\}_{j \geq 0} \\ & = & (((x_0 \Delta x_1) \Delta \ldots) \Delta x_i) \Delta (x_0 \sqcap \ldots \sqcap x_{i+1}) & \text{by Def. of } \{z_j\}_{j \geq 0} \\ & = & (((x_0 \sqcap x_1) \sqcap \ldots) \sqcap x_i) \sqcap (x_0 \sqcap \ldots \sqcap x_{i+1}) & \text{by Def. of } \Delta \\ & = & (x_0 \sqcap \ldots \sqcap x_{i+1}) & \text{by properties of } \sqcap \\ & = & (((x_0 \Delta x_1) \Delta \ldots) \Delta x_i) \Delta x_{i+1} & \text{by Def. of } \Delta \\ & = & y_{i+1} & \text{by Def. of } \{y_j\}_{j \geq 0} \end{array}$$

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

□

We can bind pair-narrowing and lower-bound pair-narrowing throught next two theorems.

Theorem 14 *Let $(P, \leq)$ be a poset and Δ be a pair-narrowing (Def. 13).*
If $\forall v, w :\ v\Delta(v \sqcap w) = v\Delta w$, then Δ is a lower bound pair-narrowing (Def. 16).

Proof: We need to focus only on the bounding property. By Definition 13, of Δ, we know that

$$(x \geq y) \Longrightarrow (x \geq (x \Delta y) \geq y)$$

We consider $u, v \in P$, with $x = v$ and $y = v \sqcap w$.
Then we have

$$v \geq v\Delta(v \sqcap w) \geq v \sqcap w$$

By assumption, we have that $\forall v, w$

$$v\Delta(v \sqcap w) = v\Delta w$$

then we get

$$v \geq v\Delta w \geq v \sqcap w$$

That is the bounding property of lower-bound pair-narrowing operator. □

Theorem 15 *Let $(P, \leq)$ be a poset and Δ be a lower-bound pair-narrowing (Def. 16). Consider $x\Delta y$, it's simple to prove that $\forall x, y \in P : y \leq x$ than Δ is a pair-narrowing (Def. 13).*

Proof: We have, by Definition 16, of Δ:

$$(x \sqcap y) \leq (x\Delta y) \leq x$$

if we have that $y \leq x$ then $x \sqcap y = y$ by definition. Therefore

$$(y \leq x) \Longrightarrow y \leq x\Delta y \leq x$$

as requested by Def. 13. □

4 Widening and Narrowing Operators wrt Galois Insertions

Widening operators have already been used in order to derive abstract domains [34]. 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.

Theorem 16 *Let ∇ be a pair-widening operator on a complete lattice $(L, \leq)$ such that $\forall x, y \in L : x \leq y \Rightarrow x\nabla x \leq y\nabla y$. 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.*

Proof: According to Def. 8, we have to show that $(\gamma_{AL}, L, A, \alpha_{LA})$ is a Galois insertion, with γ_{AL} being the identity function. By Lemma 1, it is sufficient to prove that $\forall x \in L : x \leq \gamma_{AL}(\alpha_{LA}(x))$, and that $\forall a \in A : a = \alpha_{LA}(\gamma_{AL}(a))$.

$$\begin{array}{lll} \forall x \in L : & x \leq x\nabla x, & \text{by (i) of Def. 10} \\ \Rightarrow & x \leq \alpha_{LA}(x), & \text{by definition of } \alpha_{LA} \\ \Rightarrow & x \leq \gamma_{AL}(\alpha_{LA}(x)), & \text{as } \gamma_{AL} \text{ is the identity} \end{array}$$

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

□

A corresponding result can be obtained also for set-widening operators.

