Comparing completeness properties of static analyses and their logics

David A. Schmidt[*]

Kansas State University, Manhattan, Kansas, USA

Abstract. Static analyses calculate abstract states, and their logics validate properties of the abstract states. We place into perspective the variety of forwards, backwards, functional, and logical completeness used in abstract-interpretation-based static analysis by giving examples and by proving equivalences, implications, and independences. We expose two fundamental Galois connections that underlie the logics for static analyses and reveal a new completeness variant, *O-completeness*. We also show that the key concept underlying logical completeness is *covering*, which we use to relate the various forms of completeness.

When we use a static analysis, like data-flow analysis or model checking, to validate a program for correctness or code improvement, we must carefully define the domain of properties the analysis can calculate so that it includes both the goal properties we seek to validate as well as intermediate properties that lead to the goals. Say we try to validate $\{?\}\mathtt{y := -y; x := y + 1}\{\mathit{isPositive}(\mathtt{x})\}$; our analysis requires properties like *isNegative* to calculate a sound precondition: $\{\mathit{isNegative}(\mathtt{y})\}\ \mathtt{y := -y}\ \{\mathit{isPositive}(\mathtt{y})\}\ \mathtt{x := y + 1}\ \{\mathit{isPositive}(\mathtt{x})\}$. But, is the analysis *complete* — as expressive as possible? If we can express the properties, *isNonNegative* and *isNonPositive*, then a complete analysis calculates the weakest precondition: $\{\mathit{isNonPositive}(\mathtt{y})\}\ \mathtt{y := -y; x := y + 1}\ \{\mathit{isPositive}(\mathtt{x})\}$.

The example suggests that "completeness" is a property of both static analyses as well as logics. Thanks to Cousot and Cousot [6–8, 11], we have a well-defined notion of *functional completeness*: it is when a static analysis's abstract state-transition function precisely mimicks the concrete state-transition function, modulo the Galois connection between concrete and abstract domains.

Giacobazzi, Ranzato, and Scozarri [17] showed how to refine an abstract interpretation to synthesize functionally complete transition functions; Giacobazzi and Quintarelli [16] showed that there are, in fact, two, independent notions of functional completeness — *forwards* and *backwards*. Cousot and Cousot [11] applied functional completeness to define the *logical completeness* of a logic that judges abstract values as compared to the logic that judges the concrete values. Recently, Ranzato and Tapparo [23, 24] applied Giacobazzi, et al.'s refinement techniques to build logically complete abstract logics.

The present paper's contribution is to place into perspective the variants of forwards, backwards, functional, and logical completeness by giving examples

[*] `schmidt@cis.ksu.edu`. Supported by NSF ITR-0086154 and ITR-0326577.

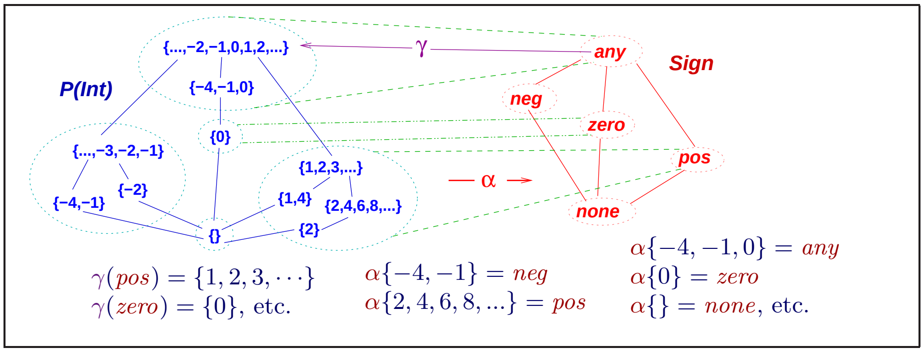


Fig. 1. Galois connection for signs; equivalence classes circled

and by proving equivalences, implications, and independences. By exposing two fundamental Galois connections that underlie logics for abstract values, we reveal yet another completeness variant, *O-logical-completeness*. We also show that the key concept underlying logical completeness notions is *covering*, which we use to relate the various forms of completeness.

1 Galois connections and functional completeness

We use Galois connections to abstract concrete data into properties. A *Galois connection* [8, 15] between two partially ordered sets, $(C, \subseteq)$ and $(A, \sqsubseteq)$, written $C\langle\alpha, \gamma\rangle A$, is a pair of functions, $\alpha : C \to A$ and $\gamma : A \to C$, such that for all $c \in C$ and $a \in A$,

$$c \subseteq \gamma(a) \text{ iff } \alpha(c) \sqsubseteq a.$$

The adjunction is equivalently defined by requiring that α and γ are monotone maps such that $id_{C\to C} \sqsubseteq \gamma \circ \alpha$ and $\alpha \circ \gamma \sqsubseteq id_{A\to A}$.

C is the *concrete domain* and A is the *abstract domain*. γ's adjoint, α, is uniquely defined as $\alpha(c) = \sqcap\{a \mid c \subseteq \gamma(a)\}$ and α's adjoint must be $\gamma(a) = \cup\{c \mid \alpha(c) \sqsubseteq a\}$[15]. γ is an *upper adjoint* of a Galois connection iff it preserves meets: $\gamma(\sqcap T) = \cap_{a\in T}\gamma(a)$, for all $T \subseteq A$. Similarly, α is a *lower adjoint* iff it preserves joins: $\alpha(\cup S) = \sqcup_{c\in S}\alpha(c)$, for all $S \subseteq C$ [15].

Figure 1 displays the classic Galois connection that abstracts sets of integers to their signs [8]. (In the Figure, C is $\mathcal{P}(Int)$ and A is $Sign$.) Each $S \in \mathcal{P}(Int)$ is abstracted to $\alpha(S) \in Sign$. Values like pos and any can be read as primitive logical propositions ($isPositive$ and $true$, respectively) or they can be used as abstract arguments and answers to static-analysis functions (e.g. $succ^\sharp(zero) = pos$). The Galois connection is *overapproximating* because $S \subseteq \gamma(\alpha(S))$, for all $S \in \mathcal{P}(C)$.

The following little-known result [21] exposes the inner structure of Galois connections:[1] *There is a Galois connection between* $(C, \subseteq)$ *and* $(A, \sqsubseteq)$ *iff*

[1] In this paper, definitions and previously proved results are embedded into the text narrative. New results and new variations of known results are stated as Propositions,

1. *C is partitioned into equivalence classes, each class, p, having a unique maximal element, $max(p)$; A is partitioned into equivalence classes, each class, q, having a unique minimal element, $min(q)$; the subposet of maximal elements in C is order-isomorphic to the subposet of minimal elements in A.*
2. *For all $c, c' \in C$, if $c \subseteq c'$, then $max([c]_\alpha) \subseteq max([c']_\alpha)$, where $[c]_\alpha$ is c's equivalence class.*
3. *For all $a, a' \in A$, if $a \sqsubseteq a'$, then $min([a]_\gamma) \sqsubseteq min([a']_\gamma)$, where $[a]_\gamma$ is a's equivalence class.*

Figure 1 illustrates the internal structure: α and γ partition their domains into equivalence classes, where the images of the two functions are order-isomorphic. Each concrete equivalence class "droops" from its canonical (maximal) element, and each abstract class "floats" from its canonical (minimal) element. In Figure 1, α is onto (hence, γ is one-one), making *Sign*'s equivalence classes singletons. The concrete domain's canonical elements are $\emptyset$, $\{\cdots, -2-1\}$, $\{0\}$ $\{1, 2, 3, \cdots\}$, and *Int*. (This is γ's image; α's image is *Sign*.) When α is onto, the Galois connection is characterized by $\gamma \circ \alpha$, a *closure map* [8, 17].

1.1 The internal logic defined by a Galois connection

For Galois connection, $C\langle\alpha, \gamma\rangle A$, say that $c \in C$ *has property* $a \in A$, written $c \models a$, iff $c \subseteq \gamma(a)$ (equivalently, iff $\alpha(c) \sqsubseteq a$). Read the elements of A as assertions in a logic with conjunction, because $c \models a_1 \sqcap_A a_2$ iff $c \models a_1$ and $c \models a_2$. This is because γ preserves $\sqcap_A$ as $\cap_C$.

Other connectives might be present (e.g., disjunction), but this is not the case for *Sign* in Figure 1, e.g., $\{0\} \models neg \sqcup pos$, but $\{0\} \not\models neg$ and $\{0\} \not\models pos$, because γ fails to preserve $\sqcup$. We will see that such "γ-preservations" lead to one notion of completeness and that there is a dual notion of "α preservation."

1.2 Sound abstract transformers

For Galois connection, $C\langle\alpha, \gamma\rangle A$, a state-transition function, $f : C \to C$, can be approximated: We say that a monotonic $f^\sharp : A \to A$ *is sound for* $f : C \to C$ iff $\alpha \circ f \sqsubseteq_{C \to A} f^\sharp \circ \alpha$, or equivalently, iff $f \circ \gamma \sqsubseteq_{A \to C} \gamma \circ f^\sharp$. That is, when $\alpha(c) = a$, $f^\sharp(a)$ computes an answer that is weaker (with respect to $\sqsubseteq_A$) than the name of $f(c)$'s α-equivalence class:

$$\begin{tikzcd} c \arrow[r, "f"] \arrow[d, "\alpha"'] & f(c) \arrow[r, "\alpha"] & \alpha(\ f(c)\ ) \arrow[d, phantom, "\sqsubseteq" sloped] \\ \alpha(\ c\ ) \arrow[rr, "f^\#"] & & f^\#(\ \alpha(\ c\ )) \end{tikzcd}$$

This makes $f^\sharp$ an overapproximation of f: $f(c) \subseteq \gamma(f^\sharp(\alpha(c)))$. The map, $f^\sharp_{best} = \alpha \circ f \circ \gamma$, is the "best" abstraction of f in the sense that $f^\sharp_{best}$ is sound for f and $f^\sharp_{best} \sqsubseteq_{A \to A} f^\sharp$ for all sound $f^\sharp$ [8] — it is the best one can do with f, α, and γ.

