

Abstract Interpretation from a Topological Perspective

David A. Schmidt*

Kansas State University, Manhattan, Kansas, USA

Abstract. Topology is the study of property sets (open sets) and continuous functions on them. Despite its applicability to abstract interpretation, topology is little used, and this paper tries to rectify the situation: 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. 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 $f : \mathbb{R} \rightarrow \mathbb{R}$ 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 [14]: To solve the domain equation, $D = D \rightarrow D$, 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 $D \rightarrow D$ to the continuous functions, Scott limited its cardinality so that the recursive domain equation had a solution.

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

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

² That is, for every chain, $C = \{c_0, c_1, \dots, c_i, \dots\} \subseteq L$, 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 .

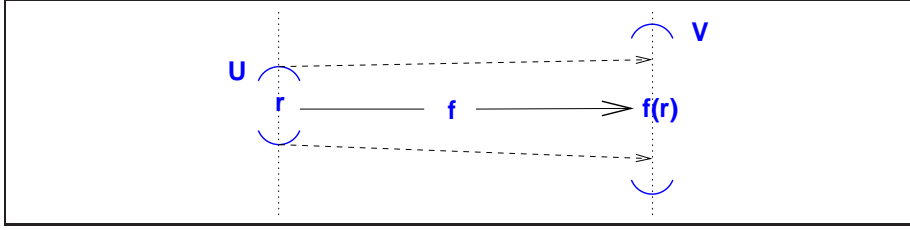


Fig. 1. Continuous function, f : When $f(r)$ falls within property (open set) V , then f maps some property, U , of r within V also.

Smyth [19] suggested that a domain’s Scott topology defines all the *computable properties* of the domain, and he established correspondences between “upper,” “lower,” and “convex” topologies to the three main variants of powerdomains [12].

Given that topology is the study of computing on properties, one would believe that it would be central to the theory of abstract interpretation [4], which studies exactly this topic. Aside from the Cousots’ use of upper closure operators to define abstract domains [6] and their statement of a Scott-like topology to define convergence [5] and Giacobazzi, et al.’s studies of *complete functions* on closure operators [11, 10], there is little to be found. Perhaps part of the problem is that topology is a study of functions’ behavior on open sets, and upper closure operators identify the topological dual, the *closed sets*.

In this paper, 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. Even more striking, Giacobazzi’s notion of forwards- and backwards-complete functions are characterized by the topologically closed and continuous maps. Finally, we build on Smyth’s topologies for powersets and show that his upper and lower topologies induce the overapproximating and underapproximating transition functions proposed by Cleaveland, et al. [2], and Dams, et al. [8], 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 [21] 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}_Σ , 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 $\bigcup S = U$). 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*, $\rho(S) = \bigcap\{K \mid S \subseteq K, K \in \mathcal{C}_\Sigma\}$.

As an example, consider the Scott-topology on an algebraic cpo: Recall that a cpo, D , is *algebraic* if there is a subset, $F_D \subseteq D$, of *finite elements*³ such that for every $d \in D$, $d = \sqcup\{e \in F_D \mid e \sqsubseteq d\}$ — the finite elements “generate” D , somewhat like the rational numbers generate the reals via Cauchy sequences [9]. (Consider $D = \mathcal{P}(Int)$; its finite elements are exactly the finite sets of integers, and \sqcup is \cup .)

We might let each finite $e \in F_D$ define the property of “having e -information level,” that is, for D , the Scott-basic open sets are $\mathcal{B}_D = \{\uparrow e \mid e \in F_D\}$.⁴ A Scott-basic-open set is like a half-open interval, $(q, \infty]$, $q \in \mathbb{Q}$, on the real line. Domain D ’s *Scott topology* is the closure of \mathcal{B}_D under unions. (For $\mathcal{P}(Int)$, finite element $S \subseteq_{finite} \mathcal{P}(Int)$ defines the Scott-basic open set, $\{T \subseteq Int \mid S \subseteq T\}$ — the property of having S -level information.)

Given topologies for sets Σ and Δ , there are standard definitions for the coarsest topologies for $\Sigma \times \Delta$, $\Sigma \rightarrow \Delta$, etc. [21].

A function, $f : \Sigma \rightarrow \Sigma$, 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 $f[U] = \{f(x) \mid x \in U\}$). 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, 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 $K \in \mathcal{C}_\Sigma$, $f[K] \in \mathcal{C}_\Sigma$.

Returning to the Scott topology on algebraic domains, we can prove that $f : D \rightarrow D$ is chain continuous iff it is continuous for the Scott-topology for D . Further, $f(d) = \sqcup\{f(e) \mid e \in F_D \text{ and } e \sqsubseteq d\}$, which asserts that f ’s behavior is completely determined by its behavior on D ’s basic-open sets.

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 $\gamma : A \rightarrow \mathcal{P}(\Sigma)$. 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 $\{none, neg, zero, pos, any\}$ — and contrast $\gamma[Sign]$ with the Scott-topology on (the discretely ordered set) Int , which is $\mathcal{P}(Int)$ (!)

We will study continuity with respect to the “open sets” $\gamma[Sign]$, and the notion we uncover will be fundamentally different than chain continuity.

³ $e \in D$ is *finite* iff for all chains $C \subseteq D$, $e \sqsubseteq \sqcup C$ implies $e \sqsubseteq c$ for some $c \in C$.

⁴ where $\uparrow e = \{d \in D \mid e \sqsubseteq d\}$ and $\uparrow S = \cup\{\uparrow e \mid e \in S\}$, for $S \subseteq D$.

