Domain Compression for Complete Abstractions

Roberto Giacobazzi and **Isabella Mastroeni**

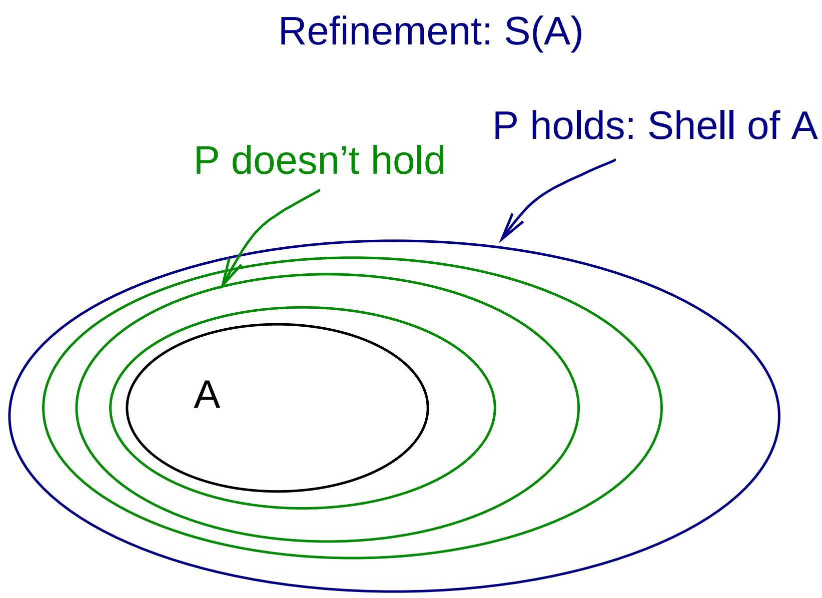
Dipartimento di Informatica

Università degli Studi di Verona

VMCAI'03

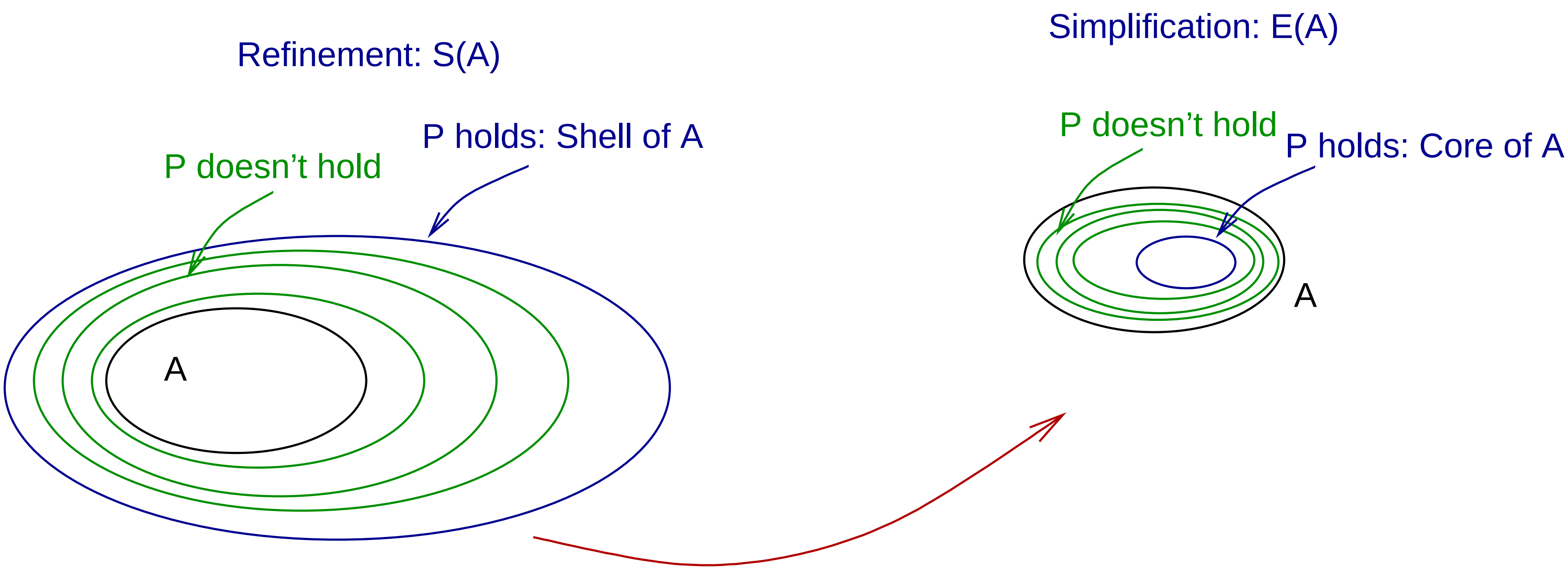
Domain Transformers

Transform domains in order to make them satisfy a property P.



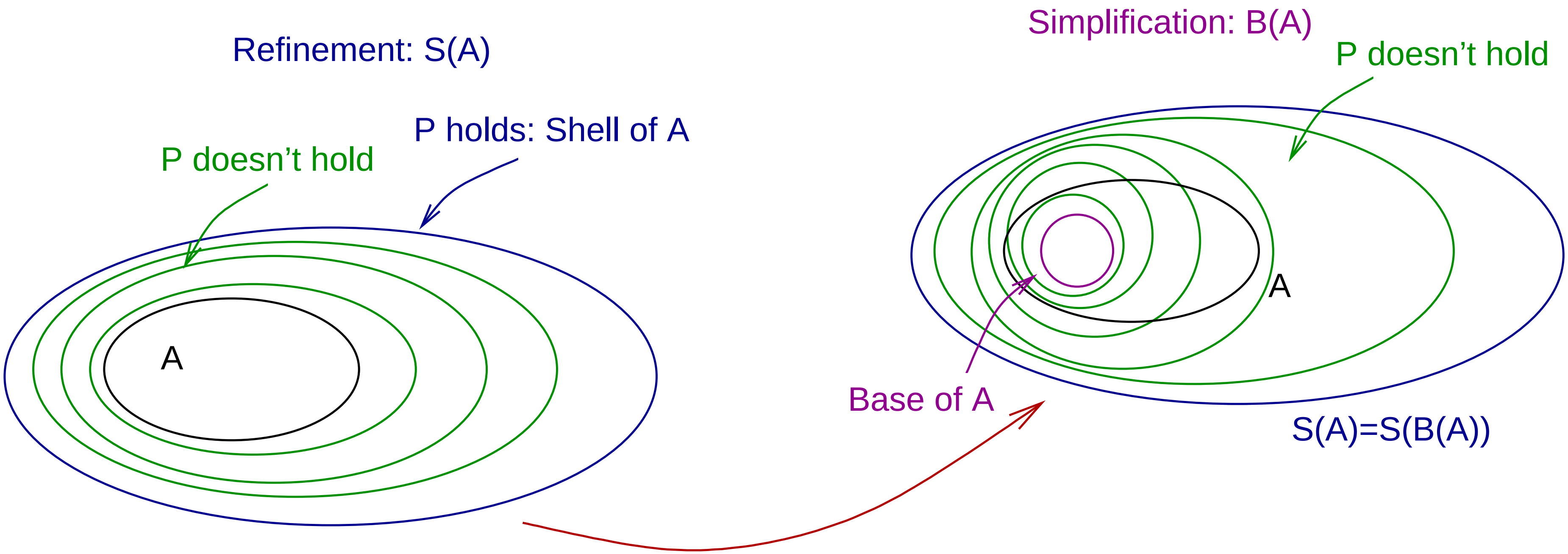
Domain Transformers

Transform domains in order to make them satisfy a property P.



Domain Transformers

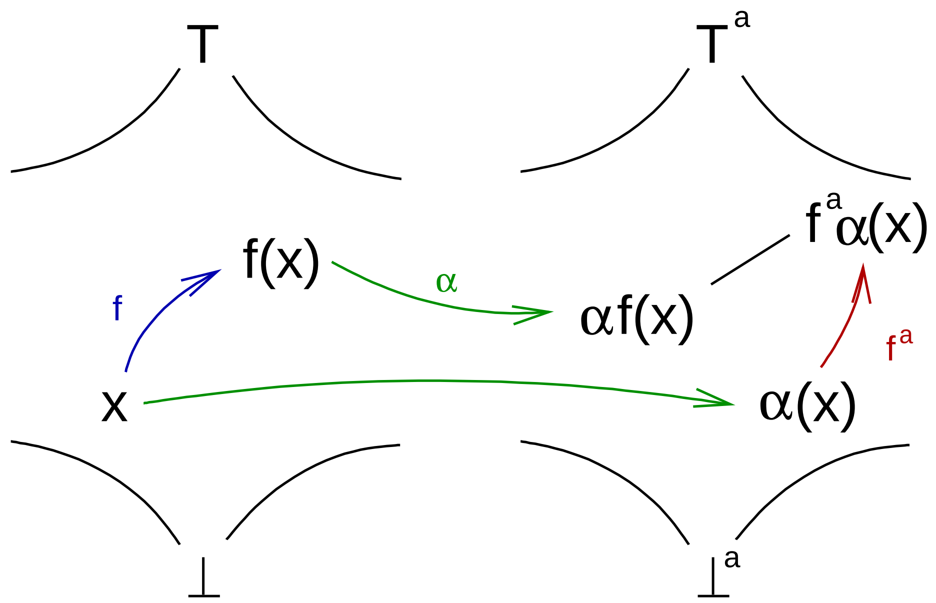
Transform domains in order to make them satisfy a property P.



Completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and ρ=$\gamma \circ \alpha$

f^a correct for f



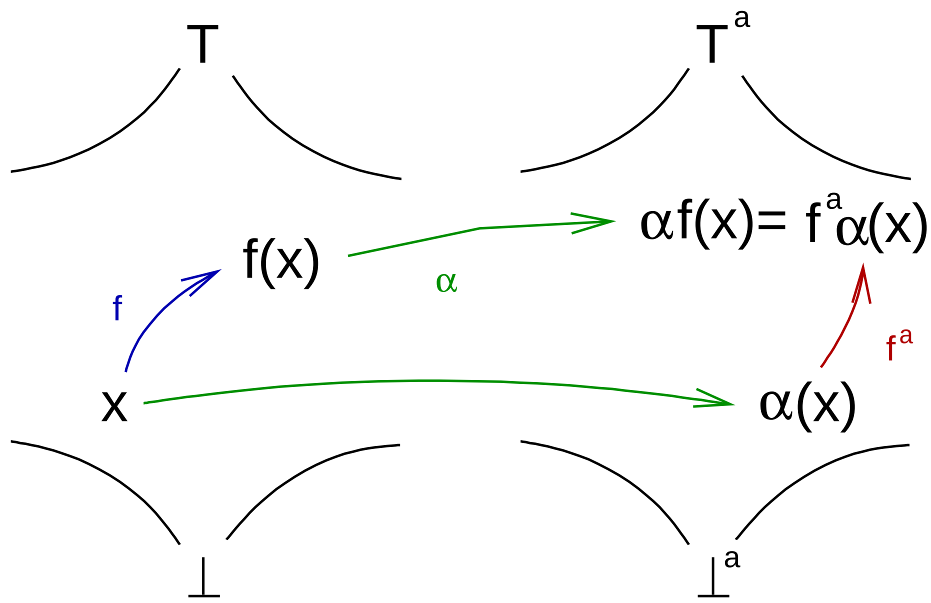
Completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and $\rho = \gamma \circ \alpha$

