Abstract Interpretation from a Topological Perspective

David A. Schmidt*

Kansas State University, Manhattan, Kansas, USA

Abstract. We develop abstract interpretation from topological principles by relaxing the definitions of open set and continuity; key results still hold. We study families of closed and open sets and show they generate post- and pre-condition analyses, respectively. Giacobazzi's forwards- and backwards-complete functions are characterized by the topologically closed and continuous maps, respectively. Finally, we show that Smyth's upper and lower topologies for powersets induce the overapproximating and underapproximating transition functions used for abstract-model checking.

1 Introduction

Topology is a major force in mathematics — it is the study of properties (*open sets*) and functions that behave well (are *continuous*) regarding the properties. For example, the real line, $\mathbb{R}$, has as open sets the open intervals, (a, b). A number $r \in \mathbb{R}$ has property (a, b) when $r \in (a, b)$, e.g., $\pi \in (3, 4)$. A function $f : \mathbb{R} \to \mathbb{R}$ is topologically continuous when it maps arguments "close together" (sharing many open sets) to answers "close together" (sharing equally many open sets), e.g., $area(r) = \pi r^2$ is continuous with respect to intervals. The continuous functions on the real line are exactly the topologically continuous functions.[1]

One application of topology to computing is Scott-domain theory [19]: To solve the domain equation, $D = D \to D$, Scott needed to limit the cardinality of functions on D. Continuity was the appropriate criterion: For complete lattice L, Scott defined L's open sets to be those subsets of L that are *(i)* upwards closed and *(ii)* closed under tails of chains.[2] Scott proved that the functions that are topologically continuous for his *Scott topology* of L are exactly the chain-continuous functions on L. By restricting $D \to D$ to the continuous functions, Scott limited its cardinality so that the recursive domain equation had a solution.

Smyth [24] suggested that a domain's Scott topology defines all the *computable properties* of the domain, and he established correspondences between

* schmidt@cis.ksu.edu. Supported by NSF ITR-0326577.

[1] In contrast, $g(r) = \mathit{if}\ r \neq 9\ \mathit{then}\ r^2\ \mathit{else}\ 0$ is discontinuous — the "closeness" of answers is destroyed at argument 9.

[2] That is, for every chain, $C = \{c_0, c_1, \cdots c_i, \cdots\} \subseteq L$, when $\sqcup C \in U$, for open set $U \subseteq L$, then there exists some $c_k \in C$ such that $c_k \in U$ also. This means C's tail, from c_k onwards, is in U.

"upper," "lower," and "convex" topologies to the three main variants of powerdomains [15]. Smyth's observations generated intensive research on the Stone duality within domain theory, leading to "domain theory in logical form" [1].

Given that topology is the study of computing on properties, one would believe that it would be central to the theory of abstract interpretation [7], which studies exactly this topic. There are indeed some precedents.

In [8], Cousot and Cousot employed topology to establish soundness of convergence: They proposed a T0-topology, the $\sqcup$-*topology*, for complete lattices, where the basic open sets are up-closed and closed under finite meets. As with the Scott topology, a function is chain continuous iff it is $\sqcup$-topologically continuous. (The two topologies coincide for algebraic lattices.) The $\sqcup$-topology explains how computation on an abstract interpretation preserves properties: When lattice L's abstract interpretation is defined by an upper closure operation, $\rho : L \to L$, the $\sqcup$-topology on $\rho[L]$ is exactly the relative topology on L: every open $U' \subseteq \rho[L]$ equals $U \cap \rho[L]$, for some open $U \subseteq L$.

One application where topology has been employed is backwards strictness analysis. A characterization of a strictness-analysis domain as open-set properties was made by Hunt [16], who observed that Clack and Peyton Jones's backwards strictness analysis employed abstract values called *frontiers*, which were finite subsets of a finite lattice, D, that represented up-closed subsets of D. Since up-closed subsets of a finite lattice are Scott-open, all monotone functions $f : D \to D$ are Scott-continuous, implying f^{-1} maps frontiers to frontiers, ensuring that the analysis preserved strictness properties "on the nose." (In the present paper, we will show that such functions f are therefore backwards complete [14].)

Dybjer formalized this property for denotational semantics definitions and domain equations, axiomatizing the Scott topology of the latter as well as the law that the inverse of a Scott-continuous function maps open sets to open sets. He then showed strictness analysis is an instance of his axiomatization [12].

The most striking application of topology to abstract domains came from Jensen [17], who utilized Abramsky's domain theory in logical form [1]. Recall that Abramsky applied Stone duality [18] to domain theory, generating a Scott domain from a set of atomic elements that act as primitive propositions in a domain logic, closing them under a set of frame axioms. Jensen observed that one can use a finite subset of the atomic elements with the frame axioms to generate an abstract domain that approximates the domain generated from all the atomic elements. Jensen called his methodology *abstract interpretation in logical form* and applied it to strictness analysis, as did Benton, who proposed his own "strictness logic" [2].

The present paper steps back from strictness analysis and frame structures and poses a general question: "Starting from naive set theory, in what sense does an abstract domain define a "topology" on the concrete domain that it approximates?" Based on this "topology," what does it mean for a function to preserve and reflect the "open" and "closed" sets? How do these notions define both forwards and backwards static analyses and how do they ensure soundness and completeness of the analyses?

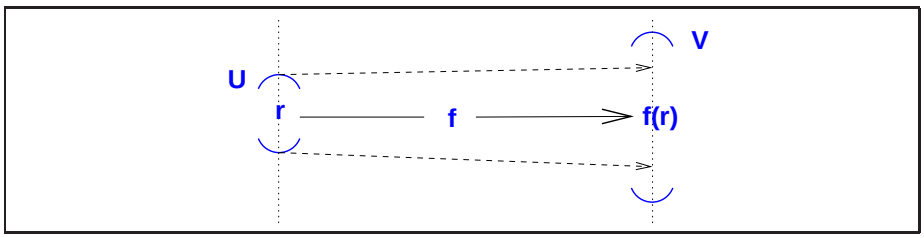


Fig. 1. Continuous function, f: When $f(r)$ falls within property (open set) V, then f maps some property, U, of r within V also.

To answer these questions, we develop abstract interpretation from topological principles by relaxing the definitions of open set and continuity so that they apply to arbitrary families of property sets. Surprisingly, key results still hold. When we study families of closed sets and open sets (induced from closure and interior operations), we discover that closed families generate postcondition analyses and open families generate precondition analyses (e.g., backwards strictness analyses). Even more striking, Giacobazzi's forwards- and backwards-complete functions [13, 14] are characterized as the topologically closed and continuous maps, respectively. Finally, we show that Smyth's upper and lower topologies for powersets [25] induce the overapproximating and underapproximating transition functions proposed by Cleaveland, et al. [5], and Dams, et al. [11], for abstract-model checking.

2 Basics of topology and abstract interpretation

We provide here the bare essentials of topology; details appear later as needed. (Willard [26] is a good reference.) For a set, Σ, a *topology*, $\mathcal{O}_\Sigma \subseteq \mathcal{P}(\Sigma)$, is a family of property sets, called the *open sets*, that are closed under union (for all $S \subseteq \mathcal{O}_\Sigma$, $\bigcup S \in \mathcal{O}_\Sigma$) and binary intersection ($U_1 \cap U_2 \in \mathcal{O}_\Sigma$ when $U_1, U_2 \in \mathcal{O}_\Sigma$) and include Σ ($\bigcup \mathcal{O}_\Sigma = \Sigma$). The complement, $\sim U = \Sigma - U$, of an open set U is a *closed set*; define $\mathcal{C}_\Sigma = \{\sim U \mid U \in \mathcal{O}_\Sigma\}$. For topology $\mathcal{O}_\Sigma$, a *base* is a subset, $\mathcal{B}_\Sigma \subseteq \mathcal{O}_\Sigma$, such that every $U \in \mathcal{O}_\Sigma$ is the union of some members of the base (for all $U \in \mathcal{O}_\Sigma$, there exists $S \subseteq \mathcal{B}_\Sigma$ such that $\cup S = U$). The members of the base are called *basic-open sets*. The topology on the real line uses open intervals, (a, b), for $a, b \in \mathbb{R}$, as its base.

For $S \subseteq \Sigma$, its *interior*, $\iota(S)$, is the largest open set within S. Indeed, $\iota(S) = \bigcup\{U \in \mathcal{O}_\Sigma \mid U \subseteq S\}$. The smallest closed set enclosing S is its *closure*, $\rho(S) = \bigcap\{K \mid S \subseteq K,\ K \in \mathcal{C}_\Sigma\}$.

Given topologies for sets Σ and Δ, there are standard definitions for the coarsest topologies for $\Sigma \times \Delta$, $\Sigma \to \Delta$, etc. [26].

