Partial Completeness of Abstract Fixpoint Checking

Patrick COUSOT

École Normale Supérieure 45 rue d'Ulm 75230 Paris cedex 05, France

mailto:Patrick.Cousot@ens.fr http://www.di.ens.fr/~cousot

KAIST, Taejon, Korea \qquad Tuesday June 13 $^{
m th}$, 2000

Motivations

KAIST, Taejon, Korea, Tuesday June 13th, 2000





Fixpoint Checking

• Model-checking safety properties of transition systems:

$$Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S ?$$

• Program static analysis by abstract interpretation:

$$\gamma(\operatorname{Ifp}^{\leq} \lambda X \cdot \alpha(I \vee F(\gamma(X)))) \leq S ?$$

 $\blacktriangleleft \triangleleft \neg -2 - [\blacksquare - \triangleright \square \triangleright$

Soundness / (Partial) Completeness

Soundness: a positive abstract answer implies a positive concrete answer. So no error is possible when reasoning in the abstract;

- **Completeness:** a positive concrete answer can always be found in the abstract;
- **Partial completeness:** in case of termination of the abstract fixpoint checking algorithms, no positive answer can be missed.

Termination is a separate problem (widening/narrowing, etc.).

 $\P \P \P - 3 - \| \blacksquare - \triangleright \square \triangleright \models$

Question

Is it possible to automatize the discovery of the abstraction needed for the generalization of model-checking to infinite (or very large) state systems?





Objective

Constructively characterize the abstractions $\langle \alpha, \gamma \rangle$ for which abstract fixpoint algorithms are partially complete.





Concrete Fixpoint Checking

KAIST, Taejon, Korea, Tuesday June 13^{th} , 2000





Concrete Fixpoint Checking Problem

- Complete lattice $\langle L, \leq, 0, 1, \vee, \wedge \rangle$;
- Monotonic transformer $F \in L \xrightarrow{\text{mon}} L$;
- Specification $\langle I, S \rangle \in L^2$;

 $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S ?$



Example

- Set of states: Σ ;
- Initial states: $I \subseteq \Sigma$;
- Transition relation: $\tau \subseteq \Sigma \times \Sigma$;
- Transition system: $\langle \Sigma, \tau, I \rangle$;
- Complete lattice: $\langle \wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap \rangle$;
- Right-image of $X \subseteq \Sigma$ by τ : $post[\tau](X) \stackrel{\triangle}{=} \{s' \mid \exists s \in X : \langle s, s' \rangle \in \tau\};$
- Reflexive transitive closure of τ : τ^{\star}

 $\blacktriangleleft \triangleleft \lhd - 8 - [\blacksquare - \triangleright \square \blacktriangleright$

Example (contd.)

- \bullet Safety specification: $S\subseteq \Sigma$
- Reachable states from *I*:

$$post[\tau^{\star}](I) = lfp^{\leq} \lambda X \cdot I \cup post[\tau](X);$$

• Satisfaction of the safety specification $(post[\tau^{\star}](I) \subseteq S)$:

$$lfp^{\leq} \lambda X \cdot I \lor post[\tau](X) \leq S ?$$

 $\blacktriangleleft \triangleleft \lhd -9 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

Concrete Fixpoint Checking Algorithm ¹

Algorithm 1

 $X := I; Go := (X \le S);$ while Go do $X' := I \lor F(X);$ $Go := (X \ne X') \& (X' \le S);$ X := X';od; return $(X \le S);$

¹ P. Cousot & R. Cousot, POPL'77

KAIST, Taejon, Korea, Tuesday June 13th, 2000

 $\blacktriangleleft \triangleleft \lnot - 10 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

(c) P. COUSOT

Partial correctness of Alg. 1

Alg. 1 is partially correct: if it ever terminates then it returns $Ifp^{\leq} \lambda X \cdot I \lor F(X) \leq S$.





Galois connection

A Galois connection, written

$$\langle L, \leq \rangle \xleftarrow{g}{f} \langle M, \sqsubseteq \rangle,$$

is such that:

- $\langle L, \leq \rangle$ and $\langle M, \sqsubseteq \rangle$ are posets;
- the maps $f \in L \mapsto M$ and $g \in M \mapsto L$ satisfy

 $\forall x \in L : \forall y \in M : f(x) \sqsubseteq y \text{ if and only if } x \leq g(y) \text{ .}$

 $\blacktriangleleft \triangleleft \frown - 12 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

Concrete Adjoinedness

In general, F has an *adjoint* \widetilde{F} such that $\langle L, \leq \rangle \xleftarrow{\widetilde{F}}{F} \langle L, \leq \rangle$.

