A calculus of logical relations for over- and underapproximating static analyses

David A. Schmidt[1]

Kansas State University, Manhattan, Kansas, USA, and
École Polytechnique, Palaiseau, FRANCE

Abstract

Motivated by Dennis Dams's studies of over- and underapproximation of state-transition systems, we define a logical-relation calculus for Galois-connection building. The calculus lets us define overapproximating Galois connections in terms of lower powersets and underapproximating Galois connections in terms of upper powersets. Using the calculus, we synthesize Dams's most-precise over- and underapproximating transition systems and obtain proofs of their soundness and best precision as corollaries of abstract-interpretation theory. As a bonus, the calculus yields a logic that corresponds to the variant of Hennessy-Milner logic used in Dams's results. Following from a corollary, we have that Dams's most-precise approximations soundly validate the most properties that hold true for the corresponding concrete system. These results bind together abstract interpretation to abstract model checking, as intended by Dams.

Galois-connection-based *abstract interpretation* underlies most static analyses of programs [9,30,36]; it supplies machinery for synthesizing sound, abstract computation functions from a program's concrete computation functions and demonstrating when the abstract functions are as precise as possible [19,40].

Abstract interpretation is well suited to static analyses that must validate universally quantified properties (e.g., for all execution paths, there is absence of arithmetic overflow [3]). Such analyses must be *overapproximating.* In contrast, nondeterministic and reactive systems possess existential properties (e.g., there exists a path to a reset state [33]), and their validation requires an *underapproximating* analysis [20,38].

In his thesis and related work [13,15], Dams studied simultaneous over- and underapproximating analyses of reactive systems, where a Galois connection

[1] `www.cis.ksu.edu/∼schmidt`. Supported by NSF ITR-0085949 and ITR-0086154.

defines the relation between a concrete system's states and the abstract states to be used in an abstract system. Dams noted a duality between over- and underapproximation and used it to define an algorithm that constructs overapproximating and underapproximating systems based on the Galois connection. Remarkably, he proved that his "mixed" over-underapproximation preserves the most temporal-logic properties true of the original reactive system ([15], Theorem 4.1.2).

Dams's results were impressive, but unfinished, for they did not employ the usual abstract-interpretation theory for synthesizing the abstract system from the concrete one and the Galois connection, nor did they yield their expressivity results from the usual corollaries of abstract-interpretation theory. In this paper, we provide the missing link between Dams's systems and abstract interpretation.

The key is using appropriate powerset domains for abstracting the codomains of the transition functions of a nondeterministic reactive system: We use lower powersets [24,26,39] to model overapproximation and upper powersets [24,26,39,46] to model underapproximation. We develop the theory within a calculus of logical relations on base types, function tyes, and upper and lower powerset types, which lets us build the over- and underapproximations in small, well understood steps. As a bonus, the logical-relations calculus yields a natural logic that matches the one Dams used in his work, and we obtain his expressivity results for free.

The paper is structured as follows. Section 1 surveys the problem area: It reviews Galois connections and state-transition systems, explains the difficulties in defining underapproximations, and describes an approach based on lower and upper powersets. Transition systems and Dams's mixed-transition systems are reviewed in Sections 2 and 3, and Section 3.1 surveys our approach to proving Dams's results with Galois-connection theory.

The formal development begins in Section 4, where Galois connections are characterized as *U-GLB-L-LUB-closed* binary relations between concrete and abstract domains. The lower and upper powerset constructions are carefully developed in Section 5, preparing the way in Section 6 for a calculus of logical relations that utilizes powerset types.

Generation and preservation of closure properties within the calculus are proved in Section 7, and Sections 8 and 9 apply the results to synthesizing Dams's most-precise over- and underapproximating analyses. Finally, Section 10 extracts a validation logic from the logical relations and shows that the most-precise approximations preserve the most properties in the logic.

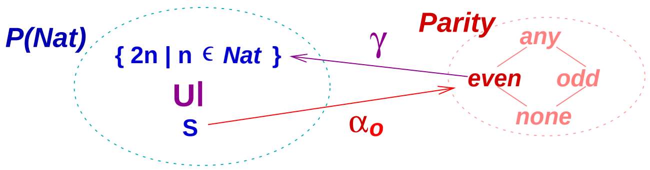


Fig. 1. Overapproximation by parity

1 Galois Connections

Let C be the set of concrete states that appear during execution, and let A be a set of abstract states that model the states in C. A typical static analysis begins from a function, $\gamma : A \rightarrow I\!\!P(C)$, that maps each $a \in A$ to those $\gamma(a) \subseteq C$ that a models. (We use $I\!\!P(\cdot)$ to denote the set-of-all-subsets construction.) To ensure termination of the static analysis [10,23], we require that A is a complete lattice and γ is monotone.

It is useful to have an inverse to γ, and a suitable inverse exists when γ is the upper adjoint of a *Galois conection*: For complete lattices, $(PC, \subseteq)$ and $(A, \sqsubseteq)$, a pair of monotone maps, $\alpha : PC \rightarrow A$ and $\gamma : A \rightarrow PC$, define a *Galois connection*, written $PC\langle\alpha,\gamma\rangle A$, iff $id_{PC} \sqsubseteq_{PC \rightarrow PC} \gamma \circ \alpha$ and $\alpha \circ \gamma \sqsubseteq_{A \rightarrow A} id_A$ [9,16]. γ is the *upper adjoint* and α is the *lower adjoint*.

An example of a Galois connection is approximation of sets of numbers by their parity — see Figure 1, where $\gamma : Parity \rightarrow I\!\!P(Nat)$ is

$$\begin{array}{ll} \gamma(none) = \{\} & \gamma(even) = \{2n \mid n \in Nat\} \\ \gamma(any) = Nat & \gamma(odd) = \{2n+1 \mid n \in Nat\} \end{array}$$

The lower adjoint, $\alpha_o : I\!\!P(Nat) \rightarrow Parity$, must be defined as

$$\alpha_o(S) = \begin{cases} none & \text{if } S = \emptyset \\ even & \text{else if } S \subseteq \{2n \mid n \in Nat\} \\ odd & \text{else if } S \subseteq \{2n+1 \mid n \in Nat\} \\ any & \text{otherwise} \end{cases}$$

Galois connections possess many useful properties; the ones used in this paper most often are:

- For a fixed $\gamma : A \rightarrow PC$, there is exactly one lower adjoint: for $S \in PC$, $\alpha(S) = \sqcap\{a \mid S \subseteq \gamma(a)\}$. Similarly, every lower adjoint, α, has exactly one upper adjoint, $\gamma(a) = \cup\{S \mid \alpha(S) \sqsubseteq a\}$.
- γ is the upper adjoint of a Galois connection iff it preserves meets: for all

$T \subseteq A$, $\gamma(\sqcap T) = \cap_{a \in T}\gamma(a)$. Similarly, α is a lower adjoint iff it preserves joins.

Abstract-interpretation theory [9,10] provides these results: for Galois connection, $PC\langle\alpha,\gamma\rangle A$, concrete computation function, $f : PC \rightarrow PC$, and f's approximation, $f^\sharp : A \rightarrow A$:

- $f^\sharp$ is *sound for* f iff $\alpha \circ f \sqsubseteq_{PC\rightarrow A} f^\sharp \circ \alpha$ iff $f \circ \gamma \sqsubseteq_{A\rightarrow PC} \gamma \circ f^\sharp$.
- The function, $f^\sharp_{best} = \alpha \circ f \circ \gamma$, is sound for f and is also *most precise*: for all $g : A \rightarrow A$ that are sound for f, $f^\sharp_{best} \sqsubseteq_{A\rightarrow A} g$.

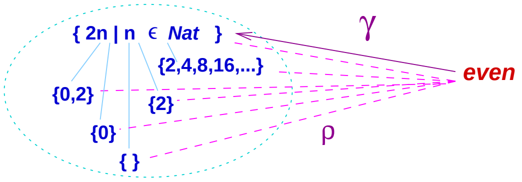
Galois connections compose, and they can be lifted to products and function spaces of complete lattices [12]; we develop these constructions later.

One construction worth reviewing now is *disjunctive completion* [10,12,19]: Given Galois connection, $PC\langle\alpha,\gamma\rangle A$, define $\mathbb{P}_\downarrow(A)$ to be the down-closed subsets of A, where a set, $T \subseteq A$, is *down closed* iff for all $a, a' \in A, a' \sqsubseteq a$ and $a \in T$ imply $a' \in T$. We can partially order the down-closed sets by subset containment and define the Galois connection, $PC\langle\alpha',\gamma'\rangle\mathbb{P}_\downarrow(A)$, where $\gamma'(T) = \cup_{a\in T}\gamma(a)$. We have that γ' preserves both meets *and* joins. In addition, we can use disjunctive completion on *both* PC and A, generating a Galois connection of form, $\mathbb{P}_\downarrow(PC)\langle\alpha'',\gamma''\rangle\mathbb{P}_\downarrow(A)$ [7]. Both forms of Galois connection play key roles in this paper.

1.1 *Over- and underapproximation as duals*

A typical static analysis begins with a Galois connection, $\mathbb{P}(C)\langle\alpha_o,\gamma\rangle A$, and employs $f^\sharp : A \rightarrow A$ to soundly approximate $f : \mathbb{P}(C) \rightarrow \mathbb{P}(C)$. This makes $f^\sharp$ *overapproximating* because it overestimates f's answer set: $f(S) \subseteq \gamma(f^\sharp(\alpha_o(S)))$, for all $S \subseteq C$. Equivalently, we say that S is *overapproximated by* $a \in A$ iff $S \subseteq \gamma(a)$. The example Galois connection for parities in Figure 1 is overapproximating.

Abstract values assert program properties. For example, a static analysis that computes a program's output to be *even* $\in$ *Parity* asserts the *universal property*, "$\forall$*even*" — all the program's outputs are even-valued numbers, that is, the program's concrete output must be a set, S, such that $S \subseteq \gamma(\mathit{even})$:



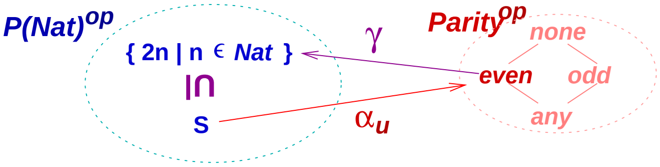


Fig. 2. Underapproximation by parity

We write $S\,\rho\,a$ to assert that S is (over)approximated by a: $S\,\rho\,a$ iff $S \subseteq \gamma(a)$, and trivially, $\gamma(a) = \cup\{S \mid S\,\rho\,a\}$ identifies the largest such set. The previous diagram shows sets that are approximated by *even*.

1.2 Underapproximation as an order-theoretic dual

The traditional way to define an *underapproximating* Galois connection is to invert the concrete and abstract domains, giving $\mathbb{P}(C)^{op}\langle\alpha_u,\gamma\rangle A^{op}$, where $\mathbb{P}(C)^{op} = (\mathbb{P}(C), \supseteq)$ and $A^{op} = (A, \sqsupseteq_A)$. So, the best underapproximation of $f : \mathbb{P}(C) \to \mathbb{P}(C)$ is $f^\flat = \alpha_u \circ f \circ \gamma$. Figure 2 presents the dual of the parity example: $S \subseteq C$ is underapproximated by $a \in A$ iff $S \supseteq \gamma(a)$.

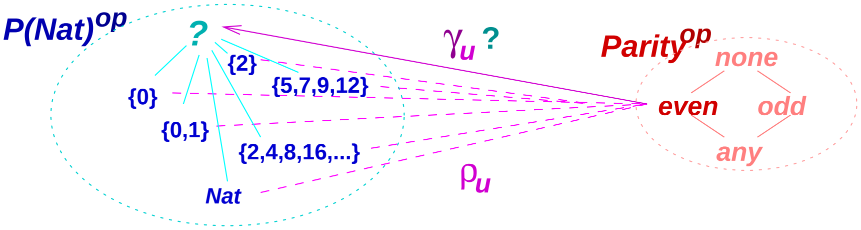
Here, $even \in Parity^{op}$ asserts that *all even numbers are included in the program's outputs* — a strong assertion. Also, we may reuse $\gamma : A \to \mathbb{P}(C)$ as the upper adjoint from A^{op} to $\mathbb{P}(C)^{op}$ iff γ preserves joins in $(A, \sqsubseteq_A)$ — another strong demand.

An unfortunate consequence of the dualization is that the underapproximation interpretation of a language's constants is often "nothing." For example, we might define the semantics of a programming language by means of an inductively defined interpretation function, $[\![\cdot]\!] : Expression \to Environment \to Nat$. For constant symbol, $\mathsf{2}$, we define its concrete semantics, $[\![\mathsf{2}]\!]_e = 2$; then, we are forced to define the parity-underapproximation interpretation, $[\![\cdot]\!]^\flat : Expression \to Environment^\flat \to Parity$, as $[\![\mathsf{2}]\!]^\flat_e = none$, because we require $\gamma([\![\mathsf{2}]\!]^\flat_e) \subseteq \{2\} = \{[\![\mathsf{2}]\!]_{\gamma(e)}\}$. Thus, many program phrases are interpreted to nothing as well, e.g., the interpretation of `x+2` goes

$$[\![\mathtt{x+2}]\!]^\flat_e = add^\flat([\![\mathtt{x}]\!]^\flat_e, [\![\mathsf{2}]\!]^\flat_e) = add^\flat(e(\mathtt{x}), none) = none$$

where $e \in Environment^\flat = Var \to Parity$, even though `x+2` preserves the parity of `x`. If we try to repair this example, say by including all constants, $n \in Nat$, in $Parity^{op}$, then to ensure that γ preserves meets, we must expand $Parity^{op}$ into $\mathbb{P}(Nat)^{op}$!

Fortunately, there is an alternative view of underapproximation: $a \in A^{op}$ asserts an *existential property* — there exists an output with property a. For example, if the overapproximating $even \in Parity$ asserts "$\forall even$," *then the underapproximating* $even \in Parity^{op}$ *should assert "*$\exists even$*"* — there exists an even number in the program's outputs. That is, the program's output is a set, S, such that $S \cap \gamma(even) \neq \emptyset$. Let $\rho_u \subseteq \mathbb{P}(C)^{op} \times A^{op}$ denote this underapproximation relationship, and for $A = Parity$ we have



That is, $S\,\rho_u\,a$ iff $S \cap \gamma(a) \neq \emptyset$. This interpretation permits a nontrivial underapproximation of constants, e.g., $[\![2]\!]^\flat_e = even$, and expressions: $[\![\mathtt{x}+2]\!]^\flat_e = add^\flat(e(\mathtt{x}), even) = e(\mathtt{x})$. But we *cannot* define an upper adjoint, $\gamma_u : Parity^{op} \rightarrow \mathbb{P}(Nat)^{op}$, in the usual way — there is no best, minimal set that contains an even number. Indeed, *even*'s concretization is not a single set — it must be a *set of sets*:

$$\gamma_u(even) = \{S \in \mathbb{P}(Nat)^{op} \mid S\,\rho_u\,even\}$$

This suggests we might lift *both* the concrete and abstract domains by powerset constructions: the concrete domain becomes sets of sets of values, and the abstract domain becomes sets of properties.

1.4 Sets of properties and their interpretations

We can generalize over- and underapproximation to multiple properties, e.g., a parity overapproximation analysis might calculate that a program's outputs fall in the set, $\{even, odd\}$. This would assert, $\forall\{even, odd\} \equiv \forall(even \vee odd)$ — all the outputs are even- or odd-valued.

When we lift the *Parity* abstract domain to a powerset, its overapproximating (universal) interpretation appears as in Figure 3. We use a *lower powerset*, $\mathbb{P}_\downarrow(Parity)$ (the elements are down-closed sets, ordered by $\subseteq$), for the abstract domain. The upper adjoint, γ, concretizes each set of abstract values to a set of concrete sets.

