

Complementation in Abstract Interpretation

G. Filé, R. Giacobazzi, F. Ranzato et al.

presented by: Zuzana Baranová

30th October 2017

Reduced Product

Domain Product

$$D_1 \times D_2 \rightarrow (D_1, D_2)$$

$$(\text{range}) \times \{\text{even, odd}\} \rightarrow ([0,6], \text{odd})$$

Reduced Product

Domain Product

$$D_1 \times D_2 \rightarrow (D_1, D_2)$$

$$(\text{range}) \times \{\text{even, odd}\} \rightarrow ([0,6], \text{odd}) \rightarrow ([1,5], \text{odd})$$

Reduced Product

Domain Product

$$D_1 \times D_2 \rightarrow (D_1, D_2)$$

$$(\text{range}) \times \{\text{even, odd}\} \rightarrow ([0,6], \text{odd}) \rightarrow ([1,5], \text{odd})$$

- the domain product is a *standalone abstract domain*

Reduced Product

Domain Product

$$D_1 \times D_2 \rightarrow (D_1, D_2)$$

$$(\text{range}) \times \{\text{even, odd}\} \rightarrow ([0,6], \text{odd}) \rightarrow ([1,5], \text{odd})$$

- the domain product is a *standalone abstract domain*

Reduced Product

- the most precise refinement of the Cartesian product
- let the information flow among the domains to mutually refine them

Galois Connection vs. Insertion

(γ, D, C, α) is an **insertion**:

$$\alpha \circ \gamma = \lambda x.x$$

then:

- α is *surjective*
- γ is *injective*

(Upper) Closure Operator

poset = set + partial order \leq

for a poset P , a function $cl :: P \rightarrow P$, which satisfies

\forall elements $x, y \in P$:

- $x \subseteq cl(x)$ *extensive*
- $x \subseteq y \implies cl(x) \subseteq cl(y)$ *increasing*
- $cl(x) = cl(cl(x))$ *idempotent*

Galois Insertion vs. Closure Operators

- D is an abstraction of C if there exist α and γ s.t. (γ, D, C, α) is a Galois insertion
- an abstract domain is "its image in the concrete domain"
- if (γ, D, C, α) is a G.i., then the closure associated with D is the operator $\rho_D = \gamma \circ \alpha$ on C

Closure Operators

$uco(C)$

- C - complete lattice
- $uco(C)$ - complete lattice of all closure operators on C

D is an abstraction of C ($C \trianglelefteq D$)

$\implies D \cong \rho_D(C)$ for some closure $\rho_D \in uco(C)$

Closure Operators

$$uco(C)$$

- C - complete lattice
- $uco(C)$ - complete lattice of all closure operators on C

D is an abstraction of C ($C \trianglelefteq D$)

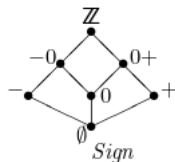
$\implies D \cong \rho_D(C)$ for some closure $\rho_D \in uco(C)$

- $uco(C)$ - complete lattice of its abstract interpretations
- .. compared w/ regard to their precision of representation

Reduced Product

given two abstract domains A and B (abstracting C)

$$A \sqcap B = glb(uco(C))$$



Complementation

- inverse operation to *reduced product* of abstract domains
- A, B - abstract domains, B more abstract than A
gives as result the most abstract domain $A \sim B$, whose
reduced product with B is exactly A
- allows to *decompose* a. domains into simpler factors

Complemented Lattice

- bounded lattice (least element 0, greatest element 1)
- every element a has a complement b ,
s.t. $a \vee b = 1$ and $a \wedge b = 0$

Complemented Lattice

- bounded lattice (least element 0, greatest element 1)
- every element a has a complement b ,
s.t. $a \vee b = 1$ and $a \wedge b = 0$
- $uco(C)$ is complemented (equiv. distributive) iff C is a complete well-ordered chain

Complemented Lattice

- bounded lattice (least element 0, greatest element 1)
- every element a has a complement b ,
s.t. $a \vee b = 1$ and $a \wedge b = 0$
- $uco(C)$ is complemented (equiv. distributive) iff C is a complete well-ordered chain [15,23]¹

¹[15] P. Dwinger. On the closure operators on a complete lattice.

[23] J. Morgado. Note on complemented closure operators of complete lattices.