Theorem 17 *Let $\nabla_\star$ be a set-widening operator on a complete lattice $(L, \leq)$ such that $\nabla_\star(\{x\})$ is defined for each x in L, and such that $\forall x, y \in L : x \leq y \Rightarrow \nabla_\star(\{x\}) \leq \nabla_\star(\{y\})$. Let A be the set $\{\nabla_\star(\{x\}) \mid x \in L\}$. Consider the function $\alpha_{LA} : L \to A$ defined by $\alpha_{LA}(x) = \nabla_\star(\{x\})$. Then, α_{LA} is the lower adjoint of a Galois insertion between L and A, with the upper adjoint being the identity function.*

Proof: The proof is similar to the proof of Theorem 16. □

4.1 Widening, Narrowing and Abstraction

The following theorem shows that pair widening is preserved through abstraction.

Theorem 18 *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 $\forall d_1, d_2 \in D : d_1 \leq d_1 \nabla_{D} d_2$.

$$\begin{array}{rcll} \gamma_{DC}(d_1) & \leq & \gamma_{DC}(d_1)\nabla_{C}\gamma_{DC}(d_2) & \text{by (ii) of Def. 10} \\ \alpha_{CD}(\gamma_{DC}(d_1)) & \leq & \alpha_{CD}(\gamma_{DC}(d_1)\nabla_{C}\gamma_{DC}(d_2)) & \text{by monotonicity of } \alpha_{CD} \\ \alpha_{CD}(\gamma_{DC}(d_1)) & \leq & d_1\nabla_{D} d_2 & \text{by definition of } \nabla_{D} \\ d_1 & \leq & d_1\nabla_{D} d_2 & \text{as } G_{CD} \text{ is a Galois insertion.} \end{array}$$

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

- *Termination.* Consider the ascending chain $\{d_i\}_{i\geq 0}$ in D. Consider the corresponding ascending chain $\gamma_{DC}(d_0) \leq \gamma_{DC}(d_1) \leq \ldots$ 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, $\hat{y}_i = \alpha_{CD}(y_i)$.

  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,

$$\begin{array}{rcll} \hat{y}_{i+1} & = & \hat{y}_i \nabla_{D} d_{i+1} & \text{by definition of the sequence } \{\hat{y}_j\}_{j\geq 0}. \\ & = & \alpha_{CD}(y_i)\nabla_{D} d_{i+1} & \text{by inductive hypotesis} \\ & = & \alpha_{CD}(y_i)\nabla_{D}\alpha_{CD}(\gamma_{DC}(d_{i+1})) & \text{as } G_{CD} \text{ is a Galois insertion} \\ & = & \alpha_{CD}(y_i \nabla_{C}\gamma_{DC}(d_{i+1})) & \text{by definition of } \nabla_{D} \\ & = & \alpha_{CD}(y_{i+1}) & \text{by definition of the sequence } \{y_j\}_{j\geq 0}. \end{array}$$

□

A corresponding result can be obtained also for set-widening operators.

Theorem 19 *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 set-widening on C. The operator ∇_{*D} defined by $\forall S \in D$, $\nabla_{*D}(S) = \alpha_{CD}(\nabla_{*C}(\gamma_{DC}(S)))$ is a set-widening operator on D.*

Proof: The proof is similar to the proof of Theorem 18.

As a corollary of Theorem 18, we can prove that pair-widening operators are preserved also when projecting a cartesian product of lattices on one of its components.

Corollary 1 *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 operator $\nabla_{A} : A \times A \to A$ defined by*

$$a \nabla_{A} a' = \pi_1(\langle a, \top\rangle \nabla \langle a', \top\rangle)$$

is a pair-widening operator.

Proof: It is sufficient to observe that the monotone functions $\alpha : A \times D \to A$ and $\gamma : A \to A \times D$ defined by

$$\begin{array}{l} \forall (a, d) \in A \times D : \ \alpha(\langle a, d\rangle) = a \\ \forall a \in A : \ \gamma(a) = \langle a, \top\rangle \end{array}$$

form a Galois insertion between A and D. Therefore, by applying Theorem 18, the binary operator $\nabla' = \alpha(\gamma(a)\nabla\gamma(a'))$ is a pair widening operator on A. To conclude, it is sufficient to observe that $\nabla_{A} = \nabla'$. □

Similarly, also, we can prove that narrowing operators are preserved by abstraction.

