

# Galois Transformers and Modular Abstract Interpreters

## Reusable Metatheory for Program Analysis

David Darais

University of Maryland, USA  
darais@cs.umd.edu

Matthew Might

University of Utah, USA  
might@cs.utah.edu

David Van Horn

University of Maryland, USA  
dvanhorn@cs.umd.edu

### Abstract

The design and implementation of static analyzers has become increasingly systematic. Yet for a given language or analysis feature, it often requires tedious and error prone work to implement an analyzer and prove it sound. In short, static analysis features and their proofs of soundness do not compose well, causing a dearth of reuse in both implementation and metatheory.

We solve the problem of systematically constructing static analyzers by introducing *Galois transformers*: monad transformers that transport Galois connection properties. In concert with a monadic interpreter, we define a library of monad transformers that implement building blocks for classic analysis parameters like context, path, and heap (in)sensitivity. Moreover, these can be composed together *independent of the language being analyzed*.

Significantly, a Galois transformer can be proved sound once and for all, making it a reusable analysis component. As new analysis features and abstractions are developed and mixed in, soundness proofs need not be reconstructed, as the composition of a monad transformer stack is sound by virtue of its constituents. Galois transformers provide a viable foundation for reusable and composable metatheory for program analysis.

Finally, these Galois transformers shift the level of abstraction in analysis design and implementation to a level where non-specialists have the ability to synthesize sound analyzers over a number of parameters.

**Categories and Subject Descriptors** F.3.2 [*Semantics of Programming Languages*]: Program analysis

**Keywords** abstract interpretation, monads, Galois connections, program analysis

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

OOPSLA '15, October 25–30, 2015, Pittsburgh, PA, USA.

Copyright is held by the owner/author(s). Publication rights licensed to ACM.

ACM 978-1-4503-3689-5/15/10...\$15.00.

<http://dx.doi.org/10.1145/2814270.2814308>

### 1. Introduction

Traditional practice in program analysis via abstract interpretation is to fix a language (as a concrete semantics) and an abstraction (as an abstraction map, concretization map or Galois connection) before constructing a static analyzer that is sound with respect to both the abstraction and the concrete semantics. Thus, each pairing of abstraction and semantics requires a one-off manual derivation of the static analyzer and construction of its proof of soundness.

Work has focused on endowing abstractions with knobs, levers, and dials to tune precision and compute efficiently. These parameters come with overloaded meanings such as object, context, path and heap sensitivities, or some combination thereof. These efforts develop families of analyses *for a specific language* and prove the framework sound.

But this framework approach suffers from many of the same drawbacks as the one-off analyzers. They are language-specific, preventing reuse of concepts across languages, and require similar re-implementations and soundness proofs. This process is still manual, tedious, difficult and error-prone. And, changes to the structure of the parameter-space require a completely new proof of soundness. And, it prevents fruitful insights and results developed in one paradigm from being applied to others, e.g., functional to object-oriented and *vice versa*.

We propose an automated alternative to structuring and implementing program analysis. Inspired by Liang, Hudak, and Jones's *Monad Transformers and Modular Interpreters* [12], we propose to start with concrete interpreters written in a specific monadic style. Changing the monad will transform the concrete interpreter into an abstract interpreter. As we show, classical program abstractions can be embodied as language-independent monads. Moreover, these abstractions can be written as monad *transformers*, thereby allowing their composition to achieve new forms of analysis. We show that these monad transformers obey the properties of *Galois connections* [5] and introduce the concept of a *Galois transformer*, a monad transformer which transports Galois connection properties.

Most significantly, Galois transformers are proven sound once and for all. Abstract interpreters, which take the form

of monad transformer stacks coupled with a monadic interpreter, inherit the soundness properties of each element in the stack. This approach enables reuse of abstractions across languages and lays the foundation for a modular metatheory of program analysis.

**Setup** We describe a simple programming language and a garbage-collecting allocating semantics as the starting point of analysis design (Section 2). We then briefly discuss three types of path and flow sensitivity and their corresponding variations in analysis precision (Section 3).

**Monadic Abstract Interpreters** We develop an abstract interpreter for our example language as a monadic function with parameters (Sections 4 and 5), one of which is a monadic effect interface combining state and nondeterminism effects (Section 4.1). These monadic effects—state and nondeterminism—encode arbitrary relational small-step state-machine semantics and correspond to state-machine components and relational nondeterminism, respectively.

Interpreters written in this style are reasoned about using various laws, including monadic effect laws, and are verified correct independent of any particular choice of parameters. Likewise, choices for these parameters are proven correct in isolation from their instantiation. When instantiated, our generic interpreter recovers the concrete semantics and a family of abstract interpreters with variations in abstract domain, abstract garbage collection, call-site sensitivity, object sensitivity, and path and flow sensitivity (Section 6). Furthermore, each derived abstract interpreter is proven correct by construction through a reusable, semantics independent proof framework (Section 8).

**Isolating Path and Flow Sensitivity** We give specific monads for instantiating the interpreter from Section 5 to path-sensitive, flow-sensitive and flow-insensitive analyses (Section 7). This leads to an isolated understanding of path and flow sensitivity as mere variations in the monad used for execution. Furthermore, these monads are language independent, allowing one to reuse the same path and flow sensitivity machinery for any language of interest, and compose seamlessly with other analysis parameters.

**Galois Transformers** To ease the construction of monads for building abstract interpreters and their proofs of correctness, we develop a framework of Galois transformers (Section 8). Galois transformers are an extension of monad transformers which transport Galois connection properties (Section 8.4). The Galois transformer framework allows us to both execute and justify the correctness of an abstract interpreter piecewise for each transformer. Galois transformers are language independent and they are proven correct once and for all in isolation from a particular semantics.

**Implementation** We implement our technique as a Haskell library and example client analysis (Section 9). Developers are able to reuse our language-independent framework for

$$\begin{aligned}
i &\in \mathbb{Z} & x &\in \text{Var} \\
a \in \text{Atom} & ::= i \mid x \mid \lambda(x).e \\
\oplus \in \text{IOp} & ::= + \mid - \\
\odot \in \text{Op} & ::= \oplus \mid @ \\
e \in \text{Exp} & ::= a \mid e \odot e \mid \text{ifo}(e)\{e\}\{e\} \\
\\
\tau \in \text{Time} & ::= \mathbb{Z} \\
l \in \text{Addr} & ::= \text{Var} \times \text{Time} \\
\rho \in \text{Env} & ::= \text{Var} \rightarrow \text{Addr} \\
\sigma \in \text{Store} & ::= \text{Addr} \rightarrow \text{Val} \\
c \in \text{Clo} & ::= \langle \lambda(x).e, \rho \rangle \\
v \in \text{Val} & ::= i \mid c \\
\kappa l \in \text{KAddr} & ::= \text{Time} \\
\kappa \sigma \in \text{KStore} & ::= \text{KAddr} \rightarrow \text{Frame} \times \text{KAddr} \\
fr \in \text{Frame} & ::= \langle \square \odot e, \rho \rangle \mid \langle v \odot \square \rangle \mid \langle \text{ifo}(\square)\{e\}\{e\}, \rho \rangle \\
\varsigma \in \Sigma & ::= \langle e, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle
\end{aligned}$$

**Figure 1.**  $\lambda$ IF Syntax and Concrete State Space

prototyping the design space of analysis features for their language of choice. Our implementation is publicly available on Hackage<sup>1</sup>, Haskell’s package manager.

**Contributions** We make the following contributions:

- A methodology for constructing monadic abstract interpreters based on *monadic effects*.
- A compositional, language-independent framework for constructing monads with varying analysis properties based on *monad transformers*.
- A compositional, language-independent proof framework for constructing Galois connections and end-to-end correctness proofs based on *Galois transformers*, an extension of monad transformers which transports Galois connection properties.
- Two new general purpose monad transformers for non-determinism which are not present in any previous work on monad transformers (even outside static analysis literature). Although applicable to settings other than static analysis, these two transformers give rise naturally to variations in path and flow sensitivity when applied to abstract interpreters.
- An isolated understanding of path and flow sensitivity in analysis as properties of the interpreter monad, which we develop independently of other analysis features.

Collectively, these contributions make progress toward a reusable metatheory for program analysis.

<sup>1</sup> <http://hackage.haskell.org/package/maam>

$$\begin{aligned}
A[\_ ] &: Atom \rightarrow (Env \times Store \rightarrow Val) \\
A[i] &(\rho, \sigma) := i \\
A[x] &(\rho, \sigma) := \sigma(\rho(x)) \\
A[\underline{\lambda}(x).e] &(\rho, \sigma) := \langle \underline{\lambda}(x).e, \rho \rangle \\
\delta[\_ ] &: IOp \rightarrow (\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}) \\
\delta[+] &(i_1, i_2) := i_1 + i_2 \\
\delta[-] &(i_1, i_2) := i_1 - i_2 \\
\\
\_ \rightsquigarrow \_ &: \mathcal{P}(\Sigma \times \Sigma) \\
\langle e_1 \odot e_2, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle e_1, \rho, \sigma, \tau, \kappa \sigma', \tau + 1 \rangle \text{ where} \\
&\kappa \sigma' := \kappa \sigma[\tau \mapsto \langle \langle \square \odot e_2, \rho \rangle, \kappa l \rangle] \\
\langle \mathbf{if0}(e_1)\{e_2\}\{e_3\}, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle e_1, \rho, \sigma, \tau, \kappa \sigma', \tau + 1 \rangle \text{ where} \\
&\kappa \sigma' := \kappa \sigma[\tau \mapsto \langle \langle \mathbf{if0}(\square)\{e_2\}\{e_3\}, \rho \rangle, \kappa l \rangle] \\
\langle a, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle e, \rho', \sigma, \tau, \kappa \sigma', \tau + 1 \rangle \text{ where} \\
&\langle \langle \square \odot e, \rho' \rangle, \kappa l' \rangle := \kappa \sigma(\kappa l) \\
&\kappa \sigma' := \kappa \sigma[\tau \mapsto \langle \langle A[a](\rho, \sigma) \odot \square \rangle, \kappa l' \rangle] \\
\langle a, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle e, \rho'', \sigma', \kappa l', \kappa \sigma, \tau + 1 \rangle \text{ where} \\
&\langle \langle \underline{\lambda}(x).e, \rho' \rangle @ \square, \kappa l' \rangle := \kappa \sigma(\kappa l) \\
&\rho'' := \rho'[x \mapsto \langle x, \tau \rangle] \\
&\sigma' := \sigma[\langle x, \tau \rangle \mapsto A[a](\rho, \sigma)] \\
\langle i_2, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle i, \rho, \sigma, \kappa l', \kappa \sigma, \tau + 1 \rangle \text{ where} \\
&\langle \langle i_1 \oplus \square, \kappa l' \rangle := \kappa \sigma(\kappa l) \\
&i := \delta[\oplus](i_1, i_2) \\
\langle i, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow \langle e, \rho', \sigma, \kappa l', \kappa \sigma, \tau + 1 \rangle \text{ where} \\
&\langle \langle \mathbf{if0}(\square)\{e_1\}\{e_2\}, \rho' \rangle, \kappa l' \rangle := \kappa \sigma(\kappa l) \\
e &:= e_1 \text{ when } i = 0; e_2 \text{ when } i \neq 0
\end{aligned}$$

**Figure 2.** Concrete Semantics

## 2. Semantics

To demonstrate our framework we design an abstract interpreter for  $\lambda\mathbf{IF}$ , a simple applied lambda calculus shown in Figure 1.  $\lambda\mathbf{IF}$  extends traditional lambda calculus with integers, addition, subtraction and conditionals. We write @ as explicit abstract syntax for function application. The state-space  $\Sigma$  for  $\lambda\mathbf{IF}$  makes allocation explicit using two separate stores for values (*Store*) and for the stack (*KStore*).

Guided by the syntax and semantics of  $\lambda\mathbf{IF}$  we develop interpretation parameters in Section 4, a monadic interpreter in Section 5, and both concrete and abstract instantiations for the interpretation parameters in Section 6. The variations in path and flow sensitivity developed in sections 7 and 8 are independent of this (or any other) semantics.

$$\begin{aligned}
\_ \rightsquigarrow^{gc} \_ &: \mathcal{P}(\Sigma \times \Sigma) \\
\varsigma &\rightsquigarrow^{gc} \varsigma' \text{ where } \varsigma \rightsquigarrow \varsigma' \\
\langle e, \rho, \sigma, \kappa l, \kappa \sigma, \tau \rangle &\rightsquigarrow^{gc} \langle e, \rho, \sigma', \kappa l, \kappa \sigma', \tau \rangle \text{ where} \\
&\kappa \sigma' := \{ \kappa l \mapsto \kappa \sigma(\kappa l) \mid \kappa l \in KR(\kappa l, \kappa \sigma) \} \\
&\sigma' := \{ l \mapsto \sigma(l) \mid l \in R(e, \rho, \sigma, \kappa l, \kappa \sigma) \} \\
\\
KR &: KAddr \times KStore \rightarrow \mathcal{P}(KAddr) \\
KR(\kappa l, \kappa \sigma) &:= \mu(X). \\
&X \cup \{ \kappa l \} \cup \{ \pi_2(\kappa \sigma(\kappa l)) \mid \kappa l \in X \} \\
R &: Exp \times Env \times Store \times KAddr \times KStore \rightarrow \mathcal{P}(Addr) \\
R(e, \rho, \sigma, \kappa l, \kappa \sigma) &:= \mu(X). \\
&X \cup \{ \rho(x) \mid x \in FV(e) \} \\
&\cup \{ l \mid l \in R\text{-Frm}(\pi_1(\kappa \sigma(\kappa l))) \}; \kappa l \in KR(\kappa l, \kappa \sigma) \\
&\cup \{ l' \mid l' \in R\text{-Val}(\sigma(l)) \}; l \in X \\
\\
R\text{-Frm} &: Frame \rightarrow \mathcal{P}(Addr) \\
R\text{-Frm}(\langle \square \odot e, \rho \rangle) &:= \{ \rho(x) \mid x \in FV(e) \} \\
R\text{-Frm}(\langle v \odot \square \rangle) &:= R\text{-Val}(v) \\
R\text{-Frm}(\langle \mathbf{if0}(\square)\{e_2\}\{e_3\}, \rho \rangle) &:= \{ \rho(x) \mid x \in FV(e_1) \cup FV(e_2) \} \\
R\text{-Val} \in Val &\rightarrow \mathcal{P}(Addr) \\
R\text{-Val}(i) &:= \{ \} \\
R\text{-Val}(\langle \underline{\lambda}(x).e, \rho \rangle) &:= \{ \rho(y) \mid y \in FV(\underline{\lambda}(x).e) \} \\
\\
collect &: \mathcal{P}(\Sigma) \\
collect &:= \mu(X). X \cup \{ \varsigma_0 \} \cup \{ \varsigma' \mid \varsigma \rightsquigarrow^{gc} \varsigma'; \varsigma \in X \} \text{ where} \\
\varsigma_0 &:= \langle e_0, \perp, \perp, 0, \perp, 1 \rangle
\end{aligned}$$

**Figure 3.** Garbage Collected Collecting Semantics

We define semantics for atomic expressions and primitive operators denotationally with  $A[\_ ]$  and  $\delta[\_ ]$ , and to compound expressions relationally with  $\_ \rightsquigarrow \_$ , shown in Figure 2.

Our abstract interpreter supports abstract garbage collection [14], the concrete analogue of which is just standard garbage collection. We include abstract garbage collection for two reasons. First, it is one of the few techniques that results in both performance *and* precision improvements for abstract interpreters. Second, we will systematically recover concrete and abstract garbage collectors with varying path and flow sensitivities through a single monadic garbage collector, an axis of generality novel in this work.

We show the garbage collected semantics in Figure 3, as well as a final collecting semantics *collect*, which will serve as the starting point for abstraction. The concrete, garbage-collected collecting semantics *collect* and a sound

static analyzer will both be recovered from instantiations of a generic monadic interpreter in Section 6.

The garbage collected semantics  $\_ \rightsquigarrow^{gc} \_$  is defined with reachability functions  $KR$  and  $R$  which define transitively reachable addresses. We write  $\mu(X).f(X)$  as the least-fixed-point of the function  $f$ .  $R$  is defined in terms of  $R\text{-Frm}$  and  $R\text{-Val}$ , which define the immediately reachable locations from a frame and value respectively. We omit the definition of  $FV$ , which is the standard recursive definition for computing free variables of an expression.

### 3. Path and Flow Sensitivity in Analysis

We identify three specific variants of path and flow sensitivity in analysis: path-sensitive, flow-sensitive and flow-insensitive. Our framework exposes the essence of path and flow sensitivity through a monadic effect interface in Section 4, and we recover each of these variations through specific monad instances in Sections 7 and 8.

