Refinement for Symbolic Trajectory Evaluation

Authors

Chalmers

Abstract. Model refinement such that it preserves symbolic trajectory evalutions.

Keywords: STE · Refinement · ?

1 Symbolic Trajectory Evaluation

Symbolic trajectory evaluation [5] (STE) is a high-performance model checking technique based on *symbolic simulation* extended with a temporal *next-time* operator to describe circuit behaviour over time. In its simplest form, STE tests the validity of an *assertion* of the form $A \Rightarrow C$, where both the *antecedent* A and *consequent* C are formulas in the following logic:

$$f ::= p \mid f \wedge f \mid P \to f \mid \mathbf{N}\, f$$

Here, p is a simple predicate over "values" in a circuit and P is a Boolean propositional formula, and the operators $\wedge$, $\to$ and $\mathbf{N}$ are conjunction, domain restriction and the next-time operator, respectively.

If the circuit contains Boolean signals, p is typically drawn from the following two predicates: $n\,\mathbf{is}\,1$ and $n\,\mathbf{is}\,0$, where n ranges over the signals (or nodes) in a circuit. For example, suppose we have a unit-delayed, two-input AND-gate, then it is reasonable to assume that the assertion $(\mathit{in_1}\,\mathbf{is}\,1 \wedge \mathit{in_2}\,\mathbf{is}\,1) \Rightarrow \mathbf{N}(\mathit{out}\,\mathbf{is}\,1)$ is true. Indeed, STE efficiently validates such statements for us.

While the truth semantics of an assertion in STE is defined as the satisfaction of its "defining" trajectory (bounded sequence of states) relative to a model structure of the circuit, what the STE algorithm computes is exactly the solution of a data-flow equation [1] in the classic format [4]. ...

2 Set-theoretic STE

Consider an arbitrary, but fixed, digital circuit M operating in discrete time. A *configuration* of M, denoted by $\mathbb{C}$, is non-empty and finite set that represents a snapshot of M at a discrete point in time. If the circuit M has m boolean signals, then its set of configurations is typically represented as a sequence $\mathbb{B}^m$, where $\mathbb{B} = \{0, 1\}$ is the set of boolean values.

Circuit Model A simple conceptual model of M is a *transition relation*, $M_R \subseteq \mathbb{C} \times \mathbb{C}$, where $(c, c') \in M_R$ means that M can move from c to c' in one step[1]. The power set of $\mathbb{C}$, denoted by $\wp(\mathbb{C})$, can be viewed as a the set of *predicates* on configurations, where $\cap$, $\cup$, and $\subseteq$ correspond to conjunction, disjunction and implication, respectively. We denote by $\cap S$ and $\cup S$ the intersection and union of all members of any $S \subseteq \wp(\mathbb{C})$.

M_R induces a *predicate transformer* $M_F \in \wp(\mathbb{C}) \to \wp(\mathbb{C})$ using the relational image operation:

$$M_F(C) = \{c' \in \mathbb{C} \mid \exists c \in C : (c, c') \in M_R\}$$

It is intuitively obvious that if M is in one of the configurations in $C \in \wp(\mathbb{C})$, then in one time step it must be in one of the configurations in $M_F(p)$. We also see that M_F distributes over arbitrary unions:

$$M_F(\cup S) = \cup\{M_F(C) \mid C \in S\}$$

for all $S \subseteq \wp(\mathbb{C})$. In general, any M_F that satisfies this distributive property also defines a M_R through the equivalence $(c, c') \in M_R \Leftrightarrow c' \in M_F(\{c\})$, that is to say, there is no loss of information going from M_R to M_F or vice versa. We adopt this functional model of M and drop its subscript.

Exactly what $\mathbb{C}$ and its signals are, is not important in this section. In practice, however, signals are typically divided into external, such as "inputs" and "outputs", and internal parts. While an input signal is generally controlled by the external environment, and thus unconstrained by M itself, non-input signals are determined by the circuit topology and functionality. For example, supposed M is the earlier example of a unit-delayed two-input AND gate, we could then define its model $M \in \wp(\mathbb{B}^3) \to \wp(\mathbb{B}^3)$ as follows:

$$M(C) = \{\langle b_1, b_2, i_1 \wedge i_2\rangle \in \mathbb{B}^3 \mid \langle i_1, i_2, o\rangle \in C\}$$

Here i_1 and i_2 refer to the two inputs of the AND gate, o the ignored output, and b_1 and b_2 are unconstrained inputs for the new configurations.

