A calculus of logical relations for generating over- and under-approximating static analyses

David A. Schmidt

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

Abstract. Motivated by Dams’s studies of over- and underapproximation of state-transition relations, we define a calculus for Galois-connection building based on logical relations. For concrete domain, $C$, and corresponding abstract domain, $A$, we work with closed, binary approximation relations of the form, $\rho_r \subseteq C \times A$. We document the closure properties required to generate a Galois connection, $C(\alpha_r, \gamma_r)A$, from $\rho_r$ and show how the closure properties are generated and preserved when lifting $\rho_r$ to a higher order relation, $\rho_{F[\tau]} \subseteq F[C] \times F[A]$.

Next, we synthesize Dams’s most-precise under- and overapproximation transition relations using a calculus of logical relations on function space, lower powerset (for overapproximation), and upper powerset (for underapproximation); corollaries from Galois-connection theory give Dams’s hard-won completeness results.

As a bonus, the calculus of logical relations induces a validation logic; for Dams’s case study, the logic is Hennessy-Milner logic. An immediate corollary is that the synthesized over- and underapproximation transition relations validate the most logical properties that hold true for the corresponding concrete state-transition relation.

Galois connections underlie most static analyses of programs [8, 27, 35]: For complete lattices, $C$ and $A$, a pair of monotone maps, $\alpha : C \to A$ and $\gamma : A \to C$, define a Galois connection, written $C(\alpha, \gamma)A$, iff $\alpha \circ \gamma \subseteq id_A$ and $\gamma \circ \alpha \supseteq id_C$ [8, 15].

Galois connections possess rich internal structure [9, 15, 32, 40], and one purpose of this paper is to use binary relations, $\rho_r \subseteq C \times A$ [4, 20], to expose this structure and generate $C(\alpha_r, \gamma_r)A$. By working within a family of logical relations, we can lift $\rho_r$ to a higher-typed relation, $\rho_{F[\tau]} \subseteq F[C] \times F[A]$, that generates a Galois connection, $F[C](\alpha_{F[\tau]}, \gamma_{F[\tau]})F[A]$, between the higher-typed domains [1, 4].

The logical-relations approach reveals an important fact: Over- and underapproximation static analyses, which should be duals, indeed arise from dual constructions: a lower (“Hoare”) powerset relation [21, 23, 36] generates an overapproximation Galois connection, and an upper (“Smyth”) powerset relation [21, 23, 36, 41] generates an underapproximation. This characterization gives a simple explanation of Dennis Dams’s detailed studies of most-precise under- and

overapproximations of state-transition systems [12, 14]. Indeed, this paper uses Dams’s work to motivate, present, and justify our formulation of Galois connections as closed, logical relations. The paper is structured as follows.

Section 1 reviews the traditional treatment of over- and underapproximation as dual constructions, exposes the inherent difficulty in the duality, and suggests an alternative approach that uses lower and upper powersets. The alternative is applied in Section 2, showing how one might simplify Dams’s results on over- and underapproximation.

The formal development begins in Section 3, where Galois connections are characterized as \( U\text{-GLB-}L\text{-LUB-closed} \) binary relations between concrete and abstract domains. The lower and upper powerset constructions are carefully developed in Section 4, preparing the way in Section 5 for a calculus of logical relations that utilizes function and powerset types.

Generation and preservation of closure properties within the calculus are proved in Section 6, and Sections 7 and 8 apply the results to synthesizing Dams’s most-precise over- and underapproximating state-transition relations. Finally, Section 9 defines a validation logic extracted from the logical relations and shows that the most-precise approximation relations preserve the most properties in the logic.

1 Over- and underapproximation as duals

Almost all Galois-connection-based static analyses are overapproximating: Given a set, \( C \), of concrete values and a complete lattice, \((A, \subseteq_A)\), of abstract values, we build a Galois connection, \((\mathcal{P}(C), \subseteq)\langle \alpha_o, \gamma \rangle (A, \subseteq_A)\), and we say that \( S \subseteq C \) is (over-)approximated by \( a \in A \) iff \( S \subseteq \gamma(a) \). A standard example is approximation by parity, e.g.,

\[
\begin{array}{c}
\mathcal{P}(\text{Nat}) \\
\{ 2n \mid n \in \text{Nat} \} \\
\text{even} \\
\gamma \\
\text{Parity} \\
\alpha_o \\
S \\
\text{odd} \\
\text{any} \\
\text{none}
\end{array}
\]

where \( \alpha_o : \mathcal{P}(\text{Nat}) \to \text{Parity} \) is defined

\[
\alpha_o(S) = \bigcup \{ \{ \text{even} \mid \exists n \in \text{Nat}, 2n \in S \} \cup \{ \text{odd} \mid \exists n \in \text{Nat}, 2n + 1 \in S \} \}
\]

and \( \gamma : \text{Parity} \to \mathcal{P}(\text{Nat}) \) is \( \gamma(\text{none}) = \{ \}, \gamma(\text{even}) = \{ 2n \mid n \in \text{Nat} \}, \) etc.

We use the abstract values to proclaim properties of a program. For example, a static analysis that computes a program’s output to be \( \text{even} \in \text{Parity} \) asserts the universal property, “\text{even}” — all the program’s outputs are even-valued numbers, that is, the program’s concrete output must be a set, \( S \), such that \( S \subseteq \gamma(\text{even}) \):
We write $S \rho a$ to assert that $S$ is 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.

### 1.1 Underapproximation as an order-theoretic dual

The traditional way to define an underapproximating Galois connection is to invert the concrete and abstract domains, giving $(\mathcal{P}(C), \supseteq)(\alpha_u, \gamma)A^{op}$, where $A^{op} = (A, \sqsubseteq_A)$. Here is the dual of the parity example:

$$
\begin{align*}
&\text{even} \quad \gamma \\
&\text{odd} \\
&\text{any} \\
&\text{none} \\
\end{align*}
$$

$S \subseteq C$ is underapproximated by $a \in A$ iff $S \supseteq \gamma(a)$.

Here, $\text{even} \in \text{Parity}^{op}$ asserts that all even numbers are included in the program’s outputs — a strong assertion. Also, we may reuse $\gamma : A \rightarrow \mathcal{P}(C)$ as the upper adjoint from $A^{op}$ to $\mathcal{P}(C)^{op}$ iff $\gamma$ preserves meets in $(A, \sqsubseteq_A)$ — another strong demand.¹

Yet another unfortunate consequence of the dualization is that the natural underapproximation interpretation of a language’s constants is often “nothing.” For example, we might define the semantics of a programming language with an inductively defined interpretation function, $\llbracket \cdot \rrbracket : \text{Expression} \rightarrow \text{Environment} \rightarrow \text{Nat}$. For constant symbol, 2, we define $\llbracket 2 \rrbracket_e = 2$; then, we are forced to define the underapproximation interpretation, $\llbracket \cdot \rrbracket : \text{Expression} \rightarrow \text{Environment}^b \rightarrow \text{Parity}$, for the constant as

$$
\llbracket 2 \rrbracket^b_e = \text{none}
$$

because we require $\gamma(\llbracket 2 \rrbracket^b_e) \subseteq \{2\} = \{\llbracket 2 \rrbracket^b_{\gamma(c)}\}$. Thus, many program phrases are interpreted to nothing as well, e.g., the interpretation of $x+2$ goes

$$
\llbracket x+2 \rrbracket^b_e = \text{add}^b(\llbracket x \rrbracket^b_e, \llbracket 2 \rrbracket^b_e) = \text{add}^b(e(x), \text{none}) = \text{none}
$$

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

¹ Recall that $\gamma : A \rightarrow C$ is the upper adjoint of a Galois connection between $C$ and $A$ iff it preserves meets: $\forall a \in A \{\gamma(a) \mid a \in T\} = \gamma(\sqcap_A T)$, for all $T \subseteq A$. 

1.2 Underapproximation as existential quantification

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 "even," then the underapproximating $even \in Parity^{op}$ should assert "Seven" — there exists an even number in the program’s outputs, which is a set taken from $\{S \in \mathcal{P}(Nat) \mid S \cap \gamma(even) \neq \emptyset\}$. Let $\rho_u \subseteq C \times A$ denote the underapproximation relationship. For $A = Parity^{op}$ we have:

![Diagram](image)

that is, $S \rho_u a$ iff $S \cap \gamma(a) \neq \emptyset$. This interpretation permits a nontrivial underapproximation of constants, e.g., $[2]^{ev} = even$, and expressions: $[x + 2]^{ev} = add^e(e(x), even) = e(x)$.

But we cannot define an upper adjoint, $\gamma_u : Parity^{op} \to \mathcal{P}(Nat)^{op}$, in the usual way:

![Diagram](image)

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:

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

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.

1.3 Sets of properties and their interpretations

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

When we lift the $Parity$ abstract domain to a powerset, its overapproximating (universal) interpretation appears as follows:

![Diagram](image)
We use a lower powerset, $\mathcal{P}_1(P(Nat))$ (the elements are down-closed sets, ordered by $\subseteq$), for the abstract domain. (Lower powersets are developed later in the paper.) The upper adjoint, $\gamma$, concretizes each set of abstract values to a set of concrete sets. \(^2\)

Frankly, the use of $\mathcal{P}_1(P(Nat))$ in place of $P(Nat)$ gives no new precision to the example,\(^3\) nor do the extra elements in $\mathcal{P}_1(Parity)$ give more expressiveness. But the dual construction yields something new: When we use sets of abstract values in underapproximation analysis, an outcome like $\{\text{even, odd}\}$ asserts $\exists \{\text{even}, \text{odd}\} \equiv \exists \text{even} \land \exists \text{odd}$ — the output set includes an even value and an odd value:

We use an upper powerset, $\mathcal{P}_1(Parity)$ (up-closed sets, ordered by $\supseteq$), for the abstract domain. The concrete domain is lifted to a lower powerset of an upper powerset; the reasons are explained later in the paper.

The Galois connection just illustrated plays a crucial role in this paper’s case study, which we now introduce.

2 Introduction to mixed-transition systems

In his thesis [12] and in subsequent work [14], Dams studied over- and underapproximations of state-transition relations, $R \subseteq C \times C$, for a discretely ordered set,

\(^2\) There are precedents for using sets of abstract values: Given $\mathcal{P}(C)(\alpha, \gamma)A$, the replacement of $A$ by $\mathcal{P}_1(A)$, giving $\mathcal{P}(C)(\alpha', \gamma')\mathcal{P}_1(A)$, where $\gamma'(T) = \cup \{\gamma(a) \mid a \in T\}$, is the disjunctive completion of $A$ [9, 11], used when $\gamma'$ must preserve joins.

Second, given a function, $\beta : C \rightarrow A$, that maps each concrete value to its best approximation, the powerset construction can be used as a categorical functor, producing $\mathcal{P}_1(C)(\mathcal{P}_1(\beta), \gamma''\mathcal{P}_1(A))$, where $\mathcal{P}_1(\beta)(S) = \{\beta(c) \mid c \in S\}$ [6].

\(^3\) Because, for $\mathcal{P}(C)(\alpha, \gamma)\mathcal{P}_1(A)$ and $\mathcal{P}_1(\mathcal{P}(C))(\alpha', \gamma')\mathcal{P}_1(A)$, we typically have that $\gamma'(T) = \{S \mid S \subseteq \gamma(T)\}$. 