Consider a combination of if-statements in our example language  $\lambda\text{IF}$  (extended with let-bindings) where an analysis cannot determine the value of  $N$ :

```

1 : let x :=                in
   2 : if0(N){                5 : let y :=
       3 : if0(N){1}{2}        6 : if0(N){5}{6}
   } else {                    in
       4 : if0(N){3}{4}      7 : exit(x, y)

```

**Path-Sensitive** A path-sensitive analysis tracks both data and control flow precisely. At program points 3 and 4 the analysis considers separate worlds:

$$3 : \{N = 0\} \quad 4 : \{N \neq 0\}$$

At program points 5 and 6 the analysis continues in two separate, precise worlds:

$$5, 6 : \{N = 0, x = 1\} \{N \neq 0, x = 4\}$$

At program point 7 the analysis correctly correlates  $x$  and  $y$ :

$$7 : \{N = 0, x = 1, y = 5\} \{N \neq 0, x = 4, y = 6\}$$

**Flow-Sensitive** A flow-sensitive analysis collects a *single* set of facts for each variable *at each program point*. At program points 3 and 4, the analysis considers separate worlds:

$$3 : \{N = 0\} \quad 4 : \{N \neq 0\}$$

Each nested if-statement then evaluates only one side of the branch, resulting in values 1 and 4. At program points 5 and 6 the analysis is only allowed one set of facts, so it must merge the possible values that  $x$  and  $N$  could take:

$$5, 6 : \{N \in \mathbb{Z}, x \in \{1, 4\}\}$$

The analysis then explores both branches at program point 6 resulting in no correlation between values for  $x$  and  $y$ :

$$7 : \{N \in \mathbb{Z}, x \in \{1, 4\}, y \in \{5, 6\}\}$$

**Flow-Insensitive** A flow-insensitive analysis collects a *single* set of facts about each variable which must hold true *for the entire program*. Because the value of  $N$  is unknown at *some* point in the program, the value of  $x$  must consider both branches of the nested if-statement. This results in the global set of facts giving four values to  $x$ :

$$\{N \in \mathbb{Z}, x \in \{1, 2, 3, 4\}, y \in \{5, 6\}\}$$

## 4. Analysis Parameters

Before constructing the abstract interpreter we first design its parameters. The interpreter, which we develop in Section 5, will be designed such that variations in these parameters will recover both concrete and a family of abstract interpreters, which we show in Section 6. To do this we extend the ideas developed in Van Horn and Might [23] with a new parameter for path and flow sensitivity: the interpreter monad.

There will be three parameters to our abstract interpreter:

1. The monad, novel in this work, which captures control effects and gives rise to path and flow sensitivity.
2. The abstract domain, which captures the abstraction of values like integers or datatypes.
3. The abstraction for time, which captures call-site and object sensitivities.

We place each of these parameters behind an abstract interface and leave their implementations opaque when defining the monadic interpreter in Section 5. Each parameter comes with laws which can be used to reason about the generic interpreter independent of a particular instantiation. Likewise, an instantiation of the interpreter need only justify that each parameter meets its local interface, which we justify in isolation from the generic interpreter.

### 4.1 The Analysis Monad

The monad for the interpreter captures the *effects* of interpretation. There are two effects in the interpreter: state and nondeterminism. The state effect will mediate how the interpreter interacts with state cells in the state space: *Env*, *Store*, *KAddr*, *KStore* and *Time*. The nondeterminism effect will mediate branching in the execution of the interpreter. Path and flow sensitivity will be recovered by altering how these effects interact in a particular choice of monad.

We use monadic state and nondeterminism effects to abstract over arbitrary relational small-step state-machine semantics. State effects correspond to the components of the state-machine and nondeterminism effects correspond to potential nondeterminism in the relation's definition.

We briefly review monad, state and nondeterminism operators and their laws. For a more detailed presentation see Liang et al. [12], Gibbons and Hinze [7] and Moggi [16].

**Monad Operators** A type operator  $m$  is a monad if it supports  $bind$ , a sequencing operator, and its unit  $return$ :

$$\begin{aligned} m &: Type \rightarrow Type \\ return &: \forall A, A \rightarrow m(A) \\ bind &: \forall AB, m(A) \rightarrow (A \rightarrow m(B)) \rightarrow m(B) \end{aligned}$$

and obeys left unit, right unit and associativity laws.

We use semicolon notation for  $bind$ —e.g.  $x \leftarrow X ; k(x)$  is sugar for  $bind(X)(k)$ —and we replace semicolons with line breaks headed by `do` for multiline monadic definitions.

**State Effect** A type operator  $m$  supports the monadic state effect for a type  $s$  if it supports  $get$  and  $put$  actions over  $s$ :

$$\begin{aligned} s &: Type & get &: m(s) \\ m &: Type \rightarrow Type & put &: s \rightarrow m(1) \end{aligned}$$

and obeys get-get, get-put, put-get and put-put laws [7].

**Nondeterminism Effect** A type operator  $m$  supports the monadic nondeterminism effect if it supports an alternation operator  $\langle + \rangle$  and its unit  $mzero$ :

$$\begin{aligned} m &: Type \rightarrow Type \\ mzero &: \forall A, m(A) \\ \langle + \rangle &: \forall A, m(A) \times m(A) \rightarrow m(A) \end{aligned}$$

$m(A)$  must have a join-semilattice structure,  $mzero$  must be a zero for  $bind$ ,  $bind$  must distribute through  $\langle + \rangle$ .

The interpreter in Section 5 will be defined generic to a monad which supports monad operators, state effects and nondeterminism effects. As a consequence, we do not reference an explicit configuration  $\varsigma$  or collections of results; instead we interact with an interface of state and nondeterminism effects. This level of indirection will be exploited in Section 7, where different monads will meet the same effect interface but yield different analysis properties.

## 4.2 The Abstract Domain

To expose the abstract domain we parameterize over  $Val$ , introduction and elimination forms for  $Val$ , and the denotation for primitive operators  $\delta[\_]$ .

$Val$  must be a join-semilattice with  $\perp$  and  $\sqcup$ :

$$\perp : Val \quad \_ \sqcup \_ : Val \times Val \rightarrow Val$$

and respect the usual join-semilattice laws.  $Val$  must be a join-semilattice so it can be merged in updates to  $Store$  to preserve soundness.

$Val$  must also support introduction and elimination between finite sets of concrete values  $\mathbb{Z}$  and  $Clo$ :

$$\begin{aligned} int-I &: \mathbb{Z} \rightarrow Val & if0-E &: Val \rightarrow \mathcal{P}(Bool) \\ clo-I &: Clo \rightarrow Val & clo-E &: Val \rightarrow \mathcal{P}(Clo) \end{aligned}$$

Introduction functions inject concrete values into abstract values. Elimination functions project abstract values into a *finite* set of concrete observations. For example, we do not require that abstract values support elimination to integers, only to finite observation of comparison with zero. The laws for the introduction and elimination functions induce a Galois connection between  $\mathcal{P}(\mathbb{Z})$  and  $Val$ :

$$\begin{aligned} \{\mathbf{true}\} &\subseteq if0-E(int-I(i)) \text{ if } i = 0 \\ \{\mathbf{false}\} &\subseteq if0-E(int-I(i)) \text{ if } i \neq 0 \\ \bigsqcup_{\substack{b \in if0-E(v) \\ i \in \theta(b)}} int-I(i) &\subseteq v \\ \text{where } \theta(\mathbf{true}) &:= \{0\} \\ \theta(\mathbf{false}) &:= \{i \mid i \in \mathbb{Z}; i \neq 0\} \end{aligned}$$

Closures must follow similar laws, inducing a Galois connection between  $\mathcal{P}(Clo)$  and  $Val$ :

$$\begin{aligned} \{c\} &\subseteq clo-E(clo-I(c)) \\ \bigsqcup_{c \in clo-E(v)} clo-I(c) &\subseteq v \end{aligned}$$

Finally,  $\delta[\_]$  must be sound w.r.t. the Galois connection between concrete values and  $Val$ :

$$\begin{aligned} int-I(i_1 + i_2) &\subseteq \delta[\langle + \rangle](int-I(i_1), int-I(i_2)) \\ int-I(i_1 - i_2) &\subseteq \delta[\langle - \rangle](int-I(i_1), int-I(i_2)) \end{aligned}$$

Supporting additional primitive types like booleans, lists, or arbitrary inductive datatypes is analogous. Introduction functions inject the type into  $Val$  and elimination functions project a finite set of discrete observations. Introduction, elimination and  $\delta$  operators must all be sound and complete following a Galois connection discipline.

## 4.3 Abstract Time

The interface we use for abstract time is familiar from Van Horn and Might [23], which introduces abstract time as a single parameter to control various forms of context sensitivity, and Smaragdakis et al. [22], which instantiates the parameter to achieve various forms of object sensitivity. We only demonstrate call-site sensitivity in this presentation; our semantics-independent Haskell library supports object sensitivity following the same methodology.

Abstract time need only support a single operation:  $tick$ :

$$Time : Type \quad tick : Exp \times KAddr \times Time \rightarrow Time$$

Remarkably, we need not state laws for  $tick$ . The interpreter will merge values which reside at the same address to preserve soundness. Therefore, any supplied implementations of  $tick$  is valid from a soundness perspective. However, different choices in  $tick$  will yield different trade-offs in precision and performance of the abstract interpreter.

$$\begin{aligned}
A^m[\_ ] &: Atom \rightarrow m(Val) \\
A^m[i] &:= return(int-I(i)) \\
A^m[x] &:= \mathbf{do} \\
&\quad \rho \leftarrow get-Env ; \sigma \leftarrow get-Store \\
&\quad \mathbf{if} \ x \in \rho \ \mathbf{then} \ return(\sigma(\rho(x))) \ \mathbf{else} \ return(\perp) \\
A^m[\lambda(x).e] &:= \rho \leftarrow get-Env ; return(clo-I(\langle \lambda(x).e, \rho \rangle)) \\
\\
step^m &: Exp \rightarrow m(Exp) \\
step^m(e) &:= \mathbf{do} \\
&\quad tick^m(e) ; \rho \leftarrow get-Env \\
e' &\leftarrow \mathbf{case} \ e \ \mathbf{of} \\
&\quad e_1 \odot e_2 \rightarrow push((\square \odot e_2, \rho)) ; return(e_1) \\
&\quad \mathbf{if}0(e_1)\{e_2\}\{e_3\} \rightarrow push((\mathbf{if}0(\square)\{e_2\}\{e_3\}, \rho)) ; return(e_1) \\
a &\rightarrow \mathbf{do} \\
&\quad v \leftarrow A^m[a] ; fr \leftarrow pop \\
&\quad \mathbf{case} \ fr \ \mathbf{of} \\
&\quad \langle \square \odot e, \rho' \rangle \rightarrow put-Env(\rho') ; push((v \odot \square)) ; return(e) \\
&\quad \langle v' \ @ \ \square \rangle \rightarrow \mathbf{do} \\
&\quad \quad \tau \leftarrow get-Time ; \sigma \leftarrow get-Store \\
&\quad \quad \langle \lambda(x).e, \rho' \rangle \leftarrow \uparrow_p(clo-E(v')) \\
&\quad \quad put-Env(\rho'[x \mapsto (x, \tau)]) \\
&\quad \quad put-Store(\sigma \sqcup [(x, \tau) \mapsto v]) ; return(e) \\
&\quad \langle v' \oplus \square \rangle \rightarrow return(\delta[\oplus](v', v)) \\
&\quad \langle \mathbf{if}0(\square)\{e_1\}\{e_2\}, \rho' \rangle \rightarrow \mathbf{do} \\
&\quad \quad put-Env(\rho') ; b \leftarrow \uparrow_p(\mathbf{if}0-E(v)) ; refine(a, b) \\
&\quad \quad \mathbf{if}(b) \ \mathbf{then} \ return(e_1) \ \mathbf{else} \ return(e_2) \\
gc(e') & ; return(e')
\end{aligned}$$

**Figure 4.** Monadic Semantics

## 5. The Interpreter

We now present a monadic interpreter for  $\lambda\text{IF}$  parameterized over  $m$ ,  $Val$  and  $Time$  from Section 4. We instantiate these parameters to obtain an analysis in Section 6.

We translate  $A[\_ ]$ , a partial denotation function, to  $A^m[\_ ]$ , a total monadic denotation function, shown in Figure 4.

Next we implement  $step^m$ , a *monadic small-step function* for compound expressions, also shown in Figure 4.  $step^m$  is a translation of  $\_ \rightsquigarrow \_$  from a relation to a monadic function with state and nondeterminism effects.

$step^m$  uses  $push$  and  $pop$  for manipulating stack frames,  $\uparrow_p$  for lifting values from  $\mathcal{P}$  into  $m$ ,  $refine$  for value refinement after branching, and a monadic version of  $tick$  called  $tick^m$ , each shown in Figure 5. Frames are pushed when the control

$$\begin{aligned}
push &: Frame \rightarrow m(1) \\
push(fr) &:= \mathbf{do} \\
&\quad \kappa l \leftarrow get-KAddr ; \kappa \sigma \leftarrow get-KStore ; \kappa l' \leftarrow get-Time \\
&\quad put-KStore(\kappa \sigma \sqcup [\kappa l' \mapsto \{fr :: \kappa l\}]) ; put-KAddr(\kappa l') \\
pop &: m(Frame) \\
pop &:= \mathbf{do} \\
&\quad \kappa l \leftarrow get-KAddr ; \kappa \sigma \leftarrow get-KStore ; fr :: \kappa l' \leftarrow \uparrow_p(\kappa \sigma(\kappa l)) \\
&\quad put-KAddr(\kappa l') ; return(fr) \\
\uparrow_p &: \forall A, \mathcal{P}(A) \rightarrow m(A) \\
\uparrow_p(\{a_1..a_n\}) &:= return(a_1) \langle + \rangle .. \langle + \rangle return(a_n) \\
refine &: Atom \times Bool \rightarrow m(1) \\
refine(i, b) &:= return(1) \\
refine(x, b) &:= \mathbf{do} \\
&\quad \rho \leftarrow get-Env ; \sigma \leftarrow get-Store \\
&\quad put-Store(\sigma[\rho(x) \mapsto b]) \\
tick^m &: Exp \rightarrow m(1) \\
tick^m(e) &:= \mathbf{do} \\
&\quad \tau \leftarrow get-Time ; \kappa l \leftarrow get-KAddr \\
&\quad put-Time(tick(e, \kappa l, \tau)) \\
gc &: Exp \rightarrow m(1) \\
gc(e) &:= \mathbf{do} \\
&\quad \rho \leftarrow get-Env ; \sigma \leftarrow get-Store \\
&\quad \kappa l \leftarrow get-KAddr ; \kappa \sigma \leftarrow get-KStore \\
&\quad put-KStore(\{\kappa l \mapsto \kappa \sigma(\kappa l) \mid \kappa l \in KR(\kappa l, \kappa \sigma)\}) \\
&\quad put-Store(\{l \mapsto \sigma(l) \mid l \in R(e, \rho, \sigma, \kappa l, \kappa \sigma)\})
\end{aligned}$$

**Figure 5.** Monadic helper functions

expression  $e$  is compound and popped when  $e$  is atomic. The interpreter looks deterministic, however the nondeterminism is hidden behind  $\uparrow_p$  and monadic bind operations  $x \leftarrow e_1 ; e_2$ . The use of  $refine$  enforces a limited form of path-condition, and will yield each variation of path and flow sensitivity given the appropriate monad.

We implement abstract garbage collection  $gc$  in a general way using the monadic effect interface, also shown in Figure 5.  $R$  and  $KR$  are as defined in Section 2. Remarkably, this single implementation supports instantiation to analyses with varying path and flow sensitivities.

**Preserving Soundness** In the monadic interpreter, updates to both the data-store and stack-store must merge rather than overwrite values. To support  $\sqcup$  for the stack store we redefine the domain to map to a powerset of frames:

$$\kappa \sigma \in KStore : KAddr \rightarrow \mathcal{P}(Frame \times KAddr)$$

$$v \in \mathbf{Val} := \mathcal{P}(\mathbf{Clo} \cup \mathbb{Z})$$

$$\tau \in \mathbf{Time} := (\mathit{Exp} \times \mathit{KAddr})^*$$

$$\begin{aligned} \mathit{int}\text{-}I &: \mathbb{Z} \rightarrow \mathbf{Val} \\ \mathit{int}\text{-}I(i) &:= \{i\} \\ \mathit{if}0\text{-}E &: \mathbf{Val} \rightarrow \mathcal{P}(\mathit{Bool}) \\ \mathit{if}0\text{-}E(v) &:= \{\mathbf{true} \mid 0 \in v\} \cup \{\mathbf{false} \mid \exists i \in v; i \neq 0\} \\ \mathit{clo}\text{-}I &: \mathit{Clo} \rightarrow \mathbf{Val} \\ \mathit{clo}\text{-}I(c) &:= \{c\} \\ \mathit{clo}\text{-}E &: \mathbf{Val} \rightarrow \mathcal{P}(\mathit{Clo}) \\ \mathit{clo}\text{-}E(v) &:= \{c \mid c \in v\} \\ \delta &: \mathbf{Val} \times \mathbf{Val} \rightarrow \mathbf{Val} \\ \delta[\![+\]\!](v_1, v_2) &:= \{i_1 + i_2 \mid i_1 \in v_1; i_2 \in v_2\} \\ \delta[\![-\]\!](v_1, v_2) &:= \{i_1 - i_2 \mid i_1 \in v_1; i_2 \in v_2\} \\ \mathit{tick} &: \mathit{Exp} \times \mathbf{Time} \rightarrow \mathbf{Time} \\ \mathit{tick}(e, \kappa l, \tau) &:= (e, \kappa l) :: \tau \end{aligned}$$

**Figure 6.** Concrete Interpreter Values and Time

**Execution** In the concrete semantics, execution takes the form of a least-fixed-point computation over the collecting semantics *collect*. This in general requires a join-semilattice structure for some  $\Sigma$  and a transition system  $\Sigma \rightarrow \Sigma$ . However, we no longer have a transition system  $\Sigma \rightarrow \Sigma$ ; we have a monadic function  $\mathit{Exp} \rightarrow m(\mathit{Exp})$  which cannot be iterated to least-fixed-point to execute the analysis.

