Model Checking: HTZ

Siddharth Bhat

Michelmas 2024

Contents

Chapter 1

Linear time properties

https://www.youtube.com/watch?v=rGDyab-T0eM&list=PLwabKnOFhE38C0o6z_bhlF_uOUlblDTjh&index=5

Definition 1 *An **Execution** is a possibly infinite sequence* $s_1 \xrightarrow{a_1} s_2 \xrightarrow{a_2} \dots$.

Definition 2 *A **Path** is a projection of an execution to the states. So a sequence of states* $s_1, s_2, \dots$.

Definition 3 *A **Trace** is a projection of the path to its set of atomic propositions. So a sequnce of labels* $L(s_1), L(s_2), \dots$.

For mathematical convenience, we rule out finite executions. One way to do this is to convert all halt states into infinite loops at the halt state.

1.0.1 Linear Time Properties

Definition 4 *A **Linear Time (LT) Property** over the atomic propositions AP is a language E of infinite words over an alphabet* $\Sigma \equiv 2^{AP}$. *That is,* $E \subseteq 2^{\mathsf{AP}^\omega}$.

For example, the **safety** of mutual exclusion is given by $\mathsf{Mutex} \equiv \{A_0 A_1 A_2 \cdots : \forall i, \neg(crit_1 \in A_i \wedge crit_2 \in A_i)\}$. Note that this contains seqeuences that need not be exhibited by the transition system.

For another example, the **liveness** of mutual exclusion contains all infinite words is given by a formula that says — if program 1 enters into the wait section $wait_1$ infinitely many times, then it enters the critical section $crit_1$ infinitely many times, as does program 2. Formally:

$$\exists^\infty i \in \mathbb{N}, wait_1 \in A_i \implies \exists^\infty i \in \mathbb{N}, crit_1 \in A_i$$
$$\exists^\infty i \in \mathbb{N}, wait_2 \in A_i \implies \exists^\infty i \in \mathbb{N}, crit_2 \in A_i$$

1.0.2 When does a transition system satisfy a linear time property?

A transition system $\mathcal{T}$ over atomic propositions AP satisfies a linear time property E iff all traces from the transtion system are contained in E.

$$\mathcal{T} \models E \equiv \mathsf{Traces}(\mathcal{T}) \subseteq E$$

1.0.3 Trace Inclusion

For two transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$, the the following are equivalent (TFAE):

1. $\mathsf{Traces}(\mathcal{T}_1) \subseteq \mathsf{Traces}(\mathcal{T}_2)$.
2. $\forall E, \mathcal{T}_2 \models E \implies T_1 \models E$.

The key idea is that since $\mathcal{T}_2$ has richer behaviours, if $\mathcal{T}_2$ obeys some behavioural constraint, then so does $\mathcal{T}_1$, if $\mathcal{T}_1$'s traces are a strict subset of $\mathcal{T}_2$. See that this tells us that LTL cannot talk about hyperproperties (properties quantifying over traces), since if we could do this, we could distinguish between the trace sets of $\mathcal{T}_1$ and $\mathcal{T}_2$. See that (2) implies (1) is easy to see by choosing $E \equiv \mathsf{Traces}(\mathcal{T}_2)$.

1.0.4 Classificaiton of LT properties

Safety Properties: Nothing bad will happen Liveness Properties: Something good will happen

1.0.5 Safety Properties

1. Mutual Exclusion
2. Deadlock Freedom
3. Every red is preceded by a yellow in a traffic light.

See that (1), (2) are properties that are local to a single state. While the third property relates two states together. So, (1), (2) are called **invariants**. Formally, invariants are given by **propositional formulae** over the atomic propositions.

Definition 5 *Let* E *be an LT property over AP. The* E *is said to be an* ***Invariant*** *if it can be characterized by a propositional formula* ϕ*. That is,* $E = \{A_0 A_1 \cdots \in 2^{AP^\omega} : \forall i, A_i \models \phi\}$

Chapter 2

Lecture 6: Liveness & Fairness

Definition 6 *E is a **Safety Property** iff for all words in $T \in E^c$, there is a finite bad prefix $A_0 \dots A_n$ such that* no extension *of this is in E. We write the set of bad prefixes for a safety property as $\mathsf{BadPrefix}(E) \subseteq A^+$*

Formally, we write:

$$T \models E \iff \mathsf{Traces}_{fin}(T) \cap \mathsf{BadPrefix}(E) = \emptyset$$

we write $\mathsf{BadPrefix}(E)$ to be the set of all finite words $A_1 \dots A_n \in A^+$ such that there is no extension which lives in E.