Theorem 20 *Let C and D be two complete lattices, s.t. $G_{CD} = (\gamma_{DC}, C, D, \alpha_{CD})$ is a Galois insertion. Let Δ_{C} be a pair-narrowing on C. The binary operator Δ_{D} defined by $\forall d_1, d_2 \in D$, $d_1 \Delta_{D} d_2 = \alpha_{CD}(\gamma_{DC}(d_1)\Delta_{C}\gamma_{DC}(d_2))$ is a pair-narrowing operator on D.*

Proof:

- *Bounding.* Let us show that $\forall d_1, d_2 \in D : (d_1 \leq d_2) \Rightarrow (d_1 \leq d_2 \Delta_{_D} d_1 \leq d_2)$.

$$\begin{array}{rcccl}
\gamma_{_{DC}}(d_1) & \leq & \gamma_{_{DC}}(d_2)\Delta_{_C}\gamma_{_{DC}}(d_1) & \leq & \gamma_{_{DC}}(d_2) \\
 & & & & \text{by Def. 13} \\
\alpha_{_{CD}}(\gamma_{_{DC}}(d_1)) & \leq & \alpha_{_{CD}}(\gamma_{_{DC}}(d_2)\Delta_{_C}\gamma_{_{DC}}(d_1)) & \leq & \alpha_{_{CD}}(\gamma_{_{DC}}(d_2)) \\
 & & & & \text{by monotonicity of } \alpha_{_{CD}} \\
\alpha_{_{CD}}(\gamma_{_{DC}}(d_1)) & \leq & d_2\Delta_{_D}d_1 & \leq & \alpha_{_{CD}}(\gamma_{_{DC}}(d_2)) \\
 & & & & \text{by definition of } \Delta_{_D} \\
d_1 & \leq & d_2\Delta_{_D}d_1 & \leq & d_2 \\
 & & & & \text{as } G_{_{CD}} \text{ is a Galois insertion.}
\end{array}$$

- *Termination.* Consider the decreasing chain $\{d_i\}_{i\geq 0}$ in D. Consider the corresponding decreasing chain $\gamma_{_{DC}}(d_0) \geq \gamma_{_{DC}}(d_1) \geq \ldots$ in C. And consider the sequence $y_0 = \gamma_{_{DC}}(d_0)$, $y_{i+1} = y_i \Delta_{_C} \gamma_{_{DC}}(d_{i+1})$. As $\Delta_{_C}$ is a pair-narrowing operator, this descending sequence stabilizes after a finite number of terms. We have to show that also the sequence $\hat{y}_0 = d_0$, $\hat{y}_{i+1} = \hat{y}_i \Delta_{_D} d_{i+1}$ stabilizes after a finite number of terms. By induction, we prove that for each i, $\hat{y}_i = \alpha_{_{CD}}(y_i)$.

  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,

$$\begin{array}{rcll}
\hat{y}_{i+1} & = & \hat{y}_i \Delta_{_D} d_{i+1} & \text{by definition of the sequence } \{\hat{y}_j\}_{j\geq 0}. \\
 & = & \alpha_{_{CD}}(y_i) \Delta_{_D} d_{i+1} & \text{by inductive hypotesis} \\
 & = & \alpha_{_{CD}}(y_i) \Delta_{_D} \alpha_{_{CD}}(\gamma_{_{DC}}(d_{i+1})) & \text{as } G_{_{CD}} \text{ is a Galois insertion} \\
 & = & \alpha_{_{CD}}(y_i \Delta_{_C} \gamma_{_{DC}}(d_{i+1})) & \text{by definition of } \Delta_{_D} \\
 & = & \alpha_{_{CD}}(y_{i+1}) & \text{by definition of the sequence } \{y_j\}_{j\geq 0}.
\end{array}$$

□

A corresponding result holds also for set-narrowing operators.