To solve this we require the existence of a Galois connection between monadic actions and some transition system:  $\Sigma \rightarrow \Sigma \xleftrightarrow[\alpha^{\Sigma \leftrightarrow m}]{\gamma^{\Sigma \leftrightarrow m}} \mathit{Exp} \rightarrow m(\mathit{Exp})$ . This Galois connection allows us to implement the analysis by transporting our interpreter to the transition system  $\Sigma \rightarrow \Sigma$  through  $\gamma^{\Sigma \leftrightarrow m}$ , and then iterating to fixed-point in  $\Sigma$ . Furthermore, it serves to *transport other Galois connections* as part of our correctness framework. This will allow us to construct Galois connections between monads  $m_1 \xleftrightarrow[\alpha^m]{\gamma^m} m_2$  and derive Galois connections between transition systems  $\Sigma_1 \xleftrightarrow[\alpha^\Sigma]{\gamma^\Sigma} \Sigma_2$ .

An execution of our interpreter is then the least-fixed-point iteration of  $\mathit{step}^m$  transported through  $\gamma^{\Sigma \leftrightarrow m}$ :

$$\mathit{analysis} := \mu(X). X \sqcup \varsigma_0 \sqcup \gamma^{\Sigma \leftrightarrow m}(\mathit{step}^m)(X)$$

where  $\varsigma_0$  is the injection of the initial program  $e_0$  into  $\Sigma$  and  $\gamma^{\Sigma \leftrightarrow m}$  has type  $(\mathit{Exp} \rightarrow m(\mathit{Exp})) \rightarrow (\Sigma \rightarrow \Sigma)$ .

## 6. Recovering Analyses

In Section 5, we defined a monadic interpreter with the uninstantiated parameters from Section 4:  $m$ ,  $\mathit{Val}$  and  $\mathit{Time}$ . To recover a concrete interpreter, we instantiate these param-

$$\begin{aligned} \psi \in \Psi &:= \mathbf{Env} \times \mathbf{KAddr} \times \mathbf{KStore} \times \mathbf{Time} \\ \mathbf{M}(A) &:= \Psi \times \mathbf{Store} \rightarrow \mathcal{P}(A \times \Psi \times \mathbf{Store}) \\ \varsigma \in \Sigma &:= \mathcal{P}(\mathit{Exp} \times \Psi \times \mathbf{Store}) \end{aligned}$$

$$\begin{aligned} \mathit{return} &: \forall A, A \rightarrow \mathbf{M}(A) \\ \mathit{return}(x)(\psi, s) &:= \{(x, \psi, s)\} \\ \mathit{bind} &: \forall AB, \mathbf{M}(A) \rightarrow (A \rightarrow \mathbf{M}(B)) \rightarrow \mathbf{M}(B) \\ \mathit{bind}(X)(f)(\psi, \sigma) &:= \bigcup_{(x, \psi', \sigma') \in X(\psi, \sigma)} f(x)(\psi', \sigma') \\ \mathit{get}\text{-}Env &: \mathbf{M}(\mathbf{Env}) \\ \mathit{get}\text{-}Env(\langle \rho, \kappa l, \kappa \sigma, \tau \rangle, \sigma) &:= \{(\rho, \langle \rho, \kappa l, \kappa \sigma, \tau \rangle, \sigma)\} \\ \mathit{put}\text{-}Env &: \mathbf{Env} \rightarrow \mathcal{P}(1) \\ \mathit{put}\text{-}Env(\rho')(\langle \rho, \kappa l, \kappa \sigma, \tau \rangle, \sigma) &:= \{(1, \langle \rho', \sigma, \kappa, \tau \rangle, \sigma)\} \\ \mathit{mzero} &: \forall A, \mathbf{M}(A) \\ \mathit{mzero}(\psi, \sigma) &:= \{\} \\ \_ \langle + \rangle \_ &: \forall A, \mathbf{M}(A) \times \mathbf{M}(A) \rightarrow \mathbf{M}(A) \\ (X_1 \langle + \rangle X_2)(\psi, \sigma) &:= X_1(\psi, \sigma) \cup X_2(\psi, \sigma) \\ \alpha^{\Sigma \leftrightarrow \mathbf{M}} &: (\Sigma \rightarrow \Sigma) \rightarrow (\mathit{Exp} \rightarrow \mathbf{M}(\mathit{Exp})) \\ \alpha^{\Sigma \leftrightarrow \mathbf{M}}(f)(e)(\psi, \sigma) &:= f(\{(e, \psi, \sigma)\}) \\ \gamma^{\Sigma \leftrightarrow \mathbf{M}} &: (\mathit{Exp} \rightarrow \mathbf{M}(\mathit{Exp})) \rightarrow (\Sigma \rightarrow \Sigma) \\ \gamma^{\Sigma \leftrightarrow \mathbf{M}}(f)(e\psi\sigma^*) &:= \bigcup_{(e, \psi, \sigma) \in e\psi\sigma^*} f(e)(\psi, \sigma) \end{aligned}$$

**Figure 7.** Concrete Interpreter Monad

eters to concrete components  $\mathbf{M}$ ,  $\mathbf{Val}$  and  $\mathbf{Time}$ , and to recover an abstract interpreter we instantiate them to abstract components  $\widehat{\mathbf{M}}$ ,  $\widehat{\mathbf{Val}}$  and  $\widehat{\mathbf{Time}}$ . Furthermore, the concrete transition system  $\Sigma$  induced by  $\mathbf{M}$  will recover the collecting semantics, which is our final target of abstraction, and the resulting analysis will take the form of an abstract transition system  $\widehat{\Sigma}$  induced by  $\widehat{\mathbf{M}}$ .

### 6.1 Recovering a Concrete Interpreter

To recover a concrete interpreter, we instantiate the generic monadic interpreter from Section 5 with concrete parameters  $\mathbf{Val}$ ,  $\delta$ ,  $\mathbf{Time}$  and  $\mathbf{M}$ , shown in Figures 6 and 7.

**The Concrete Domain** We instantiate  $\mathit{Val}$  to  $\mathbf{Val}$ , a powerset of concrete values.  $\mathbf{Val}$  has precise introduction and elimination functions  $\mathit{int}\text{-}I$ ,  $\mathit{if}0\text{-}E$ ,  $\mathit{clo}\text{-}I$  and  $\mathit{clo}\text{-}E$ , and primitive operator denotation  $\delta$ .

**Concrete Time** We instantiate  $\mathit{Time}$  to  $\mathbf{Time}$ , which captures the execution context as a sequence of previously visited expressions.  $\mathit{tick}$  is then a cons operation.

**The Concrete Monad** We instantiate  $m$  to  $\mathbf{M}$ , a powerset of concrete state space components. Monadic operators  $\mathit{bind}$

and *return* encapsulate both state-passing and set-flattening. State effects return singleton sets and nondeterminism effects are implemented with set union.

**Concrete Execution** To execute the interpreter we establish the Galois connection  $\Sigma \rightarrow \Sigma \xleftarrow[\alpha^{\Sigma \leftrightarrow M}]{\gamma^{\Sigma \leftrightarrow M}} \text{Exp} \rightarrow \mathbf{M}(\text{Exp})$  and transport the monadic interpreter through  $\gamma^{\Sigma \leftrightarrow m}$ . The injection for a program  $e_0$  into  $\Sigma$  is  $\varsigma_0 := \{\langle e_0, \perp, \perp, \bullet, \perp, \bullet \rangle\}$ .

## 6.2 Recovering an Abstract Interpreter

To recover an abstract interpreter we instantiate the generic monadic interpreter from Section 5 with abstract parameters  $\widehat{\mathbf{Val}}$ ,  $\widehat{\delta}$ ,  $\widehat{\mathbf{Time}}$  and  $\widehat{\mathbf{M}}$ , shown in Figure 8. The abstract monad operators, effects and transition system are not shown for  $\widehat{\mathbf{M}}$ ; they are identical to  $\mathbf{M}$  but with abstract components.

**The Abstract Domain** We pick a simple abstraction for integers,  $\{-, 0, +\}$ , although our technique scales to other abstract domains.  $\widehat{\mathbf{Val}}$  is defined as a powerset of abstract values.  $\widehat{\mathbf{Val}}$  has introduction and elimination functions  $\widehat{\text{int-I}}$ ,  $\widehat{\text{if0-E}}$ ,  $\widehat{\text{clo-I}}$  and  $\widehat{\text{clo-E}}$ , and primitive operator denotation  $\widehat{\delta}$ .  $\widehat{\text{if0-E}}$  and  $\widehat{\delta}$  must be conservative, returning an upper bound of the precise results returned by their concrete counterparts.

**Abstract Time** Abstract time  $\widehat{\mathbf{Time}}$  captures an approximation of the execution context as a finite sequence of previously visited expressions.  $\widehat{\text{tick}}$  is a cons operation followed by k-truncation, yielding a kCFA analysis [23].

**The Abstract Monad and Execution** The abstract monad  $\widehat{\mathbf{M}}$  is identical to  $\mathbf{M}$  up to the definition of  $\widehat{\Psi}$ . The induced state space  $\widehat{\Sigma}$  is finite, and its least-fixed-point iteration will give a sound and computable analysis.

## 6.3 End-to-End Correctness

The end-to-end correctness of the abstract instantiation of the interpreter is factored into three steps: (1) proving the parameterized monadic interpreter correct for any instantiation of  $m$ ,  $\text{Val}$  and  $\text{Time}$ ; (2) constructing Galois connections  $\mathbf{M} \xleftarrow[\alpha^m]{\gamma^m} \widehat{\mathbf{M}}$ ,  $\mathbf{Val} \xleftarrow[\alpha^v]{\gamma^v} \widehat{\mathbf{Val}}$  and  $\mathbf{Time} \xleftarrow[\alpha^t]{\gamma^t} \widehat{\mathbf{Time}}$  piecewise; and (3) transporting the combination of (1) and (2) from the monadic function space  $A \rightarrow m(B)$  to its induced transition system  $\Sigma \rightarrow \Sigma$ . The benefit of our approach is that the first step is proved once and for all (for a particular semantics) against *any* instantiation of  $m$ ,  $\text{Val}$  and  $\text{Time}$  using the reasoning principles established in Section 4. Furthermore the second step can be proved in isolation of the first, and the construction of the third step is fully systematic.

We do not give proofs for (1) or the abstractions for  $\text{Val}$  and  $\text{Time}$  for (2) in this paper, although the details can be found in prior work [3, 23]. Rather, we give definitions and proofs for the monad abstractions for (2) and their systematic mappings to transition systems for (3) through a compositional framework in Section 8.

The final correctness of the abstract interpreter is established as a partial order relationship between an abstraction

$$\begin{aligned} v \in \widehat{\mathbf{Val}} &:= \mathcal{P}(\widehat{\mathbf{Clo}} \cup \{-, 0, +\}) \\ \tau \in \widehat{\mathbf{Time}} &:= (\text{Exp} \times \text{KAddr})^{*k} \\ \psi \in \widehat{\Psi} &:= \widehat{\mathbf{Env}} \times \widehat{\mathbf{KAddr}} \times \widehat{\mathbf{KStore}} \times \widehat{\mathbf{Time}} \\ \widehat{\mathbf{M}}(A) &:= \widehat{\Psi} \times \widehat{\mathbf{Store}} \rightarrow \mathcal{P}(A \times \widehat{\Psi} \times \widehat{\mathbf{Store}}) \\ \varsigma \in \widehat{\Sigma} &:= \mathcal{P}(\text{Exp} \times \widehat{\Psi} \times \widehat{\mathbf{Store}}) \end{aligned}$$

$$\begin{aligned} \widehat{\text{int-I}} : \mathbb{Z} \rightarrow \widehat{\mathbf{Val}} & \quad \widehat{\text{int-I}}(i) := \begin{cases} \{-\} & \text{if } i < 0 \\ \{0\} & \text{if } i = 0 \\ \{+\} & \text{if } i > 0 \end{cases} \\ \widehat{\text{if0-E}} : \widehat{\mathbf{Val}} \rightarrow \mathcal{P}(\text{Bool}) & \quad \widehat{\text{if0-E}}(v) := \begin{cases} \{\text{true} \mid 0 \in v\} \cup \\ \{\text{false} \mid - \in v \vee + \in v\} \end{cases} \\ \widehat{\text{clo-I}} : \text{Clo} \rightarrow \widehat{\mathbf{Val}} & \quad \widehat{\text{clo-I}}(c) := \{c\} \\ \widehat{\text{clo-E}} : \widehat{\mathbf{Val}} \rightarrow \mathcal{P}(\text{Clo}) & \quad \widehat{\text{clo-E}}(v) := \{c \mid c \in v\} \\ \widehat{\delta} : \widehat{\mathbf{Val}} \times \widehat{\mathbf{Val}} \rightarrow \widehat{\mathbf{Val}} & \\ \widehat{\delta}[\![\ ]\!](v_1, v_2) &:= \begin{aligned} & \{i \mid 0 \in v_1 \wedge i \in v_2\} \cup \{i \mid i \in v_1 \wedge 0 \in v_2\} \\ & \cup \{+ \mid + \in v_1 \wedge + \in v_2\} \cup \{- \mid - \in v_1 \wedge - \in v_2\} \\ & \cup \{-, 0, + \mid + \in v_1 \wedge - \in v_2\} \\ & \cup \{-, 0, + \mid - \in v_1 \wedge + \in v_2\} \end{aligned} \\ \widehat{\delta}[\![-]\!](v_1, v_2) &:= \dots \text{ analogous } \dots \\ \widehat{\text{tick}} : \text{Exp} \times \widehat{\mathbf{Time}} \rightarrow \widehat{\mathbf{Time}} & \\ \widehat{\text{tick}}(e, \kappa l, \tau) &:= \lfloor (e, \kappa l) :: \tau \rfloor_k \end{aligned}$$

**Figure 8.** Abstract Interpreter Parameters

of  $\gamma^{\Sigma \leftrightarrow M}(\text{step}^m[\mathbf{M}])$ , which recovers the collecting semantics, and  $\gamma^{\widehat{\Sigma} \leftrightarrow \widehat{\mathbf{M}}}(\text{step}^m[\widehat{\mathbf{M}}])$ , the induced abstract semantics:

**Proposition 1.**

$$\alpha^{\Sigma}(\gamma^{\Sigma \leftrightarrow M}(\text{step}^m[\mathbf{M}])) \sqsubseteq \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{\mathbf{M}}}(\text{step}^m[\widehat{\mathbf{M}}])$$

The left-hand-side of the relationship is the induced “best specification” of the collecting semantics via Galois connection, and should be familiar from the literature on abstract interpretation [3, 5, 18]. This end-to-end correctness statement will be justified in a compositional setting in Section 8.

## 7. Varying Path and Flow Sensitivity

Sections 5 and 6 describe the construction of a path-sensitive analysis using our framework. In this section, we show an alternate definition for  $\widehat{\mathbf{M}}$  which yields a flow-insensitive analysis. Section 8 will generalize the definitions from this section into compositional components (monad transformers) in addition to introducing another definition for  $\widehat{\mathbf{M}}$  which yields a flow-sensitive analysis.

Before going into the details of the flow-insensitive monad, we wish to build intuition regarding what one would



expect from such a development. Recall the path-sensitive monad  $\widehat{M}$  and its state space  $\widehat{\Sigma}$  from section 6:

$$\begin{aligned}\widehat{M}(Exp) &:= \widehat{\Psi} \times \widehat{\text{Store}} \rightarrow \mathcal{P}(Exp \times \widehat{\Psi} \times \widehat{\text{Store}}) \\ \widehat{\Sigma}(Exp) &:= \mathcal{P}(Exp \times \widehat{\Psi} \times \widehat{\text{Store}})\end{aligned}$$

where  $\Psi := \widehat{\text{Env}} \times \widehat{\text{KAddr}} \times \widehat{\text{KStore}} \times \widehat{\text{Time}}$ . This is path-sensitive because  $\widehat{\Sigma}(Exp)$  can represent arbitrary *relations* between  $(Exp \times \Psi)$  and  $\widehat{\text{Store}}$ .

As discussed in Section 3, a flow-sensitive analysis will give a single set of facts per program point. This results in the following monad  $\widehat{M}^{fs}$  and state space  $\widehat{\Sigma}^{fs}$  which encode *finite maps* to  $\widehat{\text{Store}}$  rather than relations:

$$\begin{aligned}\widehat{M}^{fs}(Exp) &:= \widehat{\Psi} \times \widehat{\text{Store}} \rightarrow [(Exp \times \widehat{\Psi}) \mapsto \widehat{\text{Store}}] \\ \widehat{\Sigma}^{fs}(Exp) &:= [(Exp \times \widehat{\Psi}) \mapsto \widehat{\text{Store}}]\end{aligned}$$

Finally, a flow-insensitive analysis must contain a global set of facts for each variable, which we achieve by pulling  $\widehat{\text{Store}}$  out of the powerset:

$$\begin{aligned}\widehat{M}^{fi}(Exp) &:= \widehat{\Psi} \times \widehat{\text{Store}} \rightarrow \mathcal{P}(Exp \times \widehat{\Psi}) \times \widehat{\text{Store}} \\ \widehat{\Sigma}^{fi}(Exp) &:= \mathcal{P}(Exp \times \widehat{\Psi}) \times \widehat{\text{Store}}\end{aligned}$$

These three resulting structures,  $\widehat{\Sigma}$ ,  $\widehat{\Sigma}^{fs}$  and  $\widehat{\Sigma}^{fi}$ , capture the essence of path-sensitive, flow-sensitive and flow-insensitive transition systems, and arise naturally from  $\widehat{M}$ ,  $\widehat{M}^{fs}$  and  $\widehat{M}^{fi}$ , which each have monadic structure. We only describe  $\widehat{M}^{fi}$  directly in this section; in Section 8 we describe a more compositional set of building blocks, from which  $\widehat{M}$ ,  $\widehat{M}^{fs}$  and  $\widehat{M}^{fi}$  are recovered.

