Mining Correctness

Sigurd Schneider
sigurd@ps.uni-saarland.de

September 17, 2010

1 Setup

In full generality, a trace is a possibly infinite sequence of states, where each state is associated with a set of labels. In this setting, a trace is restricted to be a finite sequences of labels, capturing that event traces are always finite, and exactly one event happens at a time.

We consider LTL syntax as usual, but adopt the semantics to the restricted trace definition. Given a trace $\pi = l_0, ..., l_n$, we denote by π_i the sequence $l_i, ..., l_n$.

Definition 1. *(LTL Semantics) Let $\pi = l_0, ..., l_n$ be a trace. Then the satisfiability relation $\models$ is defined as follows:*

$$\begin{aligned} l_0, ..., l_n \models l &\iff l_0 = l \\ l_0, ..., l_n \models \Box t &\iff \forall i \in [0, n] : \pi_i \models t \\ l_0, ..., l_n \models \Diamond t &\iff \exists i \in [0, n] : \pi_i \models t \\ l_0, ..., l_n \models t_1 \,\mathsf{U}\, t_2 &\iff \exists i \in [0, n] : \pi_i \models t_2 \wedge \forall j \in [0, i-1] : \pi_j \models t_1 \end{aligned}$$

The propositional connectives $\wedge, \vee, \rightarrow, \neg$ are lifted as usual.

Definition 2. *The shorthands NFby, AFby, AP for LTL formulas are defined for all labels a, b as follows:*

$$\begin{aligned} \mathrm{a}\,\mathsf{NFby}\,\mathrm{b} &:= \Box(a \rightarrow \Box(\neg b)) \\ \mathrm{a}\,\mathsf{AFby}\,\mathrm{b} &:= \Box(a \rightarrow \Diamond b) \\ \mathrm{a}\,\mathsf{AP}\,\mathrm{b} &:= (\Diamond a) \rightarrow \neg b U a \end{aligned}$$

2 Assumptions

The implementation is not directly verified. Instead, the a set of assumptions is stated, from which the correctness follows. The implementation must be inspected and it must

be verified that these assumptions indeed hold for the implementation to apply the proof. The mining procedure `mine` yields a set of invariants for a set of traces.

Definition 3 (Assumptions)**.** *Let T be a set of traces. Then it is assumed that*

$$\begin{aligned}
\mathrm{a}\,\mathsf{NFby}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \forall i \in [0,n] : l_i = a \rightarrow \forall j \in [i,n] : l_j \neq b \\
\mathrm{a}\,\mathsf{AFby}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \forall i \in [0,n] : l_i = a \rightarrow \exists j \in [i,n] : l_j = b \\
\mathrm{a}\,\mathsf{AP}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \forall i \in [0,n] : l_i = b \rightarrow \exists j \in [0,i] : l_j = b
\end{aligned}$$

3 Correctness Proof

Correctness is soundness (every mined invariant holds), and completeness (all invariants that hold are mined). We establish these properties by prooving the following theorem.

Theorem 1 (Relative Correctness)**.** *Let T be a set of traces, and a, b be labels.*

$$\begin{aligned}
\mathrm{a}\,\mathsf{NFby}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{NFby}\,\mathrm{b} \\
\mathrm{a}\,\mathsf{AFby}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{AFby}\,\mathrm{b} \\
\mathrm{a}\,\mathsf{AP}\,\mathrm{b} \in \texttt{mine}(T) &\iff \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{AP}\,\mathrm{b}
\end{aligned}$$

Proof. To prove the first two statements, it suffices to expand the semantic definitions.

$$\begin{aligned}
& \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{NFby}\,\mathrm{b} && \\
\iff & \forall \pi \in T : \pi \models \Box(a \rightarrow \Box(\neg b)) && \text{Def. 2} \\
\iff & \forall \pi \in T : \forall i \in [0,n] : (\pi_i \models a) \rightarrow \forall j \in [i,n] : \pi_j \models \neg b && \text{Def. 1} \\
\iff & \forall \pi \in T : \forall i \in [0,n] : l_i = a \rightarrow \forall j \in [i,n] : l_j \neq b && \text{Def. 1} \\
\iff & \mathrm{a}\,\mathsf{NFby}\,\mathrm{b} \in \texttt{mine}(T) && \text{Def. 3}
\end{aligned}$$