Theorem 21 *Let C and D be two complete lattices, s.t. $G_{_{CD}} = (\gamma_{_{DC}}, C, D, \alpha_{_{CD}})$ is a Galois insertion. Let Δ_{*_C} be a set-narrowing on C. The operator Δ_{*_D} defined by $\forall S \in D$, $\Delta_{*_D}(S) = \alpha_{_{CD}}(\Delta_{*_C}(\gamma_{_{DC}}(S))$ is a set-narrowing operator on D.*

Proof: The proof is similar to the proof of Theorem 20.

As for widening operator, we can prove that pair-narrowing operators are preserved also when projecting a cartesian product of lattices on one of its components.

Corollary 2 *Let A and D be complete lattices, and let Δ be a pair-narrowing operator over the cartesian product $A \times D$. Let π_1 be the projection on the first argument. The binary operator $\Delta_{_A} : A \times A \to A$ defined by*

$$a \Delta_{_A} a' = \pi_1(\langle a, \top \rangle \Delta \langle a', \top \rangle)$$

is a pair-narrowing operator.

Proof: It is sufficient to observe that the monotone functions $\alpha : A \times D \to A$ and $\gamma : A \to A \times D$ defined by

$$\begin{array}{l}
\forall (a, d) \in A \times D : \ \alpha(\langle a, d \rangle) = a \\
\forall a \in A : \ \gamma(a) = \langle a, \top \rangle
\end{array}$$

form a Galois insertion between $A \times D$ and D. Therefore, by applying Theorem 20, the binary operator $\Delta' = \alpha(\gamma(a) \Delta \gamma(a'))$ is a pair narrowing operator on A. To conclude, it is sufficient to observe that $\Delta_{_A} = \Delta'$. □

4.2 Widening, Narrowing and Reduced Product

A very important operator for combining abstract domains in Abstract Interpretation, is the *reduced product* [13]. We have already seen in Theorem 5 and in Theorem 6 that the pair-widening and pair-narrowing operators can be combined when considering the cartesian product of two posets. Unfortunately, this result cannot be fully extended to the reduced product, due to the fact that pair-widening and pair-narrowing operators in general are not required to be monotone. However, getting results relating widening and narrowing operators in case of reduced product may have great impact on abstract domains used for the analysis of critical software. For instance, the octagon domain [30] can be seen as the reduced product of $2n^2$ abstract domains, each one of them focusing on an invariant of the form $\pm x \pm y \leq c$.

Definition 18 *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*:$A \times D \to A \times D$ defined by* $\text{reduce}(\langle a, d\rangle) = \sqcap\{\langle a', d'\rangle \mid \gamma_{AC}(a) \sqcap \gamma_{DC}(d) = \gamma_{AC}(a') \sqcap \gamma_{DC}(d')\}$
The reduced product $A \sqcap D$ is defined as follows:

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

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

We can prove (Lemma 6) that by combining two pair-widening operators in the reduced product at least covering is preserved, i.e. we can obtain an extrapolation operator (which does not necessarily terminate on ascending sequences, see for instance the domain of octagons [30]). The following auxiliary Lemma says that *reduce* behaves well with respect to the ordering in the reduced product $A \sqcap D$.

Lemma 5 *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. For $\hat{a} \in A, \hat{d} \in D$, $\langle a, d\rangle \in A \sqcap D$, if $a \leq \hat{a}$ and $d \leq \hat{d}$, then $\langle a, d\rangle \leq \text{reduce}(\langle \hat{a}, \hat{d}\rangle)$.*

Proof: By $\sqcap$ properties and monotonicity of γ 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 upper adjoint of the Galois insertion $(\gamma, C, A \sqcap D, \alpha)$ as in Def. 18.
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

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

□

Lemma 6 *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 $\bullet : (A \sqcap D) \times (A \sqcap D) \to (A \sqcap D)$ 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.

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

$$\begin{array}{lcll} & \langle a, d\rangle & \leq & \langle a \nabla_A a', d \nabla_D d'\rangle & \text{by covering of } \nabla_A, \nabla_D \\ \Rightarrow & \langle a, d\rangle & \leq & reduce(\langle a \nabla_A a', d \nabla_D d'\rangle) & \text{by Lemma 5} \\ \Rightarrow & \langle a, d\rangle & \leq & \langle a, d\rangle \bullet \langle a', d'\rangle & \text{by definition of } \bullet. \end{array}$$

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

The last Theorem shows that if the pairwise application of the pair-widening operators is always an element of the reduced product, the extrapolator of Lemma 6 enjoys also the termination property, thus resulting into a pair-widening operator too.