A function, $f : \Sigma \to \Sigma$, is *(topologically) continuous* iff for all $s \in \Sigma$ and $V \in \mathcal{O}_\Sigma$, if $f(s) \in V$, then there exists some $U \in \mathcal{O}_\Sigma$ such that $s \in U$ and $f[U] \subseteq V$ (where lift f to $\mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$: $f[U] = \{f(x) \mid x \in U\}$). See Figure 1. A crucial result is that f is continuous iff for all $U \in \mathcal{O}_\Sigma$, $f^{-1}(U) \in \mathcal{O}_\Sigma$ also,

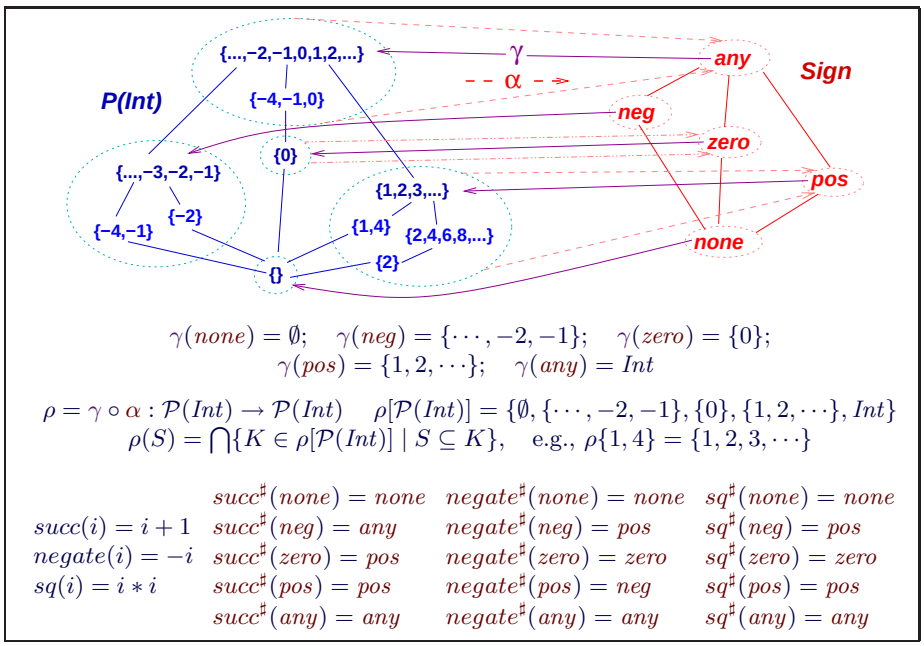


Fig. 2. Abstract domain, *Sign*, and the properties, $\rho[\mathcal{P}(Int)]$, it represents

where $f^{-1}(U) = \{x \in \Sigma \mid f(x) \in U\}$. Function f is an *open map* iff for all $U \in \mathcal{O}_\Sigma$, $f[U] \in \mathcal{O}_\Sigma$ and it is a *closed map* iff for all $K \in \mathcal{C}_\Sigma$, $f[K] \in \mathcal{C}_\Sigma$.

Abstract interpretation is computational approximation by computation on properties: For concrete data domain, Σ, select a set of property names, A, such that each $a \in A$ names the set $\gamma(a) \subseteq \Sigma$, for $\gamma : A \to \mathcal{P}(\Sigma)$. γ identifies the family of properties modelled by A. Order A s.t. $a \sqsubseteq a'$ iff $\gamma(a) \subseteq \gamma(a')$ — it should be a partial ordering.

Figure 2 displays an approximation of the integers, *Int*, by sign properties, *Sign*. (Notice *how few* properties are identified — just $\{none, neg, zero, pos, any\}$.)

When γ possesses an adjoint, $\alpha : \mathcal{P}(\Sigma) \to Sign$, then there is a Galois connection[3] and $\rho = \gamma \circ \alpha$ is an *upper closure operator* — $\rho : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ is monotone, extensive ($S \subseteq \rho(S)$), and idempotent ($\rho \circ \rho = \rho$). ρ's range, $\rho[\mathcal{P}(\Sigma)]$, identifies a family of property sets, but the family is typically *not* a topology, although it *is* closed under intersection (for all $S \subseteq \rho[\mathcal{P}(\Sigma)], \bigcap S \in \rho[\mathcal{P}(\Sigma)]$).

Computation functions, $f : \Sigma \to \Sigma$, are *soundly approximated* by $f^\sharp : A \to A$ iff $\alpha(f[S]) \sqsubseteq f^\sharp(\alpha(S))$, for all $S \in \mathcal{P}(\Sigma)$ (equivalently, iff $f[\gamma(a)] \subseteq \gamma(f^\sharp(a))$, for all $a \in A$) where we "lift" f to $f[S] = \{f(s) \mid s \in S\}$. See Figure 2.

The most precise such $f^\sharp$ is defined $f_0^\sharp = \alpha \circ f \circ \gamma$, where again, f is "lifted." When f is approximated exactly by $f_0^\sharp$ such that $f \circ \gamma = \gamma \circ f_0^\sharp$, we say f is *forwards complete*; f is forwards complete iff for all $K \in \rho[\mathcal{P}(\Sigma)]$, $f[K] \in \rho[\mathcal{P}(\Sigma)]$, that

[3] that is, $S \subseteq \gamma(a)$ iff $\alpha(S) \sqsubseteq a$, for all $S \in \mathcal{P}(\Sigma)$ and $a \in A$

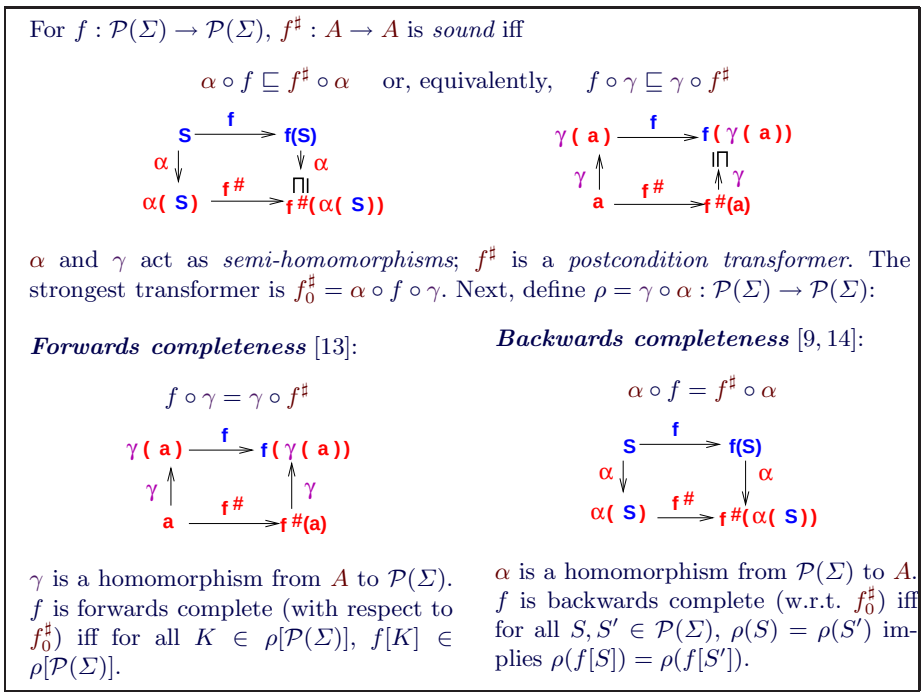


Fig. 3. Sound and complete forms of abstract functions

is, iff $f \circ \rho = \rho \circ f \circ \rho$ [13]. That is, f maps properties to properties "on the nose." When f is approximated exactly such that $\alpha \circ f = f_0^\sharp \circ \alpha$, we say f is *backwards complete*; f is backwards complete iff for all $S, S' \in \mathcal{P}(\Sigma)$, $\rho(S) = \rho(S')$ implies $\rho(f[S]) = \rho(f[S'])$, that is, iff $\rho \circ f = \rho \circ f \circ \rho$. [14, 21]. That is, f maps ρ-equivalent arguments to ρ-equivalent answers. See Figure 3. In Figure 2, *sq* is backwards but not forwards complete; *negate* is both backwards and forwards complete, and *succ* is neither.

Giacobazzi and his colleagues defined iterative refinement methods, called *shell constructions*, that add new elements to an abstract domain so that a incomplete function f becomes forwards or backwards complete, as desired [13, 14]. They showed that the shell constructions formalize the CEGAR refinement method of abstract model checking [3].

This paper's main result is the equivalence of backwards and forwards completeness to topological continuity and topologically closed maps, respectively.

3 Property families, function preservation and reflection

We now develop abstract interpretation with topological concepts.