KAIST, Taejon, Korea, Tuesday June 13th, 2000



(c) P. COUSOT

Example of Concrete Adjoinedness

- τ^{-1} is the inverse of τ ;
- $pre[\tau] \stackrel{\triangle}{=} post[\tau^{-1}];$
- Set complement $\neg X \stackrel{\triangle}{=} \Sigma \setminus X$;
- $\widetilde{pre}[\tau](X) \stackrel{\triangle}{=} \neg pre[\tau](\neg X);$

$$\langle \wp(\Sigma), \ \subseteq \rangle \xleftarrow{\widetilde{pre}[\tau]}{\operatorname{post}[\tau]} \ \langle \wp(\Sigma), \ \subseteq \rangle \ .$$

 $\blacktriangleleft \triangleleft \lnot - 14 - | \blacksquare - \triangleright \triangleright \blacktriangleright$

Fixpoint Concrete Adjoinedness

$$\begin{aligned} & \operatorname{lfp}^{\leq} \boldsymbol{\lambda} X \cdot I \lor F(X) \leq S \\ \Leftrightarrow & \exists A \in L : I \leq A \& F(A) \leq A \& A \leq S \\ \Leftrightarrow & \exists A \in L : I \leq A \& A \leq \widetilde{F}(A) \& A \leq S \\ \Leftrightarrow & I \leq \operatorname{gfp}^{\leq} \boldsymbol{\lambda} X \cdot S \land \widetilde{F}(X) . \end{aligned}$$
(1)

whence

$$\langle L, \leq \rangle \xleftarrow{\boldsymbol{\lambda} S \cdot gfp^{\leq} \boldsymbol{\lambda} X \cdot S \wedge \widetilde{F}(X)}{\boldsymbol{\lambda} I \cdot Ifp^{\leq} \boldsymbol{\lambda} X \cdot I \vee F(X)} \langle L, \leq \rangle$$

KAIST, Taejon, Korea, Tuesday June 13th, 2000

 $\blacktriangleleft \triangleleft \frown -15 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

Concrete Invariants

- $A \in L$ an *invariant* for $\langle F, I, S \rangle$ if and only if $I \leq A \& F(A) \leq A \& A \leq S$;
- The set \mathcal{I} of invariants for $\langle F, I, S \rangle$ is a complete lattice $\langle \mathcal{I}, \leq, | fp^{\leq} \lambda X \cdot I \lor F(X), gfp^{\leq} \lambda X \cdot S \land \widetilde{F}(X), \lor, \land \rangle.$



Dual Concrete Fixpoint Checking Algorithm²

Algorithm 2

 $Y := S; Go := (I \le Y);$ while Go do $Y' := S \land \widetilde{F}(Y);$ Go := $(Y \ne Y') \& (I \le Y');$ Y := Y';od; return $(I \le Y);$

KAIST, Taejon, Korea, Tuesday June $13^{\rm th}$, 2000

 $\blacktriangleleft \triangleleft \frown - 17 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

(c) P. COUSOT

² P. Cousot, 1981; E.M. Clarke & E.A. Emerson, 1981; J.-P. Queille and J. Sifakis, 1982.

Partial correctness of Alg. 2

Alg. 2 is partially correct: if it ever terminates then it returns $Ifp^{\leq} \lambda X \cdot I \lor F(X) \leq S$.





On (Dual) Fixpoint Checking

 $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S$

if and only if

$$I \leq \operatorname{gfp}^{\leq} \lambda X \cdot S \wedge \widetilde{F}(X).$$

if and only if $\textit{Ifp}^{\leq} \ \pmb{\lambda} X \cdot I \lor F(X) \leq \textit{gfp}^{\leq} \ \pmb{\lambda} X \cdot S \land \widetilde{F}(X)$



The Adjoined Concrete Fixpoint Checking Algorithm

Algorithm 3

$$X := I; \ Y := S; \ Go := (X \le Y);$$

while Go do

$$X' := I \lor F(X); \ Y' := S \land \widetilde{F}(Y);$$

$$Go := (X \ne X') \& (Y \ne Y') \& (X' \le Y');$$

$$X := X'; \ Y := Y';$$

od;
return $(X \le Y);$

 $\triangleleft \triangleleft \neg - 20 - \square \blacksquare - \triangleright \square \triangleright$

Partial correctness of Alg. 3

Alg. 3 is partially correct: if it ever terminates then it returns $Ifp^{\leq} \lambda X \cdot I \lor F(X) \leq S$.