Assertions and satisfaction A *trajectory assertion* for M is quintuple $A = (S, s_0, R, \pi_{\mathrm{a}}, \pi_{\mathrm{c}})$, where S is a finite set of *states*, $s_0 \in S$ is an *initial state*, $R \subseteq S \times S$ is a *transition relation*, $\pi_{\mathrm{a}} \in S \to \wp(\mathbb{C})$ and $\pi_{\mathrm{c}} \in S \to \wp(\mathbb{C})$ label each state s with an *antecedent* $\pi_{\mathrm{a}}(s)$ and a *consequent* $\pi_{\mathrm{c}}(s)$. We assume that $(s, s_0) \notin S$ for all $s \in S$ without any loss of generality.

The circuit model M intuitively *satisfies* an assertion A if, for every *trajectory* τ through M and every *run* ρ through A, τ satisfying the antecedents of ρ entails that τ also satisfies the consequents of ρ. To be specific, a *trajectory* of M is a non-empty sequences of configurations, $\tau \in \mathbb{C}^+$, such that $\tau_n \in M(\{\tau_{n-1}\})$ for all $n \in \mathbb{N} : 0 < n < |\tau|$. And a *run* of A is a non-empty sequence of states, $\rho \in S^+$, such that $\rho_0 = s_0$ and $(\rho_{n-1}, \rho_n) \in R$ for all $n \in \mathbb{N} : 0 < n < |\rho|$.

[1] Mention how this affects circuits with zero-delays?

A τ satisfies the antecedents of ρ, denoted by $\tau \models_{\mathrm{a}} \rho$, iff $\tau_n \in \pi_{\mathrm{a}}(\rho_n)$ for all $n \in \mathbb{N} : n < |\tau| = |\rho|$; satisfaction of consequents is defined similarly with π_{c} and denoted by $\tau \models_{\mathrm{c}} \rho$.

That M satisfies A, denoted by $M \models A$, can then be formalized as follows:

$$\forall \tau \in \mathit{Traj}(M) : \forall \rho \in \mathit{Runs}(A) : |\tau| = |\rho| \Rightarrow (\tau \models_a \rho \Rightarrow \tau \models_c \rho)$$

where $\mathit{Traj}(M)$ and $\mathit{Runs}(A)$ denote the sets of all trajectories of M and runs of A, respectively. This satisfaction can be formulated equivalently as a problem for deterministic finite automaton.

2.1 Refinement

Consider another fixed, but arbitrary, circuit model $N \in \wp(\mathbb{D}) \to \wp(\mathbb{D})$, where $\mathbb{D}$ is a non-empty and finite set of configurations. Exactly what configurations such as $\mathbb{C}$ and $\mathbb{D}$ are, were not important previously. But to reason about refinement, which relates the external behaviour of circuits, we make a distinction between their elements. Let $\sim \subseteq \mathbb{C} \times \mathbb{C}$ be an equivalence relation on $\mathbb{C}$. The equivalence class of a $c \in \mathbb{C}$ under $\sim$, denoted by $[c]$, is defined as $[c] = \{c' \in \mathbb{C} | c' \sim c\}$. With a slight abuse of notation, we overload both $\sim$ and $[\cdot]$ to accept configurations in $\mathbb{D}$. We also extend $[\cdot]$ to sets $C \subseteq \mathbb{C}$ as $[C] = \cup\{[c] \in \wp(\mathbb{C}) \mid c \in C\}$.

Refinement by trajectories Let there be a Galois connection between predicates $\wp(\mathbb{C})$ and $\wp(\mathbb{D})$ ordered by set inclusion. The usual definition of a Galois connection is in terms of an *abstraction* $\alpha \in \wp(\mathbb{C}) \to \wp(\mathbb{D})$ and a *concretisation* $\gamma \in \wp(\mathbb{D}) \to \wp(\mathbb{C})$ function, such that $\alpha(C) \subseteq D \Leftrightarrow C \subseteq \gamma(D)$ for all $C \in \wp(\mathbb{C})$ and $D \in \wp(\mathbb{D})$. For example, a Galois connection between ...