For a concrete state set, Σ, choose some $\mathcal{F}_\Sigma \subseteq \mathcal{P}(\Sigma)$ as a family of properties. (In Figure 2, the family $Sign_{Int}$ is $\{\emptyset, \{i \mid i < 0\}, \{0\}, \{i \mid i > 0\}, Int\}$.)

For each $U \in \mathcal{F}_\Sigma$, its complement is $\sim U = \Sigma - U$; for $\mathcal{F}_\Sigma$, its *complement family*, $\sim \mathcal{F}_\Sigma$, is $\{\sim U \mid U \in \mathcal{F}_\Sigma\}$. (E.g., $\sim Sign_{Int}$ is $\{Int, \{i \mid i \geq 0\}, \{i \mid i \neq 0\}, \{i \mid i \leq 0\}, \emptyset\}$.)

When property family $\mathcal{O}_\Sigma \subseteq \mathcal{P}(\Sigma)$ is closed under unions, then $\mathcal{O}_\Sigma$ is an *open family*. Every open family has an *interior* operation, ι, which computes the largest property contained within a set: $\iota : \mathcal{P}(\Sigma) \to \mathcal{O}_\Sigma$ is defined $\iota(S) = \cup\{U \in \mathcal{O}_\Sigma \mid U \subseteq S\}$.

Dually, if a property family $\mathcal{C}_\Sigma$ is closed under intersections, it is a *closed family* (*Moore family* [9]). Every closed family has a *closure* operation, ρ, which computes the smallest property covering a set: $\rho : \Sigma \to \mathcal{C}_\Sigma$ is defined $\rho(S) = \cap\{K \in \mathcal{C}_\Sigma \mid S \subseteq K\}$. ($Sign_{Int}$ in Figure 2 is a closed (but not open) family, whose closure operation is the ρ stated in the Figure.)

If $\mathcal{O}_\Sigma$ is an open family, then its complement is a closed family (and vice versa), where $\bigcap_{i\in I} K_i = \sim\bigcup_{i\in I} \sim K_i$ (where $\bigcup_{i\in I} U_i = \sim\bigcap_{i\in I} \sim U_i$).

Let $f : \Sigma \to \Delta$ be a function; define $f : \mathcal{P}(\Sigma) \to \mathcal{P}(\Delta)$ as $f[S] = \{f(s) \mid s \in S\}$. Next, define function inverse, $f^{-1} : \mathcal{P}(\Delta) \to \mathcal{P}(\Sigma)$, as $f^{-1}(T) = \{s \in \Sigma \mid f(s) \in T\}$.

For property families, $\mathcal{F}_\Sigma$ and $\mathcal{F}_\Delta$, $f : \Sigma \to \Delta$ is $\mathcal{F}_\Sigma\mathcal{F}_\Delta$*-preserving* iff for all $U \in \mathcal{F}_\Sigma$, $f[U] \in \mathcal{F}_\Delta$. In such a case, $f : \mathcal{F}_\Sigma \to \mathcal{F}_\Delta$ is well defined. To reduce notation, we use functions, $f : \Sigma \to \Sigma$, with the same domain and codomain (and we say, "f is $\mathcal{F}_\Sigma$-preserving"), but all results that follow hold for functions with distinct codomains and domains, too. (In Figure 2, *negate* is $Sign_{Int}$-preserving.)

Definition 1. *For $s \in \Sigma$ and $S \subseteq \Sigma$, let U_s (respectively, U_S) denote a member of $\mathcal{F}_\Sigma$ such that $s \in U_s$ (respectively, $S \subseteq U_S$).*

(i) *For $s \in \Sigma$, $f : \Sigma \to \Sigma$ is* continuous at s *iff for all $V_{f(s)} \in \mathcal{F}_\Sigma$, there exists some $U_s \in \mathcal{F}_\Sigma$ such that $f[U_s] \subseteq V_{f(s)}$.*

(ii) *For $S \subseteq \Sigma$, f is* continuous at S *iff for all $V_{f[S]} \in \mathcal{F}_\Sigma$, there exists some $U_S \in \mathcal{F}_\Sigma$ such that $f[U_S] \subseteq V_{f[S]}$.*

(iii) *f is $\mathcal{F}_\Sigma$-*reflecting *iff for all $V \in \mathcal{F}_\Sigma$, $f^{-1}(V) \in \mathcal{F}_\Sigma$, that is, f^{-1} is $\mathcal{F}_\Sigma$-preserving.*

Proposition 2. *(i) f is $\mathcal{F}_\Sigma$-reflecting iff f is continuous at S, for all $S \subseteq \Sigma$. (ii) If $\mathcal{F}_\Sigma$ is an open family, then f is $\mathcal{F}_\Sigma$-reflecting iff f is continuous at s, for all $s \in \Sigma$.*

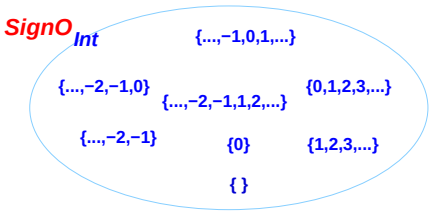
Proof. We prove (i); (ii) is a standard result [26]. Only if: for $V \in \mathcal{F}_\Sigma$, consider $f^{-1}(V)$. Because f is continuous at all $S \subseteq \Sigma$, there is some $U_{f^{-1}(V)} \in \mathcal{F}_\Sigma$ such that $f[U_{f^{-1}(V)}] \subseteq V$. But $U_{f^{-1}(V)}$ must equal $f^{-1}(V)$ for this to hold.

If: for $S \subseteq \Sigma$, say that $V_S \in \mathcal{F}_\Sigma$. Since f is reflecting, $f^{-1}(V_S) \in \mathcal{F}_\Sigma$. Thus, $f[f^{-1}(V_S)] \subseteq V_S$.□

The proofs in this paper rely on naive-set reasoning (cf. Willard [26]) and will often be omitted. We retain these critical dualities for all f and $\mathcal{F}_\Sigma$:

Proposition 3. *$f : \Sigma \to \Sigma$ is $\sim\mathcal{F}_\Sigma$-reflecting iff f is $\mathcal{F}_\Sigma$-reflecting.*

f is $\mathcal{F}_\Sigma$-preserving iff $\widetilde{f} = \sim \circ f \circ \sim$ is $\sim\mathcal{F}_\Sigma$-preserving.



$succ^\sharp\{i \mid i < 0\} = \{i \mid i \leq 0\}$
$succ^\sharp\{0\} = \{i \mid i > 0\}$
$succ^\sharp\{i \mid i > 0\} = \{i \mid i > 0\}$
$succ^\sharp\{i \mid i \leq 0\} = Int$
$succ^\sharp\{i \mid i \neq 0\} = Int$, etc.

$\rho_\cup(S) = \cup\{\rho\{s\} \mid s \in S\}$

$f^\sharp = \rho_\cup \circ f$

$\widetilde{pre}_{f^\sharp}(U) = \cup\{V \in Sign\mathcal{O}_{Int} \mid f^\sharp(V) \subseteq U\}$

For $succ(i) = i + 1$,

$\widetilde{pre}_{succ^\sharp}\{i \mid i > 0\} = \{i \mid i \geq 0\}$
$\widetilde{pre}_{succ^\sharp}\{0\} = \emptyset$
$\widetilde{pre}_{succ^\sharp}\{i \mid i < 0\} = \emptyset$
$\widetilde{pre}_{succ^\sharp}\{i \mid i \leq 0\} = \{i \mid i < 0\}$, etc.

Fig. 4. Using $Sign_{Int} = \{\emptyset, \{i \mid i < 0\}, \{0\}, \{i \mid i > 0\}, Int\}$ as a base for a topology.

In Figure 2, *negate* and *square* are $Sign_{Int}$-reflecting (but *succ* is not). This makes the two functions $\sim Sign_{Int}$ reflecting, where $\sim Sign_{Int} = \{Int, \widetilde{\{i \mid i \geq 0\}}, \{i \mid i \neq 0\}, \widetilde{\{i \mid i \leq 0\}}, \widetilde{\emptyset}\}$. Since *negate* is $Sign_{Int}$-preserving, *negate* is $\sim Sign_{Int}$-preserving, e.g., $negate\{i \mid i \geq 0\} = \{i \mid i \leq 0\}$. We exploit such dualities in the next section.

4 Applications: logics, postconditions, preconditions

A property family lists the properties that can be computed by an abstract interpretation. To implement it, we name each of the sets in the family, e.g., Figure 2 shows that $Sign = \{none, neg, zero, pos, any\}$ are the names for $Sign_{Int}$ and $\gamma : Sign \to Sign_{Int}$ concretizes each name to its property set. Within *Sign*, $a \sqsubseteq a'$ iff $\gamma(a) \subseteq \gamma(a')$. To reduce notation, the abstract interpretations in this paper are defined directly upon the property sets rather upon than the names of the sets [6, 14]. For example, we write $succ^\sharp\{0\} = \{i \mid i > 0\}$ rather than $succ^\sharp(zero) = pos$.