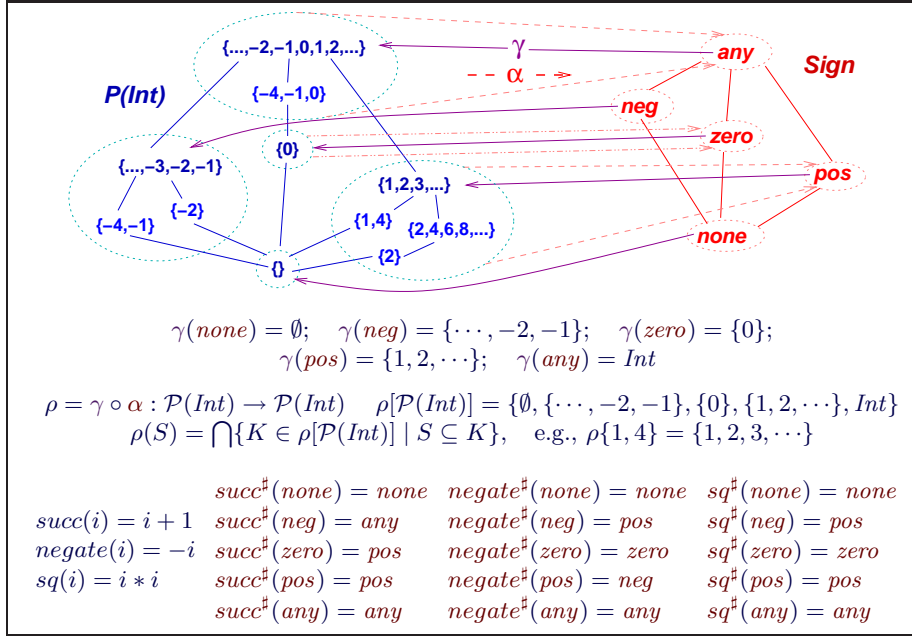


Fig. 2. Abstract domain, *Sign*, and the properties, $\rho[\mathcal{P}(\text{Int})]$, it represents

When γ possesses an adjoint, $\alpha : \mathcal{P}(\Sigma) \rightarrow \text{Sign}$, then there is a Galois connection⁵ and $\rho = \gamma \circ \alpha$ is an *upper closure operator* — $\rho : \mathcal{P}(\Sigma) \rightarrow \mathcal{P}(\Sigma)$ 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, $f : \Sigma \rightarrow \Sigma$, are *soundly approximated* by $f^\# : A \rightarrow A$ iff $\alpha(f[S]) \sqsubseteq f^\#(\alpha(S))$, for all $S \in \mathcal{P}(\Sigma)$ (equivalently, iff $f[\gamma(a)] \subseteq \gamma(f^\#(a))$, 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 $f^\#$ is defined $f_0^\# = \alpha \circ f \circ \gamma$, where again, f is “lifted.” When f is approximated exactly by $f_0^\#$ such that $f \circ \gamma = \gamma \circ f_0^\#$, 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 is, iff $f \circ \rho = \rho \circ f \circ \rho$ [10]. When f is approximated exactly such that $\alpha \circ f = f_0^\# \circ \alpha$, 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 $\rho \circ f = \rho \circ f \circ \rho$. [11, 16]. See Figure 3. In Figure 2, sq is backwards but not forwards complete; negate is both backwards and forwards complete, and succ is neither.

Later in the paper, we prove the equivalence of backwards and forwards completeness to topological continuity and closed maps.

⁵ that is, $S \subseteq \gamma(a)$ iff $\alpha(S) \sqsubseteq a$, for all $S \in \mathcal{P}(\Sigma)$ and $a \in A$

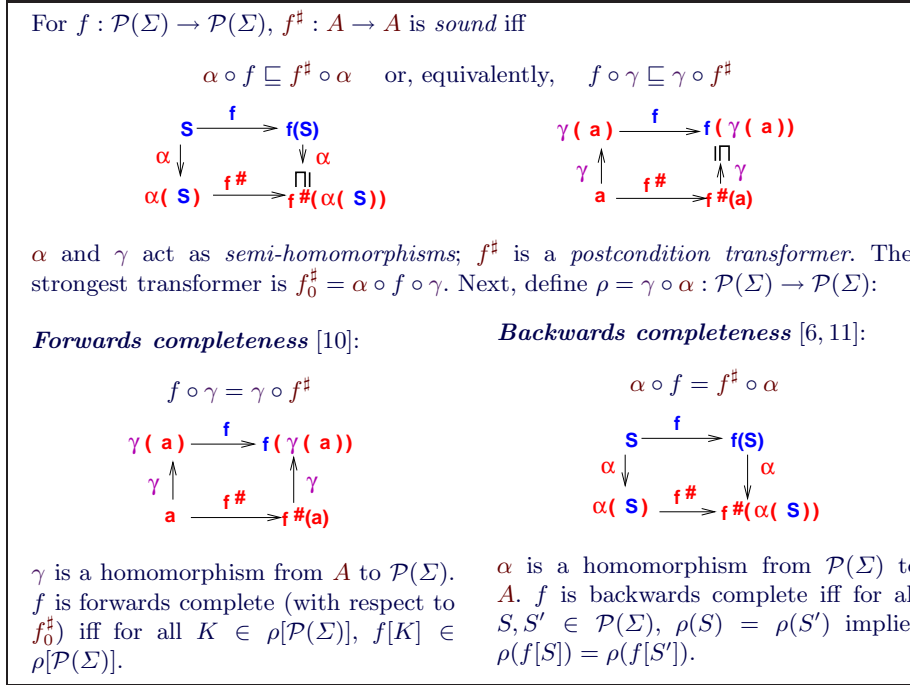


Fig. 3. Sound and complete forms of abstract functions

3 Property families, function preservation and reflection

We now develop abstract interpretation in terms of simplistic topology.