Furthermore, let the binary relation $\ll \subseteq \wp(\mathbb{C}) \times \wp(\mathbb{D})$, where $C \ll D$ reads "C can be approximated by D", be derived from the above α or γ, such that:

$$C \ll D \Leftrightarrow \alpha([C]) \subseteq [D] \qquad\qquad C \ll D \Leftrightarrow [C] \subseteq \gamma([D])$$

Here $\subseteq$ on the α-derivation side is the inclusion order of $\wp(\mathbb{D})$, and on the γ-derivation side $\subseteq$ is the inclusion order of $\wp(\mathbb{C})$. Intuitively, $\ll$ acts as an extension of the orderings inside $\wp(\mathbb{C})$ and $\wp(\mathbb{D})$ to one between equivalence classes of them. We require that $\alpha([c]) \neq \emptyset$ for all $c \in \mathbb{C}$. We extend $\ll$ to sequences component wise, such that $\tau \ll \upsilon$ iff $\{\tau_n\} \ll \{\upsilon_n\}$ for all $\tau \in \mathbb{C}^+$, $\upsilon \in \mathbb{D}^+$, and $n \in \mathbb{N} : n < |\tau| = |\upsilon|$.

We can now formalize that M *refines* N, denoted by $M \leq N$, as follows:

$$\forall \tau \in \mathit{Traj}(M) : \exists \upsilon \in \mathit{Traj}(N) : |\tau| = |\upsilon| \wedge \tau \ll \upsilon$$

In other words, for every sequence of configurations τ permitted by M, there must exist a sequence υ for N which approximates the behaviour of τ according to their equivalence relations. Example.

Refinement & assertions Recall that a trajectory assertion for N is a quintuple $A = (S, s_0, R, \pi_a, \pi_c)$, where $\pi_a \in S \to \wp(\mathbb{D})$ and $\pi_c \in S \to \wp(\mathbb{D})$ label each $s \in S$ with its antecedents and consequents, respectively. If π_a and π_c are class invariant under $\sim$, i.e. $d \in \pi_a(s) \Leftrightarrow [d] \subseteq \pi_a(s)$ for all $s \in S$ and similarly for π_c, then we refer to A as an *name trajectory assertion* and suffix it as A_n. Furthermore, we define $\gamma(A) = (S, s_0, R, \gamma(\pi_a), \gamma(\pi_c))$, where $\gamma(\pi_a) = \lambda s \in S : \gamma(\pi_a(s))$ and $\gamma(\pi_c) = \lambda s \in S : \gamma(\pi_c(s))$.

We are now ready to state that, if M refines N and A_n is satisfied in N, then a concretisation of A_n can also be satisfied in M:

Theorem 1. $M \leq N \Rightarrow (N \models A_n \Rightarrow M \models \gamma(A_n))$

Refinement can be equivalently formulated as $\ll$ being a simulation relation. More specifically, we say that M refines N by *set-theoretic simulation*, denoted by $M \leq_{\text{set}} N$, iff (1) $\ll$ is a name, i.e. $C \ll D \Rightarrow \forall c \in C : \exists d \in D : \{c\} \ll \{d\}$; and (2) $\ll$ is a *simulation relation* from $\wp(\mathbb{C})$ to $\wp(\mathbb{D})$, i.e. $C \ll D \Rightarrow M(C) \ll N(D)$. That $\ll$ is a simulation relation can also be stated directly in terms of the usual abstraction function: $\alpha([M(C)]) \subseteq N(\alpha([C]))$ for all $C \in \wp(\mathbb{C})$, or the concretisation function: $M(\gamma([D]) \subseteq \gamma(N([D]))$ for all $D \in \wp(\mathbb{D})$.

Theorem 2. $M \leq N \Leftrightarrow M \leq_{set} N$

Text.

3 Lattice-theoretic STE

Manipulating subsets of $\mathbb{B}^m$ is impractical for even moderately large m, which leads us to one of the key insights of STE. Namely, instead of manipulating subsets of $\mathbb{B}^m$ directly, one can use sequences of ternary values $\mathbb{T} = \mathbb{B} \cup \{\mathrm{X}\}$ to approximate them, whose sizes are only linear in m. Here the 1 and 0 from $\mathbb{B}$ denotes specific, defined values whereas X denotes an "unknown" value that could be either 1 or 0. This intuition induces a partial order $\sqsubseteq$ on $\mathbb{T}$, where $0 \sqsubseteq \mathrm{X}$ and $1 \sqsubseteq \mathrm{X}$[2]. For any $m \in \mathbb{N}$, this ordering on $\mathbb{T}$ is lifted component-wise to $\mathbb{T}^m$.