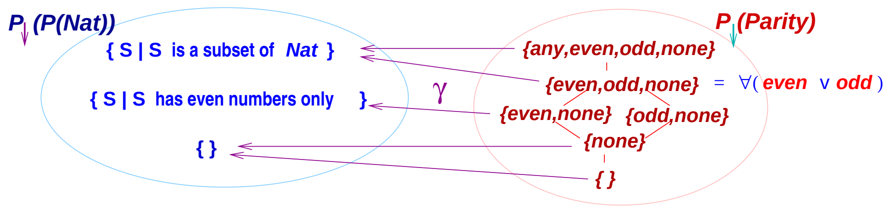

P↓(P(Nat))
{ S | S is a subset of Nat }
{ S | S has even numbers only }
{ }
γ
P↑(Parity)
{any,even,odd,none}
{even,odd,none} = ∀(even ∨ odd)
{even,none}
{odd,none}
{none}
{ }

Fig. 3. Parity overapproximation by powerset

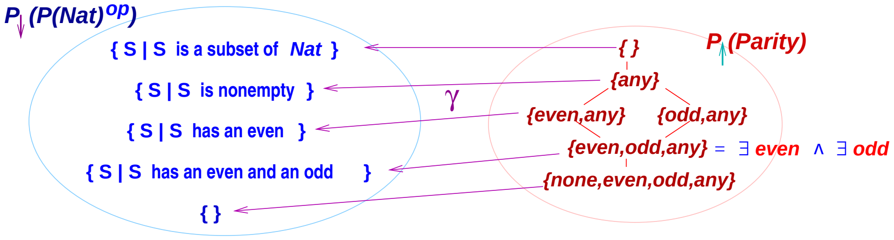


Fig. 4. Parity underapproximation by powerset

Frankly, the use of $I\!\!P_\downarrow(I\!\!P(Nat))$ in place of $I\!\!P(Nat)$ gives no new precision to the example,[2] nor do the extra elements in $I\!\!P_\downarrow(Parity)$ give more expressivity. But the dual construction yields something new: When we use sets of abstract values in underapproximation analysis, an outcome like $\{even, odd\}$ asserts $\exists\{even, odd\} \equiv \exists even \wedge \exists odd$ — the output set includes an even value and an odd value; see Figure 4.

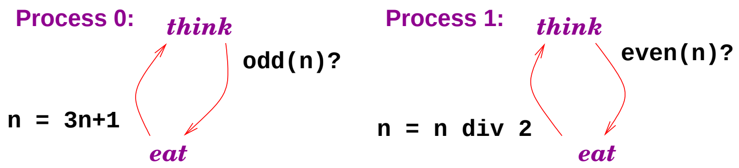
Here, we must use an *upper powerset*, $I\!\!P_\uparrow(Parity)$ (upwards-closed sets, ordered by $\supseteq$), for the abstract domain. The concrete domain must be lifted to a lower powerset of an upper powerset; the reasons are explained later in the paper.

The examples just developed play a crucial role in giving semantics to nondeterministic state-transition systems.

2 State-transition systems

A program's semantics is often defined as a *state-transition system*, (C, R_C), where C is the state set and $R_C \subseteq C \times C$ is the state-transition relation. $(c, c') \in R_C$ is drawn as $c \rightarrow c'$. See Figure 5 for an example, where a state-transition semantics is given for a two-process, "dining mathematician" program that uses a global variable, n, to compute the Collatz function [13]. (In the example, states of form $(think, think, n)$ are initial.) Though the example is deterministic, state-transition systems readily accommodate nondeterministic

[2] Because, for $I\!\!P(C)\langle\alpha', \gamma'\rangle I\!\!P_\downarrow(A)$ and $I\!\!P_\downarrow(I\!\!P(C))\langle\alpha'', \gamma''\rangle I\!\!P_\downarrow(A)$, we typically have $\gamma''(T) = \{S \mid S \subseteq \gamma(T)\}$ and also $\cup\gamma''(T) = \gamma'(T)$.



Let $C = \{(s_0, s_1, n) \mid s_0, s_1 \in \{\mathit{think}, \mathit{eat}\},\ n \geq 0\}$. R_C is defined as follows:

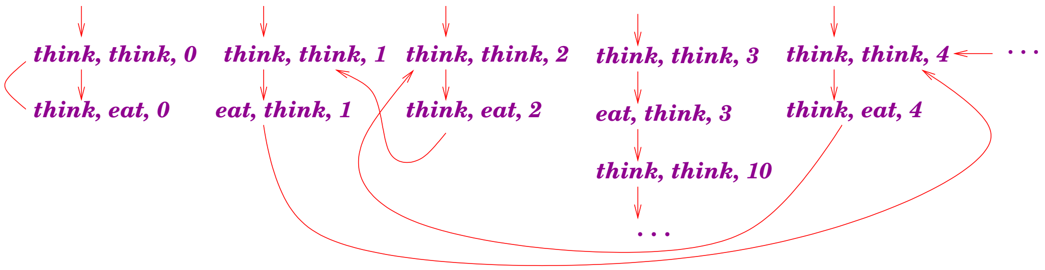


Fig. 5. A Collatz-function program and its state-transition system

Let $A = \{(s_0, s_1, p) \mid s_0, s_1 \in \{\mathit{think}, \mathit{eat}\},\ p \in \mathit{Parity}\}$. $R_A^\sharp$ is defined as

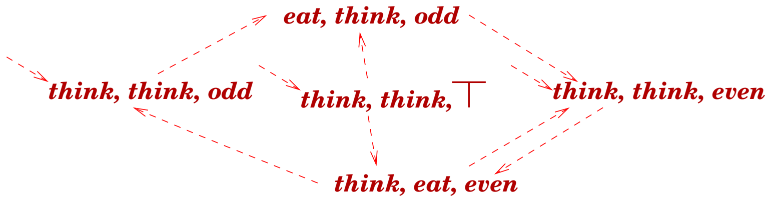


Fig. 6. An overapproximating state-transition system

and reactive programs [33].

2.1 Overapproximating transitions

Given a Galois connection, $\mathbb{P}(C)\langle\alpha, \gamma\rangle A$, we can define a state-transition system whose transition relation, $R_A^\sharp \subseteq A \times A$, overapproximates R_C. Figure 6 presents an abstraction of Figure 5 by replacing numbers by parities. Only the reachable states are shown; the transition system is nondeterministic.

The abstract states, $\{(s_0, s_1, p) \mid s_0, s_1 \in \{\mathit{think}, \mathit{eat}\},\ p \in \{\mathit{even}, \mathit{odd}\}\}$, partition the concrete-state set; when completed into a complete lattice (using $\bot$ and $\top$), the abstract-state lattice becomes a *partitioning domain* [40].

The formal relationship between the concrete and abstract systems is established by a *simulation* [13,32,33,37]: Given $\rho \subseteq C \times A$, say that R_C *is* ρ*-simulated* by $R_A^\sharp$ iff for all $c \in C, a \in A$, $c\,\rho\,a$ and $c \rightarrow c'$ imply there exists $a' \in A$ such that $a \rightarrow a'$ and $c'\,\rho\,a'$.

We call $R_A^\sharp$ *may*-transitions, because the transitions predict concrete transitions that may happen. This makes $R_A^\sharp$ an overapproximation of R_C. It is easy

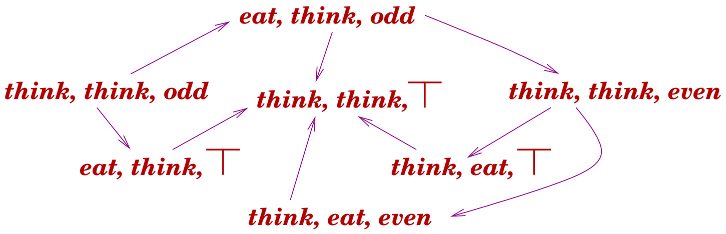


Fig. 7. An underapproximating system

to check that the structure in Figure 5 is ρ_γ-simulated by the one in Figure 6, where $(s_0, s_1, n)\, \rho_\gamma\, (s'_0, s'_1, p)$ iff $n \in \gamma(p)$, $s_0 = s'_0$, and $s_1 = s'_1$.

Given Galois connection $I\!P(C)\langle\alpha, \gamma\rangle A$ and transition system (C, R_C), Dams ([15], Definition 3.3.1) showed that one can define the minimal collection of may-transitions, $R_0^\sharp \subseteq A \times A$, as follows:

$$(a, \alpha\{c'\}) \in R_0^\sharp \text{ iff } c \in \gamma(a) \text{ and } (c, c') \in R_C$$

The precise meaning of "minimal collection" is developed later. The relation in Figure 6 is minimal. (To make a non-minimal relation, add any transitions you please — the simulation property still holds.)

2.2 Underapproximating transitions

Given the difficulties in devising an appropriate underapproximating Galois connection, it is a welcome surprise that an underapproximating transition relation can be simply defined by means of a *dual simulation* [13,32]:

Transition relation R_C is ρ-*dually simulated* by $R_A^\flat$ iff $R_A^\flat$ is ρ-simulated by R_C, that is, for all $c \in C, a \in A$, $c\, \rho\, a$ and $a \rightarrow a'$ imply there exists $c' \in C$ such that $c \rightarrow c'$ and $c'\, \rho\, a'$.

We call $R_A^\flat$ *must*-transitions, because the transitions predict concrete transitions that must appear in the concrete program. This makes $R_A^\flat$ an underapproximation of R_C.

Using the same state sets and relation, ρ_γ, as in Figure 6, Figure 7 presents a transition system that dually simulates the one in Figure 5.

We can define the maximal collection of must transitions as follows [15,44]:

$$(a, a') \in R_0^\flat \text{ iff for all } c \in \gamma(a),\ \{c' \mid (c, c') \in R_C\} \cap \gamma(a') \neq \emptyset$$

The relation in Figure 7 is maximal. (To make a non-maximal relation, remove any transitions you please — the dual-simulation property still holds.)

Although we can readily define from relation $R_C \subseteq C \times C$ a state-transition *function*, $f_R : C \to I\!\!P(C)$, as $f_R(c) = \{c' \mid (c, c') \in R\}$, it is unclear how to define over- and underapproximation transition functions from $R_A^\sharp$ and $R_A^\flat$ — the problem lies in preserving A's ordering in the functions' codomains so that the functions are well defined and monotone. The solution presented later in the paper uses the lower- and upper-powerset constructions seen earlier.

2.3 Kripke structures and logics

Given a transition system, (C, R_C), and set of primitive properties, $Prop$, we define a labelling function, $L_C : C \to I\!\!P(Prop)$, that indicates the properties possessed by each state. The transition system plus labelling function defines a *Kripke structure* [8].

For the system in Figure 5, we might define $Prop = Parity$ and then define $a \in L_C(s_0, s_1, n)$ iff $n \in \gamma(a)$, e.g., $L_C(think, think, 3) = \{odd, \top\}$.

Here is a temporal logic, a variant of *Hennessy-Milner logic* [27], for stating properties of Kripke structures; let $p \in Prop$:

$$\phi ::= p \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \Box\phi \mid \Diamond\phi$$

For $c \in C$, the logic's judgements are defined as

$c \models p$ iff $p \in L_C(c)$

$c \models \phi_1 \wedge \phi_2$ iff $c \models \phi_1$ and $c \models \phi_2$

$c \models \phi_1 \vee \phi_2$ iff $c \models \phi_1$ or $c \models \phi_2$

$c \models \Box\phi$ iff for all c' such that $c \to c'$, $c' \models \phi$

$c \models \Diamond\phi$ iff there exists c' such that $c \to c'$ and $c' \models \phi$

For example, the judgement $(think, think, 4) \models \Box\Diamond even$ holds for the system in Figure 5.

Say that R_C is ρ-simulated by $R_A^\sharp$; we can define $L_A(a) = \cap\{L_C(c) \mid c\, \rho\, a\}$ and apply the above judgement forms to states in A, using $\models_A$ to label the judgements. Then, $c\, \rho\, a$ and $a \models_A \phi$ imply $c \models \phi$ *provided that* ϕ *contains no occurrence of* $\Diamond$ [32]. (Counterexample: For Figure 6, $(think, eat, 4)\, \rho_\gamma\, (think, eat, even)$ and $(think, eat, even) \models_A \Diamond odd$, but $(think, eat, 4) \not\models \Diamond odd$.) Dually, when R_C is ρ-dual simulated by $R_A^\flat$ and L_A is defined as before, then $c\, \rho\, a$ and $a \models_A \phi$ imply $c \models \phi$ provided that ϕ contains no occurrence of $\Box$ [13].

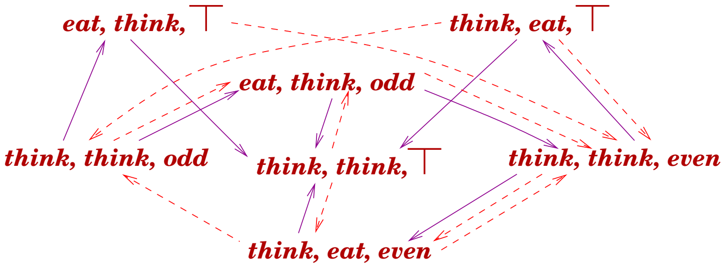


Fig. 8. A mixed-transition system

3 Mixed-transition systems

In his thesis [13] and in subsequent work [15], Dams studied simultaneous over- and underapproximation of state-transition systems, (C, R_C). A *mixed-transition system* is a triple, $(A, R^\sharp_A, R^\flat_A)$. For $\rho \subseteq C \times A$, (C, R_C) is ρ*-mixed simulated* by $(A, R^\sharp_A, R^\flat_A)$ iff R_C is ρ-simulated by $R^\sharp_A$ and ρ-dually simulated by $R^\flat_A$. Figure 8 shows (the reachable states of) the mixed-transition system assembled from Figures 6 and 7.

For mixed-transition systems, Dams provided a sound semantics for all of Hennessy-Milner logic, where in particular:

$$a \models_A \Box\phi \text{ iff for all } a' \text{ such that } (a, a') \in R^\sharp_A,\ a' \models_A \phi$$

$$a \models_A \Diamond\phi \text{ iff there exists } a' \text{ such that } (a, a') \in R^\flat_A \text{ and } a' \models_A \phi$$

Now, when $c\,\rho\,a$ and $a \models_A \phi$, then $c \models \phi$. For example, from Figure 8, we can prove $(\mathit{think}, \mathit{eat}, \mathit{even}) \models \Box(\Diamond \mathit{odd} \vee \Diamond \mathit{even})$, implying that the same property holds for all concrete states of form, $(\mathit{think}, \mathit{eat}, 2n)$, $n \geq 0$.

Given a Galois connection, $(\mathbb{P}(C), \subseteq)\langle\alpha, \gamma\rangle(A, \sqsubseteq_A)$, Dams defined the mixed transition system, $M_0 = (A, R^\sharp_0, R^\flat_0)$, where $R^\sharp_0$ is the minimal set of may-transitions for A defined earlier, and $R^\flat_0$ is the maximal set of must-transitions for A defined earlier. With impressive work, he also proved *best precision* ([15], Theorem 4.1.2) — M_0 proves the most sound properties of any sound mixed transition system. That is, if we fix A and ρ, then if (C, R_C) is ρ-mixed simulated by some $M_A = (A, R^\sharp_A, R^\flat_A)$ and $a \models_{M_A} \phi$, then $a \models_{M_0} \phi$ holds also.

3.1 Can we derive Dams's results within abstract-interpretation theory?

Dams's results are impressive but slightly ad-hoc, in that he relates concrete and abstract states via a Galois connection, yet he does not use the Galois connection to define systematically $R^\sharp_0$ and $R^\flat_0$ from R, nor does he employ the usual results from abstract-interpretation theory to show that $R_0^\sharp$ and $R_0^\flat$ are the most-precise over- and underapproximations of R. Indeed, it should be possible to construct Dams's results entirely within a framework of higher-order Galois connections and gain new insights in the process. We do so in this paper:

The key is to treat $R \subseteq C \times C$ as the function, $R : C \rightarrow I\!\!P(C)$. Then, we treat $R_A^\sharp \subseteq A \times A$ as $R_A^\sharp : A \rightarrow I\!\!P_L(A)$, where $I\!\!P_L(\cdot)$ is a *lower powerset* constructor. (An example of a lower powerset constructor is $I\!\!P_\downarrow(\cdot)$, which was used in Figure 3.)

Given Galois connection, $I\!\!P(C)\langle\alpha_\tau, \gamma_\tau\rangle A$, for the τ-typed state sets, C and A, we define the usual relation, $\rho_\tau \subseteq C \times A$, as $c\,\rho_\tau\; a$ iff $c \in \gamma_\tau(a)$, and we "lift" the Galois connection to $I\!\!P_L(I\!\!P(C))\langle\alpha_{I\!\!P_L(\tau)}, \gamma_{I\!\!P_L(\tau)}\rangle I\!\!P_L(A)$, so that

(1) function R is ρ_τ-simulated by function $R_A^\sharp$ iff $ext(R) \circ \gamma_\tau \sqsubseteq_{A \rightarrow I\!\!P_L(I\!\!P(C))} \gamma_{I\!\!P_L(\tau)} \circ R_A^\sharp$, which is abstract-interpretation soundness;
(2) the soundness of the judgement form, $a \models_A \Box\phi$, follows from Item 1;
(3) $R_{best}^\sharp = \alpha_{I\!\!P_L(\tau)} \circ ext(R) \circ \gamma_\tau$, which is the abstract-interpretation most-precise abstraction, preserves the most $\Box$-properties and equals $R_0^\sharp$.

Here, $ext(R) : I\!\!P(C) \rightarrow I\!\!P_L(I\!\!P(C))$ lifts R to operate on sets of states.

We prove similar results for underapproximations, $R_A^\flat$, the judgement form for $\Diamond\phi$, and $R_{best}^\flat : A \rightarrow I\!\!P_U(A)$, where $I\!\!P_U(\cdot)$ is an upper powerset constructor (of which $I\!\!P_\uparrow(\cdot)$ is an example from Figure 4).