## 7.1 Flow Insensitive Monad

We show the definitions for monad operators, state effects, nondeterminism effects, and mapping to transition system for the flow-insensitive monad  $\widehat{M}^{fi}$  in Figure 9.

The  $\widehat{bind}^{fi}$  operation performs the global store merging required to capture a flow-insensitive analysis. The unit for  $\widehat{bind}^{fi}$  returns one nondeterminism branch and a single global store. State effects  $\widehat{get-Env}^{fi}$  and  $\widehat{put-Env}^{fi}$  return a single branch of nondeterminism. Nondeterminism operations union the powerset and join the store pairwise. Finally, the Galois connection relating  $\widehat{M}^{fi}$  to the state space  $\widehat{\Sigma}^{fi}$  also computes powerset unions and store joins pairwise.

Instantiating the generic monadic interpreter with  $M$ ,  $\widehat{M}$  and  $\widehat{M}^{fi}$  yields a concrete interpreter, path-sensitive abstract interpreter, and flow-insensitive abstract interpreter respectively, purely by changing the underlying monad. Furthermore, the proofs of abstraction between interpreters and their induced transition systems is isolated to a proof of abstraction between monads.

## 8. A Compositional Monadic Framework

In our development thus far, any modification to the interpreter requires redesigning the monad  $\widehat{M}$  and constructing

$$\begin{aligned}\widehat{M}^{fi}(A) &:= \widehat{\Psi} \times \widehat{\text{Store}} \rightarrow \mathcal{P}(A \times \widehat{\Psi}) \times \widehat{\text{Store}} \\ \varsigma \in \widehat{\Sigma}^{fi} &:= \mathcal{P}(Exp \times \widehat{\Psi}) \times \widehat{\text{Store}}\end{aligned}$$

---


$$\begin{aligned}\widehat{return}^{fi} &: \forall A, A \rightarrow \widehat{M}^{fi}(A) \\ \widehat{return}^{fi}(x)(\psi, \sigma) &:= (\{x, \psi\}, \sigma) \\ \widehat{bind}^{fi} &: \forall AB, \widehat{M}^{fi}(A) \rightarrow (A \rightarrow \widehat{M}^{fi}(B)) \rightarrow \widehat{M}^{fi}(B) \\ \widehat{bind}^{fi}(X)(f)(\psi, \sigma) &:= \\ &(\{y\psi_{11}..y\psi_{1m_1}..y\psi_{n1}..y\psi_{nm_n}\}, \sigma_1 \sqcup .. \sqcup \sigma_n) \text{ where} \\ &(\{(x_1, \psi_1)..(x_n, \psi_n)\}, \sigma') := X(\psi, \sigma) \\ &(\{y\psi_{i1}..y\psi_{im_i}\}, \sigma_i) := f(x_i)(\psi_i, \sigma') \\ \widehat{get-Env}^{fi} &: \widehat{M}^{fi}(\widehat{\text{Env}}) \\ \widehat{get-Env}^{fi}(\langle \rho, \kappa, \tau \rangle, \sigma) &:= (\{(\rho, \langle \rho, \kappa, \tau \rangle)\}, \sigma) \\ \widehat{put-Env}^{fi} &: \widehat{\text{Env}} \rightarrow \widehat{M}^{fi}(1) \\ \widehat{put-Env}^{fi}(\rho')(\langle \rho, \kappa, \tau \rangle, \sigma) &:= (\{(1, \langle \rho', \kappa, \tau \rangle)\}, \sigma) \\ \widehat{mzero}^{fi} &: \forall A, \widehat{M}^{fi}(A) \\ \widehat{mzero}^{fi}(\psi, \sigma) &:= (\{\}, \perp) \\ \widehat{\langle + \rangle}^{fi} &: \forall A, \widehat{M}^{fi}(A) \times \widehat{M}^{fi}(A) \rightarrow \widehat{M}^{fi} A \\ (X_1 \langle + \rangle X_2)(\psi, \sigma) &:= (x\psi_1^* \sqcup x\psi_2^*, \sigma_1 \sqcup \sigma_2) \text{ where} \\ &(x\psi_i^*, \sigma_i) := X_i(\psi, \sigma) \\ \alpha^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}} &: (\widehat{\Sigma}^{fi} \rightarrow \widehat{\Sigma}^{fi}) \rightarrow (Exp \rightarrow \widehat{M}^{fi}(Exp)) \\ \alpha^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}}(f)(e)(\psi, \sigma) &:= f(\{(e, \psi)\}, \sigma) \\ \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}} &: (Exp \rightarrow \widehat{M}^{fi}(Exp)) \rightarrow (\widehat{\Sigma}^{fi} \rightarrow \widehat{\Sigma}^{fi}) \\ \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}}(f)(e\psi^*, \sigma) &:= \\ &(\{e\psi_{11}..e\psi_{n1}..e\psi_{nm_n}\}, \sigma_1 \sqcup .. \sqcup \sigma_n) \text{ where} \\ &(\{e_1, \psi_1\}..(e_n, \psi_n)) := e\psi^* \\ &(\{e\psi_{i1}..e\psi_{im_i}\}, \sigma_i) := f(e_i)(\psi_i, \sigma)\end{aligned}$$

**Figure 9.** Flow Insensitive Monad Parameter

new proofs relating  $\widehat{M}$  to  $M$ . We want to avoid reconstructing complicated monads for interpreters, especially as languages and analyses grow and change. Even more, we want to avoid reconstructing complicated *proofs* that such changes require. Toward this goal, we introduce a compositional framework for constructing monads which are correct-by-construction by extending the well-known structure of monad transformer to that of *Galois transformer*.

Galois transformers are monad transformers which transport Galois connections and mappings to an executable transition system. We make this definition precise and prove our Galois transformers correct in Section 8.4. For now we present monad transformer operations augmented with the computational part of Galois transformers: the mapping to a

transition system, which we called  $\alpha^{\Sigma \leftrightarrow M}$ ,  $\gamma^{\Sigma \leftrightarrow M}$ ,  $\alpha^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}}$  and  $\gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}^{fi}}$  in Sections 6 and 7.

There are two monadic effects used in our monadic interpreter: state and nondeterminism. For state, we review the state monad transformer  $S^t[s]$ , which is standard[12, 16], however we also show how  $S^t[s]$  maps to a transition system and obeys Galois transformer properties. For nondeterminism we develop two new monad transformers:  $\mathcal{P}^t$  and  $F^t[s]$ . These monad transformers are fully general purpose, even outside the context of program analysis, and are novel in this work. Finally we show that  $\mathcal{P}^t$  and  $F^t[s]$  map to transition systems and obey Galois transformer properties.

To create a monad with various state and nondeterminism effects, one need only construct some composition of these three monad transformers. Implementations and proofs for monadic sequencing, state effects, nondeterminism effects, and mappings to an executable transition system will come entirely for free. This means that for a language which has a different state space than the example in this paper, no added effort is required to construct a monad stack for that language; it will merely require a different selection and permutation of the same monad transformer components.

Path and flow sensitivity properties arise from the *order of composition* of state and nondeterminism monad transformers. Placing state after nondeterminism ( $S^t[s] \circ \mathcal{P}^t$  or  $S^t[s] \circ F^t[s']$ ) will result in  $s$  being path-sensitive. Placing state before nondeterminism ( $\mathcal{P}^t \circ S^t[s]$  or  $F^t[s'] \circ S^t[s]$ ) will result in  $s$  being flow-insensitive. Finally, when  $F^t[s]$  is used in place of  $S^t[s] \circ \mathcal{P}^t$  or  $\mathcal{P}^t \circ S^t[s]$ ,  $s$  will be flow-sensitive. The combination of all three sensitivities is  $M := S^t[s_1] \circ F^t[s_2] \circ S^t[s_3]$  which induces the transition system  $\Sigma(Exp) := [(Exp \times s_1) \mapsto s_2] \times s_3$ , where  $s_1$  is path-sensitive,  $s_2$  is flow-sensitive, and  $s_3$  is flow-insensitive. Using  $S^t[s]$ ,  $\mathcal{P}^t$  and  $F^t[s]$ , one can easily choose which components of the state space should be path-sensitive, flow-sensitive or flow-insensitive, purely by the order of monad composition.

In the following definitions we must refer to *bind*, *return* and other operations from the underlying monad, which we notate  $bind^m$ ,  $return^m$ ,  $\leftarrow^m$ , etc.

## 8.1 State Galois Transformer

The state Galois transformer is shown in Figure 10.  $return^{S^t}$ ,  $bind^{S^t}$ ,  $get^{S^t}$  and  $put^{S^t}$  require that  $m$  be a monad.  $mzero^{S^t}$  and  $\_ \langle + \rangle^{S^t} \_$  require that  $m$  be a monad with nondeterminism effects. And finally,  $\alpha^{S^t}$  and  $\gamma^{S^t}$  require that  $m$  maps to  $\Sigma^m$  via Galois connection  $\Sigma(A) \rightarrow \Sigma(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m(B)$ .

## 8.2 Nondeterminism Galois Transformer

The nondeterminism Galois transformer is shown in Figure 11. Crucially,  $return^{\mathcal{P}^t}$  and  $bind^{\mathcal{P}^t}$  require that  $m$  be both a monad and a *join-semilattice functor*. We attribute this requirement (and the difficulty of expressing it in Haskell) as a possible reason why it has not been discovered thus far. This functorality of  $m$  is instantiated with  $\mathcal{P}(\_)$  using the usual

$$\begin{aligned} S^t[s] &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\ S^t[s](m)(A) &:= s \rightarrow m(A \times s) \\ \Pi^{S^t}[s] &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\ \Pi^{S^t}[s](\Sigma)(A) &:= \Sigma(A \times s) \end{aligned}$$

---


$$\begin{aligned} return^{S^t} &: \forall A, A \rightarrow S^t[s](m)(A) \\ return^{S^t}(x)(s) &:= return^m(x, s) \\ bind^{S^t} &: \forall AB, S^t[s](m)(A) \rightarrow (A \rightarrow S^t[s](m)(B)) \rightarrow S^t[s](m)(B) \\ bind^{S^t}(X)(f)(s) &:= (x, s') \leftarrow^m X(s); f(x)(s') \\ get^{S^t} &: S^t[s](m)(s) \\ get^{S^t}(s) &:= return^m(s, s) \\ put^{S^t} &: s \rightarrow S^t[s](m)(1) \\ put^{S^t}(s')(s) &:= return^m(1, s') \\ mzero^{S^t} &: \forall A, S^t[s](m)(A) \\ mzero^{S^t}(s) &:= mzero^m \\ \_ \langle + \rangle^{S^t} \_ &: \forall A, S^t[s](m)(A) \times S^t[s](m)(A) \rightarrow S^t[s](m)(A) \\ (X_1 \langle + \rangle^{S^t} X_2)(s) &:= X_1(s) \langle + \rangle^m X_2(s) \\ \alpha^{S^t} &: \forall AB, \\ &(\Pi^{S^t}[s](\Sigma^m)(A) \rightarrow \Pi^{S^t}[s](\Sigma^m)(B)) \rightarrow (A \rightarrow S^t[s](m)(B)) \\ \alpha^{S^t}(f)(x)(s) &:= \alpha^m(f)(x, s) \\ \gamma^{S^t} &: \forall AB, \\ &(A \rightarrow S^t[s](m)(B)) \rightarrow (\Pi^{S^t}[s](\Sigma^m)(A) \rightarrow \Pi^{S^t}[s](\Sigma^m)(B)) \\ \gamma^{S^t}(f) &:= \gamma^m(\lambda(x, s).f(x)(s)) \end{aligned}$$

**Figure 10.** State Galois Transformer

join-semilattice on powersets:  $\{\}$  for  $\perp$  and  $\cup$  for  $\sqcup$ .  $get^{\mathcal{P}^t}$  and  $put^{\mathcal{P}^t}$  require that  $m$  be a monad with state effects. Like the state Galois transformer,  $\alpha^{\mathcal{P}^t}$  and  $\gamma^{\mathcal{P}^t}$  require that  $m$  maps to  $\Sigma^m$  via Galois connection.

**Lemma 1.** [ $\mathcal{P}^t$  laws]  *$bind^{\mathcal{P}^t}$  and  $return^{\mathcal{P}^t}$  satisfy monad laws,  $get^{\mathcal{P}^t}$  and  $put^{\mathcal{P}^t}$  satisfy state monad laws, and  $mzero^{\mathcal{P}^t}$  and  $\langle + \rangle^{\mathcal{P}^t}$  satisfy nondeterminism monad laws.*

See our proofs in the extended version of the paper, where the key lemma in proving monad laws is the join-semilattice functorality of  $m$ , namely that:

$$\begin{aligned} return^m(x \sqcup y) &= return^m(x) \sqcup^m return^m(y) \\ bind^m(X \sqcup Y)(f) &= bind^m(X)(f) \sqcup^m bind^m(Y)(f) \end{aligned}$$

## 8.3 Flow Sensitivity Galois Transformer

The flow sensitivity monad transformer, shown in Figure 12, is a unique monad transformer that combines state and nondeterminism effects, and does not arise naturally from

$$\begin{aligned}
\mathcal{P}^t &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\
\mathcal{P}^t(m)(A) &:= m(\mathcal{P}(A)) \\
\Pi^{\mathcal{P}^t} &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\
\Pi^{\mathcal{P}^t}(\Sigma)(A) &:= \Sigma(\mathcal{P}(A))
\end{aligned}$$

---


$$\begin{aligned}
return^{\mathcal{P}^t} &: \forall A, A \rightarrow \mathcal{P}^t(m)(A) \\
return^{\mathcal{P}^t}(x) &:= return^m(\{x\}) \\
bind^{\mathcal{P}^t} &: \forall AB, \mathcal{P}^t(m)(A) \rightarrow (A \rightarrow \mathcal{P}^t(m)(B)) \rightarrow \mathcal{P}^t(m)(B) \\
bind^{\mathcal{P}^t}(X)(f) &:= \mathbf{do} \\
&\quad \{x_1..x_n\} \leftarrow^m X \\
&\quad f(x_1) \sqcup^m .. \sqcup^m f(x_n) \\
get^{\mathcal{P}^t} &: \mathcal{P}^t(m)(s) \\
get^{\mathcal{P}^t} &:= s \leftarrow^m get^m; return^m(\{s\}) \\
put^{\mathcal{P}^t} &: s \rightarrow \mathcal{P}^t(m)(1) \\
put^{\mathcal{P}^t}(s) &:= u \leftarrow^m put^m(x); return^m(\{u\}) \\
mzero^{\mathcal{P}^t} &: \forall A, \mathcal{P}^t(m)(A) \\
mzero^{\mathcal{P}^t} &:= \perp^m \\
\_ \langle + \rangle^{\mathcal{P}^t} \_ &: \forall A, \mathcal{P}^t(m)(A) x \mathcal{P}^t(m)(A) \rightarrow \mathcal{P}^t(m)(A) \\
X_1 \langle + \rangle^{\mathcal{P}^t} X_2 &:= X_1 \sqcup^m X_2 \\
\alpha^{\mathcal{P}^t} &: \forall AB, \\
&\quad (\Pi^{\mathcal{P}^t}(\Sigma^m)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma^m)(B)) \rightarrow (A \rightarrow \mathcal{P}^t(m)(B)) \\
\alpha^{\mathcal{P}^t}(f)(x) &:= \alpha^m(f)(\{x\}) \\
\gamma^{\mathcal{P}^t} &: \forall AB, \\
&\quad (A \rightarrow \mathcal{P}^t(m)(B)) \rightarrow (\Pi^{\mathcal{P}^t}(\Sigma^m)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma^m)(B)) \\
\gamma^{\mathcal{P}^t}(f) &:= \\
&\quad \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^m .. \sqcup^m f(x_n))
\end{aligned}$$

**Figure 11.** Nondeterminism Galois Transformer

composing vanilla nondeterminism and state transformers. The finite map in the definition of  $F^t[s]$  is what yields flow sensitivity when instantiated to a monadic interpreter. After instantiation,  $F^t[s](m)(A)$  will be  $\widehat{\mathbf{Store}} \rightarrow [Exp \times \widehat{\Psi} \rightarrow \widehat{\mathbf{Store}}]$ , which maps each possible expression and context to a unique abstract store.