Abstract Fixpoint Checking

KAIST, Taejon, Korea, Tuesday June 13th, 2000





Abstract Interpretation

- Concrete complete lattice: $\langle L, \leq, 0, 1, \vee, \wedge \rangle$;
- Abstract complete lattice: $\langle M, \sqsubseteq, \bot, \top, \Box, \sqcup \rangle$;
- Abstraction/concretization pair $\langle \alpha, \gamma \rangle$;
- Galois connection:

 $\langle L, \leq \rangle \xleftarrow{\gamma} \langle M, \sqsubseteq \rangle.$



Example: the Recurrent Abstraction in Abstract Model-Checking

- State abstraction: $h \in \Sigma \mapsto \overline{\Sigma}$;
- Property abstraction: $\alpha_h(X) \stackrel{\triangle}{=} \{h(x) \mid x \in X\} = post[h]^3$;
- Property concretization: $\gamma_h(Y) \stackrel{\triangle}{=} \{x \mid h(x) \in Y\} = \widetilde{pre}[h];$
- Galois connection:

 $\langle \wp(\Sigma), \subseteq \rangle \xleftarrow{\gamma_h}{\alpha_h} \langle \wp(\overline{\Sigma}), \subseteq \rangle.$

• Example (rule of signs): $\Sigma = \mathbb{Z}$ so choose h(z) to be the sign of z.

 $\blacktriangleleft \triangleleft \frown - 24 - [\blacksquare - \triangleright \square \blacktriangleright$

³ Considering the function h as a relation.

Abstract Fixpoint Checking Algorithm ⁴

Algorithm 4

$$\begin{split} X &:= \alpha(I); \ Go := (\gamma(X) \leq S); \\ \textbf{while } Go \ \textbf{do} \\ X' &:= \alpha(I \lor F(\gamma(X))); \\ Go &:= (X \neq X') \& (\gamma(X') \leq S); \\ X &:= X'; \\ \textbf{od}; \\ \textbf{return if } (\gamma(X) \leq S) \ \textbf{then true else } I \ \textbf{don't know;} \end{split}$$

⁴ In P. Cousot & R. Cousot, POPL'77, $(\gamma(X) \leq S)$ is $X \sqsubseteq S'$ where $S' = \alpha(S)$.

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000

 $\blacktriangleleft \triangleleft \frown -25 - [\![\blacksquare - \triangleright]\!] \triangleright$

Partial correctness of Alg. 4

Alg. 4 is partially correct: if it terminates and returns "true" then $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S$.





Dual Abstraction







Example of Dual Abstraction

lf

- $\langle L, \leq, 0, 1, \vee, \wedge, \neg \rangle$ is a complete boolean lattice;
- $\langle M, \sqsubseteq, \bot, \top, \Box, \sqcup, \backsim \rangle$ is a complete boolean lattice;
- $\langle L, \leq \rangle \xleftarrow{\gamma}{\alpha} \langle M, \sqsubseteq \rangle;$
- $\widetilde{\alpha} \stackrel{\bigtriangleup}{=} \backsim \circ \alpha \circ \neg$ and $\widetilde{\gamma} \stackrel{\bigtriangleup}{=} \neg \circ \gamma \circ \backsim$

then

$$\langle L, \geq \rangle \xleftarrow{\widetilde{\gamma}}_{\widetilde{\alpha}} \langle M, \sqsupseteq \rangle$$

 $\blacktriangleleft \triangleleft \lnot - 28 - [\blacksquare - \triangleright \square \blacktriangleright]$

Example of Dual Abstraction (Contd.)