Theorems, and Corollaries. Due to lack of space, some proofs are omitted but can be found in the paper's accompanying technical report [28].

For Sign in Figure 1, the transformer, $\mathit{succ}^* : \mathcal{P}(\mathit{Int}) \rightarrow \mathcal{P}(\mathit{Int})$ is soundly abstracted by $\mathit{succ}^\sharp_0(a) = \mathit{any}$, whereas the best abstract transformer is $\mathit{succ}^\sharp_{\mathit{best}} = \alpha \circ \mathit{succ}^* \circ \gamma$, where $\mathit{succ}^\sharp_{\mathit{best}}(\mathit{zero}) = \mathit{succ}^\sharp_{\mathit{best}}(\mathit{pos}) = \mathit{pos}$. (For $f : C \rightarrow C$, define $f^* : \mathcal{P}(C) \rightarrow \mathcal{P}(C)$ as $f^*(S) = \{f(c) \mid c \in S\}$. Thus, for $\mathit{succ}(n) = n + 1$, we have $\mathit{succ}^*(S) = \{n + 1 \mid n \in S\}$.)

1.3 Complete abstract transformers

When the inclusions that define soundness are strengthened into equalities, this defines *functional completeness*: for $f : C \rightarrow C$ and $f^\sharp : A \rightarrow A$,

- $f^\sharp$ *is backwards (B(α)-) complete for* f iff $\alpha \circ f = f^\sharp \circ \alpha$ [8, 17]. That is, α is a homomorphism that preserves f as $f^\sharp$.
- $f^\sharp$ *is forwards (F(γ)-) complete for* f iff $f \circ \gamma = \gamma \circ f^\sharp$ [16]. That is, γ is a homomorphism that preserves $f^\sharp$ as f.

We say that $f^\sharp$ is B- (respectively, F-) complete when the α (resp. γ) is clear from the context. The two completeness notions are *not* equivalent [16], and the distinctions are subtle: For $c, c' \in C$, write $c \sim_\alpha c'$ iff $\alpha(c) = \alpha(c')$.

- There exists a B-complete $f^\sharp$ for f iff for all $c, c' \in C$, $c \sim_\alpha c'$ implies $f(c) \sim_\alpha f(c')$. In this case, we say that f *itself* is B-complete.

For B-complete $f^\sharp$, $f^\sharp(a)$ computes the *α-equivalence class* of $f(c)$, for every $c \in \gamma(a)$, but the specific value within the equivalence class is lost. If $f^\sharp$ is B-complete for f, then so is $f^\sharp_{\mathit{best}} = \alpha \circ f \circ \gamma$. So, f itself is B-complete iff $\alpha \circ f = f^\sharp_{\mathit{best}} \circ \alpha$. If α is onto and there is a B-complete $f^\sharp$ for f, then it is $f^\sharp_{\mathit{best}}$ [17].

- There exists an F-complete $f^\sharp$ for f iff for all $c \in \gamma[A]$, $f(c) \in \gamma[A]$.[2] In this case, we say that f *itself* is F-complete [16].

For F-complete $f^\sharp$, $f^\sharp(a)$ computes the *concrete value of f applied to the canonical element,* $\gamma(a) \in C$ — it computes $\gamma(f^\sharp(a))$ — but the values and even the *equivalence-class names* of the noncanonical elements in C are lost. If $f^\sharp$ is F-complete for f, so is $f^\sharp_{\mathit{best}}$; f itself is F-complete iff $f \circ \gamma = \gamma \circ f^\sharp_{\mathit{best}}$. If γ is 1-1 and there is an F-complete $f^\sharp$ for f, then it is $f^\sharp_{\mathit{best}}$ [16].

The existence of a B- and an F-complete $f^\sharp$ for f depend solely on the Galois connection and f itself. Figure 2 graphs the behaviors of a B-complete and an F-complete $f : C \rightarrow C$ on the equivalence classes of C induced by a Galois connection. Based on Figures 1 and 2, we can readily verify some Sign-completeness properties: square^* is B-complete but not F-complete; negate^* is both B- and F-complete; succ^* is neither;[3] and enum^* is F-complete but not B-complete, where $\mathit{enum}(n) = \mathit{if}\ (n\ \mathit{mod} 2 = 0)\ \mathit{then}\ (n\ \mathit{div} 2)\ \mathit{else}\ (n\ \mathit{div}(-2))$.

When α is not onto (that is, γ is not 1-1), there can be multiple abstract transformers $f^\sharp$ that are F-complete for f:

[2] Please recall, for function $f : C \rightarrow C$ and set $S \subseteq C$, that $f[S]$ denotes $\{f(s) \mid s \in S\}$.

[3] where $\mathit{square}(n) = n * n$ and $\mathit{negate}(n) = -n$ and $\mathit{succ}(n) = n + 1$

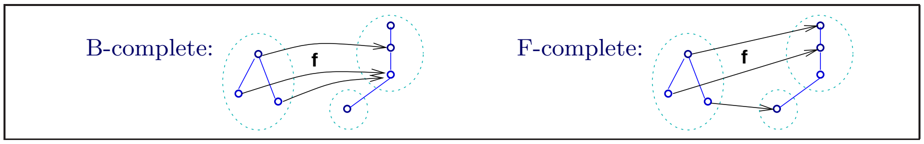


Fig. 2. Behavior of a B-complete and an F-complete $f : C \to C$

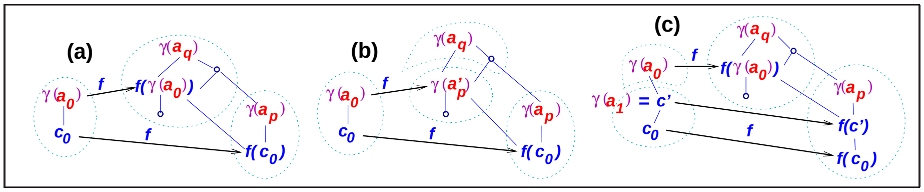


Fig. 3. Incompleteness (a) and its forwards (b) and backwards (c) refinements

Proposition 1. *$f \circ \gamma = \gamma \circ f^\sharp$ iff, for all $a \in A$, (i) $f(\gamma(a)) \in \gamma[A]$, and (ii) $f^\sharp_{best}(a) \sim_\gamma f^\sharp(a)$.*

Proof. The only-if-part is immediate: Since $f \circ \gamma = \gamma \circ f^\sharp$, then $f(\gamma(a)) \in \gamma[A]$ and $\gamma \circ \alpha \circ f \circ \gamma = \gamma \circ f^\sharp$. For the if-part, by (ii) we have $\gamma \circ f^\sharp = \gamma \circ \alpha \circ f \circ \gamma$, which equals $f \circ \gamma$, by (i). □

Proposition 2. *$\alpha \circ f = f^\sharp \circ \alpha$ iff, (i) for all $c, c' \in C$, $c \sim_\alpha c'$ implies $f(c) \sim_\alpha f(c')$, and (ii) for all $a \in \alpha[C]$, $f^\sharp_{best}(a) = f^\sharp(a)$.*

Proof. Similar to the previous Proposition. □

Say that $f : C \to C$ is not itself F-complete (see Figure 3(a)); to make it so, we must ensure that f maps C-canonical arguments to C-canonical answers. To do this, for each $c \in \gamma[A]$ (that is, $c = \gamma(a_0)$), where $f(c) \notin \gamma[A]$, we make a new equivalence class, $\downarrow f(c) \cap [f(c)]_\alpha$, in C whose maximal, canonical element is $f(c) = \gamma(a'_p)$, where a'_p is a new A-element.[4] If we close the canonical elements under $\cap$ (making even more new equivalence classes) and repeat until convergence, then f becomes F-complete. This is the *F-complete-shell construction* [16, 23] — it adds elements by computing "forwards" from f. See Figure 3(b).

For example, since *square** is not F-complete for *Sign*, we systematically add to *Sign* new values that represent the canonical elements, $\{1, 4, 9, \cdots\}$, $\{1, 16, 81, \cdots\}$, $\{1, 256, 6561, \cdots\}$, $\ldots$; this time, the procedure does not finitely converge.

Dually, if $f : C \to C$ is not B-complete, we must make f map α-related arguments to α-related answers. We can either split equivalence classes in f's domain (the *B-complete shell construction* [17]) or merge equivalence classes in f's range (the *B-complete-core construction* [17]).

[4] Recall, for $c \in C$, that $\downarrow c = \{c' \in C \mid c' \subseteq c\}$.

Consider the former, and say there is some $c_0 \in C$ such that $f(c_0) \not\sim_\alpha f(max[c_0]_\alpha)$. We compute the set, $[c_0]_\alpha \cap f^{-1}([f(c_0)]_\alpha)$, and we select the maximal elements, c', from this set as the canonical elements of new equivalence classes, $\downarrow c' \cap [c']_\alpha$. If we close under $\cap$ and repeat until convergence, then f becomes B-complete.[5] The B-complete shell construction adds elements by computing "backwards" from f. See Figure 3(c).

For example, $succ^*$ is not B-complete for $Sign$, because $succ^*\{-1,-2,...\} \not\sim_\alpha succ^*\{-2\}$: the former maps into Int's equivalence class, and the latter maps into the class of negative ints. $[\{-2\}]_\alpha \cap f^{-1}[succ^*\{-2\}]_\alpha$ collects all nonempty sets of negative numbers less than -1; the maximal set in this collection is $\{-2,-3,\cdots\}$, and this set becomes the canonical element of a new equivalence class. We repeat the refinements and add these new canonical elements: $\{-i,-(i+1),...\}$ and $\{-i\}$, for all $i > 1$.