C, of states. (See the example state-transition system, (C, R), in Figure 1.) Given complete lattice, (A, ⊆A), and the Galois connection, (P(C), ⊆)(α, γ)(A, ⊆A), Dams defined an overapproximating transition relation, R² ⊆ A × A, and an underapproximating transition relation, R⁰ ⊆ A × A, as follows:

\[ aR²a' \text{ iff } a' \in \{ \alpha(Y) \mid Y \in \min\{ S' \mid R²³(\gamma(a), S') \} \} \]

\[ aR⁰a' \text{ iff } a' \in \{ \alpha(Y) \mid Y \in \min\{ S' \mid R⁰³(\gamma(a), S') \} \} \]

The difficult-to-read definitions are analyzed later in the paper. To understand them here, we write c ρ a — c is approximated by a — if c ∈ γ(a). Then,

- if c ρ a and c R c', then a R² a', where c' ρ a' — R² covers (overapproximates) all transitions that R may perform.
- if c ρ a and a R² a', then c R c', where c' ρ a' — R² asserts (underapproximates) some transition that R must perform.

In the terminology of process algebra, R² ρ-simulates R, and R ρ⁻¹-simulates R⁰. See Figure 1 for an example mixed transition system, (A, R², R⁰).

For the branching-time modalities □ (∀R) and (∃R), defined as

\[ a \models □ \phi \text{ iff for all } a', aR²a' \text{ implies } a' \models \phi \]
\[ a \models (\exists \phi \text{ iff there exists } a' \text{ such that } aR²a' \text{ and } a' \models \phi \]

Dams proved soundness: a □ ϕ and c ρ a imply c □ ϕ, for the usual interpretation of □ ϕ [16]. With impressive work, Dams also proved “best precision” [14]: For all ρ- (and ρ⁻¹-) simulations, R² and R⁰ preserve the most □(μ-calculus [29, 30]) properties.

2.1 Can we derive Dams’ results within Galois-connection theory?

Dams’ results are impressive but somewhat ad-hoc, in that he relates concrete and abstract states via a Galois connection, yet he does not use Galois connections to define and relate the over- and underapproximating abstract-transition relations to the concrete one. Indeed, it should be possible to reconstruct Dams’ results entirely within a theory of higher-order Galois connections and gain new insights in the process. We do so in this paper:

First, we treat R ⊆ C × C as R : C → P(C). This makes R² : A → P_L(A), where P_L(·) is a lower (downset-closed, ⊆-ordered) powerset constructor.⁵

Given the Galois connection, (P(C))(α, γ)(A), on states, we “lift” it to a Galois connection on sets of states, \( F[P(C)](α_{F[r]}, γ_{F[r]})(A) \), so that

1. \( R² \) ρ-simulates \( R² \) if ext(R) □ γ₂A F[P(C)] γ₉F[τ] R²
2. the soundness of \( a \models □ \phi \) follows from Item 1
3. \( R¹ \)₉best = α₉F[τ] ext(R) γ₉ preserves the most □-properties

⁴ For the record, \( R²³(M, N) \) holds iff there exist m ∈ M and n ∈ N such that mRn, and \( R⁰³(M, N) \) holds iff for all m ∈ M, there exists n ∈ N such that mRn.

⁵ Think of the elements of P_L(A) as properties, like \{ even, odd, none \} ⊆ \{ even, odd, none \} ∪ \{ even, odd, none \} ⊆ \{ even, odd, none \}, as described in Section 1.3.
Concrete transition system, \((C, R)\):
\[
C = \{c_0, c_1, c_2\}
\]
\[
R = \{(c_0, c_1), (c_1, c_2)\}
\]

Approximating the state set, \(C\), by \(A = \{\perp, a_0, a_{12}, \top\}\); \(\alpha : \mathcal{P}(C) \to A\) is:
\[
\alpha(c_0) = a_0, \quad \alpha(c_1) = a_{12} = \alpha(c_2) = \alpha(c_1, c_2),
\]
\[
\alpha(c_0, c_1, c_2) = \top = \alpha(c_0, c_1) = \alpha(c_0, c_2), \quad \alpha(\{\}) = \perp
\]

Overapproximating (“may” : \(\exists\)) transition system:
\[
A = \{\perp, a_0, a_{12}, \top\}
\]
\[
R^\triangleright = \{(a_0, a_{12}), (a_{12}, a_{12}), (\top, a_{12})\}
\]

Underapproximating (“must” : \(\forall\)) transition system:
\[
A = \{\perp, a_0, a_{12}, \top\}
\]
\[
R^\triangleleft = \{(a_0, a_{12}), (\perp, \perp)\}
\]

The mixed transition system is \((A, R^\triangleright, R^\triangleleft)\).

where \(ext(R)\) lifts \(R\) to operate on state sets; we develop this later.

We do similar work for \(R^{\text{best}} : A \to \mathcal{P}_U(A)\) and \(\Diamond \phi\), where \(\mathcal{P}_U(\cdot)\) is an upper (upset-closed, \(\supseteq\)-ordered) powerset constructor.\(^6\)

While constructing the Galois connection for \(\mathcal{P}_L(A)\), we must ask the crucial question: \(\text{What is } F[\mathcal{P}(C)]?\) That is, \(\text{how should we concretize those sets, } T \in \mathcal{P}_L(A)?\)

We answer this question with the ideas from Section 1: We write \(c \rho_T a\) to assert that \(c \in C\) is approximated by \(a \in A\). (As usual, for Galois connection, \(\mathcal{P}(C)(\alpha, \gamma_\top) A\), define \(c \rho_T a\) iff \(c \in \gamma_\top(a)\)). In the case of overapproximation, \(S \in \mathcal{P}(C)\) is approximated by \(T \in \mathcal{P}_L(A)\) iff \(S \rho_{L(\top)} T\), where

\[
S \rho_{L(\top)} T \text{ iff for every } c \in S, \text{ there exists } a \in T \text{ such that } c \rho_T a
\]

\(^6\) Think of the elements of \(\mathcal{P}_U(A)\) as properties, like \(\{\text{even}, \text{odd}, \top\} \equiv \exists(\text{even}, \text{odd}, \top) \equiv \exists \text{even} \land \exists \text{odd}\) from Section 1.3.

\(^7\) This is the lower half of the Egli-Milner ordering, such that when \(\rho_T \subseteq C \times C\) is \(\subseteq_\top\), freely generates the lower (“Hoare”) powerdomain [23, 36].
This suggests \( F[\mathcal{P}(C)] \) might be \( \mathcal{P}(C) \), and the concretization, \( \gamma_{L(\tau)} : \mathcal{P}_L(A) \rightarrow \mathcal{P}(C) \), might be \( \gamma_{L(\tau)}(T) = \{S \mid S \mathcal{P}_L(\tau) T\} \), which concretizes \( T \) to the largest set that is approximated by \( T \), yielding the commonly found Galois connection, \( \mathcal{P}(C)(\alpha_{L(\tau)} \cdot \gamma_{L(\tau)}) \mathcal{P}_L(A) \), so that \( R_{best} = \alpha_{L(\tau)} \circ ext(R) \circ \gamma_{\tau} \).

But, as suggested in Section 1.3, we might define \( F[\mathcal{P}(C)] \) as \( \mathcal{P}_L(\mathcal{P}(C)) \), because if an abstract state \( a \in A \) concretizes to a set of states, \( \gamma_{\tau}(a) \subseteq C \), then set \( T \in \mathcal{P}_L(A) \) should concretize to a set of sets of states. That is, \( \exists \in \mathcal{P}_L(\mathcal{P}(C)) \) is approximated by \( T \in \mathcal{P}_L(A_\tau) \) iff for every set \( S \in \exists \), \( S \rho_{L(\tau)} T \):

\[
\gamma_{L(\tau)} : \mathcal{P}_L(A_\tau) \rightarrow \mathcal{P}_L(\mathcal{P}(C)) \text{ as } \gamma_{L(\tau)}(T) = \{S \mid S \mathcal{P}_L(\tau) T\}, \text{ which concretizes } T \text{ to the set of all sets approximated by } T.
\]

As hinted in Section 1, both approaches to overapproximation generate the same definition of \( R_{best} : A \rightarrow \mathcal{P}_L(A) \), but the remainder of this paper shows why a sound underapproximation must utilize the second approach, where \( F[\mathcal{P}(C)] = \mathcal{P}_L(\mathcal{P}(C)^{op}) \). A set of sets, \( \exists \in \mathcal{P}_L(\mathcal{P}(C)^{op}) \), is underapproximated by a set \( T \in \mathcal{P}_U(A) \) iff for every set \( S \in \exists \), \( S \rho_{U(\tau)} T \), where

\[
S \rho_{U(\tau)} T \text{ iff for every } a \in T, \text{ there exists some } c \in S \text{ such that } c \rho_{\tau} a. \tag{8}
\]

Thus, \( \gamma_{U(\tau)} : \mathcal{P}_U(A) \rightarrow \mathcal{P}_L(\mathcal{P}(C)^{op}) \) is defined \( \gamma_{U(\tau)}(T) = \{S \mid S \mathcal{P}_U(\tau) T\} \), which yields Dams’s results for underapproximation. Figure 2 precisely restates the parity example in terms of this construction.

### 2.2 Overview of the results in this paper

We redevelop and extend Dams’s results [12, 14] within a higher-order Galois-connection framework [11]:

1. We show how Galois connections are generated from U-GLB-L-LUB-closed binary relations (cf. [10, 33, 39]) 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.

\[ \text{This is the upper half of the Egli-Milner ordering, and when } \rho_{\tau} \subseteq C \times C \text{ is } \subseteq_{\tau}, \text{ freely generates the upper ("Smyth") powerdomain [23, 36].} \]
Let \( \text{Nat} \) be the discretely ordered set of natural numbers, and let complete lattice

\[
\text{Parity} = \{\text{even}, \text{odd}, \text{none}\}
\]

We have the obvious Galois connection, \( \mathcal{P}(\text{Nat}) \xrightarrow{\alpha_{\text{Par}}} \gamma_{\text{Par}} \text{Parity} \), where \( \gamma_{\text{Par}}(\text{even}) = \{2n \mid n \in \text{Nat}\} \), \( \gamma_{\text{Par}}(\text{any}) = \text{Nat} \), etc. We can lift this to:

\[
\gamma_{\mathcal{U}(\text{Par})} : \mathcal{P}(\text{Parity}) \rightarrow \mathcal{P}(\mathcal{P}(\text{Nat})^{\circ})
\]

where \( \mathcal{P}(\text{Parity}) \) are the superset-ordered, up-closed subsets of \( \text{Parity} \), and \( \mathcal{P}(\mathcal{P}(\text{Nat})^{\circ}) \) are the subset-ordered, superset-closed subsets of \( \mathcal{P}(\text{Nat}) \).

\( \gamma_{\mathcal{U}(\text{Par})} \) is defined as follows:

\[
\begin{align*}
\gamma_{\mathcal{U}(\text{Par})}\{\} &= \text{all subsets of } \text{Nat} \\
\gamma_{\mathcal{U}(\text{Par})}\{\text{any}\} &= \text{nonempty subsets of } \text{Nat} \\
\gamma_{\mathcal{U}(\text{Par})}\{\text{even, any}\} &= \text{all sets with an even number} \\
\gamma_{\mathcal{U}(\text{Par})}\{\text{even, odd, any}\} &= \text{all sets with an even and an odd number} \\
\gamma_{\mathcal{U}(\text{Par})}\{\text{none, even, odd, any}\} &= \{\}
\end{align*}
\]

2. We define lower and upper powerset constructions, which are weaker forms of powerdomains appropriate for abstraction studies [11, 21, 36], and we note that the appropriate approximation relations on powersets are exactly the standard lower (“Hoare”) and upper (“Smyth”) orderings [36].

