On Designing A Safety Monitor For Autonomous Vehicles : A Case Study

Aaron Kane, Omar Chowdhury, Philip Koopman, and Anupam Datta

Carnegie Mellon University
{akane, omarc, koopman, danupam}@cmu.edu

Abstract. **Keywords:** autonomous vehicle safety, runtime monitoring, linear temporal logic

1 Introduction

2 Autonomous Vehicle Safety Specification Language ($\alpha\mathcal{VSL}$)

In this section, we introduce our safety specification language for autonomous vehicles, which we call $\alpha\mathcal{VSL}$ (short for, *autonomous vehicle safety specification language*). $\alpha\mathcal{VSL}$ is based on *propositional metric temporal logic* (MTL) [1]. The syntax of $\alpha\mathcal{VSL}$ is given below.

$\varphi ::= \mathtt{t} \mid p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{S}_{\mathbb{I}} \varphi_2 \mid \varphi_1 \mathcal{U}_{\mathbb{I}} \varphi_2 \mid \ominus_{\mathbb{I}} \varphi \mid \bigcirc_{\mathbb{I}} \varphi$

We denote safety policies written in $\alpha\mathcal{VSL}$ with φ, ϕ, and ψ (possibly with subscripts). We assume we are given a finite set of propositions, denoted by $\mathcal{P}$, propositions from which can be used to specify safety policies. Each proposition $p \in \mathcal{P}$ is a formula of $\alpha\mathcal{VSL}$. We have logical connectives $(\neg, \vee)$ and also have past $(\mathcal{S}, \ominus)$ and future $(\mathcal{U}, \bigcirc)$ temporal operators. Each temporal operator has an interval (denoted by $\mathbb{I}$) associated with it in which the formula is evaluated. The interval has the form $[lo, hi]$ where $lo, hi \in \mathbb{N}$ and $lo \leq hi$. The interval imposes an additional time interval constraint in which the immediate sub-formula must be true. For instance, $\varphi_1 \mathcal{S}_{[lo,hi]} \varphi_2$ is true represents that φ_2 was true within lo to hi time of the current time in the past and after that point on, φ_1 has been true. For past temporal operators, we allow the high end point of $\mathbb{I}$ to be ∞. However, we require our φ to be *future bounded*, *i.e.*, the high end point of $\mathbb{I}$ associated with all future temporal operators to be finite and bounded. This restriction is necessary for the termination of our safety monitoring algorithm. This will be made clear later.

Derived Operators. In our syntax, we present a minimal set of logical connectives and temporal operators. Other logical connectives and temporal operators can be derived using the following equivalences. (Logical false) $\mathtt{f} \equiv \neg\mathtt{t}$. (Conjunction) $\varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2)$. (Logical implication) $\varphi_1 \rightarrow \varphi_2 \equiv \neg\varphi_1 \vee \varphi_2$. (Logical equivalence) $\varphi_1 \leftrightarrow \varphi_2 \equiv (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$. (Past temporal operator "once") $\diamondsuit_{\mathbb{I}} \varphi \equiv (\mathtt{t} \mathcal{S}_{\mathbb{I}} \varphi)$. (Past temporal operator "historically")

$\boxminus_{\mathbb{I}}\varphi \equiv \neg\diamondsuit_{\mathbb{I}}\neg\varphi$. (Future temporal operator "eventually") $\diamondsuit_{\mathbb{I}}\varphi \equiv (\mathtt{t}\,\mathcal{U}_{\mathbb{I}}\varphi)$. (Future temporal operator "henceforth") $\square_{\mathbb{I}}\varphi \equiv \neg\diamondsuit_{\mathbb{I}}\neg\varphi$.

Semantics. $\alpha\mathcal{VSL}$ formulas are interpreted over time-stamped *traces*. A trace σ is a sequence of states, each of which maps all propositions in $\mathcal{P}$, to either $\mathtt{t}$ or $\mathtt{f}$. We denote the i^{th} position of the trace with σ_i where $i \in \mathbb{N}$. Moreover, each σ_i has an associated time stamp denoted by τ_i where $\tau_i \in \mathbb{N}$. We denote the sequence of time stamps with τ. For all $i, j \in \mathbb{N}$ such that $i < j$, we require $\tau_i < \tau_j$. For a given trace σ and time stamp sequence τ, we write $\sigma, \tau, i \models \varphi$ to denote that the formula φ is true with respect to the i^{th} position of σ and τ. We define $\sigma, \tau, i \models \varphi$ inductively in the following way.

- $\sigma, \tau, i \models \mathtt{t}$
- $\sigma, \tau, i \models p \iff \sigma_i(p) = \mathtt{t}$.
- $\sigma, \tau, i \models \neg\varphi \iff \sigma, \tau, i \not\models \varphi$.
- $\sigma, \tau, i \models \varphi_1 \vee \varphi_2 \iff \sigma, \tau, i \models \varphi_1$ or $\sigma, \tau, i \models \varphi_2$.
- $\sigma, \tau, i \models \varphi_1 \,\mathcal{S}_{[lo,hi]} \varphi_2 \iff$ there exists a $k \leq i$ such that $lo \leq \tau_i - \tau_k \leq hi$ and $\sigma, \tau, k \models \varphi_2$, and for all j such that $k < j \leq i$, $\sigma, \tau, j \models \varphi_1$ holds.
- $\sigma, \tau, i \models \varphi_1 \,\mathcal{U}_{[lo,hi]} \varphi_2 \iff$ there exists a $k \geq i$ such that $lo \leq \tau_k - \tau_i \leq hi$ and $\sigma, \tau, k \models \varphi_2$, and for all j such that $i \leq j < k$, $\sigma, \tau, j \models \varphi_1$ holds.
- $\sigma, \tau, i \models \ominus_{[lo,hi]} \varphi \iff i > 0$, $lo \leq (\tau_i - \tau_{i-1}) \leq hi$, and $\sigma, \tau, i-1 \models \varphi$.
- $\sigma, \tau, i \models \bigcirc_{[lo,hi]} \varphi \iff lo \leq (\tau_{i+1} - \tau_i) \leq hi$, and $\sigma, \tau, i+1 \models \varphi$.

3 Runtime Monitoring Algorithm

4 Implementation and Evaluation

5 Related Work

6 Conclusion

References

1. Koymans, R.: Specifying real-time properties with metric temporal logic. Real-Time Systems **2**(4) (1990) 255–299