The shell constructions show that the match between $f : C \to C$ and Galois connection $\alpha\langle C, A\rangle\gamma$ must be "perfect" to achieve completeness.

The fixed point operators are well behaved with respect to completeness: Say that when $f^\sharp$ is B- (resp., F-)complete for f, then $G^\sharp(f^\sharp)$ is B- (F-)complete for $G(f)$. We have

- $\alpha \circ lfpG = lfpG^\sharp \circ \alpha$, when α is continuous
- $\alpha \circ gfpG = gfpG^\sharp \circ \alpha$, when α is co-continuous and $\alpha(\top) = \top$
- $lfpG \circ \gamma = \gamma \circ lfpG^\sharp$, when γ is continuous and $\gamma(\bot) = \bot$
- $gfpG \circ \gamma = \gamma \circ lfpG^\sharp$, when γ is co-continuous.

See Cousot and Cousot [8] and Ranzato and Tapparo [25] for elaboration.

2 Program logics

A *logic for* C consists of a set of assertions, $\mathcal{L}$, and a judgement relation, $\models \subseteq C \times \mathcal{L}$; we write $c \models \phi$ when (c, ϕ) is in the relation. For example, a $\models$ based on Figure 1 might give us $\{2,4,6\} \models even$ and $\{4\} \models any$.

Section 1.1 noted that a Galois connection defines an "internal logic," where $\mathcal{L} = A$ and for all $c \in C$, $c \models a$ iff $c \subseteq \gamma(a)$ (iff $\alpha(c) \sqsubseteq a$). But most program logics are extensions of A, and given a Galois connection, $\mathcal{P}(D)\langle\alpha,\gamma\rangle A$ — *the concrete domain is a powerset* — we obtain this *inductively defined logic*:

1. an inductively defined set of assertions,

$$\mathcal{L} \ni \phi ::= a \mid op_i(\phi_j)_{0<j\leq ar(i)}, \text{ for } i \in I$$

   where op_i has arity $ar(i) \geq 0$, for every $i \in I$.
2. an inductively defined interpretation, $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(D)$:

$$\begin{aligned}&[\![a]\!] = \gamma(a)\\ &[\![op_i(\phi_j)_{0<j\leq ar(i)}]\!] = g_i([\![\phi_j]\!])_{0<j\leq ar(i)}, \quad \text{where } g_i : \mathcal{P}(D)^{ar(i)} \to \mathcal{P}(D).\end{aligned}$$

Given Galois connection, $\mathcal{P}(D)\langle\alpha,\gamma\rangle A$, define $\mathcal{L}$ as follows:

$$a \in \mathit{Prim} = A \text{ (the primitive assertions)}$$
$$\mathcal{L} \ni \phi ::= \ a \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid [f]\phi$$

$$[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(D)$$

$$\begin{array}{ll} [\![a]\!] = \gamma(a) & [\![[f]\phi]\!] = \widetilde{pre}_f[\![\phi]\!] \\ [\![\phi_1 \wedge \phi_2]\!] = [\![\phi_1]\!] \cap [\![\phi_2]\!] & \quad \text{where } \widetilde{pre}_f(S) = \{c \in D \mid f(c) \subseteq S\} \\ [\![\phi_1 \vee \phi_2]\!] = [\![\phi_1]\!] \cup [\![\phi_2]\!] & \quad \text{and } f : D \to \mathcal{P}(D) \text{ is a state-transition function} \end{array}$$

Fig. 4. An inductively defined precondition logic

For $S \in \mathcal{P}(D)$, define $S \models \phi$ iff $S \subseteq [\![\phi]\!]$. See the example in Figure 4. Using Figures 4 and 1 and one-variable assignment programs, we can validate, for example, the precondition assertion, $\{-2,-4,0\} \models [\mathtt{x} := -\mathtt{x}; \mathtt{x} := \mathtt{x}+1]pos$.

The logic defines program correctness and transformation properties, and when we wish to validate a precondition assertion like $S_0 \models [f]\phi$ (or a postcondition assertion like $f^*(S_0) \models \phi$) via a static analysis, we use $f^\sharp : A \to A$ to approximate $f^* : \mathcal{P}(D) \to \mathcal{P}(D)$ and we use $a_0 \in A$ to approximate S_0. We then attempt to validate $a_0 \models [f^\sharp]\phi$ (resp., $f^\sharp(a_0) \models^A \phi$):

- For $\mathcal{P}(D)\langle\alpha,\gamma\rangle A$, a judgement relation, $\models^A \subseteq A \times \mathcal{L}$, is γ*-sound* for $\models \subseteq \mathcal{P}(D) \times \mathcal{L}$ iff for all $a \in A$ and $\phi \in \mathcal{L}$, $a \models^A \phi$ implies $\gamma(a) \models \phi$.

For example, a γ-sound $\models^A$ might validate that $neg \models^A [\mathtt{x} := -\mathtt{x}; \mathtt{x} := \mathtt{x}+1]pos$.

Define $[\![\phi]\!]^A = \{a \mid a \models^A \phi\}$. Since γ is monotonic, it is natural to demand that $\models^A$ be *downclosed*: $a_0 \sqsubseteq_A a_1$ and $a_1 \models^A \phi$ imply $a_0 \models^A \phi$. Downclosure is central to soundness — here is a second definition of soundness that shows why:

- For $\mathcal{P}(D)\langle\alpha,\gamma\rangle A$, $\models^A \subseteq A \times \mathcal{L}$ is α*-sound* for $\models \subseteq \mathcal{P}(D) \times \mathcal{L}$ iff for all $S \in \mathcal{P}(D)$ and $\phi \in \mathcal{L}$, $\alpha(S) \models^A \phi$ implies $S \models \phi$.

Proposition 3. *If $\models^A$ is downclosed, then $\models^A$ is γ-sound for $\models$ iff $\models^A$ is α-sound for $\models$.*

Proof. If-part: From γ-soundness and $\alpha(S) \models^A \phi$, we infer that $\gamma(\alpha(S)) \models \phi$. Since $S \subseteq \gamma(\alpha(S))$, the downclosedness of $\models^A$ lets us deduce that $S \models \phi$.

Only-if part: Assume $a \models^A \phi$. Since $\alpha(\gamma(a)) \sqsubseteq a$, we have $\alpha(\gamma(a)) \models^A \phi$ by downclosedness. By α-soundness, we conclude that $\gamma(a) \models \phi$. □

Hereafter, we speak only of "soundness" and omit γ (resp., α).

Let $(\mathcal{P}_\downarrow(A), \subseteq)$ define the complete lattice of downclosed subsets of A, ordered by subset inclusion, and for $\gamma : A \to \mathcal{P}(D)$, define $\overline{\gamma} : \mathcal{P}_\downarrow(A) \to \mathcal{P}(D)$ as $\overline{\gamma}(T) = \gamma^*(T)$, that is, $\cup_{a \in T}\gamma(a)$.[6] Here is yet another equivalent definition of soundness, stated in terms of $\overline{\gamma}$, $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(D)$, and $[\![\cdot]\!]^A : \mathcal{L} \to \mathcal{P}_\downarrow(A)$:

[5] f must be chain continuous for the technique to converge correctly [16].

[6] $\mathcal{P}_\downarrow(A)$ is in fact the *disjunctive completion* of A [8, 9], often used to lift a γ that does not preserve $\sqcup_A$ into a $\overline{\gamma}$ that preserves $\cup_{\mathcal{P}_\downarrow(A)}$, in effect adding disjunction to $\mathcal{P}_\downarrow(A)$'s internal logic.

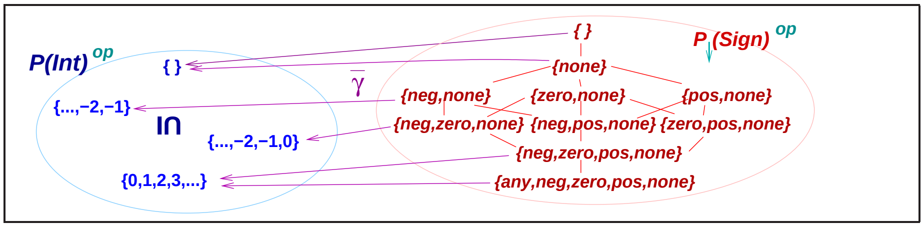


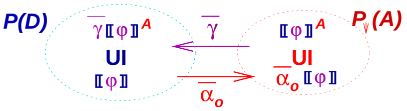
Fig. 5. Dualized disjunctive completion of Galois connection of signs

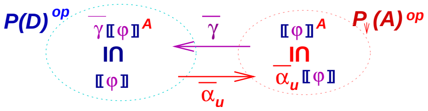
- $[\![\cdot]\!]^A$ *is sound for* $[\![\cdot]\!]$ iff $\overline{\gamma}[\![\phi]\!]^A \subseteq [\![\phi]\!]$, for all $\phi \in \mathcal{L}$.