There is a weakened form of Stone duality here [1, 18]: a property family $\mathcal{F}_\Sigma$ has a frame-like "logic" whose "primitive propositions" are the $U \in \mathcal{F}_\Sigma$ and "connectives" are the functions that are $\mathcal{F}_\Sigma$-preserving. Based on Figure 2, we know that $Sign_{Int}$'s logic includes

$$\phi ::= U \mid \phi_1 \cap \phi_2 \mid negate\ \phi$$

where $U \in Sign_{Int}$. $\cap$ appears because the family is closed; *negate* appears because it is $Sign_{Int}$-preserving. A set S *has property* ϕ iff $S \subseteq \phi$, e.g., $\{1, 3\}$ has property $negate\{i \mid i < 0\}$. (When $\mathcal{F}_\Sigma$ is a topology, its logic is a frame [18] and includes *false* (empty set), *true* (Σ), disjunction (union), and conjunction (intersection).)

Ideally, for conducting an abstract interpretation, a program's transition functions, $f : \Sigma \to \Sigma$, are A-preserving — fall within the logic (cf. [16]). This

rarely happens, e.g., a program that counts by ones uses the transition function, $succ : Int \to Int$, $succ(i) = i + 1$, which is not $Sign_{Int}$-preserving. In this case, we must define a $succ^\sharp : Sign_{Int} \to Sign_{Int}$ to soundly approximate $succ$.

If property family $\mathcal{C}_\Sigma$ is closed, we use its closure operator, ρ, to define from $f : \Sigma \to \Sigma$ its *overapproximation* $f^\sharp : \mathcal{C}_\Sigma \to \mathcal{C}_\Sigma$ as $f^\sharp = \rho \circ f$. Function $f^\sharp$ generates sound postconditions, because this relational assertion ("Hoare triple"),

$$\{\phi\} f \{f^\sharp(\phi)\}$$

holds true (where $\{\phi\} f \{\psi\}$ asserts $f[\phi] \subseteq \psi$, for $\phi, \psi \in \mathcal{C}_\Sigma$). Because $f^\sharp(\phi) = \rho(f[\phi])$ is the *smallest* set in $\mathcal{C}_\Sigma$ that contains $f[\phi]$, it is the *strongest postcondition of f and ϕ expressible in $\mathcal{C}_\Sigma$*: $\{\phi\} f \{\psi\}$ implies $\{\phi\} f \{f^\sharp(\phi)\}$ and $f^\sharp(\phi) \subseteq \psi$.[4] (For example, for $Sign_{Int}$, $succ^\sharp = \rho \circ succ$, so that $succ^\sharp\{0\} = \rho(succ\{0\}) = \rho\{1\} = \{i \mid i \geq 0\}$, etc.)

When f is forwards complete (cf. Figure 3), we have completeness in the entire codomain: for *every* $S \subseteq \mathcal{P}(\Sigma)$, $\{\phi\} f \{S\}$ implies $\{\phi\} f \{f^\sharp(\phi)\}$ and $f^\sharp(\phi) \subseteq S$. When f is backwards complete, completeness extends to the entire domain: for every $S \subseteq \mathcal{P}(\Sigma)$, $\{S\} f \{\psi\}$ implies $\{S\} f \{f^\sharp(\rho(S))\}$ and $f^\sharp(\rho(S)) \subseteq \psi$. But each completeness notion yields nothing more in the logic than the strongest postcondition — what deeper property is hiding here? (See the next section.)

In summary, a forwards static analysis calculates postconditions [6, 7], and the development suggests this moral:

Use a closed family of properties to generate a postcondition analysis.

What if we desire preconditions from a forwards analysis? We must first define $f^\sharp$'s inverse, $f^{\sharp -}_{\mathcal{C}_\Sigma} : \mathcal{C}_\Sigma \to \mathcal{P}(\mathcal{C}_\Sigma)$, as

$$(\star) \qquad f^{\sharp -}_{\mathcal{C}_\Sigma}(U) = \{V \in \mathcal{C}_\Sigma \mid f^\sharp(V) \subseteq U\}$$

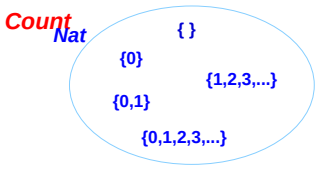
We have, for all $V \in f^{\sharp -}_{\mathcal{C}_\Sigma}(\phi)$, that $\{V\} f \{\phi\}$ holds true, but $\cup f^{\sharp -}_{\mathcal{C}_\Sigma}(U)$ *itself* is not necessarily expressible in the closed family, $\mathcal{C}_\Sigma$.

To repair the flaw, we close $\mathcal{C}_\Sigma$ under unions, that is, *we use it as a base for a topology* on Σ, namely, $\mathcal{CO}_\Sigma = \{\cup T \mid T \subseteq \mathcal{C}_\Sigma\}$, which is both an open *and* a closed family. (The closure map $\rho_\cup : \mathcal{CO}_\Sigma \to \mathcal{CO}_\Sigma$ equals $\rho_\cup(S) = \cup\{\rho\{s\} \mid s \in S\}$.) Now, we approximate with $\mathcal{CO}_\Sigma$: for $f : \Sigma \to \Sigma$, we define $f^\sharp : \mathcal{CO}_\Sigma \to \mathcal{CO}_\Sigma$ as $f^\sharp = \rho_\cup \circ f$; we define $f^{\sharp -}_{\mathcal{CO}_\Sigma} : \mathcal{CO}_\Sigma \to \mathcal{P}(\mathcal{CO}_\Sigma)$ as $f^{\sharp -}_{\mathcal{CO}_\Sigma}(U) = \{V \in \mathcal{CO}_\Sigma \mid f^\sharp(V) \subseteq U\}$, like before; and this makes $f^\sharp$'s weakest precondition, $\widetilde{pre}_{f^\sharp} : \mathcal{CO}_\Sigma \to \mathcal{CO}_\Sigma$, well defined: $\widetilde{pre}_{f^\sharp}(U) = \cup f^{\sharp -}_{\mathcal{CO}_\Sigma}(U)$.[5]

In lattice theory, closure under unions is called *disjunctive completion* [10]. Figure 4 shows the disjunctive completion of $Sign_{Int}$ to $Sign\mathcal{O}_{Int}$ and the precondition function for $succ^\sharp$. Now, we have preconditions, but the extra sets generated by the disjunctive completion may make the abstract domain *too large* for a practical static analysis.

[4] If $\mathcal{F}_\Sigma$ is not closed, then the $f : \Sigma \to \Sigma$ must be approximated by some $f^\sharp : \mathcal{F}_\Sigma \to \mathcal{F}_\Sigma$ such that $\{U\} f \{f^\sharp(U)\}$ holds for all $U \in \mathcal{F}_\Sigma$.

[5] Since $\mathcal{CO}_\Sigma$ possesses an interior operation, ι, we can define the precondition as merely $\iota \circ f^{-1}$, and one can prove that $\widetilde{pre}_{f^\sharp} = \iota \circ f^{-1}$ [22].



For $Nat = \{0, 1, 2, \cdots\}$,
$Count_{Nat} = \{\emptyset, \{0\}, \{0, 1\}, \{1, 2, 3, \cdots\}, Nat\}$

$\iota(S) = \cup\{U \mid U \subseteq S\}$, e.g.,
$\iota\{0, 1, 2\} = \{0, 1\}$
$\iota\{2, 4, 6, 8, \cdots\} = \emptyset$

For $succ(n) = n + 1$,
$succ^{-o} = \iota \circ succ^{-1}$, e.g.,

$succ^{-o}\{0, 1\} = \{0\}$
$succ^{-o}\{0\} = \emptyset = succ^{-o}(\emptyset)$
$succ^{-o}\{1, 2, 3, \cdots\} = Nat = succ^{-o}(Nat)$

Fig. 5. Open family for counting analysis

If we are primarily interested in preconditions, we should start with an *open* family of properties (one closed under unions), $\mathcal{O}_\Sigma \subseteq \mathcal{P}(\Sigma)$, so that we have straightaway an interior operation, $\iota : \Sigma \to \mathcal{O}_\Sigma$. An open family's logic includes disjunction as well as the inverses of those functions that are $\mathcal{O}_\Sigma$-reflecting.