Definition 7 *A **minimal bad prefix** is a bad prefix that itself contains no proper bad prefix.*

Theorem 1 *Every invariant E defined by a propositional formula ϕ is a safety property.*

Proof. all finite words of the form $A_1 \dots A_n$ such that $A_n \not\models \phi$ is the bad prefix.

Definition 8 *The **prefix set** of an infinite word σ is the set of words $pref(A_1 A_2 \dots) \equiv \{A_1 \dots A_n : \forall n \geq 0\}$.*

Definition 9 *The **prefix set** of a property E is the union of the prefix closures of all the words in it. $pref(E) \equiv \bigcup_{\sigma \in E} pref(\sigma)$.*

Definition 10 *The **prefix closure** of a property E is:*

$$pref(E) \equiv \{\sigma \in (2^{AP})^\omega : pref(\sigma) \subseteq pref(E)\}$$

Theorem 2 *E is a safety property iff $\mathsf{BadPrefix}(E) \subseteq pref(E)$.*

Proof.

2.1 Safety Property as closed sets

Let $X \equiv 2^{AP}$, our space from where we pick up events in the trace. Define a metric on the space of infinite sequences X^ω. Given two executions $\vec{x}, \vec{y} \in X^\omega$, we measure their similarity in the smallest index they differ (Idea from the paper "LTL is Closed Under Topological Closure"). We define a metric with $d(\vec{x}, \vec{x}) \equiv 0$, and $d(\vec{x}, \vec{y}) = 2^{-i}$ if i is the smallest index such that $\vec{x}[i] \neq \vec{y}[i]$. (Think why this obeys transitive).

The distance between a trace $\vec{x}$ and a property $S \subseteq X^\omega$ is the infimum of the distances from every element in S: $d(x, S) \equiv \inf_{y \in S} d(x, y)$. Using this, we will show that safety properties correspond to closed sets, and liveness properties correspond to dense sets.

2.1.1 Safety Properties

Under this interpretation, a safety property is a closed set. Intuitively, we are stating that every limit point of S is in S. Written differently, we are saying that $\forall \vec{x} \in X, d(\vec{x}, S) = 0 \implies \vec{x} \in S$. (Compare this to the closed interval $[0, 1]$ versus the open $(0, 1)$). Alternatively, we can think in terms of limit points. S contains all its limit points. If we have a property $\vec{x}$, and we can write a sequence $\vec{s_1}, \vec{s_2}, \ldots$, where each $s_i \in S$, and $d(s_i, \vec{x}) < 2^i$, then since S is closed, we must have that $\lim_i \vec{s_i} = \vec{x} \in S$. From our safety interpretation, this means that s_1 and $\vec{x}$ can diverge at step 2, but this already tells us that $\vec{x}$ is safe upto 2 steps. Similarly, s_2 and $\vec{x}$ diverge at step 4, this tells us that $\vec{x}$ is safe upto 4 steps. Repeating this, we can see that $d(s_i, \vec{x}) < 2^i$ establishes that $\vec{x}$ is safe for 2^i steps, and thus it must be safe for all time.

2.1.2 Liveness Properties

Recall that a liveness property is that which can extend any finite trace. This can be seen as a *denseness* condition on the set, because intuitively, every trace is arbitrarily close to the liveness property. (Think of $\mathbb{Q} \in \mathbb{R}$). Intuitively, suppose we have a trace $\vec{x}$, and let L be a liveness property. Now, since every finite prefix $\vec{x}[:i] \in X^*$ must be extensible to a new property $\vec{l_i} \in X^\omega$ such that $\vec{x}[:i] = \vec{l}[:i]$ (i.e., $d(\vec{x}, \vec{l_i}) \leq 2^{-i}$), this implies that in fact, the sequence $\vec{l_1}, \vec{l_2}, \vec{l_3}, \ldots$ establishes that $\inf_i d(\vec{x}, \vec{l_i}) = 0$. Therefore, any property $\vec{x}$ is arbitrarily close to $\vec{L}$.

2.1.3 Decomposition Theorem

We prove in trace semantics that any property can be written as the intersection of a safety and liveness property. Is it true that any set of a metric space can be written as the intersection of a closed set and a dense set? Yes. For a given set S, let the closed set be its closure, $C_S \equiv \overline{S}$. See that C_S is an overapproximation, since it has added the limit points $C - S$. See that the set of limit points has empty interior, so its complement will be dense. We define the dense set $D_S \equiv X - (C - S)$, or $X - \texttt{extra}$.