f^a B−complete for f

|||

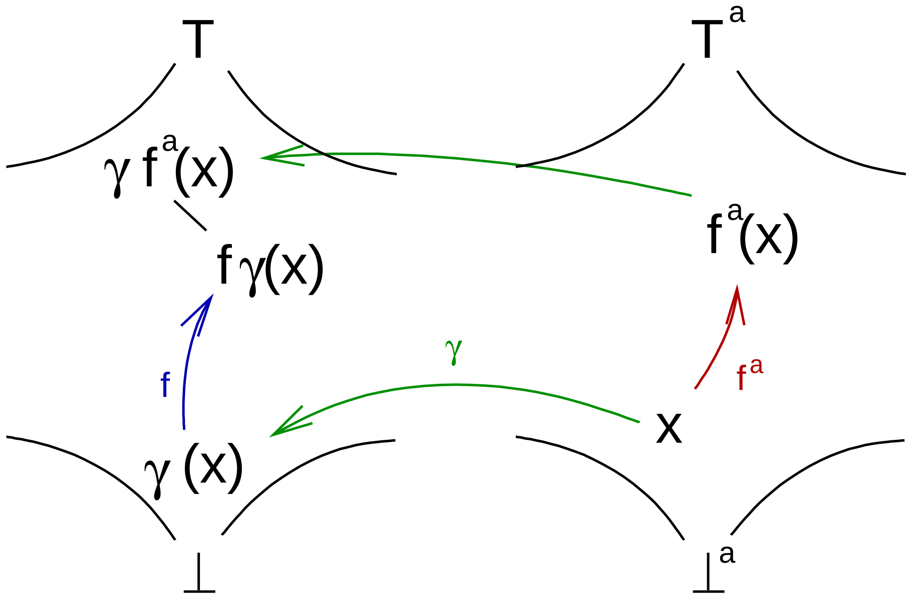
$\rho f = \rho f \rho$



Completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and $\rho = \gamma \circ \alpha$

f^a correct for f



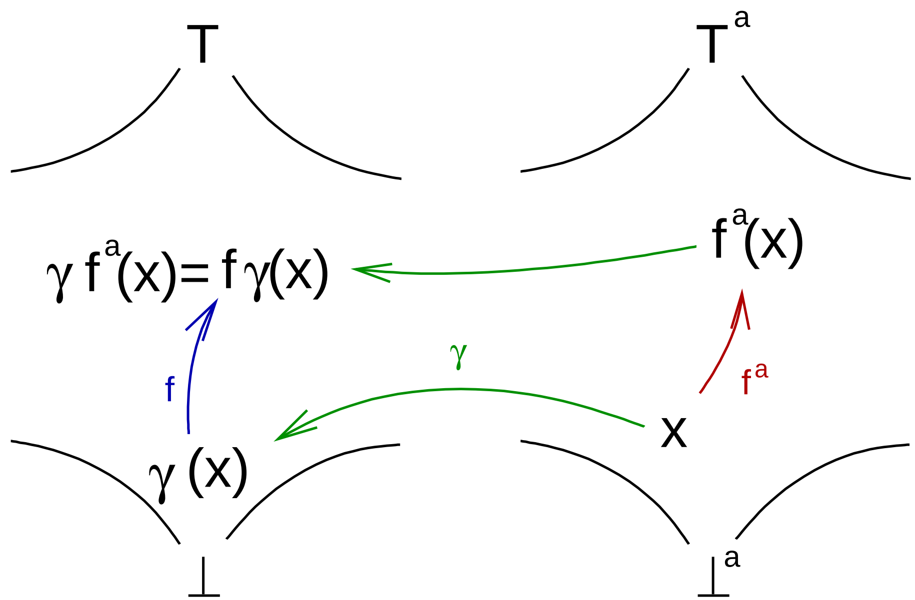
Completeness

Let $< A, \alpha, \gamma, C >$ a Galois insertion. [Cousot & Cousot '77,'79]
$f : C \longrightarrow C$, $f^a = \alpha \circ f \circ \gamma : A \longrightarrow A$ (b.c.a. of f) and $\rho = \gamma \circ \alpha$

f^a F−complete for f

$|||$

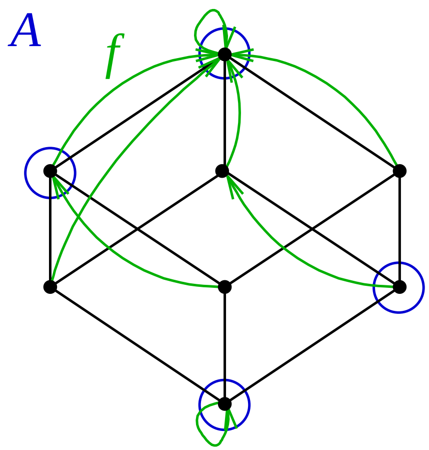
$f\rho = \rho f \rho$



Complete Shells

C complete lattice, A abstract domain, $f : C \longrightarrow C$ continuous.
[Giacobazzi et al. 2000]

- Let A B-complete for f iff $\bigcup_{y \in A} max(\left\{ x \,\middle|\, f(x) \leq y \right\}) \subseteq A$.

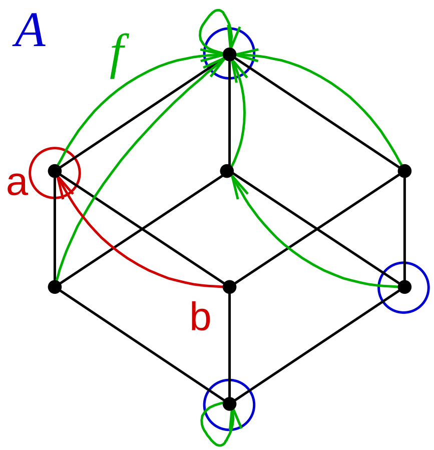


$S^B_f(A) = gfp(\lambda X. A \sqcap M(\bigcup_{y \in X} max(\left\{ x \,\middle|\, f(x) \leq y \right\})))$ B−Shell of A for f

Complete Shells

C complete lattice, A abstract domain, $f : C \longrightarrow C$ continuous.
[Giacobazzi et al. 2000]

- Let A B-complete for f iff $\bigcup_{y\in A} max(\left\{ x \;\middle|\; f(x) \leq y \right\}) \subseteq A$.



$$max\left\{ x \;\middle|\; f(x) \leq a \right\} = \{b\} \not\subseteq A$$

$$\Downarrow$$

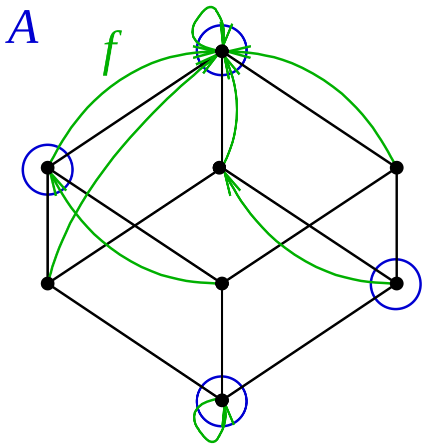
A not B−complete for f

$S^B_f(A) = gfp(\lambda X.A \sqcap M(\bigcup_{y\in X} max(\left\{ x \;\middle|\; f(x) \leq y \right\})))$ B−Shell of A for f

Complete Shells

C complete lattice, A abstract domain, $f : C \longrightarrow C$ continuous.
[Giacobazzi et al. 2000]

- Let A F-complete for f iff $\forall x \in A. f(x) \in A$.

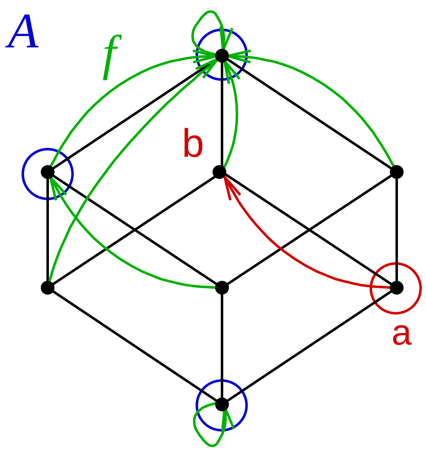


$$S_f^F(A) = gfp(\lambda X. A \sqcap M(f(X)))$$ F−Shell of A for f

Complete Shells

C complete lattice, A abstract domain, $f : C \longrightarrow C$ continuous.
[Giacobazzi et al. 2000]

- Let A F-complete for f iff $\forall x \in A. f(x) \in A$.



$f(a)=b$ not in A

$\Downarrow$

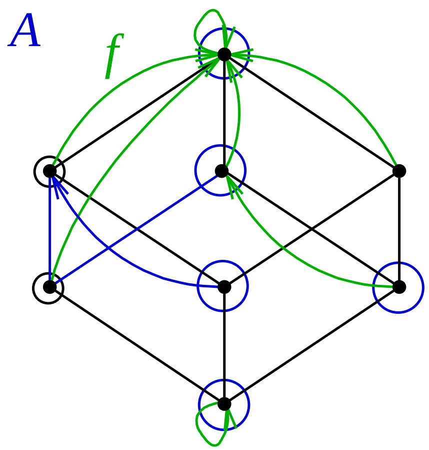
A not F−complete for f

$S^F_f(A) = gfp(\lambda X. A \sqcap M(f(X)))$ F−Shell of A for f

Domain Compression

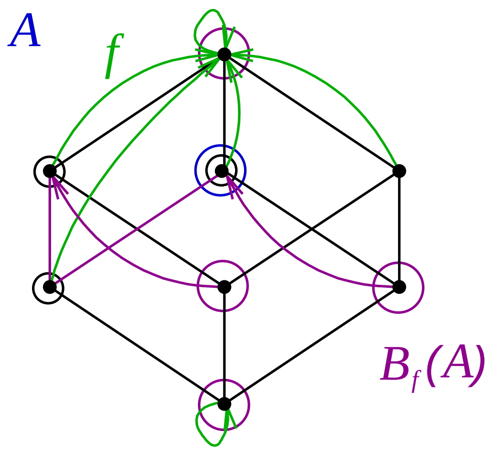
Let R_f a completeness refinement;

Let B_f the COMPRESSOR of R_f iff: $R_f B_f(A) = R_f(A)$.



Domain Compression

Let R_f a completeness refinement;
Let B_f the COMPRESSOR of R_f iff: $R_f B_f(A) = R_f(A)$.



$\Rightarrow$ $R_f B_f(A) = R_f(A)$

B_f erases all the information that R_f can generate.

$\Downarrow$

B_f is the INVERSE of R_f

Domain Compression

Let R_f a completeness refinement;
Let B_f the COMPRESSOR of R_f iff: $R_f B_f(A) = R_f(A)$.

B_f erases all the information that R_f can generate.

$$\Downarrow$$

B_f is the INVERSE of R_f

$$B_f(A) = \bigsqcup \left\{ X \,\middle|\, R_f(X) = R_f(A) \right\}$$

Domain Compression

Let R_f a completeness refinement;
Let B_f the COMPRESSOR of R_f iff: $R_f B_f(A) = R_f(A)$.