We *underapproximate* the inverses of transition functions: For $f : \Sigma \to \Sigma$, define $f^{-o} : \mathcal{O}_\Sigma \to \mathcal{O}_\Sigma$ as $f^{-o} = \iota \circ f^{-1}$. This implies

$$\{f^{-o}(\psi)\}f\{\psi\}$$

holds true and $f^{-o}(\psi)$ is the *weakest precondition of* f *and* ψ *expressible in* $\mathcal{O}_\Sigma$*:* $\{\phi\}f\{\psi\}$ implies $\{f^{-o}(\psi)\}f\{\psi\}$ and $\phi \subseteq f^{-o}(\psi)$. Further, we can formalize the two forms of completeness with respect to ι, but we see in the next section a topological characterization.

Figure 5 defines an open (but not closed) family, $Count_{Nat}$, for a backwards counting analysis. The successor operation, $succ : Nat \to Nat$, is $Count_{Nat}$-reflecting, so $succ^{-1}$ lives in the family's logic and $succ^{-o} = succ^{-1}$. (See the Figure.) Predecessor ($pred(n) = n - 1$) is not reflecting, and $pred^{-o} = \iota \circ pred^{-1}$ yields $pred^{-o}\{0, 1\} = \iota\{0, 1, 2\} = \{1\}$, etc. Abstract domain $Count_{Nat}$ is imperfect, e.g., it cannot prove the assertion, $\{\{0\}\}succ; pred\{\{0\}\}$. As indicated by research on backwards strictness analysis [2, 12, 16, 17], the moral is:

Use an open family of properties to generate a precondition analysis.

There is no need to work from a closed property family.[6]

Because the complement of a closed family is open (and vice versa), we can move from a postcondition analysis to a precondition one: Say that $\mathcal{C}_\Sigma$ is closed so that $\mathcal{O}_\Sigma = {\sim}\mathcal{C}_\Sigma$ is open. First, every $\mathcal{C}_\Sigma$-reflecting f is $\mathcal{O}_\Sigma$-reflecting, and for every $\mathcal{C}_\Sigma$-preserving $f : \Sigma \to \Sigma$, $\widetilde{f}$ is $\mathcal{O}_\Sigma$-preserving, by Proposition 3. (So, $\mathcal{C}_\Sigma$'s conjunction operation is preserved in $\mathcal{O}_\Sigma$'s logic as disjunction.) We have

Lemma 4. *For all* $f : \Sigma \to \Sigma$ *and* $S \subseteq \Sigma$, ${\sim}f^{-1}(S) = f^{-1}({\sim}S)$.
For closed family $\mathcal{C}_\Sigma$ *and* $\mathcal{O}_\Sigma = {\sim}\mathcal{C}_\Sigma$, ${\sim} \circ \rho = \iota \circ {\sim}$.

[6] But there is an adjoint here, $\mathcal{P}(\Sigma)^{op}\langle\iota, id\rangle\mathcal{O}_\Sigma^{op}$ — $\subseteq$ becomes $\supseteq$.

Proposition 5. *For all* $S \subseteq \Sigma$, $\widetilde{f^{-1}}(S) = f^{-1}(S)$.
$(\widetilde{f^{-1}})^\sharp(U) = f^{-o}(U)$, *for all* $U \in \mathcal{O}_\Sigma$. *(Note:* $(\widetilde{f^{-1}})^\sharp = \sim \circ (f^{-1})^\sharp \circ \sim$.*)*

Proof. We prove the second claim, $(\widetilde{f^{-1}})^\sharp(U) = \sim \circ \rho \circ f^{-1} \circ \sim (\sim K)$, where $U = \sim K$. This equals $\sim \rho(f^{-1}(K)) = \iota(\sim f^{-1}(K))$, by the previous lemma, which equals $\iota(f^{-1}(\sim K))$, by the lemma, which equals $f^{-o}(U)$. □

The last result says that, by using $\mathcal{C}_\Sigma$'s closure operator to define the overapproximating $(f^{-1})^\sharp$, we can compute an *underapproximating*, weakest-precondition analysis on $\mathcal{O}_\Sigma = \sim\mathcal{C}_\Sigma$ defined as $(\widetilde{f^{-1}})^\sharp$.

As an example, consider $\sim \mathit{Sign}_{\mathit{Int}} = \{\mathit{Int}, \{i \mid i \geq 0\}, \{i \mid i \neq 0\}, \{i \mid i \leq 0\}, \emptyset\}$, based on Figure 2. This open family's logic includes

$$\psi \ ::= \sim U \mid \psi_1 \cup \psi_2 \mid \mathit{negate}^{-1}\psi \mid \mathit{sq}^{-1}\psi, \quad \text{for } U \in \mathit{Sign}_{\mathit{Int}}$$

Because *succ* is not $\mathit{Sign}_{\mathit{Int}}$-reflecting, we underapproximate it by $\mathit{succ}^{-o} = (\widetilde{\mathit{succ}^{-1}})^\sharp$. We have $\mathit{succ}^{-o}\{i \mid i \neq 0\} = \{i \mid i \geq 0\}$; $\mathit{succ}^{-o}\mathit{Int} = \mathit{Int}$; and $\mathit{succ}^{-o}(U) = \emptyset$, otherwise. In this fashion, a postcondition analysis based on $\mathcal{C}_\Sigma$ defines a precondition analysis on $\sim\mathcal{C}_\Sigma$.

Finally, every $\mathcal{F}_\Sigma$ possesses both a logic for validation (viz., $\mathcal{F}_\Sigma$'s sets and its preserving operators) as well as a dual, *refutation logic*: $\sim\mathcal{F}_\Sigma$'s logic. We say that S *has property* $\neg\phi$ if $S \subseteq \sim\phi$, for $\sim\phi \in \sim\mathcal{F}_\Sigma$. This is the foundation for three-valued static analyses [20], where one uses a single abstract domain to compute validation, refutation, and "don't know" judgements.

5 From continuity to completeness

As stated earlier, there is a correspondence between functions that preserve and reflect property sets and abstract-interpretation-complete functions:

Recall that $f : \Sigma \to \Sigma$ is $\mathcal{F}_\Sigma$-preserving iff for all $S \in \mathcal{F}_\Sigma$, $f[S] \in \mathcal{F}_\Sigma$. But this is *exactly the definition of abstract-interpretation forwards completeness* when $\mathcal{F}_\Sigma$ is a closed family. In topological terms, f is a closed map.

We now prove that $\mathcal{F}_\Sigma$-reflection is exactly backwards completeness when $\mathcal{F}_\Sigma$ is a closed family. For $S, S' \subseteq \Sigma$, write $S \leq_{\mathcal{F}_\Sigma} S'$ iff for all $K \in \mathcal{F}_\Sigma, S \subseteq K$ implies $S' \subseteq K$. This is called the *specialization ordering* in topology. Write $S \equiv_{\mathcal{F}_\Sigma} S'$ iff $S \leq_{\mathcal{F}_\Sigma} S'$ and $S' \leq_{\mathcal{F}_\Sigma} S$. The following definition is the usual one for abstract-interpretation backwards completeness:

Definition 6. *For property family,* $\mathcal{F}_\Sigma$, $f : \Sigma \to \Sigma$ *is* $B_{\mathcal{F}_\Sigma}$-complete *iff for all* $S, S' \subseteq \Sigma$, $S \equiv_{\mathcal{F}_\Sigma} S'$ *implies* $f[S] \equiv_{\mathcal{F}_\Sigma} f[S']$.

Proposition 7. *If* f *is* $\mathcal{F}_\Sigma$*-reflecting, then it is* $B_{\mathcal{F}_\Sigma}$*-complete.*

Proof. Assume $S \leq_\Sigma S'$ and show $f[S] \leq_\Sigma f[S']$: Say that $f[S] \subseteq K \in \mathcal{F}_\Sigma$; since f is reflecting, $f^{-1}(K) \in \mathcal{F}_\Sigma$, too, and $S \subseteq f^{-1}(K)$. Because $S \leq_\Sigma S'$, $S' \subseteq f^{-1}(K)$, implying $f[S'] \subseteq K$. □

The converse of the above might not hold, but say that $\mathcal{C}_\Sigma$ is a closed family so that $\rho(S) = \cap\{K \in \mathcal{C}_\Sigma \mid S \subseteq K\}$; we can prove the converse:

Lemma 8. *For all $S \subseteq \Sigma$, $S \equiv_{\mathcal{C}_\Sigma} \rho(S)$.*
For all $S, S' \subseteq \Sigma$, $S \equiv_{\mathcal{C}_\Sigma} S'$ iff $\rho(S) = \rho(S')$.

Lemma 9. *The following are equivalent for closed family, $\mathcal{C}_\Sigma$:*
(i) f is $B_{\mathcal{C}_\Sigma}$-complete;
(ii) for all $S \subseteq \Sigma$, $f[S] \equiv_{\mathcal{C}_\Sigma} f[\rho(S)]$;
(iii) $\rho \circ f = \rho \circ f \circ \rho$.