This definition suggests an adjunction using $\overline{\gamma}$; there are *two* possible ones:

Proposition 4. *For $\mathcal{P}(D)$, $\mathcal{P}_\downarrow(A)$, and $\gamma : A \to \mathcal{P}(D)$,*

1. *$\mathcal{P}(D)\langle\overline{\alpha_o}, \overline{\gamma}\rangle\mathcal{P}_\downarrow(A)$ is a Galois connection, where $\overline{\alpha_o}(S) = \bigcap\{T \mid S \subseteq \overline{\gamma}(T)\} = \downarrow\{\alpha\{c\} \mid c \in S\}$, where $\downarrow T = \{a \mid$ exists $a' \in T$ such that $a \sqsubseteq a'\}$.*
2. *$\mathcal{P}(D)^{op}\langle\overline{\alpha_u}, \overline{\gamma}\rangle\mathcal{P}_\downarrow(A)^{op}$ is a Galois connection, where $\overline{\alpha_u}(S) = \bigcup\{T \mid \overline{\gamma}(T) \subseteq S\} = \{a \mid \gamma(a) \subseteq S\}$, where $(P, \sqsubseteq_P)^{op}$ is $(P, \sqsupseteq_P)$.*





The one and the same $\overline{\gamma}$ is the upper adjoint of both Galois connections because $\overline{\gamma}$ preserves *both* meets (intersections) *and* joins (unions) in $\mathcal{P}_\downarrow(A)$.[7]

Why two Galois connections? The one in Proposition 4(2) defines an underapproximation such that when we *define* $[\![\phi]\!]^A = \overline{\alpha_u}[\![\phi]\!]$, we underapproximate the concrete logic. The Galois connection in Proposition 4(1) can be used to overapproximate transforms, $f^* : \mathcal{P}(D) \to \mathcal{P}(D)$, by $f^\sharp : \mathcal{P}_\downarrow(A) \to \mathcal{P}_\downarrow(A)$. But the logical interpretation, $[\![\phi]\!]^A = \overline{\alpha_o}[\![\phi]\!]$, is sound *iff, for all $\phi \in \mathcal{L}$, $\overline{\gamma}(\overline{\alpha_o}[\![\phi]\!]) = [\![\phi]\!]$*.

Figure 5 shows the completion of $Sign$ to $\mathcal{P}_\downarrow(Sign)^{op}$. Here, $\overline{\alpha_u}$ is not onto, which becomes significant later. Proposition 4 justifies the following:

Proposition 5. *For $\phi \in \mathcal{L}$, the following are equivalent:*

1. *$[\![\cdot]\!]^A$ is sound for $[\![\cdot]\!]$, that is, $\overline{\gamma}[\![\phi]\!]^A \subseteq [\![\phi]\!]$, that is, $[\![\phi]\!]^A \subseteq \overline{\alpha_u}[\![\phi]\!]$.*
2. *$T \subseteq [\![\phi]\!]^A$ implies $\overline{\gamma}(T) \subseteq [\![\phi]\!]$, for all $T \in \mathcal{P}_\downarrow(A)$.*
3. *$\overline{\alpha_o}(S) \subseteq [\![\phi]\!]^A$ implies $S \subseteq [\![\phi]\!]$, for all $S \in \mathcal{P}(D)$.*
4. *$[\![\phi]\!] \subseteq S$ implies $[\![\phi]\!]^A \subseteq \overline{\alpha_u}(S)$, for all $S \in \mathcal{P}(D)$.*

Proof. It is easy to prove Item *1* equivalent to each of *2*, *3*, and *4*. Here is the equivalence of *1* and *3*:

1 implies 3: Assume $\overline{\alpha_o}(S) \subseteq [\![\phi]\!]^A$. By the definition of Galois connection, $S \subseteq \overline{\gamma}[\![\phi]\!]^A$. By *1*, $S \subseteq \phi$.

[7] If we use $\mathcal{P}(A)$ instead, we find that $\overline{\gamma} : \mathcal{P}(A) \to \mathcal{P}(D)$ does not preserve meets.

3 implies 1: By the definition of the Galois connection, $\overline{\alpha_o}(\overline{\gamma}\llbracket\phi\rrbracket^A) \subseteq \llbracket\phi\rrbracket^A$. Using *3* (set $S = \overline{\gamma}\llbracket\phi\rrbracket^A$), we have $\overline{\gamma}\llbracket\phi\rrbracket^A \subseteq \llbracket\phi\rrbracket$. □

The three adjunction maps, $\overline{\gamma}$, $\overline{\alpha_o}$, and $\overline{\alpha_u}$, give us three ways to define soundness. Items *3.* and *4.* in the Proposition justify the slogan that one "overapproximates the model" and "underapproximates the logic" for sound static analysis.

Finally, we note that a soundness assertion of the form, "$\overline{\alpha_o}\llbracket\phi\rrbracket \subseteq \llbracket\phi\rrbracket^A$" is faulty, because $\llbracket\phi\rrbracket \subseteq \overline{\gamma}(\overline{\alpha_o}\llbracket\phi\rrbracket)$.

3 Logical completeness

In symbolic logic, one formal system, $\mathcal{A}$, is $\mathcal{L}$-sound for another formal system, $\mathcal{C}$, iff every property $\phi \in \mathcal{L}$ that is validated in $\mathcal{A}$ can be validated in $\mathcal{C}$. When the converse holds true as well, then $\mathcal{A}$ is $\mathcal{L}$-complete for $\mathcal{C}$. In like fashion, we might strengthen each of the implications in Items *2-4* in Proposition 5 into equivalences: For $\llbracket\cdot\rrbracket : \mathcal{L} \to \mathcal{P}(D)$ and $\llbracket\cdot\rrbracket^A : \mathcal{L} \to \mathcal{P}_\downarrow(A)$, we define these properties:

- *best preservation:* for all $\phi \in \mathcal{L}$ and $T \in \mathcal{P}_\downarrow(A)$, $T \subseteq \llbracket\phi\rrbracket^A$ iff $\overline{\gamma}(T) \subseteq \llbracket\phi\rrbracket$.
- *strong preservation:* for all $\phi \in \mathcal{L}$ and $S \in \mathcal{P}(D)$, $S \subseteq \llbracket\phi\rrbracket$ iff $\overline{\alpha_o}(S) \subseteq \llbracket\phi\rrbracket^A$.
- *lower preservation:* for all $\phi \in \mathcal{L}$ and $S \in \mathcal{P}(D)$, $\llbracket\phi\rrbracket \subseteq S$ iff $\llbracket\phi\rrbracket^A \subseteq \overline{\alpha_u}(S)$.

In particular, strong preservation asserts for all $c \in D$, $\{c\} \models \phi$ iff there exists some $a_0 \in A$[8] such that $c \in \gamma(a_0)$ and $a_0 \models^A \phi$ — every c that "makes ϕ hold" can be validated by $\models^A$ (and a_0). In contrast, best preservation states that $a \models^A \phi$ iff for all $c \in \gamma(a)$, $\{c\} \models \phi$ — every a that "makes ϕ hold" can be validated by $\models^A$. We soon see that lower-preservation is equivalent, surprisingly, to strong preservation.

The obvious question to ask is, "What is the relationship between the above logical preservation properties and functional completeness?" Working from the Galois connection, $\mathcal{P}(D)^{op}\langle\overline{\alpha_u},\overline{\gamma}\rangle\mathcal{P}_\downarrow(A)^{op}$, and the functions, $\llbracket\cdot\rrbracket : \mathcal{L} \to \mathcal{P}(D)$ and $\llbracket\cdot\rrbracket^A : \mathcal{L} \to \mathcal{P}_\downarrow(A)$, we calculate these definitions of functional completeness:[9]

- $\llbracket\cdot\rrbracket^A$ is *B($\overline{\alpha_u}$)-complete for* $\llbracket\cdot\rrbracket$ iff $\overline{\alpha_u}\llbracket\phi\rrbracket = \llbracket\phi\rrbracket^A$
- [25] $\llbracket\cdot\rrbracket^A$ is *F($\overline{\gamma}$)-complete for* $\llbracket\cdot\rrbracket$ iff $\llbracket\phi\rrbracket = \overline{\gamma}\llbracket\phi\rrbracket^A$

This strengthens into equalities the subset inclusions in Item *1*, Proposition 5. As before, we use the terms, "B-complete" and "F-complete," as abbreviations for B($\overline{\alpha_u}$)-complete and F($\overline{\gamma}$)-complete, respectively.

The relationships within this soup of definitions go as follows:

Theorem 6. *For $\mathcal{P}(D)\langle\alpha,\gamma\rangle A$, $\llbracket\cdot\rrbracket : \mathcal{L} \to \mathcal{P}(D)$, and $\llbracket\cdot\rrbracket^A : \mathcal{L} \to \mathcal{P}_\downarrow(A)$,*

- *B-complete iff best preservation*

[8] Indeed, the a_0 is $\overline{\alpha_o}\{c\}$.

[9] We use implicitly the identity Galois connection on arguments from $\mathcal{L}$.

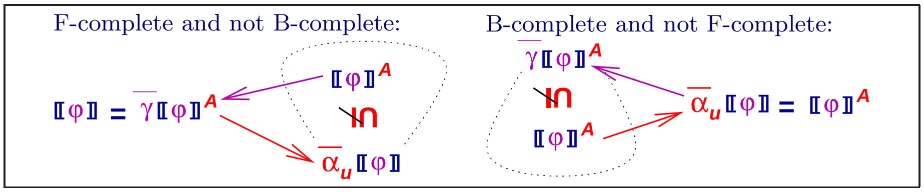

F-complete and not B-complete:
⟦φ⟧ = γ̄⟦φ⟧^A
⟦φ⟧^A
⊈
ᾱ_u⟦φ⟧
B-complete and not F-complete:
γ̄⟦φ⟧^A
⊈
⟦φ⟧^A
ᾱ_u⟦φ⟧ = ⟦φ⟧^A

Fig. 6. Independence of F- and B-completeness of interpretation functions

– *F-complete iff strong preservation iff lower preservation*

Proof. The results follow from application of the definitions and the properties of Galois connections. Here is the proof that F-completeness is equivalent to lower preservation; thanks to Proposition 5, we need only prove the following:

(i) F-completeness and $\llbracket\phi\rrbracket^A \subseteq \overline{\alpha_u}(S)$ imply $\llbracket\phi\rrbracket \subseteq S$: Assume $\llbracket\phi\rrbracket^A \subseteq \overline{\alpha_u}(S)$; then, $\overline{\gamma}\llbracket\phi\rrbracket^A \subseteq \overline{\gamma}(\overline{\alpha_u}(S)) \subseteq S$, by definition of Galois connection. By F-completeness, $\overline{\gamma}\llbracket\phi\rrbracket^A = \llbracket\phi\rrbracket \subseteq S$.