3. We use the powerset types within a family of logical relations, show when the logical relations preserve the closure properties in Item 1, and show that simulation can be proved via logical relations. We use the logical relations to build U-GLB-L-LUB-closed relations on the powerset types in Section 2.1, and we prove that Dams’s most-precise over- and underapproximating state-transition relations are the abstract functions defined from 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]), note their resemblance to Hennessey-Milner logic [24], and obtain easy proofs of soundness and best precision of the abstract functions.
3 Closed binary relations generate Galois connections

The following results are assembled from [4, 10, 20, 33, 34, 39, 40]: Let $C$ and $A$ be complete lattices, and let $c \rho a$ means $c$ is approximated by $a$.

**Definition 1.** For all $c, c' \in C$, for $a, a' \in A$, for $c \rho \subseteq C \times A$, $c \rho a$ is defined as $c$ being approximated by $a$.

1. U-closed iff $c \rho a$ and $a \subseteq a'$ imply $c \rho a'$
2. GLB-closed iff $c \rho \cap \{a \mid c \rho a\}$
3. L-closed iff $c \rho a$ and $c' \subseteq c$ imply $c' \rho a$
4. LUB-closed iff $\cup\{c \mid c \rho a\} \rho a$.

U- and L-closure ensure the soundness of an approximation relation, $\rho$, 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 $\alpha_\rho(c) = \cap \{a \mid c \rho a\}$ and $\gamma_\rho(a) = \cup \{c \mid c \rho a\}$.

**Proof.** $\alpha_\rho$ and $\gamma_\rho$ are monotone by L- and U-closure, respectively. We compute $\gamma_\rho(\alpha_\rho(c_0)) = \cup G$, 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 $c_0 \subseteq C \cup G$. The proof for $\alpha_\rho(\gamma_\rho(a_0))$ is similar.

Diagrammed, Proposition 2 looks like this:

Note that $c \rho a$ if $c \subseteq C \gamma_\rho(a)$ if $\alpha_\rho(c) \subseteq A a$.

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

Hartmanis and Stearns [20] use the Corollary to assert that $\rho_{\alpha\gamma}$ defines a pair algebra.

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

**Proof.** For (1), we have $c \rho \cap \{a \mid c \rho a\}$, by GLB-closure. Since $T \subseteq \{a \mid c \rho a\}$, $\cap \{a \mid c \rho a\} \subseteq \cap T$, implying $c \rho \cap T$, by U-closure. The proof for (2) is similar.
Let \(\text{Int}\) be the discretely ordered set of integers:

\[
\text{Int} = \{2m \mid m \in \text{Nat}\}
\]

\(\rho\) is U-GLB-closed but not LUB-closed. It is completed to

\[
\rho \subseteq P(\text{Int}) \times \text{Parity}.
\]

### 3.1 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 \(\rho\) lacks LUB-closure. We complete \(C\) to a powerset:

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

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

**Corollary 6.** If \(\rho \subseteq C \times A\) is U-GLB-closed, then \(P(C)(\alpha_{\rho^+}, \gamma_{\rho^+})A\) is a Galois connection, where \(\gamma_{\rho^+}(a) = \{c \mid c \rho a\}\) and \(\alpha_{\rho^+}(S) = \cap \{a \mid S \rho a\}\).

Note that \(c \rho a\) iff \(c \in \gamma_{\rho^+} a\).

The construction defined in Corollary 6 is fundamental to static analysis; Figure 3 shows a typical application. There is no implementation penalty in applying the Corollary, because the abstract domain retains its existing cardinality.

There is a less-well known dual completion:

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

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

**Corollary 8.** For sets \(C\) and \(A\) and \(\rho \subseteq C \times A\), we have that \(\overline{\rho^\top} \subseteq P(C) \times P(A)^{op}\) defines the Galois connection where

\[
\alpha_{\overline{\rho^\top}}(S) = \{a \mid \text{for all } c \in S, c \rho a\}
\]

\[
\gamma_{\overline{\rho^\top}}(T) = \{c \mid \text{for all } a \in T, c \rho a\}
\]
4 Powersets

When $D$ is partially ordered, the naive set-of-all-subsets construction will not suffice for the powerset of $D$.\footnote{Due to monotonicity requirements: e.g., for $a, b \in D$, say that $a \sqsubseteq b$. Then we must have that $[a] \subseteq [b]$ in $D$’s powerset, even though $\{a\} \nsubseteq \{b\}$.} We now introduce the form of powerset we employ:

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

- $(E, \sqsubseteq_E)$ is a complete lattice
- $\emptyset \cdot \emptyset$, the singleton operation, is monotone
- $\emptyset$, 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 $\text{ext}(f) : E \rightarrow M$ such that $\text{ext}(f)[d] = f(d)$, for all $d \in D$.

The definition is far weaker than that of Hennessy and Plotkin [23, 36], who demand that $(E, \sqsubseteq_E, \emptyset_E)$ form a (continuous) semi-lattice and for all (continuous) semi-lattices, $(M, \sqsubseteq_M, \\cup_M)$, that $\text{ext}(f)(S \cup T) = \text{ext}(f)(S) \cup_M \text{ext}(f)(T)$, where $\text{ext}(f)$ must be uniquely defined.

We omit the additional requirements because they often force $E$ to have “too many” elements than what can be practically implemented in a static analysis. (Of course, this makes $\cup$ less precise than true set union, a feature seen in many static analyses.)

Here are examples from Cousot and Cousot [11] of our format of powerset:

- **Down-set (order-ideal) completion:** For $d \in D$, $S \subseteq D$, define $|d| = \{e \in D \mid e \sqsubseteq d\}$ and $|S| = \bigcup \{|d| \mid d \in S\}$. Define $\mathcal{P}_1(D) = (\{|S| \mid S \subseteq D\}, \subseteq, \sqsubseteq, \sqcup)$. For $f : D \rightarrow M$, define $\text{ext}(f)(S) = \sqcup_{d \in S} f(d)$.
- **Scott-closed-set completion:** $(\mathcal{C}(S) \mid S \subseteq D), \subseteq, \sqsubseteq, \sqcup)$, where $\mathcal{C}(S)$ defines the Scott closure of $S \subseteq D$ is downwards closed and closed under least-upper bounds of directed sets in $D$. $\text{ext}(f)$ is defined as just seen.
- **Join completion (subsets of $\mathcal{P}_1(D)$):** $(M, \sqsubseteq, \sqcup, \sqcap)$, where $M \subseteq \{\|d\| \mid S \subseteq D\}$ is a Moore family (that is, closed under all intersections). $\text{ext}(f)$ is defined as before.

Join completions “add new joins” to $D$; the trivial join completion is $\text{triv}_L(D) = (\{|d| \mid d \in D\}, \subseteq, \sqsubseteq, \sqcup)$, which is order-isomorphic to $D$, and the most detailed join completion is $\mathcal{P}_1(D)$. The Scott-closed-set completion is a join completion. Figure 4 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 $\|d\| = \{e \in D \mid d \sqsubseteq e\}$ and $\|S\| = \bigcup \{|d| \mid d \in S\}$. Define $\mathcal{P}_1(D) = (\{|S| \mid S \subseteq D\}, \supseteq, \sqsubseteq, \sqcup)$. For monotone $f : D \rightarrow M$, let $\text{ext}(f) : \mathcal{P}_1(D) \rightarrow M$ be $\text{ext}(f)(S) = \sqcap_{d \in S} f(d)$.
- **Dual-join completion (subsets of $\mathcal{P}_1(D)$):** $(M, \supseteq, \sqcup, \sqcap)$, where $M \subseteq \{\|d\| \mid S \subseteq D\}$ is a Moore family. The trivial dual-join completion, $\text{triv}_U(D) = (\{|d| \mid d \in D\}, \supseteq, \sqsubseteq, \sqcap)$, is order-isomorphic to $D$. \[\footnote{Due to monotonicity requirements: e.g., for $a, b \in D$, say that $a \sqsubseteq b$. Then we must have that $[a] \subseteq [b]$ in $D$’s powerset, even though $\{a\} \nsubseteq \{b\}$.} \]
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.

4.1 Lower and strongly lower powersets

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

**Definition 10.** Powerset $P_L(D) = (E, \subseteq, \{\cdot\}, \uplus)$ is

1. a lower powerset iff $(S_1 \subseteq E S_2$ if, for all $x \in S_1$, there exists $y \in S_2$ such that $x \subseteq_D y$).
2. a strongly lower powerset iff $(S_1 \subseteq E S_2$ iff, for all $x \in S_1$, there exists $y \in S_2$ such that $x \subseteq_D y$).

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

The definition of lower powerset is the starting point for powerdomain theory [36], but we will see momentarily that the monotonicity requirements for $\{\cdot\}$ and $\uplus$ force every lower powerset to be strongly lower.

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

1. $S \subseteq E S \uplus T$
2. $S \subseteq_E \{\{d\} \mid d \in S\}$
3. $S \subseteq T$ iff for all $d \in S$, then $d \in T$ also
4. $d \in S$ iff $\{d\} \subseteq E S$
5. $S \subseteq T$ iff $S \subseteq_E T$
6. $d \subseteq_D e$ iff $\{d\} \subseteq_E \{e\}$.
Proof. Clause (1): for arbitrary \( d \in D \), let \( d \in S \), that is, \( \{d\} \sqcup S = S \). Then \( \{d\} \cup S \sqcup T = S \sqcup T \), implying \( S \sqsubseteq S \sqcup T \), by the definition of lower powerset.

Clause (3): if: By the definition of lower powerset, \( S \sqsubseteq T \), hence \( S \sqcup T \sqsubseteq T \sqcup T = T \), by (1) and the monotonicity of \( \sqcup \).

only if: Assume \( S \sqcup T = T \) and say that \( \{d\} \sqcup S = S \). Then, \( T = S \sqcup T = \{d\} \sqcup S \sqcup T = \{d\} \sqcup T \).

Clause (4): if: Assume \( \{d\} \sqsubseteq S \). By monotonicity, \( \{d\} \sqcup S \sqsubseteq S \sqcup S = S \), and \( S \sqsubseteq \{d\} \sqcup S \), by (1). Hence, \( \{d\} \sqcup S = S \).

only if: By (1), \( \{d\} \sqsubseteq \{d\} \sqcup S \); but \( d \in S \) implies that \( \{d\} \sqcup S = S \).

Clause (5): if: \( S \sqsubseteq T \) and monotonicity imply \( S \sqcup T \sqsubseteq T \sqcup T = T \). By (1), \( T \sqsubseteq S \sqcup T \), hence \( S \sqcup T = T \).

only if: By definition, \( S \sqcup T = T \), and by (1), \( S \sqsubseteq S \sqcup T \).

Clause (2): Let \( M = \{ \{d\} \mid d \in S \} \).
\( \subseteq \): For arbitrary \( d \in D \), say that \( d \in S \); then \( \{d\} \subseteq \sqcup M \), implying \( d \in \sqcup M \), by (4). By the definition of lower powerset, \( S \subseteq \sqcup M \).
\( \sqsubseteq \): For every \( \{d\} \in M \), \( \{d\} \sqsubseteq \{d\} \sqcup S = S \). 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, \( id : D \rightarrow D \), 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 \( d \in_D e \).

Corollary 12. Every lower powerset is strongly lower.

Proof. For \( P_L(D) = (E, \sqsubseteq_E, \{\cdot \}, \uplus) \) and \( S, T \in E \), say that \( S \sqsubseteq T \) and say that \( d \in S \). By Clause 4 of Proposition 11, \( \{d\} \sqsubseteq_S S \sqcup T \), implying that \( d \in T \).

Theorem 13. For every lower powerset, \( P_L(D) = (E, \sqsubseteq_E, \{\cdot \}, \uplus) \),

1. \( \uplus = \sqcup_E \); and
2. \( P_L(D) \) is isomorphic to a join completion of \( D \), where \( \tilde{\in} \) is \( \in \) and \( \cap \) is \( \cap \).