For the recurrent abstraction in abstract model-checking $\alpha_h(X)$ $\stackrel{\triangle}{=} \{h(x) \mid x \in X\} = post[h] \text{ we have:}$ • $\langle \wp(\Sigma), \subseteq \rangle \xleftarrow{\widetilde{pre}[h]} \langle \wp(\Sigma), \subseteq \rangle;$ • $\widetilde{pre}[h](X) = \neg pre[h](\neg X) \text{ and } \widetilde{post}[h](X) = \neg post[h](\neg X),$ so: • $\langle \wp(\Sigma), \supset \rangle \xleftarrow{pre[h]} \langle \wp(\Sigma), \supset \rangle$

•
$$\langle \wp(\Sigma), \supseteq \rangle \xleftarrow{i \to 1} \langle \wp(\Sigma), \supseteq \rangle.$$

 $\widetilde{post[h]}$

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000

 $\blacktriangleleft \triangleleft \frown - 29 - || \blacksquare - \triangleright || \triangleright ||$

Abstract Adjoinedness

$$\langle L, \leq \rangle \xleftarrow{\gamma}{\alpha} \langle M, \sqsubseteq \rangle, \langle L, \leq \rangle \xleftarrow{\widetilde{F}}{F} \langle L, \leq \rangle \text{ and } \langle L, \geq \rangle \xleftarrow{\widetilde{\gamma}}{\widetilde{\alpha}} \langle M, \sqsupseteq \rangle \text{ imply:}$$

$$\langle M, \sqsubseteq \rangle \xleftarrow{\widetilde{\alpha} \circ \widetilde{F} \circ \gamma}_{\alpha \circ F \circ \widetilde{\gamma}} \langle M, \sqsubseteq \rangle.$$

 $\blacktriangleleft \triangleleft \neg - 30 - | \blacksquare - \triangleright | \triangleright \triangleright$



The Dual Abstract Fixpoint Checking Algorithm

Algorithm 5

 $Y := \widetilde{\alpha}(S); Go := (I \leq \widetilde{\gamma}(Y));$ while Go do $Y' := \widetilde{\alpha}(S \wedge \widetilde{F}(\widetilde{\gamma}(Y)));$ $Go := (Y \neq Y') \& (I \leq \widetilde{\gamma}(Y'));$ Y := Y';od; return if $(I \leq \widetilde{\gamma}(Y))$ then true else I don't know;

 $\blacktriangleleft \triangleleft \neg - 31 - | \blacksquare - \triangleright \triangleright \blacktriangleright$

Partial correctness of Alg. 5

Alg. 5 is partially correct: if it terminates and returns "true" then $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S$.





The Particular Case of Complement Abstraction

⟨L, ≤, 0, 1, ∨, ∧, ¬⟩ is a complete boolean lattice;
 ⟨M, ⊑, ⊥, ⊤, ⊔, ⊓, ∽⟩ is a complete boolean lattice;
 ⟨L, ≤⟩ ↔ ⟨M, ⊑⟩;
 ⟨L, ≤⟩ ↔ ⟨F → ⟨L, ≤⟩;
 ℱ → ∘ F ∘ ¬, α → ∞ ∘ α ∘ ¬ and γ → ¬ ∘ γ ∘ ∽.

KAIST, Taejon, Korea , Tuesday June 13^{th} , 2000

 $\blacktriangleleft \triangleleft \neg - 33 - | \blacksquare - \triangleright | \triangleright \triangleright$

The Contrapositive Abstract Alg. 5 becomes: Fixpoint Checking Algorithm Algorithm 6

$$Z := \alpha(\neg S); \quad Go := (I \land \gamma(Z) = 0);$$

while Go do

$$Z' := \alpha(\neg S \lor F(\gamma(Z)));$$

$$Go := (Z \neq Z') \& (I \land \gamma(Z') = 0);$$

$$Z := Z';$$

od;

return if $(I \land \gamma(Z) = 0)$ then true else I don't know;

 $\blacktriangleleft \triangleleft - 34 - \| \blacksquare - \triangleright \square \triangleright \models$

Partial correctness of Alg. 6

Alg. 6 is partially correct: if it terminates and returns "true" then $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S$.





