Modeling and Verifying a Lego Car Using Hybrid I/O Automata

A. Fehnker, F.W. Vaandrager, M. Zhang

Nijmegen Institute for Computing and Information Sciences/

NIII-R0308 March 2003

Nijmegen Institute for Computing and Information Sciences
Faculty of Science
Catholic University of Nijmegen
Toernooiveld 1
6525 ED Nijmegen
The Netherlands

Modeling and Verifying a Lego Car Using Hybrid I/O Automata

Ansgar FEHNKER[1] Frits VAANDRAGER[2*]
Miaomiao ZHANG[2*]

[1] *Dept. of Electrical and Computer Engineering,*
5000 Forbes Ave., Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA
ansgar@ece.cmu.edu

[2] *Nijmeegs Instituut voor Informatica en Informatiekunde*
University of Nijmegen, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
fvaan@cs.kun.nl, miaomiao@cs.kun.nl

Abstract. We illustrate the application of the hybrid I/O automata framework of Lynch, Segala & Vaandrager by using it to model and analyze the behavior of a simple Lego car with caterpillar treads. We derive constraints on the values of the parameters that occur in our hybrid model that guarantee that the car will always move forward along a black tape, and will never get off the tape or move backward. In order to simplify the correctness proof, we introduce a transition systems that abstracts from the hybrid automaton in a rather drastic manner, but still preserves validity of the correctness properties in which we are interested. Even though our original model does not involve any disturbances, the general parametric analysis of the system allows us to exend our results in a trivial manner to a hybrid model in which several disturbances are allowed (mistakes in measurements of lengths, drift and jitter of the hardware clock, velocity, and distance between the two caterpillar treads).
AMS Subject Classification (1991): 68Q05, 68Q60, 93A25, 93C83.
CR Subject Classification (1991): D.2.4, F.1.1, F.3.1.
Keywords & Phrases: Hybrid Systems, Hybrid I/O Automata, Verification, Parametric Analysis.

1 Introduction

Recent years have seen a rapid growth of interest in *hybrid systems*—systems that intermix discrete and continuous behavior. Typical hybrid systems include computer components, which operate in discrete program steps, and real-world components, whose behavior over time intervals evolves according to physical constraints. Such systems are used in many application domains, including automated transportation, avionics, automotive control, robotics, process control, embedded devices, consumer electronics, and mobile computing. Hybrid systems can be very complex, and therefore very difficult to describe and reason about. At the same time, because they involve real-world activity, they often have stringent safety requirements. This combination of factors leads to a need for rigorous mathematical models for

*Research supported by PROGRESS project TES4199, Verification of Hard and Softly Timed Systems (HaaST) and EU IST project IST-2001-35304 Advanced Methods for Timed Systems (AMETIST). Author names are listed alphabetically; all three authors made an equally significant contribution to this paper.

describing hybrid systems and their properties, and for practical analysis methods based on these models.

In earlier work together with Nancy Lynch (MIT) and Roberto Segala (University of Verona), the second author developed a basic mathematical framework to support description and analysis of hybrid systems: the *Hybrid Input/Output Automaton (HIOA)* model [10]. In the present paper we illustrate the application of the HIOA framework by using it to model and analyze the behavior of a simple Lego car, displayed in Figure 1. Although this case

Figure 1: Lego car.

study literally is a "toy example", our mechanical model is rather simplistic, and of course there are no genuine safety requirements involved, we think the analysis is nontrivial and interesting. The case study illustrates in a simple setting several issues that arise in hybrid systems analysis, while in the end its complexity is comparable to that of of some real-world, safety-critical hybrid systems case studies that have been reported elsewhere in the literature [1, 2, 7, 8, 11].

The case we consider in this paper is taken from a setup that is used at the University of Nijmegen to illustrate the use and need of formal methods to students from secondary school and university. The setup, inspired by the well-known railroad crossing verification problem [4], consists of a train, a train gate and a car. There are sensors to detect an approaching train and to detect whether the train gates close properly. The train gate uses an infrared interface for communication with the train in case the gate fails. The car has two sensors, located between the front wheels, that allow it to follow a black tape, and one additional sensor, located at the top in front of the car, to detect the state of the traffic light at the train gates. Jeroen Kratz [6], who built the setup, verified the correctness of the controller of the train gate with the model checking tool UPPAAL. In this paper, we concentrate on the modeling and analysis of the car. Figure 2 gives a schematic view.