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

Clause (2): For lower powerset, \( P_L(D) = (E, \sqsubseteq_E, \{\cdot \}, \uplus) \), we define the join completion consisting of those subsets of \( D \)-elements expressed by \( E \): For each \( S \in E \), define
\[
Mem(S) = \{ d \in D \mid d \in S \}
\]
and define \( M = \{ Mem(S) \mid S \in E \}, \sqsubseteq \), which is order-isomorphic to \( (E, \sqsubseteq_E) \), where the order isomorphism is \( Mem(\cdot) \), which follows from Proposition 11(3).

Next, we define
\[
P_M(D) = (M, \sqsubseteq_M)
\]
This structure is a join completion because each set, \( Mem(S) = \{ d \in D \mid d \in S \} \) is down closed and the sets form a Moore family. Down closure follows from Proposition 11(4): for \( a, b \in D \) and \( S \in E \), \( a \sqsubseteq_D b \in S \) implies \( \{a\} \sqsubseteq_E \{b\} \sqsubseteq E S \), implying \( a \in S \).
To show that $P_M(D)$ forms a Moore family, we must show closure under arbitrary intersections, 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

$$\cap_{i \in I} M_i = \text{Mem}(\cap_{i \in I} S_i), \text{ where } M_i = \text{Mem}(S_i)$$

For $\subseteq$, assume for $d \in D$ and for all $j \in I$, that $d \in \text{Mem}(S_j)$, that is, $d \in S_j$, and by 11(4). This implies $\{d\} \subseteq S_j$, which implies $\{d\} \cup \cap_{i \in I} S_i \subseteq \cap_{i \in I} S_i$. Thus, $\cap_{i \in I} M_i \subseteq \text{Mem}(\cap_{i \in I} S_i)$.

Next, we show that the isomorphism, $\text{Mem}(\cdot)$ preserves the singleton and union operations. For singleton, we must show for all $i \in I$, $d \in \text{Mem}(S_i)$ implies $d \in \text{Mem}(S_i)$. Since, for all $j \in I$, $d \in \cap_{i \in I} S_i$, we have $d \in \text{Mem}(S_j)$, by 11(4). Thus, $\text{Mem}(\cap_{i \in I} S_i) \subseteq \cap_{i \in I} \text{Mem}(S_i)$.

Finally, we establish that $\cap_{i \in I} S_i$ is LUB-closed. The first equivalence is immediate; for the second, we have $d \in \text{Mem}(S_i)$ iff $\{d\} \subseteq \text{Mem}(S_i)$ iff $\{d\} \subseteq \cap_{i \in I} S_i$ iff $d \in \text{Mem}(S_i)$.

We finish by noting that in $P_M(D)$ is order-isomorphic to $(E, \subseteq)$.

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 $P_L(C) = (E, \subseteq, \{\cdot\}, \cup)$ be a join completion (lower powerset). Recall that $\overline{\rho} \subseteq P_L(C) \times A$ is defined $S \overline{\rho} a$ iff for all $c \in S, c \rho a$. For any choice of $P_L(C)$:

1. $\overline{\rho}$ is L-closed.
2. If $\rho$ 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 $\gamma_\rho(a) = \{c \mid c \rho a\}$.

**Proof.** (1): L-closure follows because $\subseteq_E$ is $\subseteq$.

Clause(2): U-closure of $\overline{\rho}$ follows immediately from the U-closure of $\rho$. For GLB-closure, we must show that $S \overline{\rho} \cap M_S$, where $M_S = \{a \mid S \overline{\rho} a\}$, that is, for all $c \in S, c \rho \cap M_S$. 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 $\{c \mid c \rho a\} = \cup M_a$. 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 $\cap M_a$. 

Corollary 15. If \( \rho \subseteq C \times A \) is L-U-GLB-closed, then \( \mathcal{P}_L(C)(\alpha_{\rho}, \gamma_{\rho})A \) is a Galois connection.

Proof. Since \( \rho \) is L-closed, all sets \( \{ c \mid c \rho a \} \) are downwards closed.

Often, one need not lift \( C \) to \( \mathcal{P}_L(C) \) to obtain a Galois connection: the minimal join completion of (down-closed) sets \( \{ c \mid c \rho a \} \), for all \( a \in A \), also suffices. For example, say that \( \text{Int} \) and \( \rho \) in Figure 3 are replaced by \( \text{Int}^{\uparrow} \) from Figure 4 and by \( \rho \subseteq \text{Int}^{\uparrow} \times \text{Sign} \), which is defined to be \( \rho \) augmented by \( \top \rho \) any and \( \bot \rho a \), for all \( a \in \text{Sign} \). Figure 4 shows \( \rho \)'s minimal join completion.

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 \( \bar{\rho} \subseteq \mathcal{P}_L(C) \times A \), \( S \in \mathcal{P}_L(C) \), and \( a \in A \),

\[
S \bar{\rho} a \iff S \rho a.
\]

Proof. Only if: \( S \bar{\rho} a \) iff for all \( c \in S \), \( c \rho a \). Because \( \rho \) is L-LUB-closed, Lemma 4 implies \( \sqcup S \rho a \).

If: \( \sqcup S \rho a \) implies \( c \rho a \) by L-closure, for all \( c \in S \).

The Proposition explains why \( \mathcal{P}_L(\mathcal{P}(\text{Nat})) \) was no more expressive than \( \mathcal{P}(\text{Nat}) \) as the concrete domain in the Galois connections for the parity example in Section 1.

From this point onwards, we use the notation, \( \mathcal{P}_L(D) \), to denote any lower powerset. When a specific instance of a lower powerset is required (e.g., \( \mathcal{P}_L(D) \) or \( \text{triv}_L(D) \)), we will clearly indicate this.

4.2 Upper powersets

Definition 17. Powerset \( \mathcal{P}_U(D) = (E, \sqsubseteq, \{ \cdot \}, \cup, \cup) \) is an upper powerset iff \( (S_1 \sqsubseteq S_2 \text{ if, for all } y \in S_2, \text{ there exists } x \in S_1 \text{ such that } x \subseteq_D y) \). The extension operation is defined \( \text{ext}(f)(S) = \cap_L \{ f(x) \mid x \in S \} \), for monotone \( f : D \rightarrow M \).

The results proved for lower powersets dualize without complication:

Proposition 18. For upper powerset \( \mathcal{P}_U(D) = (E, \sqsubseteq, \{ \cdot \}, \cup, \cup) \), \( S, T \in E \), define \( S \sqsubseteq T \text{ iff } S \cup T = T \); thus \( d \in S \text{ iff } \{d\} \sqsubseteq S \). For all \( S, T \in E \) and \( d \in D \),

1. \( S \sqsubseteq T \sqsubseteq_E S \)
2. \( S \sqsubseteq_E \cap \{\{d\} \mid d \in S\} \)
3. \( S \sqsubseteq T \text{ iff for all } d \in S, \text{ then } d \in T \) also
4. \( d \in S \text{ iff } S \sqsubseteq_E \{d\} \)
5. \( d \sqsubseteq_E T \text{ iff } T \sqsubseteq_E S \)
6. \( d \sqsubseteq_D e \text{ iff } \{d\} \sqsubseteq_E \{e\} \)

Corollary 19. Every upper powerset is strongly upper: for \( \mathcal{P}_U(D) = (E, \sqsubseteq_E \), \( \{ \cdot \}, \cup, \cup \) and \( S_1, S_2 \in E \), \( S_1 \sqsubseteq_E S_2 \) iff for all \( y \in S_2 \), there exists \( x \in S_1 \) such that \( x \subseteq_D y \).
Theorem 20. For every upper powerset, \( \mathcal{P}_U(D) = (E, \subseteq_E, \emptyset \cdot \emptyset, \cup) \),

1. \( \cup = \cap_E \); and
2. \( \mathcal{P}_U(D) \) is isomorphic to a dual-join completion of \( D \), where \( \bar{\xi} \) is \( \in \) and \( \cup \) is \( \cap \), namely, \( (\mathcal{M}, \cup, \cap, \mathcal{M}) \), where \( \mathcal{M} = (\{\text{Mem}(S) \mid S \in E\}, \supseteq) \) and \( \text{Mem}(S) = \{d \in D \mid d \bar{\in} S\} \).

Theorem 21. For complete lattices \( C \) and \( A \), let \( \rho \subseteq C \times A \) and let \( \mathcal{P}_U(A) = (E, \subseteq, \emptyset \cdot \emptyset, \cup) \) be a dual join completion (upper powerset). Define \( \rho^+ \subseteq C \times \mathcal{P}_U(A) \) as \( c \rho^+ T \) iff for all \( a \in T \), \( c \rho a \). For any choice of \( \mathcal{P}_U(A) \):

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

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

From this point onwards, we use the notation, \( \mathcal{P}_U(D) \), to denote any upper powerset. When a specific instance of upper powerset is required (e.g., \( \mathcal{P}_1(D) \) or \( \text{triv}_U(D) \)), we will clearly indicate this.

## 5 Logical relations

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

\[
\tau ::= b \mid \tau_1 \to \tau_2 \mid L(\tau) \mid U(\tau) \mid \top
\]

We use \( L(\tau) \) to abbreviate \( \mathcal{P}_L(\tau) \) and \( U(\tau) \) for \( \mathcal{P}_U(\tau) \). Only typing \( \top \) is non-standard; it is a special case of \( L(\tau) \) that we retain for convenience, because it appears so often in the practice of generating Galois connections.

We attach the typings to concrete and abstract domains, \( D \), as follows:

- \( D_b \) is given, for base type \( b \)
- \( D_{\tau_1 \to \tau_2} \) are the monotone functions from \( D_{\tau_1} \) to \( D_{\tau_2} \), ordered pointwise
- \( D_{L(\tau)} \) is a lower powerset generated from \( D_\tau \)
- \( D_{U(\tau)} \) is an upper powerset generated from \( D_\tau \)

Since \( \bar{\rho} \subseteq \mathcal{P}_L(C) \times A \) is the completion of \( \rho \subseteq C \times A \) (cf. Theorem 14), we define

- \( C_\tau \) is \( C_{L(\tau)} \), for concrete domain \( C_\tau \)
- \( A_\tau \) is \( A_{U(\tau)} \), for abstract domain \( A_\tau \)

Next, we define the family of logical relations, \( \rho_\tau \subseteq C_\tau \times A_\tau \):

- \( \rho_b \) is given, for base type \( b \) (e.g., \( \rho_{\text{parity}} \subseteq \text{Int} \times \text{Parity} \))
- \( f \rho_{\tau_1 \to \tau_2} f^2 \) iff for all \( c \in C_{\tau_1}, a \in A_{\tau_2}, c \rho_{\tau_1} a \) implies \( f(c) \rho_{\tau_2} f^2(a) \)
- \( S_{\rho_{L(\tau)}} T \) iff for all \( c \bar{\in} S \), there exists \( a \bar{\in} T \) such that \( c \rho_T a \)
- \( S_{\rho_{U(\tau)}} T \) iff for all \( a \bar{\in} T \), there exists \( c \bar{\in} S \) such that \( c \rho_T a \)
- \( S_{\rho_\tau} a \) iff for all \( c \in S, c \rho_\tau a \)
The definitions read as expected, e.g., \( f \rho_{\tau_1 \rightarrow \tau_2} f^* \) asserts that \( f \) is approximated by \( f^* \) 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 \( S \rho_C \) uses \( \in \) (rather than \( \in \)) to emphasize that \( C \rho_C \) is (a lower powerset treated as) a join completion. Indeed, when \( \rho_C \) is U-closed, then \( \rho_C \subseteq \mathcal{P}_L(C) \times A \) is merely an instance of \( \rho_L(\tau) \subseteq \mathcal{P}_L(C) \times \text{triv}_L(A) \):

**Proposition 22.** Recall that \( \text{triv}_L(D) = (\{ \{d \mid d \in D\}, \subseteq, \emptyset, \cup \} \approx D \). When \( \rho_C \subseteq C \times A \) is U-closed, then \( \rho_C = \rho_L(\tau) \), for \( \rho_L(\tau) \subseteq \mathcal{P}_L(C) \times \text{triv}_L(A) \).