B_f erases all the information that R_f can generate.

$$\Downarrow$$

B_f is the INVERSE of R_f

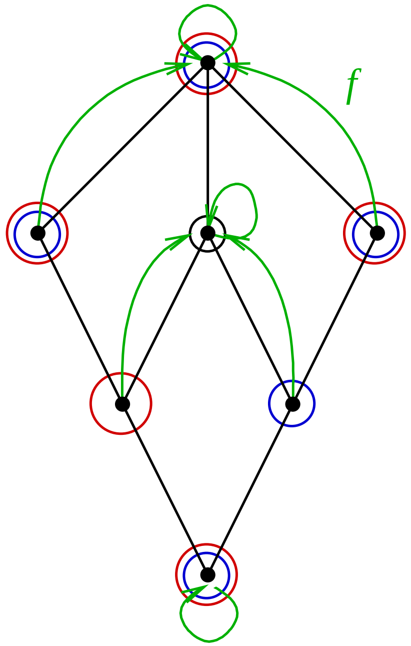
$$B_f(A) = \bigsqcup \left\{ X \;\middle|\; R_f(X) = R_f(A) \right\}$$

PROBLEMS: The compressor usually fails monotonicity.
The shell usually fails reversibility.

$\Rightarrow$ Shells and compressors don't behave like adjunctions.

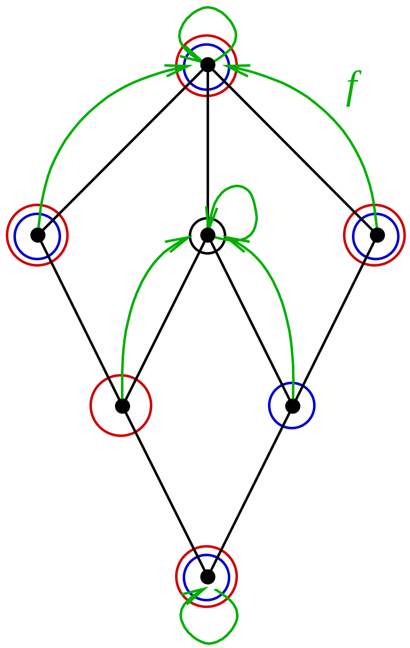
Shells & Compessors as Adjoints

- Shells can fail reversibility:



Shells & Compessors as Adjoints

- Shells can fail reversibility:

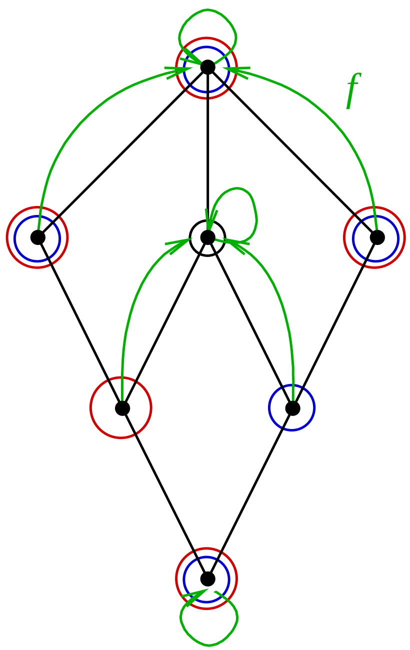


$\Rightarrow$

It doesn't exist the most abstract domain with the same shell.

Shells & Compessors as Adjoints

- Shells can fail reversibility:



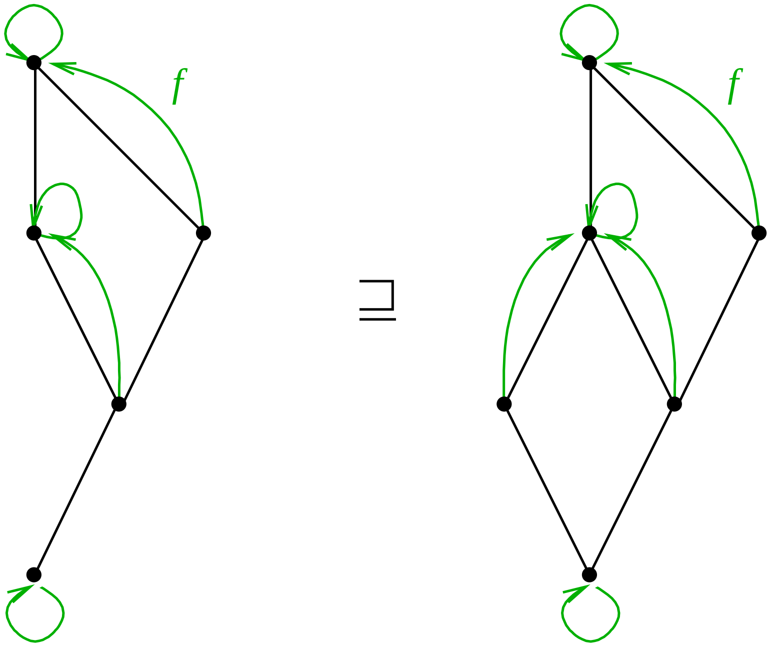
$\Rightarrow$

It doesn't exist the most abstract domain with the same shell.

SOLUTION: Join-uniformity!
[Giacobazzi & Ranzato '98]

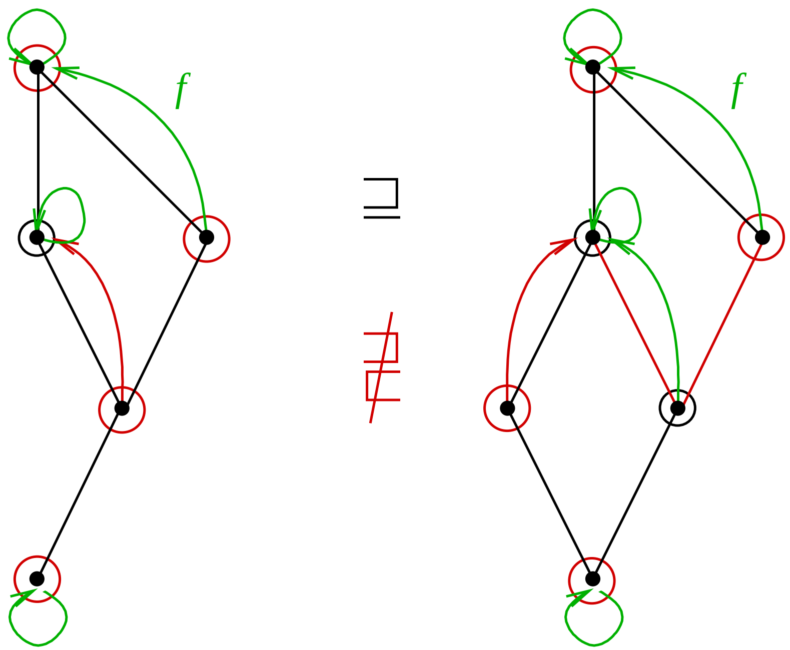
Shells & Compessors as Adjoints

- Compressors can fail monotonicity:



Shells & Compessors as Adjoints

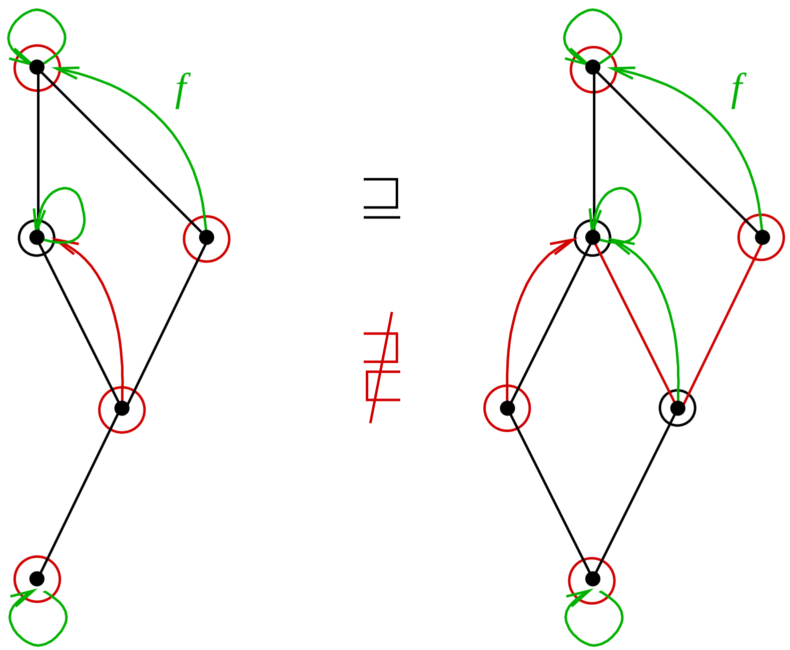
- Compressors can fail monotonicity:



$\Rightarrow$ Not monotone

Shells & Compessors as Adjoints

- Compressors can fail monotonicity:



$\sqsupseteq$

$\not\sqsupseteq$

$\Rightarrow$ Not monotone

SOLUTION: Lifted order $\sqsubseteq^R$!

$$A \sqsubseteq^R B \text{ iff } R(A) \sqsubseteq R(B) \wedge (R(A) = R(B) \Rightarrow A \sqsubseteq B)$$

Shells & Compessors as Adjoints

Theorem:

[Giacobazzi & Ranzato '98]

If $R \in \mathit{lco}(\mathit{uco}(C))$ is join-uniform then:

- $< \mathit{uco}(C), \sqsubseteq^R >$ is a complete lattice;
- $R \in \mathit{lco}(< \mathit{uco}(C), \sqsubseteq^R >)$

$\Longrightarrow$ The compressor B is the right adjoint of R!

Join-Uniformity

R join-uniform iff

$$R\left(\sqcup \left\{ X \,\middle|\, R(X) = R(A) \right\}\right) = R(A)$$

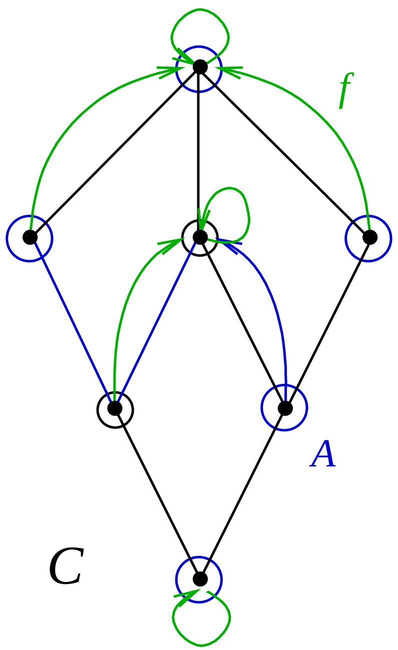
$\Longrightarrow$ $B(A) = \sqcup \left\{ X \,\middle|\, R(X) = R(A) \right\}$ base of A.

Join-Uniformity

R join-uniform iff

$$R\left(\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}\right)=R(A)$$

$\Longrightarrow B(A)=\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}$ base of A.



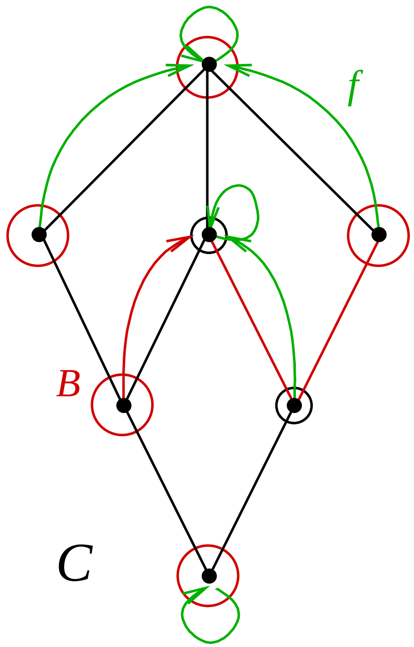
$$R(A)=C$$

Join-Uniformity

R join-uniform iff

$$R\left(\sqcup\left\{\ X \ \middle|\ R(X)=R(A)\ \right\}\right)=R(A)$$

$\Longrightarrow$ $B(A)=\sqcup\left\{\ X \ \middle|\ R(X)=R(A)\ \right\}$ base of A.