The car is equipped with a Lego RCX brick. This brick periodically executes a control program written in NQC, a C like language especially designed for the RCX platform. When the car is put on the black tape and switched on, it moves forward as long as both sensors detect the black tape. If a sensor detects the white underground, then the control program tells the opposite caterpillar tread to move backward. Thus, if the left sensor senses white and the right sensor senses black, the result is that the car turns to the right and the central position of the car remains unchanged. Similarly, if the right sensor detects the white underground, the direction of the left caterpillar tread is reversed. If both sensors detect the white underground then the car moves backward. If the orientation of the car is almost perpendicular to the direction of the tape then it may start bumping back and forth between different sides of the tape, and as a result even change the direction in which it moves.

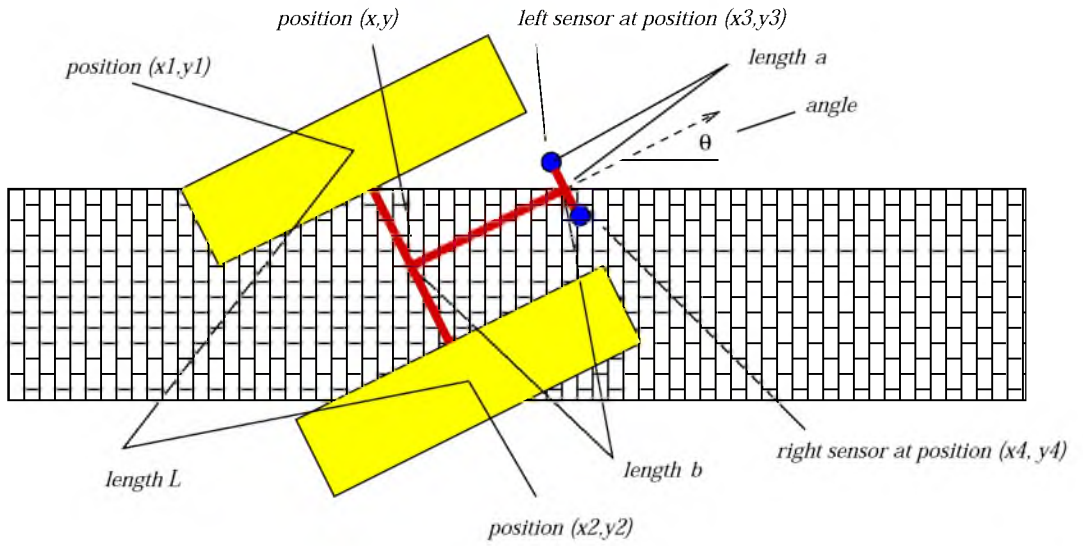

Figure 2: Schematic view of the Lego car.

The verification challenge proposed by Ansgar Fehnker [3] is to establish under which assumptions on the initial orientation of the car it will always move in a forward direction, i.e., the two caterpillar treads are never in backward mode simultaneously. Fehnker modeled the behavior of the car as a hybrid automaton, and using a (self written) tool that over approximates the set of reachable states based on bounded polyhedra, he was able to verify the following properties for specific values of the parameters measured on the physical car: if initially the car moves forward with an angle between -45 and 45 degrees then:

1. the car always stays on the tape and never moves backward,
2. the right sensor gets never closer to the upper boundary of the tape than 2.1 mm,
3. if the car is in forward mode the car moves in the direction of the x-axis with at least 8.9 cm/s (speed of car is 13 cm/s).

Experiments with the physical car confirm these results. In the present paper, we improve on the results of [3] in three ways: (1) our model is compositional: instead of a single automaton, we use a network of interacting hybrid I/O automata to model the car; (2) rather than verifying the correctness of the car for a single, specific choice of parameter values, we derive (by hand) general constraints on the parameters which ensure correctness; (3) our analysis also deals with various disturbances (clock drift and jitter, variations of car speed, inaccuracies in measurements on physical car).