Note that $\mathbb{T}^m$ does not quite form a complete lattice because it lacks a bottom: both $0 \sqsubseteq \mathrm{X}$ and $1 \sqsubseteq \mathrm{X}$ but 0 and 1 are equally defined. A special bottom element $\perp$ is therefore introduced, such that $\perp \sqsubseteq t$ and $\perp \neq t$ for all $t \in \mathbb{T}^m$. The extended $\mathbb{T}^m_\perp = \mathbb{T}^m \cup \{\perp\}$ then becomes a complete lattice. We denote the top element $\langle \mathrm{X}, \ldots, \mathrm{X} \rangle$ of $\mathbb{T}^m_\perp$ by $\top$.

Ternary lattices Generalising from any specific domain, let $(\hat{\mathbb{P}}, \sqsubseteq)$ be a finite, complete lattice of *abstract predicates* in which the meet $\sqcap$ and join $\sqcup$ of any subset $\hat{S} \subseteq \hat{\mathbb{P}}$ exists. Similar to the previous set operations for power sets, $\sqcap$, $\sqcup$ and $\sqsubseteq$ correspond to conjunction, disjunction and implication for abstract

[2] We use the reverse ordering of what is originally used in STE to make the abstraction-correspondence clear between $\cap$ and $\sqcap$, $\cup$ and $\sqcup$, and $\subseteq$ and $\sqsubseteq$.

predicates, respectively. Furthermore, for any $\hat{S} \subseteq \hat{\mathbb{P}}$, we denote by $\sqcap\hat{S}$ and $\sqcup\hat{S}$ the meet and join of all members of $\hat{S}$.

Let there be a Galois connection relating "concrete" predicates $\wp(\mathbb{C})$ and abstract predicates $\hat{\mathbb{P}}$. As before, the Galois connection is defined in terms of an *abstraction* $\hat{\alpha} \in \wp(\mathbb{C}) \rightarrow \hat{\mathbb{P}}$ and a *concretisation* $\hat{\gamma} \in \hat{\mathbb{P}} \rightarrow \wp(\mathbb{C})$ function, such that $\hat{\alpha}(C) \sqsubseteq \hat{p} \Leftrightarrow C \subseteq \hat{\gamma}(\hat{p})$ for all $C \in \wp(\mathbb{C})$ and $\hat{p} \in \hat{\mathbb{P}}$. For example, a Galois connection from $\wp(\mathbb{B}^m)$ to $\mathbb{T}^m_\perp$ for any $m \in \mathbb{N}$ can be defined in a natural way through its concretisation function $\hat{\gamma} \in \mathbb{T}^m_\perp \rightarrow \wp(\mathbb{B}^m)$:

$$\begin{aligned}\hat{\gamma}(\langle t_0, \ldots, t_{m-1}\rangle) &= \{\langle b_0, \ldots, b_{m-1}\rangle \in \mathbb{B}^m \mid \forall i < m : t_i \neq \mathrm{X} \Rightarrow b_i = t_i\} \\ \hat{\gamma}(\perp) &= \emptyset\end{aligned}$$

which list each concrete predicate approximated by a given abstract predicate.

Abstract circuit model An *abstract predicate transformer* $\hat{M} \in \hat{\mathbb{P}} \rightarrow \hat{P}$ is an *abstract interpretation* [1,2] of $M \in \wp(\mathbb{C}) \rightarrow \wp(\mathbb{C})$ iff (1) $\hat{M}$ preserves $\perp$, i.e. $\hat{M}(\perp) = \perp$; (2) $\hat{M}$ is monotonic, i.e. $\hat{p} \sqsubseteq \hat{q} \Rightarrow \hat{M}(\hat{p}) \sqsubseteq \hat{M}(\hat{q})$ for all $\hat{p}, \hat{q} \in \hat{\mathbb{P}}$; and (3) α, or γ, form a *simulation relation* between the predicates $\wp(\mathbb{C})$ and $\hat{P}$, i.e. $\alpha(M(C)) \sqsubseteq \hat{M}(\alpha(C))$ for all $C \in \wp(\mathbb{C})$, or $M(\gamma(\hat{p})) \subseteq \gamma(\hat{M}(\hat{p}))$ for all $\hat{p} \in \hat{\mathbb{P}}$.

