Refinement for Symbolic Trajectory Evaluation

Author and Author

Chalmers

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

Keywords: STE · Refinement · ?

1 Symbolic Trajectory Evaluation

Symbolic trajectory evaluation [3] (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:

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

Here, p is a simple predicate over "values" in a circuit and P is a Boolean propositional formula, and the operators $\wedge$, $\rightarrow$ 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 $(in_1\ \mathbf{is}\,1 \wedge in_2\ \mathbf{is}\,1) \Rightarrow \mathbf{N}(out\ \mathbf{is}\,1)$ 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 [2]. ...

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, suppose 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* a trajectory assertion A if, for every path τ through M and every path ρ through A, τ satisfying the antecedents of ρ entails that τ also satisfies the consequents of ρ. To be specific, a path τ in M is referred to as a *trajectory* and is defined as 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 path, or *run*, ρ of A is similarly a non-empty sequence of states, $\rho \in S^+$,

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

such that $\rho_0 = s_0$ and $(\rho_{n-1}, \rho_n) \in R$ for all $n \in \mathbb{N} : 0 < n < |\rho|$. A finite trajectory τ satisfies the antecedents of a finite run 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:

$$\forall \tau \in \mathit{Traj}(M)^n : \forall \rho \in \mathit{Runs}(A)^n : |\tau| = |\rho| \Rightarrow (\tau \models_{\mathrm{a}} \rho \Rightarrow \tau \models_{\mathrm{c}} \rho)$$

where $\mathit{Traj}(M)^n$ and $\mathit{Runs}(A)^n$ denote the sets of all finite 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 visible 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 $[c] = \{c' \in \mathbb{C} \mid c' \sim c\}$. With a slight abuse of notation, we overload both $\sim$ and $[\cdot]$ to accept configurations in $\mathbb{D}$. Furthermore, we extend $[\cdot]$ to sets $C \subseteq \mathbb{C}$ by taking the union of its image, i.e. $[C] = \cup\{[c] \in \wp(\mathbb{C}) \mid c \in C\}$.

Let there be a Galois connection between the predicates $\wp(\mathbb{C})$ and $\wp(\mathbb{D})$ ordered by set inclusion, given in terms of two monotone functions: an *abstraction* $\alpha \in \wp(\mathbb{C}) \to \wp(\mathbb{D})$ and a *concretisation* $\gamma \in \wp(\mathbb{D}) \to \wp(\mathbb{C})$ function. An essential property of a Galois connection is that, for all $C \in \wp(\mathbb{C})$ and $D \in \wp(\mathbb{D})$, the pair α and γ satisfy the equality: $\alpha(C) \subseteq D \Leftrightarrow C \subseteq \gamma(D)$. Intuitively, this relation is an extension of the partial orderings inside $\wp(\mathbb{C})$ and $\wp(\mathbb{D})$ to an ordering between them. Every configuration must have an abstraction: $\alpha([\{c\}]) \neq \emptyset$ for all $c \in \mathbb{C}$.

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

$$\forall \tau \in \mathit{Traj}(M)^\infty : \exists \upsilon \in \mathit{Traj}(N)^\infty : \alpha([\tau]) \subseteq [\upsilon]$$

where $\mathit{Traj}(M)^\infty$ and $\mathit{Traj}(N)^\infty$ denotes the sets of all *infinite* trajectories in M and N, respectively, and $\alpha([\tau]) \subseteq [\upsilon]$ implies that $\alpha([\tau_n]) \subseteq [\upsilon_n]$ for all $n \in \mathbb{N}$. The sets of finite and infinite trajectories are related: $\tau \in \mathit{Traj}(M)^n \Leftrightarrow \exists \rho \in \mathit{Traj}(M)^\infty : \tau \prec \rho$. This is true if M cannot get stuck: $M(\{c\}) \neq \emptyset$ for all $c \in \mathbb{C}$.