In order to simplify the correctness proof, we introduce a transition systems $\mathcal{A}$ that abstracts from the hybrid automaton in a rather drastic manner, but still preserves validity of the correctness properties in which we are interested. Even though our original model does not involve any disturbances, our general parametric analysis of the system allows us to exend our results in a trivial manner to a hybrid model in which several disturbances are allowed (mistakes in measurements of lengths, drift and jitter of the hardware clock, velocity, and distance between the two caterpillar treads). The use of abstractions in system verification is of course very common. The way in which we handle disturbances appears to be new, and will hopefully be applicable to other examples as well.

The rest of this paper is structured as follows. In Section 2, we model the Lego car as a composition of six hybrid automata: the chassis, the two caterpillar treads, the two sensors,

and the RCX brick. Section 3 presents the abstract transition system model of the Lego car, and relates this model to the hybrid model of Section 2. Section 4 presents the correctness properties that we want to prove, the constraints needed for their validity, as well as the correctness proofs. A generalization of our results to a setting with disturbances is discussed in Section 5. Finally, Section 6 presents some directions for future work.

Although this paper heavily relies on the theory of hybrid I/O automata as developed in [10], it should be readable without detailed knowledge of this theory. Only readers who want to understand all the fine points about our model and correctness proofs (What are the precise requirements on trajectories of a hybrid automaton? How exactly are composition and hiding operations defined? Why does theory of [10] imply that the model contains no time deadlocks? Etc) will need to study [10] first.

2 Hybrid Automaton Model

We model the Lego car as a network of hybrid automata. The overall architecture of our model is displayed in Figure 3. There are six components, which communicate through shared variables. In accordance with Figure 2, variables $x1, y1$ and $x2, y2$ give the position of the left resp. right caterpillar thread. Variables $\theta 1$ and $\theta 2$ give the orientation of the caterpillar threads. Variables $x3, y3$ and $x4, y4$ indicate the position of the left resp. right sensor. Variables $sensor1$ and $sensor2$ are used to communicate sensor values from the sensors to the RCX, and variables $control1$ and $control2$ for sending control signals from the RCX to the electric motors that drive the caterpillar threads.

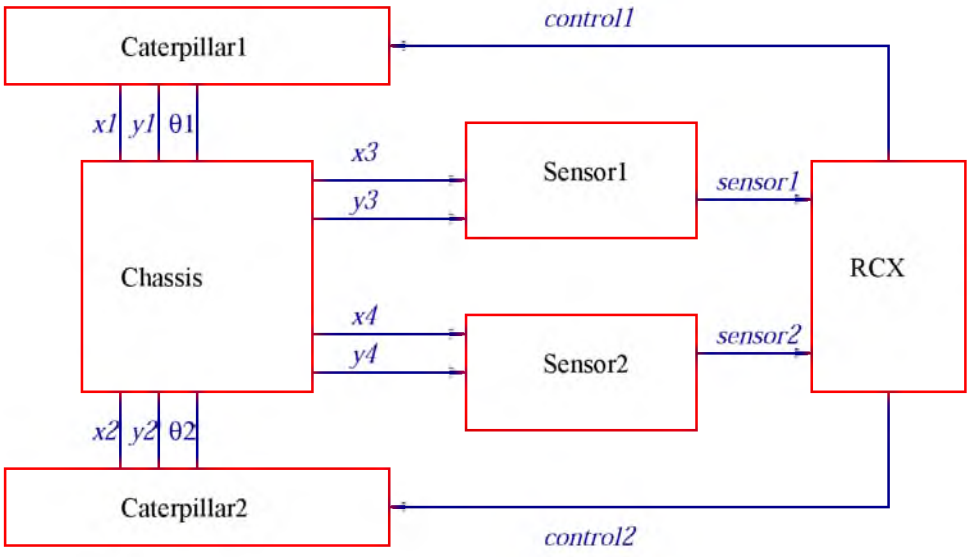

Figure 3: Network of hybrid automata for Lego car.

The following positive real-valued parameters play a role in our model:

- L: the distance between the two caterpillar treads,
- V: the speed of the car when in forward mode,
- a: half the distance between the two sensors,
- b: the distance between the center of the car and the line connecting both sensors,
- t_{sample}: the sampling time,

- α: we assume the initial orientation of the car is in the interval $[-\alpha, \alpha]$; with $\alpha < \frac{\pi}{2}$.
- B: the tape stretches, parallel to the x-axis, between upper bound B and lower bound $-B$.