Note that $\hat{M}$, unlike its concrete model M it interprets, does not distribute over arbitrary join; information is potentially discarded by the ternary logic that would have been kept in binary logic. As an example, let the following $\hat{M}$ abstract the previous model of an unit-delayed two-input AND gate:

$$\begin{array}{ll}\hat{M}(\langle 1, 1, \hat{p}_2\rangle) \;\;\;= \langle \mathrm{X}, \mathrm{X}, 1\rangle & \hat{M}(\langle 0, 0, \hat{p}_2\rangle) = \langle \mathrm{X}, \mathrm{X}, 0\rangle \\ \hat{M}(\langle 0, \mathrm{X}, \hat{p}_2\rangle) \;\;\;= \langle \mathrm{X}, \mathrm{X}, 0\rangle & \hat{M}(\langle \mathrm{X}, 0, \hat{p}_2\rangle) = \langle \mathrm{X}, \mathrm{X}, \mathrm{X}\rangle \\ \hat{M}(\langle \hat{p}_0, \hat{p}_1, \hat{p}_2\rangle) = \langle \mathrm{X}, \mathrm{X}, \mathrm{X}\rangle & \end{array}$$

where the last and most general matching is overlapped by the more specific matchings above it. If we apply $\hat{M}$ to the join of $\langle 0, 1, \mathrm{X}\rangle$ and $\langle 1, 0, \mathrm{X}\rangle$, or if we apply $\hat{M}$ to them individually and then join, we get two different results:

$$\begin{array}{lll}\hat{M}(\langle 0, 1, \mathrm{X}\rangle \sqcup \langle 1, 0, \mathrm{X}\rangle) & = \hat{M}(\langle \mathrm{X}, \mathrm{X}, \mathrm{X}\rangle) & = \langle \mathrm{X}, \mathrm{X}, \mathrm{X}\rangle \\ \hat{M}(\langle 0, 1, \mathrm{X}\rangle) \sqcup \hat{M}(\langle 1, 0, \mathrm{X}\rangle) & = \langle \mathrm{X}, \mathrm{X}, 0\rangle \sqcup \langle \mathrm{X}, \mathrm{X}, 0\rangle & = \langle \mathrm{X}, \mathrm{X}, 0\rangle\end{array}$$

The inequality $\sqcup\{\hat{M}(\hat{p}) \mid \hat{p} \in \hat{S}\} \sqsubseteq \hat{M}(\sqcup\hat{S})$ for all $\hat{S} \sqsubseteq \hat{P}$ does however hold, since it is implied by the monotonicity of $\hat{M}$.

Assertions and satisfaction A trajectory assertion for an abstract model $\hat{M}$ is a quintuple $\hat{A} = (S, s_0, R, \hat{\pi}_a, \hat{\pi}_c)$, where S, s_0, and R are as in section 2 and $\hat{\pi}_a \in S \rightarrow \hat{\mathbb{P}}$ and $\hat{\pi}_c \in S \rightarrow \hat{\mathbb{P}}$ label each state $s \in S$ with an abstract predicate for its antecedent and consequent, respectively. $\hat{M}$ satisfies $\hat{A}$ intuitively if, for every state $s \in S$, the information gathered from $\hat{M}$ when restricted by the antecedents in states before s, implies the consequent for s. Before we can formalize this intuition, however, we must introduce a few functions.

For all functions $\hat{\Phi} \in S \to \hat{\mathbb{P}}$ and states $s \in S$, define $\hat{F} \in S \to (\hat{\mathbb{P}} \to \hat{\mathbb{P}})$ and $\hat{\mathcal{F}} \in (S \to \hat{\mathbb{P}}) \to (S \to \hat{\mathbb{P}})$ as follows:

$$\hat{F}(s)(\hat{p}) = \hat{M}(\pi_{\mathrm{a}}(s) \sqcap \hat{p}) \tag{1}$$

$$\hat{\mathcal{F}}(\Phi)(s) = \textbf{if } (s = s_0) \textbf{ then } \top \textbf{ else } \sqcup \{\hat{F}(s')(\Phi(s')) \mid (s', s) \in R\} \tag{2}$$

We see that $\hat{F}$ preserves $\bot$, and both $\hat{F}$ and $\hat{\mathcal{F}}$ are monotonic; two $\hat{\Phi}, \hat{\Phi}' \in S \to \hat{\mathbb{P}}$ are ordered as $\hat{\Phi} \sqsubseteq \hat{\Phi}' \Leftrightarrow \forall s \in S : \hat{\Phi}(s) \sqsubseteq \hat{\Phi}'(s)$. Let $\hat{\Phi}_* \in S \to \hat{\mathbb{P}}$ be the least fixpoint of the equation $\hat{\Phi} = \hat{\mathcal{F}}(\hat{\Phi})$ [3]. Since both S and $\hat{\mathbb{P}}$ are finite, $\hat{\Phi}_*$ is given by $\lim \hat{\Phi}_n(s)$, where $\hat{\Phi}_n$ is defined as follows:

$$\hat{\Phi}_n = \textbf{if } (n = 0) \textbf{ then } (\lambda s \in S : \bot) \textbf{ else } \hat{\mathcal{F}}(\hat{\Phi}_{n-1}) \tag{3}$$