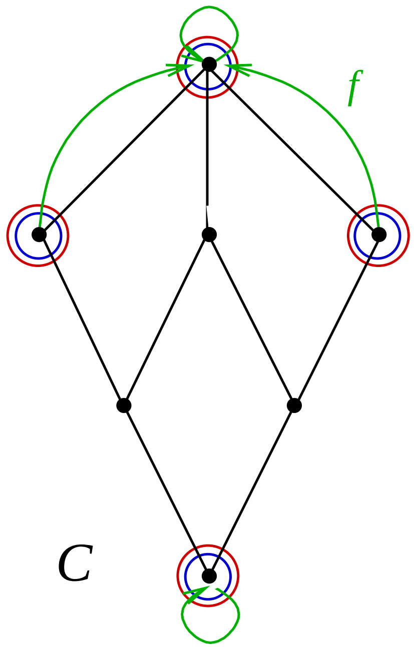
$R(A)=C$ $\qquad$ $R(B)=C$

Join-Uniformity

R join-uniform iff

$$R\left(\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}\right)=R(A)$$

$\Longrightarrow$ $B(A)=\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}$ base of A.



$R(A)=C$ $\quad$ $R(B)=C$

$$\Downarrow$$

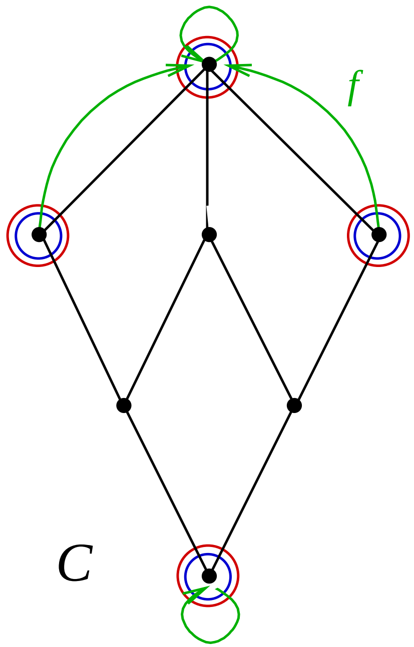
$$R(A\sqcup B)\neq C$$

Join-Uniformity

R join-uniform iff

$$R\left(\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}\right)=R(A)$$

$\Longrightarrow$ $B(A)=\sqcup\left\{\ X \,\middle|\, R(X)=R(A)\ \right\}$ base of A.



$$R(A)=C \qquad R(B)=C$$

$$\Downarrow$$

$$R(A\sqcup B)\neq C$$

$\Longrightarrow$ Given $f : C \longrightarrow C$, when R_f is join-uniform?

A necessary condition

Let C a finite lattice, $f : C \longrightarrow C$:

$f^1(x) = f(x)$, $f^{n+1}(x) = f(f^n(x))$

$\dot{f}(C) = \left\{ x \in C \,\middle|\, \exists y \in C \setminus \{x\} \,.\, f(y) = x \right\}$ f-REDUCIBLE

firr$(C) = C \setminus \dot{f}(C)$ f-IRREDUCIBLE

$$\exists x \in \mathit{Mirr}(C) \cap \dot{f}(C) \,.\, \exists n \in \mathbb{N} \,.\, f^n(x) = x$$

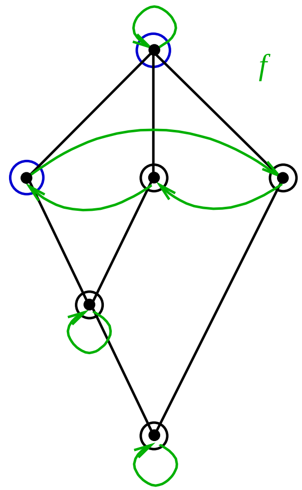
$$\Downarrow$$

R_f is not join-uniform.

A necessary condition

Let C a finite lattice, $f : C \longrightarrow C$:

$$\exists x \in \mathit{Mirr}(C) \cap \dot{f}(C) \,.\, \exists n \in \mathbb{N} \,.\, f^n(x) = x$$
$$\Downarrow$$
R_f is not join-uniform.



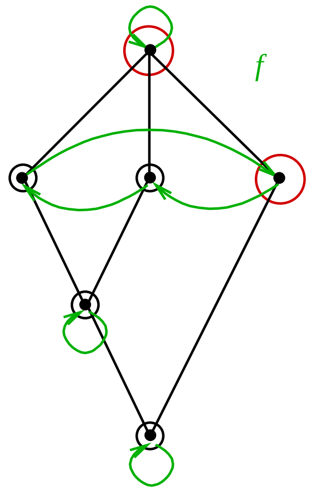
A necessary condition

Let C a finite lattice, $f : C \longrightarrow C$:

$$\exists x \in \mathit{Mirr}(C) \cap \dot{f}(C) \,.\, \exists n \in \mathbb{N} \,.\, f^n(x) = x$$

$$\Downarrow$$

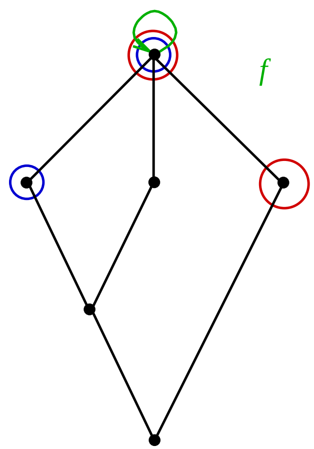
R_f is not join-uniform.



A necessary condition

Let C a finite lattice, $f : C \longrightarrow C$:

$$\exists x \in \mathit{Mirr}(C) \cap \dot{f}(C) \,.\, \exists n \in \mathbb{N} \,.\, f^n(x) = x$$
$$\Downarrow$$
R_f is not join-uniform.

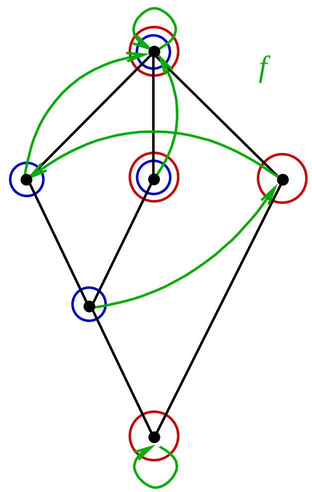


A necessary condition

Let C a finite lattice, $f : C \longrightarrow C$:

$$\exists x \in \mathit{Mirr}(C) \cap \dot{f}(C) \,.\, \exists n \in \mathbb{N} \,.\, f^n(x) = x$$
$$\Downarrow$$
R_f is not join-uniform.

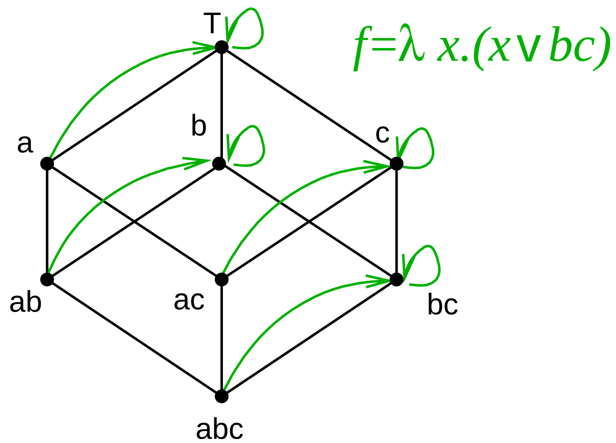
$\Rightarrow$ The inverse implication doesn't hold!



R_f not join-uniform and no cycles of f!

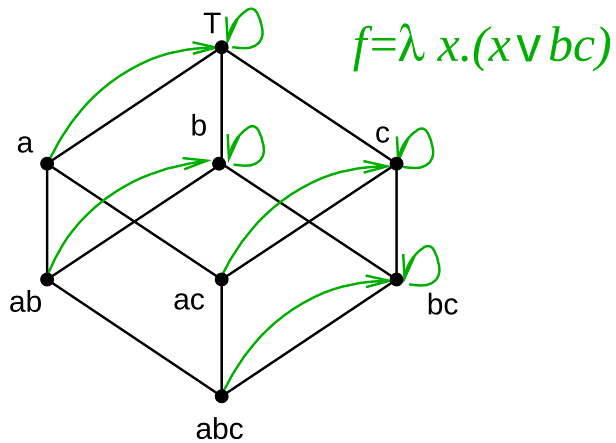
Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.



Reversing R_f

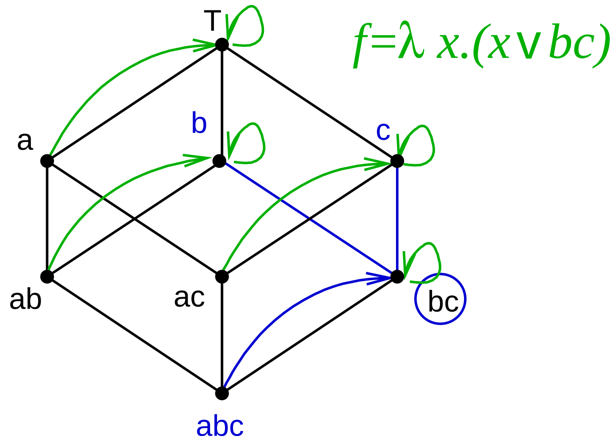
Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.



- G(x)=min$\left\{ Z \subseteq C \;\middle|\; x \notin Z \text{ and } (\bigwedge Z = x \text{ or } f(Z) = x) \right\}$

Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

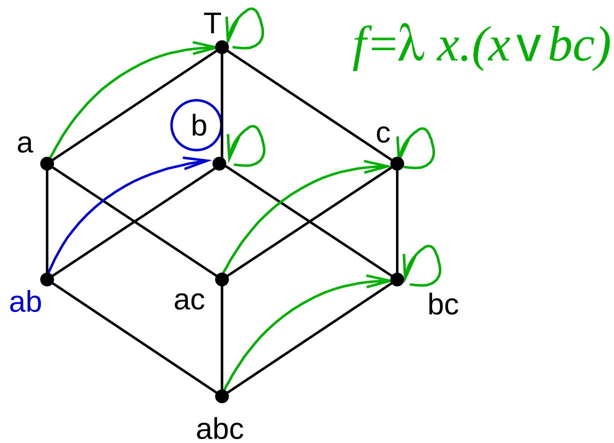


- G(x)=min$\left\{ Z \subseteq C \;\middle|\; x \notin Z \text{ and } (\bigwedge Z = x \text{ or } f(Z) = x) \right\}$

x =bc $\quad\Longrightarrow\quad$ G(bc)={{b,c},{abc}}

Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

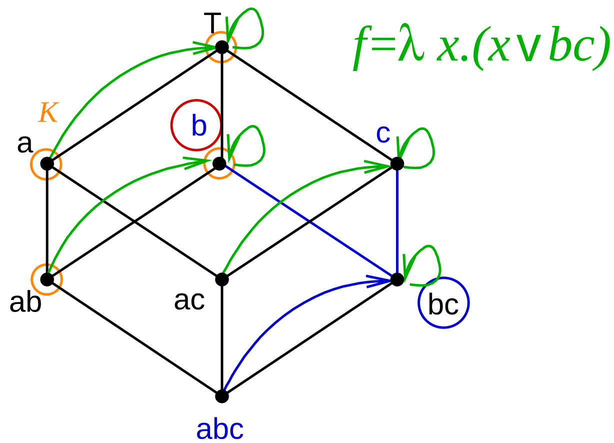


- G(x)=min$\left\{ Z \subseteq C \;\middle|\; x \notin Z \text{ and } (\bigwedge Z = x \text{ or } f(Z) = x) \right\}$

x =b $\quad\Longrightarrow\quad$ G(b)={{ab}}

Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.