For a closed family, reflection (topological continuity) is backwards completeness:

Theorem 10. *For $\mathcal{C}_\Sigma$, $f : \Sigma \to \Sigma$ is $B_{\mathcal{C}_\Sigma}$-complete iff f is $\mathcal{C}_\Sigma$-reflecting.*

Proof. The if-part is already proved. For the only-if part, assume $f[S] \subseteq K \in \mathcal{C}_\Sigma$ and show there is some $L_S \in \mathcal{C}_\Sigma$ such that $f[L_S] \subseteq K$. Let $\rho(S)$ be the L_S: we have $f[\rho(S)] \equiv_{\mathcal{C}_\Sigma} f[S]$ which implies $f[\rho(S)] \subseteq K$. Use the Lemma above. □

Corollary 11. *(i) if f is backwards complete for $\mathcal{C}_\Sigma$, then f^{-1} is forwards complete for both $\mathcal{C}_\Sigma$ and $\sim\mathcal{C}_\Sigma$.*
(ii) f is forwards complete for $\mathcal{C}_\Sigma$ iff $\tilde{f}$ is forwards complete for $\sim\mathcal{C}_\Sigma$.

Proof. By Proposition 3 and the previous Theorem.

The characterizations of forwards completeness as property preservation and backwards completeness as property reflection (continuity) apply to open families as well. They also link the shell constructions of Giacobazzi, et al. [13, 14], to refinements of topologies and the characterization of function continuity to convergence of nets [26].

6 Relation to partial-order backwards completeness

The crucial characterization of backwards completeness by Giacobazzi, et al. [14] is made in a "frame-theory" presentation [18], where $(\mathcal{P}(\Sigma), \subseteq)$ is abstracted to a complete lattice, $(D, \sqsubseteq)$, and $\mathcal{C}_\Sigma$ is abstracted to $\rho[D] \subseteq D$, namely, the fixed points of upper closure map, $\rho : D \to D$. We can rephrase their work in terms of our development:

First, define $f^- : D \to \mathcal{P}(D)$ as $f^-(d) = \{e \in D \mid f(e) \sqsubseteq d\}$. When f^- is chain-continuous, then $f^-(d)$ has a set of maximal points, denoted by $max(f^-(d))$. When f is an *additive* function, that is, $f(\sqcup S) = \sqcup_{d \in S} f(d)$, for all $S \subseteq D$, then $max(f^-(d))$ is a singleton set. *This is the case for the point-set topology used in the previous section.*

Let $\rho[D]$ define D's closed family of "properties" and let $f : D \to D$ be chain-continuous. First, (i) f is *continuous at* $d \in D$ iff for all $e \in \rho[D]$, if $f(d) \sqsubseteq e$, then there exists $d' \in \rho[D]$ such that $d \sqsubseteq d'$ and $f(d') \sqsubseteq e$. Next, (ii) f is *ρ-reflecting* iff for all $e \in \rho[D]$, $max((f^-(d)) \subseteq \rho[D]$ (that is, the maximum elements of $f^-(d)$ are in $\rho[D]$). It is easy to prove that (i) and (ii) are equivalent.

We define $d \equiv_{\rho[D]} d'$ iff for all $e \in \rho[D]$, $d \sqsubseteq e$ iff $d' \sqsubseteq e$, that is, iff $\rho(d) = \rho(d')$. This yields the definition of backwards completeness: f is backwards-ρ-complete if $d \equiv_{\rho[D]} d'$ implies $f(d) \equiv_{\rho[D]} f(d')$ for all $d, d' \in D$, that is, $\rho \circ f = \rho \circ f \circ \rho$. We have immediately the main result of Giacobazzi, et al. [14] in the "frame theory": $f : D \to D$ is backwards-ρ-complete iff it is ρ-reflecting.

7 Nondeterminism and semicontinuity

Model-checking applications of abstract interpretation commence with transition *relations* on $\Sigma \times \Sigma$, which we will treat as functions of arity, $f : \Sigma \to \mathcal{P}(\Sigma)$. The property family for $\mathcal{P}(\Sigma)$ is different from Σ's and depends on how we define f's preimage, a map, $\mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$. We have two choices: for $S \subseteq \Sigma$,

$$pre_f(S) = \{c \in \Sigma \mid f(c) \cap S \neq \emptyset\}$$
$$\widetilde{pre}_f(S) = \{c \in \Sigma \mid f(c) \subseteq S\}$$

The following definitions come from Vietoris [25]:

Definition 12. *For property family, $\mathcal{F}_\Sigma \subseteq \Sigma$,*
$f : \Sigma \to \mathcal{P}(\Sigma)$ is lower semicontinuous *for $\mathcal{F}_\Sigma$ iff pre_f is $\mathcal{F}_\Sigma$-preserving.*
$f : \Sigma \to \mathcal{P}(\Sigma)$ is upper semicontinuous *for $\mathcal{F}_\Sigma$ iff $\widetilde{pre}_f$ is $\mathcal{F}_\Sigma$-preserving.*

Say we want pre_f in the logic for $\mathcal{F}_\Sigma$; what property family for $\mathcal{P}(\Sigma)$ is appropriate? The answer was found by Smyth [25]: define $\mathcal{O}^L_{\mathcal{F}_\Sigma} \subseteq \mathcal{P}(\mathcal{P}(\Sigma))$ to be the open family generated by taking all unions of the base, $\mathcal{B}^L_{\mathcal{F}_\Sigma} = \{\exists U \mid U \in \mathcal{F}_\Sigma\}$, where $\exists U = \{S \subseteq \Sigma \mid S \cap U \neq \emptyset\}$. (Read $\exists U$ as "all the sets that meet property U"). Indeed, for all $U \in \mathcal{F}_\Sigma$, $f^{-1}(\exists U) = pre_f(U)$. $\mathcal{O}^L_{\mathcal{F}_\Sigma}$ is called the *lower topology based on* $\mathcal{F}_\Sigma$. This result is due to Smyth [25]:

Proposition 13. *If $\mathcal{O}_\Sigma \subseteq \Sigma$ is an open family for Σ, then $f : \Sigma \to \mathcal{P}(\Sigma)$ is lower semicontinuous for $\mathcal{O}_\Sigma$ iff f is $\mathcal{O}_\Sigma\mathcal{O}^L_{\mathcal{O}_\Sigma}$-reflecting.*

That is, pre_f lies in the logic for $\mathcal{O}_\Sigma$ iff f is $\mathcal{O}_\Sigma\mathcal{O}^L_{\mathcal{O}_\Sigma}$-reflecting. When $f : \Sigma \to \mathcal{P}(\Sigma)$ is not lower semicontinuous, we simply use $\mathcal{O}_\Sigma$'s interior operator, ι, to approximate pre_f by $\iota \circ pre_f : \mathcal{O}_\Sigma \to \mathcal{O}_\Sigma$, like in Section 4.

We can rephrase the previous Proposition in terms of its dual, closed family and discover a well-travelled path: For open family, $\mathcal{O}_\Sigma$, and $\mathcal{C}_\Sigma = {\sim}\mathcal{O}_\Sigma$, we have that ${\sim}\mathcal{O}^L_{\mathcal{O}_\Sigma}$ is a closed family whose members are all the intersections of sets taken from the (co)base, $\mathcal{B}^U_{\mathcal{C}_\Sigma} = \{\forall K \mid K \in \mathcal{C}_\Sigma\}$, where $\forall K = \{S \subseteq \Sigma \mid S \subseteq K\}$. (Read $\forall K$ as "all the sets covered by property K.") Indeed, for all $K \in \mathcal{C}_\Sigma$, $f^{-1}(\forall K) = \widetilde{pre}_f(K)$. We name the closed family: $\mathcal{C}^U_{\mathcal{C}_\Sigma} = {\sim}\mathcal{O}^L_{\mathcal{O}_\Sigma}$.

Corollary 14. *Let $\mathcal{C}_\Sigma$ be a closed family and define $\mathcal{O}_\Sigma = {\sim}\mathcal{C}_\Sigma$.*
pre_f is $\mathcal{O}_\Sigma$-preserving iff $\widetilde{pre}_f$ is $\mathcal{C}_\Sigma$-preserving.
f is $\mathcal{O}_\Sigma\mathcal{O}^L_{\mathcal{O}_\Sigma}$-reflecting iff it is $\mathcal{C}_\Sigma\mathcal{C}^U_{\mathcal{C}_\Sigma}$-reflecting.
Hence, $\widetilde{pre}_f$ is $\mathcal{C}_\Sigma$-preserving iff f is $\mathcal{C}_\Sigma\mathcal{C}^U_{\mathcal{C}_\Sigma}$-reflecting iff f is upper semicontinuous for $\mathcal{C}_\Sigma$.