(ii) Lower preservation implies $\llbracket\phi\rrbracket \subseteq \overline{\gamma}\llbracket\phi\rrbracket^A$: By definition of Galois connection, $\llbracket\phi\rrbracket^A \subseteq \overline{\alpha_u}(\overline{\gamma}\llbracket\phi\rrbracket^A)$. By lower preservation (what was proved in *(i)*, where we set $S = \overline{\gamma}\llbracket\phi\rrbracket^A$), we have the result.

Here is a second example, which shows the equivalence of F-completeness and strong preservation:

(iii) F-completeness and $S \subseteq \llbracket\phi\rrbracket$ imply $\overline{\alpha_o}(S) \subseteq \llbracket\phi\rrbracket^A$: Assume $S \subseteq \llbracket\phi\rrbracket$; then $S \subseteq \overline{\gamma}\llbracket\phi\rrbracket^A$, by F-completeness. The definition of Galois connection gives us the result: $\overline{\alpha_o}(S) \subseteq \overline{\alpha_o}(\overline{\gamma}\llbracket\phi\rrbracket^A) \subseteq \llbracket\phi\rrbracket^A$.

(iv) Strong preservation implies $\llbracket\phi\rrbracket \subseteq \overline{\gamma}\llbracket\phi\rrbracket^A$: Using the definition of strong presevation (what was proved in (iii), where we set $S = \llbracket\phi\rrbracket$), we have that $\overline{\alpha_o}\llbracket\phi\rrbracket \subseteq \llbracket\phi\rrbracket^A$. By the definition of Galois connection, we get $\llbracket\phi\rrbracket \subseteq \overline{\gamma}(\overline{\alpha_o}\llbracket\phi\rrbracket)) \subseteq \overline{\gamma}\llbracket\phi\rrbracket^A$, which is the result.

Finally, here is the proof of equivalence between B-completeness and best preservation:

(v) B-completeness and $\overline{\gamma}(T) \subseteq \llbracket\phi\rrbracket$ imply $T \subseteq \llbracket\phi\rrbracket^A$: From the assumption and the definition of Galois connection, we get $T \subseteq \overline{\alpha_u}(\overline{\gamma}(T)) \subseteq \overline{\alpha_u}\llbracket\phi\rrbracket \subseteq \overline{\alpha_u}\llbracket\phi\rrbracket$. By B-completeness, $\overline{\alpha_u}\llbracket\phi\rrbracket = \llbracket\phi\rrbracket^A$, and we have the result.

(vi) Best preservation implies $\overline{\alpha_u}\llbracket\phi\rrbracket \subseteq \llbracket\phi\rrbracket^A$: By the Galois connection, $\overline{\gamma}(\overline{\alpha_u}\llbracket\phi\rrbracket) \subseteq \llbracket\phi\rrbracket^A$. By best preservation (set $T = \overline{\alpha_u}\llbracket\phi\rrbracket$), we get the result. □

B- and F-completeness are *independent*, as shown by Figure 6. The first diagram shows how F-completeness holds yet B-completeness fails when there are distinct assertions in $\mathcal{P}_\downarrow(A)$ that concretize to the same set. For example, say that $a \models^A \phi_1 \vee \phi_2$ *iff* $a \models^A \phi_1$ *or* $a \models^A \phi_2$ (cf. Figure 4). Consider $\llbracket \mathit{neg} \vee \mathit{zero} \vee \mathit{pos}\rrbracket^A$ and $\llbracket \mathit{any} \vee \mathit{neg} \vee \mathit{zero} \vee \mathit{pos}\rrbracket^A$, which denote different sets in $\mathcal{P}_\downarrow(\mathit{Sign})^{op}$ but both concretize to Int. This is F-complete but not B-complete.

The absence of B-completeness in an abstract logic is a famous trouble spot, e.g., we are asked to validate $\mathit{any} \models^A \mathit{neg} \vee \mathit{zero} \vee \mathit{pos}$ — the above definition fails to do so, and a *focus* or *materialization* operation [14, 26] must be employed to decompose any into a set of covering cases, such as $\{\mathit{neg}, \mathit{zero}, \mathit{pos}\}$ (because $\gamma(\mathit{any}) \subseteq \gamma(\mathit{neg}) \cup \gamma(\mathit{zero}) \cup \gamma(\mathit{pos})$), and a proof-by-cases analysis is undertaken.[10]

The second diagram shows that F-completeness can fail when there is some $[\![\phi]\!]$ that cannot be exactly expressed in $\mathcal{P}_{\downarrow}(A)$. For example, without altering Sign, add to $\mathcal{L}$ the new assertion, $\mathit{equals1}$, such that $[\![\mathit{equals1}]\!] = \{1\}$, and define $[\![\mathit{equals1}]\!]^A = \overline{\alpha_u}[\![\mathit{equals1}]\!] = \{\mathit{none}\}$. F-completeness fails. The absence of F-completeness produces spurious counterexamples, e.g., a static analysis of

```
x:= 1; if x=1 then safe() else error()
```

using Sign announces that `error()` is reachable. This false counterexample is eliminated by *counterexample guided abstraction refinement* [2, 3, 27]), which adds new values to Sign (in this case, one), moving towards F-completeness [16].

In the previous section, we noted that the set inclusion, $\overline{\alpha_o}[\![\phi]\!] \subseteq [\![\phi]\!]^A$, does not guarantee soundness. Nonetheless, starting from Galois connection, $\mathcal{P}(D)\langle\overline{\alpha_o}, \overline{\gamma}\rangle\mathcal{P}_{\downarrow}(A)$, we define yet one more variant of functional completeness:

$$[\![\cdot]\!]^A \text{ is } B(\overline{\alpha_o})\text{-}\mathit{complete\ for}\ [\![\cdot]\!] \text{ iff } \overline{\alpha_o}[\![\phi]\!] = [\![\phi]\!]^A.$$

For clarity, we use *O-complete* as a synonym for $B(\overline{\alpha_o})$*-complete*. O-completeness is again independent from F-completeness, but with the concept of a *covering*, we can make many connections:

- For $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(D)$ and $\overline{\gamma} : Q \to \mathcal{P}(D)$, $\overline{\gamma}$ *covers* $[\![\cdot]\!]$ iff for all $\phi \in \mathcal{L}$, $[\![\phi]\!] \in \overline{\gamma}[Q]$.
- For $[\![\cdot]\!]^A : \mathcal{L} \to \mathcal{P}_{\downarrow}(A)$ and $\overline{\alpha} : P \to \mathcal{P}_{\downarrow}(A)$, $\overline{\alpha}$ *covers* $[\![\cdot]\!]^A$ iff for all $\phi \in \mathcal{L}$, $[\![\phi]\!]^A \in \overline{\alpha}[P]$.

Proposition 7. *Let $\overline{\alpha}$, $\overline{\gamma}$ be the adjoints of a Galois connection. Then,*

- $\overline{\gamma}$ *covers* $[\![\cdot]\!]$ *iff* $\overline{\gamma}(\overline{\alpha}[\![\phi]\!]) = [\![\phi]\!]$ *for all* $\phi \in \mathcal{L}$
- $\overline{\alpha}$ *covers* $[\![\cdot]\!]^A$ *iff* $\overline{\alpha}(\overline{\gamma}[\![\phi]\!]^A) = [\![\phi]\!]^A$ *for all* $\phi \in \mathcal{L}$.

Proof. The results hold because each equivalence class in $\mathcal{P}(D)$ (resp., $\mathcal{P}_{\downarrow}(A)$) holds exactly one value that lies in the image of $\overline{\gamma}[\mathcal{P}_{\downarrow}(A)]$ (resp., $\overline{\alpha}[\mathcal{P}(D)]$). □

Propositions 1, 2, and 7 characterize completeness:

Theorem 8. *Let $\overline{\alpha}$, $\overline{\gamma}$ be the adjoints of a Galois connection:*

- $[\![\cdot]\!]^A$ *is* $F(\overline{\gamma})$*-complete for* $[\![\cdot]\!]$ *iff* $\overline{\gamma}$ *covers* $[\![\cdot]\!]$ *and* $[\![\phi]\!]^A \sim_{\overline{\gamma}} \overline{\alpha}[\![\phi]\!]$*, for all* $\phi \in \mathcal{L}$.

[10] In theory, the redundant elements in A can be removed by applying the backwards-complete-core construction, closing the sets in $\mathcal{P}_{\downarrow}(A)$ under join.

- $[\![\cdot]\!]^A$ *is B($\overline{\alpha}$)-complete for* $[\![\cdot]\!]$ *iff* $\overline{\alpha}$ *covers* $[\![\cdot]\!]^A$ *and* $[\![\phi]\!]^A \sim_{\overline{\gamma}} \overline{\alpha}[\![\phi]\!]$*, for all* $\phi \in \mathcal{L}$*.*

Proof. The first result is a direct translation of Proposition 1, where $[\![\cdot]\!]^\sharp_{best} = \overline{\alpha} \circ [\![\cdot]\!] \circ id_{\mathcal{L}}$, that is $[\![\phi]\!]^\sharp_{best} = \overline{\alpha}[\![\phi]\!]$, for $\phi \in \mathcal{L}$.