The Adjoined Abstract Fixpoint Checking Algorithm

Algorithm 7

 $X := \alpha(I); \ Y := \widetilde{\alpha}(S); \ Go := (\gamma(X) \le S) \& (I \le \widetilde{\gamma}(Y));$ while Go do

 $X' := \alpha(I \lor F \circ \gamma(X)); \ Y' := \widetilde{\alpha}(S \land \widetilde{F} \circ \widetilde{\gamma}(Y));$ $Go := (X \neq X') \& (Y \neq Y') \& (\gamma(X') \leq S) \& (I \leq \widetilde{\gamma}(Y'));$ $X := X'; \ Y := Y';$

od;

 $\mathbf{return} \ \mathbf{if} \ (\gamma(X) \leq S) \ | \ (I \leq \widetilde{\gamma}(Y)) \ \mathbf{then} \ \mathit{true} \ \mathbf{else} \ \mathit{I} \ \mathit{don't} \ \mathit{know};$

 $\blacktriangleleft \triangleleft \neg - 36 - | \blacksquare - \triangleright \square \triangleright$

Partial correctness of Alg. 7

Alg. 7 is partially correct: if it terminates and returns "true" then $Ifp^{\leq} \lambda X \cdot I \vee F(X) \leq S$.





Further Requirements for Program Static Analysis

- In program static analysis, one cannot compute γ , $\tilde{\gamma}$ and \leq and sometimes neither I nor S may even be machine representable;
- So Alg. 7, which can be useful in model-checking, is of *limited interest* in program static analysis;
- Such problems do no appear in abstract model checking since the concrete model is almost always machine-representable (although sometimes too large).

 $\blacktriangleleft \triangleleft - 38 - \blacksquare - \triangleright \triangleright \blacktriangleright$

Additional Hypotheses

In order to be able to check termination in the abstract, we assume:

1. $\forall X \in L : \gamma \circ \widetilde{\alpha}(X) \leq X$; 2. $\forall X \in L : X \leq \widetilde{\gamma} \circ \alpha(X)$.





Example: the Recurrent Abstraction in Abstract Model-Checking

Continuing with the abstraction of p. 24 with

$$\alpha \stackrel{\triangle}{=} post[h] \qquad \gamma \stackrel{\triangle}{=} \widetilde{pre}[h]$$

and
$$\widetilde{\alpha} \stackrel{\triangle}{=} \widetilde{post}[h] \qquad \widetilde{\gamma} \stackrel{\triangle}{=} pre[h],$$

we have: 1. $\forall X \in L : \gamma \circ \widetilde{\alpha}(X) \subseteq X$; 2. $\forall X \in L : X \subseteq \widetilde{\gamma} \circ \alpha(X)$.

KAIST, Taejon, Korea, Tuesday June $13^{\rm th}$, 2000

 $\blacktriangleleft \triangleleft \lnot - 40 - [\blacksquare - \rhd \bowtie \blacktriangleright$

The Adjoined Abstract Fixpoint Abstract Checking Algorithm

Algorithm 8

$$\begin{split} X &:= \alpha(I); \ Y := \widetilde{\alpha}(S); \ Go := (X \sqsubseteq Y); \\ \textbf{while } Go \ \textbf{do} \\ X' &:= \alpha(I) \sqcup \alpha \circ F \circ \gamma(X); \ Y' := \widetilde{\alpha}(S) \sqcap \widetilde{\alpha} \circ \widetilde{F} \circ \widetilde{\gamma}(Y); \\ Go &:= (X \neq X') \& (Y \neq Y') \& (X' \sqsubseteq Y'); \\ X &:= X'; \ Y := Y'; \\ \textbf{od}; \end{split}$$

return if $X \sqsubseteq Y$ then true else I don't know;

 $\blacktriangleleft \blacktriangleleft \lhd -41 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

Partial correctness of Alg. 8

Alg. 8 is partially correct: if it ever terminates and returns "true" then $lfp^{\leq} \lambda X \cdot I \vee F(X) \leq S$.





Partially complete abstraction

KAIST, Taejon, Korea, Tuesday June 13th, 2000





Partially Complete Abstraction (definition) 5

Definition 9 The abstraction $\langle \alpha, \gamma \rangle$ is *partially complete* if, whenever Alg. 4 terminates and $Ifp \stackrel{\leq}{\longrightarrow} \lambda X \cdot I \lor F(X) \leq S$ then the returned result is "*true*".

 $\blacktriangleleft \triangleleft \lnot - 44 - [\blacksquare - \triangleright \square \blacktriangleright$

⁵ Observe that this notion of *partial completeness* is different from the notions of *fixpoint completeness* ($\alpha(Ifp^{\leq}G) = Ifp^{\equiv} \alpha \circ G \circ \gamma$) and the stronger one of *local completeness* ($\alpha \circ G = \alpha \circ G \circ \gamma \circ \alpha$) considered in P. Cousot & R. Cousot, POPL'79.