**Proof.** We freely use the isomorphism, \( \| \) : \( A \rightarrow \text{triv}_L(A) \):

\[ \subseteq : \text{Assume } S \rho_C a; \text{ then for all } c \in S, c \rho_C a. \text{ This implies } S \rho_L(\tau) \downarrow a. \]

\[ \supseteq : \text{Assume } S \rho_L(\tau) \downarrow a ; \text{ this gives for all } c \in S, \text{ there exists } a' \in \| a \text{ such that } c \rho_C a'. \text{ By U-closure, we have } c \rho_C a, \text{ hence, } S \rho_C a. \]

The dual result holds for \( \rho_C \subseteq C \times \mathcal{P}_U(A) \): It equals \( \rho_U(\tau) \subseteq \text{triv}_U(C) \times \mathcal{P}_U(A) \).

### 5.1 Simulations are logical relations

State-transition relations are often related by means of simulations. The standard definition goes as follows:

**Definition 23.** For \( \rho \subseteq C \times A \) and transition relations, \( R \subseteq C \times C, R^\rho \subseteq A \times A \), \( R^\rho \rho \)-simulates \( R \), written \( R \triangleleft_\rho R^\rho \), iff for all \( c, c', a \in C, a \in A \),

\[ c \rho a \text{ and } c R c' \implies \text{there exists } a' \in \| a \text{ such that } a R^\rho a' \text{ and } c' \rho a'. \]

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

**Proposition 24.** For \( \rho_b \subseteq C_b \times A_b \), if \( R : C_b \rightarrow \mathcal{P}_L(C_b) \) and \( R^\rho : A_b \rightarrow \mathcal{P}_L(A_b) \)

are monotone, then

\[ R \triangleleft_{\rho_b} R^\rho \text{ iff } R \rho_b \rightarrow_{L(b)} R^\rho. \]

A dual simulation, \( R^\rho \triangleleft_{\rho^{-1}} R \), is beautifully characterized as \( R \rho_b \rightarrow_{L(b)} R^\rho \).

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.

### 6 Closure properties of logical relations

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

**Proposition 25.** For \( \rho_T \subseteq C \times A \),
1. \( \rho_L(\tau), \rho_U(\tau), \) and \( \rho_T \) are \( L \)-closed; if \( \rho_T \) is \( L \)-closed, then so is \( \rho_T \to \tau \).
2. \( \rho_L(\tau) \) and \( \rho_U(\tau) \) are \( U \)-closed; if \( \rho_T \) is \( U \)-closed, then so are \( \rho_T \to \tau \) and \( \rho_T \).
3. If \( \rho_T \) is \( U \)-GLB-closed, then so are \( \rho_T \to \tau \), \( \rho_L(\tau) \), and \( \rho_T \).
4. If \( \rho_T \) is \( L \)-LUB-closed, then so are \( \rho_T \to \tau \) and \( \rho_U(\tau) \).

Proof. Clause (1): To show \( L \)-closure for \( \rho_L(\tau) \), we use \( \mathcal{P}_L(C_\tau) \)'s join-closure representation, due to Theorem 13, where \( \mathcal{P}_L(C_\tau) \) 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 \( a \in T \) such that \( c' \rho_T a \). The proof of \( L \)-closure for \( \rho_T \), where \( \mathcal{P}_L(C_\tau) \) is also a join completion, is the same.

For \( \rho_U(\tau) \), we use \( \mathcal{P}_U(C_\tau) \)'s dual-join-closure representation, due to Theorem 20, where \( \mathcal{P}_U(C_\tau) \) is \( \supseteq \). Given \( S' \supseteq S \rho_U(\tau) T \), we see that for every \( a \in T \), there exists \( c \in S \) such that \( c \rho_T a \), and \( c \in S' \) as well.

For \( \rho_T \to \tau \), assume that \( f' \subseteq f \rho_T \to \tau f' \); if \( \rho_T \to \tau f \), then \( f(c) \rho_T f'(a) \). Since \( f'(c) \subseteq f(c) \), the result comes from the \( L \)-closure of \( \rho_T \).

Clause (2): Similar to (1), but recall from Proposition 22 that \( U \)-closure is not ensured for \( \rho_T \).

Clause (3): For \( \rho_T \to \tau \), we must show \( f \rho_T \to \tau \cap F \), where \( F = \{ f^2 \mid f \rho_T \to \tau f \} \). Assume that \( c \rho_T a \); for all \( f^2 \in F \), we have \( f(c) \rho_T f^2(a) \). By Lemma 4, we have that \( f(c) \rho_T \cap \{ f^2(a) \mid f^2 \in F \} \), and by the definition of meet in the complete lattice of monotone functions, we have \( \cap \{ f^2(a) \mid f^2 \in F \} = (\cap F)(a) \).

For \( \rho_L(\tau) \), we must show \( S \rho_L(\tau) \cap M \), where \( M = \{ T \mid S \rho_L(\tau) T \} \). For every \( c \in S \), for each \( T \in M \), there is some \( a_i \in T_i \) such that \( c \rho_T a_i \). By Lemma 4, we have \( c \rho_T \cap_j a_j \), where \( j \) indexes the sets in \( M \).

Since \( a_i \in T_i \) implies \( \{ a_i \} \subseteq T_i \), for all \( T_i \in M \), we have \( \{ \cap_j a_j \} \subseteq T_i \), also. Hence, \( \{ \cap_j a_j \} \subseteq \cap M \), implying \( \{ \cap_j a_j \} \cap \cap M \), by Proposition 11. The proof for \( \rho_T \) 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.\(^\text{10}\) The following subsections explore these issues.

### 6.1 Lower powersets: \( \rho_L(\tau) \subseteq \mathcal{P}_L(C_\tau) \times \mathcal{P}_L(A_\tau) \)

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

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

**Proposition 26.** For all \( \rho_T \subseteq C_\tau \times A_\tau \), for any choice of \( \mathcal{P}_L(A_\tau) \), \( \rho_L(\tau) \subseteq \mathcal{P}_L(C_\tau) \times \mathcal{P}_L(A_\tau) \) is LUB-closed.

\(^\text{10}\) This difficulty is foreshadowed by Backhouse and Backhouse [4], whose results are summarized in Section 10.
Proof. In $\mathcal{P}_1(C_\tau)$, join is set union, meaning that $c \in \bigcup\{S \mid S \rho_{L(\tau)} T\}$ 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, $\mathcal{P}_{Scott}(D) = \{(Scott(S) \mid S \subseteq D), \subseteq, \downarrow, Scott \circ \downarrow\}$, where $Scott(S)$ is the closure of $S$ in $D$'s Scott topology, there exist U-LUB closed relations, $\rho_\tau \subseteq C \times A$, where $\rho_{L(\tau)} \subseteq \mathcal{P}_{Scott}(C) \times \mathcal{P}_{Scott}(A)$ 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 $\rho_{L(\tau)} \subseteq \mathcal{P}_{Scott}(C_\tau) \times \mathcal{P}_{Scott}(A_\tau)$.

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

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 $c_i \rho_\tau \cap \{a_j \mid i \leq j\}$, for all $i \geq 0$, and the $\cap \{a_j \mid i \leq j\}$’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.

In any case, there is no implementation penalty in employing Proposition 26 to generate LUB-closed $\rho_{L(\tau)} \subseteq \mathcal{P}_1(C_\tau) \times \mathcal{P}_L(A_\tau)$ for lower powerset $\mathcal{P}_L(A)$, so we freely do so.

The other question is regarding the cardinality of $\mathcal{P}_L(A_\tau)$ — how large should it be? Given the transition function, $R : C_\tau \rightarrow \mathcal{P}_L(C_\tau)$, if we desire (forwards) completeness [18] for $R^\downarrow_{best} : A_\tau \rightarrow \mathcal{P}_L(A_\tau)$, then we should ensure, for every $c \in C_\tau$, that there exists $T \in \mathcal{P}_L(A_\tau)$ that exactly approximates $R(c)$. That is, for all $c \in C_\tau$, we require

$$R(c) = \bigcup\{S \in \mathcal{P}_L(A_\tau) \mid S \rho_{L(\tau)} T\}.$$

Here is one such counterexample: Let $Ord$ be the ordinals up to $\omega_0$, ordered as a chain, and let $Nat^\downarrow$ be the flat lattice of numbers. We have this U-LUB-closed relation, $\rho_N \subseteq Ord \times Nat^\downarrow$:

$$\rho_N = \{(0, \bot)\} \cup \{(j, i) \mid j \leq i\} \cup \{(v, T) \mid v \in Ord\}$$

If we lift the lattices to their lower powerdomains, $\mathcal{P}_{Scott}(Ord)$ and $\mathcal{P}_{Scott}(Nat^\downarrow)$, we see that LUB-closure is lost: For $T_0 = Nat^\downarrow \cup \{\bot\} \in \mathcal{P}_{Scott}(Nat^\downarrow)$, we have that

$$\{S \in \mathcal{P}_{Scott}(Ord) \mid S \rho_{L(N)} T_0\} = \{\{i \mid i \geq 0\}$$

But $\sqcup\{\{i \mid i \geq 0\} = Ord$, and it is not the case that there exists $a \in T_0$ such that $\omega_0 \rho_N a$. 

1. $S \subseteq D$ is Scott closed iff $S = \uparrow S$ and for all chains, $c_0 \subseteq D c_1 \subseteq D \cdots c_i \subseteq D \cdots \subseteq S$, then $\cup\{c_i \mid i \geq 0\} \in S$. Scott$(S) = \cap\{S' \subseteq D \mid S'$ is Scott-closed and $S \subseteq S'$

12. Here is one such counterexample: Let $Ord$ be the ordinals up to $\omega_0$, ordered as a chain, and let $Nat^\downarrow$ be the flat lattice of numbers. We have this U-LUB-closed relation, $\rho_N \subseteq Ord \times Nat^\downarrow$:

$$\rho_N = \{(0, \bot)\} \cup \{(j, i) \mid j \leq i\} \cup \{(v, T) \mid v \in Ord\}$$

If we lift the lattices to their lower powerdomains, $\mathcal{P}_{Scott}(Ord)$ and $\mathcal{P}_{Scott}(Nat^\downarrow)$, we see that LUB-closure is lost: For $T_0 = Nat^\downarrow \cup \{\bot\} \in \mathcal{P}_{Scott}(Nat^\downarrow)$, we have that

$$\{S \in \mathcal{P}_{Scott}(Ord) \mid S \rho_{L(N)} T_0\} = \{\{i \mid i \geq 0\}$$

But $\sqcup\{\{i \mid i \geq 0\} = Ord$, and it is not the case that there exists $a \in T_0$ such that $\omega_0 \rho_N a$. 

11. $S \subseteq D$ is Scott closed iff $S = \uparrow S$ and for all chains, $c_0 \subseteq D c_1 \subseteq D \cdots c_i \subseteq D \cdots \subseteq S$, then $\cup\{c_i \mid i \geq 0\} \in S$. Scott$(S) = \cap\{S' \subseteq D \mid S'$ is Scott-closed and $S \subseteq S'$

12. Here is one such counterexample: Let $Ord$ be the ordinals up to $\omega_0$, ordered as a chain, and let $Nat^\downarrow$ be the flat lattice of numbers. We have this U-LUB-closed relation, $\rho_N \subseteq Ord \times Nat^\downarrow$:
6.2 Upper powersets: $\rho_{\tau\tau} \subseteq \mathcal{P}_U(C_{\tau}) \times \mathcal{P}_U(A_{\tau})$

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

**Proposition 28.** Recall that $\mathcal{P}_1(A) = \{\uparrow D \mid D \subseteq A\}$, $\mathcal{P}_U(C) \times \mathcal{P}_1(A)$, is GLB-closed, for all choices of upper powersets, $\mathcal{P}_U(C)$.