Theorem 22 *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 $\nabla : (A \sqcap D) \times (A \sqcap D) \to (A \sqcap D)$ defined by $\forall \langle a, d \rangle, \langle a', d' \rangle \in A \sqcap D : \langle a, d \rangle \nabla \langle a', d' \rangle =$ reduce$(\langle a \nabla_A a', d \nabla_D d' \rangle)$ is a pair-widening operator.

Proof: By Lemma 6, we need to focus only on the termination property.
Consider the increasing sequence $\langle a_0, d_0 \rangle \leq \langle a_1, d_1 \rangle \ldots$ 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 $a_0 \leq a_1 \leq \ldots$ in A, and the increasing sequence $d_0 \leq d_1 \leq \ldots$ 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 $\forall i : \langle a'_i, d'_i \rangle = \langle \hat{a}_i, \hat{d}_i \rangle$.

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:

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

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 $\{\hat{d}_j\}_{j \geq 0}$. □

For narrowing operators, we can define a theorem corresponding to theorem 22. Also in this case we need some auxiliary lemma.

Lemma 7 *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. For $a \in A$, $d \in D$, reduce$(\langle a, d \rangle) \leq \langle a, d \rangle$.*

Proof: By Def. 18: *reduce*$(\langle a, d \rangle) = \sqcap S$, where $S = \{\langle a', d' \rangle \mid \gamma_{AC}(a) \sqcap \gamma_{DC}(d) = \gamma_{AC}(a') \sqcap \gamma_{DC}(d')\}$. We know that $\langle a, d \rangle \in S$ and that all elements of S are comparable, than *reduce*$(\langle a, d \rangle) \leq \langle a, d \rangle$. □

Lemma 8 *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. For $\hat{a} \in A, \hat{d} \in D$, $\langle a, d \rangle \in A \sqcap D$, if $\hat{a} \leq a$ and $\hat{d} \leq d$, then* reduce$(\langle \hat{a}, \hat{d} \rangle) \leq \langle a, d \rangle$.

Proof: By $\sqcap$ properties and monotonicity of γ functions, $\gamma_{AC}(a) \sqcap \gamma_{DC}(d) \geq \gamma_{AC}(\hat{a}) \sqcap \gamma_{DC}(\hat{d})$. Therefore, *reduce*$(\langle \hat{a}, \hat{d} \rangle)$ is such that

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

where γ is the upper adjoint of the Galois insertion $(\gamma, C, A \sqcap D, \alpha)$ as in Def. 18.
By applying α to both expressions, by monotonicity of α we get

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

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

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

□

Theorem 23 *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 Δ_A and Δ_D be pair-narrowing operators defined on the lattice A and D, respectively, such that $\forall \langle a, d\rangle \in A \sqcap D$, $\forall a' \in A$, $\forall d' \in D : \langle a \Delta_A a', d \Delta_D d'\rangle \in A \sqcap D$.
Then the binary operator $\Delta : (A \sqcap D) \times (A \sqcap D) \to (A \sqcap D)$ defined by $\forall \langle a, d\rangle, \langle a', d'\rangle \in A \sqcap D : \langle a, d\rangle \Delta \langle a', d'\rangle =$ reduce$(\langle a \Delta_A a', d \Delta_D d'\rangle)$ is a pair-narrowing operator.