Like nondeterminism,  $return^{\mathcal{P}^t}$  and  $bind^{\mathcal{P}^t}$  require that  $m$  be both a monad and a *join-semilattice functor*. This functoriality of  $m$  is instantiated with  $[_ \mapsto s]$  using the usual join-semilattice on finite maps:  $\{\}$  for  $\perp$  and:

$$Y \sqcup Z := \{x \mapsto y \sqcup z \mid \{x \mapsto y\} \in X \wedge \{x \mapsto z\} \in Y\}$$

$get^{\mathcal{P}^t}$  and  $put^{\mathcal{P}^t}$  require that  $m$  be a monad. Like the nondeterminism Galois transformer,  $\alpha^{\mathcal{P}^t}$  and  $\gamma^{\mathcal{P}^t}$  require that  $m$  maps to  $\Sigma^m$  via Galois connection.

$$\begin{aligned}
F^t[s] &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\
F^t[s](m)(A) &:= s \rightarrow m([A \mapsto s]) \\
\Pi^{F^t[s]} &: (Type \rightarrow Type) \rightarrow (Type \rightarrow Type) \\
\Pi^{F^t[s]}(\Sigma)(A) &:= \Sigma([A \mapsto s])
\end{aligned}$$

---


$$\begin{aligned}
return^{F^t} &: \forall A, A \rightarrow F^t[s](m)(A) \\
return^{F^t}(x)(s) &:= return^m(\{x \mapsto s\}) \\
bind^{F^t} &: \forall AB, F^t[s](m)(A) \rightarrow (A \rightarrow F^t[s](m)(B)) \rightarrow F^t[s](m)(B) \\
bind^{F^t}(X)(f)(s) &:= \mathbf{do} \\
&\quad \{x_1 \mapsto s_1 .. x_n \mapsto s_n\} \leftarrow^m X(s) \\
&\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n) \\
get^{F^t} &: F^t[s](m)(s) \\
get^{F^t}(s) &:= return^m\{s \mapsto s\} \\
put^{F^t} &: s \rightarrow F^t[s](m)(1) \\
put^{F^t}(s')(s) &:= return^m\{1 \mapsto s'\} \\
mzero^{F^t} &: \forall A, F^t[s](m)(A) \\
mzero^{F^t}(s) &:= \perp^m \\
\_ \langle + \rangle^{F^t} \_ &: \forall A, F^t[s](m)(A) x F^t[s](m)(A) \rightarrow F^t[s](m)(A) \\
(X_1 \langle + \rangle^{F^t} X_2)(s) &:= X_1(s) \sqcup^m X_2(s) \\
\alpha^{F^t} &: \forall AB, \\
&\quad (\Pi^{F^t[s]}(\Sigma^m)(A) \rightarrow \Pi^{F^t[s]}(\Sigma^m)(B)) \rightarrow (A \rightarrow F^t[s](m)(B)) \\
\alpha^{F^t}(f)(x)(s) &:= \alpha^m(f)(\{x \mapsto s\}) \\
\gamma^{F^t} &: \forall AB, \\
&\quad (A \rightarrow F^t[s](m)(B)) \rightarrow (\Pi^{F^t[s]}(\Sigma^m)(A) \rightarrow \Pi^{F^t[s]}(\Sigma^m)(B)) \\
\gamma^{F^t}(f) &:= \\
&\quad \gamma^m(\lambda(\{x_1 \mapsto s_1 .. x_n \mapsto s_n\}).f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n))
\end{aligned}$$

**Figure 12.** Flow Sensitivity Galois Transformer

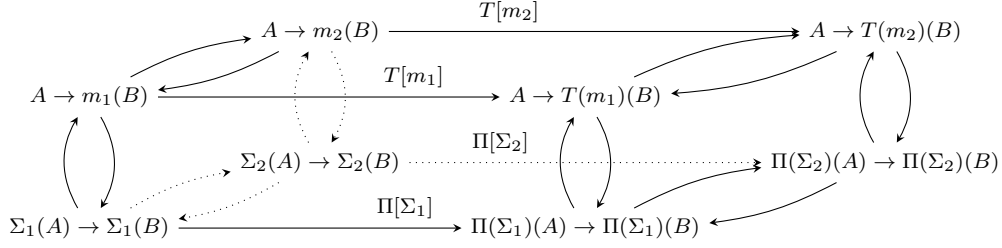
**Lemma 2.** *[ $F^t$  laws]  $bind^{F^t}$  and  $return^{F^t}$  satisfy monad laws,  $get^{F^t}$  and  $put^{F^t}$  satisfy state monad laws, and  $mzero^{F^t}$  and  $\langle + \rangle^{F^t}$  satisfy nondeterminism monad laws.*

See our proofs in the extended version of the paper. Monad and nondeterminism laws are analogous to those for nondeterminism, and also rely on the join-semilattice functoriality of  $m$ . State monad laws are proved by calculation.

## 8.4 Galois Transformers

The capstone of our framework is the fact that monad transformers  $S^t[s]$ ,  $\mathcal{P}^t$  and  $F^t[s]$  are also *Galois transformers*.

**Definition 1.** *A monad transformer  $T$  is a Galois transformer with transition system  $\Pi$  if:*



**Figure 13.** Galois Transformer Commuting Cube of Abstractions

1.  $T$  transports Galois connections between monads  $m_1$  and  $m_2$  into Galois connections between  $T(m_1)$  and  $T(m_2)$ :

$$\begin{array}{ccc}
 A \rightarrow m_2(B) & \xrightarrow{T[m_2]} & A \rightarrow T(m_2)(B) \\
 \alpha^m \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \gamma^m & & T[\alpha^m] \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) T[\gamma^m] \\
 A \rightarrow m_1(B) & \xrightarrow{T[m_1]} & A \rightarrow T(m_1)(B)
 \end{array}$$

$T[m]$  must be monotonic, and  $T$  must commute with Galois connections, that is for all  $f : A \rightarrow m_1(B)$ :

$$T[m_2](\alpha^m(f)) = T[\alpha^m](T[m_1](f))$$

2.  $\Pi$  transports Galois connections between induced transition systems  $\Sigma_1$  and  $\Sigma_2$  into Galois connections between  $\Pi(\Sigma_1)$  and  $\Pi(\Sigma_2)$ :

$$\begin{array}{ccc}
 \Sigma_2(A) \rightarrow \Sigma_2(B) & \xrightarrow{\Pi[\Sigma_2]} & \Pi(\Sigma_2)(A) \rightarrow \Pi(\Sigma_2)(B) \\
 \alpha^\Sigma \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \gamma^\Sigma & & \Pi[\alpha^\Sigma] \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \Pi[\gamma^\Sigma] \\
 \Sigma_1(A) \rightarrow \Sigma_1(B) & \xrightarrow{\Pi[\Sigma_1]} & \Pi(\Sigma_1)(A) \rightarrow \Pi(\Sigma_1)(B)
 \end{array}$$

$\Pi[\Sigma]$  must be monotonic, and  $\Pi$  must commute with Galois connections, that is for all  $f : \Sigma_1(A) \rightarrow \Sigma_1(B)$ :

$$\Pi[\Sigma_2](\alpha^\Sigma(f)) = \Pi[\alpha^\Sigma](\Pi[\Sigma_1](f))$$

3.  $T$  and  $\Pi$  transport transition system mappings between  $m$  and  $\Sigma$  into transition system mappings between  $T(m)$  and  $\Pi(\Sigma)$ :

$$\begin{array}{ccc}
 A \rightarrow m(B) & \xrightarrow{T[m]} & A \rightarrow T(m)(B) \\
 \alpha^{\Sigma \leftrightarrow m} \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \gamma^{\Sigma \leftrightarrow m} & & T[\alpha^{\Sigma \leftrightarrow m}] \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) T[\gamma^{\Sigma \leftrightarrow m}] \\
 \Sigma(A) \rightarrow \Sigma(B) & \xrightarrow{\Pi[\Sigma]} & \Pi(\Sigma)(A) \rightarrow \Pi(\Sigma)(B)
 \end{array}$$

$T[\gamma^{\Sigma \leftrightarrow m}]$  must commute asymmetrically (in the partial order) with  $T$  and  $\Pi$ , that is for all functions  $f : A \rightarrow m(B)$ :

$$\Pi[\Sigma](\gamma^{\Sigma \leftrightarrow m}(f)) \subseteq T[\gamma^{\Sigma \leftrightarrow m}](T[m](f))$$

**Lemma 3** (Galois Transformer Properties).  $S^t[s]$ ,  $\mathcal{P}^t$  and  $F^t[s]$  are Galois transformers.

Definitions for  $\alpha^{\Sigma \leftrightarrow \gamma}$  and  $\gamma^{\Sigma \leftrightarrow \gamma}$  from property (3) are shown in Figures 10, 11 and 12. Definitions of other Galois connections and commutativity proofs are given in the appendix.

These three properties of Galois transformers snap together in a three-dimensional diagram, shown in Figure 13 which relates abstractions between monads  $m_1$  and  $m_2$  and their transition systems  $\Sigma_1$  and  $\Sigma_2$  to their actions under  $T$  and  $\Pi$ . The left-hand side of the cube is a commuting square of abstractions between  $m_1$ ,  $m_2$ ,  $\Sigma_1$  and  $\Sigma_2$ . The right-hand side of the cube is constructed from the composition of properties (1) through (3) as the front, top, back, and bottom faces of the cube, and is a commuting square of abstractions between  $T(m_1)$ ,  $T(m_2)$ ,  $\Pi(\Sigma_1)$  and  $\Pi(\Sigma_2)$ . The whole cube commutes, by combining the commuting properties of the left face and the commuting properties of (1) through (3).

**Theorem 1.** If  $T$  is a Galois transformer with transition system  $\Pi$ , given a commuting square of abstractions between monads  $m_1$  and  $m_2$  and their transition systems  $\Sigma_1$  and  $\Sigma_2$ ,  $T$  and  $\Pi$  construct a commuting square of abstractions between monads  $T(m_1)$  and  $T(m_2)$  and their transition systems  $\Pi(\Sigma_1)$  and  $\Pi(\Sigma_2)$ .

The proof is the composition of Galois transformer properties, as shown in the Figure 13.

The consequence of this theorem is that any two compositions of Galois transformers  $T_1 \circ \dots \circ T_n$  and  $U_1 \circ \dots \circ U_n$  where  $U_i$  is an abstraction of  $T_i$  will yield a commuting square of abstractions between monads  $(T_1 \circ \dots \circ T_n)(ID)$  and  $(U_1 \circ \dots \circ U_n)(ID)$  and their induced transition systems  $(\Pi^{T_1} \circ \dots \circ \Pi^{T_n})(ID)$  and  $(\Pi^{U_1} \circ \dots \circ \Pi^{U_n})(ID)$ . This is the first step in proving the resulting abstract interpreter correct; we need to establish a commuting square of abstractions between a concrete monad, an abstract monad, and their induced concrete and abstract transition systems.

## 8.5 End-to-End Correctness with Galois Transformers

In the setting of abstract interpretation, we instantiate the Galois transformer framework described above with two compositions of monad transformers yielding a commuting square of abstractions between the concrete monad  $M$ , the

abstract monad  $\widehat{M}$ , and concrete and abstract transition systems  $\Sigma$  and  $\widehat{\Sigma}$ :

$$\begin{array}{ccc}
Exp \rightarrow M(Exp) & \xrightarrow{\alpha^M} & Exp \rightarrow \widehat{M}(Exp) \\
\alpha_{\Sigma \leftrightarrow M} \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \gamma_{\Sigma \leftrightarrow M} & \gamma^M & \alpha_{\widehat{\Sigma} \leftrightarrow \widehat{M}} \left( \begin{array}{c} \uparrow \\ \downarrow \end{array} \right) \gamma_{\widehat{\Sigma} \leftrightarrow \widehat{M}} \\
\Sigma(Exp) \rightarrow \Sigma(Exp) & \xrightarrow{\alpha^\Sigma} & \widehat{\Sigma}(Exp) \rightarrow \widehat{\Sigma}(Exp) \\
& \gamma^\Sigma &
\end{array}$$

This diagram shows how to relate monadic interpreters to transition systems (the vertical axis of the diagram), and concrete semantics to abstract semantics (the horizontal axis of the diagram). The top half is where we write the monadic interpreter, and the bottom half is where we execute the analysis as the least-fixed point of a transition system.

We use this commuting square to systematically relate a recovered collecting semantics with the induced abstract transition system in the following theorem:

**Theorem 2.** *Given a commuting square of abstraction between  $M$ ,  $\widehat{M}$ ,  $\Sigma$  and  $\widehat{\Sigma}$ , and a generic monadic interpreter  $step^m$ , if  $collect = \gamma^{\Sigma \leftrightarrow M}(step^m[M])$  recovers the collecting semantics, then  $analysis = \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}}(step^m[\widehat{M}])$  is a sound abstraction of the collecting semantics.*

*Proof.* Given that  $step^m$  is monotonic in the monad parameter  $m$ , instantiating it with  $M$  and  $\widehat{M}$  will result in:

$$\alpha^M(step^m[M]) \sqsubseteq step^m[\widehat{M}]$$

Transporting through  $\gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}}$ , which is monotonic by virtue of forming a Galois connection with  $\alpha^{\widehat{\Sigma} \leftrightarrow \widehat{M}}$ , we have:

$$(1) \quad \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}}(\alpha^M(step^m[M])) \sqsubseteq \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}}(step^m[\widehat{M}]) = analysis$$

Next, we abstract the recovered collecting semantics to form its best specification for abstraction:

$$(2) \quad \alpha^{\widehat{\Sigma}}(collect) = \alpha^{\widehat{\Sigma}}(\gamma^{\Sigma \leftrightarrow M}(step^m[M]))$$

Finally, we exploit the commutativity of the square of abstractions between  $M$ ,  $\widehat{M}$ ,  $\Sigma$  and  $\widehat{\Sigma}$  to relate the recovered collecting semantics with the abstract monadic semantics:

$$(3) \quad \alpha^{\widehat{\Sigma}}(\gamma^{\Sigma \leftrightarrow M}(step^m[M])) \sqsubseteq \gamma^{\widehat{\Sigma} \leftrightarrow \widehat{M}}(\alpha^M(step^m[M]))$$

The transitive combination of (1), (2) and (3) establishes the soundness of the derived abstract execution system w.r.t. the recovered collecting semantics:  $\alpha^{\widehat{\Sigma}}(collect) \sqsubseteq analysis$ .  $\square$

This theorem proves Proposition 1 in Section 6.3 after instantiating the example to the Galois transformer framework.

## 8.6 Applying the Framework to Our Semantics

Our setting is the ground-truth semantics  $\_ \rightsquigarrow^{gc} \_$  from Section 2 and the generic interpreter  $step^m$  from Section 5.

To recover the concrete collecting semantics, we instantiate  $step^m$  to the concrete parameters for the domain and time from Section 6.1, and synthesize the monad as a combination of state and nondeterminism Galois transformers:

$$M := (S^t[\Psi] \circ S^t[Store] \circ \mathcal{P}^t)(ID)$$

To recover a path-sensitive abstract interpreter we instantiate  $step^m$  to the abstract parameters for the domain and time from Section 6.2, and synthesize the monad as a combination of state and nondeterminism Galois transformers:

$$\widehat{M} := (S^t[\widehat{\Psi}] \circ S^t[\widehat{Store}] \circ \mathcal{P}^t)(ID)$$

which abstracts  $M$  piecewise. Both the implementation and correctness of the induced abstract transition system are constructed for free by Theorems 1 and 2.

To recover a flow-sensitive abstract interpreter we synthesize the monad as a combination of state and flow-sensitive Galois transformers:

$$\widehat{M}^{fs} := (S^t[\widehat{\Psi}] \circ F^t[\widehat{Store}])(ID)$$

which abstracts  $\widehat{M}$  piecewise.

Finally, to recover a flow-insensitive abstract interpreter we synthesize the monad as a permuted combination of state and nondeterminism Galois transformers:

$$\widehat{M}^{ps} := (S^t[\widehat{\Psi}] \circ \mathcal{P}^t \circ S^t[\widehat{Store}])(ID)$$

which abstracts  $\widehat{M}^{ps}$  piecewise.

## 8.7 Applying the Framework to Another Semantics

Our Galois transformers framework is semantics independent, and the proofs in Section 8.4 need not be reproved for another semantic setting. To use our framework and establish an end-to-end correctness theorem, the user must:

- Design a generic monadic interpreter for their semantics using an interface of monadic effects
- Prove their interpreter monotonic w.r.t. parameters
- Prove that the induced concrete transition system recovers the concrete collecting semantics of interest.

The user then enjoys the following for free:

- A combination of state, nondeterminism and flow-sensitive Galois transformers which supports the monadic effect interface unique to the semantics.
- The ability to rearrange monad transformers to recover variations in path and flow sensitivities.
- An induced, executable abstract interpreter for each stack of monad transformers.
- A proof that each induced abstract interpreter is a sound abstraction of the collecting semantics, as a result of Theorems 1 and 2.

## 9. Implementation

We have implemented our framework in Haskell and applied it to compute analyses for  $\lambda$ IF. Our implementation provides path sensitivity, flow sensitivity, and flow insensitivity as a semantics-independent monad library. The code shares a striking resemblance with the math.

Our implementation is suitable for prototyping and exploring the design space of static analyzers. Our analyzer supports exponentially more compositions of analysis features than any current analyzer. For example, our implementation is the first which can combine arbitrary choices in call-site, object, path and flow sensitivities. Furthermore, the user can choose different path and flow sensitivities independently for each component of the state space.

Our implementation `maam` supports command-line flags for garbage collection, mCFA, call-site sensitivity, object sensitivity, and path and flow sensitivity.

```
./maam prog.lam --gc --mcfa --kdfa=1 --ocfa=2
--data-store=flow-sen --stack-store=path-sen
```

Each flag is implemented independently of each other applied to a single parameterized monadic interpreter. Furthermore, using Galois transformers allows us to prove each combination correct in one fell swoop.

A developer wishing to use our library to develop analyzers for their language of choice inherits as much of the analysis infrastructure as possible. We provide call-site, object, path and flow sensitivities as language-independent libraries. To support analysis for a new language a developer need only implement:

- A monadic semantics for their language, using state and nondeterminism effects.
- The abstract value domain, and optionally the concrete value domain if they wish to recover concrete execution.
- Intentional optimizations for their semantics like garbage collection and mcfa.

The developer then receives the following for free through our analysis library:

- A family of monads which implement their effect interface and give different path and flow sensitivities.
- Mechanisms for call-site and object sensitivities.
- An execution engine for each monad to drive the analysis.

Not only is a developer able to reuse our implementation of call-site, object, path and flow sensitivities, they need not understand the execution machinery or soundness proofs for them either. They need only verify that their monadic semantics is monotonic w.r.t. the analysis parameters, and that their abstract value domain forms a Galois connection. The execution and correctness of the final analyzer is constructed automatically given these two properties.

Our implementation is publicly available and can be installed as a cabal package: `cabal install maam`.