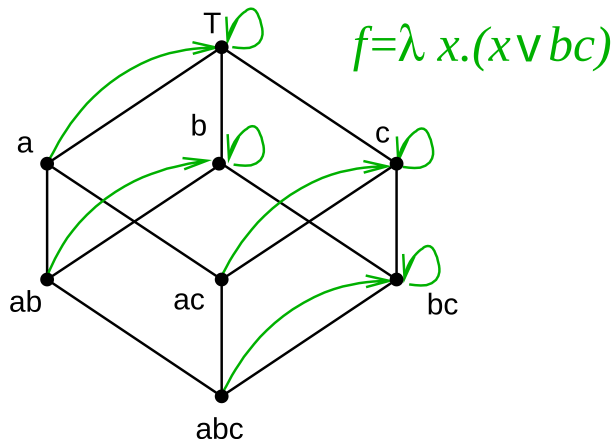
- $\overset{\curvearrowleft}{X}(K) = \left\{ \bigcup_{x \in X} Y_x \;\middle|\; \begin{array}{l} ((G(x) \neq \varnothing \text{ and } x \notin K) \Rightarrow Y_x \in G(x)) \\ ((G(x) = \varnothing \text{ or } x \in K) \Rightarrow Y_x = \{x\}) \end{array} \right\}$

  X={bc,b}, K={T,a,b,ab} $\Longrightarrow$ $\overset{\curvearrowleft}{X}(K)$={{b,c},{b,abc}}

- $X \rightarrow_K Y$ if $Y \in \overset{\curvearrowleft}{X}(K)$

Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.



- $\Gamma_x^0(K) = \{x\}$
  $\Gamma_x^{n+1}(K) = \left\{ Y \,\middle|\, (X \in \Gamma_x^n(K) \Rightarrow (X \to_K Y,\ X \not\subseteq K)),\ \text{no cycles} \right\}$

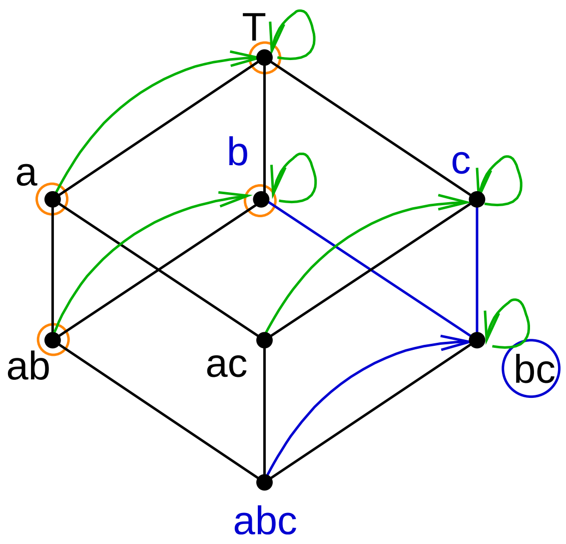
x =bc is generated by K={T,a,b,ab}?

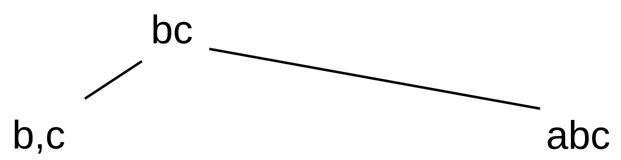
Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

- $\Gamma_x^0(K) = \{x\}$
  $\Gamma_x^{n+1}(K) = \left\{ Y \;\middle|\; (X \in \Gamma_x^n(K) \;\Rightarrow\; (X \to_K Y,\; X \not\subseteq K)),\ \text{no cycles} \right\}$

  x =bc is generated by K={T,a,b,ab}?



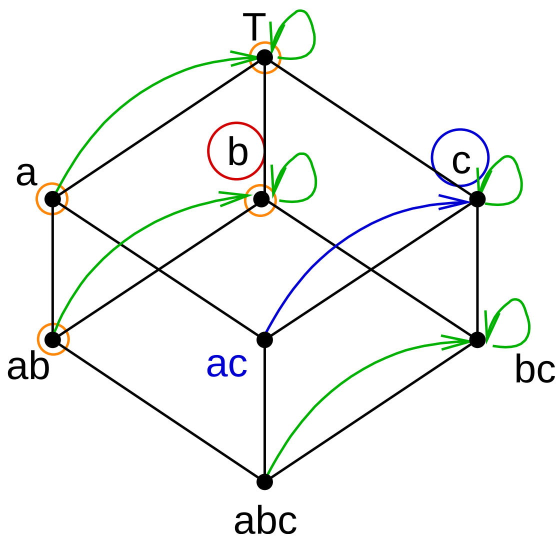


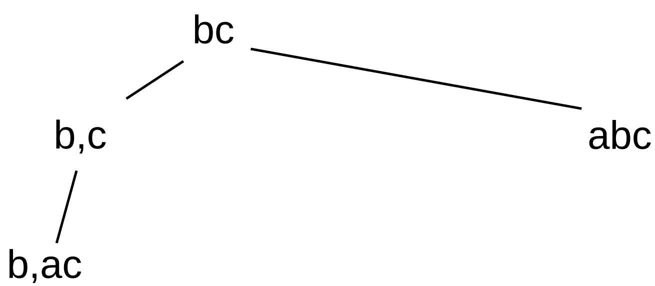
Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

- $\Gamma_x^0(K) = \{x\}$
  $\Gamma_x^{n+1}(K) = \left\{ Y \;\middle|\; (X \in \Gamma_x^n(K) \;\Rightarrow\; (X \to_K Y,\; X \not\subseteq K)),\ \text{no cycles} \right\}$

x =bc is generated by K={T,a,b,ab}?



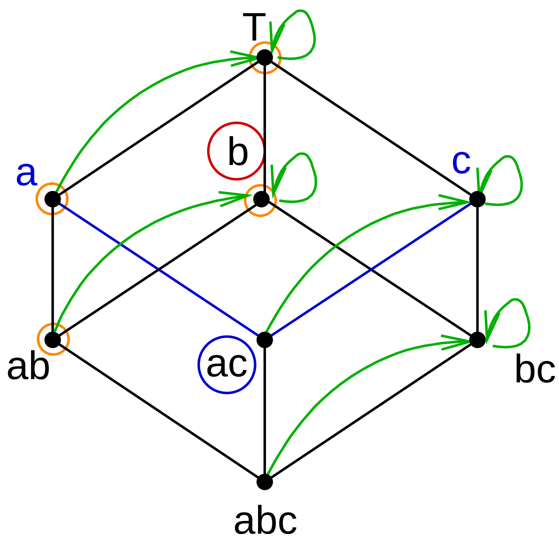


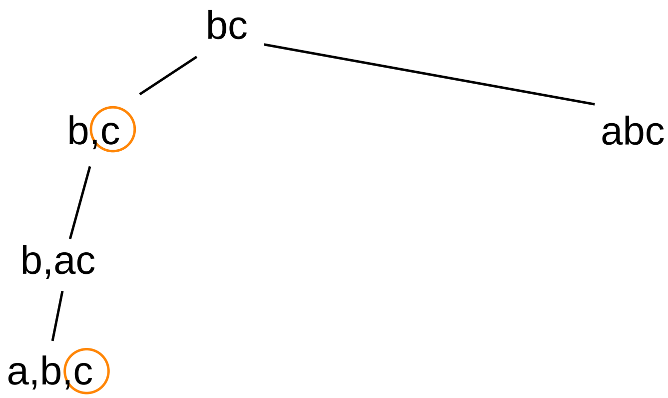
Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

- $\Gamma_x^0(K) = \{x\}$
  $\Gamma_x^{n+1}(K) = \left\{ Y \;\middle|\; (X \in \Gamma_x^n(K) \Rightarrow (X \to_K Y,\ X \not\subseteq K)),\ \text{no cycles} \right\}$

  x =bc is generated by K={T,a,b,ab}?



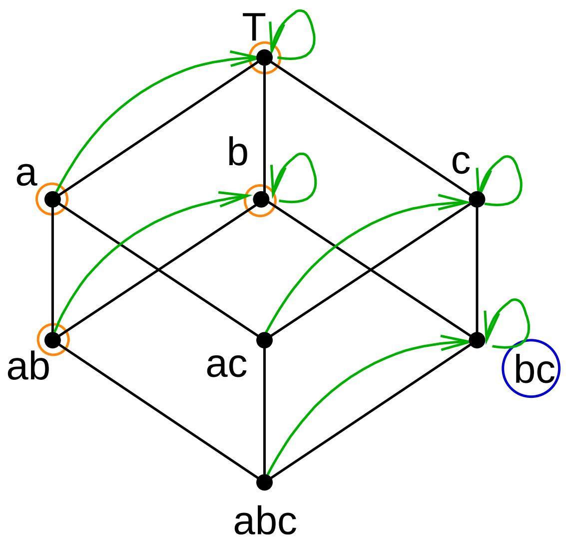


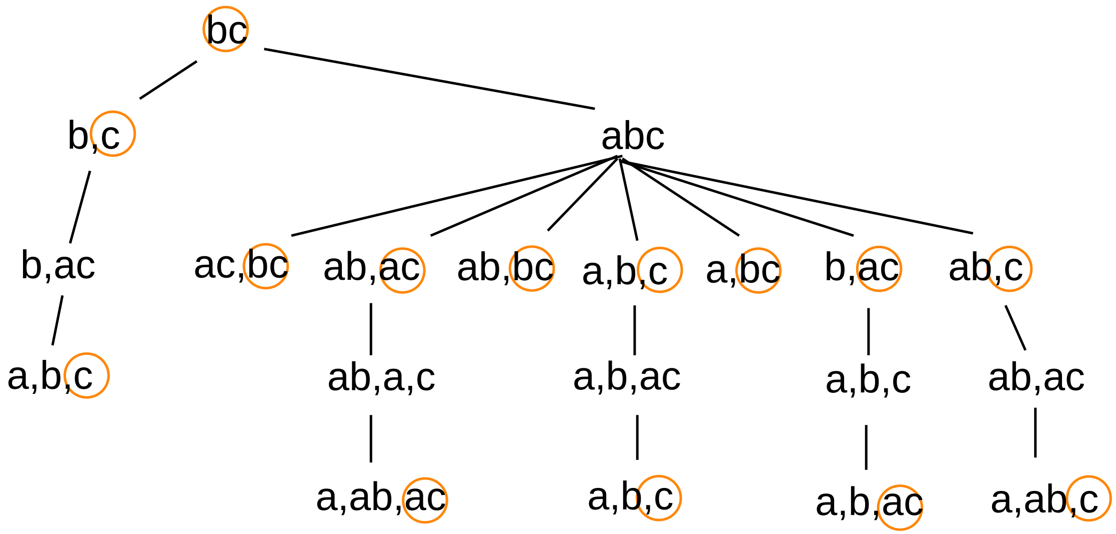
Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

- $\Gamma^0_x(K) = \{x\}$
  $\Gamma^{n+1}_x(K) = \left\{ Y \,\middle|\, (X \in \Gamma^n_x(K) \;\Rightarrow\; (X \rightarrow_K Y,\ X \not\subseteq K)),\ \text{no cycles} \right\}$

  x =bc is generated by K={T,a,b,ab}?