Recall that a trajectory assertion for N is a quintuple $A = (S, s_0, R, \pi_{\mathrm{a}}, \pi_{\mathrm{c}})$, where $\pi_{\mathrm{a}} \in S \to \wp(\mathbb{D})$ and $\pi_{\mathrm{c}} \in S \to \wp(\mathbb{D})$ label each $s \in S$ with its antecedents and consequents, respectively. If π_{a} and π_{c} are invariant under the equivalence class $\sim$ of $\mathbb{D}$, i.e. $\pi_{\mathrm{a}}(s) = [\pi_{\mathrm{a}}(s)]$ and $\pi_{\mathrm{c}}(s) = [\pi_{\mathrm{c}}(s)]$ for all $s \in S$, then we refer to A as an *trajectory class assertion* and suffix it as A_c. Furthermore, we define $\gamma(A) = (S, s_0, R, \gamma(\pi_{\mathrm{a}}), \gamma(\pi_{\mathrm{c}}))$, where $\gamma(\pi_{\mathrm{a}}) = \lambda s \in S : \gamma(\pi_{\mathrm{a}}(s))$ and similarly $\gamma(\pi_{\mathrm{c}}) = \lambda s \in S : \gamma(\pi_{\mathrm{c}}(s))$.

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

Let $\ll \subseteq \wp(\mathbb{C}) \times \wp(\mathbb{D})$ be a *simulation relation* between predicates $\mathbb{C}$ and $\mathbb{D}$ ordered by set inclusion, such that, if $C \ll D$ for all $C \in \mathbb{C}$ and $D \in \mathbb{D}$, then the following conditions hold: $\alpha([C]) \subseteq [D]$, and $M(C) \ll N(D)$. ...

We say that M refines N by *set-theoretic simulation*, denoted by $M \leq_{\text{set}} N$, if there exists a simulation relation $\ll$ such that $\mathbb{C} \ll \mathbb{D}$. ...

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

A Appendices

A.1 Proof of Theorem 1

We freely expand the definition of $[\cdot]$ for $\emptyset$, singletons $\{c \in \mathbb{C}\}$, and $\mathbb{C}$.

Lemma 1. $C = [C] \wedge [d] \cap C \neq \emptyset \Rightarrow [d] \subseteq C$

$$\begin{aligned} [d] \cap C \neq \emptyset &\Rightarrow \exists x : x \in [d] \wedge x \in C && \text{(definition of } \cap) \\ &\Leftrightarrow \exists x : x \in [d] \wedge [x] \subseteq C && \text{(invariance of } C) \\ &\Rightarrow [d] \subseteq C && ([x] = [d]) \end{aligned}$$

Lemma 2. $d \in \pi_c(s) \wedge \alpha([c]) \subseteq [d] \Rightarrow c \in \gamma(\pi_c(s))$

$$\begin{aligned} d \in \pi_{\mathrm{c}}(s) &\Leftrightarrow [d] \subseteq \pi_{\mathrm{c}}(s) && \text{(invariance of } \pi_{\mathrm{c}}) \\ &\Rightarrow \alpha([c]) \subseteq \pi_{\mathrm{c}}(s) && (\alpha([c]) \subseteq [d] \text{ assumption}) \\ &\Rightarrow \alpha(\{c\}) \subseteq \pi_{\mathrm{c}}(s) && (\alpha \text{ distributes over } \cup) \\ &\Leftrightarrow c \in \gamma(\pi_{\mathrm{c}}(s)) && \text{(Galois connection)} \end{aligned}$$

Lemma 3. $c \in \gamma(\pi_a(s)) \wedge \alpha([c]) \subseteq [d] \Rightarrow d \in \pi_a(s)$

$$\begin{aligned} c \in \gamma(\pi_{\mathrm{a}}(s)) &\Leftrightarrow \alpha(\{c\}) \subseteq \pi_{\mathrm{a}}(s) && \text{(Galois connection)} \\ \alpha([c]) \subseteq [d] &\Rightarrow \alpha(\{c\}) \subseteq [d] && (\alpha \text{ distributes over } \cup) \\ &\Rightarrow [d] \subseteq \pi_{\mathrm{a}}(s) && \text{(lemma 1 and equation 1)} \end{aligned} \tag{1}$$

Lemma 4. $\tau \in \mathit{Traj}(M)^n \Leftrightarrow \exists \upsilon \in \mathit{Traj}(M)^\infty : \tau \prec \upsilon$

Proof of lemma.