**Proof.** In $\mathcal{P}_1(A)$, 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 $\rho_{\tau\tau} \subseteq \mathcal{P}_{\text{Smyth}}(C_{\tau}) \times \mathcal{P}_{\text{Smyth}}(A_{\tau})$, is GLB-closed, where $\mathcal{P}_{\text{Smyth}}(D)$ is the upper (“Smyth”) powerdomain of $D$ [36, 41].

Because it is expensive to implement sets-of-all-subsets constructions like $\mathcal{P}_1(A)$ and $\mathcal{P}_{\text{Smyth}}(A_{\tau})$, we might search for a coarser, dual-join completion of $A_{\tau}$. Given the concrete transition function, $R : C_{\tau} \to \mathcal{P}_U(C_{\tau})$, if we desire forwards completeness for $R_{\text{best}}^2 : A_{\tau} \to \mathcal{P}_U(A_{\tau})$, then we should ensure, for every $c \in C_{\tau}$, that there exists $T \in \mathcal{P}_U(A_{\tau})$ that exactly approximates $R(c)$:

$$R(c) = \cap \{S \in \mathcal{P}_U(A_{\tau}) \mid S \rho_{\tau\tau} T\}.$$

6.3 Function spaces: $\rho_{\tau \rightarrow \tau} \subseteq (C_{\tau1} \rightarrow C_{\tau2}) \times (A_{\tau1} \rightarrow A_{\tau2})$

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

**Proposition 29.** Let $\rho_{\tau} \subseteq \mathcal{C}_{\tau} \times \mathcal{A}_{\tau}$, for $i \in 1..2$, be U-GLB-L-LUB-closed, so that there are the Galois connections, $C_{\tau}, \{\alpha_{\rho_{\tau}}, \gamma_{\rho_{\tau}}\}, A_{\tau}$, $i \in 1..2$. For $f : C_{\tau1} \to C_{\tau2}$, $f^2 : A_{\tau1} \to A_{\tau2}$,

$$f \rho_{\tau_1 \tau_2} f^2 \iff \alpha_{\rho_{\tau_2}} \circ f \subseteq A_1 \to A_2 \ f^2 \circ \alpha_{\rho_{\tau_1}}.$$  

where $c, \rho_{\tau}, a, i \iff \alpha_{\tau_1 \{c\}} \subseteq a_i$, $i \in 1..2$

**Proof.** If: Assume $c \rho_{\tau} a$, implying $\alpha_{\tau_1 \{c\}} \subseteq a$. By monotonicity, $f^2(\alpha_{\tau_1 \{c\}}) \subseteq f^2(a)$. Using the assumption, we deduce $\alpha_{\tau_2}(f(a)) \subseteq f^2(a)$, implying $f(a) \rho_{\tau_2} f^2(a)$.

Only if: By definition, for all $c \in C_{\tau_1}$, $c \rho_{\tau} \alpha_{\tau_1 \{c\}}$. By assumption, we obtain $f(c) \rho_{\tau_2} f^2(\alpha_{\tau_1 \{c\}})$, which implies by definition, gives $\alpha_{\rho_{\tau_2}}(f(c)) \subseteq f^2(\alpha_{\rho_{\tau_1 \{c\}}} \{c\})$.

As a corollary, $f \rho_{\tau_1 \tau_2} f_{\text{best}}^2$, where $f_{\text{best}}^2(a) = \alpha_{\rho_{\tau_2}} \circ f \circ \gamma_{\rho_{\tau_1}}$.

If $\rho_{\tau_2}$ is not LUB-closed, we might complete it to $\rho_{\tau_2} \subseteq \mathcal{P}_1(C_2) \times A_2$ and generate $\rho_{\tau_1 \tau_2} \subseteq (C_1 \to \mathcal{P}_1(C_2)) \times (A_1 \to A_2)$. Or, we might generate the relation, $\rho_{\tau_1 \tau_2} \subseteq \mathcal{P}_1(C_1 \to C_2) \times (A_1 \to A_2)$; in this latter case, the Galois connection is $\mathcal{P}_1(C_1 \to C_2)(\alpha_{\phi}, \gamma_{\phi})(A_1 \to A_2)$, where $\gamma_{\phi} f^2 = \{f \mid \gamma_{\phi} \rho_{\tau_1 \tau_2} f^2 = \{f \mid \forall c \in C_1; f(c) \subseteq C_2 \ gamma_{\phi}(f^2(\alpha_{\tau_1 \{c\}}))\}$. These and other interesting Galois connections generated from relations on functions can be found in [11].


7 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 \( \mathcal{P}(C)(\alpha, \gamma)A \), Dams \([12, 14]\) proved that the most precise, sound, abstract transition relation \( R^0_0 \subseteq A \times A \) is

\[
R^0_0(a, a') \text{ iff } a' \in \{ \alpha(Y) \mid Y \in \min\{ \mathcal{S}' \mid R^{\mathcal{S}}(\gamma(a), \mathcal{S}') \} \}
\]

where \( R^{\mathcal{S}}(M, N) \) holds iff there exist \( m \in M \) and \( n \in N \) such that \( mRn \).

Recoded as a function, \( R^0_0 : A \to \mathcal{P}(A) \), and simplified, this reads

\[
R^0_0(a) = \{ \alpha(c') \mid \exists c \in \gamma(a), c' \in R(c) \}
\]

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

Dams’s notions of soundness and best precision were stated in terms of properties in branching-time temporal-logic: Soundness meant that logical properties true of \( R \) also held for \( R_0 \), and best precision meant that \( R_0 \) 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 results for free.)

Given \( \mathcal{U}-\text{GLB} \)-closed \( \rho_0 \subseteq C \times A \) and transition function \( R : C \to \mathcal{P}(C) \), we generate the \( \mathcal{L}-\text{LUB}-\text{U}-\text{GLB} \)-closed relations, \( \rho_{\mathcal{U}} \subseteq \mathcal{P}(C) \times A \) and \( \rho_{\mathcal{L}(b)} \subseteq \mathcal{P}(C) \times \mathcal{P}_L(A) \), and their corresponding Galois connections,

\[
\mathcal{P}(C)(\alpha_{\mathcal{U}}, \gamma_{\mathcal{U}})A \text{ and } \mathcal{P}(C)(\alpha_{\mathcal{L}(b)}, \gamma_{\mathcal{L}(b)})\mathcal{P}_L(A)
\]

These give us the domain and codomain of the abstract transition function, \( R^2_{\text{best}} : A \to \mathcal{P}_L(A) \), which we define in the usual fashion \([9]\):

\[
R^2_{\text{best}}(a) = (\alpha_{\mathcal{L}(b)} \circ \text{ext}_{\mathcal{U}}(R) \circ \gamma_{\mathcal{U}})(a)
\]

\[
\cap \{ T \in \mathcal{P}_L(A) \mid (\text{ext}_{\mathcal{U}}(R)(\gamma_{\mathcal{U}}(a)))\rho_{\mathcal{L}(b)}T \}
\]

(Note that \( \text{ext}_{\mathcal{U}}(R) : \mathcal{P}(C) \to \mathcal{P}(C) \) is \( \text{ext}_{\mathcal{U}}(R)(S) = \cup_{c \in S} R(c) \).) When we choose \( \mathcal{P}_1(A) \) for \( \mathcal{P}_L(A) \), we can prove that the above equals

\[
\cup\{ \{ \alpha_{\mathcal{U}}(c') \} \mid \exists c \in \gamma_{\mathcal{U}}(a), c' \in R(c) \}
\]

\[
= \cup\{ \{ \alpha_{\mathcal{U}}(c') \mid \exists c \in \gamma_{\mathcal{U}}(a), c' \in R(c) \}
\]

This is Dams’s definition, when one takes into account the partial ordering on \( A \) so that operations on \( \mathcal{P}_1(A) \) are monotone and fixed points exist.\(^{13}\) Appealing to the standard results \([9]\), we have that \( R^2_{\text{best}} \) 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 \( A \to \mathcal{P}_L(A) \).

\(^{13}\) Dams does not address the monotonicity issue, but no harm is done: For all \( a \in A \), \( R^0_0(a) \equiv R^2_{\text{best}}(a) \) with respect to the lower-powerset equivalence defined in Definition 10.
7.1 Lifting the concrete domain

In unpublished work [13], Dams justified his definition of \( R_0^c \) in terms of the Galois connections synthesized in the previous subsection. But as noted in Sections 1.3 and 2.1, we can justify \( R_0^c \) 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, \( \mathcal{P}(C)(\alpha_{\overline{R}}, \gamma_{\overline{R}})A \), for the domain of the abstract transition function, but the Galois connection for the codomain is generated from U-GLB-L-LUB-closed \( \rho_{\overline{L(b)}} \subseteq \mathcal{P}_i(\mathcal{P}(C)) \times \mathcal{P}_L(A) \):

![Diagram showing the lifting process](image)

The diagram reminds us that a set of abstract values, \( T \in \mathcal{P}_L(A) \) concretizes to the set \( \overline{T} \), such that for every \( S \in \overline{T} \), \( S \) is overapproximated by \( T \). The Galois connection is \( \mathcal{P}_i(\mathcal{P}(C))(\alpha_{\overline{L(b)}}, \gamma_{\overline{L(b)}})\mathcal{P}_L(A) \). We define \( R_{\text{best2}}^c : A \rightarrow \mathcal{P}_L(A) \) as

\[
R_{\text{best2}}^c = \alpha_{\overline{L(b)}} \circ R^* \circ \gamma_{\overline{b}}
\]

where \( R^*(S) = (\text{ext}_{\overline{b}}(\{\cdot\} \circ R))(S) = \cup\{\|R(c)\| \mid c \in S\} \)

Here, \( \{\cdot\} : \mathcal{P}(C) \rightarrow \mathcal{P}_i(\mathcal{P}(C)) \) is \( \{S\} = \{S' \mid S' \subseteq S\} \), so \( R^*(S) = \{\{R(c)\} \mid c \in S\} \); showing that \( R^* \) maps a set of arguments to all subsets of \( R \)-successor sets. By calculation, we can show that \( R_{\text{best2}}^c = R_{\text{best}}^c \).

This redevelopment of \( R_{\text{best}}^c \) is notational overkill, but there is an important point: *Simulation equivalence is preserved when a concrete transition function is lifted to a function that maps a set of arguments to a set of sets of answers.*

**Proposition 30.** Let \( R : C \rightarrow \mathcal{P}(C) \) and \( R^c : A \rightarrow \mathcal{P}_L(A) \). Then the following are equivalent:

1. \( R \rho_R^c \)
2. \( \rho_{\overline{b}} \circ \rho_{\overline{L(b)}} \circ R^c \)
3. \( \text{ext}_{\overline{b}}(R) \circ \rho_{\overline{L(b)}} \circ R^c \), assuming \( \rho_{\overline{L(b)}} \) is LUB-closed
4. \( R^* \circ \rho_{\overline{b}} \circ \rho_{\overline{L(b)}} \circ R^c \), assuming \( \rho_{\overline{L(b)}} \) is LUB-closed

**Proof.** Recall that \( \text{ext}_{\overline{b}}(R)(S) = \cup\{\{R(c)\} \mid c \in S\} \) and \( R^*(S) = \cup\{\|R(c)\| \mid c \in S\} \).