For the physical car displayed in Figure 1, these parameters take the following values: $L = 10.3\text{cm}$, $V = 13\text{cm/s}$, $a = 0.8\text{cm}$, $b = 2.2\text{cm}$, $t_{sample} = 0.1\text{s}$, $2B = 2.5\text{cm}$. In [3], α was set to $\frac{\pi}{4}$.

2.1 Chassis

The main function of the chassis is to keep the various parts of the car fixed relative to each other. Correspondingly, our HA model of the chassis specifies, via a number of algebraic equations, the positions of the attached components relative to the position and orientation of the chassis itself. Hybrid automaton Chassis has no actions nor discrete transitions. The HA Chassis has a number of variables, all with type real and as dynamic type the set of piecewise differentiable functions. State variables x and y give the position of the center of the car, and state variable θ specifies the orientation of the car relative to the x-axis. Let PLS and PRS be abbreviations for the y-coordinates of the left and right sensor, respectively:

$$PLS \equiv y + b\sin\theta + a\cos\theta \tag{1}$$
$$PRS \equiv y + b\sin\theta - a\cos\theta \tag{2}$$

The initial states consists of those valuations of x, y and θ such that the center of the car and the two sensors are all on the tape, and the initial angle is in the interval $[-\alpha, \alpha]$:

$$\theta \in [-\alpha, \alpha] \wedge y \in [-B, B] \wedge PLS \in [-B, B] \wedge PRS \in [-B, B] \tag{3}$$

External variables $x1, y1$ give the position of the left caterpillar tread, and $\theta 1$ specifies its orientation. Similarly, external variables $x2, y2$ give the position of the right caterpillar tread, and $\theta 2$ specifies its orientation. External variables $x3, y3$ specify the position of the left sensor, and external variables $x4, y4$ specify the position of the right sensor. In accordance with the scheme of Figure 2, we obtain the following algebraic equations, which are required to hold in each state of each trajectory:

$$\theta 1 = \theta 2 = \theta \tag{4}$$
$$x1 = x - \frac{1}{2}L\sin\theta \tag{5}$$
$$y1 = y + \frac{1}{2}L\cos\theta \tag{6}$$
$$x2 = x + \frac{1}{2}L\sin\theta \tag{7}$$
$$y2 = y - \frac{1}{2}L\cos\theta \tag{8}$$
$$x3 = x + b\cos\theta - a\sin\theta \tag{9}$$
$$y3 = y + b\sin\theta + a\cos\theta \tag{10}$$
$$x4 = x + b\cos\theta + a\sin\theta \tag{11}$$
$$y4 = y + b\sin\theta - a\cos\theta \tag{12}$$

2.2 Caterpillar Treads

We describe the hybrid automaton Caterpillar1, which models the behavior of the left caterpillar tread. The definition of hybrid automaton Caterpillar2, modeling the right caterpillar

tread, is symmetric and not given here. Caterpillar1 has external variables $x1$, $y1$ and $\theta 1$, with type real and as dynamic type the set of piecewise differentiable functions. Variables $x1$ and $y1$ give the position of the center of the left caterpillar tread, and $\theta 1$ gives the orientation. In addition, the HA has a Boolean discrete external variable $control1$: the control signal which determines whether the caterpillar tread moves forward or backward. Since the HA has no internal variables, the set of states is a singleton, equal to the set of initial states. The HA also has no actions nor discrete transitions; it only allows trajectories that satisfy, in each state, the following differential equations:

$$\dot{x1} = \textbf{if } control1 \textbf{ then } V\cos\theta 1 \textbf{ else } -V\cos\theta 1 \tag{13}$$

$$\dot{y1} = \textbf{if } control1 \textbf{ then } V\sin\theta 1 \textbf{ else } -V\sin\theta 1 \tag{14}$$