3.2 Overview of the technical developments

The above-mentioned results follow from a careful reformulation of Galois connections based on a logical-relation calculus and a simplified powerdomain theory:

(1) We show how Galois connections are generated from *U-GLB-L-LUB-closed* binary relations (cf. [11,34,43]) and show how to incrementally build from an"unclosed" binary approximation relation on primitive type to a U-GLB-L-LUB-closed one on higher type.
(2) We define lower and upper powerset constructions, which are weaker forms of powerdomains appropriate for abstraction studies [12,24,39], and we note that the appropriate approximation relations on powersets are exactly the standard lower ("Hoare") and upper ("Smyth") orderings [39].
(3) We insert upper- and lower-powerset types into a family of logical relations, show when the logical relations preserve the closure properties

in Item 1, and show that simulations can be constructed with logical relations. We use the logical relations to build U-GLB-L-LUB-closed relations on powerset types, and we prove that Dams's most-precise over- and underapproximating state-transition relations are the most-precise abstract-computation functions defined from the concrete computation functions and the Galois connections extracted from the U-GLB-L-LUB-closed relations.

(4) We extract validation and refutation logics from the logical relations (cf. [2]), state their relation to Hennessey-Milner logic [27], and obtain easy proofs of soundness and best precision of the abstract state-transition functions.

The remainder of the paper provides the technical development.

4 Closed binary relations generate Galois connections

The following results are assembled from [5,11,22,34,35,43,45]: Let C and A be complete lattices, and let $\rho \subseteq C \times A$, where $c\,\rho\;a$ means c is approximated by a.

Definition 1 *For all $c, c' \in C$, for $a, a' \in A$, for $\rho \subseteq C \times A$, ρ is*

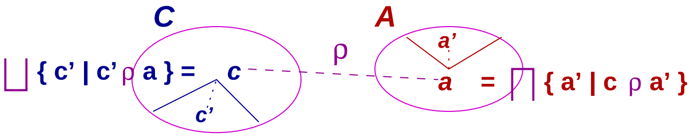
(1) U-closed *iff $c\,\rho\;a$ and $a \sqsubseteq_A a'$ imply $c\,\rho\;a'$*
(2) GLB-closed *iff $c\,\rho\;\sqcap\{a \mid c\,\rho\;a\}$*
(3) L-closed *iff $c\,\rho\;a$ and $c' \sqsubseteq_C c$ imply $c'\,\rho\;a$*
(4) LUB-closed *iff $\sqcup\{c \mid c\,\rho\;a\}\,\rho\;a$.*

U- and L-closure ensure the soundness of an approximation relation, ρ, and GLB- and LUB-closure ensure the existence of most precise abstractions and concretizations.

Proposition 2 *For U-GLB-L-LUB-closed $\rho \subseteq C \times A$, $C\langle\alpha_\rho, \gamma_\rho\rangle A$ is a Galois connection, where $\alpha_\rho(c) = \sqcap\{a \mid c\,\rho\;a\}$ and $\gamma_\rho(a) = \sqcup\{c \mid c\,\rho\;a\}$.*

PROOF. α_ρ and γ_ρ are monotone by L- and U-closure, respectively. We compute $\gamma_\rho(\alpha_\rho(c_0)) = \sqcup G$, where $G = \{c \mid c\,\rho\;\alpha_\rho(c_0)\}$. By GLB-closure, $c_0\,\rho\;\alpha_\rho(c_0)$, hence $c \in G$, implying that $c_0 \sqsubseteq_C \sqcup G$. The proof for $\alpha_\rho(\gamma_\rho(a_0))$ is similar.

Diagrammed, Proposition 2 looks like this:



Note that $c\,\rho\,a$ iff $c \sqsubseteq_C \gamma_\rho(a)$ iff $\alpha_\rho(c) \sqsubseteq_A a$.

Corollary 3 *For Galois connection, $C\langle\alpha,\gamma\rangle A$, define $\rho_\gamma \subseteq C \times A$ as $\{(c,a) \mid c \sqsubseteq_C \gamma(a)\}$. Then, ρ_γ is U-GLB-L-LUB-closed and $\langle\alpha_{\rho_\gamma},\gamma_{\rho_\gamma}\rangle = \langle\alpha,\gamma\rangle$.*

Hartmanis and Stearns [22] use the Corollary to assert that $\rho_{\alpha\gamma}$ defines a *pair algebra*.

Lemma 4 *(1) If ρ is U-GLB-closed, and for all $a \in T \subseteq A$, $c\,\rho\,a$, then $c\,\rho\,\sqcap T$.*
(2) If ρ is L-LUB-closed, and for all $c \in S \subseteq C$, $c\,\rho\,a$, then $\sqcup S\,\rho\,a$.

PROOF. For (1), we have $c\,\rho\,\sqcap\{a \mid c\,\rho\,a\}$, by GLB-closure. Since $T \subseteq \{a \mid c\,\rho\,a\}$, $\sqcap\{a \mid c\,\rho\,a\} \sqsubseteq \sqcap T$, implying $c\,\rho\,\sqcap T$, by U-closure. The proof for (2) is similar.

4.1 Completing a U-GLB-closed $\rho \subseteq C \times A$

Often one has a discretely ordered set, C, a complete lattice, A, and a natural approximation relation, $\rho \subseteq C \times A$. But there is no Galois connection between C and A, because ρ lacks LUB-closure. We complete C to a powerset:

Proposition 5 *For set C, complete lattice A, and $\rho \subseteq C \times A$, define $\overline{\rho} \subseteq \mathbb{P}(C) \times A$ as $S\,\overline{\rho}\,a$* iff *for all $c \in S$, $c\,\rho\,a$. Then $\overline{\rho}$ is L-LUB-closed, and if ρ is U-GLB-closed, then so is $\overline{\rho}$.*

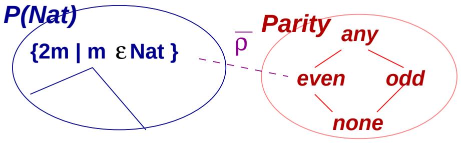
PROOF. $\overline{\rho}$ is L-closed because $\mathbb{P}(C)$ is ordered by $\subseteq$; it is LUB-closed because $\sqcup_{\mathbb{P}(C)}$ is $\cup$. U-closure of $\overline{\rho}$ follows immediately from ρ's U-closure. For GLB-closure, we must show $S\,\overline{\rho}\,\sqcap G$, where $G = \{a \mid S\,\overline{\rho}\,a\}$. For each $c_0 \in S$, we have $c_0\,\rho\,a$, for all $a \in G$. By Lemma 4, we have $c_0\,\rho\,\sqcap G$; hence, $S\,\overline{\rho}\,\sqcap G$.

Corollary 6 *If $\rho \subseteq C \times A$ is U-GLB-closed, then $\mathbb{P}(C)\langle\alpha_{\overline{\rho}},\gamma_{\overline{\rho}}\rangle A$ is a Galois connection, where $\gamma_{\overline{\rho}}(a) = \{c \mid c\,\rho\,a\}$ and $\alpha_{\overline{\rho}}(S) = \sqcap\{a \mid S\,\overline{\rho}\,a\}$.*

Note that $c\,\rho\,a$ iff $c \in \gamma_{\overline{\rho}}(a)$ iff $\alpha_{\overline{\rho}}\{c\} \sqsubseteq a$. The construction defined in Corollary 6 is fundamental to static analysis; Figure 9 shows a typical application.

Let Nat be the discretely ordered set of natural numbers.

$\rho \subseteq Nat \times Parity$ is
$2n\, \rho\; even$
$2n+1\, \rho\; odd$
$n\, \rho\; any$



ρ is U-GLB-closed but not LUB-closed. It is completed to $\overline{\rho} \subseteq I\!P(Nat) \times Parity$.

Fig. 9. Completing $\rho \subseteq Nat \times Parity$ to $\overline{\rho} \subseteq I\!P(Nat) \times Parity$

There is a less-well known dual completion:

Proposition 7 *For partially ordered set C,* set *A, and $\rho \subseteq C \times A$, define $\rho^+ \subseteq C \times I\!P(A)^{op}$ as $c\, \rho^+\, T$ iff for all $a \in T$, $c\, \rho\, a$. Then ρ^+ is U-GLB-closed, and if ρ is L-LUB-closed, then so is ρ^+.*

The two completions can be combined to generate the classical *polarity Galois connection* [17] between $I\!P(C)$ and $I\!P(A)^{op}$:

Corollary 8 *For sets C and A and $\rho \subseteq C \times A$, we have that $\overline{\rho^+} \subseteq I\!P(C) \times I\!P(A)^{op}$ defines the Galois connection where $\alpha_{\overline{\rho^+}}(S) = \{a \mid \text{for all } c \in S, c\, \rho\, a\}$ and $\gamma_{\overline{\rho^+}}(T) = \{c \mid \text{for all } a \in T, c\, \rho\, a\}$.*

5 Powersets

When D is partially ordered, the naive set-of-all-subsets construction will not suffice for the powerset of D.[3] We now introduce the form of powerset we employ:

Definition 9 *For a partially ordered set, D, a* powerset of D *is*
$P[D] = (E, \sqsubseteq_E, \{\!|\cdot|\!\} : D \rightarrow E, \uplus : E \times E \rightarrow E)$*, such that*

- *$(E, \sqsubseteq_E)$ is a complete lattice*
- *$\{\!|\cdot|\!\}$, the singleton operation, is monotone*
- *$\uplus$, the union operation, is monotone, absorptive, commutative, and associative*
- *For every monotone $f : D \rightarrow M$, where M is a complete lattice, there is a monotone $ext(f) : E \rightarrow M$ such that $ext(f)\{\!|d|\!\} = f(d)$, for all $d \in D$. (This implies $ext(f)(E_1) \sqcup_M ext(f)(E_2) \sqsubseteq_M ext(f)(E_1 \uplus E_2)$.)*

The definition is weaker than that of Hennessy and Plotkin [26,39], who demand that $(E, \sqsubseteq_E, \uplus_E)$ form a continuous semi-lattice and for all continuous semi-lattices, $(M, \sqsubseteq_M, \uplus_M)$, that $ext(f)(S \uplus_E T) = ext(f)(S) \uplus_M ext(f)(T)$,

[3] Due to monotonicity requirements: e.g., for $a, b \in D$, say that $a \sqsubseteq b$. Then we must have that $\{\!|a|\!\} \sqsubseteq \{\!|b|\!\}$ in D's powerset, even though $\{a\} \not\subseteq \{b\}$.

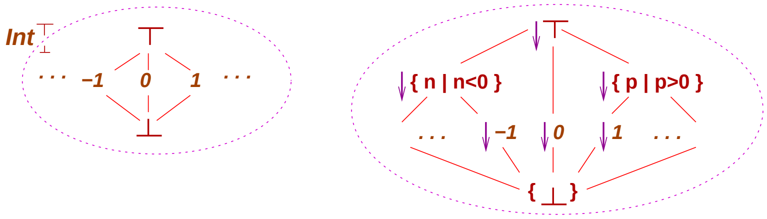


Fig. 10. Complete lattice $Int_{\bot}^{\top}$ and one possible join completion

where $ext(f)$ must be uniquely defined. We omit these requirements because we use monotone (rather than Scott-continuous) functions and because they force E to have "too many" elements than what can be practically implemented in a static analysis. (Of course, this makes $\uplus$ less precise than true set union, a feature seen in many static analyses.)

Here are examples from Cousot and Cousot [12] of our format of powerset:

- **Down-set (order-ideal) completion:** For $d \in D$, $S \subseteq D$, define $\downarrow d = \{e \in D \mid e \sqsubseteq d\}$ and $\downarrow S = \cup\{\downarrow d \mid d \in S\}$. Define $I\!\!P_{\downarrow}(D) = (\{\downarrow S \mid S \subseteq D\}, \subseteq, \downarrow, \cup)$. For $f : D \rightarrow M$, define $ext(f)(S) = \sqcup_{d \in S} f(d)$.
- **Scott-closed-set completion:** $(\{Cl(S) \mid S \subseteq D\}, \subseteq, \downarrow, \cup)$, where $Cl(S)$ defines the Scott closure of S — S is downwards closed and closed under least-upper bounds of chains in D. $ext(f)$ is defined as just seen.
- **Join completion (subsets of $I\!\!P_{\downarrow}(D)$):** $(M, \subseteq, \downarrow, \sqcup_M)$, where $M \subseteq \{\downarrow S \mid S \subseteq D\}$ is a *Moore family* (that is, closed under all intersections). $ext(f)$ is defined as before.

Join completions "add new joins" to D; the trivial join completion is $triv_L(D) = (\{\downarrow d \mid d \in D\}, \subseteq, \downarrow, \downarrow \circ \sqcup_D)$, which is order-isomorphic to D, and the most detailed join completion is $I\!\!P_{\downarrow}(D)$. The Scott-closed-set completion is a join completion. Figure 10 presents an example join completion.

There exists a dual family of powersets based on superset ordering:

Up-set (filter) completion: For $d \in D$ and $S \subseteq D$, define $\uparrow d = \{e \in D \mid d \sqsubseteq e\}$ and $\uparrow S = \cup\{\uparrow d \mid d \in S\}$. Define $I\!\!P_{\uparrow}(D) = (\{\uparrow S \mid S \subseteq D\}, \supseteq, \uparrow, \cup)$. For monotone $f : D \rightarrow M$, let $ext(f) : I\!\!P_{\uparrow}(D) \rightarrow M$ be $ext(f)(S) = \sqcap_{d \in S} f(d)$.

Dual-join completion (subsets of $I\!\!P_{\uparrow}(D)$): $(M, \supseteq, \uparrow, \sqcap_M)$, where $M \subseteq \{\uparrow S \mid S \subseteq D\}$ is a Moore family. The trivial dual-join completion, $triv_U(D) = (\{\uparrow d \mid d \in D\}, \supseteq, \uparrow, \uparrow \circ \sqcap_D)$, is order-isomorphic to D.

The examples demonstrate that our definition of powerset is truly weak — *any* complete lattice can be treated a powerset in terms of its trivial join- or dual-join-completion. This weakness is deliberate, because it lets us develop a dualizable theory of over- and underapproximation that applies to all abstract-interpretation domains and not just to abstract domains generated from a sets-of-all-subsets construction.

5.1 Lower and strongly lower powersets

For powerset $P[D] = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$, $S \in E$ and $d \in D$, we define $d \tilde{\in} S$ iff $\{\!|d|\!\} \uplus S = S$.

Definition 10 *Powerset $I\!P_L(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$ is*

(1) a lower powerset *iff ($S_1 \sqsubseteq_E S_2$ if, for all $x \tilde{\in} S_1$, there exists $y \tilde{\in} S_2$ such that $x \sqsubseteq_D y$).*
(2) a strongly *lower powerset iff ($S_1 \sqsubseteq_E S_2$ iff, for all $x \tilde{\in} S_1$, there exists $y \tilde{\in} S_2$ such that $x \sqsubseteq_D y$).*

The extension operation is defined $ext(f)(S) = \sqcup_M \{f(x) \mid x \tilde{\in} S\}$, for monotone $f : D \to M$.

The definition of lower powerset is the starting point for powerdomain theory for continuous functions [39], but we will see momentarily that in the category of monotone functions, every lower powerset must be strongly lower. The lower powerset ordering is also known as the "Hoare ordering" [39].

For a set, N, $I\!P(N)$ (with subset ordering and the usual singleton and union operations) is a lower powerset; more interesting examples are $I\!P_\downarrow(Parity)$ and $I\!P_\downarrow(I\!P(Nat))$ from Figure 3.

Proposition 11 *For lower powerset $I\!P_L(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$, $S, T \in E$, define $S \tilde{\subseteq} T$ iff $S \uplus T = T$; thus, $d \tilde{\in} S$ iff $\{\!|d|\!\} \tilde{\subseteq} S$. For all $S, T \in E$ and $d \in D$,*

(1) $S \sqsubseteq_E S \uplus T$
(2) $S =_E \sqcup\{\{\!|d|\!\} \mid d \tilde{\in} S\}$
(3) $S \tilde{\subseteq} T$ iff for all $d \tilde{\in} S$, then $d \tilde{\in} T$ also
(4) $d \tilde{\in} S$ iff $\{\!|d|\!\} \sqsubseteq_E S$
(5) $S \tilde{\subseteq} T$ iff $S \sqsubseteq_E T$
(6) $d \sqsubseteq_D e$ iff $\{\!|d|\!\} \sqsubseteq_E \{\!|e|\!\}$.

PROOF. Clause (1): for arbitrary $d \in D$, let $d \tilde{\in} S$, that is, $\{\!|d|\!\} \uplus S = S$. Then $\{\!|d|\!\} \uplus S \uplus T = S \uplus T$, implying $S \sqsubseteq S \uplus T$, by the definition of lower powerset.