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

(3) implies (2): Assume \( c \rho_R a \); this implies \( \{c\} \rho_{\overline{b}} a \), which implies that \( R(c) = \text{ext}_{\overline{b}}(R)\{c\} \rho_{\overline{L(b)}} R^c(a) \).

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

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

Similar equivalences will prove useful when working with underapproximations.

8 Synthesizing a most-precise dual simulation

An underapproximation analysis uses an abstract transition function, \(R: A \to P_U(A)\), and it is tempting to try constructing a Galois connection of the form, \(P(C)^{op}(\alpha_{U(b)}) \gamma_{U(b)})P_U(A)\). But this requires that \(\rho_{U(b)} \subseteq P(C)^{op} \times P_U(A)\) be LUB-closed, which is difficult to achieve.\(^{14}\)

Fortunately, we can apply the approach seen in the previous Section and define a sound, overapproximation of underapproximations in terms of \(\rho_{U(\tau)} \subseteq P_1(P_U(C)) \times P_U(A)\):

\[
\rho_{U(\tau)}(P_U(C)) \subseteq P_U(A)
\]

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

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

1. Begin with a U-GLB-closed \(\rho_b \subseteq C \times A\);
2. Lift it to a U-L-GLB-closed \(\rho_{U(b)} \subseteq P(C)^{op} \times P_1(A)\);\(^{15}\)
3. Complete it to a U-GLB-L-LUB-closed \(\rho_{U(\tau)} \subseteq P_1(P(C)^{op}) \times P_1(A)\).

The resulting Galois connection, \(P_1(P(C)^{op})\langle \alpha_{U(b)}, \gamma_{U(b)}\rangle P_1(A)\), is

\[
\gamma_{U(b)}(T) = \{ S \mid S \rho_{U(\tau)} T \}
\]

\[
\alpha_{U(\tau)} S = \cap \{ T \in P_U(A) \mid \text{for all } S \in S, S \rho_{U(b)} T \}
\]

An example of the construction was seen in Figure 2.

Recall that Dams proved, for Galois connection \(P(C)\langle \alpha, \gamma\rangle A\) and transition relation \(R \subseteq C \times C\), that the most precise, sound, underapproximating abstract transition relation, \(R_0^0 \subseteq A \times A\) is

\(^{14}\) Recall the example in Section 1.2: \(\rho_{U(\text{Parity})} \subseteq P(\text{Nat})^{op} \times P_1(\text{Parity})\). What is the least set of natural numbers that “witnesses” \{even, any\}? \{0\}? \{2\}? LUB-closure fails.

\(^{15}\) \(C\) is a set, so \(P(C)^{op}\), ordered by \(\supseteq\), is an upper powerset.
\[ R_0(a, a') \iff a' \in \{ \alpha(Y) \mid Y \in \min\{ S' \mid R^{\#}(\gamma(a), S') \} \} \]

where \( R^{\#}(M, N) \) holds iff for all \( m \in M \), there exists \( n \in N \) such that \( m R n \) [14]. Dams noted, for some \( a \in A \), that \( \min\{ S' \mid R^{\#}(\gamma(a), S') \} \) might be empty [14]; in such a case he decreed that \( R_0 \) is undefined, \( \min \) should be removed, and the following definition should be used instead:

\[ R_1(a, a') \iff a' \in \{ \alpha(Y) \mid Y \in \{ S' \mid R^{\#}(\gamma(a), S') \} \} \]

This always yields a sound and complete \( R_1 \) (but with larger cardinality than \( R_0 \), when the latter exists). We will study this anomaly momentarily.

Recoded as a function and simplified, \( R_1 \) reads

\[ R_1(a) = \{ \alpha(Y) \mid Y \in \{ S' \mid \forall c \in \gamma(a), R(c) \cap S' \neq \emptyset \} \} \]

The Galois-connection machinery gives us the same result: given transition function, \( R : C \to \mathcal{P}(C) \), we use the Galois connection, \( \mathcal{P}(C) (\alpha_\gamma, \gamma_\beta) A \), to generate the domain, and we use \( \mathcal{P}_1(\mathcal{P}(C)^{op})\langle \alpha_{U(b)} \rangle \gamma_{U(b)} A \), which was derived at the beginning of this section, to generate the codomain of the abstract transition function, \( R_{\text{best}} : A \to \mathcal{P}_1(A) \):

\[ R_{\text{best}} = \alpha_{U(b)} \circ R^* \circ \gamma_{\beta}, \text{ where } R^* = \text{ext}_{\mathcal{P}_1} \langle \cdot \rangle \circ R \]

Now, \( \langle \cdot \rangle \circ R : C \to \mathcal{P}_1(\mathcal{P}(C)^{op}) = \{ \cdot \rangle \circ R(c) = \{ S' \mid S' \supseteq R(c) \} \}

This makes \( R^* = \text{ext}_{\mathcal{P}_1} \langle \cdot \rangle \circ R : \mathcal{P}(C) \to \mathcal{P}_1(\mathcal{P}(C)^{op}) \) equal to \( R^*(S) = \bigcup_{c \in S} \{ S' \mid S' \supseteq R(c) \} = \bigcup_{c \in S} \{ S' \mid S' \supseteq R(c) \} = \{ S' \supseteq R(c) \mid c \in S \} \).

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

\[ R_{\text{best}}(a) = \bigcap\{ T \in \mathcal{P}_1(A) \mid \{ S' \supseteq R(c) \mid c \in \gamma_{\beta}(a) \} \rho_{U(b)} T \}
= \bigcap\{ T \in \mathcal{P}_1(A) \mid \{ R(c) \mid c \in \gamma_{\beta}(a) \} \rho_{U(b)} T \}
= \bigcap\{ T \in \mathcal{P}_1(A) \mid \forall c \in \gamma_{\beta}(a), \forall a' \in T, R(c) \cap \gamma_{\beta}(a') \neq \emptyset \} \}

because \( a' \rho_{\beta} a' \iff c' \in \gamma_{\beta}(a') \).

We now show that \( R_{\text{best}} = R_1 = R_0 \) (when the last function exists). For \( a \in A \), let

\[ D_i = R_i^a, \text{ for } i = 0..1, \text{ and } \]

\[ B_a = \{ T \in \mathcal{P}_1(A) \mid \forall c \in \gamma_{\beta}(a), \forall a' \in T, R(c) \cap \gamma_{\beta}(a') \neq \emptyset \} \}, \]

so that \( R_{\text{best}}(a) = \bigcap B_a \). 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 \( s \in \gamma_{\beta} \). For every \( \alpha_\gamma(Y) \) in \( D_i^a \), we have that \( R(s) \cap Y \neq \emptyset \).
Since \( \alpha_\gamma, \gamma_{\beta} \) form a Galois connection, we have that \( R(s) \cap \gamma_{\beta}(\alpha_\gamma(Y)) \neq \emptyset \).
Hence, \( D_i^a \in B_a \).

For (ii), we must show \( D_i^a \subseteq \mathcal{P}_1(A) T \), for all \( T \in B_a \). That is, for all \( a \in T \), there exists \( a' \in D_i^a \) such that \( a' \subseteq A a \). The definition of \( B_a \) tells us, for all such \( T \), for all \( s \in \gamma_{\beta}(a) \), that \( R(s) \cap \gamma_{\beta}(a) \neq \emptyset \).
In the case for $D^1_a$, its definition tells us that $\alpha_{\ell}(\gamma_\ell(a)) \in D^1_a$, and the definition of Galois connection implies $\alpha_{\ell}(\gamma_\ell(a)) \subseteq A$. In the case for $D^0_a$, there is some minimal $S' \subseteq \gamma_\ell(a)$ such that $R(s) \cap S' \neq \emptyset$. The result follows as for $D^1_a$.

This concludes the demonstration that $R_{\text{best}}^1 = R_1^1 = R_0^0$. The reasoning tacitly assumes that $D^1_a$ is an element of $\mathcal{P}_1(A)$, that is, $D^1_a$ 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 $\mathcal{P}_1(A)$.

Finally, dual simulation lifts to sets of arguments:

**Proposition 31.** $R^\circ \triangleleft_{p^{-1}} R$ iff $R \rho_{\varepsilon-U(b)} R^\circ$ iff $R^* \rho_{\varepsilon-U(b)} R^\circ$, assuming that $\rho_{U(\beta)}$ is LUB-closed.

*Proof.* Similar to the proof of Proposition 30.

## 9 Validation and refutation logics

Hennessy and Milner proved that $\Box \Diamond$-propositions (Hennessy-Milner logic) characterize transition relations up to bisimilarity [24]. Loiseaux, et al. [31], 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 $R^\circ_{\text{best}}$ and $R^0_{\text{best}}$ possess the most $\Box \Diamond$-propositions of any sound, mixed transition system.

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

$\tau ::= b \mid \tau_1 \rightarrow \tau_2 \mid L(\tau) \mid U(\tau) \mid \top$

where $\top$ 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 $\tau_1 \rightarrow \tau_2$, $f.\phi$ denotes an “application” property that holds for an argument, $d$, of type $\tau_1$, exactly when $\phi$ holds for the answer, $f(d)$, of type $\tau_2$.

$\forall \phi$ holds for set $S$ of type $\mathcal{P}_L(\tau)$ when $\phi$ holds for each of $S$’s $\tau$-typed elements. The dual property, $\exists \phi$, is validated on $\mathcal{P}_U(\tau)$-typed sets.

We formalize these notions: Assume, for all types, $\tau$, that the logical relations, $\rho_{\varepsilon} \subseteq C_{\tau} \times \mathcal{A}_\tau$, are defined for fixed domains $C_{\tau}$ and $\mathcal{A}_\tau$. Assume also, for all function symbols, $f$, typed $\tau_1 \rightarrow \tau_2$, there are interpretations $f^A : C_{\tau_1} \rightarrow C_{\tau_2}$, and $f^A : A_{\tau_1} \rightarrow A_{\tau_2}$, such that $f^A \rho_{\varepsilon} f^A.$
Definition 32. The semantics of the assertion language is defined by the following family of well-typed judgements; let $D_\tau$ denote either a concrete domain, $C_\tau$, or an abstract domain, $A_\tau$:

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

\[
d \models_{\tau_1 \rightarrow \tau_2} f.\phi \iff f(d) \models_{\tau_2} \phi, \text{ for } d \in D_{\tau_1} \text{ and } f \in D_{\tau_1 \rightarrow \tau_2}
\]

\[
S \models_{L(\tau)} \forall \phi \text{ iff for all } d \in S, d \models_\tau \phi, \text{ for } S \in D_{L(\tau)}
\]

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

Since $\tau$ is an instance of $P_L(\tau)$, define

\[
S \models_\tau \phi \text{ iff for all } c \in S, c \models_\tau \phi, \text{ for } S \in C_{L(\tau)}
\]

\[
a \models_\tau \phi \text{ iff } a \models_\tau \phi, \text{ for } a \in A_\tau.
\]

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

We can abbreviate $d \models_{\tau \rightarrow L(\tau)} R.\forall \phi$ by $d \models \forall R \phi$ (as in description logic [3]) or by $[R]\phi$ (Hennessy-Milner logic [24]) or by $\Box \phi$ when the system studied has only one transition function, $R : D_\tau \rightarrow P(D_\tau)$ (CTL [7]). This hides the reasoning on sets. Similarly, $d \models_{\tau \rightarrow U(\tau)} R.\exists \phi$ can be abbreviated by $d \models \exists R \phi$ or $(R)\phi$ or $\Diamond \phi$.

The judgements for $\forall R \phi$ and $\exists R \phi$ employ $R^2$ and $R^\ast$, respectively, to validate the assertions, motivating Dams’s mixed transition systems.\(^{16}\)

9.1 Soundness of judgements

We work with well-typed judgements defined on a families of typed concrete and abstract domains and a family of logical relations.