## 10. Related Work

*Overview* Program analysis comes in many forms such as points-to [1], flow [10], or shape analysis [2], and the literature is vast. (See Hind [9], Midtgaard [13] for surveys.) Much of the research has focused on developing families or frameworks of analyses that endow the abstraction with a number of knobs, levers, and dials to tune precision and compute efficiently (some examples include Milanova et al. [15], Nielson and Nielson [17], Shivers [21], Van Horn and Might [23]; there are many more). These parameters come in various forms with overloaded meanings such as object [15, 22], context [20, 21], path [6], and heap [23] sensitivities, or some combination thereof [11].

These various forms can all be cast in the theory of abstraction interpretation of Cousot and Cousot [4, 5] and understood as computable approximations of an underlying concrete interpreter. Our work demonstrates that if this underlying concrete interpreter is written in monadic style, monad transformers are a useful way to organize and compose these various kinds of program abstractions in a modular and language-independent way.

This work is inspired by the trifecta combination of Cousot and Cousot’s theory of abstract interpretation based on Galois connections [3–5], Moggi’s original monad transformers [16] which were later popularized in Liang et al.’s *Monad Transformers and Modular Interpreters* [12], and Sergey et al.’s *Monadic Abstract Interpreters* [19].

Liang et al. [12] first demonstrated how monad transformers could be used to define building blocks for constructing (concrete) interpreters. Their interpreter monad *InterpM* bears a strong resemblance to ours. We show this “building blocks” approach to interpreter construction also extends to *abstract* interpreter construction using Galois transformers. Moreover, we show that these monad transformers can be proved sound via a Galois connection to their concrete counterparts, ensuring the soundness of any stack built from sound blocks of Galois transformers. Soundness proofs of various forms of analysis are notoriously brittle with respect to language and analysis features. A reusable framework of Galois transformers offers a potential way forward for a modular metatheory of program analysis.

Cousot [3] develops a “calculational approach” to analysis design whereby analyses are not designed and then verified *post facto*, but rather derived by positing an abstraction and calculating it from the concrete interpreter using Galois connections. These calculations are done by hand. Our approach offers the ability to automate the calculation process for a limited set of abstractions for small-step state machines, where the abstractions are correct-by-construction through the composition of monad transformers.

We build directly on the work of Abstracting Abstract Machines (AAM) by Van Horn and Might [23] and Smaragdakis et al. [22] in our parameterization of abstract time to achieve call-site and object sensitivity. We follow the AAM

philosophy of instrumenting a concrete semantics *first* and performing a systematic abstraction *second*. This greatly simplifies the Galois connection arguments during systematic abstraction, at the cost of proving the correctness of the instrumented semantics.

**Monadic Abstract Interpreters** Sergey et al. first introduced the concept of writing abstract interpreters in monadic style in *Monadic Abstract Interpreters* (MAI) [19], where variations in analysis are also recovered through monads.

In MAI, the framework's interface is based on *denotation functions* for every syntactic form of the language. The denotation functions in MAI are language-specific and specialized to their example language. MAI uses a single monad stack fixed to the denotation function interface: state on top of list. New analyses are achieved through multiple denotation functions into this single monad. Analyses in MAI are all fixed to be path-sensitive, and the methodology for incorporating other path or flow properties is to surgically instrument the execution of the analysis with a custom Galois connection. Lastly, the framework provides no reasoning principles or proofs of soundness for the resulting analysis. A user of MAI must inline the definitions of each analysis and prove each implementation correct from scratch.

Our framework is based on state and nondeterminism *monadic effects*. This interface comes equipped with laws, allowing one to verify the correctness of a monadic interpreter independent of a particular monad. State and nondeterminism monadic effects capture arbitrary small-step relational semantics, and are language independent. Because we place the monadic interpreter behind an interface of effects with laws, we are able to introduce language-independent monads which capture flow-sensitivity and flow-insensitivity, and we show how to compose these features with other analysis design choices. The monadic effect interface also allows us to separate the monad from the abstract domain. Finally, our framework is compositional through the use of monad transformers, and constructs execution engines and end-to-end soundness proofs for free.

**Widening for Control-Flow** Hardekopf et al. also introduce a unifying account of control flow properties in *Widening for Control-Flow* (WCF) [8], accounting for path, flow and call-site sensitivities. WCF achieves this through an instrumentation of the abstract machine's state space which is allowed to track arbitrary contextual information, up to the path-history of the entire execution. WCF also develops a modular proof framework, proving the bulk of soundness proofs for each instantiation of the instrumentation at once.

Our work achieves similar goals, although isolating path and flow sensitivity is not our primary objective. While WCF is based on a language-dependent instrumentation of the semantics, we achieve variations in path and flow sensitivity by modifying control properties of the interpreter through language-independent monads.

Particular strengths of WCF are the wide range of choices for control-flow sensitivity which are shown to be implementable within the design, and the modular proof framework. For example, WCF is able to also account for call-site sensitivity through their design; we must account for call-site sensitivity through a different mechanism.

Particular strengths of our work is the understanding of path and flow sensitivity not through instrumentation but through semantics-independent control properties of the interpreter, and also a modular proof framework, although modular in a different sense from WCF. We also show how to compose different path and flow sensitivity choices for independent components of the state space, like a flow-sensitive data-store and path-sensitive stack-store, for example.

## 11. Conclusion

We have shown that *Galois transformers*, monad transformers that transport Galois connections and mappings to an executable transition system, are effective, language-independent building blocks for constructing program analyzers, and form the basis of a modular, reusable and composable metatheory for program analysis.

In the end, we hope language independent characterizations of analysis ingredients will both facilitate the systematic construction of program analyses and bridge the gap between various communities which often work in isolation.

## Acknowledgments

This material is partially based on research sponsored by DARPA under agreements number AFRL FA8750-15-2-0092 and FA8750-12-2-0106 and by NSF under CAREER grant 1350344. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

## References

- [1] L. O. Andersen. *Program Analysis and Specialization for the C Programming Language*. PhD thesis, DIKU, University of Copenhagen, 1994.
- [2] D. R. Chase, M. Wegman, and F. K. Zadeck. Analysis of pointers and structures. PLDI '90. ACM, 1990.
- [3] P. Cousot. The calculational design of a generic abstract interpreter. In *Calculational System Design*. NATO ASI Series F. IOS Press, Amsterdam, 1999.
- [4] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. POPL '77. ACM, 1977.
- [5] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. POPL '79. ACM, 1979.
- [6] M. Das, S. Lerner, and M. Seigle. ESP: Path-sensitive program verification in polynomial time. PLDI '02. ACM, 2002.
- [7] J. Gibbons and R. Hinze. Just do it: Simple monadic equational reasoning. ICFP '11. ACM, 2011.

- [8] B. Hardekopf, B. Wiedermann, B. Churchill, and V. Kashyap. Widening for Control-Flow. VMCAI '14. Springer Berlin Heidelberg, 2014.
- [9] M. Hind. Pointer analysis: haven't we solved this problem yet? PASTE '01. ACM, 2001.
- [10] N. D. Jones. Flow analysis of lambda expressions (preliminary version). ICALP '81. Springer-Verlag, 1981.
- [11] G. Kastrinis and Y. Smaragdakis. Hybrid context-sensitivity for points-to analysis. PLDI '13. ACM, 2013.
- [12] S. Liang, P. Hudak, and M. Jones. Monad transformers and modular interpreters. POPL '95. ACM, 1995.
- [13] J. Midtgaard. Control-flow analysis of functional programs. *ACM Comput. Surv.*, 2012.
- [14] M. Might and O. Shivers. Improving flow analyses via  $\Gamma$ CFA: Abstract garbage collection and counting. ICFP '06, 2006.
- [15] A. Milanova, A. Rountev, and B. G. Ryder. Parameterized object sensitivity for points-to analysis for Java. *ACM Trans. Softw. Eng. Methodol.*, 2005.
- [16] E. Moggi. An abstract view of programming languages. Technical report, Edinburgh University, 1989.
- [17] F. Nielson and H. R. Nielson. Infinitary control flow analysis: a collecting semantics for closure analysis. POPL '97. ACM, 1997.
- [18] F. Nielson, H. R. Nielson, and C. Hankin. *Principles of Program Analysis*. Springer-Verlag, 1999.
- [19] I. Sergey, D. Devriese, M. Might, J. Midtgaard, D. Darais, D. Clarke, and F. Piessens. Monadic abstract interpreters. PLDI '13. ACM, 2013.
- [20] M. Sharir and A. Pnueli. *Two Approaches to Interprocedural Data Flow Analysis*, chapter 7. Prentice-Hall, Inc., 1981.
- [21] O. Shivers. *Control-flow analysis of higher-order languages*. PhD thesis, Carnegie Mellon University, 1991.
- [22] Y. Smaragdakis, M. Bravenboer, and O. Lhoták. Pick your contexts well: Understanding object-sensitivity. POPL '11. ACM, 2011.
- [23] D. Van Horn and M. Might. Abstracting abstract machines. ICFP '10. ACM, 2010.

## A. Proofs

### A.1 Lemma 3 [ Galois Transformers ] (Section 8.4)

**State**  $S^t[s]$  is a Galois transformer. Recall the definition of  $S^t[s]$  and  $\Pi^{S^t}[s]$ :

$$S^t[s](m)(A) := s \rightarrow m(A \times s)$$

$$\Pi^{S^t}[s](\Sigma)(A) := \Sigma(A \times s) \rightarrow \Sigma(A \times s)$$

**State Property (1):** The action  $S^t[s]$  on functions:

$$S^t[s] : (A \rightarrow m(B)) \rightarrow A \rightarrow S^t[s](m)(B)$$

$$S^t[s](f)(x)(s) := y \leftarrow^m f(x) ; \text{return}^m(y, s)$$

To transport Galois connections, we assume a Galois connection  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  and define  $\alpha$  and  $\gamma$ :

$$\alpha : (A \rightarrow S^t[s](m_1)(B)) \rightarrow A \rightarrow S^t[s](m_2)(B)$$

$$\alpha(f)(x)(s) := \alpha^m(\lambda(x, s).f(x)(s))(x, s)$$

$$\gamma : (A \rightarrow S^t[s](m_2)(B)) \rightarrow A \rightarrow S^t[s](m_1)(B)$$

$$\gamma(f)(x)(s) := \gamma^m(\lambda(x, s).f(x)(s))(x, s)$$

$\alpha$  and  $\gamma$  are monotonic by inspection, and extensive and reductive:

$$\begin{aligned} \text{extensive} : \forall fxs, f(x)(s) \sqsubseteq \gamma(\alpha(f))(x)(s) \\ \gamma(\alpha(f))(x)(s) \\ &= \gamma^m(\lambda(x, s).\alpha^m(\lambda(x, s).f(x)(s))(x, s))(x, s) \\ &\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &= \gamma^m(\alpha^m(\lambda(x, s).f(x)(s)))(x, s) \quad \wr \eta\text{-reduction} \wr \\ &\sqsupseteq (\lambda(x, s).f(x)(s))(x, s) \quad \wr \gamma^m \circ \alpha^m \text{ extensive} \wr \\ &= f(x)(s) \quad \wr \beta\text{-reduction} \wr \quad \blacksquare \\ \text{reductive} : \forall fxs, \alpha(\gamma(f))(x)(s) \sqsubseteq f(x)(s) \\ \alpha(\gamma(f))(x)(s) \\ &= \alpha^m(\lambda(x, s).\gamma^m(\lambda(x, s).f(x)(s))(x, s))(x, s) \\ &\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &= \alpha^m(\gamma^m(\lambda(x, s).f(x)(s))(x, s))(x, s) \quad \wr \eta\text{-reduction} \wr \\ &\sqsubseteq (\lambda(x, s).f(x)(s))(x, s) \quad \wr \alpha^m \circ \gamma^m \text{ reductive} \wr \\ &= f(x)(s) \quad \wr \beta\text{-reduction} \wr \quad \blacksquare \end{aligned}$$

Finally, Property (1) commutes, assuming that the Galois connection  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  is homomorphic:

$$\begin{aligned} \text{goal} : S^t[s](m_2)(\alpha^m(f))(x)(s) &= \alpha(S^t[s](m_1)(f))(x)(s) \\ \alpha(S^t[s](m_1)(f))(x)(s) \\ &= \alpha^m(\lambda(x, s).y \leftarrow^{m_1} f(x) ; \text{return}^{m_1}(y, s))(s, x) \\ &\quad \wr \text{definition of } \alpha \text{ and } S^t[s][m_1] \wr \\ &= (\lambda(x, s).y \leftarrow^{m_1} \alpha^m(f)(x) ; \text{return}^{m_2}(y, s))(s, x) \\ &\quad \wr \alpha^m \text{ homomorphic on } \text{bind}^{m_1} \text{ and } \text{return}^{m_1} \wr \\ &= y \leftarrow^{m_2} \alpha^m(f)(x) ; \text{return}^{m_2}(y, s) \quad \wr \beta\text{-reduction} \wr \\ &= S^t[s](m_2)(\alpha^m(f))(s)(x) \quad \wr \text{definition of } S^t[s] \wr \quad \blacksquare \end{aligned}$$

**State Property (2):** The action  $\Pi^{S^t}[s]$  on functions uses the mapping to monadic functions defined in Property (3):

$$\Pi^{S^t}[s] : (\Sigma(A) \rightarrow \Sigma(B)) \rightarrow \Pi^{S^t}[s](\Sigma)(A) \rightarrow \Pi^{S^t}[s](\Sigma)(B)$$

$$\Pi^{S^t}[s](f)(\varsigma) := \gamma^{\Sigma \leftrightarrow m}(S^t[s](\alpha^{\Sigma \leftrightarrow m}(f)))(\varsigma)$$

To transport Galois connections, we assume a Galois connection  $\Sigma_1(A) \rightarrow \Sigma_1(B) \xleftarrow[\alpha^\Sigma]{\gamma^\Sigma} \Sigma_2(A) \rightarrow \Sigma_2(B)$  and define  $\alpha$



and  $\gamma$  as instantiations of  $\alpha^\Sigma$  and  $\gamma^\Sigma$ :

$$\begin{aligned} \alpha &: (\Pi^{S^t}[s](\Sigma_1)(A) \rightarrow \Pi^{S^t}[s](\Sigma_1)(B)) \\ &\rightarrow \Pi^{S^t}[s](\Sigma_2)(A) \rightarrow \Pi^{S^t}[s](\Sigma_2)(B) \\ \gamma &: (\Pi^{S^t}[s](\Sigma_2)(A) \rightarrow \Pi^{S^t}[s](\Sigma_2)(B)) \\ &\rightarrow \Pi^{S^t}[s](\Sigma_1)(A) \rightarrow \Pi^{S^t}[s](\Sigma_1)(B) \\ \gamma(f)(\varsigma) &:= \gamma^\Sigma(f)(\varsigma) \quad \alpha(f)(\varsigma) := \alpha^\Sigma(f)(\varsigma) \end{aligned}$$

Monotonicity, reductive and extensive properties carry over by definition. Finally, Property (2) commutes, assuming that  $\alpha^\Sigma$  and  $\alpha^m$  commute with both  $\gamma^{\Sigma \leftrightarrow m}$  and  $\alpha^{\Sigma \leftrightarrow m}$ :

$$\begin{aligned} \text{goal} &: \Pi^{S^t}[s][\Sigma_2](\alpha^\Sigma(f))(\varsigma) = \alpha^\Sigma(\Pi^{S^t}[s][\Sigma_1](f))(\varsigma) \\ \alpha^\Sigma(\Pi^{S^t}[s][\Sigma_1](f)(\varsigma)) &= \alpha^\Sigma(\gamma^{\Sigma \leftrightarrow m}(S^t[s](\alpha^{\Sigma \leftrightarrow m}(f))))(\varsigma) \quad \text{\textit{definition of } } \Pi^{S^t}[s][\Sigma_1] \text{ \textit{}} \\ &= \alpha^\Sigma(\gamma^{\Sigma \leftrightarrow m}(\lambda(x)(s).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow m}(f)(x) ; \\ &\quad \text{return}^{m_1}(y, s)))(\varsigma) \quad \text{\textit{definition of } } S^t[s] \text{ \textit{}} \\ &= \gamma^{\Sigma \leftrightarrow m}(\alpha^m(\lambda(x)(s).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow m}(f)(x) ; \\ &\quad \text{return}^{m_1}(y, s)))(\varsigma) \quad \text{\textit{ } } \alpha^\Sigma \text{ and } \gamma^{\Sigma \leftrightarrow m} \text{ commute \textit{}} \\ &= \gamma^{\Sigma \leftrightarrow m}(\lambda(x)(s).y \leftarrow^{m_2} \alpha^m(\alpha^{\Sigma \leftrightarrow m}(f))(x) ; \\ &\quad \text{return}^{m_2}(y, s))(\varsigma) \quad \text{\textit{ } } \alpha^m \text{ homomorphic \textit{}} \\ &= \gamma^{\Sigma \leftrightarrow m}(\lambda(x)(s).y \leftarrow^{m_2} \alpha^{\Sigma \leftrightarrow m}(\alpha^\Sigma(f))(x) ; \\ &\quad \text{return}^{m_2}(y, s))(\varsigma) \quad \text{\textit{ } } \alpha^m \text{ and } \alpha^{\Sigma \leftrightarrow m} \text{ commute \textit{}} \\ &= \gamma^{\Sigma \leftrightarrow m}(S^t[s](\alpha^{\Sigma \leftrightarrow m}(\alpha^\Sigma(f))))(\varsigma) \quad \text{\textit{definition of } } S^t[s] \text{ \textit{}} \\ &= \Pi^{S^t}[s][\Sigma_2](\alpha^\Sigma(f))(\varsigma) \quad \text{\textit{definition of } } \Pi^{S^t}[s][\Sigma_2] \text{ \textit{}} \quad \blacksquare \end{aligned}$$