The second result follows less directly. In Proposition 2, Clause *(i)* becomes $\phi = \phi'$ implies $[\![\phi]\!] = [\![\phi']\!]$, so only Clause *(ii)* remains: show $\overline{\alpha}[\![\phi]\!] = [\![\phi]\!]^A$ iff $\overline{\alpha}$ covers $[\![\cdot]\!]^A$ and $[\![\phi]\!]^A \sim_{\overline{\gamma}} \overline{\alpha}[\![\phi]\!]$. The if-part is immediate; for the only-if-part, $\overline{\alpha}$ covers $[\![\cdot]\!]^A$, because $\overline{\alpha}[\![\phi]\!] = [\![\phi]\!]^A$ implies that $\overline{\alpha}(\overline{\gamma}[\![\phi]\!]^A) = \overline{\alpha}[\![\phi]\!] = [\![\phi]\!]^A$ (cf. the proof of Prop. 7). This is because all three values must live in the same equivalence class, and there is exactly one $\overline{\alpha}$-image point in the class. Next, $\overline{\gamma}[\![\phi]\!]^A = \overline{\gamma}(\overline{\alpha}[\![\phi]\!])$ by applying $\overline{\gamma}$. □

Both forms of completeness require the same, best equivalence-class precision and vary *only on the covering properties of* $\overline{\alpha}$ *and* $\overline{\gamma}$*.*

Corollary 9.

- *If* $[\![\cdot]\!]^A$ *is F-complete for* $[\![\cdot]\!]$ *and* $\overline{\alpha_u}$ *covers* $[\![\cdot]\!]^A$*, then* $[\![\cdot]\!]^A$ *is B-complete.*
- *If* $[\![\cdot]\!]^A$ *is B-complete for* $[\![\cdot]\!]$ *and* $\overline{\gamma}$ *covers* $[\![\cdot]\!]$*, then* $[\![\cdot]\!]^A$ *is F-complete.*
- *If* $[\![\cdot]\!]^A$ *is F-complete for* $[\![\cdot]\!]$ *and* $\overline{\alpha_o}$ *covers* $[\![\cdot]\!]^A$*, then* $[\![\cdot]\!]^A$ *is O-complete.*
- *If* $[\![\cdot]\!]^A$ *is O-complete for* $[\![\cdot]\!]$ *and* $\overline{\gamma}$ *covers* $[\![\cdot]\!]$*, then* $[\![\cdot]\!]^A$ *is sound and F-complete.*

The Corollary explains why Ranzato and Tapparo, who work exclusively with onto $\overline{\alpha}$ functions, gravitate to proving F-completeness results [23–25].

4 Inductively defined abstract logics

Given $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}(D)$, we can define $[\![\cdot]\!]^A : \mathcal{L} \to \mathcal{P}_\downarrow(A)$ to be $[\![\phi]\!]^A = \overline{\alpha_u}[\![\phi]\!]$, and consequently, $a \models^A \phi$ iff $\gamma(a) \subseteq [\![\phi]\!]$, but this definition is not inductively defined and is unlikely to be finitely computable. Assuming that $\mathcal{L}$ is defined inductively, we denote its inductive abstract interpretation as $[\![\cdot]\!]^A_{ind} : \mathcal{L} \to \mathcal{P}_\downarrow(A)$ and define it as

$$[\![op_i(\phi_j)_{0<j\leq ar(i)}]\!]^A_{ind} = g_i^\sharp([\![\phi_i]\!]^A_{ind})_{0<i\leq ar(i)}$$
$$\text{where } g_i^\sharp : \mathcal{P}_\downarrow(A) \to \mathcal{P}_\downarrow(A) \text{ is sound for } g_i : \mathcal{P}(D) \to \mathcal{P}(D).$$

For example, based on Figure 4, we might define

$$[\![a]\!]^A_{ind} = \overline{\alpha_u}(\gamma(a)) \qquad [\![\phi_1 \vee \phi_2]\!]^A_{ind} = [\![\phi_1]\!]^A_{ind} \cup_{\mathcal{P}_\downarrow(A)} [\![\phi_2]\!]^A_{ind}$$
$$[\![\phi_1 \wedge \phi_2]\!]^A_{ind} = [\![\phi_1]\!]^A_{ind} \cap_{\mathcal{P}_\downarrow(A)} [\![\phi_2]\!]^A_{ind} \qquad [\![[f]\phi]\!]^A_{ind} = \widetilde{pre}_{f^\sharp}[\![\phi]\!]^A_{ind}$$

It is well known that such a $[\![\cdot]\!]^A_{ind}$ is sound for $[\![\cdot]\!]$ and also that, for all g_i and $g_i^\sharp$, if each $g_i^\sharp$ is B-complete (respectively, F-complete) for g_i, then $[\![\cdot]\!]^A_{ind}$ is B-complete (F-complete) for $[\![\cdot]\!]$. Because the fixed-point operators are well behaved, we can easily add recursively defined operators to the logic [11, 25].

For a logic with operators, op_i, and interpretations, g_i, we define each $g^\sharp_{i\ best} = \overline{\alpha_u} \circ g_i \circ \overline{\gamma}^{ar(i)} : \mathcal{P}_\downarrow(A)^{ar(i)} \rightarrow \mathcal{P}_\downarrow(A)$ so that

$$[\![op_i(\phi_j)_{0<j\leq ar(i)}]\!]^A_{best} = g^\sharp_{i\ best}([\![\phi_j]\!]^A_{best})_{0<j\leq ar(i)}$$

Call this inductively defined interpretation, $[\![\cdot]\!]^A_{best}$.

Corollary 10. *$[\![\cdot]\!]^A_{best}$ is F-complete for $[\![\cdot]\!]$ iff $\overline{\gamma}$ covers $[\![\cdot]\!]$.*

Corollary 11. *If $\overline{\gamma}$ covers $[\![\cdot]\!]$, then $[\![\cdot]\!]^A_{best}$ is B-complete for $[\![\cdot]\!]$.*

So, there is one crucial abstract interpretation where F-completeness implies B-completeness. No dual result is known where B-completeness implies F-completeness. Indeed, it is always the case that $\overline{\alpha_u}$ covers $[\![\cdot]\!]^A_{best}$, so there is no relation between the B-completeness of $[\![\cdot]\!]^A_{best}$ and $\overline{\alpha_u}$-covering.

5 Applications

5.1 $\mathcal{L} = A$

A standard static analysis computes on A-values and also uses them as the assertions of a correctness or transformation logic.

Given $C\langle\alpha,\gamma\rangle A$, use the Galois connection's internal logic: $\mathcal{L} = A$, and $c \models a$ iff $c \subseteq \gamma(a)$. Although the abstract judgement, $a' \models^A a$ iff $\gamma(a') \subseteq \gamma(a)$, would be best, one typically settles for its computable variant, $a' \models^A a$ iff $a' \sqsubseteq a$, that is, $[\![a]\!]^A = \downarrow a$. This makes $[\![\cdot]\!]^A$ F($\overline{\gamma}$)-complete (and sound!) for $[\![\cdot]\!]$. But $[\![\cdot]\!]^A$ might not be O-complete nor B-complete:

Proposition 12. *For all $a \in A$, $\overline{\alpha_o}(\gamma(a)) \subseteq \downarrow a \subseteq \overline{\alpha_u}(\gamma(a))$. But when α is onto, the second inclusion is an equality.*

Proof. The two subset inclusions hold because $\gamma(a) = \overline{\gamma}(\downarrow a)$. For the equality, we note that $\overline{\alpha_u}(\gamma(a)) = \{a' \mid \gamma(a') \subseteq \gamma(a)\}$, and we must prove that $\gamma(a') \subseteq \gamma(a)$ implies $a' \sqsubseteq a$. But $\alpha(\gamma(a')) \sqsubseteq \alpha(\gamma(a))$, and since α is onto, $\alpha(\gamma(a')) = a'$ (similarly for a). □

Say that $f(c_0) \models a_p$ holds, and we try to show this by validating $f^\sharp_{best}(a_0)) \models^A a_p$, where $a_0 = \alpha(c_0)$, but we fail. Since $f^\sharp_{best}(a_0) \sqsubseteq a_p$ iff $f(\gamma(a_0)) \subseteq \gamma(a_p)$, we must adjust either a_p or a_0; see Figure 3(a).

Perhaps we "weaken" a_p by making $f(\gamma(a_0))$ itself into a new canonical element, i.e., A gets the new element, a'_p, such that $\gamma(a'_p) = f(\gamma(a_0))$. This makes $f^\sharp_{best}(a_0) \models^A a'_p$ hold *as well as* $f^\sharp_{best}(a_0) \models^A a_p \sqcup a'_p$. This is an F-refinement step; see Figure 3(b).

Or we "strengthen" a_0 to a new element, a_1: Let c' be a maximal element from the set, $f^{-1}[\gamma(a_p)]_\alpha \cap [\gamma(a_0)]_\alpha$ and define $\gamma(a_1) = c'$. Now, $\alpha(c_0) = a_1$, and $f^\sharp_{best}(a_1) \models^A a_p$ holds. This is a B-refinement step; see Figure 3(c).

5.2 Partition domains

An abstract domain used in model checking is the *partition domain* [3, 23, 24]: Let D and A be discretely ordered sets, and let $\delta : D \to A$ be an onto function; δ defines the equivalence relation, $c \sim_\delta c'$ iff $\delta(c) = \delta(c')$, and it partitions D, where A are the partition names. Define $\gamma : A \to \mathcal{P}(D)$ as $\gamma(a) = \delta^{-1}(a)$. *There is no Galois connection.* The logic looks like Figure 4 but includes negation:

$$[\![\neg\phi]\!] = \sim [\![\phi]\!]$$

($\sim$ is set complement.) As usual, $\{c\} \models \phi$ iff $c \in [\![\phi]\!]$.