We can now adopt the definition of satisfaction from [1], and say that $\hat{M}$ *satisfies* a trajectory assertion $\hat{A}$, denoted by $\hat{M} \models_{\mathrm{lat}} \hat{A}$, iff $\hat{\Phi}_*(s) \sqcap \pi_\alpha(s) \sqsubseteq \pi_{\mathrm{c}}(s)$ for all $s \in S$. That $\hat{M}$ satisfies $\hat{A}$ implies that a concretisation of $\hat{A}$ can also be satisfied by the original, set-based model M.

3.1 Refinement

Let the abstract predicate transformer $\hat{N} \in \hat{\mathbb{Q}} \to \hat{\mathbb{Q}}$ be an abstract interpretation of the earlier circuit model N, where $\hat{\mathbb{Q}}$ is an abstract predicate for which there exists a Galois connection to $\wp(\mathbb{D})$.

Let the equivalence in $\hat{\mathbb{P}}$ be identified by a function $[\![\cdot]\!] \in \hat{\mathbb{P}} \to \hat{\mathbb{P}}$, such that $[\![\cdot]\!]$ (?) preserves bottom, i.e. $[\![\bot]\!] = \bot$; (1) is idempotent, i.e. $[\![([\![\hat{p}]\!])]\!] = [\![\hat{p}]\!]$; (2) is monotonic, i.e. $\hat{p} \sqsubseteq \hat{q} \Rightarrow [\![\hat{p}]\!] \sqsubseteq [\![\hat{q}]\!]$; and (3) name, i.e. $[\![\hat{p}]\!] \sqsubseteq [\![\hat{q}]\!] \Leftrightarrow \hat{p} \sqsubseteq [\![\hat{q}]\!]$.

Let there exist a Galois connection between $\hat{\mathbb{P}}$ and $\hat{\mathbb{Q}}$, given by the usual functions for abstraction $\hat{\alpha} \in \hat{\mathbb{P}} \to \hat{\mathbb{Q}}$ and concretisation $\hat{\gamma} \in \hat{\mathbb{Q}} \to \hat{\mathbb{P}}$, such that $\hat{\alpha}(\hat{p}) \sqsubseteq \hat{q} \Leftrightarrow \hat{p} \subseteq \hat{\gamma}(\hat{q})$ for all $\hat{p} \in \hat{\mathbb{P}}$ and $\hat{q} \in \hat{\mathbb{Q}}$.

Let the binary relation $\lll \subseteq \hat{\mathbb{P}} \times \hat{\mathbb{Q}}$ be derived from the above $\hat{\alpha}$ or $\hat{\gamma}$:

$$\hat{p} \lll \hat{q} \Leftrightarrow \hat{\alpha}([\![\hat{p}]\!]) \sqsubseteq [\![\hat{q}]\!] \qquad\qquad \hat{p} \lll \hat{q} \Leftrightarrow [\![\hat{p}]\!] \sqsubseteq \hat{\gamma}([\![\hat{q}]\!])$$

Here $\sqsubseteq$ on $\hat{\alpha}$-derivation side is the partial order of $\hat{\mathbb{Q}}$, and on the $\hat{\gamma}$-derivation side $\sqsubseteq$ is the partial order of $\hat{\mathbb{P}}$.

Finally, we say that $\hat{M}$ refines $\hat{N}$ by *lattice-theoretic simulation*, denoted by $\hat{M} \leq_{\mathrm{lat}} \hat{N}$, iff (1) $\lll$ is a simulation relation, i.e. $\hat{p} \lll \hat{q} \Rightarrow \hat{M}(\hat{p}) \lll \hat{N}(\hat{q})$.

Theorem 3. $\hat{M} \leq_{lat} \hat{N} \Rightarrow (\hat{N} \models_{lat} \hat{A}_n \Rightarrow \hat{M} \models_{lat} \hat{\gamma}(\hat{A}_n))$

Theorem 4. $\hat{M} \leq_{lat} \hat{N} \Rightarrow M \leq_{set} N$

A Appendices

A.1 Theorem 1

We first prove a few lemmas.