**State Property (3):** Assume a Galois connection  $\Sigma(A) \rightarrow \Sigma(B) \xleftarrow[\alpha^{\Sigma \leftrightarrow m}]{\gamma^{\Sigma \leftrightarrow m}} A \rightarrow m(B)$ . The Galois connection between  $S^t[s](m)$  and  $\Pi^{S^t}[s](\Sigma)$  is defined:

$$\begin{aligned} \alpha &: (\Pi^{S^t}[s](\Sigma)(A) \rightarrow \Pi^{S^t}[s](\Sigma)(B)) \rightarrow A \rightarrow S^t[s](m)(B) \\ \alpha(f)(x)(s) &:= \alpha^{\Sigma \leftrightarrow m}(f)(x, s) \\ \gamma &: (A \rightarrow S^t[s](m)(B)) \rightarrow \Pi^{S^t}[s](\Sigma)(A) \rightarrow \Pi^{S^t}[s](\Sigma)(B) \\ \gamma(f)(\varsigma) &:= \gamma^{\Sigma \leftrightarrow m}(\lambda(x, s) \rightarrow f(x)(s))(\varsigma) \end{aligned}$$

$\alpha$  and  $\gamma$  are monotonic by inspection, and extensive and reductive:

$$\begin{aligned} \text{extensive} &: \forall f \varsigma, f(\varsigma) \sqsubseteq \gamma(\alpha(f))(\varsigma) \\ \gamma(\alpha(f))(\varsigma) &= \gamma^{\Sigma \leftrightarrow m}(\lambda(x, s) \rightarrow \alpha^{\Sigma \leftrightarrow m}(f)(x, s))(\varsigma) \quad \text{\textit{definition of } } \alpha \text{ and } \gamma \text{ \textit{}} \\ &= \gamma^{\Sigma \leftrightarrow m}(\alpha^{\Sigma \leftrightarrow m}(f))(\varsigma) \quad \text{\textit{ } } \eta \text{-reduction \textit{}} \\ &\sqsupseteq f(\varsigma) \quad \text{\textit{ } } \gamma^{\Sigma \leftrightarrow m} \circ \alpha^{\Sigma \leftrightarrow m} \text{ extensive \textit{}} \quad \blacksquare \\ \text{reductive} &: \forall f x s, \alpha(\gamma(f))(x)(s) \sqsubseteq f(x)(s) \\ \alpha(\gamma(f))(x)(s) &= \alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(\lambda(x, s) \rightarrow f(x)(s)))(x, s) \\ &\quad \text{\textit{definition of } } \alpha \text{ and } \gamma \text{ \textit{}} \\ &\sqsubseteq (\lambda(x, s) \rightarrow f(x)(s))(x, s) \quad \text{\textit{ } } \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive \textit{}} \\ &= f(x)(s) \quad \text{\textit{ } } \beta \text{-reduction \textit{}} \quad \blacksquare \end{aligned}$$

Finally, Property (3) commutes:

$$\begin{aligned} \text{goal} &: \Pi^{S^t}[s][\Sigma](\gamma^{\Sigma \leftrightarrow m}(f))(\varsigma) \sqsubseteq \gamma(S^t[s](f))(\varsigma) \\ \Pi^{S^t}[s][\Sigma](\gamma^{\Sigma \leftrightarrow m}(f))(\varsigma) &= \gamma^{\Sigma \leftrightarrow m}(\lambda(x, s) \rightarrow S^t[s](\alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(f)))(x)(s))(\varsigma) \\ &\quad \text{\textit{definition of } } \Pi^{S^t}[s][\Sigma] \text{ \textit{}} \\ &\sqsubseteq \gamma^{\Sigma \leftrightarrow m}(\lambda(x, s) \rightarrow S^t[s](f)(x)(s))(\varsigma) \\ &\quad \text{\textit{ } } \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive \textit{}} \\ &= \gamma(S^t[s](f))(\varsigma) \quad \text{\textit{definition of } } \gamma \text{ \textit{}} \quad \blacksquare \end{aligned}$$

**Nondeterminism**  $\mathcal{P}^t$  is a Galois transformer. Recall the definition of  $\mathcal{P}^t$  and  $\Pi^{\mathcal{P}^t}$ :

$$\mathcal{P}^t(m)(A) := m(\mathcal{P}(A)) \quad \Pi^{\mathcal{P}^t}(\Sigma)(A) := \Sigma(\mathcal{P}(A))$$

**Nondeterminism Property (1):** The action  $\mathcal{P}^t$  on functions:

$$\begin{aligned} \mathcal{P}^t &: (A \rightarrow m(B)) \rightarrow A \rightarrow \mathcal{P}^t(m)(B) \\ \mathcal{P}^t(f)(x) &:= y \leftarrow^m f(x) ; \text{return}^m(\{y\}) \end{aligned}$$

To transport Galois connections, we assume a Galois connection  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  define  $\alpha$  and  $\gamma$ :

$$\begin{aligned} \alpha &: (A \rightarrow \mathcal{P}(m_1)(B)) \rightarrow A \rightarrow \mathcal{P}(m_2)(B) \\ \alpha(f)(x) &= \alpha^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x\}) \\ \gamma &: (A \rightarrow \mathcal{P}(m_2)(B)) \rightarrow A \rightarrow \mathcal{P}(m_1)(B) \\ \gamma(f)(x) &= \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n))(\{x\}) \end{aligned}$$

$\alpha$  and  $\gamma$  are monotonic by inspection, and extensive and reductive:

$$\begin{aligned} \text{extensive} &: \forall f x, f(x) \sqsubseteq \gamma(\alpha(f))(x) \\ \gamma(\alpha(f))(x) &= \gamma^m(\lambda(\{x_1..x_n\}). \\ &\quad \alpha^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_1\}) \\ &\quad \sqcup^{m_2} .. \sqcup^{m_2} \\ &\quad \alpha^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_n\}))(\{x\}) \\ &\quad \text{\textit{definition of } } \alpha \text{ and } \gamma \text{ \textit{}} \\ &= \gamma^m(\lambda(\{x_1..x_n\}). \\ &\quad (\{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_1\}) ; \alpha^m(\lambda(\{x_1..x_n\}). \\ &\quad \quad f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_1..x_n\})) \\ &\quad \sqcup^{m_2} .. \sqcup^{m_2} \\ &\quad (\{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_n\}) ; \alpha^m(\lambda(\{x_1..x_n\}). \\ &\quad \quad f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_1..x_n\}))(\{x\}) \\ &\quad \text{\textit{left-unit of } } m_2 \text{ \textit{}} \\ &\sqsupseteq \gamma^m(\lambda(\{x_1..x_n\}). \\ &\quad (\{x_1..x_n\} \leftarrow^{m_2} \alpha^m(\gamma^m(\text{return}^{m_2}(\{x_1\}))) ; \\ &\quad \quad \alpha^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_1..x_n\})) \\ &\quad \sqcup^{m_2} .. \sqcup^{m_2} \\ &\quad (\{x_1..x_n\} \leftarrow^{m_2} \alpha^m(\gamma^m(\text{return}^{m_2}(\{x_n\}))) ; \\ &\quad \quad \alpha^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))(\{x_1..x_n\}))) \\ &\quad (\{x\}) \quad \text{\textit{ } } \alpha^m \circ \gamma^m \text{ reductive \textit{}} \end{aligned}$$

$$\begin{aligned}
&= \gamma^m(\lambda(\{x_1..x_n\}). \\
&\quad (\alpha^m(\{x_1..x_n\} \leftarrow^{m_1} \text{return}^{m_1}(\{x_1\}); \\
&\quad \quad f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))) \sqcup^{m_2} .. \sqcup^{m_2} \\
&\quad (\alpha^m(\{x_1..x_n\} \leftarrow^{m_1} \text{return}^{m_1}(\{x_n\}); \\
&\quad \quad f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))) (\{x\}) \\
&\quad \wr \alpha^m \text{ and } \gamma^m \text{ homomorphic on } \text{bind}^{m_2} \text{ and } \text{return}^{m_2} \wr \\
&= \gamma^m(\alpha^m(\lambda(\{x_1..x_n\}).\{x_1..x_n\} \leftarrow \text{return}^{m_1}(\{x_1..x_n\}); \\
&\quad f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n))) (\{x\}) \\
&\quad \wr \text{join-semilattice functoriality of } m \wr \\
&\sqsubseteq \{x_1..x_n\} \leftarrow \text{return}^{m_1}(\{x\}); f(x_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n) \\
&\quad \wr \gamma^m \circ \alpha^m \text{ extensive } \wr \\
&= f(x) \quad \wr \text{left-unit of } m \wr \quad \blacksquare \\
\text{reductive} : \forall f x, \alpha(\gamma(f))(x) \sqsubseteq f(x) \\
\alpha(\gamma(f))(x) \\
&= \alpha^m(\lambda(\{x_1..x_n\}). \\
&\quad \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_1\}) \\
&\quad \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_n\})) (\{x\}) \\
&\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\
&= \alpha^m(\lambda(\{x_1..x_n\}). \\
&\quad (\{x_1..x_n\} \leftarrow^{m_1} \text{return}^{m_1}(\{x_1\}); \gamma^m(\lambda(\{x_1..x_n\}). \\
&\quad \quad f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_1..x_n\})) \\
&\quad \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad (\{x_1..x_n\} \leftarrow^{m_1} \text{return}^{m_1}(\{x_2\}); \gamma^m(\lambda(\{x_1..x_n\}). \\
&\quad \quad f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_1..x_n\})) (\{x\}) \\
&\quad \wr \text{left-unit of } m_1 \wr \\
&\sqsubseteq \alpha^m(\lambda(\{x_1..x_n\}). \\
&\quad (\{x_1..x_n\} \leftarrow^{m_1} \gamma^m(\alpha^m(\text{return}^{m_1}(\{x_1\}))); \\
&\quad \quad \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_1..x_n\})) \\
&\quad \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad (\{x_1..x_n\} \leftarrow^{m_1} \gamma^m(\alpha^m(\text{return}^{m_1}(\{x_n\}))); \\
&\quad \quad \gamma^m(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x_1..x_n\})) \\
&\quad (\{x\}) \quad \wr \gamma^m \circ \alpha^m \text{ extensive } \wr \\
&= \alpha^m(\lambda(\{x_1..x_n\}). \\
&\quad \gamma^m(\{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_1\}); f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) \\
&\quad \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad \gamma^m(\{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_1\}); f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n))) \\
&\quad (\{x\}) \quad \wr \alpha^m \text{ and } \gamma^m \text{ homomorphic on } \text{bind}^{m_1} \text{ and } \text{return}^{m_1} \wr \\
&= \alpha^m(\gamma^m(\lambda(\{x_1..x_n\}).\{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_1..x_n\}); \\
&\quad f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)) (\{x\}) \\
&\quad \wr \text{join-semilattice functoriality of } m \wr \\
&\sqsubseteq \{x_1..x_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x\}); f(x_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n) \\
&\quad \wr \alpha^m \circ \gamma^m \text{ reductive } \wr \\
&= f(x) \quad \wr \text{left-unit of } m \wr \quad \blacksquare
\end{aligned}$$

Finally, Property (1) commutes, assuming that the Galois connection  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  is homomorphic:

$$\begin{aligned}
\text{goal} : \forall f s, \mathcal{P}^t[m_2](\alpha^m(f))(x) &= \alpha(\mathcal{P}^t[m_1](f))(x) \\
\alpha(\mathcal{P}^t[m_1](f))(x) \\
&= \alpha^m(\lambda(\{x_1..x_n\}). \\
&\quad (y \leftarrow^{m_1} f(x_1); \text{return}^{m_1}(\{y\})) \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad (y \leftarrow^{m_1} f(x_n); \text{return}^{m_1}(\{y\}))) (\{x\}) \\
&\quad \wr \text{definition of } \alpha \text{ and } \mathcal{P}^t[m_1](f) \wr \\
&= y \leftarrow^{m_2} \alpha^m(f)(x); \text{return}^{m_2}(\{y\}) \\
&\quad \wr \text{homomorphic on } \text{bind}^{m_1} \text{ and } \text{return}^{m_1} \wr \\
&= \mathcal{P}^t[m_2](\alpha^m(f))(x) \quad \wr \text{definition of } \mathcal{P}^t[m_2] \wr \quad \blacksquare
\end{aligned}$$

*Nondeterminism Property (2):* The action  $\Pi^{\mathcal{P}^t}$  on functions uses the mapping to monadic functions defined in Property (3):

$$\begin{aligned}
\Pi^{\mathcal{P}^t} : (\Sigma(A) \rightarrow \Sigma(B)) &\rightarrow \Pi^{\mathcal{P}^t}(\Sigma)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma)(B) \\
\Pi^{\mathcal{P}^t}(f)(\varsigma) &:= \gamma^{\Sigma \leftrightarrow \gamma}(\mathcal{P}^t(\alpha^{\Sigma \leftrightarrow \gamma}(f)))
\end{aligned}$$

To transport Galois connections, we assume a Galois connection  $\Sigma_1(A) \rightarrow \Sigma_1(B) \xleftarrow[\alpha^\Sigma]{\gamma^\Sigma} \Sigma_2(A) \rightarrow \Sigma_2(B)$  and define  $\alpha$  and  $\gamma$  as instantiations of  $\alpha^\Sigma$  and  $\gamma^\Sigma$ :

$$\begin{aligned}
\alpha : (\Pi^{\mathcal{P}^t}(\Sigma_1)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma_1)(B)) &\rightarrow \Pi^{\mathcal{P}^t}(\Sigma_2)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma_2)(B) \\
\gamma : (\Pi^{\mathcal{P}^t}(\Sigma_2)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma_2)(B)) &\rightarrow \Pi^{\mathcal{P}^t}(\Sigma_1)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma_1)(B) \\
\alpha(f)(\varsigma) &:= \alpha^\Sigma(f)(\varsigma) \quad \gamma(f)(\varsigma) := \gamma^\Sigma(f)(\varsigma)
\end{aligned}$$

Monotonicity, reductive and extensive properties carry over by definition. Finally, Property (2) commutes, assuming that  $\alpha^\Sigma$  and  $\alpha^m$  commute with both  $\gamma^{\Sigma \leftrightarrow m}$  and  $\alpha^{\Sigma \leftrightarrow m}$ :

$$\begin{aligned}
\text{goal} : \Pi^{\mathcal{P}^t}[\Sigma_2](\alpha^\Sigma(f))(\varsigma) &= \alpha^\Sigma(\Pi^{\mathcal{P}^t}[\Sigma_1](f))(\varsigma) \\
\alpha^\Sigma(\Pi^{\mathcal{P}^t}[\Sigma_1](f))(\varsigma) \\
&= \alpha^\Sigma(\gamma^{\Sigma \leftrightarrow \gamma}(\mathcal{P}^t(\alpha^{\Sigma \leftrightarrow \gamma}(f))))(\varsigma) \quad \wr \text{definition of } \Pi^{\mathcal{P}^t} \wr \\
&= \alpha^\Sigma(\gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow \gamma}(f)(x); \text{return}^{m_1}(\{y\}))) (\varsigma) \\
&\quad \wr \text{definition of } \mathcal{P}^t \wr \\
&= \gamma^{\Sigma \leftrightarrow \gamma}(\alpha^m(\lambda(x).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow \gamma}(f)(x); \text{return}^{m_1}(\{y\}))) (\varsigma) \\
&\quad \wr \alpha^\Sigma \text{ and } \gamma^{\Sigma \leftrightarrow \gamma} \text{ commute } \wr \\
&= \gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x).y \leftarrow^{m_2} \alpha^m(\alpha^{\Sigma \leftrightarrow \gamma}(f))(x); \text{return}^{m_2}(\{y\})) (\varsigma) \\
&\quad \wr \alpha^m \text{ homomorphic on } \text{bind}^{m_1} \text{ and } \text{return}^{m_2} \wr \\
&= \gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x).y \leftarrow^{m_2} \alpha^{\Sigma \leftrightarrow \gamma}(\alpha^\Sigma(f))(x); \text{return}^{m_2}(\{y\})) (\varsigma) \\
&\quad \wr \alpha^m \text{ and } \alpha^{\Sigma \leftrightarrow \gamma} \text{ commute } \wr \\
&= \Pi^{\mathcal{P}^t}[\Sigma_2](\alpha^\Sigma(f))(\varsigma) \quad \wr \text{definition of } \Pi^{\mathcal{P}^t}[\Sigma_2] \text{ and } \alpha^\Sigma \wr \quad \blacksquare
\end{aligned}$$

*Nondeterminism Property (3):* Assume a Galois connection  $\Sigma(A) \rightarrow \Sigma(B) \xleftarrow[\alpha^{\Sigma \leftrightarrow m}]{\gamma^{\Sigma \leftrightarrow m}} A \rightarrow m(B)$ . The Galois connection between  $\mathcal{P}^t(m)$  and  $\Pi^{\mathcal{P}^t}(\Sigma)$  is:

$$\begin{aligned}
\alpha : (\Pi^{\mathcal{P}^t}(\Sigma)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma)(B)) &\rightarrow A \rightarrow \mathcal{P}^t(m)(B) \\
\alpha(f)(x) &:= \alpha^{\Sigma \leftrightarrow m}(f)(\{x\})
\end{aligned}$$

$$\begin{aligned} \gamma &: (A \rightarrow \mathcal{P}^t(m)(B)) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma)(A) \rightarrow \Pi^{\mathcal{P}^t}(\Sigma)(B) \\ \gamma(f)(s) &:= \gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^m .. \sqcup^m f(x_n))(s) \end{aligned}$$