From γ, we define $\overline{\gamma}$, $\overline{\alpha_o}$, and $\overline{\alpha_u}$. Since $\mathcal{P}(A)$ is a Boolean lattice and $\overline{\gamma}$ is 1-1, we have that $\overline{\gamma}$ preserves $\cup$, $\cap$, and $\sim$. In addition, $[\![\cdot]\!]^A$, defined as

$$\begin{array}{ll} [\![a]\!]^A = \overline{\alpha_u}(\gamma(a)) & \qquad [\![\phi_1 \wedge \phi_2]\!]^A = [\![\phi_1]\!]^A \cap [\![\phi_2]\!]^A \\ [\![\neg\phi]\!]^A = \sim [\![\phi]\!]^A & \qquad [\![\phi_1 \vee \phi_2]\!]^A = [\![\phi_1]\!]^A \cup [\![\phi_2]\!]^A \end{array}$$

is F($\overline{\gamma}$)-complete and equals $[\![\cdot]\!]^A_{best}$. Since both $\overline{\alpha_u}$ and $\overline{\alpha_o}$ cover $[\![\cdot]\!]^A$, the logic is also B- and O-complete.

The usual application of a partition domain is to model checking, and the usual model-checking logic includes the modality, $[f]\phi$, for $f : D \to \mathcal{P}(D)$ (cf. Figure 4), which is abstracted by a sound $f^\sharp : A \to \mathcal{P}(A)$ as follows:

$$[\![[f]\phi]\!]^A = \widetilde{pre}_{f^\sharp_{best}} [\![\phi]\!]^A, \quad \text{where } \widetilde{pre}_{f^\sharp}(T) = \{a' \mid f^\sharp(a') \subseteq T\}.$$

We know that $\widetilde{pre}_{f^\sharp_{best}} = (\widetilde{pre}_f)^\sharp_{best} = \overline{\alpha_u} \circ \widetilde{pre}_f \circ \overline{\gamma}$ [29]. The definition is sound but might not be complete.

The following holds for *all* abstract domains (not just partition domains):

Theorem 13. *For $\widetilde{pre}_f : \mathcal{P}(D) \to \mathcal{P}(D)$, $f : D \to \mathcal{P}(D)$, and $f^* : \mathcal{P}(D) \to \mathcal{P}(D)$, defined as $f^*(S) = \cup_{c \in S} f(c)$,*

1. *$\widetilde{pre}_f$ is F($\overline{\gamma}$)-complete iff f^* is B($\overline{\alpha_o}$)-complete.*
2. *$\widetilde{pre}_f$ is B($\overline{\alpha_u}$)-complete iff f^* is F($\overline{\gamma}$)-complete.*

Proof. We first prove *2.* For the if-part, assume f^* is F-complete; we must show $\overline{\alpha_u}(\widetilde{pre}_f(S)) \subseteq (\overline{\alpha_u} \circ \widetilde{pre}_f \circ \overline{\gamma})(\overline{\alpha_u}(S))$. When we expand the definitions in the subset inclusion, we learn that we must assume $f^*[\gamma(a)] \subseteq S$ and prove $f^*(\gamma(a)) \subseteq \overline{\gamma}(\overline{\alpha_u}(S))$. The assumption expands to $\overline{\gamma}(\overline{\alpha_u}(f^*(\gamma(a))) \subseteq \overline{\gamma}(\overline{\alpha_u}(S))$. Now, its left-hand side equals $\overline{\gamma}(\overline{\alpha_u}(f^*(\overline{\gamma}(\downarrow a))))$. Since f^* is F-complete, this equals $f^*(\gamma(a))$ and gives the result.

For the only-if-part, we must show for all $S \in \overline{\gamma}[\mathcal{P}_\downarrow(A)]$ that $f^*(S) \in \overline{\gamma}[\mathcal{P}_\downarrow(A)]$, that is, $f^*(\overline{\gamma}(\overline{\alpha_u}(S))) \subseteq (\overline{\gamma} \circ \overline{\alpha_u} \circ f^*)(\overline{\gamma}(\overline{\alpha_u}(S)))$. Now, $f^*(\overline{\gamma}(\overline{\alpha_u}(S))) = f^*(\cup_{a \in \overline{\alpha_u}(S)})$. By the B-completeness of $\widetilde{pre}_f$, which can be stated as, for all S, $f^*(\gamma(a)) \subseteq S$ iff $f^*(\gamma(a)) \subseteq \gamma(\overline{\alpha_u}(S))$, we can instantiate $S = f^*(\overline{\gamma}(\overline{\alpha_u}(S)))$, and we have that $f^*(\gamma(a)) \subseteq (\overline{\gamma} \circ \overline{\alpha_u})(f^*(\overline{\gamma}(\overline{\alpha_u}(S))))$; the left-hand side equals $\cup_{a \in \overline{\alpha_u}(S)} f^*(\gamma(a))$. Since f^* preserves unions, the result follows.

We next prove *1*. For the if-part, we must show that $\widetilde{pre}_f(\overline{\gamma}(T)) = (\overline{\gamma} \circ \overline{\alpha_u} \circ \widetilde{pre}_f \circ \overline{\gamma})(T)$. When we expand the definitions in the equation, we discover that we must prove $\cup\{S \mid f^*(S) \subseteq \overline{\gamma}(T)\} \subseteq \cup\{\gamma(a) \mid f^*(\gamma(a)) \subseteq \overline{\gamma}(T)\}$. (Soundness gives us the $\supseteq$ inclusion.)

So, for arbitrary S_0, assume that $f^*(S_0) \subseteq \overline{\gamma}(T)$. Since f^* is B-complete, we have that $f^*(S_0) \sim_{\overline{\alpha_o}} f^*(\overline{\gamma}(\overline{\alpha_o}(S_0)))$. We also have $S_0 \subseteq \overline{\gamma}(\overline{\alpha_o}(S_0))$. Since $f^*(S_0) \subseteq \overline{\gamma}(T)$, and the latter is a maximal point in its equivalence class, we have that $f^*(\overline{\gamma}(\overline{\alpha_o}(S_0))) \subseteq \overline{\gamma}(T)$ as well, implying that $\overline{\gamma}(\overline{\alpha_o}(S_0))$ lies in the goal set, $\{\gamma(a) \mid f^*(\gamma(a)) \subseteq \overline{\gamma}(T)\}$.

For the only-if-part, we must show $\overline{\alpha_o}(f^*(\overline{\gamma}(\overline{\alpha_o}(S)))) \subseteq \overline{\alpha_o}(f^*(S))$ for all $S \in \mathcal{P}(D)$. First consider the set, $G_S = \widetilde{pre}_f(\overline{\gamma}(\overline{\alpha_o}(f^*(S))))$; we have that $S \subseteq G_S$, because $f^*(S) \subseteq \overline{\gamma}(\overline{\alpha_o}(f^*(S)))$ and $\widetilde{pre}_f(f^*(S)) \supseteq S$. Since $\widetilde{pre}_f$ is F-complete, we have $G_S \in \overline{\gamma}[\mathcal{P}_\downarrow(A)]$, and we also have $\overline{\gamma}(\overline{\alpha_o}(S)) \subseteq G_S$.

This implies $f^*(\overline{\gamma}(\overline{\alpha_o}(S))) \subseteq \overline{\gamma}(\overline{\alpha_o}(f^*(S)))$, by the definition of $\widetilde{pre}_f$. We apply $\overline{\alpha_o}$ and obtain $(\overline{\alpha_o} \circ f^* \circ \overline{\gamma} \circ \overline{\alpha_o})(S) \subseteq (\overline{\alpha_o} \circ \overline{\gamma} \circ \overline{\alpha_o} \circ f^*)(S) = \overline{\alpha_o}(f^*(S))$, which is the result. □

Giacobazzi and Quintarelli [16] (and Mastroeni [20]) show how to apply the F-complete shell construction to additive (continuous) f to achieve Item *1* above.

Recall that $pre_f(S) = \sim\widetilde{pre}_f(\sim S)$ [19]; When pre_f is not F-complete, Ranzato and Tapparo apply the F-complete-shell construction to pre_f [23]. The resulting abstract domain is still partitioned and its $\overline{\gamma}$ preserves $\sim$, so the equivalence, $\sim pre_f(\sim S) = \widetilde{pre}_f(S)$, yields F-completeness for $\widetilde{pre}_f$, too. $\overline{\gamma}$ is 1-1 as well (it preserves $\sim$), meaning $\overline{\alpha_o}$ is onto, giving B-completeness.

5.3 Predicate abstraction

When an abstract domain is generated from a set, A, of assertions for variables within a program (e.g., `x>y`, `¬(y=0)`, ...), it is called a *predicate abstraction* [1, 2, 18, 27]. The resulting static analysis annotates program points with sets of predicates that hold true at the program points.

We begin with the concrete state set, D, predicate set, A, and judgement relation, $\models \subseteq D \times A$. Think of A as a "subbasis" for domain generation. We generate the Galois connection, $\mathcal{P}(D)\langle\alpha, \gamma\rangle\mathcal{P}(A)^{op}$, where $\alpha(S) = \{a \mid S \models a\}$ (it maps S to all the predicates that hold true for S) and $\gamma(T) = \cap_{a \in T}\{c \mid c \models a\}$. (To understand γ, read $T \in \mathcal{P}(A)^{op}$ as $\bigwedge_{a \in T} a$.) The Galois connection is overapproximating, so $f^\sharp : \mathcal{P}(A)^{op} \rightarrow \mathcal{P}(A)^{op}$ computes sound postconditions for $f^* : \mathcal{P}(D) \rightarrow \mathcal{P}(D)$. The logical assertions are conjunctions,

$$\mathcal{L} \ni \phi \ ::= \ \bigwedge T, \ \text{where } T \in \mathcal{P}(A)$$

interpreted by $\mathcal{P}(A)$'s internal logic: for $c \in D$, $\{c\} \models \bigwedge T$ iff $c \in \gamma(T)$.

The definition of the abstract judgement is crucial: if it is merely $T \models^A \bigwedge T'$ iff $T' \subseteq T$, then we have F($\overline{\gamma}$)-completeness but likely lose B($\overline{\alpha_u}$)-completeness, because it is possible that $a_1 \neq a_2$ and $\gamma\{a_1\} \subseteq \gamma\{a_2\}$, e.g., $\gamma\{\texttt{x>2}\} \subseteq \gamma\{\texttt{x>0}\}$ but `x>2` $\not\models^A$ `x>0`. For this reason, implementations typically employ theorem provers that enforce $T \models^A \phi$ *iff* $T \Rightarrow \phi$ (that is, the prover uses T to deduce ϕ).