Lemma 1. $[d] \cap \pi_a(\rho) \neq \emptyset \Rightarrow [d] \subseteq \pi_a(\rho)$

Since they intersect, there must exist $d' \in [d]$ such that $d' \in \pi_{\mathrm{a}}(\rho)$. By the invariance of $\pi_{\mathrm{a}}(\rho)$, it must be that $[d'] = [d] \subseteq \pi_{\mathrm{a}}(\rho)$. □

Lemma 2. $d \in \pi_c(\rho) \wedge \{c\} \ll \{d\} \Rightarrow c \in \gamma(\pi_c(\rho))$

By the invariance of π_{c}, $d \in \pi_{\mathrm{c}}(\rho) \Rightarrow [d] \subseteq \pi_{\mathrm{c}}(\rho)$ which, by the monotonicity of γ, implies $\gamma([d]) \subseteq \gamma(\pi_{\mathrm{c}}(\rho))$. By definition of $\{c\} \ll \{d\}$, we know $[c] \subseteq \gamma([d])$, thus $[c] \subseteq \gamma(\pi_{\mathrm{c}}(\rho))$. □

Lemma 3. $c \in \gamma(\pi_a(\rho)) \wedge \{c\} \ll \{d\} \Rightarrow d \in \pi_a(\rho)$

By the invariance of π_{a} and the definition of $\gamma(\pi_{\mathrm{a}})$, $c \in \gamma(\pi_{\mathrm{a}}(\rho))$ states that $[c] \subseteq \gamma(\pi_{\mathrm{a}}(\rho))$. And thus $\alpha([c]) \subseteq \alpha(\gamma(\pi_{\mathrm{a}}(\rho)) \subseteq \pi_{\mathrm{a}}(\rho)$ by the monotonicity of α. By definition $\{c\} \ll \{d\}$, we also have that $\alpha([c]) \subseteq [d]$. Since $\alpha([c]) \neq \emptyset$, it must be that $[d] \cap \pi_{\mathrm{a}}(\rho) \neq \emptyset$, and thus $[d] \subseteq \pi_{\mathrm{a}}(\rho)$ by lemma 1. Then, by the invariance of π_{a}, we must have that $d \in \pi_{\mathrm{a}}(\rho)$. □

For the theorem, we are given $\tau \in \mathit{Traj}(M)$ and $\rho \in \mathit{Runs}(\gamma(A))$, such that $|\tau| = |\rho|$ and $\tau_n \in \gamma(\pi_{\mathrm{a}}(\rho_n))$ for all $n \in \mathbb{N} : n < |\tau|$. We must then show that $\tau_n \in \gamma(\pi_{\mathrm{c}}(\rho_n))$. By the refinement assumption, there must exist a $\upsilon \in \mathit{Traj}(N)$ such that $|\tau| = |\upsilon| = |\rho|$ and $\{\tau_n\} \ll \{\upsilon_n\}$. By lemma 3, we know $\upsilon_n \in \pi_{\mathrm{a}}(\rho_n)$ and thus $\upsilon_n \in \pi_{\mathrm{c}}(\rho_n)$. Lemma 2 then states that $\tau_n \in \gamma(\pi_{\mathrm{c}}(\rho_n))$. □

A.2 Theorem 2

We first show a lemma.

Lemma 4. $C \ll D \wedge D \subseteq D' \Rightarrow C \ll D'$

That C is approximated by D' follows immediately: $\alpha(C) \subseteq D \subseteq D'$. The first property of $\ll$ follows from the definition of subset, and the second by the monotonicity of N: $\alpha(M(C)) \subseteq N(D) \subseteq N(D')$. □

We prove each direction of the theorem separately.

$(\Rightarrow)$: If $C \ll D$, then by definition $\alpha([C]) \subseteq [D]$. As α distributes over arbitrary union, it follows that $\alpha([c]) \subseteq [D]$ for all $c \in C$. Furthermore, applying the assumption $M \leq N$ to one-length trajectories starting in c, there must also exist $d \in \mathbb{D}$ such that $\{c\} \ll \{d\}$, or $\alpha([c]) \subseteq [d]$ by definition of $\ll$. Since $\alpha([c]) \neq \emptyset$, it must be that $[d] \cap [D] \neq \emptyset$. By lemma 1 then, we know $[d] \subseteq [D]$ and thus $d \in D$. This shows that the first property of $\ll$ is implied. For the second property, that $\ll$ is a simulation relation, consider all two-length trajectories from C. For any $c' \in M(C)$, there exists a $d' \in N(D)$ such that $\{c'\} \ll \{d'\}$, which implies that $\{c'\} \ll N(D)$ by lemma 4. Combining all such orderings, we have the desired $M(C) \ll N(D)$. □