Characterization of Partially Complete Abstractions for Algorithm 4

Theorem 10 The abstraction $\langle \alpha, \gamma \rangle$ is partially complete for Alg. 4 if and only if $\alpha(L)$ contains an abstract value A such that $\gamma(A)$ is an invariant for $\langle F, I, S \rangle$.

Intuition: finding a partially complete abstraction is as difficult as making an invariance proof (since finding the invariant is the only difficulty).

 $\blacktriangleleft \triangleleft - 45 - | \blacksquare - \triangleright | \triangleright \triangleright$

The <u>Most</u> Abstract Partially Complete Abstraction (Definition)

Definition 11 The most abstract partially complete abstraction $\langle \overline{\alpha}, \overline{\gamma} \rangle$, if it exists, is defined such that:

- 1. The abstract domain $\overline{M} = \overline{\alpha}(L)$ has the smallest possible cardinality;
- 2. If another abstraction $\langle \alpha', \gamma' \rangle$ is a partially complete abstraction with the same cardinality, then there exists a bijection β such that $\forall x \in \overline{M} : \gamma'(\beta(x)) \leq \overline{\gamma}(x)^{-6}$.

 $\blacktriangleleft \triangleleft \lnot - 46 - [\blacksquare - \triangleright \square \blacktriangleright$

⁶ Otherwise stated, the abstract values in $\overline{\alpha}(L)$ are more approximate than the corresponding elements in $\alpha'(L)$.

Characterization of the <u>Most</u> Abstract Complete Abstraction

Theorem 12 The most abstract partially complete abstraction for Alg. 4 is such that:

- if S = 1 then $\overline{M} = \{\top\}$ where $\overline{\alpha} \stackrel{\triangle}{=} \lambda X \cdot \top$ and $\overline{\gamma} \stackrel{\triangle}{=} \lambda Y \cdot 1$;
- if $S \neq 1$ then $\overline{M} = \{\bot, \top\}$ where $\bot \sqsubseteq \bot \sqsubset \top \sqsubseteq \top$ with $\langle \overline{\alpha}, \overline{\gamma} \rangle$ such that:

 $\overline{\alpha}(X) \stackrel{\Delta}{=} \text{ if } X \leq gfp^{\leq} \lambda X \cdot S \wedge \widetilde{F}(X) \text{ then } \perp \text{ else } \top$ $\overline{\gamma}(\perp) \stackrel{\Delta}{=} gfp^{\leq} \lambda X \cdot S \wedge \widetilde{F}(X) \qquad (2)$ $\overline{\gamma}(\top) \stackrel{\Delta}{=} 1$

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000

 $\blacktriangleleft \triangleleft - 47 - | \blacksquare - \triangleright | \triangleright \triangleright$

The Least Abstract Partially Complete Abstraction (Definition)

Definition 13 Dually, the *least abstract partially complete abstraction* $\langle \overline{\alpha}, \overline{\gamma} \rangle$, if it exists, is defined such that:

- 1. The abstract domain $\overline{M} = \overline{\alpha}(L)$ has the smallest possible cardinality;
- 2. If another abstraction $\langle \alpha', \gamma' \rangle$ is a partially complete abstraction with the same cardinality, then there exists a bijection β such that $\forall x \in \overline{M} : \overline{\gamma}(x) \leq \gamma'(\beta(x))^{-7}$.

 $\blacktriangleleft \triangleleft \lnot - 48 - [\blacksquare - \triangleright \square \blacktriangleright$

⁷ Otherwise stated, the abstract values in $\overline{\alpha}(L)$ are less approximate than the corresponding elements in $\alpha'(L)$.