Proof:

- *Bounding* We have to show that $\forall \langle a, d\rangle, \langle a', d'\rangle \in A \sqcap D$, $(\langle a, d\rangle \leq \langle a', d'\rangle) \Rightarrow (\langle a, d\rangle \leq \langle a, d\rangle \Delta \langle a', d'\rangle \leq \langle a', d'\rangle)$

$$\begin{array}{lcccll} \langle a, d\rangle & \leq & \langle a \Delta_A a', d \Delta_D d'\rangle & \leq & \langle a', d'\rangle & \text{by bounding of } \Delta_A \text{ and } \Delta_D \\ \langle a, d\rangle & \leq & \mathit{reduce}(\langle a \Delta_A a', d \Delta_D d'\rangle) & \leq & \langle a', d'\rangle & \text{by Lemma 5 and Lemma 7 or Lemma 8} \\ \langle a, d\rangle & \leq & \langle a, d\rangle \Delta \langle a', d'\rangle & \leq & \langle a', d'\rangle & \text{by definition of } \Delta \end{array}$$

- *Termination* Consider the increasing sequence $\langle a_0, d_0\rangle \leq \langle a_1, d_1\rangle \ldots$ 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 $a_0 \leq a_1 \leq \ldots$ in A, and the increasing sequence $d_0 \leq d_1 \leq \ldots$ in D. By the termination property of Δ_A and Δ_D, we know that the corresponding sequences $\hat{a}_0 = a_0$, $\hat{a}_{i+1} = \hat{a}_i \Delta_A a_{i+1}$, and $\hat{d}_0 = d_0$, $\hat{d}_{i+1} = \hat{d}_i \Delta_D d_{i+1}$ stabilize after a finite number of terms.

  We show by induction that the increasing sequence $\langle a'_0, d'_0\rangle = \langle a_0, d_0\rangle$, $\langle a'_{i+1}, d'_{i+1}\rangle = \langle a'_i, d'_i\rangle \Delta \langle a_{i+1}, d_{i+1}\rangle$ is such that $\forall i : \langle a'_i, d'_i\rangle = \langle \hat{a}_i, \hat{d}_i\rangle$.

  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:

$$\begin{array}{lcll} \langle a'_{i+1}, d'_{i+1}\rangle & = & \langle a'_i, d'_i\rangle \Delta \langle a_{i+1}, d_{i+1}\rangle & \text{by definition of } \{\langle a'_j, d'_j\rangle\}_{j \geq 0} \\ & = & \text{reduce}(a'_i \Delta_A a_{i+1}, d'_i \Delta_D d_{i+1}) & \text{by def. of } \Delta \\ & = & \langle \hat{a}_i \Delta_A a_{i+1}, \hat{d}_i \Delta_D d_{i+1}\rangle & \text{by the hypothesis} \\ & = & \langle \hat{a}_{i+1}, \hat{d}_{i+1}\rangle & \text{by def. of } \{\hat{a}_j\}_{j \geq 0} \text{ and } \{\hat{d}_j\}_{j \geq 0} \end{array}$$

  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 $\{\hat{d}_j\}_{j \geq 0}$

□

We can also obtain the corresponding results for set-widening and set-narrowing operators.

Theorem 24 *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 set-widening operators defined on the lattice A and D, respectively, such that $\forall S \subseteq A \sqcap D$, $\langle \nabla_{*A}(\{a_i \mid \langle a_i, d_i\rangle \in S\}), \nabla_D(\{d_i \mid \langle a_i, d_i\rangle \in S\})\rangle \in A \sqcap D$.
Then the operator $\nabla_* : \wp(A \sqcap D) \nrightarrow (A \sqcap D)$ defined by $\forall S \subseteq A \sqcap D : \nabla_*(\{S\}) =$ reduce$(\langle \nabla_{*A}(\{a_i \mid \langle a_i, d_i\rangle \in S\}), \nabla_{*D}(\{d_i \mid \langle a_i, d_i\rangle \in S\})\rangle)$ is a set-widening operator.