Proof. 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 $\tau' \in \mathit{Traj}(M)^\infty$ and $\upsilon' \in \mathit{Traj}(N)^\infty$ such that $\tau \prec \tau'$ and $\alpha([\tau']) \subseteq [\upsilon']$. Let $\upsilon \prec \upsilon'$ such that $|\upsilon| = |\tau|$, which implies that $\alpha([\tau]) \subseteq [\upsilon]$. Lemma 3 then shows that $\upsilon_n \in \pi_{\mathrm{a}}(\rho_n)$ and, by the assumption, we have $\upsilon_n \in \pi_{\mathrm{c}}(\rho_n)$. Lemma 2 then shows that $\tau_n \in \gamma(\pi_{\mathrm{c}}(\rho_n))$.

A.2 Proof of Theorem 2

Proof. We show each direction of the theorem separately.
⇒ Proof.
⇐ Proof.

A.3 Proof of Theorem ??

First a lemma that shows $[\![\hat{p} \sqcap \hat{\pi}_{\mathrm{a}}(s)]\!] \Leftrightarrow [\![\hat{p}]\!] \sqcap \hat{\pi}_{\mathrm{a}}(s)$ is a reasonable assumption.

Lemma 5. $([D] = D) \Rightarrow ([C \cap D] \Leftrightarrow [C] \cap D)$

$$\begin{aligned} x \in [C \cap D] &\Leftrightarrow \exists y : x \sim y \wedge y \in C \wedge y \in D && \text{(definition of } [\cdot] \text{ and } \cap) \\ &\Leftrightarrow \exists y : x \sim y \wedge y \in C \wedge x \in D && (x \sim y \text{ and } D = [D]) \\ &\Leftrightarrow x \in [C] \cap D && \text{(definition of } [\cdot] \text{ and } \cap) \end{aligned}$$

Secondly we show a few helpful lemmas that regard the fix-points and functions used to determine satisfaction with $\hat{M}$ and $\hat{N}$. Before that, we duplicate the earlier definitions of F, $\mathcal{F}$ and Φ to differentiate between those used with $\hat{M}$ and those with $\hat{N}$. Specifically, let G, $\mathcal{G}$ and Ψ be equivalent operations for $\hat{N}$, as F, $\mathcal{F}$ and Φ are for $\hat{M}$:

$$\begin{aligned} G(s)(\hat{q}) &= \hat{N}(\pi_a(s) \sqcap \hat{q}) \\ \mathcal{G}(\Psi)(s) &= \textbf{if } (s = s_0) \textbf{ then } \top \textbf{ else } \sqcup \{G(s')(\Psi(s')) \mid (s', s) \in R\} \\ \Psi_n &= \textbf{if } (n = 0) \textbf{ then } (\lambda s \in S : \bot) \textbf{ else } \mathcal{G}(\Psi_{n-1}) \end{aligned}$$

Furthermore, let Ψ_* be the least fixpoint of $\Psi = \mathcal{G}(\Psi)$ and given by $\lim \Psi_n(s)$.

Lemma 6. $\bot \lll \bot \wedge \top \lll \top$

A Galois connection always relates the two tops and bottoms, i.e. $\hat{\alpha}(\top) \sqsubseteq \top$ and $\hat{\alpha}(\bot) \sqsubseteq \bot$. Because $[\![\cdot]\!]$ preserves both tops and bottoms, it then follows that both $\hat{\alpha}([\![\top]\!]) \sqsubseteq [\![\top]\!]$, or $\top \lll \top$, and $\hat{\alpha}([\![\bot]\!]) \sqsubseteq [\![\bot]\!]$, or $\bot \lll \bot$, holds as well.

Lemma 7. $\hat{p} \lll \hat{q} \Rightarrow \forall s \in S : F(s)(\hat{p}) \lll G(s)(\hat{q})$

$$\begin{aligned} \hat{\gamma}([\![G(s)(\hat{q})]\!]) &= \hat{\gamma}([\![\hat{N}(\hat{\pi}_{\mathrm{a}}(s) \sqcap \hat{q})]\!]) && \text{(definition of } G) \\ &\sqsupseteq [\![\hat{M}(\hat{\gamma}(\hat{\pi}_{\mathrm{a}}(s) \sqcap \hat{q}))]\!] && \text{(simulation relation?)} \\ &= [\![\hat{M}(\hat{\gamma}(\hat{\pi}_{\mathrm{a}}(s)) \sqcap \hat{\gamma}(\hat{q}))]\!] && (\hat{\gamma} \text{ distributes over } \sqcap) \\ &\sqsupseteq [\![\hat{M}(\hat{\gamma}(\hat{\pi}_{\mathrm{a}}(s)) \sqcap \hat{p})]\!] && \text{(Galois connection?)} \\ &= [\![F(s)(\hat{p})]\!] && \text{(definition of } F) \end{aligned}$$