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}_Σ , 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}_Σ is an *open family*. If it is also closed under binary intersection and $\Sigma \in \mathcal{O}_\Sigma$, then it is a topology. Every open family has an *interior* operation, ι , which computes the largest property contained within a set: $\iota : \mathcal{P}(\Sigma) \rightarrow \mathcal{O}_\Sigma$ is defined $\iota(S) = \cup\{U \in \mathcal{O}_\Sigma \mid U \subseteq S\}$.

Dually, if a property family \mathcal{C}_Σ is closed under intersections, it is a *closed family* (*Moore family* [6]). Every closed family has a *closure* operation, ρ , which computes the smallest property covering a set: $\rho : \Sigma \rightarrow \mathcal{C}_\Sigma$ 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}_Σ 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 $f : \Sigma \rightarrow \Delta$ be a function; define $f : \mathcal{P}(\Sigma) \rightarrow \mathcal{P}(\Delta)$ as $f[S] = \{f(s) \mid s \in S\}$. Next, define function inverse, $f^{-1} : \mathcal{P}(\Delta) \rightarrow \mathcal{P}(\Sigma)$, as $f^{-1}(T) = \{s \in \Sigma \mid f(s) \in T\}$.

For property families, \mathcal{F}_Σ and \mathcal{F}_Δ , $f : \Sigma \rightarrow \Delta$ 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, $f : \mathcal{F}_\Sigma \rightarrow \mathcal{F}_\Delta$ is well defined. To reduce notation, we use functions, $f : \Sigma \rightarrow \Sigma$, with the same domain and codomain (and we say, “ f is \mathcal{F}_Σ -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. Let U_s (respectively, U_S) denote a member of \mathcal{F}_Σ such that $s \in U_s$ (resp., $S \subseteq U_S$).

(i) For $s \in \Sigma$, $f : \Sigma \rightarrow \Sigma$ 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}_Σ -reflecting iff for all $V \in \mathcal{F}_\Sigma$, $f^{-1}(V) \in \mathcal{F}_\Sigma$, that is, f^{-1} is \mathcal{F}_Σ -preserving.

Part (ii), a mild generalization of (i), is needed because \mathcal{F}_Σ might not be an open family. If \mathcal{F}_Σ is a topology, then (iii) asserts that f is topologically continuous. For all property families, \mathcal{F}_Σ , we retain this fundamental result:

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

Proof. We prove (i); (ii) is a standard result [21]. 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.

Only 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, $f[f^{-1}(V_S)] \subseteq V_S$. \square

The proofs in this paper rely on naive-set reasoning (cf. Willard [21]) and will often be omitted. We retain these critical dualities for all f and \mathcal{F}_Σ :

Proposition 3. $f : \Sigma \rightarrow \Sigma$ is $\sim\mathcal{F}_\Sigma$ -reflecting iff f is \mathcal{F}_Σ -reflecting.
 f is \mathcal{F}_Σ -preserving iff $f = \sim \circ f \circ \sim$ is $\sim\mathcal{F}_\Sigma$ -preserving.

In Figure 2, *negate* and *square* are Sign_{Int} -reflecting (but *succ* is not). This makes the two functions $\sim\text{Sign}_{Int}$ reflecting, where $\sim\text{Sign}_{Int} = \{Int, \{i \mid i \geq 0\}, \{i \mid i \neq 0\}, \{i \mid i \leq 0\}, \emptyset\}$. Since *negate* is Sign_{Int} -preserving, *negate* is $\sim\text{Sign}_{Int}$ -preserving, e.g., $\text{negate}\{i \mid i \geq 0\} = \{i \mid i \leq 0\}$. 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.,

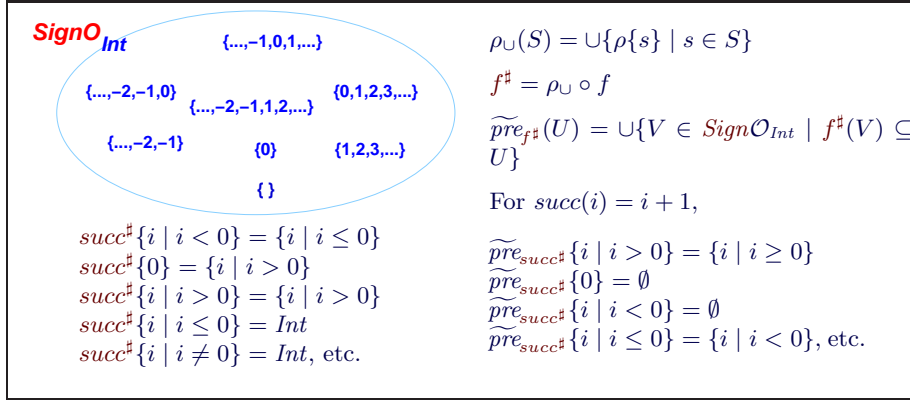


Fig. 4. Using $Sign_{Int} = \{\emptyset, \{i \mid i < 0\}, \{0\}, \{i \mid i > 0\}, Int\}$ as a base for a topology.

Figure 2 shows that $Sign = \{none, neg, zero, pos, any\}$ are the names for $Sign_{Int}$ and $\gamma : Sign \rightarrow Sign_{Int}$ 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 [3, 11]. For example, we write $succ^{\#}\{0\} = \{i \mid i > 0\}$ rather than $succ^{\#}(zero) = pos$.

Each property family \mathcal{F}_{Σ} possesses a “language” or “logic” whose “primitive propositions” are all the $U \in \mathcal{F}_{\Sigma}$ and whose “connectives” are those functions that are \mathcal{F}_{Σ} -preserving. Based on Figure 2, $Sign_{Int}$ ’s logic includes

$$\phi ::= U \mid \phi_1 \cap \phi_2 \mid \text{negate } \phi$$

where $U \in Sign_{Int}$, $\cap : \mathcal{P}(Int) \times \mathcal{P}(Int) \rightarrow \mathcal{P}(Int)$ is set intersection, and $\text{negate} : Int \rightarrow Int$ is $\text{negate}(i) = -i$. \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 $\text{negate}\{i \mid i < 0\}$.