Complemented Lattice

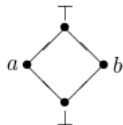
- bounded lattice (least element 0, greatest element 1)
- every element a has a complement b ,
s.t. $a \vee b = 1$ and $a \wedge b = 0$
- $uco(C)$ is complemented (equiv. distributive) iff C is a complete well-ordered chain
- too restrictive for abstract interpretation

Complementation

for a lattice L :

- each closure operator ρ is uniquely determined by the set of its fixpoints, which is its image $\rho(L)$
- a set $X \subseteq L$ is the set of fixpoints of a closure operator iff X is a Moore-family of L ; i.e. $\top \in X$ and X is meet-closed

Example



$$\rho_1 = \{\top\}$$

$$\rho_2 = \{\top, a\}$$

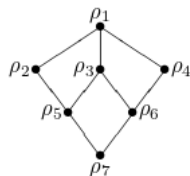
$$\rho_3 = \{\top, \perp\}$$

$$\rho_4 = \{\top, b\}$$

$$\rho_5 = \{\top, a, \perp\}$$

$$\rho_6 = \{\top, b, \perp\}$$

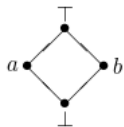
$$\rho_7 = \{\top, a, b, \perp\}$$



Pseudo-complement

- "calling abusively complement of an abstract interpretation the pseudo-complement of its associated closure operator"
- for a meet-semilattice L and $x \in L$:
 x^* such that $x \wedge x^* = \perp$
 $\forall y \in L. (x \wedge y = \perp) \implies (y \preceq x^*)$
- for a complete lattice L :
 $x^* = \vee \{y \in L \mid x \wedge y = \perp\}$

Example



$$\rho_1^* =$$

$$\rho_2^* =$$

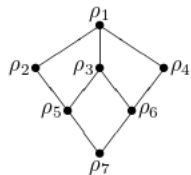
$$\rho_3^* =$$

$$\rho_4^* =$$

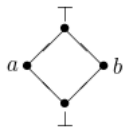
$$\rho_5^* =$$

$$\rho_6^* =$$

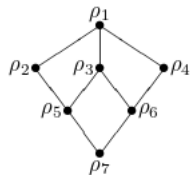
$$\rho_7^* =$$



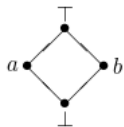
Example



$$\begin{aligned}\rho_1^* &= \\ \rho_2^* &= \\ \rho_3^* &= \\ \rho_4^* &= \rho_2 \\ \rho_5^* &= \\ \rho_6^* &= \\ \rho_7^* &= \end{aligned}$$



Example



$$\rho_1^* = \rho_7$$

$$\rho_2^* = \rho_4$$

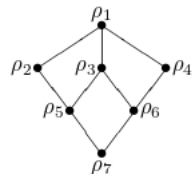
$$\rho_3^* = \rho_7$$

$$\rho_4^* = \rho_2$$

$$\rho_5^* = \rho_4$$

$$\rho_6^* = \rho_2$$

$$\rho_7^* = \rho_1$$



Pseudo-complement

- let B be an abstract domain abstracting another abstract domain A ($A \sqsubseteq B$)
- if A is pseudo-complemented, then the complement of B relative to A is the pseudo-complement B^*
- we denote this complement $A \sim B$
- $(A \sim B) \times B = A$
- shows which properties representable by A are ignored by the abstraction B

Chain-inf Distributivity

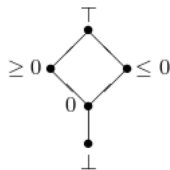
$uco(C)$ is pseudo-complemented $\iff C$ is *chain-inf distributive*
for any chain $C \subseteq L$ and for each $x \in L$

$$x \wedge (\vee C) = \vee_{y \in C} (x \wedge y)$$

Domain Decomposition

- A *decomposition* of a domain is a tuple $\langle D_i \rangle_{i \in I}$ such that $D = \sqcap_{i \in I} D_i$
- each D_i is an abstraction of D

Domain Decomposition



$$\rho_1 = \{T\}$$

$$\rho_2 = \{T, \geq 0\}$$

$$\rho_3 = \{T, 0\}$$

$$\rho_4 = \{T, \perp\}$$

$$\rho_5 = \{T, \leq 0\}$$

$$\rho_6 = \{T, \geq 0, \perp\}$$

$$\rho_7 = \{T, \geq 0, 0\}$$

$$\rho_8 = \{T, 0, \perp\}$$

$$\rho_9 = \{T, \leq 0, 0\}$$

$$\rho_{10} = \{T, \leq 0, \perp\}$$

$$\rho_{11} = \{T, \geq 0, 0, \perp\}$$

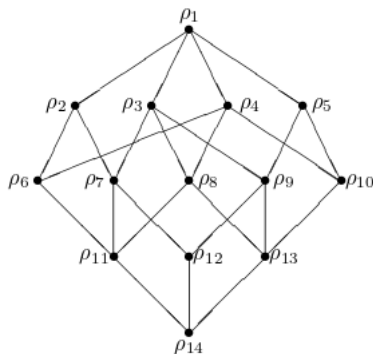
$$\rho_{12} = \{T, \leq 0, \geq 0, 0\}$$