Reversing R_f

Let C a finite lattice, $X \subseteq C$, $x \in C$, K an abstract domain.

Theorem:

Let $\Gamma_x(K)$ the tree generated by $\Gamma_x^n(K)$ and $L_x(K)$ the set of leaves of $\Gamma_x(K)$.

- $X \in L_x(K) \;\Rightarrow\; x \in R_f(X)$

  {a,b,ac}$\in L_{\text{bc}} \quad\Rightarrow\quad$ bc $\in R_f($ {a,b,ac}$))$

- $x \in R_f(K) \;\Rightarrow\; \exists Y \in L_x(K)\,.\,Y \subseteq K$

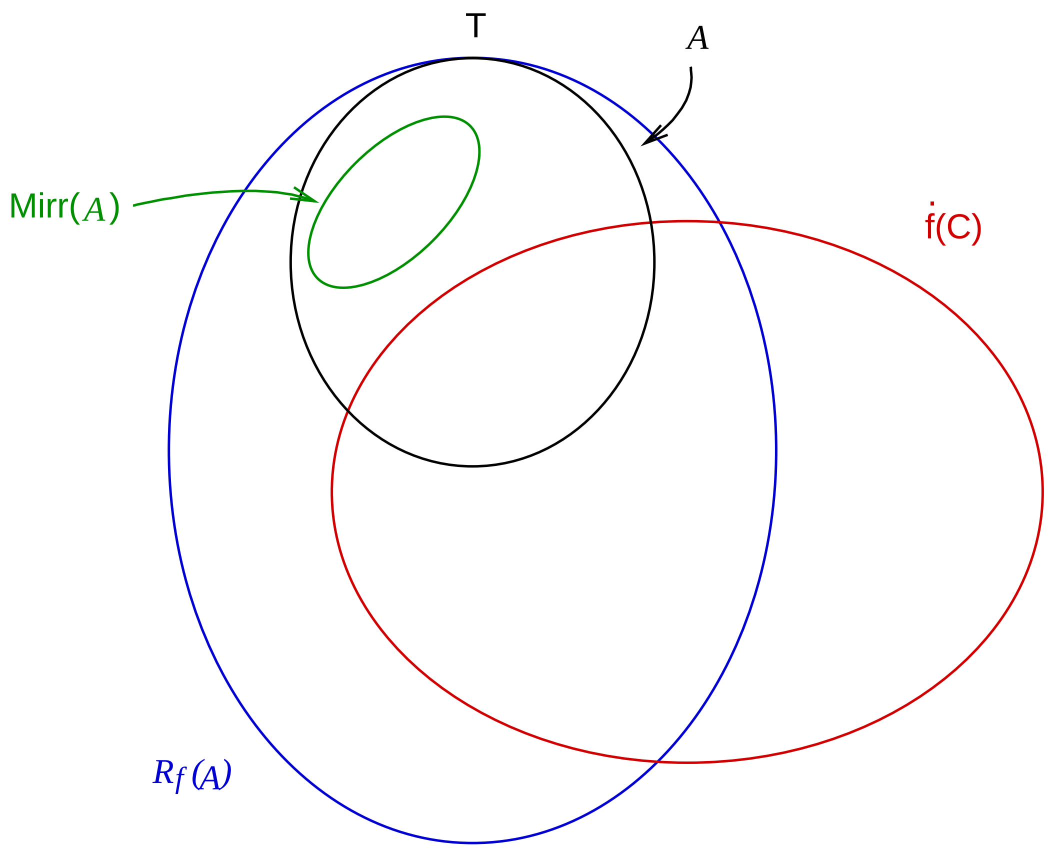
  $\forall Y \in L_x(K)\,.\,Y \not\subseteq \delta \;\Rightarrow\;$ bc $\notin R_f(K) = R_f($ {T,a,b,ab}$)$

The Scenario

Let C be a finite lattice, A, K abstract domains, $A \sqsubseteq K$.

M_f^A=Mirr$\left(\left\{ x \in \dot{f}(C) \smallsetminus A \;\middle|\; \exists L \in L_x(A) \,.\, L \subseteq A \right\}\right) \cup$ Mirr(A)

$$M_f^A \subseteq R_f(K) \;\Rightarrow\; R_f(K) = R_f(A)$$

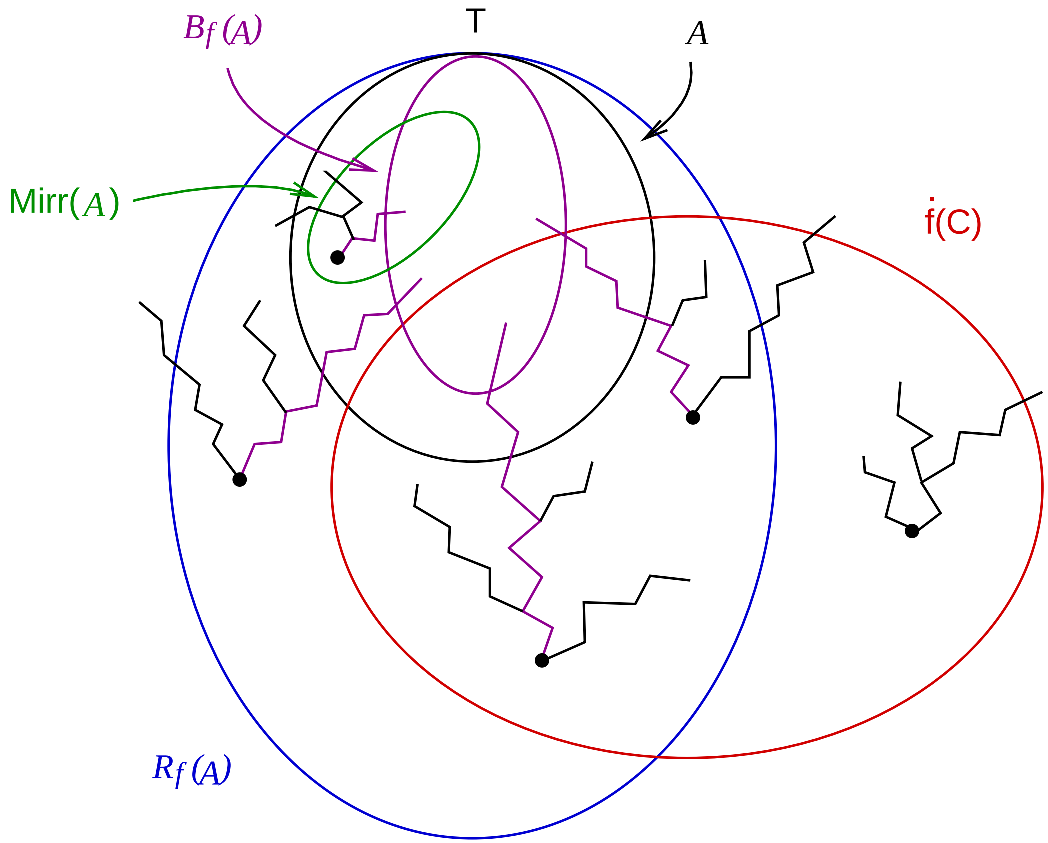


The Scenario

Let C be a finite lattice, A, K abstract domains, $A \sqsubseteq K$.

M_f^A=Mirr($\left\{ x \in \dot{f}(C) \setminus A \;\middle|\; \exists L \in L_x(A) \,.\, L \subseteq A \right\}$)$\cup$ Mirr(A)

$$M_f^A \subseteq R_f(K) \;\Rightarrow\; R_f(K) = R_f(A)$$

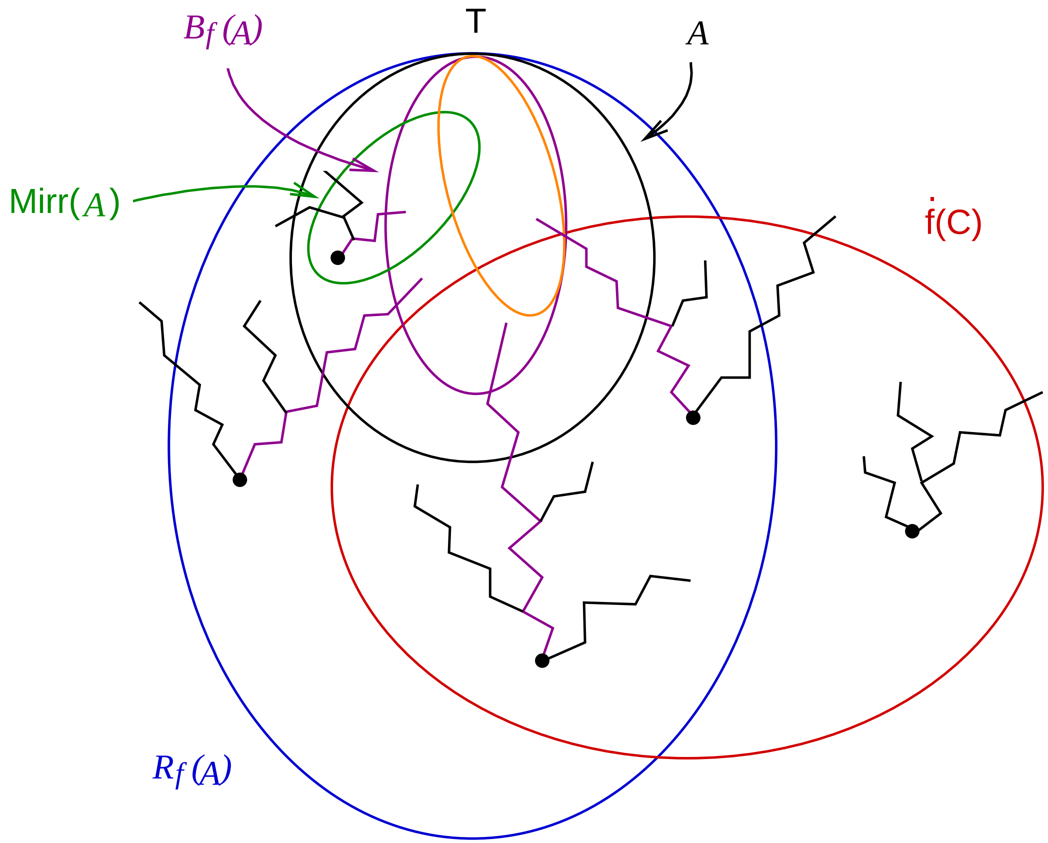


The Scenario

Let C be a finite lattice, A, K abstract domains, $A \sqsubseteq K$.