When \mathcal{F}_{Σ} is a topology, its logic includes *false* (empty set) and *true* (Σ) and connectives for disjunction (union) and conjunction (intersection). If it contains negation (complementation), the topology forms a Boolean algebra.

A perfectly tailored abstract interpretation, $A \subseteq \mathcal{P}(\Sigma)$, makes a program’s transition functions, $f : \Sigma \rightarrow \Sigma$, A -preserving. This almost never happens. (E.g., a program that counts by ones uses the transition function, $succ : Int \rightarrow Int$, $succ(i) = i + 1$, which is not $Sign_{Int}$ -preserving. For this reason, we must approximate $succ$ by some $succ^{\#} : Sign_{Int} \rightarrow Sign_{Int}$.)

If a property family, \mathcal{C}_{Σ} , is closed, we use its closure operator, ρ , to define from $f : \Sigma \rightarrow \Sigma$ its overapproximation $f^{\#} : \mathcal{C}_{\Sigma} \rightarrow \mathcal{C}_{\Sigma}$ as $f^{\#} = \rho \circ f$. The approximation is *sound* because this relational assertion (“Hoare triple”),

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

holds true (where $\{\phi\}f\{\psi\}$ asserts $f[\phi] \subseteq \psi$, for $\phi, \psi \in \mathcal{C}_{\Sigma}$). Because $f^{\#}(\phi) = \rho(f(\phi))$ is the *smallest* set in \mathcal{C}_{Σ} that contains $f(\phi)$, it is the *strongest postcondi-*

tion of f and ϕ expressible in \mathcal{C}_Σ : $\{\phi\}f\{\psi\}$ implies $\{\phi\}f\{f^\#(\phi)\}$ and $f^\#(\phi) \subseteq \psi$, which we abbreviate to $\{\phi\}f\{f^\#(\phi) \subseteq \psi\}$.⁶

When $f^\#$ is forwards complete for f , we have completeness in the codomain: for $S \subseteq \mathcal{P}(\Sigma)$, $\{\phi\}f\{S\}$ implies $\{\phi\}f\{f^\#(\phi) \subseteq S\}$ (because $f \circ \rho = \rho \circ f \circ \rho$). When $f^\#$ is backwards complete, completeness extends to the domain: for $S \subseteq \mathcal{P}(\Sigma)$, $\{S\}f\{\psi\}$ implies $\{S\}f\{f^\#(\rho(S)) \subseteq \psi\}$ (because $\rho \circ f = \rho \circ f \circ \rho$).

For example, for $Sign_{Int}$, $succ^\# = \rho \circ succ$, so that $succ^\#\{0\} = \rho(succ\{0\}) = \rho\{1\} = \{i \mid i \geq 0\}$, etc. The moral is this:

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

To calculate preconditions, first define $f^\#$'s inverse, $f^\#_{\mathcal{C}_\Sigma}^- : \mathcal{C}_\Sigma \rightarrow \mathcal{P}(\mathcal{C}_\Sigma)$, as

$$(*) \quad f^\#_{\mathcal{C}_\Sigma}^-(U) = \{V \in \mathcal{C}_\Sigma \mid f^\#(V) \subseteq U\}$$

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

To repair the flaw, we close \mathcal{C}_Σ under unions, that is, we use it as a base for a topology⁷ 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 $\rho_\cup : \mathcal{CO}_\Sigma \rightarrow \mathcal{CO}_\Sigma$ equals $\rho_\cup(S) = \cup\{\rho\{s\} \mid s \in S\}$ by pointwise reasoning.) Now, we approximate with \mathcal{CO}_Σ : for $f : \Sigma \rightarrow \Sigma$, we define $f^\# : \mathcal{CO}_\Sigma \rightarrow \mathcal{CO}_\Sigma$ as $f^\# = \rho_\cup \circ f$; we define $f^\#_{\mathcal{CO}_\Sigma}^- : \mathcal{CO}_\Sigma \rightarrow \mathcal{P}(\mathcal{CO}_\Sigma)$ as $f^\#_{\mathcal{CO}_\Sigma}^-(U) = \{V \in \mathcal{CO}_\Sigma \mid f^\#(V) \subseteq U\}$, like before; and this makes $f^\#$'s weakest precondition, $\widetilde{pre}_{f^\#} : \mathcal{CO}_\Sigma \rightarrow \mathcal{CO}_\Sigma$, well defined: $\widetilde{pre}_{f^\#}(U) = \cup f^\#_{\mathcal{CO}_\Sigma}^-(U)$.⁸

In lattice theory, closure under unions is called *disjunctive completion* [7]. Figure 4 shows the disjunctive completion of $Sign_{Int}$ to $Sign\mathcal{O}_{Int}$ and the precondition function for $succ^\#$. Now, we can reason both forwards *and* backwards within the same property family, but the extra sets generated by the disjunctive completion may be *too many* for a practical static analysis.

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

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

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

⁶ If \mathcal{F}_Σ is not closed, then the $f : \Sigma \rightarrow \Sigma$ must be approximated by some $f^\# : \mathcal{F}_\Sigma \rightarrow \mathcal{F}_\Sigma$ such that $\{U\}f\{f^\#(U)\}$ holds for all $U \in \mathcal{F}_\Sigma$.