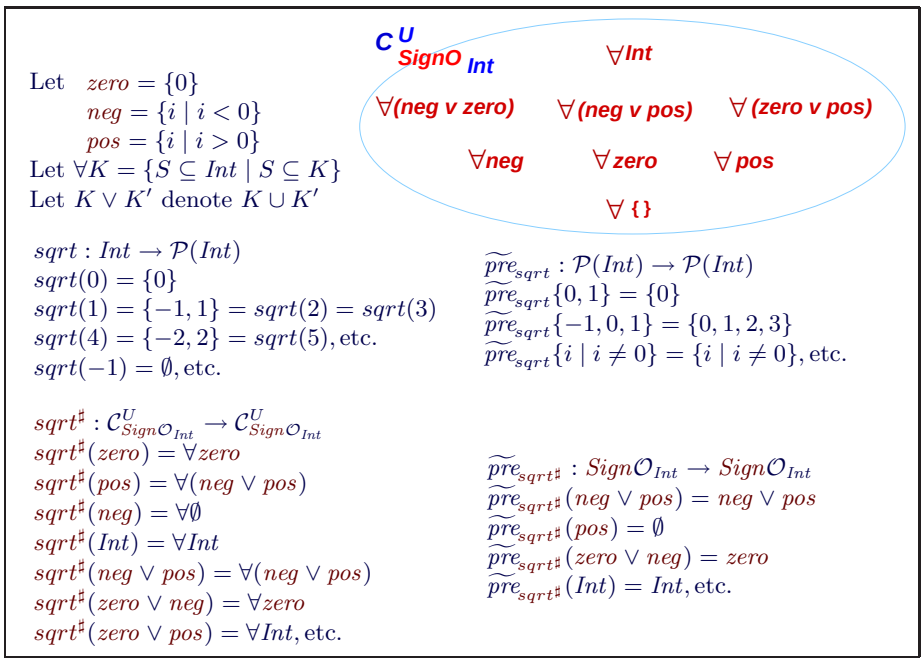


Fig. 6. $sqrt$, upper topology on $SignO_{Int}$, and $sqrt^\sharp$

Proof. By Propositions 3 and 13. □

The corollary tells us $\widetilde{pre}_f$ lies in $\mathcal{C}_\Sigma$'s logic when $f : \Sigma \to \mathcal{P}(\Sigma)$ is upper semicontinuous. But what if f is not? Then we must approximate it by some $f^\sharp : \mathcal{C}_\Sigma \to \mathcal{C}^U_{\mathcal{C}_\Sigma}$ from which we induce a $\mathcal{C}_\Sigma$-preserving $\widetilde{pre}_{f^\sharp}$. (Alas, we have no interior map to aid us, only a closure map.)

To do this, we need some insight: First, each $M \in \mathcal{C}^U_{\mathcal{C}_\Sigma}$ is a set of sets formed as $M = \bigcap_{i \in I}\{\forall K_i \mid K_i \in \mathcal{C}_\Sigma\}$. Read property M as "$\forall K_1 \wedge \forall K_2 \wedge \cdots \wedge \forall K_i \wedge \cdots$" — M's members are sets covered by property K_1 and covered by property K_2 and ... covered by property K_i and so on. For $f : \Sigma \to \mathcal{P}(\Sigma)$, we express its relational assertions in the form,

$$\{\phi\} f \{\forall\psi_1 \wedge \forall\psi_2 \wedge \cdots \wedge \forall\psi_i \wedge \cdots\}$$

By pointwise reasoning, the M defined above equals $\forall\bigcap\{K_i \mid K_i \in \mathcal{C}_\Sigma\}$, read as "$\forall(K_1 \wedge K_2 \wedge \cdots \wedge K_i \wedge \cdots)$." But $\bigcap\{K_i \mid K_i \in \mathcal{C}_\Sigma\} \in \mathcal{C}_\Sigma$, meaning that the relational assertion reverts to this benign format:

$$\{\phi\} f \{\forall\psi\}$$

for $\phi, \psi \in \mathcal{C}_\Sigma$. (You can write it as "$\phi \models [f]\psi$.") The quantifier reminds us that f's answer is a *set* of Σ-values, covered by ψ. And, $\phi \subseteq \widetilde{pre}_f(\psi) = f^{-1}(\forall\psi)$.

Say we approximate $f : \Sigma \to \mathcal{P}(\Sigma)$ by $f^\sharp(K) = \rho_U(f[K])$, where ρ_U is the closure operation for $\mathcal{C}^U_{\mathcal{C}_\Sigma}$: $\rho_U(T) = \bigcap\{\forall K \mid T \subseteq \forall K, K \in \mathcal{C}_\Sigma\}$. That is, $\rho_U(T)$

computes the conjunction of all properties K that cover all the sets in T. We have, as usual, that $\{\phi\}f\{f^\sharp(\phi)\}$. Next, the approximation of $\widetilde{pre}_f$ must be made sound: $\widetilde{pre}_{f^\sharp}(K) \subseteq \widetilde{pre}_f(K) = f^{-1}(\forall K)$, for all $K \in \mathcal{C}_\Sigma$. We work from Equation $(\star)$ in Section 4; $f^\sharp$'s inverse image is

$$f^\sharp{}^-_{\mathcal{C}_\Sigma}(K) = \{K' \in \mathcal{C}_\Sigma \mid f^\sharp(K') \subseteq \forall K\}$$

We wish to define $\widetilde{pre}_{f^\sharp}(K) = \cup f^\sharp{}^-(K)$, but $\widetilde{pre}_{f^\sharp}$'s image might fall outside of $\mathcal{C}_\Sigma$. This issue arose in Section 4, and we repeat the development there: build the disjunctive completion of $\mathcal{C}_\Sigma$ (closure under unions), $\mathcal{CO}_\Sigma$; redefine $f^\sharp : \mathcal{CO}_\Sigma \to \mathcal{C}^U_{\mathcal{CO}_\Sigma}$; and define $\widetilde{pre}_{f^\sharp} : \mathcal{CO}_\Sigma \to \mathcal{CO}_\Sigma$ as $\widetilde{pre}_{f^\sharp}(K) = \cup f^\sharp{}^-_{\mathcal{CO}_\Sigma}(K)$.

Figure 6 displays an integer square-root function, $sqrt : Int \to \mathcal{P}(Int)$. The disjunctive completion of $Sign_{Int}$ produces the topology, $Sign\mathcal{O}_{Int}$, in Figure 4, from which we generate $\mathcal{C}^{\mathcal{U}}_{Sign\mathcal{O}_{Int}}$, illustrated in Figure 6. This form of abstract domain is used for checking the box-modality of modal-mu calculus.

There is a dual development. Starting again with Σ and its property family, $\mathcal{F}_\Sigma$, define the property family for $\mathcal{P}(\Sigma)$, namely, $\mathcal{O}^U_{\mathcal{F}_\Sigma} \subseteq \mathcal{P}(\mathcal{P}(\Sigma))$, as the open family generated by taking all unions of the base, $\mathcal{B}^U_{\mathcal{F}_\Sigma} = \{\forall U \mid U \in \mathcal{F}_\Sigma\}$, where $\forall U = \{S \subseteq \Sigma \mid S \subseteq U\}$. This is the *upper topology based on* $\mathcal{F}_\Sigma$. (Recall, for all $U \in \mathcal{F}_\Sigma$, that $f^{-1}(\forall U) = \widetilde{pre}_f(U)$.)

Proposition 15. *[25] Let $\mathcal{O}_\Sigma \subseteq \Sigma$ be an open family. $f : \Sigma \to \mathcal{P}(\Sigma)$ is upper semicontinuous for $\mathcal{O}_\Sigma$ iff f is $\mathcal{O}_\Sigma\mathcal{O}^U_{\mathcal{O}_\Sigma}$-reflecting.*

When f is not upper semicontinuous, we may use $\iota \circ \widetilde{pre}_f : \mathcal{O}_\Sigma \to \mathcal{O}_\Sigma$, where ι is $\mathcal{O}_\Sigma$'s interior operator. The dual goes as follows: $\mathcal{C}^L_{\mathcal{C}_\Sigma} = {\sim}\mathcal{O}^U_{\mathcal{O}_\Sigma}$, whose members are all intersections of sets from the (co)base, $\mathcal{B}^L_{\mathcal{C}_\Sigma} = \{\exists K \mid K \in \mathcal{C}_\Sigma\}$, where $\exists K = \{S \subseteq \Sigma \mid S \cap K \neq \emptyset\}$. For all $K \in \mathcal{C}_\Sigma$, $f^{-1}(\exists K) = pre_f(K)$.