2.3 Sensors

We describe the hybrid automaton Sensor1, which models the behavior of the left sensor. The definition of hybrid automaton Sensor2, modeling the right sensor, is symmetric and not given here. Sensor1 has external variables $x3$ and $y3$, with type real and as dynamic type the set of piecewise differentiable functions, which give the position of the sensor. In addition, the HA has a discrete external variable $sensor1$, with enumerated type $\{black, white\}$, via which the sensed value is communicated to the RCX. Again, since the HA has no internal variables, the set of states is a singleton, equal to the set of initial states, and there are no actions nor discrete transitions. The HA only allows trajectories that satisfy, in each state, the following algebraic equation:

$$sensor1 = \textbf{if } y3 \in [-B, B] \textbf{ then } black \textbf{ else } white \tag{15}$$

2.4 The RCX

The RCX brick periodically samples the values provided by both sensors, and based on the sampled values it may decide to change the control signals for the caterpillar treads (or, more precisely, for the motors that make them move). The behavior of the brick is modeled by a hybrid automaton RCX. This HA has a real-valued internal clock variable c to measure the time that has elapsed since the last sampling. The dynamic type of c is the set of piecewise differentiable functions. In addition, RCX has internal discrete variables $s1$, $s2$, $sample1$ and $sample2$, with enumerated type $\{black, white\}$, used to record the sensor values, resp. the latest values sampled from the two sensors. The set of states consists of all valuations of the variables c, $s1$, $s2$, $sample1$ and $sample2$ with $c \leq t_{sample}$. The set of initial states consists of all states satisfying

$$c = 0 \ \wedge \ sample1 = sample2 = black \tag{16}$$

The RCX automaton has two discrete external variables $sensor1$ and $sensor2$, with enumerated type $\{black, white\}$, by which it gets values from the sensors. In addition, it has two discrete external Boolean variables $control1$ and $control2$, used for communication with the caterpillar treads. The HA has just one internal action $tick$. The $tick$ labeled discrete transitions are defined by the following predicate:

$$c \geq t_{sample} \wedge c' = 0 \wedge sample1' = s1 \wedge sample2' = s2 \tag{17}$$

For trajectories we require that

$$sample1 \text{ and } sample2 \text{ remain constant throughout} \tag{18}$$

for each state on a trajectory except the first one

$$s1 = sensor1 \wedge s2 = sensor2 \tag{19}$$

and moreover the following equations hold everywhere:

$$\begin{aligned} \dot{c} &= 1 && (20)\\ control1 &= \textbf{if } sample2 = black \textbf{ then } true \textbf{ else } false && (21)\\ control2 &= \textbf{if } sample1 = black \textbf{ then } true \textbf{ else } false && (22) \end{aligned}$$

2.5 The Composed System

The components Chassis, Caterpillar1 and Caterpillar2 cannot be viewed as hybrid I/O automata. Variable $x1$, for instance is neither an output of Chassis nor an output of Caterpillar1: its value is determined by the interaction of the (differential) equations of the components. However, after hiding external variables $x1$, $y1$, $\theta 1$, $x2$, $y2$, $\theta 2$, the composition of the three automata is a hybrid I/O automaton, if we view $control1$ and $control2$ as inputs, and $x3$, $y3$, $x4$, $y4$ as outputs:

$$\mathsf{Plant} = \mathsf{VarHide}(\{x1, y1, \theta 1, x2, y2, \theta 2\}, (\mathsf{Chassis}\|\mathsf{Caterpillar1}\|\mathsf{Caterpillar2}\|)) \tag{23}$$

The Sensor1 component can easily be viewed as an HIOA by taking $x3$ and $y3$ as inputs, and $sensor1$ as output. Similarly, Sensor2 can be viewed as an HIOA by taking $x4$ and $y4$ as inputs, and $sensor2$ as output. Also RCX can be viewed as an HIOA: inputs are $sensor1$ and $sensor2$, and outputs are $control1$ and $control2$.