⁷ assuming every $c \in \Sigma$ belongs to some $V \in \mathcal{C}_\Sigma$

⁸ Since \mathcal{CO}_Σ possesses an interior operation, ι , we can define the precondition as merely $\iota \circ f^{-1}$, and one can prove that $\widetilde{pre}_{f^\#} = \iota \circ f^{-1}$ [17].

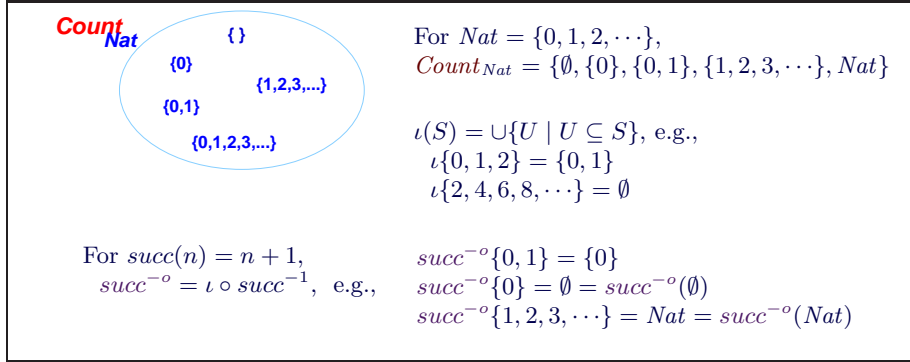


Fig. 5. Open family for counting analysis

holds true and $f^{-o}(\psi)$ is the *weakest precondition of f and ψ expressible in \mathcal{O}_Σ* : $\{\phi\}f\{\psi\}$ implies $\{\phi \subseteq f^{-o}(\psi)\}f\{\psi\}$. Further, we might define the two forms of completeness with respect to ι : $\{S\}f\{\psi\}$ implies $\{S \subseteq f^{-o}(\psi)\}f\{\psi\}$ (when $f^{-1} \circ \iota = \iota \circ f^{-1} \circ \iota$), and also $\{\phi\}f\{S\}$ implies $\{\phi \subseteq f^{-o}(\iota(S))\}f\{S\}$ (when $\iota \circ f^{-1} = \iota \circ f^{-1} \circ \iota$).

But we will see in the next section there is a topological principle underlying these completeness definitions.

Figure 5 defines an open (but not closed) family, $Count_{Nat}$, for a counting analysis. The successor operation, $succ : Nat \rightarrow Nat$, 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, $\{0\}succ; pred\{0\}$. (Adding $\{1\}$ to the family will help.) But the moral is:

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

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}_Σ is closed so that $\mathcal{O}_\Sigma = \sim\mathcal{C}_\Sigma$ is open. First, every \mathcal{C}_Σ -reflecting f is \mathcal{O}_Σ -reflecting, and for every \mathcal{C}_Σ -preserving $f : \Sigma \rightarrow \Sigma$, f is \mathcal{O}_Σ -preserving, by Proposition 3. (So, if \mathcal{C}_Σ is a topology, its binary conjunction and disjunction operations are preserved in \mathcal{O}_Σ 's logic as disjunction and conjunction, respectively.) We have

Lemma 4. For all $f : \Sigma \rightarrow \Sigma$ and $S \subseteq \Sigma$, $\sim f^{-1}(S) = f^{-1}(\sim S)$.

For closed family \mathcal{C}_Σ and $\mathcal{O}_\Sigma = \sim\mathcal{C}_\Sigma$, $\sim \circ \rho = \iota \circ \sim$.

These results yield

Proposition 5. For all $S \subseteq \Sigma$, $\widetilde{f^{-1}}(S) = f^{-1}(S)$.

If f is onto, then $\widetilde{f}(U) \subseteq f(U)$, for all $U \in \mathcal{O}_\Sigma$.

$(f^{-1})^\#(U) = f^{-o}(U)$, for all $U \in \mathcal{O}_\Sigma$. (Note: $(f^{-1})^\# = \sim \circ (f^{-1})^\# \circ \sim$.)

Proof. We prove the last 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 $f^{-o}(U)$. \square

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

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

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

Because *succ* is not *Sign_{Int}*-reflecting, we underapproximate it by $\text{succ}^{-o} = (\widetilde{\text{succ}^{-1}})^\sharp$. We have $\text{succ}^{-o}\{i \mid i \neq 0\} = \{i \mid i \geq 0\}$; $\text{succ}^{-o}Int = Int$; and $\text{succ}^{-o}(U) = \emptyset$, otherwise. This loss of precision can be alleviated somewhat by a disjunctive completion of *Sign_{Int}*.

In this fashion, a postcondition analysis based on \mathcal{C}_Σ defines a precondition analysis on $\sim \mathcal{C}_\Sigma$.

Finally, every \mathcal{F}_Σ possesses both a logic for validation (viz., \mathcal{F}_Σ '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 [15], where one uses a single abstract domain to compute validation, refutation, and “don't know” judgements.

5 From continuity to completeness

As hinted earlier, there is a correspondence between functions that preserve and reflect the property sets of their domain/codomain and abstract-interpretation-complete functions.

Recall that $f : \Sigma \rightarrow \Sigma$ is \mathcal{F}_Σ -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}_Σ is a closed family, that is, when $\rho[\mathcal{P}(\Sigma)] = \mathcal{F}_\Sigma$. In topological terms, f is a closed map.

We now prove that \mathcal{F}_Σ -reflection is exactly backwards completeness when \mathcal{F}_Σ 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}_Σ , $f : \Sigma \rightarrow \Sigma$ 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}_Σ -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 $f[S'] \subseteq K$. \square

The converse of the above might not hold, but say that \mathcal{C}_Σ is a closed family and $\rho(S) = \bigcap \{K \in \mathcal{C}_\Sigma \mid S \subseteq K\}$; 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}_Σ :*

- (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}_Σ , $f : \Sigma \rightarrow \Sigma$ is $B_{\mathcal{C}_\Sigma}$ -complete iff f is \mathcal{C}_Σ -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. \square

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

(ii) *f is forwards complete for \mathcal{C}_Σ 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) can be applied to open families as well and neatly summarizes the previous developments of sound and complete abstract transformers.