M_f^A=Mirr$\left(\left\{\, x \in \dot{f}(C) \smallsetminus A \;\middle|\; \exists L \in L_x(A) \,.\, L \subseteq A \,\right\}\right) \cup$ Mirr(A)

$$M_f^A \subseteq R_f(K) \;\Rightarrow\; R_f(K) = R_f(A)$$



Computing the Base

Let C a finite lattice, A an abstract domain.

$$\text{D}(A) = \left\{ A \setminus \{x\} \;\middle|\; x \in \text{Mirr}(A) \setminus (\text{Mirr}(C) \cap \text{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

Computing the Base

Let C a finite lattice, A an abstract domain.

$$\mathrm{D}(A)=\left\{ A \smallsetminus \{x\} \;\middle|\; x \in \mathrm{Mirr}(A) \smallsetminus (\mathrm{Mirr}(C) \cap \mathrm{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

STEP 1: P(A):=$\varnothing$, N_1:={A};

Computing the Base

Let C a finite lattice, A an abstract domain.

$$\mathrm{D}(A) = \left\{ A \smallsetminus \{x\} \;\middle|\; x \in \mathrm{Mirr}(A) \smallsetminus (\mathrm{Mirr}(C) \cap \mathrm{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

STEP 1: $\mathrm{P}(A) := \varnothing$, $N_1 := \{A\}$;

STEP N+1: $K_n \in N_n$, $\mathrm{D}(K_n) = \varnothing \;\Rightarrow\; \mathrm{P}(A) := \mathrm{P}(A) \cup \{K_n\}$;

Computing the Base

Let C a finite lattice, A an abstract domain.

$$\mathsf{D}(A)=\left\{ A \setminus \{x\} \,\middle|\, x \in \mathsf{Mirr}(A) \setminus (\mathsf{Mirr}(C) \cap \mathsf{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

STEP 1: $\mathsf{P}(A)$:=$\varnothing$, N_1:=$\{A\}$;

STEP N+1: $K_n \in N_n$, $\mathsf{D}(K_n)$=$\varnothing$ $\Rightarrow$ $\mathsf{P}(A)$:=$\mathsf{P}(A) \cup \{K_n\}$;

$$U_n := \left\{ K \in \mathsf{D}(K_n) \,\middle|\, \exists y \in M_f^A \setminus K \,.\, \forall L \in L_y(K) \,.\, L \not\subseteq K \right\}$$

$$N_{n+1}^{K_n} := \mathsf{D}(K_n) \setminus U_n$$

Computing the Base

Let C a finite lattice, A an abstract domain.

$$\mathrm{D}(A)\text{=}\left\{ A \smallsetminus \{x\} \;\middle|\; x \in \mathrm{Mirr}(A) \smallsetminus (\mathrm{Mirr}(C) \cap \mathrm{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

STEP 1: P(A):=$\varnothing$, N_1:={A};

STEP N+1: $K_n \in N_n$, D(K_n)=$\varnothing$ $\Rightarrow$ P(A):=P(A)$\cup${K_n};

U_n:=$\left\{ K \in \mathrm{D}(K_n) \;\middle|\; \exists y \in M_f^A \smallsetminus K \,.\, \forall L \in L_y(K) \,.\, L \not\subseteq K \right\}$

$N_{n+1}^{K_n}$:=D(K_n)$\smallsetminus U_n$

$N_{n+1}^{K_n} = \varnothing$ $\Rightarrow$ P(A):=P(A)$\cup${K_n} and N_{n+1}:=$\bigcup_{K_n \in N_n} N_{n+1}^{K_n}$

Computing the Base

Let C a finite lattice, A an abstract domain.

$$\text{D}(A)=\left\{ A \setminus \{x\} \,\middle|\, x \in \text{Mirr}(A) \setminus (\text{Mirr}(C) \cap \text{firr}(C)) \right\}$$

$\Longrightarrow$ Induction on the construction of N_n such that $K \in N_n$ are the candidate bases for $R_f(A)$ after n steps of the algorithm.

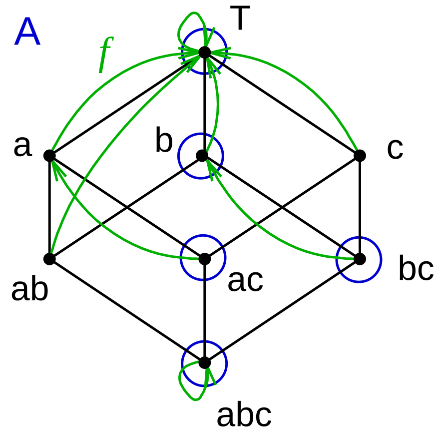
$\Longrightarrow$ The algorithm terminates and

- $\forall n \in \mathbb{N} \,.\, \forall K \in N_n : \; A \sqsubseteq K, \; R_f(K) \sqsubseteq A$ and $(K_1 \in N_{n+1} \setminus N_n \;\Rightarrow\; |K_1| < |K|)$
- P will include the minimal candidate bases.

$R_f(A)$ is join-uniform with base $B_f(A)$ iff
P(A)=\{$B_f(A)$\}.

Example

A={T,b,ac,bc,abc}

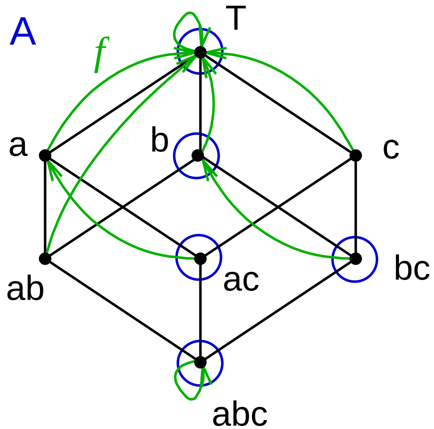


Mirr(A)={b,ac,bc}

M_f^A={a,b,ac,bc}

Example

$A=\{T,b,ac,bc,abc\}$



$Mirr(A)=\{b,ac,bc\}$

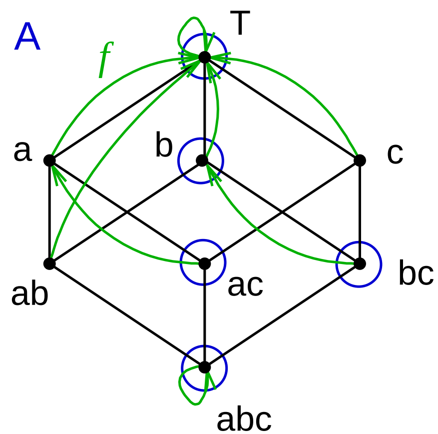
$M_f^A=\{a,b,ac,bc\}$

$P=\varnothing$

STEP 1: $N_1=\{A\}=\{\{T,b,ac,bc,abc\}\}$

Example

$A=\{T,b,ac,bc,abc\}$



$Mirr(A)=\{b,ac,bc\}$

$M_f^A=\{a,b,ac,bc\}$

$P=\varnothing$

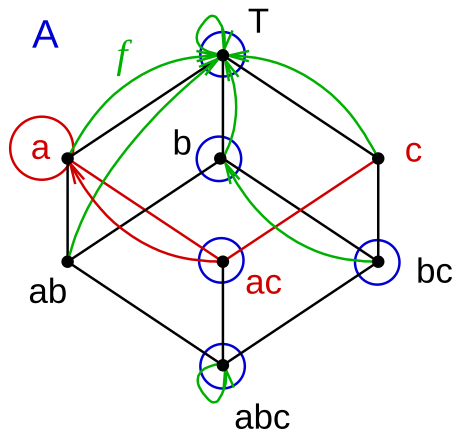
STEP 1: $N_1=\{A\}=\{\{T,b,ac,bc,abc\}\}$

STEP 2: $B_1=\{T,b,ac,bc,abc\}$ $D(B_1)=\{\{T,ac,bc,abc\},\{T,b,ac,abc\},\{T,b,bc,abc\}\}$

$U_1=\varnothing$

Example

$A=\{\top,b,ac,bc,abc\}$



$Mirr(A)=\{b,ac,bc\}$

$M_f^A=\{a,b,ac,bc\}$

$P=\varnothing$

STEP 1: $N_1=\{A\}=\{\{\top,b,ac,bc,abc\}\}$

STEP 2: $B_1=\{\top,b,ac,bc,abc\}$ $D(B_1)=\{\{\top,ac,bc,abc\},\{\top,b,ac,abc\},\{\top,b,bc,abc\}\}$

Γ_a :

a

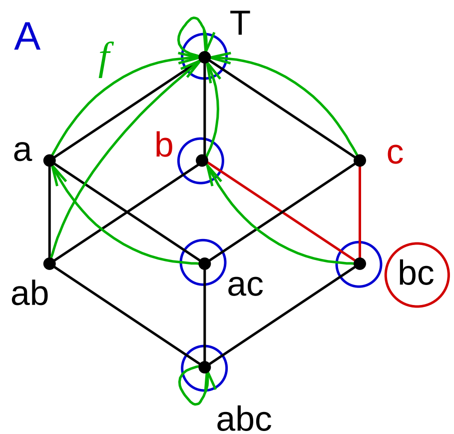
ac $\longrightarrow$ $\{\top,bc,ac,abc\}$ and $\{\top,b,ac,abc\}$

a,c

$U_1=\{\{\top,b,bc,abc\}\}$

Example

A={T,b,ac,bc,abc}



Mirr(A)={b,ac,bc}

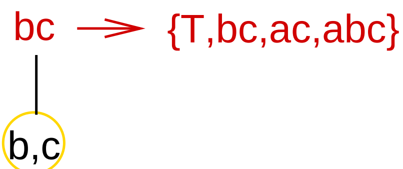
M_f^A={a,b,ac,bc}

P= ∅

STEP 1: N_1={A}={{T,b,ac,bc,abc}}

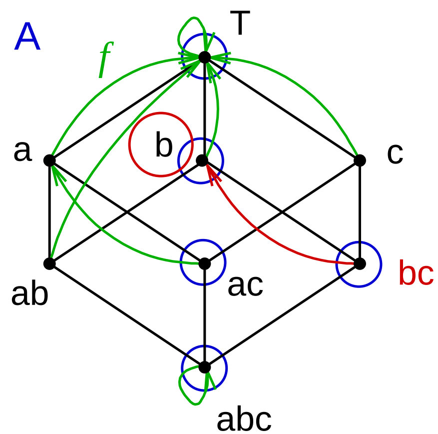
STEP 2: B_1={T,b,ac,bc,abc} $D(B_1)$={{T,ac,bc,abc},{T,b,ac,abc},{T,b,bc,abc}}

Γ_{bc}:



U_1={{T,b,bc,abc},{T,b,ac,abc}}

Example



$A = \{T, b, ac, bc, abc\}$

$Mirr(A) = \{b, ac, bc\}$

$M_f^A = \{a, b, ac, bc\}$

$P = \varnothing$

STEP 1: $N_1 = \{A\} = \{\{T, b, ac, bc, abc\}\}$

STEP 2: $B_1 = \{T, b, ac, bc, abc\}$ $D(B_1) = \{\{T, ac, bc, abc\}, \{T, b, ac, abc\}, \{T, b, bc, abc\}\}$

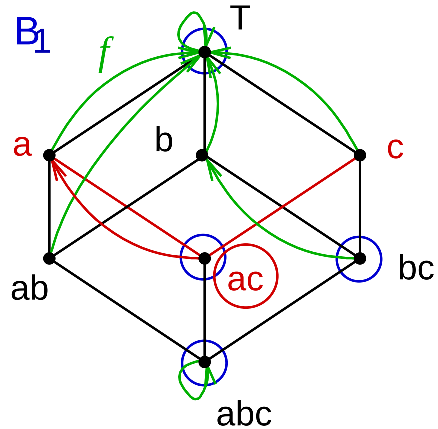
Γ_b :

$$\begin{array}{l} b \\ | \\ bc \longrightarrow \{T, bc, ac, abc\} \end{array}$$

$U_1 = \{\{T, b, bc, abc\}, \{T, b, ac, abc\}\}$ $\boxed{N_2 = \{\{T, ac, bc, abc\}\}}$