Clause (3): if: By the definition of lower powerset, $S \sqsubseteq T$, hence $S \uplus T \sqsubseteq T \uplus T = T$, by (1) and the monotonicity of $\uplus$.
only if: Assume $S \uplus T = T$ and say that $\{\!|d|\!\} \uplus S = S$. Then, $T = S \uplus T = \{\!|d|\!\} \uplus S \uplus T = \{\!|d|\!\} \uplus T$.

Clause(4): if: Assume $\{\!|d|\!\} \sqsubseteq S$. By monotonicity, $\{\!|d|\!\} \uplus S \sqsubseteq S \uplus S = S$, and $S \sqsubseteq \{\!|d|\!\} \uplus S$, by (1). Hence, $\{\!|d|\!\} \uplus S = S$.
only if: By (1), $\{\!|d|\!\} \sqsubseteq \{\!|d|\!\} \uplus S$; but $d\tilde{\in}S$ implies that $\{\!|d|\!\} \uplus S = S$.

Clause (5): if: $S \sqsubseteq T$ and monotonicity imply $S \uplus T \sqsubseteq T \uplus T = T$. By (1), $T \sqsubseteq S \uplus T$, hence $S \uplus T = T$.
only if: By definition, $S \uplus T = T$, and by (1), $S \sqsubseteq S \uplus T$.

Clause (2): Let $M = \{\{\!|d|\!\} \mid d\tilde{\in}S\}$.
$\sqsubseteq$: For arbitrary $d \in D$, say that $d\tilde{\in}S$; then $\{\!|d|\!\} \sqsubseteq \sqcup M$, implying $d\tilde{\in} \sqcup M$, by (4). By the definition of lower powerset, $S \sqsubseteq \sqcup M$.
$\sqsupseteq$: For every $\{\!|d|\!\} \in M$, $\{\!|d|\!\} \sqsubseteq \{\!|d|\!\} \uplus S = S$. This implies $\sqcup M \sqsubseteq S$.

Clause (6): only if: follows from the monotonicity of $\{\!| \cdot |\!\}$.
if: Assume $\{\!|d|\!\} \sqsubseteq_E \{\!|e|\!\}$, and note for the identity function, $id : D \to D$, that $ext(id)\{\!|x|\!\} = id(x) = x$, for all $x \in D$. Since $ext(id)$ must be monotone, we have $ext(id)\{\!|d|\!\} \sqsubseteq_D ext(id)\{\!|e|\!\}$, implying $d \sqsubseteq_D e$.

Corollary 12 *Every lower powerset is strongly lower.*

PROOF. For $\mathbb{P}_L(D) = (E, \sqsubseteq_E, \{\!| \cdot |\!\}, \uplus)$ and $S, T \in E$, say that $S \sqsubseteq T$ and say that $d\tilde{\in}S$. By Clause 4 of Proposition 11, $\{\!|d|\!\} \sqsubseteq S \sqsubseteq T$, implying that $d\tilde{\in}T$.

More surprising, monotonicity and the lower powerset ordering forces a lower powerset's $\uplus$ to be its join and forces every lower powerset to be a join completion where $\tilde{\in}$ is $\in$:

Theorem 13 *For every lower powerset, $\mathbb{P}_L(D) = (E, \sqsubseteq_E, \{\!| \cdot |\!\}, \uplus)$,*

(1) $\uplus = \sqcup_E$
(2) let $M = (\{Mem(S) \mid S \in E\}, \subseteq)$, where $Mem(S) = \{d \in D \mid d\tilde{\in}S\}$. Then M is a join completion of D and isomorphic to E, and $\mathbb{P}_L(D)$ is isomorphic to $(\{Mem(S) \mid S \in E\}, \subseteq, \downarrow, \sqcup_M)$, and $\tilde{\in}$ is $\in$ and $\sqcap_M$ is $\cap$.

PROOF. Clause (1): For $S, T \in E$, $S \uplus T$ is an upper bound of both. To see that it is least, consider any other upper bound, C: By Proposition 11(5), we have $S\tilde{\subseteq}C$ and $T\tilde{\subseteq}T$. This means $S \uplus C = C$ and $T \uplus C = C$, implying $S \uplus T \uplus C = C$, giving $S \uplus T\tilde{\subseteq}C$. By Proposition 11(5), we have $S \uplus T \sqsubseteq C$.

Clause (2): For lower powerset, $\mathbb{P}_L(D) = (E, \sqsubseteq_E, \{\!| \cdot |\!\}, \uplus)$, we define the join completion of D consisting of those subsets of D-elements expressed by E: For each $S \in E$, define $\mathit{Mem}(S) = \{d \in D \mid d \tilde{\in} S\}$ and define

$$M = (\{\mathit{Mem}(S) \mid S \in E\}, \subseteq),$$

which is order-isomorphic to $(E, \sqsubseteq_E)$, where the order isomorphism is $\mathit{Mem}(\cdot)$, which follows from Proposition 11(3). This structure is a join completion because we will show that each set, $\mathit{Mem}(S) = \{d \in D \mid d \tilde{\in} S\}$ is down closed and the sets form a Moore family. Down closure follows from Proposition 11(4): for $a, b \in D$ and $S \in E$, $a \sqsubseteq_D b \tilde{\in} S$ implies $\{\!\!|a|\!\!\} \sqsubseteq_E \{\!\!|b|\!\!\} \sqsubseteq_E S$, implying $a \tilde{\in} S$.

To show that $\mathbb{P}_M(D)$ forms a Moore family, we show closure under arbitrary insersections, that is, $\cap_{i \in I} M_i \in M$ for every family, $\{M_i\}_{i \in I} \subseteq M$. We do so by proving $\cap_{i \in I} M_i = \mathit{Mem}(\sqcap_{i \in I} S_i)$, where $M_i = \mathit{Mem}(S_i)$.

For $\subseteq$, assume for $d \in D$ and for all $j \in I$, that $d \in \mathit{Mem}(S_j)$, that is, $d \tilde{\in} S_j$, that is, $\{\!\!|d|\!\!\} \sqsubseteq S_j$, by 11(4). This implies $\{\!\!|d|\!\!\} \sqcup \sqcap_{i \in I} S_i \sqsubseteq S_j$, which implies $\{\!\!|d|\!\!\} \sqcup \sqcap_{i \in I} S_i \sqsubseteq \sqcap_{i \in I} S_i$. Next, $\sqcap_{i \in I} S_i \sqsubseteq \{\!\!|d|\!\!\} \sqcup \sqcap_{i \in I} S_i$, and by the definition of $\tilde{\in}$, we have $d \tilde{\in} \sqcap_{i \in I} S_i$, and so then, $\cap_{i \in I} M_i \subseteq \mathit{Mem}(\sqcap_{i \in I} S_i)$.

For $\supseteq$, say that $d \in \mathit{Mem}(\sqcap_{i \in I} S_i)$, that is, $d \tilde{\in} \sqcap_{i \in I} S_i$. Since, for all $j \in I$, $d \tilde{\in} \sqcap_{i \in I} S_i \sqsubseteq S_j$, we have $d \in \mathit{Mem}(S_j)$, by 11(4). Thus, $\mathit{Mem}(\sqcap_{i \in I} S_i) \subseteq \cap_{i \in I} \mathit{Mem}(S_i)$.

Next, we define $\mathbb{P}_M(D) = (M, \downarrow, \sqcup_M)$, and we show that the isomorphism, $\mathit{Mem}(\cdot)$, preserves the singleton and union operations: For singleton, we must show for all $d \in D$, that $\mathit{Mem}(\{\!\!|d|\!\!\}_E) = \downarrow d$. The left-hand side of the equation equals $\{e \in D \mid e \tilde{\in} \{\!\!|d|\!\!\}_E\}$. By Proposition 11(4) and (6), this equals $\{e \in D \mid e \sqsubseteq d\}$. For union, we must show that $a \sqcup_M b = \mathit{Mem}(\mathit{Mem}^{-1}(a) \sqcup_E \mathit{Mem}^{-1}(b))$, since $\uplus_E$ is $\sqcup_E$, due to Clause (1) of this Theorem. But this follows because M is order-isomorphic to $(E, \sqsubseteq_E)$.

For $f : D \to M$, we define $\mathit{ext}(f)_M : M \to M$ as merely $\mathit{ext}(f)_M(M) = \mathit{Mem}(\mathit{ext}(f)_E(\mathit{Mem}^{-1}(M)))$. Finally, we establish that $d \tilde{\in}_E S$ iff $d \in \mathit{Mem}(S)$ iff $d \tilde{\in} \mathit{Mem}(S)$: The first equivalence is immediate; for the second, we have $d \tilde{\in} \mathit{Mem}(S)$ iff $\{\!\!|d|\!\!\} \tilde{\subseteq} \mathit{Mem}(S)$ iff $\{\!\!|d|\!\!\} \subseteq \mathit{Mem}(S)$ iff $\downarrow d \subseteq \mathit{Mem}(S)$ iff $d \in \mathit{Mem}(S)$. We finish by noting that $\sqcap$ in $\mathbb{P}_M(D)$ is $\cap$ because $\mathbb{P}_M(D)$ is a Moore family.

Theorem 13 lets us generalize Proposition 5 so that it performs completions with lower powersets:

Theorem 14 *For complete lattices C and A, let $\rho \subseteq C \times A$ and let $\mathbb{P}_L(C) = (E, \subseteq, \{\!\!| \cdot |\!\!\}, \uplus)$ be a lower powerset that is a join completion. Recall that $\overline{\rho} \subseteq \mathbb{P}_L(C) \times A$ is defined $S \, \overline{\rho} \, a$* iff *for all $c \in S$, $c \, \rho \, a$. For any choice of*

$I\!\!P_L(C)$:

(1) $\overline{\rho}$ is L-closed.
(2) If ρ is U-GLB-closed, then *$\overline{\rho}$ is U-GLB-closed.*
(3) If for all $a \in A$, $\{c \mid c\,\rho\ a\} \in E$, then $\overline{\rho}$ is LUB-closed.

The resulting Galois connection defines $\gamma_{\overline{\rho}}(a) = \{c \mid c\,\rho\ a\}$.

PROOF. Clause (1): L-closure follows because $\sqsubseteq_E$ is $\subseteq$.

Clause(2): U-closure of $\overline{\rho}$ follows immediately from the U-closure of ρ. For GLB-closure, we must show that $S\,\overline{\rho}\ \sqcap M_S$, where $M_S = \{a \mid S\,\overline{\rho}\ a\}$, that is, for all $c \in S$, $c\,\rho\ \sqcap M_S$. Since $M_S \subseteq \{a \mid c\,\rho\ a\}$, the result follows from Lemma 4(1).

Clause (3): To prove LUB-closure, for $a \in A$, define $M_a = \{S \in E \mid S\,\overline{\rho}\ a\}$; we will prove that $\{c \mid c\,\rho\ a\} = \sqcup M_a$. Say that $S' \in M_a$, that is, for all $c' \in S'$, $c'\,\rho\ a$. Then, $S' \subseteq \{c \mid c\,\rho\ a\}$, making $\{c \mid c\,\rho\ a\}$ an upper bound of M_a. But $\{c \mid c\,\rho\ a\}$ belongs to M_a, meaning that it equals $\sqcap M_a$.

Corollary 15 *If $\rho \subseteq C \times A$ is L-U-GLB-closed, then $I\!\!P_\downarrow(C)\langle\alpha_{\overline{\rho}}, \gamma_{\overline{\rho}}\rangle A$ is a Galois connection.*

PROOF. Since ρ is L-closed, all sets $\{c \mid c\,\rho\ a\}$ are downwards closed and belong to $I\!\!P_\downarrow(C)$.

Finally, we note that "completing" a relation that already has L-LUB closure maintains the existing precision:

Proposition 16 *If $\rho \subseteq C \times A$ is L-LUB-closed, then for $\overline{\rho} \subseteq I\!\!P_L(C) \times A$, $S \in I\!\!P_L(C)$, and $a \in A$, $S\,\overline{\rho}\ a$ iff $(\sqcup S)\,\rho\ a$.*

PROOF. only if: $S\,\overline{\rho}\ a$ iff for all $c \in S$, $c\,\rho\ a$. Because ρ is L-LUB-closed, Lemma 4 implies $\sqcup S c\,\rho\ a$.

if: $\sqcup S\,\rho\ a$ implies $c\,\rho\ a$ by L-closure, for all $c \in S$.

The Proposition explains why $I\!\!P_\downarrow(I\!\!P(Nat))$ was no more expressive than $I\!\!P(Nat)$ as the concrete domain in the Galois connections for the parity example in Figure 3.

From this point onwards, we use the notation, $I\!\!P_L(D)$, to denote any lower powerset. When a specific instance of a lower powerset is required (e.g., $I\!\!P_\downarrow(D)$ or $triv_L(D)$), we will clearly indicate this.

5.2 Upper powersets

Definition 17 *Powerset* $I\!\!P_U(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$ *is an* upper powerset *iff* ($S_1 \sqsubseteq_E S_2$ *if, for all* $y \tilde{\in} S_2$*, there exists* $x \tilde{\in} S_1$ *such that* $x \sqsubseteq_D y$). *The extension operation is defined* $ext(f)(S) = \sqcap_L\{f(x) \mid x \tilde{\in} S\}$, *for monotone* $f : D \to M$.

The upper powerset ordering is also known as the "Smyth ordering" [39].

For a set, N, $I\!\!P(N)^{op}$ (with superset ordering and the usual singleton and union operations) is an upper powerset; a more interesting example is $I\!\!P_\uparrow(Parity)$ in Figure 4.

The results proved for lower powersets dualize without complication:

Proposition 18 *For upper powerset* $I\!\!P_U(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$, $S, T \in E$, *define* $S \tilde{\subseteq} T$ *iff* $S \uplus T = T$; *thus* $d \tilde{\in} S$ *iff* $\{\!|d|\!\} \tilde{\subseteq} S$. *For all* $S, T \in E$ *and* $d \in D$,

(1) $S \uplus T \sqsubseteq_E S$
(2) $S =_E \sqcap\{\{\!|d|\!\} \mid d \tilde{\in} S\}$
(3) $S \tilde{\subseteq} T$ *iff for all* $d \tilde{\in} S$, *then* $d \tilde{\in} T$ *also*
(4) $d \tilde{\in} S$ *iff* $S \sqsubseteq_E \{\!|d|\!\}$
(5) $S \tilde{\subseteq} T$ *iff* $T \sqsubseteq_E S$
(6) $d \sqsubseteq_D e$ *iff* $\{\!|d|\!\} \sqsubseteq_E \{\!|e|\!\}$

Corollary 19 *Every upper powerset is strongly upper: for* $I\!\!P_U(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$ *and* $S_1, S_2 \in E$, $S_1 \sqsubseteq_E S_2$ *iff for all* $y \tilde{\in} S_2$, *there exists* $x \tilde{\in} S_1$ *such that* $x \sqsubseteq_D y$.

Theorem 20 *For every upper powerset,* $I\!\!P_U(D) = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$,

(1) $\uplus = \sqcap_E$; *and*
(2) let $M = (\{Mem(S) \mid S \in E\}, \supseteq)$, *where* $Mem(S) = \{d \in D \mid d \tilde{\in} S\}$. *Then* M *is a dual-join completion of* D *and isomorphic to* E, *and* $I\!\!P_U(D)$ *is isomorphic to* $(\{Mem(S) \mid S \in E\}, \supseteq, \uparrow, \sqcap_M)$, *and* $\tilde{\in}$ *is* $\in$ *and* $\sqcup_M$ *is* $\cap$.

Theorem 21 *For complete lattices* C *and* A, *let* $\rho \subseteq C \times A$ *and let* $I\!\!P_U(A) = (E, \subseteq, \{\!|\cdot|\!\}, \uplus)$ *be an upper powerset that is a dual-join completion. Define* $\rho^+ \subseteq C \times I\!\!P_U(A)$ *as* $c\, \rho^+\, T$ iff for all $a \in T$, $c\, \rho\, a$. *For any choice of* $I\!\!P_U(A)$:

(1) ρ^+ *is U-closed.*
(2) If ρ *is L-LUB-closed, then so is* ρ^+.
(3) If for all $c \in C$, $\{a \mid c\, \rho\, a\} \in E$, *then* ρ^+ *is LUB-closed.*

The resulting Galois connection defines $\alpha_{\rho^+}(c) = \{a \mid c\,\rho\, a\}$*.*

From this point onwards, we use the notation, $I\!\!P_U(D)$, to denote any upper powerset. When a specific instance of upper powerset is required (e.g., $I\!\!P_\uparrow(D)$ or $triv_U(D)$), we will clearly indicate this.