6 Relation to partial-order backwards completeness

The crucial characterization of backwards completeness by Giacobazzi, et al. [11] is made in a “frame-theory” presentation [13], where $(\mathcal{P}(\Sigma), \sqsubseteq)$ is abstracted to a complete lattice, (D, \sqsubseteq) , and \mathcal{C}_Σ is abstracted to $\rho[D] \subseteq D$, namely, the fixed points of upper closure map, $\rho : D \rightarrow D$. We can rephrase their work in terms of our development:

First, define $f^- : D \rightarrow \mathcal{P}(D)$ 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 $f : D \rightarrow D$ 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 $e \in \rho[D]$, $\max(f^-(d)) \subseteq \rho[D]$. 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. [11] in the “frame theory”:

$f : D \rightarrow D$ is backwards- ρ -complete iff it is ρ -reflecting.

7 Nondeterminism and semicontinuity

A nondeterministic transition function has arity, $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$. The property family (topology) for $\mathcal{P}(\Sigma)$ must be different from Σ 's, and it depends on how we define f 's preimage, a map, $\mathcal{P}(\Sigma) \rightarrow \mathcal{P}(\Sigma)$. We have two choices: for $S \subseteq \Sigma$,

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

The following definitions are due to Vietoris [20]:

Definition 12. For property family, $\mathcal{F}_\Sigma \subseteq \Sigma$,

$f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ is lower semicontinuous for \mathcal{F}_Σ iff pre_f is \mathcal{F}_Σ -preserving.
 $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ is upper semicontinuous for \mathcal{F}_Σ iff \widetilde{pre}_f is \mathcal{F}_Σ -preserving.

Say we want pre_f in the logic for \mathcal{F}_Σ ; what property family for $\mathcal{P}(\Sigma)$ is appropriate? The answer was found by Smyth [20]: define $\mathcal{O}_{\mathcal{F}_\Sigma}^L \subseteq \mathcal{P}(\mathcal{P}(\Sigma))$ to be the open family generated by taking all unions of the base, $\mathcal{B}_{\mathcal{F}_\Sigma}^L = \{\exists U \mid U \in \mathcal{F}_\Sigma\}$, 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 $U \in \mathcal{F}_\Sigma$, $f^{-1}(\exists U) = pre_f(U)$. $\mathcal{O}_{\mathcal{F}_\Sigma}^L$ is called the *lower topology based on \mathcal{F}_Σ* . This result is due to Smyth [20]:

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

That is, pre_f lies in the logic for \mathcal{O}_Σ iff f is $\mathcal{O}_\Sigma \mathcal{O}_{\mathcal{O}_\Sigma}^L$ -reflecting.

When $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ is not lower semicontinuous, we simply use \mathcal{O}_Σ 's interior operator, ι , to approximate pre_f by $\iota \circ pre_f : \mathcal{O}_\Sigma \rightarrow \mathcal{O}_\Sigma$, like in Section 4.

But most static analyses are stated in terms of closed families. We can rephrase the previous Proposition in terms of its dual, a closed family, and discover a well-travelled path:

For open family, \mathcal{O}_Σ , and $\mathcal{C}_\Sigma = \sim \mathcal{O}_\Sigma$, we can readily calculate that $\sim \mathcal{O}_{\mathcal{O}_\Sigma}^L$ is a closed family whose members are all the intersections of sets taken from the (co)base, $\mathcal{B}_{\mathcal{C}_\Sigma}^U = \{\forall K \mid K \in \mathcal{C}_\Sigma\}$, 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: $\mathcal{C}_{\mathcal{C}_\Sigma}^U = \sim \mathcal{O}_{\mathcal{O}_\Sigma}^L$.

Corollary 14. Let \mathcal{C}_Σ be a closed family and define $\mathcal{O}_\Sigma = \sim \mathcal{C}_\Sigma$.

pre_f is \mathcal{O}_Σ -preserving iff \widetilde{pre}_f is \mathcal{C}_Σ -preserving.

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

Hence, \widetilde{pre}_f is \mathcal{C}_Σ -preserving iff f is $\mathcal{C}_\Sigma \mathcal{C}_{\mathcal{C}_\Sigma}^U$ -reflecting iff f is upper semicontinuous for \mathcal{C}_Σ .