Theorem 25 *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 Δ_{*A} and Δ_{*D} be set-narrowing operators defined on the lattice A and D, respectively, such that $\forall S \subseteq A \sqcap D$, $\langle \Delta_{*A}(\{a_i \mid \langle a_i, d_i\rangle \in S\}), \Delta_{*D}(\{d_i \mid \langle a_i, d_i\rangle \in S\})\rangle \in A \sqcap D$.
Then the operator $\Delta_* : \wp(A \sqcap D) \nrightarrow (A \sqcap D)$ defined by $\forall S \subseteq A \sqcap D : \Delta_*(\{S\}) =$ reduce$(\langle \Delta_{*A}(\{a_i \mid \langle a_i, d_i\rangle \in S\}), \Delta_{*D}(\{d_i \mid \langle a_i, d_i\rangle \in S\})\rangle)$ is a set-narrowing operator.

The proofs of these Theorems are similar to Theorem 22 and Theorem 23, respectively.

5 Conclusions and Future Work

We investigated which properties are necessary to support a systematic design of widening and narrowing operators. As far as we know, this is the first attempt to provide a general comparison of the different notions of widening and narrowing 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 defined on abstract domains where only the concretization function is available or where the least upper bound operator is not always defined. We are currently investigating how to enhance domains and widening and narrowing operators with suitable metrics that allow to get a quantitative comparison of their precision and/or of their speed to reach a fixed-point.
Notice that most of the papers in the literature use only the widening operator without defining any corresponding narrowing operator; it would be interesting to investigate narrowing operators to analyse the resulting improvements with respect to accuracy already mentioned. For instance, for the abstract domain $LInt$ whose elements on linear inequations with interval coefficients [32]. Narrowing operator can be defined on the lines of Example 5 that may improve the overall precision of the analysis.

Aknowledgments

Work partially supported by MIUR Project PRIN 2007 "SOFT" and by RAS project TESLA - Tecniche di enforcement per la sicurezza dei linguaggi e delle applicazioni.

References

[1] R. Bagnara, P. M. Hill, E. Ricci, and E. Zaffanella. Precise widening operators for convex polyhedra. *Science of Computer Programming*, 58(1-2):28–56, 2005.

[2] R. Bagnara, P. M. Hill, and E. Zaffanella. Widening operators for powerset domains. *Software Tools for Technology Transfer*, 8(4/5):449–466, 2006.

[3] Roberto Bagnara, Patricia M. Hill, Elena Mazzi, and Enea Zaffanella. Widening operators for weakly-relational numeric abstractions. In *Static Analysis: Proceedings of the 12th International Symposium, volume 3672 of Lecture Notes in Computer Science*, pages 3–18. SpringerVerlag, 2005.

[4] Gareth Birkhoff. *Lattice Theory*. American Mathematical Society Colloquium Publications, Rhode Island, 1973.

[5] Bruno Blanchet, Patrick Cousot, Radhia Cousot, Jérome Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, and Xavier Rival. A static analyzer for large safety-critical software. In *PLDI '03: Proc. of the ACM SIGPLAN 2003 conference on Programming language design and implementation*, pages 196–207, 2003.

[6] Tae-Hyoung Choi, Oukseh Lee, Hyunha Kim, and Kyung-Goo Doh. A practical string analyzer by the widening approach. In *APLAS*, pages 374–388, 2006.

[7] Agostino Cortesi. Widening operators for abstract interpretation. In *SEFM '08: Proceedings of the 2008 Sixth IEEE International Conference on Software Engineering and Formal Methods*, pages 31–40, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[8] Agostino Cortesi, Baudouin Le Charlier, and Pascal Van Hentenryck. Combinations of abstract domains for logic programming: open product and generic pattern construction. *Science of Computer Programming*, 38(1–3):27–71, 2000.

[9] Agostino Cortesi, Gilberto Filé, Francesco Ranzato, Roberto Giacobazzi, and Catuscia Palamidessi. Complementation in abstract interpretation. *ACM Trans. Program. Lang. Syst.*, 19(1):7–47, 1997.

[10] Agostino Cortesi, Gilberto Filé, and William Winsborough. The quotient of an abstract interpretation. *Theoretical Computer Science*, 202(1-2):163 – 192, 1998.

[11] P. Cousot. Proving the absence of run-time errors in safety-critical avionics code. In C. Kirsch and R. Wilhelm, editors, *Proc. 7th ACM & IEEE International Conference on Embedded Sofware, Embedded Systems, (EMSOFT 2007)*, pages 7–9, Salzburg, Austria, 2007. ACM press.