$\alpha$  and  $\gamma$  are monotonic by inspection, and extensive and reductive:

$$\begin{aligned} \text{extensive} &: \forall f s, f(s) \sqsubseteq \gamma(\alpha(f))(s) \\ \gamma(\alpha(f))(s) &= \gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1..x_n\}). \\ &\quad \alpha^{\Sigma \leftrightarrow m}(f)(\{x_1\}) \sqcup^m .. \sqcup^m \alpha^{\Sigma \leftrightarrow m}(f)(\{x_n\}))(s) \\ &\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &= \gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1..x_n\}).\alpha^{\Sigma \leftrightarrow m}(f)(\{x_1..x_n\}))(s) \\ &\quad \wr \text{join-semilattice functoriality of } m \wr \\ &\sqsupseteq f(s) \quad \wr \gamma^{\Sigma \leftrightarrow m} \circ \alpha^{\Sigma \leftrightarrow m} \text{ extensive and } \eta \text{-reduction} \wr \quad \blacksquare \\ \text{reductive} &: \forall f x, \alpha(\gamma(f))(x) \sqsubseteq f(x) \\ \alpha(\gamma(f))(x) &= \alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1..x_n\}).f(x_1) \sqcup^m .. \sqcup^m f(x_n)))(\{x\}) \\ &\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &\sqsubseteq (\lambda(\{x_1..x_n\}).f(x_1) \sqcup^m .. \sqcup^m f(x_n))(\{x\}) \\ &\quad \wr \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive} \wr \\ &= f(x) \quad \wr \beta \text{-reduction} \wr \quad \blacksquare \end{aligned}$$

Finally, Property (3) commutes:

$$\begin{aligned} \text{goal} &: \Pi^{\mathcal{P}^t}(\gamma^{\Sigma \leftrightarrow m}(f))(s) \sqsubseteq \gamma(\mathcal{P}^t(f))(s) \\ \Pi^{\mathcal{P}^t}(\gamma^{\Sigma \leftrightarrow m}(f))(s) &= \gamma^{\Sigma \leftrightarrow m}(\mathcal{P}^t(\alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(f))))(s) \quad \wr \text{definition of } \Pi^{\mathcal{P}^t} \wr \\ &\sqsubseteq \gamma^{\Sigma \leftrightarrow m}(\mathcal{P}^t(f))(s) \quad \wr \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive} \wr \\ &= \gamma(\mathcal{P}^t(f))(s) \quad \wr \text{definition of } \gamma \wr \quad \blacksquare \end{aligned}$$

**Flow Sensitivity**  $F^t[s]$  is a Galois transformer. Recall the definition of  $F^t[s]$  and  $\Pi^{F^t}[s]$ :

$$F^t[s](m)(A) := s \rightarrow m([A \mapsto s]) \quad \Pi^{F^t}[s](\Sigma)(A) := \Sigma([A \mapsto s])$$

**Flow Sensitivity Property (I):** The action  $F^t[s]$  on functions:

$$\begin{aligned} F^t[s] &: (A \rightarrow m(B)) \rightarrow A \rightarrow F^t[s](m)(B) \\ F^t[s](f)(x)(s) &:= y \leftarrow^m f(x); \text{return}^m(\{y \mapsto s\}) \end{aligned}$$

To transport Galois connections we assume a Galois connection  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  and define  $\alpha$  and  $\gamma$ :

$$\begin{aligned} \alpha &: (A \rightarrow F^t[s](m_1)(B)) \rightarrow A \rightarrow F^t[s](m_2)(B) \\ \alpha(f)(x)(s) &:= \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n))(\{x \mapsto s\}) \\ \gamma &: (A \rightarrow F^t[s](m_2)(B)) \rightarrow A \rightarrow F^t[s](m_1)(B) \\ \gamma(f)(x)(s) &:= \gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n))(\{x \mapsto s\}) \end{aligned}$$

$\alpha$  and  $\gamma$  are monotonic by inspection.  $\alpha$  and  $\gamma$  are extensive and reductive:

$$\begin{aligned} \text{extensive} &: \forall f x s, f(x)(s) \sqsubseteq \gamma(\alpha(f))(x)(s) \\ \gamma(\alpha(f))(x)(s) &= \gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \quad f(x_1)(s_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n)(s_n))(\{x_1 \mapsto s_1\}) \\ &\quad \sqcup^{m_2} .. \sqcup^{m_2} \\ &\quad \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \quad f(x_1)(s_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n)(s_n))(\{x_n \mapsto s_n\})) \\ &\quad (\{x \mapsto s\}) \quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &\sqsupseteq \gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad (\{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_2} \\ &\quad \quad \alpha^m(\gamma^m(\text{return}^{m_2}(\{x_1 \mapsto s_1\}))))); \\ &\quad \alpha^m(f(x_1)(s_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n)(s_n))) \\ &\quad \sqcup^{m_2} .. \sqcup^{m_2} \\ &\quad (\{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_2} \\ &\quad \quad \alpha^m(\gamma^m(\text{return}^{m_2}(\{x_n \mapsto s_n\}))))); \\ &\quad \alpha^m(f(x_1)(s_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n)(s_n)))(\{x \mapsto s\}) \\ &\quad \wr \text{left-unit of } m \text{ and } \alpha^m \circ \gamma^m \text{ reductive} \wr \\ &= \gamma^m(\alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_1} \\ &\quad \quad \text{return}^{m_1}(\{x_1 \mapsto s_1..x_n \mapsto s_n\})); \\ &\quad f(x_1)(s_1) \sqcup^{m_1} .. \sqcup^{m_1} f(x_n)(s_n)))(\{x \mapsto s\}) \\ &\quad \wr \alpha^m \text{ and } \gamma^m \text{ homomorphic and join functoriality} \wr \\ &\sqsupseteq f(x)(s) \quad \wr \gamma^m \circ \alpha^m \text{ extensive and left-unit of } m \wr \quad \blacksquare \\ \text{reductive} &: \forall f x s, \alpha(\gamma(f))(x)(s) \sqsubseteq f(x)(s) \\ \alpha(\gamma(f))(x)(s) &= \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \quad f(x_1)(s_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)(s_n))(\{x_1 \mapsto s_1\}) \\ &\quad \sqcup^{m_1} .. \sqcup^{m_1} \\ &\quad \gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad \quad f(x_1)(s_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)(s_n))(\{x_n \mapsto s_n\})) \\ &\quad (\{x \mapsto s\}) \quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\ &\sqsubseteq \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\ &\quad (\{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_1} \gamma^m(\alpha^m(\text{return}^{m_1}(\{x_1 \mapsto s_1\}))))); \\ &\quad \gamma^m(f(x_1)(s_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)(s_n))) \\ &\quad \sqcup^{m_1} .. \sqcup^{m_1} \\ &\quad (\{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_1} \gamma^m(\alpha^m(\text{return}^{m_1}(\{x_n \mapsto s_n\}))))); \\ &\quad \gamma^m(f(x_1)(s_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)(s_n)))(\{x \mapsto s\}) \\ &\quad \wr \text{left-unit of } m \text{ and } \gamma^m \circ \alpha^m \text{ extensive} \wr \end{aligned}$$

$$\begin{aligned}
&= \alpha^m(\gamma^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}))) \\
&\quad \{x_1 \mapsto s_1..x_n \mapsto s_n\} \leftarrow^{m_2} \text{return}^{m_2}(\{x_1 \mapsto s_1..x_n \mapsto s_n\}); \\
&\quad f(x_1)(s_1) \sqcup^{m_2} .. \sqcup^{m_2} f(x_n)(s_n))(\{x \mapsto s\}) \\
&\quad \wr \alpha^m \text{ and } \gamma^m \text{ homomorphic and join functoriality } \wr \\
&\sqsubseteq f(x)(s) \quad \wr \alpha^m \circ \gamma^m \text{ extensive and left-unit of } m \wr \quad \blacksquare
\end{aligned}$$

Finally, Property (1) commutes, assuming that  $A \rightarrow m_1(B) \xleftarrow[\alpha^m]{\gamma^m} A \rightarrow m_2(B)$  is homomorphic:

$$\begin{aligned}
\text{goal} : \forall f s, F^t[s][m_2](\alpha^m(f))(x)(s) &= \alpha(F^t[s][m_1](f))(x)(s) \\
\alpha(F^t[s][m_1](f))(x)(s) & \\
&= \alpha^m(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\})). \\
&\quad (y \leftarrow^{m_1} f(x); \text{return}^{m_1}(y_1)(s_1)) \sqcup^{m_1} .. \sqcup^{m_1} \\
&\quad (y \leftarrow^{m_1} f(x); \text{return}^{m_1}(y_n)(s_n))(\{x \mapsto s\}) \\
&\quad \wr \text{definition of } \alpha \text{ and } F^t[s][m_1] \wr \\
&= y \leftarrow^{m_2} \alpha^m(f)(x); \text{return}^{m_2}(y)(s) \\
&\quad \wr \text{homomorphic on } \text{bind}^{m_1} \text{ and } \text{return}^{m_1} \wr \\
&= F^t[s][m_2](\alpha^m(f))(x) \quad \wr \text{definition of } F^t[s][m_2] \wr \quad \blacksquare
\end{aligned}$$

*Flow Sensitivity Property (2):* The action  $\Pi^{F^t[s]}$  on functions uses the mapping to monadic functions defined in Property (3):

$$\begin{aligned}
\Pi^{F^t[s]} : (\Sigma(A) \rightarrow \Sigma(B)) &\rightarrow \Pi^{F^t[s]}(\Sigma(A) \rightarrow \Pi^{F^t[s]}(\Sigma)(B)) \\
\Pi^{F^t[s]}(f)(s) &:= \gamma^{\Sigma \leftrightarrow \gamma}(F^t[s](\alpha^{\Sigma \leftrightarrow \gamma}(f)))
\end{aligned}$$

To transport Galois connections, we assume a Galois connection  $\Sigma_1(A) \rightarrow \Sigma_1(B) \xleftarrow[\Sigma_2]{\Sigma_1} \Sigma_2(A) \rightarrow \Sigma_2(B)$  and define  $\alpha$  and  $\gamma$  as instantiations of  $\alpha^{\Sigma}$  and  $\gamma^{\Sigma}$ :

$$\begin{aligned}
\alpha : (\Pi^{F^t[s]}(\Sigma_1)(A) \rightarrow \Pi^{F^t[s]}(\Sigma_1)(B)) & \\
&\rightarrow \Pi^{F^t[s]}(\Sigma_2)(A) \rightarrow \Pi^{F^t[s]}(\Sigma_2)(B) \\
\gamma : (\Pi^{F^t[s]}(\Sigma_2)(A) \rightarrow \Pi^{F^t[s]}(\Sigma_2)(B)) & \\
&\rightarrow \Pi^{F^t[s]}(\Sigma_1)(A) \rightarrow \Pi^{F^t[s]}(\Sigma_1)(B) \\
\alpha(f)(s) = \alpha^{\Sigma}(f)(s) \quad \gamma(f)(s) = \gamma^{\Sigma}(f)(s) &
\end{aligned}$$

Monotonicity, reductive and extensive properties carry over by definition. Finally, Property (2) commutes, assuming that  $\alpha^{\Sigma}$  and  $\alpha^m$  commute with both  $\gamma^{\Sigma \leftrightarrow m}$  and  $\alpha^{\Sigma \leftrightarrow m}$ :

$$\begin{aligned}
\text{goal} : \Pi^{F^t[s]}[\Sigma_2](\alpha^{\Sigma}(f))(s) &= \alpha^{\Sigma}(\Pi^{F^t[s]}[\Sigma_1](f))(s) \\
\alpha^{\Sigma}(\Pi^{F^t[s]}[\Sigma_1](f))(s) & \\
&= \alpha^{\Sigma}(\gamma^{\Sigma \leftrightarrow \gamma}(F^t[s](\alpha^{\Sigma \leftrightarrow \gamma}(f))))(s) \quad \wr \text{definition of } \Pi^{F^t[s]} \wr \\
&= \alpha^{\Sigma}(\gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x)(s).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow \gamma}(f)(x); \\
&\quad \text{return}^{m_1}(\{y \mapsto s\}))) (s) \quad \wr \text{definition of } F^t[s] \wr \\
&= \gamma^{\Sigma \leftrightarrow \gamma}(\alpha^m(\lambda(x)(s).y \leftarrow^{m_1} \alpha^{\Sigma \leftrightarrow \gamma}(f)(x); \\
&\quad \text{return}^{m_1}(\{y \mapsto s\}))) (s) \quad \wr \alpha^{\Sigma} \text{ and } \gamma^{\Sigma \leftrightarrow \gamma} \text{ commute } \wr
\end{aligned}$$

$$\begin{aligned}
&= \gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x)(s).y \leftarrow^{m_2} \alpha^m(\alpha^{\Sigma \leftrightarrow \gamma}(f))(x); \\
&\quad \text{return}^{m_2}(\{y \mapsto s\}))(s) \quad \wr \alpha^m \text{ homomorphic } \wr \\
&= \gamma^{\Sigma \leftrightarrow \gamma}(\lambda(x)(s).y \leftarrow^{m_2} \alpha^{\Sigma \leftrightarrow \gamma}(\alpha^{\Sigma}(f))(x); \\
&\quad \text{return}^{m_2}(\{y \mapsto s\}))(s) \quad \wr \alpha^m \text{ and } \alpha^{\Sigma \leftrightarrow \gamma} \text{ commute } \wr \\
&= \Pi^{F^t[s]}[\Sigma_2](\alpha^{\Sigma}(f))(s) \quad \wr \text{definition of } \Pi^{F^t[s]}[\Sigma_2] \text{ and } \alpha^{\Sigma} \wr \quad \blacksquare
\end{aligned}$$

*Flow Sensitivity Property (3):* Assume a Galois connection:

$$\Sigma(A) \rightarrow \Sigma(B) \xleftarrow[\alpha^{\Sigma \leftrightarrow m}]{\gamma^{\Sigma \leftrightarrow m}} A \rightarrow m(B)$$

The Galois connection between  $F^t[s](m)$  and  $\Pi^{F^t[s]}(\Sigma)$  is:

$$\begin{aligned}
\alpha : (\Pi^{F^t[s]}(\Sigma)(A) \rightarrow \Pi^{F^t[s]}(\Sigma)(B)) &\rightarrow A \rightarrow F^t[s](m)(B) \\
\alpha(f)(x)(s) &:= \alpha^{\Sigma \leftrightarrow m}(f)(\{x \mapsto s\}) \\
\gamma : (A \rightarrow F^t[s](m)(B)) &\rightarrow \Pi^{F^t[s]}(\Sigma)(A) \rightarrow \Pi^{F^t[s]}(\Sigma)(B) \\
\gamma(f)(s) &:= \gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\
&\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n))(s)
\end{aligned}$$

$\alpha$  and  $\gamma$  are monotonic by inspection.  $\alpha$  and  $\gamma$  are extensive and reductive:

$$\begin{aligned}
\text{extensive} : \forall f s, f(s) &\sqsubseteq \gamma(\alpha(f))(s) \\
\gamma(\alpha(f))(s) & \\
&= \gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\
&\quad \alpha^{\Sigma \leftrightarrow m}(f)(\{x_1 \mapsto s_1\}) \sqcup^m .. \sqcup^m \alpha^{\Sigma \leftrightarrow m}(f)(\{x_n \mapsto s_n\}))(s) \\
&\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\
&= \gamma^{\Sigma \leftrightarrow m}(\alpha^{\Sigma \leftrightarrow m}(f))(s) \quad \wr \text{join-semilattice functoriality of } m \wr \\
&\sqsupseteq f(s) \quad \wr \gamma^{\Sigma \leftrightarrow m} \circ \alpha^{\Sigma \leftrightarrow m} \text{ extensive } \wr \quad \blacksquare \\
\text{reductive} : \forall f x, \alpha(\gamma(f))(x)(s) &\sqsubseteq f(x)(s) \\
\alpha(\gamma(f))(x)(s) & \\
&= \alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\
&\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n)))(\{x \mapsto s\}) \\
&\quad \wr \text{definition of } \alpha \text{ and } \gamma \wr \\
&\sqsubseteq (\lambda(\{x_1 \mapsto s_1..x_n \mapsto s_n\}). \\
&\quad f(x_1)(s_1) \sqcup^m .. \sqcup^m f(x_n)(s_n))(\{x \mapsto s\}) \\
&\quad \wr \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive } \wr \\
&= f(x)(s) \quad \wr \beta \text{-reduction } \wr \quad \blacksquare
\end{aligned}$$

Finally, Property (3) commutes:

$$\begin{aligned}
\text{goal} : \Pi^{F^t[s]}(\gamma^{\Sigma \leftrightarrow m}(f))(s) &\sqsubseteq \gamma(F^t[s](f))(s) \\
\Pi^{F^t[s]}(\gamma^{\Sigma \leftrightarrow m}(f))(s) & \\
&= \gamma^{\Sigma \leftrightarrow m}(F^t[s](\alpha^{\Sigma \leftrightarrow m}(\gamma^{\Sigma \leftrightarrow m}(f))))(s) \quad \wr \text{definition of } \Pi^{F^t[s]} \wr \\
&\sqsubseteq \gamma^{\Sigma \leftrightarrow m}(F^t[s](f))(s) \quad \wr \alpha^{\Sigma \leftrightarrow m} \circ \gamma^{\Sigma \leftrightarrow m} \text{ reductive } \wr \\
&= \gamma(F^t[s](f))(s) \quad \wr \text{definition of } \gamma \wr \quad \blacksquare
\end{aligned}$$