($\Leftarrow$) : We show this claim by induction on the length of τ. For the base case, when $|\tau| = 1$, we are given $\tau = \langle \tau_1 \rangle$ where τ_1 is unconstrained, i.e. we only know that $\tau_1 \in \mathbb{C}$. But a Galois connection always relates the most general states of its two partially ordered sets, so $\alpha(\{\mathbb{C}\}) \subseteq \{\mathbb{D}\}$. As $[\{\mathbb{C}\}] = \{\mathbb{C}\}$ and $[\{\mathbb{D}\}] = \{\mathbb{D}\}$, we also know that $\alpha([\{\mathbb{C}\}]) \subseteq [\{\mathbb{D}\}]$, or $\{\mathbb{C}\} \ll \{\mathbb{D}\}$. Using the first property of $\ll$ then tells us that there exists $d \in \mathbb{D}$ such that $\{\tau_1\} \ll \{d\}$. For the inductive step, when $|\tau| = n + 1$, we are given $\tau = \langle \ldots, \tau_n \rangle$ and assume there exists $\upsilon = \langle \ldots, \upsilon_n \rangle$ such that $\tau \ll \upsilon$. By the simulation property of $\ll$, we have that $M(\tau_n) \ll N(\upsilon_n)$. Applying the first property of $\ll$ then states that there exists $d \in N(\upsilon_n)$ such that $\{\tau_{n+1}\} \ll \{d\}$ for any $\tau_{n+1} \in M(\tau_n)$. The concatenation of υ and d, denoted $\upsilon^\frown\langle d \rangle$, thus forms a valid trajectory in $\mathit{Traj}(N)$ which satisfies the properties $|\tau| = |\upsilon^\frown\langle d \rangle|$ and $\tau \ll \upsilon^\frown\langle d \rangle$. □

A.3 Theorem 3

We first show a few lemmas.

Lemma 5. $\bot \lll \bot$

A Galois connection always relates the two bottoms, $\hat{\alpha}(\bot) \subseteq \bot$, which implies that $\hat{\alpha}([\![\bot]\!]) \subseteq [\![\bot]\!]$, or $\bot \lll \bot$, since $[\![\cdot]\!]$ preserves bottom. As $\hat{M}$ and $\hat{N}$ also preserves bottom, it follows that $\hat{M}(\bot) = \bot \lll \bot = \hat{N}(\bot)$. □

Lemma 6. $\hat{p} \lll \hat{q} \wedge \hat{r} \lll \hat{s} \Rightarrow (\hat{p} \sqcup \hat{r}) \lll (\hat{q} \sqcup \hat{s})$

By definition of $\lll$ and the monotonicity of $[\![\cdot]\!]$, we both have $\hat{\alpha}([\![\hat{p}]\!]) \sqsubseteq [\![\hat{q}]\!] \sqsubseteq ([\![\hat{q} \sqcup \hat{s}]\!])$ and $\hat{\alpha}([\![\hat{r}]\!]) \sqsubseteq [\![\hat{s}]\!] \sqsubseteq ([\![\hat{q} \sqcup \hat{s}]\!])$. Because join produces the least upper bound, it follows that $([\![\hat{p} \sqcup \hat{r}]\!]) \sqsubseteq \hat{\gamma}([\![\hat{q} \sqcup \hat{s}]\!])$, or $(\hat{p} \sqcup \hat{r}) \lll (\hat{q} \sqcup \hat{s})$

Text.

A.4 Theorem 4

Text.

References

1. Chou, C.T.: The mathematical foundation of symbolic trajectory evaluation. In: International Conference on Computer Aided Verification. pp. 196–207. Springer (1999)
2. Cousot, P.: Abstract interpretation. ACM Computing Surveys (CSUR) **28**(2), 324–328 (1996)

3. Davey, B.A., Priestley, H.A.: Introduction to lattices and order. Cambridge university press (2002)
4. Muchnick, S., et al.: Advanced compiler design implementation. Morgan kaufmann (1997)
5. Seger, C.J.H., Bryant, R.E.: Formal verification by symbolic evaluation of partially-ordered trajectories. Formal Methods in System Design **6**(2), 147–189 (1995)