Characterization of the <u>Least</u> Abstract Complete Abstraction

Theorem 14 Dually, the least abstract partially complete abstraction for Alg. 4 is such that:

- if I = 1 then $\underline{M} = \{\top\}$ where $\underline{\alpha} \stackrel{\triangle}{=} \lambda X \cdot \top$ and $\underline{\gamma} \stackrel{\triangle}{=} \lambda Y \cdot 1$;
- if $I \neq 1$ then $\underline{M} = \{\bot, \top\}$ where $\bot \sqsubseteq \bot \sqsubset \top \sqsubseteq \top$ with $\langle \underline{\alpha}, \underline{\gamma} \rangle$ such that:

 $\underline{\alpha}(X) \stackrel{\triangle}{=} \text{ if } X \leq I f p^{\leq} \lambda X \cdot I \vee F(X) \text{ then } \bot \text{ else } \top$ $\underline{\gamma}(\bot) \stackrel{\triangle}{=} I f p^{\leq} \lambda X \cdot I \vee F(X) \qquad (3)$ $\underline{\gamma}(\top) \stackrel{\triangle}{=} 1$

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000

 $4 \leq 4 \leq -49 = 1 = - > \Rightarrow >$

The Minimal Partially Complete Abstractions for Algorithm 4

Theorem 15

• The set \mathcal{A} of partially complete abstractions of minimal cardinality for Alg. 4 is the set of all $\langle M, \sqsubseteq, \alpha, \gamma \rangle$ such that $M = \{\bot, \top\}$ with $\bot \sqsubseteq \bot \sqsubseteq \top \sqsubseteq \top, \langle L, \leq \rangle \xleftarrow{\gamma}{\alpha} \langle M, \sqsubseteq \rangle$, $\gamma(\bot) \in \mathcal{I}$ and $\bot = \top$ if and only if $\gamma(\top) \in \mathcal{I}$.

 $\blacktriangleleft \triangleleft \lnot - 50 - [\blacksquare - \triangleright \bowtie \blacktriangleright$

The Complete Lattice of Minimal Complete Abstractions for Alg. 4

Theorem 16

- The relation $\langle \{\bot, \top\}, \sqsubseteq, \alpha, \gamma \rangle \preceq \langle \{\bot', \top'\}, \sqsubseteq', \alpha', \gamma' \rangle$ if and only if $\gamma(\bot) \leq \gamma'(\bot')$ is a pre-ordering on \mathcal{A} .
- Let $\langle \{\bot, \top\}, \sqsubseteq, \alpha, \gamma \rangle \cong \langle \{\bot', \top'\}, \sqsubseteq', \alpha', \gamma' \rangle$ if and only if $\gamma(\bot) = \gamma'(\bot')$ be the corresponding equivalence.
- The quotient \mathcal{A}_{\cong} is a complete lattice ⁸ for \preceq with infimum class representative $\langle \underline{M}, \underline{\sqsubseteq}, \underline{\alpha}, \gamma \rangle$ and supremum $\langle \overline{M}, \overline{\sqsubseteq}, \overline{\alpha}, \overline{\gamma} \rangle$.

 $\blacktriangleleft \triangleleft \lnot - 51 - [\blacksquare - \triangleright \square \blacktriangleright]$

⁸ Observe however that it is not a sublattice of the lattice of abstract interpretations of P. Cousot & R. Cousot, POPL'77, POPL'79 with reduced product as glb.

Intuition for Minimal Partially Complete Abstractions

- There is a one to one correspondance partially complete abstractions of minimal cardinality for Alg. 4 and the set of invariants for proving $lfp \stackrel{\leq}{\longrightarrow} \lambda X \cdot I \lor F(X) \leq S$;
- Similar results hold for the other Algs. 6, 7 & 8.



Conclusion

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000



© P. Cousot

On the Automatic Inference of Partially Complete Abstractions

- The automatic inference of partially complete abstractions is an active subject of research ¹¹;
- Th. 10 shows that the problem boils down to the automatic inference of invariants;
- After immoderate hopes in the seventies, there was no breakthrough for the last 20 years in automatic program proving;

¹¹ Graf & Loiseaux, CAV'93; Loiseaux, Graf, Sifakis, Bouajjani & Bensalem FMSD(6:1)'95, Graf & Saïdi, CAV'97; Bensalem, Lakhnech & Owre CAV'98; Colon & Uribe, CAV'98; Abdulla, Annichini, Bensalem, Bouajjani, Habermehl & Lakhnech, CAV'99; Das, Dill & Park, CAV'99; Saïdi & Shankar, CAV'99, etc.

On the Automatic Inference of Partially Complete Abstractions (contd.)

• Can we expect the abstraction to be ever automatized in abstract model-checking?





THE END, THANK YOU.

KAIST, Taejon, Korea , Tuesday June $13^{\rm th}$, 2000