$$\rho_{13} = \{T, \leq 0, 0, \perp\}$$

$$\rho_{14} = D$$

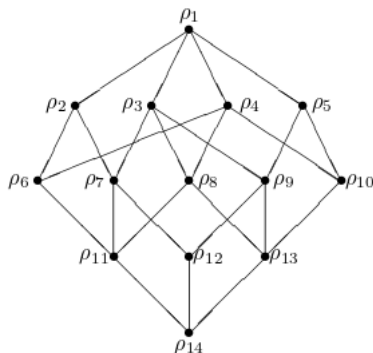
Domain Decomposition

$\rho_1 = \{\top\}$; $\rho_2 = \{\top, \geq 0\}$; $\rho_3 = \{\top, 0\}$; $\rho_4 = \{\top, \perp\}$; $\rho_5 = \{\top, \leq 0\}$;
 $\rho_6 = \{\top, \geq 0, \perp\}$; $\rho_7 = \{\top, \geq 0, 0\}$; $\rho_8 = \{\top, 0, \perp\}$; $\rho_9 = \{\top, \leq 0, 0\}$;
 $\rho_{10} = \{\top, \leq 0, \perp\}$; $\rho_{11} = \{\top, \geq 0, 0, \perp\}$; $\rho_{12} = \{\top, \leq 0, \geq 0, 0\}$;
 $\rho_{13} = \{\top, \leq 0, 0, \perp\}$; $\rho_{14} = \{\top, \geq 0, \leq 0, 0, \perp\}$



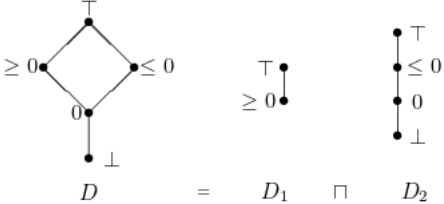
Domain Decomposition

$\rho_1 = \{\top\}$; $\rho_2 = \{\top, \geq 0\}$; $\rho_3 = \{\top, 0\}$; $\rho_4 = \{\top, \perp\}$; $\rho_5 = \{\top, \leq 0\}$;
 $\rho_6 = \{\top, \geq 0, \perp\}$; $\rho_7 = \{\top, \geq 0, 0\}$; $\rho_8 = \{\top, 0, \perp\}$; $\rho_9 = \{\top, \leq 0, 0\}$;
 $\rho_{10} = \{\top, \leq 0, \perp\}$; $\rho_{11} = \{\top, \geq 0, 0, \perp\}$; $\rho_{12} = \{\top, \leq 0, \geq 0, 0\}$;
 $\rho_{13} = \{\top, \leq 0, 0, \perp\}$; $\rho_{14} = \{\top, \geq 0, \leq 0, 0, \perp\}$

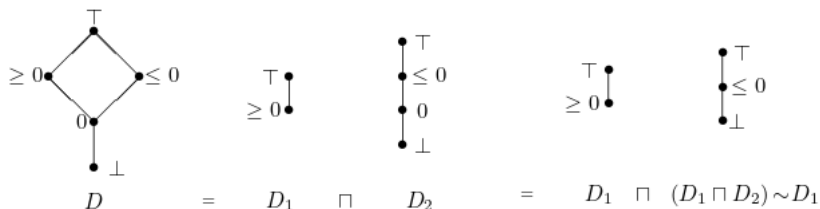


$\rho_1^* = \rho_{14}$; $\rho_2^* = \rho_{10}$; $\rho_3^* = \rho_{14}$; $\rho_4^* = \rho_{12}$; $\rho_5^* = \rho_6$; $\rho_6^* = \rho_5$;
 $\rho_7^* = \rho_{10}$; $\rho_8^* = \rho_{12}$; $\rho_9^* = \rho_6$; $\rho_{10}^* = \rho_2$; $\rho_{11}^* = \rho_5$; $\rho_{12}^* = \rho_4$;
 $\rho_{13}^* = \rho_2$; $\rho_{14}^* = \rho_1$

Domain Decomposition



Domain Decomposition



Sharing

- complementation used to characterize what is left when we eliminate from it the information useful for ground-dependency analysis (expressed by a more abstract domain Def)
- the complement of Def w/ respect to $Sharing$, called $Sharing^+$, captures precisely variable aliasing and no ground-dependency information