Lemma 8. $\forall s \in S : \Phi_*(s) \lll \Psi_*(s)$

Since $\Phi_*(s) = \lim \Phi_n(s)$ and $\Psi_*(s) = \lim \Psi_n(s)$, it suffices to prove that $\Phi_n(s) \lll \Psi_n(s)$ for all $s \in S$ and $n \in \mathbb{N}$. We do so by induction on n. The base case, where $\Phi_0(s) = \bot$ and $\Psi_0(s) = \bot$, follows from lemma 6. For the inductive step, assume that $\Phi_n(s) \lll \Psi_n(s)$ for all $s \in S$. For $s = s_0$, we have that $\Phi_{n+1}(s_0) = \top$ and $\Psi_{n+1}(s_0) = \top$, which also follows from lemma 6. For any $s \neq s_0$, we have:

$$
\begin{aligned}
\hat{\gamma}([\![\Psi_{n+1}(s)]\!]) &= \hat{\gamma}([\![\sqcup\{G(s')(\Psi_n(s')) \mid (s', s) \in R\}]\!]) && \text{(definition of } \Psi_{n+1} \text{ and } \mathcal{G}) \\
&= \hat{\gamma}(\sqcup\{[\![G(s')(\Psi_n(s'))]\!] \mid (s', s) \in R\}) && ([\![\cdot]\!] \text{ distributes over } \sqcup) \\
&\sqsupseteq \sqcup\{\hat{\gamma}([\![G(s')(\Psi_n(s'))]\!]) \mid (s', s) \in R\} && (\hat{\gamma} \text{ is monotone}) \\
&\sqsupseteq \sqcup\{[\![F(s')(\Phi_n(s')]\!] \mid (s', s) \in R\} && \text{(I.H and lemma 7)} \\
&= [\![\sqcup\{F(s')(\Phi_n(s') \mid (s', s) \in R\}]\!] && ([\![\cdot]\!] \text{ distributes over } \sqcup) \\
&= [\![\Phi_{n+1}(s)]\!] && \text{(definition of } \Phi_{n+1} \text{ and } \mathcal{F})
\end{aligned}
$$

Consider an arbitrary $s \in S$ and let $\hat{p} = \Phi_*(s) \sqcap \hat{\gamma}(\hat{\pi}_{\mathrm{a}}(s))$, where $\hat{p} \sqsubseteq \Phi_*(s)$ and $\hat{p} \sqsubseteq \hat{\gamma}(\hat{\pi}_{\mathrm{a}}(s))$, or $\hat{\alpha}(\hat{p}) \sqsubseteq \hat{\pi}_{\mathrm{a}}(s)$. Lemma 8 tells us $\Phi_*(s) \lll \Psi_*(s)$, and thus $\hat{\alpha}(\hat{p}) \sqsubseteq \hat{\alpha}([\![\hat{p}]\!]) \sqsubseteq \hat{\alpha}([\![\Phi_*(s)]\!]) \sqsubseteq [\![\Psi_*(s)]\!]$ by the monotonicity of $[\![\cdot]\!]$ and $\hat{\alpha}$. Using the invariance of $\hat{\pi}_{\mathrm{a}}(s)$ and property name of $[\![\cdot]\!]$, we note that the assumption can be restated as $\hat{\pi}_{\mathrm{c}}(s) \sqsupseteq \Psi_*(s) \sqcap \hat{\pi}_{\mathrm{a}}(s) = [\![\Psi_*(s) \sqcap \hat{\pi}_{\mathrm{a}}(s)]\!] = [\![\Psi_*(s)]\!] \sqcap \hat{\pi}_{\mathrm{a}}(s)$. It then follows that $\alpha(\hat{p}) \sqsubseteq \hat{\pi}_{\mathrm{c}}(s)$, or $\hat{p} \sqsubseteq \hat{\gamma}(\hat{\pi}_{\mathrm{c}}(s))$ as desired.

A.4 Proof of Theorem ??

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. Muchnick, S., et al.: Advanced compiler design implementation. Morgan kaufmann (1997)
3. 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)