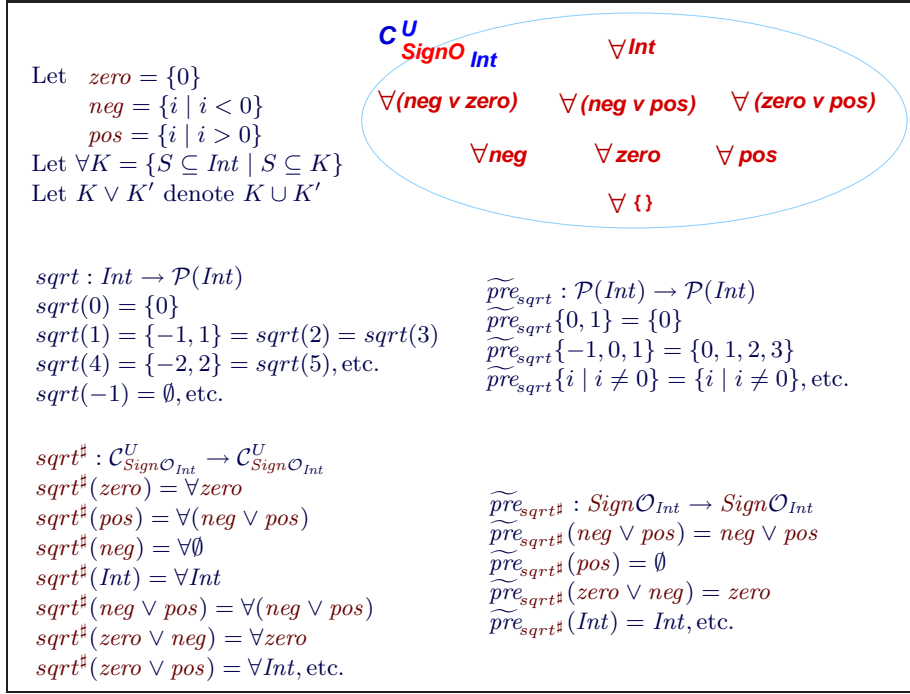


Fig. 6. $sqrt$, upper topology on $SignO_{Int}$, and $sqrt^\#$

Proof. By Propositions 13 and 3. \square

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

To do this, we need some insight: First, each $M \in \mathcal{C}_{\mathcal{C}_\Sigma}^U$ 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 “ $\forall K_1 \wedge \forall K_2 \wedge \dots \wedge \forall K_i \wedge \dots$ ” — 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 $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$, we express its relational assertions in the form,

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

By pointwise reasoning, the M defined above equals $\forall \bigcap \{K_i \mid K_i \in \mathcal{C}_\Sigma\}$, read as “ $\forall(K_1 \wedge K_2 \wedge \dots \wedge K_i \wedge \dots)$.” 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 $\phi, \psi \in \mathcal{C}_\Sigma$. (If you prefer, you can write “ $\phi \models [f]\psi$.”) The quantifier reminds us that f 's answer is a *set* of Σ -values, covered by property ψ . And, $\phi \subseteq \widetilde{pre}_f(\psi) = f^{-1}(\forall\psi)$.

Say we approximate $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ by $f^\#(K) = \rho_U(f[K])$, where ρ_U is the closure operation for \mathcal{C}_Σ^U : $\rho_U(T) = \bigcap \{\forall K \mid T \subseteq \forall K, K \in \mathcal{C}_\Sigma\}$. That is, $\rho_U(T)$ computes the conjunction of all properties K that cover all the sets in T . We have, as usual, that $\{\phi\}f\{f^\#(\phi)\}$. Next, the approximation of \widetilde{pre}_f must be made sound: $\widetilde{pre}_{f^\#}(K) \subseteq \widetilde{pre}_f(K) = f^{-1}(\forall K)$, for all $K \in \mathcal{C}_\Sigma$. We work from Equation (\star) in Section 4; $f^\#$'s inverse image is

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

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

Figure 6 displays an integer square-root function, $sqr : Int \rightarrow \mathcal{P}(Int)$. The disjunctive completion of $Sign_{Int}$ produces the topology, $Sign\mathcal{O}_{Int}$, in Figure 4, from which we generate $\mathcal{C}_{Sign\mathcal{O}_{Int}}^U$, illustrated in Figure 6. This is the form of abstract domain typically used for ACTL-style “abstract model checking.” [1].

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

When Σ 's family is closed under unions, we can exploit this result:

Proposition 15. [20] *Let $\mathcal{O}_\Sigma \subseteq \Sigma$ be an open family. $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ is upper semicontinuous for \mathcal{O}_Σ iff f is $\mathcal{O}_\Sigma \mathcal{O}_\Sigma^U$ -reflecting.*

When f is not upper semicontinuous, we may use $\iota \circ \widetilde{pre}_f : \mathcal{O}_\Sigma \rightarrow \mathcal{O}_\Sigma$, where ι is \mathcal{O}_Σ 's interior operator.

The dual goes as follows: $\mathcal{C}_{\mathcal{C}_\Sigma}^L = \sim \mathcal{O}_{\mathcal{C}_\Sigma}^U$, whose members are all intersections of sets from the (co)base, $\mathcal{B}_{\mathcal{C}_\Sigma}^L = \{\exists K \mid K \in \mathcal{C}_\Sigma\}$, 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}_Σ -preserving iff pre_f is \mathcal{C}_Σ -preserving.*

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

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

Say that $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ is not lower semicontinuous. When we approximate it by $f^b : \mathcal{C}_\Sigma \rightarrow \mathcal{C}_{\mathcal{C}_\Sigma}^L$, what is the result? What is pre_{f^b} ? The answers that follow summarize significant research on underapproximation of transition functions [2, 8, 18].

Each $M \in \mathcal{C}_{\mathcal{C}_\Sigma}^L$ 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 “ $\exists K_1 \wedge \exists K_2 \wedge \dots \wedge \exists K_i \wedge \dots$ ” — each of M 's members is a set that meets (*witnesses*) K_1 and K_2 and ... K_i and so on. For $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$, we express its relational assertions in the form,