6 Logical relations

Approximation relations on higher types are naturally defined by logical relations. We employ base types, function types, lower and upper powerset types, and the "completion type" from Theorem 14:

$$\tau \ ::= \ b \mid \tau_1 \rightarrow \tau_2 \mid L(\tau) \mid U(\tau) \mid \overline{\tau}$$

We use $L(\tau)$ to abbreviate the type, $I\!\!P_L(\tau)$, and $U(\tau)$ to abbreviate $I\!\!P_U(\tau)$. Only typing $\overline{\tau}$ is nonstandard; it is a special case of $L(\tau)$ that we retain for convenience, because it appears so often in practice (cf. Figure 9).

We attach the typings to concrete *and* abstract domains, D, as follows:

D_b is given

$D_{\tau_1 \rightarrow \tau_2}$ are the monotone functions from D_{τ_1} to D_{τ_2}, ordered pointwise

$D_{L(\tau)}$ is a lower powerset generated from D_τ

$D_{U(\tau)}$ is an upper powerset generated from D_τ

Since $\overline{\rho} \subseteq I\!\!P_L(C) \times A$ is the completion of $\rho \subseteq C \times A$ (cf. Theorem 14), we define

$$C_{\overline{\tau}} \text{ is } C_{L(\tau)}, \text{ for concrete domain } C_\tau$$

$$A_{\overline{\tau}} \text{ is } A_\tau, \text{ for abstract domain } A_\tau$$

Here are examples: Both Nat and *Parity* in Figure 9 have the same base type — call it N. Then, $I\!\!P(Nat)$ in the same Figure has type $\overline{N}$. This means domain *Parity* also has type $\overline{N}$.

Next, we see that $I\!\!P_\downarrow(Parity)$ in Figure 3 has type $L(N)$ and its concrete counterpart, $I\!\!P_\downarrow(I\!\!P(Nat))$, has type $\overline{L(N)}$ (as well as $L(\overline{N})$ and $L(\overline{L(N)})$). $I\!\!P_\uparrow(Parity)$ in Figure 4 has type $U(N)$, and $I\!\!P_\downarrow(I\!\!P(Nat)^{op})$, has type $\overline{U(N)}$.

The typings are important to defining the family of logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$:

ρ_b is given, for base type b (e.g., $\rho_N \subseteq \mathit{Int} \times \mathit{Parity}$ in Figure 9)

$f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp$ iff for all $c \in C_{\tau_1}, a \in A_{\tau_1}, c \, \rho_{\tau_1} \, a$ implies $f(c) \, \rho_{\tau_2} \, f^\sharp(a)$

$S \, \rho_{L(\tau)} \, T$ iff for all $c \tilde{\in} S,$ there exists $a \tilde{\in} T$ such that $c \, \rho_\tau \, a$

$S \, \rho_{U(\tau)} \, T$ iff for all $a \tilde{\in} T,$ there exists $c \tilde{\in} S$ such that $c \, \rho_\tau \, a$

$S \, \rho_{\overline{\tau}} \, a$ iff for all $c \in S, c \, \rho_\tau \, a$

The definitions read as expected, e.g., $f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp$ asserts that f is approximated by $f^\sharp$ because arguments related by approximation map to answers related by approximation.

$S \, \rho_{L(\tau)} \, T$ defines an *overapproximation* relationship: S is overapproximated by T because every element of S has an approximant in T. Dually, $S \, \rho_{U(\tau)} \, T$ defines an *underapproximation* relationship, because every element in T is witnessed by a concrete element in S.

The definition of $S \, \rho_{\overline{\tau}} \, a$ uses $\in$ (rather than $\tilde{\in}$) to emphasize that $C_{\overline{\tau}}$ is (a lower powerset treated as) a join completion. Indeed, when ρ_τ is U-closed, then $\rho_{\overline{\tau}} \subseteq \mathbb{P}_L(C_\tau) \times A_\tau$ is merely an instance of $\rho_{L(\tau)} \subseteq \mathbb{P}_L(C_\tau) \times \mathit{triv}_L(A)$:

Proposition 22 *Recall that* $\mathit{triv}_L(D) = (\{\downarrow d \mid d \in D\}, \subseteq, \downarrow, \downarrow \circ \sqcup_D) \approx D$. *When* $\rho_\tau \subseteq C \times A$ *is U-closed, then* $\rho_{\overline{\tau}} = \rho_{L(\tau)}$, *for* $\rho_{L(\tau)} \subseteq \mathbb{P}_L(C_\tau) \times \mathit{triv}_L(A)$.

PROOF. We freely use the isomorphism, $\downarrow : A \to \mathit{triv}_L(A)$:

$\subseteq$: Assume $S \, \rho_{\overline{\tau}} \, a$; then for all $c \in S$, $c \, \rho_\tau \, a$. This implies $S \, \rho_{L(\tau)} \downarrow a$.

$\supseteq$: Assume $S \, \rho_{L(\tau)} \downarrow a$; this gives for all $c \tilde{\in} S$, there exists $a' \in \downarrow a$ such that $c \, \rho_\tau \, a'$. By U-closure, we have $c \, \rho_\tau \, a$, hence, $S \, \rho_{\overline{\tau}} \, a$.

Returning to the examples, relation ρ in Figure 9 is more precisely defined as the typed relation, $\rho_N \subseteq \mathit{Nat} \times \mathit{Parity}$; this makes $\bar{\rho}$ typed as $\rho_{\overline{N}} \subseteq \mathbb{P}(\mathit{Nat}) \times \mathit{Parity}$, which induces the Galois connection, $\mathbb{P}(\mathit{Nat})\langle \alpha_{\rho_{\overline{N}}}, \gamma_{\rho_{\overline{N}}} \rangle, \mathit{Parity}$.

Similarly, underlying γ in Figure 4 is the logical relation, $\rho_{\overline{U(N)}} \subseteq \mathbb{P}_\downarrow(\mathbb{P}(\mathit{Nat})^{op}) \times \mathbb{P}_\uparrow(\mathit{Parity})$. The γ in Figure 3 is generated from $\rho_{\overline{L(N)}} \subseteq \mathbb{P}_\downarrow(\mathbb{P}(\mathit{Nat})) \times \mathbb{P}_\downarrow(\mathit{Parity})$. The details are spelled out in a later section.

Two state-transition relations are related by a simulation. The standard definition goes as follows:

Definition 23 *For $\rho \subseteq C \times A$ and transition relations, $R \subseteq C \times C$, $R^\sharp \subseteq A \times A$, $R^\sharp$ ρ-*simulates *R, written $R \lhd_\rho R^\sharp$, iff for all $c, c' \in C, a \in A$, $c \,\rho\, a$ and $(c, c') \in R$ imply there exists $a' \in A$ such that $(a, a') \in R^\sharp$ and $c' \,\rho\, a'$.*

From this definition of simulation, we gain immediately this important result:

Proposition 24 *For $\rho_b \subseteq C_b \times A_b$, if $R : C_b \to I\!\!P_L(C_b)$ and $R^\sharp : A_b \to I\!\!P_L(A_b)$ are monotone, then*

$$R \lhd_{\rho_b} R^\sharp \textit{ iff } R \,\rho_{b \to L(b)}\, R^\sharp.$$

A dual simulation, $R^\flat \lhd_{\rho_b^{-1}} R$, is beautifully characterized as $R \,\rho_{b \to U(b)}\, R^\flat$.

For an example, consider Figures 5 and 6: Let state sets C and A have base type, *State*, and define

$$(s_0, s_1, n) \,\rho_{State}\, (s_0', s_1', p) \text{ iff } s_0 = s_0', s_1 = s_1', \text{ and } p \in \gamma(n)$$

for $\gamma : \mathit{Parity} \to I\!\!P(\mathit{Nat})$ in Figure 1. The concrete transition relation in Figure 5 is coded as the function, $R : C_{State} \to I\!\!P(C_{State})$, and the abstract transition relation in Figure 6 is encoded by a function, $R^\sharp : A_{State} \to I\!\!P_\downarrow(A_{State})$.[4] We have that $R \lhd_{\rho_{State}} R^\sharp$.

Similarly, for the underapproximating transition relation in Figure 7, we have that $R^\flat \lhd_{\rho_{State}^{-1}} R$, where $R : C_{State} \to I\!\!P(C_{State})^{op}$ and $R^\flat : A_{State} \to I\!\!P_\uparrow(A_{State})$. The simulations hold even when A_{State} is not a complete lattice, but it is easy to complete A_{State} and preserve the results.

We will employ these characterizations of simulation and dual-simulation to construct optimal over- and underapproximating transition relations from Galois connections generated from closed, logical relations.

7 Closure properties of logical relations

Many closure properties are preserved by the type constructors, and a few are generated new:

[4] When $(s_0, s_1, p) \in R^\sharp(a)$, then $(s_0, s_1, \bot) \in R^\sharp(a)$ also. This causes no harm.

Proposition 25 *For $\rho_\tau \subseteq C_\tau \times A_\tau$,*

(1) $\rho_{L(\tau)}$, $\rho_{U(\tau)}$, and $\rho_{\overline{\tau}}$ are L-closed; if ρ_τ is L-closed, then so is $\rho_{\tau'\to\tau}$.
(2) $\rho_{L(\tau)}$ and $\rho_{U(\tau)}$ are U-closed; if ρ_τ is U-closed, then so are $\rho_{\tau'\to\tau}$ and $\rho_{\overline{\tau}}$.
(3) If ρ_τ is U-GLB-closed, then so are $\rho_{\tau'\to\tau}$, $\rho_{L(\tau)}$, and $\rho_{\overline{\tau}}$.
(4) If ρ_τ is L-LUB-closed, then so are $\rho_{\tau'\to\tau}$ and $\rho_{U(\tau)}$.

PROOF. Clause (1): To show L-closure for $\rho_{L(\tau)}$, we use $I\!\!P_L(C_\tau)$'s join-closure representation, due to Theorem 13, where $\sqsubseteq_{I\!\!P_L(C_\tau)}$ is $\subseteq$. Given $S' \subseteq S\,\rho_{L(\tau)}\;T$, we see that for all $c' \in S'$, $c' \in S$ as well, and there exists $a\tilde{\in}T$ such that $c'\,\rho_\tau\;a$. The proof of L-closure for $\rho_{\overline{\tau}}$, where $I\!\!P_L(C_\tau)$ is also a join completion, is the same.

For $\rho_{U(\tau)}$, we use $I\!\!P_U(C_\tau)$'s dual-join-closure representation, due to Theorem 20, where $\sqsubseteq_{I\!\!P_U(C_\tau)}$ is $\supseteq$. Given $S' \supseteq S\,\rho_{U(\tau)}\;T$, we see that for every $a\tilde{\in}T$, there exists $c \in S$ such that $c\,\rho_\tau\;a$, and $c \in S'$ as well.

For $\rho_{\tau'\to\tau}$, assume that $f' \sqsubseteq f\,\rho_{\tau'\to\tau}\;f^\sharp$; if $c\,\rho_{\tau_1}\;a$, then $f(c)\,\rho_{\tau_2}\;f^\sharp(a)$. Since $f'(c) \sqsubseteq f(c)$, the result comes from the L-closure of ρ_{τ_2}.

Clause (2): Similar to (1), but recall from Proposition 22 that U-closure is not ensured for $\rho_{\overline{\tau}}$.

Clause (3): For $\rho_{\tau'\to\tau}$, we must show $f\,\rho_{\tau'\to\tau}\;\sqcap F$, where $F = \{f^\sharp \mid f\,\rho_{\tau'\to\tau}\;f\}$. Assume that $c\,\rho_\tau\;a$; for all $f^\sharp \in F$, we have $f(c)\,\rho_{\tau'}\;f^\sharp(a)$. By Lemma 4, we have that $f(c)\,\rho_{\tau'}\;\sqcap\{f^\sharp(a) \mid f^\sharp \in F\}$, and by the definition of meet in the complete lattice of monotone functions, we have $\sqcap\{f^\sharp(a) \mid f^\sharp \in F\} = (\sqcap F)(a)$.

For $\rho_{L(\tau)}$, we must show $S\,\rho_{L(\tau)}\;\sqcap M$, where $M = \{T \mid S\,\rho_{L(\tau)}\;T\}$. For every $c \in S$, for each $T_i \in M$, there is some $a_i\tilde{\in}T_i$ such that $c\,\rho_\tau\;a_i$. By Lemma 4, we have $c\,\rho_\tau\;\sqcap_j a_j$, where j indexes the sets in M.

Since $a_i\tilde{\in}T_i$ implies $\{\!|a_i|\!\} \sqsubseteq T_i$, for all $T_i \in M$, we have $\{\!|\sqcap_j a_j|\!\} \sqsubseteq T_i$, also. Hence, $\{\!|\sqcap_j a_j|\!\} \sqsubseteq \sqcap M$, implying $\{\!|\sqcap_j a_j|\!\}\tilde{\in}\sqcap M$, by Proposition 11. The proof for $\rho_{\overline{\tau}}$ is similar.

Clause (4): Similar to (3).

Missing are assurances of LUB-closure preservation for $\rho_{L(\tau)}$ and GLB-closure preservation for $\rho_{U(\tau)}$, which depend on the specific powersets used.[5] The following subsections explore these issues.

[5] This difficulty is foreshadowed by Backhouse and Backhouse [5], whose results are summarized in Section 11.

7.1 Lower powersets: $\rho_{L(\tau)} \subseteq \mathbb{P}_L(C_\tau) \times \mathbb{P}_L(A_\tau)$

Let $\rho_\tau \subseteq C \times A$. As noted by Proposition 22, when ρ_τ is U-closed, then $\rho_{\overline{\tau}} \subseteq \mathbb{P}_L(C_\tau) \times A_\tau$ is an instance of $\rho_{L(\tau)} \subseteq \mathbb{P}_L(C_\tau) \times \mathbb{P}_L(A_\tau)$. Closure-preservation properties of $\rho_{\overline{\tau}}$ are documented by Theorem 14.

In the case when $\mathbb{P}_L(A_\tau)$ is an arbitrary lower powerset, one can always employ $\mathbb{P}_\downarrow(C)$ to obtain LUB-closure:

Proposition 26 *For all $\rho_\tau \subseteq C_\tau \times A_\tau$, for any choice of $\mathbb{P}_L(A_\tau)$, $\rho_{L(\tau)} \subseteq \mathbb{P}_\downarrow(C_\tau) \times \mathbb{P}_L(A_\tau)$ is LUB-closed.*

PROOF. In $\mathbb{P}_\downarrow(C_\tau)$, join is set union, meaning that $c \in \sqcup\{S \mid S\,\rho_{L(\tau)}\,T\}$ iff there is some S' such that $c \in S'$ and $S'\,\rho_{L(\tau)}\,T$.

In the general case, preservation of LUB-closure is delicate. For example, for the lower powerdomain construction, $\mathbb{P}_{Scott}(D) = (\{Scott(S) \mid S \subseteq D\}, \subseteq, \downarrow, Scott \circ \cup)$, where $Scott(S)$ is the closure of S in D's Scott-topology, there exist U-L-LUB closed relations, $\rho_\tau \subseteq C \times A$, where $\rho_{L(\tau)} \subseteq \mathbb{P}_{Scott}(C) \times \mathbb{P}_{Scott}(A)$ is *not* LUB-closed. But we do have:

Proposition 27 *If $\rho_\tau \subseteq C_\tau \times A_\tau$ is U-GLB-L-LUB-closed, then so is $\rho_{L(\tau)} \subseteq \mathbb{P}_{Scott}(C_\tau) \times \mathbb{P}_{Scott}(A_\tau)$.*

PROOF. In showing LUB-closure, the only interesting case is when $c \in \sqcup\overline{S}$, where $\overline{S} = \sqcup\{S \in \mathbb{P}_{Scott}(C) \mid S\,\rho_{L(\tau)}\,T\}$ and c is the least-upper bound of a chain, $\{c_0, c_1, \cdots, c_i, \cdots\} \subseteq \cup\overline{S}$, for $T \in \mathbb{P}_{Scott}(A)$.

In this situation, for all $i \geq 0$, $c_i\,\rho_\tau\,a_i$, for some $a_i \in T$. By L-GLB-closure, each $c_i\,\rho_\tau\ \sqcap\{a_j \mid i \leq j\}$, for all $i \geq 0$, and the $\sqcap\{a_j \mid i \leq j\}$'s form a chain, for $i \geq 0$. The least-upper bound of this chain falls in T, because it is Scott-closed, and by U-LUB closure (which implies Scott-inclusivity), we have that c is related to this least-upper bound.

7.2 Upper powersets: $\rho_{U(\tau)} \subseteq \mathbb{P}_U(C_\tau) \times \mathbb{P}_U(A_\tau)$

Here, GLB-closure is not guaranteed, but we have the following:

Proposition 28 *Recall that $\mathbb{P}_\uparrow(A) = (\{\uparrow D \mid D \subseteq A\}, \supseteq, \uparrow, \cup)$. Then $\rho_{U(\tau)} \subseteq \mathbb{P}_U(C) \times \mathbb{P}_\uparrow(A)$, is GLB-closed, for all choices of upper powersets, $\mathbb{P}_U(C)$.*

PROOF. In $I\!P_{\uparrow}(A)$, meet is set union, which gives GLB-closure.