$$\begin{aligned}
& \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{AFby}\,\mathrm{b} && \\
\iff & \forall \pi \in T : \pi \models \Box(a \rightarrow \Diamond b) && \text{Def. 2} \\
\iff & \forall \pi \in T : \forall i \in [0,n] : (\pi_i \models a) \rightarrow \exists j \in [i,n] : \pi_j \models b && \text{Def. 1} \\
\iff & \forall \pi \in T : \forall i \in [0,n] : l_i = a \rightarrow \exists j \in [i,n] : l_j = b && \text{Def. 1} \\
\iff & \mathrm{a}\,\mathsf{AFby}\,\mathrm{b} \in \texttt{mine}(T) && \text{Def. 3}
\end{aligned}$$

The third proof requires a lemma.

$$
\begin{aligned}
& \forall \pi \in T : \pi \models \mathrm{a}\,\mathsf{AP}\,\mathrm{b} \\
\iff & \forall \pi \in T : \pi \models (\Diamond b) \rightarrow (\neg b)\,\mathsf{U}\,a && \text{Def. 2} \\
\iff & \forall \pi \in T : (\exists i \in [0,n] : \pi_i \models b) \rightarrow \exists j \in [0,n] : \pi_j \models a \wedge \forall k \in [0,j-1] : \pi_k \models \neg b && \text{Def. 1} \\
\iff & \forall \pi \in T : (\exists i \in [0,n] : l_i = b) \rightarrow \exists j \in [0,n] : l_j = a \wedge \forall k \in [0,j-1] : l_k \neq b && \text{Def. 1} \\
\iff & \forall \pi \in T : (\forall i \in [0,n] : l_i \neq b) \vee (\exists j \in [0,n] : l_j = a \wedge \forall k \in [0,j-1] : l_k \neq b) && \text{Def. } \rightarrow \\
\iff & \forall \pi \in T : \forall i \in [0,n] : l_i = b \rightarrow \exists j \in [0,i] : l_j = a && \text{Lem. 1} \\
\iff & \mathrm{a}\,\mathsf{AFby}\,\mathrm{b} \in \mathtt{mine}(T) && \text{Def. 3}
\end{aligned}
$$

□

Lemma 1. *We proof that for all traces $\pi = l_0, ..., l_n$, and for all labels a, b, we have*

$$
\begin{aligned}
& (\forall i \in [0,n] : l_i \neq b) \vee (\exists j \in [0,n] : l_j = a \wedge \forall k \in [0,j-1] : l_k \neq b) \\
\iff & \forall i \in [0,n] : l_i = b \rightarrow \exists j \in [0,i] : l_j = a
\end{aligned}
$$

Proof. Each direction is proven separately.

⇒ The claim must follow from each of the disjuncts separately.

- Then $\forall i \in [0,n] : l_i \neq b$, and the claim is trivial.
- Then there is $j \in [0,n]$ such that $l_j = a \wedge \forall k \in [0,j-1] : l_k \neq b$. Let $i \in [0,n]$. The claim is proven by case analysis on i.
  - Case $i < j$. Then $\forall k \in [0,j-1] : l_k \neq b$ and the claim holds trivially.
  - Case $i \geq j$. Then the claim holds since $l_j = a$.

⇐ We either have that $\forall i \in [0,n] : l_i \neq b$, in which case the claim holds by assumption, or there is an $i \in [0,n]$ such that $l_i = b$, and we have to show the conjunction $\exists j \in [0,n] : l_j = a \wedge \forall k \in [0,j-1] : l_k \neq b$.

Using $l_i = b$, the assumption provides $\exists j \in [0,i] : l_j = a$, which implies the left conjunct that had to be shown. Now let j be the smallest number such that $l_j = a$. i.e. such that $\forall j' \in [0,j-1] : l_{j'} \neq a$. Consider the contra-positive of the assumption: $\forall i \in [0,n] : (\forall j \in [0,i] : l_j \neq a) \rightarrow l_i \neq b$. Since j is the smallest witness it follows that $\forall k \in [0,j-1] : l_k \neq b$, which is the right conjunct and thus completes the proof.

□