Example

$A=\{T,b,ac,bc,abc\}$



$Mirr(A)=\{b,ac,bc\}$

$M_f^A=\{a,b,ac,bc\}$

$P=\varnothing$

STEP 2: $N_2=\{\{T,ac,bc,abc\}\}$

STEP 3: $B_2=\{T,ac,bc,abc\}$ $\quad D(B_2)=\{\{T,ac,abc\},\{T,bc,abc\}\}$

Γ_{ac}:

ac $\twoheadrightarrow$ {T,ac,abc}

|

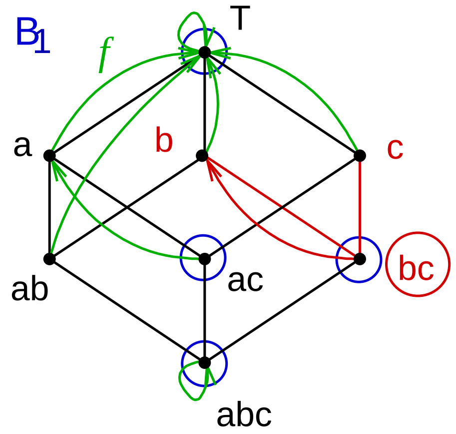
a,c

|

ac,c

$U_2=\{\{T,bc,abc\}\}$

Example



Mirr(A)={b,ac,bc}

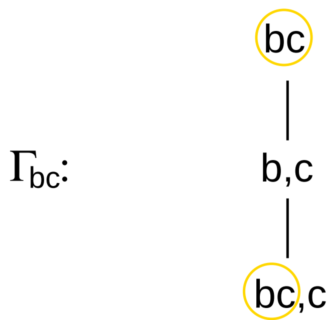
M_f^A={a,b,ac,bc}

A={T,b,ac,bc,abc}

$\boxed{\text{P=\{\{T,ac,bc,abc\}\}}}$ BASE

STEP 2: N_2={{T,ac,bc,abc}}

STEP 3: B_2={T,ac,bc,abc} D(B_2)={{T,ac,abc},{T,bc,abc}}



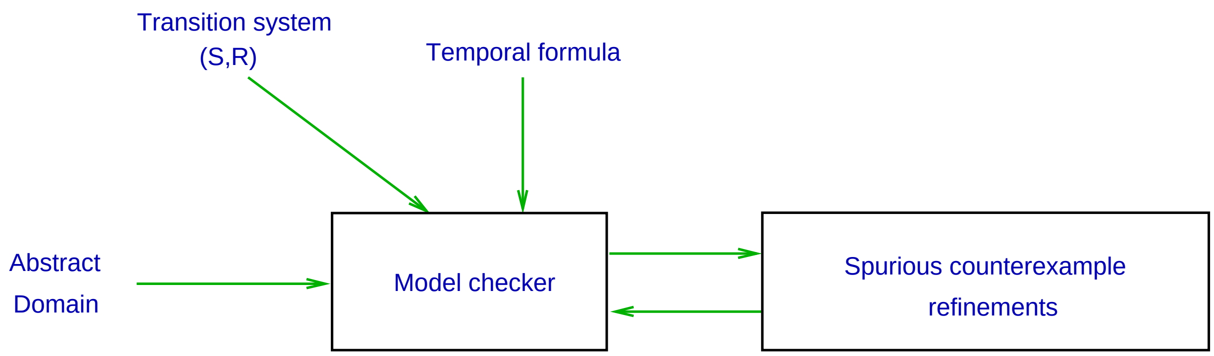
U_2={{T,bc,abc},{T,ac,abc}}

$\boxed{N_3 = \varnothing}$ $\longrightarrow$ HALTS

Conclusions: Model Checking

Let $\mathbb{M} =< \Sigma, \Sigma_0, \tau, L >$ a Kripke structure modeling P;
Let φ a temporal formula;
Let $\mathbb{M}^A$ the abstract model for P with partition induced by A.

$$\mathbb{M}^A \models \varphi \quad \Rightarrow \quad \mathbb{M} \models \varphi$$ [Clarke et al. '00]

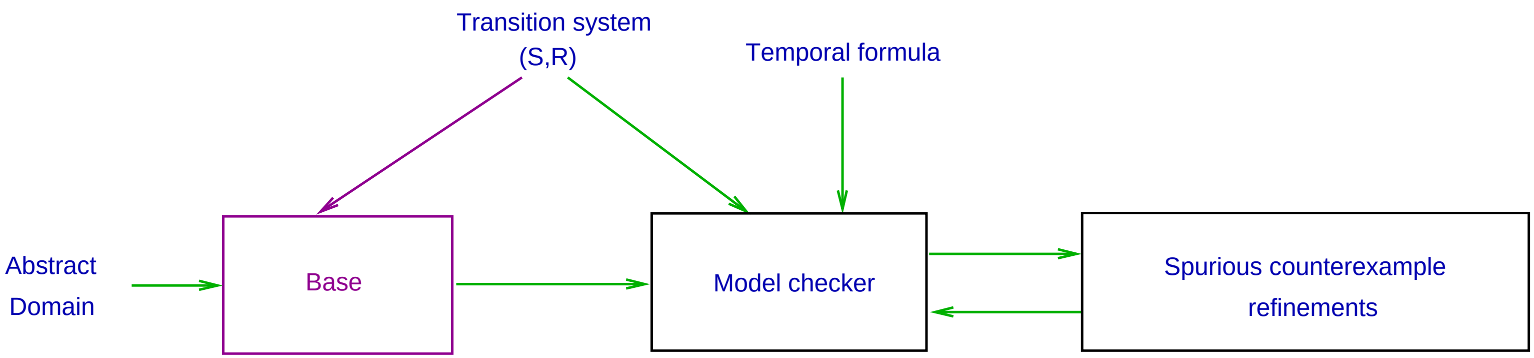


F-completeness w.r.t. $\widetilde{pre}[\tau] \quad \Rightarrow \quad \mathbb{M}^A \not\models \varphi \quad \Rightarrow \quad \mathbb{M} \not\models \varphi$
[Giacobazzi & Quintarelli '01]

Conclusions: Model Checking

Let $\mathbb{M} =< \Sigma, \Sigma_0, \tau, L >$ a Kripke structure modeling P;
Let φ a temporal formula;
Let $\mathbb{M}^A$ the abstract model for P with partition induced by A.

$$\mathbb{M}^A \models \varphi \quad \Rightarrow \quad \mathbb{M} \models \varphi$$ [Clarke et al. '00]



$$\Downarrow$$

$\mathbb{M}^{B_{\widetilde{pre}[\tau]}(A)}$ is the simplest model
on which to check a formula
yet achieving the same precision as A does.

Future works: Geometry of Domain Transformers

lco(C) F−compl
join−unif ——— Compressor

We studied the inversion of a join-uniform F-completeness refinement!

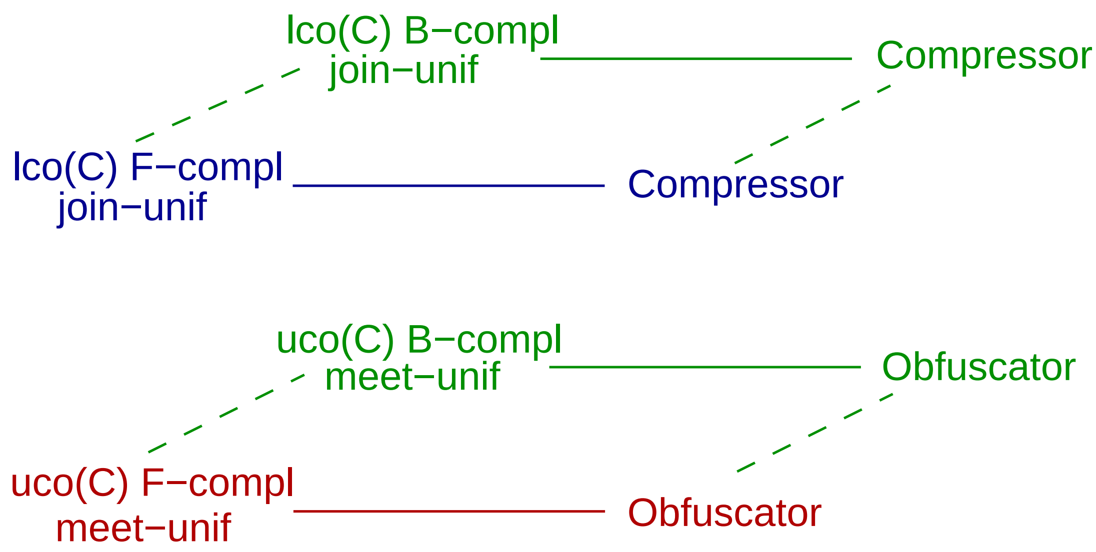
Future works: Geometry of Domain Transformers

lco(C) F−compl
join−unif — Compressor

uco(C) F−compl
meet−unif — Obfuscator

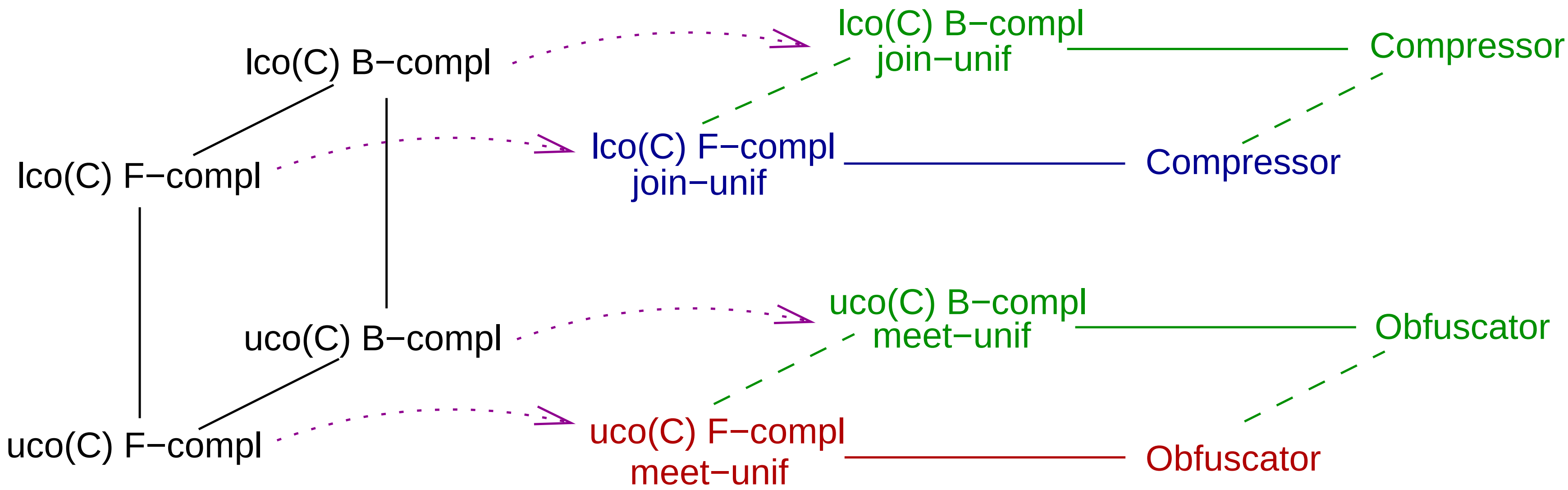
Which are the inversions of meet-uniform F-completeness simplifications?

Future works: Geometry of Domain Transformers



What about B-completeness refinements and simplifications?

Future works: Geometry of Domain Transformers



How can we make a transformer invertible?