And as suggested by Proposition 27, if $\rho_\tau \subseteq C_\tau \times A_\tau$ is U-GLB-L-LUB-closed, then $\rho_{U(\tau)} \subseteq I\!P_{Smyth}(C_\tau) \times I\!P_{Smyth}(A_\tau)$, is GLB-closed, where $I\!P_{Smyth}(D)$ is the upper ("Smyth") powerdomain of D [39,46].

7.3 Function spaces: $\rho_{\tau_1 \to \tau_2} \subseteq (C_{\tau_1} \to C_{\tau_2}) \times (A_{\tau_1} \to A_{\tau_2})$

The following result, crucial to the rest of the paper, equates Galois-connection-based soundness to the logical relation between functions:

Proposition 29 *Let $\rho_{\tau_i} \subseteq C_{\tau_i} \times A_{\tau_i}$, for $i \in 1..2$, be U-GLB-L-LUB-closed. so that there are the Galois connections, $C_{\tau_i}\langle \alpha_{\rho_{\tau_i}}, \gamma_{\rho_{\tau_i}} \rangle A_{\tau_i}$, $i \in 1..2$. For $f : C_{\tau_1} \to C_{\tau_2}$, $f^\sharp : A_{\tau_1} \to A_{\tau_2}$,*

$$f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp \textit{ iff } \alpha_{\rho_{\tau_2}} \circ f \sqsubseteq_{C_1 \to A_2} f^\sharp \circ \alpha_{\rho_{\tau_1}} \textit{ iff } f \circ \gamma_{\rho_{\tau_1}} \sqsubseteq_{A_1 \to C_2} \gamma_{\rho_{\tau_2}} \circ f^\sharp.$$

PROOF. If: Assume $c \, \rho_{\tau_1} \, a$, implying $\alpha_{\tau_1}(c) \sqsubseteq a$. By monotonicity, $f^\sharp(\alpha_{\tau_1}(c)) \sqsubseteq f^\sharp(a)$. Using the assumption, we deduce $\alpha_{\tau_2}(f(a)) \sqsubseteq f^\sharp(a)$, implying $f(a) \, \rho_{\tau_2} \, f^\sharp(a)$.

Only if: By definition, for all $c \in C_{\tau_1}$, $c \, \rho_{\tau_1} \, \alpha_{\tau_1}(c)$. By assumption, we obtain $f(c) \, \rho_{\tau_2} \, f^\sharp(\alpha_{\tau_1}(c))$, which by definition, gives $\alpha_{\rho_{\tau_2}}(f(c)) \sqsubseteq f^\sharp(\alpha_{\rho_{\tau_1}}(c))$.

The remaining equivalence follows from the definition of Galois-connection-based soundness.

As a corollary, $f \, \rho_{\tau_1 \to \tau_2} \, {f^\sharp}_{best}$, where ${f^\sharp}_{best}(a) = \alpha_{\rho_{\tau_2}} \circ f \circ \gamma_{\rho_{\tau_1}}$.

Starting again with $\rho_{\tau_i} \subseteq C_{\tau_i} \times A_{\tau_i}$, $i \in 1..2$, if we have that ρ_{τ_2} is not LUB-closed, then we might complete it to $\rho_{\overline{\tau_2}} \subseteq I\!P_{\downarrow}(C_2) \times A_2$ and generate $\rho_{\tau_1 \to \overline{\tau_2}} \subseteq (C_1 \to I\!P_{\downarrow}(C_2)) \times (A_1 \to A_2)$. Or, we might generate the relation, $\rho_{\overline{\tau_1 \to \tau_2}} \subseteq I\!P_{\downarrow}(C_1 \to C_2) \times (A_1 \to A_2)$; in this latter case, the Galois connection is $I\!P_{\downarrow}(C_1 \to C_2)\langle \alpha^\phi, \gamma^\phi \rangle (A_1 \to A_2)$, where $\gamma^\phi f^\sharp = \{f \mid f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp\} = \{f \mid \text{for all } c \in C_1, f(c) \sqsubseteq_{C_2} \gamma_{\tau_2}(f^\sharp(\alpha_{\tau_1}(c)))\}$. These and other interesting Galois connections generated from relations on functions can be found in [12].

8 Synthesizing a most-precise simulation

With the logical-relations machinery in hand, we address Dams's problem of synthesizing a most precise simulation (overapproximation) of a concrete transition relation.

Given the set of concrete states, C, transition relation $R \subseteq C \times C$, and a Galois connection $\mathbb{P}(C)\langle\alpha, \gamma\rangle A$, Dams [13,15] proved that the most precise, sound, abstract transition relation $R_0^\sharp \subseteq A \times A$ is

$$R_0^\sharp(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \mathit{min}\{S' \mid R^{\exists\exists}(\gamma(a), S')\}\}$$

where $R^{\exists\exists}(M, N)$ holds iff there exist $m \in M$ and $n \in N$ such that $(m, n) \in R$. Recoded as a function, $R_0^\sharp : A \to \mathbb{P}(A)$, and simplified, this reads

$$R_0^\sharp(a) = \{\alpha\{c'\} \mid \exists c \in \gamma(a), c' \in R(c)\}$$

because the sets, $\mathit{min}\{S' \mid R^{\exists\exists}(\gamma(a), S')\}$, are singletons.

Dams's notions of soundness and best precision were stated in terms of properties in Hennessy-Milner logic: Soundness meant that logical properties true of $R_0^\sharp$ also held for R, and best precision meant that $R_0^\sharp$ preserved the most properties of all sound abstractions of R.

By using Galois-connection techniques, we can derive soundness and best precision in a logic-independent, model-theoretic sense. Later we introduce the temporal logic and gain Dams's expressivity results for free.

Given U-GLB-closed $\rho_b \subseteq C \times A$ and transition function $R : C \to \mathbb{P}(C)$, we generate the L-LUB-U-GLB-closed relations, $\rho_{\overline{b}} \subseteq \mathbb{P}(C) \times A$ and $\rho_{L(b)} \subseteq \mathbb{P}(C) \times \mathbb{P}_L(A)$, and their corresponding Galois connections, $\mathbb{P}(C)\langle\alpha_{\overline{b}}, \gamma_{\overline{b}}\rangle A$ and $\mathbb{P}(C)\langle\alpha_{L(b)}, \gamma_{L(b)}\rangle\mathbb{P}_L(A)$. These give us the domain and codomain of the abstract transition function, $R_{\mathit{best}}^\sharp : A \to \mathbb{P}_L(A)$, which we define by means of abstract interpretation [10]:

$$\begin{aligned} R_{\mathit{best}}^\sharp(a) &= (\alpha_{L(b)} \circ \mathit{ext}_{\overline{b}}(R) \circ \gamma_{\overline{b}})(a) \\ &= \sqcap\{T \in \mathbb{P}_L(A) \mid (\mathit{ext}_{\overline{b}}(R)(\gamma_{\overline{b}}(\ a)))\rho_{L(b)}T\} \end{aligned}$$

(Note that $\mathit{ext}_{\overline{b}}(R) : \mathbb{P}(C) \to \mathbb{P}(C)$ is $\mathit{ext}_{\overline{b}}(R)(S) = \cup_{c\in S}R(c)$.) When we choose $\mathbb{P}_\downarrow(A)$ for $\mathbb{P}_L(A)$, we can prove that the above equals

$$\sqcup\{\{\!|\alpha_{\overline{b}}\{c'\}|\!\} \mid \exists c \in \gamma_{\overline{b}}(a), c' \in R(c)\} \ = \ \cup\{\downarrow \alpha_{\overline{b}}\{c'\} \mid \exists c \in \gamma_{\overline{b}}(a), c' \in R(c)\}$$

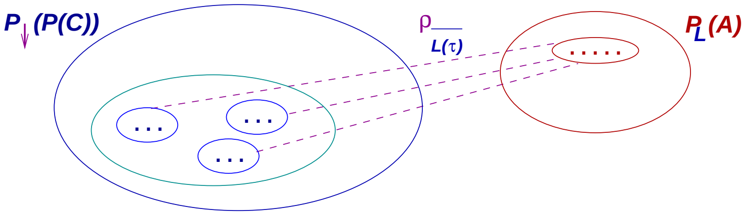
This is Dams's definition, when one takes into account the partial ordering on

A so that operations on $I\!\!P_{\downarrow}(A)$ are monotone.[6] Appealing to the standard results [10], we have that $R^\sharp_{best}$ is sound (cf. Proposition 29) with respect to R and is the most precise sound abstraction (that is, the meet of all sound abstractions) in domain $A \rightarrow I\!\!P_L(A)$.

Figure 6 presents $R^\sharp_{best}$ for the Collatz function, R, in Figure 5. (Transitions involving $\perp$ are omitted from the Figure.)

8.1 *Lifting the concrete domain*

In unpublished work [14], Dams justified his definition of $R^\sharp_0$ in terms of the Galois connections synthesized in the previous subsection. But as noted in Sections 1.4 and 3.1, we can justify $R^\sharp_0$ with a concrete domain whose elements are sets of sets of states: Given concrete-state set, C, and the transition relation $R \subseteq C \times C$, we retain the Galois connection, $I\!\!P(C)\langle\alpha_{\overline{b}}, \gamma_{\overline{b}}\rangle A$, for the domain of the abstract transition function, but the Galois connection for the codomain is generated from U-GLB-L-LUB-closed $\rho_{\overline{L(b)}} \subseteq I\!\!P_{\downarrow}(I\!\!P(C)) \times I\!\!P_L(A)$:



The diagram reminds us that a set of abstract values, $T \in I\!\!P_L(A)$ concretizes to the set, $\overline{S}$, such that for every $S \in \overline{S}$, S is overapproximated by T. The Galois connection is $I\!\!P_{\downarrow}(I\!\!P(C))\langle\alpha_{\overline{L(b)}}, \gamma_{\overline{L(b)}}\rangle I\!\!P_L(A)$. We define $R^\sharp_{best2} : A \rightarrow I\!\!P_L(A)$ as

$$R^\sharp_{best2} = \alpha_{\overline{L(b)}} \circ R^* \circ \gamma_{\overline{b}}$$

$$\text{where } R^*(S) = (ext_{\overline{b}}(\{\!|\cdot|\!\} \circ R))(S) = \sqcup\{\{\!|R(c)|\!\} \mid c \in S\}$$

Here, $\{\!|\cdot|\!\} : I\!\!P(C) \rightarrow I\!\!P_{\downarrow}(I\!\!P(C))$ is $\{\!|S|\!\} =\downarrow\{S\} = \{S' \mid S' \subseteq S\}$, so $R^*(S) =\downarrow\{R(c) \mid c \in S\}$, showing that R^* maps a set of arguments to all subsets of R-successor sets. By calculation, we can show that $R^\sharp_{best2}$ equals $R^\sharp_{best}$. An example of the construction is seen in Figure 3.

This redevelopment of $R^\sharp_{best}$ is notational overkill, but there is an important point: *Simulation equivalence is preserved when a concrete transition function*

[6] Dams does not address the monotonicity issue, but no harm is done: For all $a \in A$, $R^\sharp_0(a) \equiv R^\sharp_{best}(a)$ with respect to the lower-powerset equivalence in Definition 10.

is lifted to a function that maps a set of arguments to a set of answer sets:

Proposition 30 *Let $R : C \to \mathbb{P}(C)$ and $R^\sharp : A \to \mathbb{P}_L(A)$. Then the following are equivalent:*

(1) $R \lhd_\rho R^\sharp$
(2) $R\, \rho_{b \to L(b)}\, R^\sharp$
(3) $ext_{\overline{b}}(R)\, \rho_{\overline{b} \to L(b)}\, R^\sharp$*, assuming* $\rho_{L(b)}$ *is LUB-closed*
(4) $R^*\, \rho_{\overline{b} \to \overline{L(b)}}\, R^\sharp$*, assuming* $\rho_{\overline{L(b)}}$ *is LUB-closed*

PROOF. Recall that $ext_{\overline{b}}(R)(S) = \sqcup\{R(c) \mid c \in S\}$ and $R^*(S) = \sqcup\{\{\!|R(c)|\!\} \mid c \in S\}$.

(1) is equivalent to (2) by Proposition 24.

(3) implies (2): Assume $c\, \rho_b a$; this implies $\{c\}\, \rho_{\overline{b}}\, a$, which implies that $R(c) = ext_{\overline{b}}(R)\{c\}\, \rho_{L(b)}\, R^\sharp(a)$.

(4) implies (3): Assume $S\, \rho_{\overline{b}}\, a$. By assumption, we have $\sqcup\{\{\!|R(c)|\!\} \mid c \in S\}\, \rho_{\overline{L(b)}}\, R^\sharp(a)$. So, for all $c \in S$, we have $\{\!|R(c)|\!\}\, \rho_{\overline{L(b)}}\, R^\sharp(a)$, which implies $R(c)\, \rho_{L(b)}\, R^\sharp(a)$. The result follows from the LUB-closure of $\rho_{L(b)}$ and the definition of $ext_{\overline{b}}(R)$.

(2) implies (4): Assume $S\, \rho_{\overline{b}}\, a$. For every $c \in S$, we have $R(c)\, \rho_{L(b)}\, R^\sharp(a)$, by assumption. By Proposition 11(4) and (6), we know that $S' \in \{\!|R(c)|\!\}$ iff $S' \sqsubseteq R(c)$. By L-closure of $\rho_{L(b)}$, this means $\{\!|R(c)|\!\}\, \rho_{\overline{L(b)}}\, R^\sharp(a)$. The result follows from LUB-closure of $\rho_{\overline{L(b)}}$ and the definition of R^*.

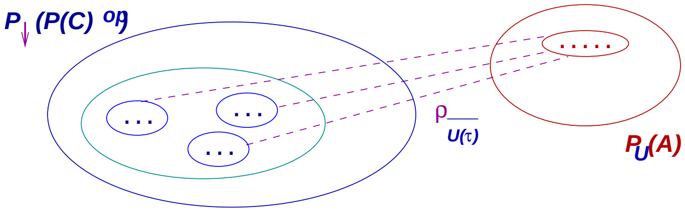
Similar equivalences will prove useful with underapproximations.

9 Synthesizing a most-precise dual simulation

An underapproximation analysis uses an abstract transition function, $R^\flat : A \to \mathbb{P}_U(A)$, and it is tempting to try constructing a Galois connection of the form, $\mathbb{P}(C)^{op}\langle\alpha_{U(b)}, \gamma_{U(b)}\rangle\mathbb{P}_U(A)$. But this requires $\rho_{U(b)} \subseteq \mathbb{P}(C)^{op} \times \mathbb{P}_U(A)$ be LUB-closed, which is difficult to achieve.[7] Fortunately, we can apply the

[7] Recall the example in Section 1.3: $\rho_{U(N)} \subseteq \mathbb{P}(Nat)^{op} \times \mathbb{P}_{\uparrow}(Parity)$. What is the least set of numbers that "witnesses" $\{even, any\}$? $\{0\}$? $\{2\}$? LUB-closure fails.

approach seen in the previous Section and define a *sound, overapproximation of underapproximations* in terms of $\rho_{\overline{U(\tau)}} \subseteq I\!\!P_{\downarrow}(I\!\!P_U(C)) \times I\!\!P_U(A)$:



A set of abstract values, $T \in I\!\!P_U(A)$, abstracts the set of sets, $\overline{S} \in I\!\!P_L(I\!\!P(C)^{op})$, iff T underapproximates each $S \in \overline{S}$.

We can incrementally construct $\rho_{\overline{U(\tau)}}$:

(1) Begin with a U-GLB-closed $\rho_b \subseteq C \times A$;
(2) Lift it to a U-L-GLB-closed $\rho_{U(b)} \subseteq I\!\!P(C)^{op} \times I\!\!P_{\uparrow}(A)$;[8]
(3) Complete it to a U-GLB-L-LUB-closed $\rho_{\overline{U(b)}} \subseteq I\!\!P_{\downarrow}(I\!\!P(C)^{op}) \times I\!\!P_{\uparrow}(A)$.

The resulting Galois connection, $I\!\!P_{\downarrow}(I\!\!P(C)^{op})\langle \alpha_{\overline{U(b)}}, \gamma_{\overline{U(b)}} \rangle I\!\!P_{\uparrow}(A)$, is defined

$$\gamma_{\overline{U(b)}}(T) = \{S \mid S\, \rho_{U(\tau)}\ T\}$$
$$\alpha_{\overline{U(\tau)}}\overline{S} = \sqcap\{T \in I\!\!P_U(A) \mid \text{ for all } S \in \overline{S}, S\, \rho_{U(b)}\ T\}$$

An example of the construction is seen in Figure 4.