A second situation where completeness can fail is the calculation of imprecise postconditions. Suppose that we fail to prove $f^\sharp(a_0) \models \phi$. As we know from Section 5.1, we can either weaken ϕ or strengthen a_0. The latter is usually chosen, and we know that the B-complete refinement of f^* corresponds to the F-complete refinement of $\widetilde{pre}_f$ (Theorem 13 and [16]). This is the standard predicate-abstraction refinement strategy [2, 27].

Disjunctive predicate abstraction: We can add disjunction to the predicate-abstraction domain by constructing the disjunctive completion of $\mathcal{P}(A)^{op}$. The elements of $\mathcal{P}_\downarrow(\mathcal{P}(A)^{op})$ are downclosed sets of sets of A-elements. Read such a $\overline{T} \in \mathcal{P}_\downarrow(\mathcal{P}(A)^{op})$ as the disjunctive normal form (DNF), $\bigvee_{T \in \overline{T}}(\bigwedge_{a \in T} a)$.

This coincides with the definition of $\overline{\gamma} : \mathcal{P}_\downarrow(\mathcal{P}(A)^{op}) \to \mathcal{P}(D)$, which is $\overline{\gamma}(\overline{T}) = \bigcup_{T \in \overline{T}} \gamma(T) = \bigcup_{T \in \overline{T}}(\bigcap_{a \in T} \gamma(a))$. Since the sets are downclosed (here, closed under superset), both union (disjunction) and intersection (conjunction) operations *automatically normalize to DNF*.[11]

Disjunctive completion gives us the Galois connection, $\mathcal{P}(D)\langle\overline{\alpha_o}, \overline{\gamma}\rangle\mathcal{P}_\downarrow(\mathcal{P}(A)^{op})$, completing the "basis" elements from $\mathcal{P}(A)^{op}$ to DNF elements [2]. The Galois connection supports this logic and its two interpretations:

$$\phi \ ::= \ a \mid \bigwedge_{i>0} \phi_i \mid \bigvee_{i>0} \phi_i$$

$$\begin{array}{ll}
[\![a]\!] = \gamma\{a\} & [\![a]\!]^A = \{T \in \mathcal{P}(A)^{op} \mid T \Rightarrow a\} \\
[\![\bigwedge_{i\geq 0} \phi_i]\!] = \bigcap_{i\geq 0} [\![\phi_i]\!] & [\![\bigwedge_{i>0} \phi_i]\!]^A = \bigcap_{i>0} [\![\phi_i]\!]^A \\
[\![\bigvee_{i\geq 0} \phi_i]\!] = \bigcup_{i\geq 0} [\![\phi_i]\!] & [\![\bigvee_{i>0} \phi_i]\!]^A = \bigcup_{i>0} [\![\phi_i]\!]^A
\end{array}$$

We have F($\overline{\gamma}$)-completeness, but B($\overline{\alpha_u}$)-completeness typically fails for disjunction, for the reasons given above.

6 Related Work

As noted in the Introduction, Galois-connection-based functional completeness was defined by Cousot [6] and Cousot and Cousot [8]. Mycroft [22] was perhaps the first to use B-completeness to define logical completeness; at the same time, Clarke, Grumberg, and Long [4] defined "exactness," stated in terms of homomorphisms, $h : D \to A$: $h(c) \models^A \phi$ iff $c \models \phi$, which is strong preservation.

Abstractions of state-transition systems led both Cleaveland, Iyer, and Yankevich [5] and Dams, Gerth, and Grumberg [13] to define an "optimal" abstract transition system as one that proves the most sound logical properties of a concrete system. Their definitions are not Galois-connection based but use the definition of strong preservation and yield strong preservation when Galois-connections are present.

Cousot and Cousot [10] formalized B-functional completeness and showed that it is preserved in inductively defined interpretations; they applied the results

[11] An implementation of DNF will likely employ the normalization law, $S \wedge (\bigvee_i T_i) \Leftrightarrow \bigvee_i (S \wedge T_i)$, instead of using downclosed sets of sets.

to proving logical B-completeness of a family of temporal logics and showing that B-completeness is preserved by fixed-point operators [11].

Giacobazzi, Ranzato, and Scozzari [17] defined an iterative method for abstract-domain completion so that transfer functions are B-complete. Giacobazzi and Quintarelli [16] introduced F-completeness, defined its completion method, and used it to formalize counter-example-guided-abstraction refinement [3].

A thorough study of logical F-completeness (strong preservation) has been undertaken by Ranzato and Tapparo: for the class of partition domains, they showed that the minimal refinement of a partition domain to possess all sound properties of its corresponding concrete domain is iterative F-completion [23]. They also showed that the Paige-Tarjan algorithm for constructing a minimal bisimular abstract-transition system is an instance of F-completion [24]. Finally, they formalized strong preservation as logical F-completeness and showed that F-completeness is preserved by fixed-point operators [25]. The present paper was inspired by their work.

Finally, in his thesis [12], Dams proposed yet one more variant of logical completeness — *Dams's strong preservation* is defined as follows:

$$\text{for all } c \in D \text{ and } a \in A,\ c \in \gamma(a) \text{ iff (for all } \phi,\ a \models^A \phi \text{ iff } c \models \phi).$$

For *sets* A and D, onto $\delta : D \to A$, and $\gamma(a) = \delta^{-1}$, Dams's strong preservation implies *both* strong and best preservation.

Acknowledgements: I am grateful for discussions with Dennis Dams, Roberto Giacobazzi, Michael Huth, Isabella Mastroeni, Kedar Namjoshi, Francesco Ranzato, and Francesco Tapparo. Anindya Banerjee and the referees gave helpful suggestions for improving the paper.

References

1. T. Ball, A. Podelski, and S.K. Rajamani. Boolean and cartesian abstractions for model checking C programs. In *TACAS'01*, pages 268–283. LNCS 2031, 2001.
2. T. Ball, A. Podelski, and S.K. Rajamani. Relative completeness of abstraction refinement for software model checking. In *TACAS'02*, pages 158–172. Springer LNCS 2280, 2002.
3. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement. In *CAV'00*, pages 154–169. Springer LNCS 1855, 2000.
4. E.M. Clarke, O. Grumberg, and D.E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, 1994.
5. R. Cleaveland, P. Iyer, and D. Yankelevich. Optimality in abstractions of model checking. In *Proc. SAS'95*. Springer LNCS 983, 1995.
6. P. Cousot. *Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique de programmes.* PhD thesis, University of Grenoble, 1978.
7. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs. In *Proc. 4th ACM Symp. POPL*, pages 238–252, 1977.

8. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM Symp. POPL*, pages 269–282, 1979.
9. P. Cousot and R. Cousot. Higher-order abstract interpretation. In *Proceedings IEEE Int. Conf. Computer Lang.*, 1994.
10. P. Cousot and R. Cousot. Compositional and inductive semantic definitions in fixpoint, equational, constraint, closure-condition, rule-based and game theoretic form. In *Proc. CAV'95*, pages 293–308. Springer LNCS 939, 1995.
11. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. 27th ACM Symp. on Principles of Programming Languages*, pages 12–25. ACM Press, 2000.
12. D. Dams. *Abstract interpretation and partition refinement for model checking.* PhD thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.
13. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Prog. Lang. Systems*, 19:253–291, 1997.
14. D. Dams and K. Namjoshi. The existence of finite abstractions for branching time model checking. In *Proc. IEEE Symp. LICS'04*, pages 335–344, 2004.
15. B.A. Davey and H.A Priestley. *Introduction to Lattices and Order, 2d ed.* Cambridge Univ. Press, 2002.
16. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples, and refinements in abstract model checking. In *SAS'01*, pages 356–373. LNCS 2126, 2001.
17. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47:361–416, 2000.
18. S. Graf and H. Saidi. Verifying invariants using theorem proving. In *Proc. CAV'96*, Springer LNCS 1102, 1996.
19. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for verification of concurrent systems. *Formal Methods in System Design*, 6:1–36, 1995.
20. I. Mastroeni. *Abstract non-interference: an abstract-intepretation-based approach to secure information flow.* PhD thesis, University of Verona, IT, 2006.
21. A. Melton, G. Strecker, and D. Schmidt. Galois connections and computer science applications. In *Category Theory and Computer Programming*, pages 299–312. Springer LNCS 240, 1985.
22. A. Mycroft. Completeness and predicate-based abstract interpretation. In *Proc. ACM Symp. Partial Evaluation (PEPM'93)*, pages 179–185, 1993.
23. F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. ESOP*, LNCS 2986, pages 18–32. Springer, 2004.
24. F. Ranzato and F. Tapparo. An abstract interpretation-based refinement algorithm for strong preservation. In *TACAS'05*, LNCS 3440, pages 140–156. Springer, 2005.
25. F. Ranzato and F. Tapparo. Strong preservation of temporal fixpoint-based operators by abstract interpretation. In *Proc. Conf. VMCAI'06*, LNCS 3855, pages 332–347. Springer Verlag, 2006.
26. M. Sagiv, T. Reps, and R. Wilhelm. Parametric shape analysis via 3-valued logic. *ACM TOPLAS*, 24:217–298, 2002.
27. H. Saidi. Model checking guided abstraction and analysis. In *Proc. SAS'00*, pages 377–396. Springer LNCS 1824, 2000.
28. D.A. Schmidt. Comparing completeness properties of static analyses and their logics. Technical Report 06-03, Kansas State University, 2006.
29. D.A. Schmidt. Underapproximating predicate transformers. In *Proc. SAS'06*, LNCS. Springer, 2006.