[12] P. Cousot and R. Cousot. Static determination of dynamic properties of programs. In *Proceedings of the Second International Symposium on Programming*, pages 106–130. Dunod, Paris, France, 1976.

[13] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the Sixth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 269–282, San Antonio, Texas, 1979. ACM Press, New York, NY.

[14] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *6th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '79)*, pages 269–282. ACM Press, 1979.

[15] P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of Logic and Computation*, 2(4):511–547, August 1992.

[16] P. Cousot and R. Cousot. Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. In *Proc. Int. Workshop on Programming Language Implementation and Logic Programming*, volume 631 of *LNCS*, pages 269–295. Springer-Verlag, 1992.

[17] P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *5th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 84–97. ACM Press, 1978.

[18] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, Cambridge, 1990.

[19] Vijay D'Silva. Widening for automata. In *PhD thesis, Institut fur Informatik, Universitaat Zurich*, 2006.

[20] Vijay D'Silva, Mitra Purandare, and Daniel Kroening. Approximation refinement for interpolation-based model checking. In *VMCAI*, 2008.

[21] Jérôme Feret. Static analysis of digital filters. In *European Symposium on Programming (ESOP'04)*, number 2986 in LNCS. Springer-Verlag, 2004.

[22] Roberto Giacobazzi and Francesco Ranzato. The reduced relative power operation on abstract domains. *Theoretical Computer Science*, 216(1-2):159 – 211, 1999.

[23] P. Granger. Static analysis of linear congruence equalities among variables of a program. In *Int. Joint Conference on Theory and Practice of Software Development (TAPSOFT'91)*, volume 464 of *LNCS*, pages 169–192. Springer-Verlag, April 1991.

[24] P. Granger. Improving the results of static analyses programs by local decreasing iteration. In *Proceedings of FSTTCS*, volume 652 of *Lectures Notes in Computer Science*, pages 68–79. Springer-Verlag, 1992.

[25] Pascal Van Hentenryck, Agostino Cortesi, and Baudouin Le Charlier. Type analysis of prolog using type graphs. In *SIGPLAN Conference on Programming Language Design and Implementation*, pages 337–348, 1994.

[26] K. Rustan M. Leino and Francesco Logozzo. Using widenings to infer loop invariants inside an smt solver, or: A theorem prover as abstract domain. In *Workshop on Invariant Generation (WING 2007), Hagenberg, Austria, June 25-26*, 2007.

[27] Francesco Logozzo and Manuel Fahndrich. A weakly relational domain for the efficient validation of array accesses. In *23th ACM Symposium on Applied Computing (SAC 2008), Fortaleza, Brazil*, 2008.

[28] A. Miné. The octagon abstract domain. In *AST 2001 in WCRE 2001*, IEEE, pages 310–319. IEEE CS Press, October 2001.

[29] A. Miné. *Weakly Relational Numerical Abstract Domains*. PhD thesis, École Polytechnique, Palaiseau, France, December 2004. `http://www.di.ens.fr/~mine/these/these-color.pdf`.

[30] A. Miné. The octagon abstract domain. *Higher-Order and Symbolic Computation*, 19(1):31–100, 2006.

[31] F. Nielson, Riis H. Nielson, and C. L. Hankin. *Principles of Program Analysis*. Springer, second printing, 2005 edition, 1999.

[32] Viswanath Ramachandran, Pascal Van Hentenryck, and Agostino Cortesi. Abstract domains for reordering clp(rlin) programs. *J. Log. Program.*, 42(3):217–256, 2000.

[33] Xavier Rival and Laurent Mauborgne. The trace partitioning abstract domain. *ACM Trans. Program. Lang. Syst.*, 29(5):7–47, 2007.

[34] Arnaud Venet. Abstract cofibered domains: Application to the alias analysis of untyped programs. In *Proc. of the 3rd Int. Symposium on Static Analysis (SAS 96)*, pages 366–382. Springer-Verlag, 1996.