Recall that Dams proved, for Galois connection $I\!\!P(C)\langle\alpha,\gamma\rangle A$ and transition relation $R \subseteq C \times C$, that the most precise, sound, underapproximating abstract transition relation, $R_0^\flat \subseteq A \times A$ is

$$R_0^\flat(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \mathit{min}\{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}$$

where $R^{\forall\exists}(M,N)$ holds iff for all $m \in M$, there exists $n \in N$ such that $(m,n) \in R$. Dams noted, for some $a \in A$, that $\mathit{min}\{S' \mid R^{\forall\exists}(\gamma(a), S')\}$ might be *empty* [15]; in such a case he decreed that $R_0^\flat$ is undefined, *min* should be removed, and the following definition should be used instead:

$$R_1^\flat(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}$$

This always yields a sound and most-precise $R_1^\flat$ (but with larger cardinality than $R_0^\flat$, when the latter exists). We study this anomaly momentarily.

[8] C is a set, so $I\!\!P(C)^{op}$, ordered by $\supseteq$, is an upper powerset.

Recoded as a function and simplified, $R_1^\flat$ reads

$$R_1^\flat(a) = \{\alpha(Y) \mid \text{for all } c \in \gamma(a), R(c) \cap Y \neq \{\}\,\}$$

The Galois-connection machinery gives us the same result: given transition function, $R : C \to I\!P(C)$, we use the Galois connection, $I\!P(C)\langle\alpha_{\overline{b}}, \gamma_{\overline{b}}\rangle A$, to generate the domain, and we use $I\!P_\downarrow((I\!P(C)^{op}))\langle\alpha_{\overline{U(b)}}, \gamma_{\overline{U(b)}}\rangle I\!P_\uparrow(A)$, which was derived at the beginning of this section, to generate the codomain of the abstract transition function, $R^\flat_{best} : A \to I\!P_\uparrow(A)$:

$$R^\flat_{best} = \alpha_{\overline{U(b)}} \circ R^* \circ \gamma_{\overline{b}}, \;\; \text{where } R^* = \mathit{ext}_{\overline{b}}(\{\!|\cdot|\!\} \circ R)$$

Now, $\{\!|\cdot|\!\} \circ R : C \to I\!P_\downarrow(I\!P(C)^{op})$ is $(\{\!|\cdot|\!\} \circ R)(c) = \downarrow_{I\!P(C)^{op}} R(c) = \{S' \mid S' \supseteq R(c)\}$. This makes $R^* = \mathit{ext}_{\overline{b}}(\{\!|\cdot|\!\} \circ R) : I\!P(C) \to I\!P_\downarrow(I\!P(C)^{op})$ equal to $R^*(S) = \sqcup_{c\in S}\{S' \mid S' \supseteq R(c)\} = \cup_{c\in S}\{S' \mid S' \supseteq R(c)\} = \{S' \supseteq R(c) \mid c \in S\}$.

That is, R^* maps a set of arguments to all supersets of R-successor sets. We simplify $R^\flat_{best}$ and obtain

$$\begin{aligned} R^\flat_{best}(a) &= \sqcap\{T \in I\!P_\uparrow(A) \mid \{S' \supseteq R(c) \mid c \in \gamma_{\overline{b}}(a)\}\,\rho_{\overline{U(b)}}\, T\} \\ &= \sqcap\{T \in I\!P_\uparrow(A) \mid \{R(c) \mid c \in \gamma_{\overline{b}}(a)\}\,\rho_{\overline{U(b)}}\, T\} \\ &= \sqcap\{T \in I\!P_\uparrow(A) \mid \text{for all } c \in \gamma_{\overline{b}}(a), \text{for all } a' \in T, R(c) \cap \gamma_{\overline{b}}(a') \neq \{\}\,\} \end{aligned}$$

because $c'\,\rho_b\,a'$ iff $c' \in \gamma_{\overline{b}}(a')$. We now show that $R^\flat_{best} = R^\flat_1 = R^\flat_0$ (when the last function exists). For $a \in A$, let

$$\begin{aligned} &D^i_a = R^\flat_i(a), \;\; \text{for } i \in 0..1, \;\; \text{and} \\ &B_a = \{T \in I\!P_\uparrow(A) \mid \text{for all } c \in \gamma_{\overline{b}}(a), \text{for all } a' \in T, R(c) \cap \gamma_{\overline{b}}(a') \neq \{\}\,\}, \end{aligned}$$

so that $R^\flat_{best}(a) = \sqcap B_a$. We show that *(i)* $D^i_a \in B_a$, and *(ii)* D^i_a is a lower bound of B_a. This gives the desired equalities.

For *(i)*, consider $s \in \gamma_{\overline{b}}$. For every $\alpha_{\overline{b}}(Y)$ in D^i_a, we have that $R(s) \cap Y \neq \{\,\}$. Since $\alpha_{\overline{b}}, \gamma_{\overline{b}}$ form a Galois connection, we have that $R(s) \cap \gamma_{\overline{b}}(\alpha_{\overline{b}}(Y)) \neq \{\,\}$. Hence, $D^i_a \in B_a$.

For *(ii)*, we must show $D^i_a \sqsubseteq_{I\!P_\uparrow(A)} T$, for all $T \in B_a$. That is, for all $a \in T$, there exists $a' \in D^i_a$ such that $a' \sqsubseteq_A a$. The definition of B_a tells us, for all such T, for all $s \in \gamma_{\rho_{\overline{b}}}(a)$, that $R(s) \cap \gamma_{\rho_{\overline{b}}}(a) \neq \{\,\}$.

In the case for D^1_a, its definition tells us that $\alpha_{\rho_{\overline{b}}}(\gamma_{\rho_{\overline{b}}}(a)) \in D^1_a$, and the definition of Galois connection implies $\alpha_{\rho_{\overline{b}}}(\gamma_{\rho_{\overline{b}}}(a)) \sqsubseteq_A a$. In the case for D^0_a, there is some minimal $S' \subseteq \gamma_{\rho_{\overline{b}}}(a)$ such that $R(s) \cap S' \neq \{\}$. The result follows as for D^1_a.

This concludes the demonstration that $R^\flat_{best} = R^\flat_1 = R^\flat_0$. The reasoning tacitly assumes that D^i_a is an element of $I\!\!P_\uparrow(A)$, that is, D^i_a is upwards closed in A. Although D^0_a might not be upwards closed, it is *equivalent* to $\uparrow_A D^0_a = D^1_a$ with respect to the upper-powerset equivalence defined in Definition 17. This explains why both D^0_a and D^1_a are "the" greatest lower bound — they are the same element in $I\!\!P_\uparrow(A)$. Figure 7 presents $R^\flat_{best}$ (that is, $R^\flat_1$) for the Collatz function, R, in Figure 5.

Finally, dual simulation lifts to sets of arguments:

Proposition 31 *$R^\flat \lhd_{\rho^{-1}} R$ iff $R\, \rho_{b \to U(b)}\, R^\flat$ iff $R^*\, \rho_{\overline{b} \to \overline{U(b)}}\, R^\flat$, assuming that $\rho_{\overline{U(b)}}$ is LUB-closed.*

PROOF. Similar to the proof of Proposition 30.

10 Validation and refutation logics

Hennessy and Milner proved that $\Box\Diamond$-propositions (*Hennessy-Milner logic*) characterize transition relations up to bisimilarity [27]. Loiseaux, et al. [32], proved that all $\Box$-properties true of a sound overapproximating transition relation are preserved in the corresponding concrete transition relation and that when one overapproximating transition relation is more precise than another, then the first preserves all the $\Box$-properties of the second. Dams extended this result to underapproximations and $\Diamond$-properties and proved that his definitions of $R^\sharp_{best}$ and $R^\flat_{best}$ possess the most $\Box\Diamond$-propositions of any sound, mixed transition system.

In this section, we manufacture Hennessey-Milner logic from our family of logical relations (cf. [2]) and obtain the above results as corollaries of abstract-interpretation theory. Recall that these are the typings of the logical relations,

$$\tau \ ::= \ b \mid \tau_1 \to \tau_2 \mid L(\tau) \mid U(\tau) \mid \overline{\tau}$$

where $\overline{\tau}$ is an instance of $L(\tau)$. For each of the first four typings, we extract a corresponding assertion form that can be validated on elements with the indicated typing. Here is the assertion language:

$$\phi \ ::= \ p \mid f.\phi \mid \forall\phi \mid \exists\phi$$

Primitive assertions, p, are validated on elements of base type. For function

f of type $\tau_1 \to \tau_2$, $f.\phi$ denotes an "application" property that holds for an argument, d, of type τ_1, exactly when ϕ holds for the answer, $f(d)$, of type τ_2. $\forall\phi$ holds for set S of type $\mathbb{P}_L(\tau)$ when ϕ holds for each of S's τ-typed elements. The dual property, $\exists\phi$, is validated on $\mathbb{P}_U(\tau)$-typed sets.

We formalize these notions: Assume, for all types, τ, that the logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$, are defined for fixed domains C_τ and A_τ. Assume also, for all function symbols, f, typed $\tau_1 \to \tau_2$, there are interpretations $f^\natural : C_{\tau_1} \to C_{\tau_2}$, and $f^\sharp : A_{\tau_1} \to A_{\tau_2}$, such that $f^\natural \, \rho_{\tau_1 \to \tau_2} \, f^\sharp$.

Definition 32 *The semantics of the assertion language is defined by the following family of well-typed judgements; let D_τ denote either a concrete domain, C_τ, or an abstract domain, A_τ:*

$$d \models_b p \text{ is given, for } d \in D_b$$

$$d \models_{\tau_1 \to \tau_2} f.\phi \;\text{ iff } f(d) \models_{\tau_2} \phi, \;\text{ for } d \in D_{\tau_1} \text{ and } f \in D_{\tau_1 \to \tau_2}$$

$$S \models_{L(\tau)} \forall\phi \;\text{ iff for all } d \tilde{\in} S, d \models_\tau \phi, \;\text{ for } S \in D_{L(\tau)}$$

$$S \models_{U(\tau)} \exists\phi \;\text{ iff there exists } d \tilde{\in} S \text{ such that } d \models_\tau \phi, \;\text{ for } S \in D_{U(\tau)}$$

Since $\overline{\tau}$ is an instance of $\mathbb{P}_L(\tau)$, define

$$S \models_{\overline{\tau}} \phi \textit{ iff for all } c \in S, c \models_\tau \phi \textit{ for } S \in C_{L(\tau)}$$

$$a \models_{\overline{\tau}} \phi \textit{ iff } a \models_\tau \phi, \;\textit{ for } a \in A_\tau$$

At the end of this section, we show how to dispense with $\models_{\overline{\tau}}$.

We can abbreviate $d \models_{\tau \to L(\tau)} R.\forall\phi$ by $d \models \forall R\phi$ (as in *description logic* [4]) or by $[R]\phi$ (*Hennessy-Milner logic* [27]) or by $\Box\phi$ when the system studied has only one transition function, $R : D_\tau \to \mathbb{P}(D_\tau)$. This hides the reasoning on sets. Similarly, $d \models_{\tau \to U(\tau)} R.\exists\phi$ can be abbreviated by $d \models \exists R\phi$ or $\langle R\rangle\phi$ or $\Diamond\phi$.

The judgements for $\forall R\phi$ and $\exists R\phi$ employ $R^\sharp$ and $R^\flat$, respectively, to validate the assertions, motivating Dams's mixed transition systems. [9]

[9] For concrete set, C_τ, $\mathbb{P}(C_\tau)$ is a lower powerset and $\mathbb{P}(C_\tau)^{op}$ is an upper powerset, so we use the concrete transition function, R, to validate $\forall\phi$ and $\exists\phi$-properties on concrete sets.

Definition 33 *For type τ, the typed judgement form, $\models_\tau \phi$, is* sound *iff for all $c \in C_{\tau'}$ and $a \in A_{\tau'}$, if $c \,\rho_{\tau'}\, a$ and $a \models_\tau \phi$ holds true, then $c \models_{\tau'} \phi$ holds true.*[10]

Assume that $\models_b p$ is sound for each $\rho_b \subseteq C_b \times A_b$.[11]

Theorem 34 *For all types, τ, all judgement forms, $\models_\tau \phi$, are sound.*

PROOF. The proof is an easy induction on the structure of τ. For example, for $\tau = \tau_1 \to \tau_2$, say that $c \,\rho_{\tau_1}\, a$ and $a \models_{\tau_1 \to \tau_2} f.\phi$. Then, $f^\sharp(a) \models_{\tau_2} \phi$. Since $f^\natural \,\rho_{\tau_1 \to \tau_2}\, f^\sharp$, we have $f^\natural(c) \,\rho_{\tau_2}\, f^\sharp(a)$, and by the induction hypothesis, $f^\natural(c) \models_{\tau_2} \phi$.

10.2 Best precision of judgements

Say that a judgement form, $\models_{\tau'} \phi$, is *monotone* if $a \models_{\tau'} \phi$ and $a' \sqsubseteq_\tau a$ imply $a' \models_{\tau'} \phi$, for all $a, a' \in A_\tau$.[12]

We assume that all base-type judgements, $\models_b p$, are monotone, and from this it follows that all judgement forms are monotone.[13] As a consequence, we have immediately Dams's best-precision result:

Theorem 35 *For a fixed family of logical relations and domains, concrete transition function, $R^\natural : C_b \to I\!P(C_b)$, and Galois connection, $I\!P(C_b)\langle\alpha,\gamma\rangle A_b$, we have that $R^\sharp_{best} : A_b \to I\!P_L(A_b)$ and $R^\flat_{best} : A_b \to I\!P_U(A_b)$ soundly prove the most typed judgements, $a \models_\tau \phi$, for all $a \in A_{\tau'}$.*

PROOF. Given the domains, logical relations, and $R^\natural : C_b \to I\!P(C_b)$, say that we have sound over- and underapproximation functions, $R^\sharp_0 : A_b \to I\!P_L(A_b)$ and $R^\flat_0 : A_b \to I\!P_U(A_b)$ for interpreting the function symbol, R, in the assertion language. Call the resulting family of typed judgements, $\models^0$.

[10] Judgement form $\models_{\tau_1 \to \tau_2} f.\phi$ shows that τ' need not be τ.

[11] Example: Use elements $a \in A_b$ as the base-typed assertions, define $c \models_b a$ iff $c \,\rho_b\, a$, and then define $a' \models_b a$ iff for all $c \in C_b$, $c \,\rho_b\, a'$ implies $c \models_b a$.

[12] The intuition is that $\gamma_{\rho_\tau}(a') \subseteq \gamma_{\rho_\tau}(a) \subseteq [\![\phi]\!] \subseteq C_\tau$, where $[\![\phi]\!] = \{c \in C_\tau \mid c \models_{\tau'} \phi\}$.

[13] When ρ_b is U-closed and also ($a \models_b p$ iff for all $c \,\rho_b\, a, c \models_b p$), then $\models_b p$ is monotone.

Similarly, let $\models^{best}$ be the typed-judgement family when R is interpreted by $R^{\sharp}_{best}$ and $R^{\flat}_{best}$.

We must show, whenever $a \models^{0}_{\tau} \phi$, that $a \models^{best}_{\tau} \phi$ as well. The result follows by an induction on the structure of τ, and the only interesting case is the judgement form, $a \models^{0}_{b \to \tau'} R.\phi$, for $\tau' \in \{L(b), U(b)\}$. Consider $\tau' = L(b)$: By hypothesis, $R^{\sharp}_{0}(a) \models^{0}_{L(b)} \phi$. But $R^{\sharp}_{best} \sqsubseteq_{A_{b \to L(b)}} R^{\sharp}_{0}$, by the definition of Galois connection [10], and monotonicity tells us $R^{\sharp}_{best}(a) \models^{best}_{L(b)} \phi$. Similar reasoning holds for $\tau' = U(b)$.

Dams's result was proved for a logic with conjunction and disjunction. So, we define the connectives,

$$d \models_{\tau} \phi_1 \wedge \phi_2 \text{ iff } d \models_{\tau} \phi_1 \text{ and } d \models_{\tau} \phi_2$$

$$d \models_{\tau} \phi_1 \vee \phi_2 \text{ iff } d \models_{\tau} \phi_1 \text{ or } d \models_{\tau} \phi_2$$

The definitions are sound and monotone. To revise Theorem 35 to include the connectives, we must revise the proof so that it proceeds by induction on the structure of the assertions, ϕ, rather than the types, τ, in $\models_{\tau} \phi$. To do so, it is simplest to discard the judgement form, $\models_{\overline{\tau}} \phi$, since Proposition 22 lets us encode the "concrete judgement," $S \models_{\overline{\tau}} \phi$, by $S \models_{L(\tau)} \forall\phi$ and encode the "abstract judgement," $a \models_{\overline{\tau}} \phi$, by $\downarrow\! a \models_{L(\tau)} \forall\phi$ when all base-typed relations, $\rho_b \subseteq C_b \times A_b$, are U-closed and monotone.