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

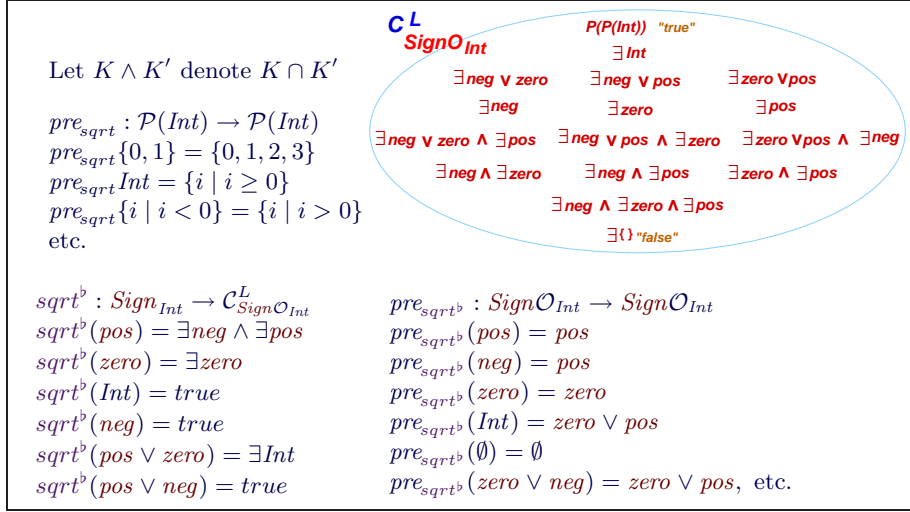


Fig. 7. Lower topology on $SignO_{Int}$ and $sqrt^b$

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 $f : \Sigma \rightarrow \mathcal{P}(\Sigma)$ by $f^b(K) = \rho_L(f[K])$, where ρ_L is the closure operation for $\mathcal{C}_{\mathcal{C}_\Sigma}^L$: $\rho_L(T) = \bigcap \{\exists K \mid T \subseteq \exists K, K \in \mathcal{C}_\Sigma\}$. That is, $\rho_L(T)$ collects all the properties, K , that are witnessed (met) by each of the sets in T . We have $\{\phi\}f\{f^b(\phi)\}$, and $f^b(\phi)$ is the strongest postcondition in the logic associated with $\mathcal{C}_{\mathcal{C}_\Sigma}^L$, the “language of witnesses.” Once again, we define $f^b_{\mathcal{C}_\Sigma}(K) = \{K' \in \mathcal{C}_\Sigma \mid f^b(K') \subseteq \exists K\}$ and $pre_{f^b}(K) = \bigcup f^b_{\mathcal{C}_\Sigma}(K)$. This is the definition used by Cleaveland [2], Dams [8], and Schmidt [18] to prove that pre_{f^b} computes weakest preconditions for f within the logics for \mathcal{C}_Σ and $\mathcal{C}_{\mathcal{C}_\Sigma}^L$. When pre_{f^b} ’s image does not fall within \mathcal{C}_Σ — see $pre_{sqrt^b}(Int)$ in Figure 7, for example — disjunctive completion of \mathcal{C}_Σ to a topology again saves the day. The moral is:

Although described as closed families, abstract domains are often topologies.

Figure 7 shows $\mathcal{C}_{SignO_{Int}}^L$ and the corresponding definitions of $sqrt^b$ and pre_{sqrt^b} that would be used for abstract ECTL (“liveness”) model checking.

8 Conclusion

We have applied topological concepts to reach quickly deep results from abstract interpretation theory. Topological concepts also guide us to proper formulation of forwards and backwards analyses and give proper abstractions of nondeterministic transition functions.

This paper has just scratched the surface of what topology can do. Applications of product, quotient, and weak topologies to abstract domains deserve

investigation, as do notions like convergence, clustering, covering, and compactness. Many hints are waiting in Smyth's paper [20].

Acknowledgements: This paper was inspired by a presentation Mike Smyth gave in Edinburgh in December 1982. I thank Mike for his many inspiring papers and explanations. The trailblazing works of Radhia and Patrick Cousot and Roberto Giacobazzi and his colleagues are also greatly appreciated.

References

1. E.M. Clarke, O. Grumberg, and D.A. Peled. *Model Checking*. MIT Press, 2000.
2. R. Cleaveland, P. Iyer, and D. Yankelevich. Optimality in abstractions of model checking. In *Proc. SAS'95*, LNCS 983. Springer, 1995.
3. P. Cousot. Semantic foundations of program analysis. In S. Muchnick and N. Jones, editors, *Program Flow Analysis*, pages 303–342. Prentice Hall, 1981.
4. 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.
5. 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.
6. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM Symp. POPL*, pages 269–282, 1979.
7. P. Cousot and R. Cousot. Higher-order abstract interpretation. In *Proceedings IEEE Int. Conf. Computer Lang.*, 1994.
8. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Prog. Lang. Systems*, 19:253–291, 1997.
9. M. Dummett. *Intuitionism*. Oxford University Press, 1977.
10. 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.
11. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47:361–416, 2000.
12. C. Gunter and D.S. Scott. Semantic domains. In *Handbook of Theoretical Computer Science, Vol. B*, pages 633–674. MIT Press, 1991.
13. P. Johnstone. *Stone Spaces*. Cambridge University Press, 1986.
14. J.C. Reynolds. Notes on a lattice-theoretic approach to the theory of computation. Technical report, Computer Science, Syracuse University, 1972.
15. M. Sagiv, T. Reps, and R. Wilhelm. Parametric shape analysis via 3-valued logic. *ACM TOPLAS*, 24:217–298, 2002.
16. D.A. Schmidt. Comparing completeness properties of static analyses and their logics. In *Proc. APLAS'06*, LNCS 4279, pages 183–199. Springer, 2006.
17. D.A. Schmidt. Underapproximating predicate transformers. In *Proc. SAS'06*, LNCS 4134, pages 127–143. Springer, 2006.
18. D.A. Schmidt. A calculus of logical relations for over- and underapproximating static analyses. *Science of Computer Programming*, 64:29–53, 2007.
19. M.B. Smyth. Effectively given domains. *Theoretical Comp. Sci.*, 5:257–274, 1977.
20. M.B. Smyth. Powerdomains and predicate transformers: a topological view. In *Proc. ICALP'83*, LNCS 154, pages 662–675. Springer, 1983.
21. S. Willard. *General Topology*. Dover Publications, 2004.