Definition 33. For type $\tau$, 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.\(^{17}\)

Assume that $\models_b p$ is sound for each $\rho_b \subseteq C_b \times A_b$.\(^ {18}\)

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

Proof. The proof is an easy induction on the structure of $\tau$. For example, for $\tau = \tau_1 \rightarrow \tau_2$, say that $c \rho_\tau a$ and $a \models_{\tau_1 \rightarrow \tau_2} f.\phi$. Then, $f^2(a) \models_{\tau_2} \phi$. Since $f^3 \rho_{\tau_1 \rightarrow \tau_2} f^2$, we have $f^2(c) \rho_{\tau_2} f^3(a)$, and by the induction hypothesis, $f^3(c) \models_{\tau_2} \phi$.

\(^{16}\) For concrete set, $C_\tau$, $P(C_\tau)$ is a lower powerset and $P(C_\tau)^{op}$ is an upper powerset, so we use the concrete transition function, $R$, to validate $\forall \phi$ and $\exists \phi$-properties on concrete sets.

\(^{17}\) Judgement form $\models_{\tau_1 \rightarrow \tau_2} f.\phi$ shows that $\tau'$ need not be $\tau$.

\(^{18}\) 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 $c \models_b a$. 
9.2 Best precision of judgements

Say that a judgement form, \( \vdash_{\tau} \phi \), is monotone if \( a \vdash_{\tau} \phi \) and \( a' \subseteq_{\tau} \phi \) imply \( a' \vdash_{\tau} \phi \), for all \( a, a' \in A_{\tau} \).

We assume that all base-type judgements, \( \vdash_{b} p \), are monotone, and from this it follows that all judgement forms are monotone.\(^{20}\) 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, \( R^b : C_b \to \mathcal{P}(C_b) \), and Galois connection, \( \mathcal{P}(C_b) \langle \alpha, \gamma \rangle A_b \), we have that \( R^b_{\text{best}} : A_b \to \mathcal{P}_L(A_b) \) and \( R^b_{\text{best}} : A_b \to \mathcal{P}_U(A_b) \) soundly prove the most typed judgements, \( a \vdash_{\tau} \phi \), for all \( a \in A_{\tau} \).

**Proof.** Given the domains, logical relations, and \( R^b : C_b \to \mathcal{P}(C_b) \), say that we have sound over- and underapproximation functions, \( R^b_\alpha : A_b \to \mathcal{P}_L(A_b) \) and \( R^b_\beta : A_b \to \mathcal{P}_U(A_b) \) for interpreting the function symbol, \( R \), in the assertion language. Call the resulting family of typed judgements, \( \vdash^0 \). Similarly, let \( \vdash^\text{best} \) be the typed-judgement family when \( R \) is interpreted by \( R^b_{\text{best}} \) and \( R^b_{\text{best}} \).

We must show, whenever \( a \vdash^0_{\tau} \phi \), that \( a \vdash^\text{best}_{\tau} \phi \) as well. The result follows by an induction on the structure of \( \tau \), and the only interesting case is the judgement form, \( a \vdash^0_{b_{\tau}} R \phi \), for \( \tau' \in \{L(b), U(b)\} \). Consider \( \tau' = L(b) \): By hypothesis, \( R^b_\alpha(a) \vdash^0_{L(b)} \phi \). But \( R^b_{\text{best}} \subseteq_{A_{\text{b}} \times L(b)} R^b_\alpha \), by the definition of Galois connection \([9]\), and monotonicity tells us \( R^b_{\text{best}}(a) \vdash^\text{best}_{L(b)} \phi \). Similar reasoning holds for \( \tau' = U(b) \).

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

\[
\begin{align*}
d \vdash_{\tau} \phi_1 \land \phi_2 & \iff d \vdash_{\tau} \phi_1 \text{ and } d \vdash_{\tau} \phi_2 \\
& d \vdash_{\tau} \phi_1 \lor \phi_2 \iff d \vdash_{\tau} \phi_1 \text{ or } d \vdash_{\tau} \phi_2
\end{align*}
\]

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, \( \phi \), rather than the types, \( \tau \), in \( \vdash_{\tau} \phi \). To do so, it is simplest to discard the judgement form, \( \vdash_{\tau} \phi \), since Proposition 22 lets us encode the “concrete judgement,” \( S \vdash_{\tau} \phi \), by \( S \vdash_{L(\tau)} \forall \phi \) and encode the “abstract judgement,” \( a \vdash_{\tau} \phi \), by \( \downarrow a \vdash_{L(\tau)} \forall \phi \) when all base-typed relations, \( \rho_b \subseteq C_b \times A_b \), are U-closed and monotone.

9.3 Validating \( \neg \phi \) requires a refutation logic

For \( c \in C \), we define \( c \vdash_{\tau} \neg \phi \) iff \( c \not\vdash_{\tau} \phi \).

The logic developed so far validates properties, and we might have also a logic that refutes them: Read \( a \vdash_{\tau} \neg \phi \) as “it is not possible that any value modelled by \( a \in A_{\tau} \) has property \( \phi \).” Here is the definition of a refutation logic:

\(^{19}\)The intuition is that \( \gamma_{\rho_{b}}(a') \subseteq \gamma_{\rho_{b}}(a) \subseteq \llbracket \phi \rrbracket \subseteq C_{\tau} \), where \( \llbracket \phi \rrbracket = \{ c \in C_{\tau} \mid c \vdash_{\tau} \phi \} \).

\(^{20}\)When \( \rho_b \) is U-closed and also \( a \vdash_{b} p \iff \forall a \in A_{b} \), then \( a \vdash_{b} p \) is monotone.
For a fixed family of logical relations and domains, concrete transition function, $R^\tau : C_\tau \to P(C_\tau)$, and Galois connection, $P(C_\tau) \times (\mathcal{P}(C_{\gamma(\tau)}) \to A_{\gamma(\tau)})$, we have that $R^\tau_{\text{best}} : A_\tau \to L(A_\tau)$ and $R^\tau_{\text{best}} : A_\tau \to P_U(A_\tau)$ soundly prove the most typed judgements, $a \models_\tau \phi$ and $a \models_\tau \phi$, for all $a \in A_\tau$.

**Proof.** A simultaneous but routine induction on assertions, $\phi$, in $\models_\tau \phi$ and $\models_\tau \phi$.

The Sagiv-Reps-Wilhelm TVLA system simultaneously calculates validation and refutation logics[38]. Indeed, we might combine $\rho_\tau(L(\gamma(\tau)))$ and $\rho_\tau(U(\gamma(\tau))$ into $\rho_\tau \subseteq \mathcal{P}(C) \times (\mathcal{P}(L(A)) \times \mathcal{P}(U(A)))$. This motivates sandwich- and mixed-powerdomains in a theory of over-underapproximation of sets [5, 19, 22, 25, 26].

### 10 Related work

In addition to Dams’s work [12, 14], three other lines of research deserve mention:

---

21 The intuition is that $a \models_\tau \phi$ implies $\gamma_\tau(a) \cap [\phi] = \emptyset$. For base types, $b$, define $a \models_\tau p$ iff for all $c \in C_\tau$, $c \rho_b a$ implies $c \not\models_\tau p$. When $\rho_b$ is U-closed, $\models_\tau p$ is sound and monotone.
10.1 Loiseaux, et al. [31]

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 $\mathcal{P}(C)(\text{post}[\rho], \text{pre}[\rho])/\mathcal{P}(A)$ is always a Galois connection.\footnote{Indeed, it is an axiality [17]; $\text{pre}[\rho] = \lambda T.\{c \mid \{a \mid c \rho a\} \subseteq T\}$ is $\rho$ “reduced” to an underapproximation function, and $\text{post}[\rho] = \lambda S.\{a \mid \exists c \in S, c \rho a\}$. $A$’s partial ordering, if any, is forgotten.}

For $R \subseteq C \times C$ and $R^2 \subseteq A \times A$, simulation is equivalently defined as $R$ is $\rho$-simulated by $R^2$ iff $R^{-1} \cdot \rho \subseteq \rho \cdot (R^2)^{-1}$ treating $R^{-1}$ and $(R^2)^{-1}$ as functions, we can define Galois-connection soundness as

$$(R^2)^{-1} \text{ is a sound overapproximation for } R^{-1} \text{ with respect to } \gamma \text{ iff }\quad \text{pre}[R] \circ \gamma \subseteq \mathcal{P}(A) \rightarrow \mathcal{P}(C) \gamma \circ \text{pre}[R^2] $$

For $\rho$, $R$, $R^2$, Loiseaux, et al. prove

1. $R$ is $\rho$-simulated by $R^2$ iff $(R^2)^{-1}$ is sound for $R^{-1}$ w.r.t. $\text{pre}[\rho]$.
2. $a \models \phi \in ACTL$ [$7$] implies $c \models \phi$, for $c \rho a$.

10.2 Backhouse and Backhouse [4]

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 $\{(c, a) \mid \alpha c \subseteq A a\} = \rho = \{(c, a) \mid c \subseteq A \gamma a\}$.

For the category, $\mathcal{C}$, of partially ordered sets (objects) and binary relations (morphisms), if an endofunctor, $\sigma : \mathcal{C} \Rightarrow \mathcal{C}$, 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 $\sigma$ maps pair algebras to pair algebras, that is, $\sigma$ is a unary type constructor that lifts a Galois connection between $C$ and $A$ to one between $\sigma C$ and $\sigma A$.

The result generalizes to $n$-ary functors and applies to the standard functors, $\tau \times \tau$, $\tau \rightarrow \tau$, $\text{List}(\tau)$, etc. But the result does not apply to $\mathcal{P}_L(\tau)$ nor $\mathcal{P}_U(\tau)$ — invertibility (2) fails.

10.3 Ranzato and Tapparo [37]

Ranzato and Tapparo studied the completion of upper closure maps, $\mu : \mathcal{P}(C) \rightarrow \mathcal{P}(C)$.\footnote{An upper closure map, $\mu : \mathcal{P}(C) \rightarrow \mathcal{P}(C)$, is monotone, extensive, and idempotent, and induces the Galois connection, $\mathcal{P}(C)(\mu, \text{id})/\mathcal{P}(C)$.} Given a logic, $\mathcal{L}$, of form, $\phi ::= \text{op}_j(\phi_j)_{0 \leq j < |\text{op}|}$, its semantics, $[\cdot] \subseteq \mathcal{P}(C)$, has format

$$[\text{op}_i(\phi_j)] = \text{f}_i([\phi_j])_{0 \leq j < |\text{op}_i|}$$
where each \( f_i : \mathcal{P}(C)^{|op_i|} \to \mathcal{P}(C) \) gives the semantics of connector \( op_i \). The abstract semantics has form, \([op_i(\phi_j)]^\mu = (\mu \circ f_i)([\phi_j]^\mu)\), and \([\phi]^\mu \in \mu[\mathcal{P}(C)]\).

Upper closure \( \mu \) is \( \mathcal{L} \)-preserving if, for all \( S \subseteq C \), \( \mu S \subseteq [\phi]^\mu \) implies \( S \subseteq [\phi] \), and it is \( \mathcal{L} \)-strongly preserving if the implies is replaced by iff.

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

\[
\text{complete}(\mu) = \text{gfp}(\lambda \rho. \mu \cap \mathcal{M}(R_{\{f_i\}}(\rho)))
\]

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

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

Acknowledgments

Michael Huth and Radha Jagadeesan provided valuable advice within earlier collaborations. Radhia Cousot provided a supportive environment at École Polytechnique. Tino Cortesi, Patrick Cousot, Dennis Dams, and the referees made useful comments.

References