10.3 Validating $\neg\phi$ requires a refutation logic

For $c \in C$, we define $c \models_{\tau} \neg\phi$ *iff* $c \not\models_{\tau} \phi$.

The logic developed so far validates properties, and we might have also a logic that *refutes* them: Read $a \models^{\neg}_{\tau'} \phi$ as "it is not possible that any value modelled by $a \in A_{\tau}$ has property ϕ." Here is the definition of a refutation logic:

$$a \models^{\neg}_{b} p \;\; \textit{is given, for } a \in A_b$$

$$a \models^{\neg}_{\tau_1 \to \tau_2} f.\phi \;\; \textit{iff } f^{\sharp}(a) \models^{\neg}_{\tau_2} \phi, \;\textit{for } a \in A_{\tau_1}, f^{\sharp} \in A_{\tau_1 \to \tau_2}$$

$$T \models^{\neg}_{U(\tau)} \forall\phi \;\; \textit{iff there exists } a \tilde{\in} T, a \models^{\neg}_{\tau} \phi, \;\textit{for } T \in A_{U(\tau)}$$

$$T \models^{\neg}_{L(\tau)} \exists\phi \;\; \textit{iff for all } a \tilde{\in} T, a \models^{\neg}_{\tau} \phi, \;\textit{for } T \in A_{L(\tau)}$$

In the refutation logic, the roles of $\mathbb{P}_L(\tau)$ and $\mathbb{P}_U(\tau)$ are exchanged.

Definition 36 $\models^{\neg}_{\tau'} \phi$ *is* sound *iff for all $c \in C_{\tau}$, $a \in A_{\tau}$, $c\, \rho_{\tau}\, a$ and $a \models^{\neg}_{\tau'} \phi$*

imply $c \not\models_{\tau'} \phi$.

Proposition 37 *For all types, τ, $\models^{\neg}_{\tau} \phi$ is sound and monotone, assuming that the base-type judgements, $\models^{\neg}_{b} p_b$, are.*[14]

A corollary of the above is a best-precision theorem, analogous to Theorem 35, for the refutation logic. Indeed, when we add these two (sound and monotone) definitions, unioning the two logics [28,31],

$$a \models_{\tau} \neg\phi \textit{ iff } a \models^{\neg}_{\tau} \phi$$

$$a \models^{\neg}_{\tau} \neg\phi \textit{ iff } a \models_{\tau} \phi$$

we maintain the best-precision theorem for the unioned logic:

Theorem 38 *For a fixed family of logical relations and domains, concrete transition function, $R^{\natural} : C_b \to \mathbb{P}(C_b)$, and Galois connection, $\mathbb{P}(C_b)\langle\alpha, \gamma\rangle A_b$, we have that $R^{\sharp}_{best} : A_b \to L(A_b)$ and $R^{\flat}_{best} : A_b \to \mathbb{P}_U(A_b)$ soundly prove the most typed judgements, $a \models_{\tau} \phi$ and $a \models^{\neg}_{\tau} \phi$, for all $a \in A_{\tau'}$.*

PROOF. A simultaneous but routine induction on assertions, ϕ, in $\models_{\tau} \phi$ and $\models^{\neg}_{\tau} \phi$.

The Sagiv-Reps-Wilhelm TVLA system simultaneously calculates validation and refutation logics[42]. Indeed, we might *combine* $\rho_{L(\tau)}$ and $\rho_{U(\tau)}$ into $\rho_{P\tau} \subseteq \mathbb{P}(C) \times (\mathbb{P}_L(A) \times \mathbb{P}_U(A))$. This motivates sandwich- and mixed-powerdomains in a theory of over-underapproximation of sets [6,21,25,28,29].

11 Related work

In addition to Dams's work [13,15], three other lines of research deserve mention:

[14] The intuition is that $a \models^{\neg}_{\tau'} \phi$ implies $\gamma_{\rho_{\tau}}(a) \cap [\![\phi]\!] = \{\}$. For base types, b, define $a \models^{\neg}_{b} p$ iff for all $c \in C_b$, $c\,\rho_b\, a$ implies $c \not\models_b p$. When ρ_b is U-closed, $\models^{\neg}_{b} p$ is sound and monotone.

11.1 Loiseaux, et al. [32]

Loiseaux, et al. showed an equivalence between simulations and Galois connections: For *sets* C and A, and $\rho \subseteq C \times A$, they note that $I\!\!P(C)\langle post[\rho], \tilde{pre}[\rho]\rangle I\!\!P(A)$ is always a Galois connection. [15]

For $R \subseteq C \times C$ and $R^\sharp \subseteq A \times A$, the notion of simulation is equivalently defined as R *is* ρ*-simulated by* $R^\sharp$ *iff* $R^{-1} \cdot \rho \subseteq \rho \cdot (R^\sharp)^{-1}$ Treating R^{-1} and $(R^\sharp)^{-1}$ as functions, we can define Galois-connection soundness as

$$(R^\sharp)^{-1} \textit{ is a sound overapproximation for } R^{-1} \textit{ with respect to } \gamma \textit{ iff}$$
$$pre[R] \circ \gamma \sqsubseteq_{I\!\!P(A) \rightarrow I\!\!P(C)} \gamma \circ pre[R^\sharp]$$

For ρ, R, $R^\sharp$, Loiseaux, et al. prove

1. R is ρ-simulated by $R^\sharp$ iff $(R^\sharp)^{-1}$ is sound for R^{-1} w.r.t. $\tilde{pre}[\rho]$.
2. $a \models \phi \in ACTL$ [8] implies $c \models \phi$, for $c\,\rho\,a$.

11.2 Backhouse and Backhouse [5]

Backhouse and Backhouse saw that Galois connections can be characterized within relational algebra, and they reformulated key results of Abramsky [1]: $\rho \subseteq C \times A$ is a *pair algebra* iff there exist $\alpha : C \rightarrow A$ and $\gamma : A \rightarrow C$ such that $\{(c, a) \mid \alpha(c) \sqsubseteq_A a\} = \rho = \{(c, a) \mid c \sqsubseteq_C \gamma(a)\}$.

For the category, C, of partially ordered sets *(objects)* and binary relations *(morphisms)*, *if* an endofunctor, $\sigma : C \Rightarrow C$, is also

(1) *monotonic*: for relations, $R, S \subseteq C \times C'$, $R \subseteq S$ implies $\sigma R \subseteq \sigma S$
(2) *invertible*: for all relations, $R \subseteq C \times C'$, $(\sigma R)^{-1} = \sigma(R^{-1})$,

then σ maps pair algebras to pair algebras, that is, σ is a unary type constructor that lifts a Galois connection between C and A to one between σC and σA.

The result generalizes to n-ary functors and applies to the standard functors, $\tau \times \tau$, $\tau \rightarrow \tau$, *List*(τ), etc. *But the result does not apply to* $I\!\!P_L(\tau)$ *nor* $I\!\!P_U(\tau)$ — *invertibility* (2) *fails.*

[15] Indeed, it is an *axiality* [17]: $\tilde{pre}[\rho] = \lambda T.\{c \mid \{a \mid c\,\rho\,a\} \subseteq T\}$ is ρ "reduced" to an underapproximation function, and $post[\rho] = \lambda S.\{a \mid \text{ exists } c \in S, c\,\rho\,a\}$. A's partial ordering, if any, is forgotten.

Ranzato and Tapparo studied the completion of upper closure maps, $\mu : \mathbb{P}(C) \rightarrow \mathbb{P}(C)$.[16] Given a logic, L, of form, $\phi \ ::= \ op_i(\phi_j)_{0<j<|op_i|}$, its semantics, $[\![\,\cdot\,]\!] \subseteq \mathbb{P}(C)$, has format

$$[\![op_i(\phi_j)]\!] = \mathbf{f_i}([\![\phi_j]\!])_{0<j<|op_i|}$$

where each $\mathbf{f_i} : \mathbb{P}(C)^{|op_i|} \rightarrow \mathbb{P}(C)$ gives the semantics of connector op_i. The abstract semantics has form, $[\![op_i(\phi_j)]\!]^\mu = (\mu \circ \mathbf{f_i})([\![\phi_j]\!]^\mu)$, and $[\![\phi]\!]^\mu \in \mu[\mathbb{P}(C)]$.

Upper closure μ is *L-preserving* if, for all $S \subseteq C$, $\mu S \subseteq [\![\phi]\!]^\mu$ *implies* $S \subseteq [\![\phi]\!]$, and it is *L-strongly preserving* if the *implies* is replaced by *iff*.

Ranzato and Tapparo showed that the coarsest upper closure that is strongly preserving is $\mu_L(S) = \cup\{T \subseteq C \mid$ for all $\phi, S \models \phi$ implies $T \models \phi\}$. Given an L-preserving μ, Ranzato and Tapparo apply the domain-completion technique of Giacobazzi and Quintarelli [18] to complete μ to its coarsest, strongly preserving form:

$$complete(\mu) = gfp(\lambda\rho.\mu \sqcap M(R_{\{\mathbf{f_i}\}}(\rho)))$$

where $\sqcap$ operates in the complete lattice of upper closures, M is the Moore completion, and $R_F(\mu) = \{f(\overline{x}) \mid f \in F, \overline{x} \in \mu[\mathbb{P}(C)]^{|f|}\}$ adds the image points of the logical operations, $\mathbf{f_i}$, to the domain.

In subsequent work [41], Ranzato and Tapparo applied the construction to synthesizing the Paige-Tarjan algorithm for computing the coarsest refinement of a state partition that bisimulates a Kripke structure: A state partition is expressed within a *partitioning domain* generated by an upper closure map, and the resulting strongly preserving closure preserves the most properties of the original Kripke structure within Hennessy-Milner logic.

This technique can be applied to the present paper to generate strongly preserving, over- and underapproximating Galois connections.

Acknowledgments

Michael Huth, and Radha Jagadeesen provided valuable advice within earlier collaborations. Radhia Cousot provided a supportive environment at École

[16] An upper closure map, $\mu : \mathbb{P}(C) \rightarrow \mathbb{P}(C)$, is monotone, extensive, and idempotent, and induces the Galois connection, $\mathbb{P}(C)\langle\mu, id\rangle\mu[\mathbb{P}(C)]$.

Polytechnique. Tino Cortesi, Patrick Cousot, Dennis Dams, and the referees contributed many useful comments.

References

[1] S. Abramsky. Abstract interpretation, logical relations, and Kan extensions. *J. Logic and Computation*, 1:5–41, 1990.

[2] S. Abramsky. Domain theory in logical form. *Ann.Pure Appl.Logic*, 51:1–77, 1991.

[3] B. Blanchet, et al. Design and implementation of a special-purpose static program analyzer for safety-critical real-time embedded software. In T. Mogensen, D. Schmidt, and I.H. Sudborough, editors, *The Essence of Computation*. Springer LNCS 2566, 2002.

[4] F. Baader, et al. *The Description Logic Handbook*. Cambridge Univ. Press, 2003.

[5] K. Backhouse and R. Backhouse. Galois connections and logical relations. In *Mathematics of Program Construction*, LNCS 2386. Springer Verlag, 2002.

[6] P. Buneman, S. Davidson, and A. Watters. A semantics for complex objects and approximate queries. In *7th ACM Symp. Principles of Database Systems*, 1988.

[7] G. Burn, C. Hankin, and S. Abramsky. Strictness analysis for higher-order functions. *Science of Computer Programming*, 7:249–278, 1986.

[8] E.M. Clarke, O. Grumberg, and D.A. Peled. *Model Checking*. MIT Press, 2000.

[9] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs. In *Proc. 4th ACM Symp. on Principles of Programming Languages*, pages 238–252. ACM Press, 1977.

[10] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM Symp. on Principles of Programming Languages*, pages 269–282. ACM Press, 1979.

[11] P. Cousot and R. Cousot. Abstract interpretation frameworks. *J. Logic and Computation*, 2:511–547, 1992.

[12] P. Cousot and R. Cousot. Higher-order abstract interpretation. In *Proceedings IEEE Int. Conf. Computer Lang.*, 1994.

[13] D. Dams. *Abstract interpretation and partition refinement for model checking.* PhD thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.

[14] D. Dams. personal communication, 2004.

[15] D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Prog. Lang. Systems*, 19:253–291, 1997.

[16] B.A. Davey and H.A. Priestly. *Introduction to Lattices and Order, 2d ed.* Cambridge Univ. Press, 2002.

[17] M. Erné, J. Koslowski, A. Melton, and G. Strecker. A primer on Galois connections. In *Summer Conference on General Topology and Applications*, Vol. 704, pages 103–125. Annuals of N.Y. Academy of Sciences, 1993.

[18] R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples, and refinements in abstract model checking. In *Static Analysis Symposium*, LNCS 2126, pages 356–373. Springer Verlag, 2001.

[19] R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47:361–416, 2000.

[20] O. Grumberg, F. Lerda, O. Strichman, and M. Theobald. Proof-guided underapproximation-widening for multi-process systems. In *Symp. Princ. of Programming Languages*. ACM, 2005.

[21] C. Gunter. The mixed power domain. *Theoretical Comp. Sci.*, 103:311–334, 1992.

[22] J. Hartmanis and R.E. Stearns. Pair algebras and their application to automata theory. *J. Information and Control*, 7:485–507, 1964.

[23] M. Hecht. *Flow Analysis of Computer Programs*. Elsevier, 1977.

[24] R. Heckmann. *Power domain constructions*. PhD thesis, Univ. Saarbrücken, 1990.

[25] R. Heckmann. Set domains. In *Proc. European Symp. Programming*, LNCS, pages 177–196. Springer Verlag, 1990.

[26] M. Hennessy and G. Plotkin. Full abstraction for a simple parallel programming language. In *Mathematical Foundations of Computer Science*, LNCS 74, pages 108–120. Springer Verlag, 1979.

[27] M.C.B. Hennessy and Robin Milner. Algebraic laws for non-determinism and concurrency. *JACM*, 32:137–161, 1985.

[28] M. Huth, R. Jagadeesan, and D.A. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In *Proc. European Symp. Programming*, LNCS, pages 155–169. Springer Verlag, 2001.

[29] M. Huth, R. Jagadeesan, and D.A. Schmidt. A domain equation for refinement of partial systems. *Mathematical Structures in Computer Science*, 14:469–505, 2004.

[30] N. Jones and F. Nielson. Abstract interpretation: a semantics-based tool for program analysis. In S. Abramsky, D. Gabbay, and T. Maibaum, editors, *Handbook of Logic in Computer Science, Vol. 4*, pages 527–636. Oxford Univ. Press, 1995.

[31] P. Kelb. Model checking and abstraction: a framework preserving both truth and failure information. Technical Report Technical report, OFFIS, University of Oldenburg, Germany, 1994.

[32] C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for verification of concurrent systems. *Formal Methods in System Design*, 6:1–36, 1995.

[33] R. Milner. *Communication and Concurrency.* Prentice-Hall, 1989.

[34] A. Mycroft and N.D. Jones. A relational framework for abstract interpretation. In *Programs as Data Objects*, LNCS 217, pages 156–171. Springer Verlag, 1985.

[35] F. Nielson. Two-level semantics and abstract interpretation. *Theoretical Comp. Sci.*, 69:117–242, 1989.

[36] F. Nielson, H.R. Nielson, and C. Hankin. *Principles of Program Analysis.* Springer Verlag, 1999.

[37] D. Park. Concurrency and automata in infinite strings. Lecture Notes in Computer Science 104, pages 167–183. Springer, 1981.

[38] C. Pasăreanu, R. Pelánek, and W. Visser. Concrete model checking with abstract matching and refinement. In *Computer-Aided Verification (CAV'05)*, LNCS. Springer Verlag, 2005.

[39] G. Plotkin. Domains. Lecture notes, Univ. Pisa/Edinburgh, 1983.

[40] F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. European Symp. Programming*, LNCS 2986, pages 18–32. Springer Verlag, 2004.

[41] F. Ranzato and F. Tapparo. An abstract-interpretation-based refinement algorithm for strong preservation. In *Proc. 11th Conf. on Tools and Algs. for Const. and Anal. of Systems*, LNCS 3440, pages 140–156. Springer Verlag, 2005.

[42] M. Sagiv, T. Reps, and R. Wilhelm. Parametric shape analysis via 3-valued logic. In *Proceedings 28th ACM POPL*, 1999.

[43] D.A. Schmidt. Structure-preserving binary relations for program abstraction. In *The Essence of Computation*, LNCS 2566, pages 246–266. Springer Verlag, 2002.

[44] D.A. Schmidt. Closed and logical relations for over- and under-approximation of powersets. In R. Giacobazzi, editor, *Static Analysis Symposium (SAS'04)*, LNCS 3148, pages 22–37. Springer Verlag, 2004.

[45] Z. Shmuely. The structure of Galois connections. *Pacific J. Mathematics*, 54:209–225, 1974.

[46] M. Smyth. Powerdomains. *Journal of Computer and System Sciences*, 16:23–36, 1978.