Corollary 16. *$\widetilde{pre}_f$ is $\mathcal{O}_\Sigma$-preserving iff pre_f is $\mathcal{C}_\Sigma$-preserving.*

f is $\mathcal{O}_\Sigma\mathcal{O}^U_{\mathcal{O}_\Sigma}$-reflecting iff it is $\mathcal{C}_\Sigma\mathcal{C}^L_{\mathcal{C}_\Sigma}$-reflecting.

Hence, pre_f is $\mathcal{C}_\Sigma$-preserving iff f is $\mathcal{C}_\Sigma\mathcal{C}^L_{\mathcal{C}_\Sigma}$-reflecting iff f is lower semicontinuous for $\mathcal{C}_\Sigma$.

Say that $f : \Sigma \to \mathcal{P}(\Sigma)$ is not lower semicontinuous. When we approximate it by $f^\flat : \mathcal{C}_\Sigma \to \mathcal{C}^L_{\mathcal{C}_\Sigma}$, what is the result? What is $pre_{f^\flat}$? The answer summarizes significant research on underapproximation [5, 11, 23].

Each $M \in \mathcal{C}^L_{\mathcal{C}_\Sigma}$ is a set of sets of form $M = \bigcap_{i\in I}\{\exists K_i \mid K_i \in \mathcal{C}_\Sigma\}$. Read M as "$\exists K_1 \wedge \exists K_2 \wedge \cdots \wedge \exists K_i \wedge \cdots$" — each of M's members is a set that meets (*witnesses*) K_1 and K_2 and ... K_i and so on. For $f : \Sigma \to \mathcal{P}(\Sigma)$, we express its relational assertions in the form,

$$\{\phi\}f\{\exists\psi_1 \wedge \exists\psi_2 \wedge \cdots \wedge \exists\psi_i \wedge \cdots\}$$

for $\psi_i \in \mathcal{C}_\Sigma$. (In the case of $\{\phi\}f\{\exists\psi\}$ you can write "$\phi \models \langle f\rangle\psi$." And, $\phi \subseteq pre_f(\psi) = f^{-1}(\exists\psi)$.)

We approximate $f : \Sigma \to \mathcal{P}(\Sigma)$ by $f^\flat(K) = \rho_L(f[K])$, where ρ_L is the closure operation for $\mathcal{C}^L_{\mathcal{C}_\Sigma}$: $\rho_L(T) = \bigcap\{\exists K \mid T \subseteq \exists K,\ K \in \mathcal{C}_\Sigma\}$. That is, $\rho_L(T)$ collects

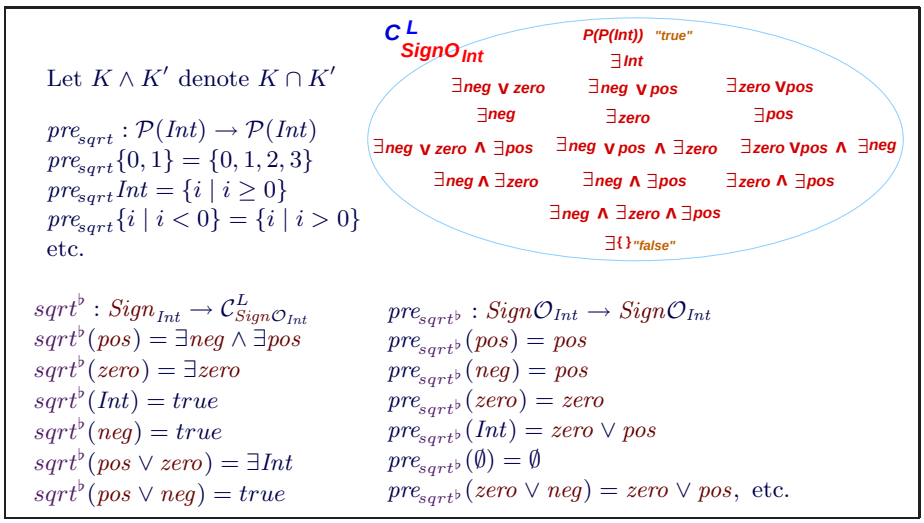


Fig. 7. Lower topology on $Sign\mathcal{O}_{Int}$ and $sqrt^\flat$

all the properties, K, that are witnessed (met) by each of the sets in T. We have $\{\phi\}f\{f^\flat(\phi)\}$, and $f^\flat(\phi)$ is the strongest postcondition in the logic associated with $\mathcal{C}^L_{\mathcal{C}_\Sigma}$, the "language of witnesses." Once again, we define $f^\flat\bar{}_{\mathcal{C}_\Sigma}(K) = \{K' \in \mathcal{C}_\Sigma \mid f^\flat(K') \subseteq \exists K\}$ and $pre_{f^\flat}(K) = \cup f^\flat\bar{}_{\mathcal{C}_\Sigma}(K)$. This is the definition used by Cleaveland [5], Dams [11], and Schmidt [23] to prove that $pre_{f^\flat}$ computes weakest preconditions for f within the logics for $\mathcal{C}_\Sigma$ and $\mathcal{C}^L_{\mathcal{C}_\Sigma}$. When $pre_{f^\flat}$'s image does not fall within $\mathcal{C}_\Sigma$ — see $pre_{sqrt^\flat}(Int)$ in Figure 7, for example — disjunctive completion of $\mathcal{C}_\Sigma$ to a topology again saves the day. The final moral, contained in Cousot and Cousot's use of topology in 1977 [8], is:

Every abstract domain defines a base for a topology on the corresponding concrete domain.

Acknowledgements: This paper was inspired by a presentation Mike Smyth gave in Edinburgh in December 1982; I thank Mike for his clear, intuitive papers and explanations. The trailblazing works of Radhia and Patrick Cousot and Roberto Giacobazzi and his colleagues are also greatly appreciated. I also thank the referees for their detailed comments and many helpful suggestions.

References

1. S. Abramsky. Domain theory in logical form. *Ann.Pure Appl.Logic*, 51:1–77, 1991.
2. N. Benton. Strictness logic and polymorphic invariance. In *Proc. Logical Found. Comp. Sci*, pages 33–44, 1992.
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.A. Peled. *Model Checking*. MIT Press, 2000.
5. R. Cleaveland, P. Iyer, and D. Yankelevich. Optimality in abstractions of model checking. In *Proc. SAS'95*, LNCS 983. Springer, 1995.
6. P. Cousot. Semantic foundations of program analysis. In S. Muchnick and N. Jones, editors, *Program Flow Analysis*, pages 303–342. Prentice Hall, 1981.
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. Static determination of dynamic properties of recursive procedures. In E.J. Neuhold, editor, *Formal Description of Programming Concepts*, pages 238–277. North-Holland, 1978.
9. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM Symp. POPL*, pages 269–282, 1979.
10. P. Cousot and R. Cousot. Higher-order abstract interpretation. In *Proceedings IEEE Int. Conf. Computer Lang.*, 1994.
11. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Prog. Lang. Systems*, 19:253–291, 1997.
12. P. Dybjer. Inverse image analysis generalises strictness analysis. *Information and Computation*, 90:194–216, 1991.
13. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples, and refinements in abstract model checking. In *Static Analysis Symposium*, LNCS 2126, pages 356–373. Springer Verlag, 2001.
14. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47:361–416, 2000.
15. C. Gunter and D.S. Scott. Semantic domains. In *Handbook of Theoretical Computer Science, Vol. B*, pages 633–674. MIT Press, 1991.
16. S. Hunt. Frontiers and open sets in abstract intepretation. In *Proc. ACM Symp. Functional Prog. and Comp. Architecture*, pages 194–216, 1989.
17. T. Jensen. *Abstract Interpretation in Logical Form*. PhD thesis, Imperial College, London, 1992.
18. P. Johnstone. *Stone Spaces*. Cambridge University Press, 1986.
19. J.C. Reynolds. Notes on a lattice-theoretic approach to the theory of computation. Technical report, Computer Science, Syracuse University, 1972.
20. M. Sagiv, T. Reps, and R. Wilhelm. Parametric shape analysis via 3-valued logic. *ACM TOPLAS*, 24:217–298, 2002.
21. D.A. Schmidt. Comparing completeness properties of static analyses and their logics. In *Proc. APLAS'06*, LNCS 4279, pages 183–199. Springer, 2006.
22. D.A. Schmidt. Underapproximating predicate transformers. In *Proc. SAS'06*, LNCS 4134, pages 127–143. Springer, 2006.
23. D.A. Schmidt. A calculus of logical relations for over- and underapproximating static analyses. *Science of Computer Programming*, 64:29–53, 2007.
24. M.B. Smyth. Effectively given domains. *Theoretical Comp. Sci.*, 5:257–274, 1977.
25. M.B. Smyth. Powerdomains and predicate transformers: a topological view. In *Proc. ICALP'83*, LNCS 154, pages 662–675. Springer, 1983.
26. S. Willard. *General Topology*. Dover Publications, 2004.