The complete system that we wish to analyze is obtained by composing all the HIOAs in parallel, and hiding the external variables:

$$\begin{aligned} \mathcal{H} = \mathsf{VarHide}(&\{x3, y3, x4, y4, sensor1, sensor2, control1, control2\},\\ &(\mathsf{Plant}\|\mathsf{Sensor1}\|\mathsf{Sensor2}\|\mathsf{RCX})) \end{aligned} \tag{24}$$

As pointed out in [10], the composition of HIOAs need not be an HIOA. However, since the HIOA RCX is *oblivious* (the time at which the output changes does not depend on the inputs), it follows straightforwardly from the theory of [10] that indeed $\mathcal{H}$ is an HIOA. In addition, the theory of [10] implies that since all components of $\mathcal{H}$ are trivially *receptive* (and their composition is a HIOA), also the composition is receptive. This means in particular that from each reachable state of $\mathcal{H}$ there exists an execution in which time diverges.

2.6 Simplifying the Plant Description

By adding equations (5) and (7), resp. (6) and (8), and then taking the derivatives, we obtain that in each state along a trajectory of Chassis||Caterpillar1||Caterpillar2:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \dot{x1} + \dot{x2} \\ \dot{y1} + \dot{y2} \end{pmatrix} \tag{25}$$

Similarly, by subtracting equations (5) and (7), resp. (6) and (8), using (4), and then taking derivatives, we obtain:

$$\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}\dot{\theta} = \frac{1}{L}\begin{pmatrix} \dot{x2} - \dot{x1} \\ \dot{y2} - \dot{y1} \end{pmatrix} \tag{26}$$

Combining identities (25) and (26) with equations (13) and (14) for $\dot{x1}$ and $\dot{y1}$ (as well as the corresponding equations for $\dot{x2}$ and $\dot{y2}$), allows us to identify four different cases. Depending on the values of *control1* and *control2*, the car moves with velocity V forward in direction θ (implication (27)), rotates clockwise with angular velocity $\frac{2V}{L}$ (implication (28)), rotates counterclockwise with angular velocity $\frac{2V}{L}$ (implication (29)), or moves backward with velocity V in direction $\theta + \pi$ (implication (30)):

$$control1 \wedge control2 \;\Rightarrow\; \dot{x} = V\cos\theta \wedge \dot{y} = V\sin\theta \wedge \dot{\theta} = 0 \tag{27}$$

$$control1 \wedge \neg control2 \;\Rightarrow\; \dot{x} = 0 \wedge \dot{y} = 0 \wedge \dot{\theta} = \frac{-2V}{L} \tag{28}$$

$$\neg control1 \wedge control2 \;\Rightarrow\; \dot{x} = 0 \wedge \dot{y} = 0 \wedge \dot{\theta} = \frac{2V}{L} \tag{29}$$

$$\neg control1 \wedge \neg control2 \;\Rightarrow\; \dot{x} = -V\cos\theta \wedge \dot{y} = -V\sin\theta \wedge \dot{\theta} = 0 \tag{30}$$

If the car rotates then the number of revolutions per time unit is $\omega = \frac{V}{\pi L}$. By covering one of the sensors with black tape and then placing the car on a white underground, we measured that the car can make a full turn in 2.5s (so $\omega = (2.5\text{s})^{-1}$). Since we also measured $V = 13\text{cm/s}$ and $L = 10.3\text{cm}$, the prediction from our model agrees with reality ($\frac{\pi 10.3}{13} \approx 2.5$).

3 An Abstract Model

We want to find constraints on the parameters that ensure that for all reachable states of HIOA $\mathcal{H}$:

$$sample1 = black \vee sample2 = black \tag{31}$$

If it would be possible to reach a state in which *sample1* and *sample2* both equal *white* then we would have a situation where both signals *control1* and *control2* are *false*, and consequently both caterpillar treads move backward, which is what we want to rule out. In addition, the parameter constrains should ensure that infinitely often the car gets into forward mode. In temporal logic notation:

$$\Box\Diamond(c = 0 \wedge sample1 = black \wedge sample2 = black) \tag{32}$$

In order to find the desired constraints, we define an abstraction of the HIOA $\mathcal{H}$. There are three key ideas which justify this abstraction:

- Since the values of *sample1* and *sample2* do not change along a trajectory (18), it suffices to prove that assertion (31) holds initially and immediately following any discrete transition of $\mathcal{H}$. Therefore, in our abstraction, we only consider those states of $\mathcal{H}$ in which the clock variable c has value 0. Hence we can omit variable c in the abstraction.

- In this paper we assume that the tape is straight without bends, and runs parallel to the x-axis. As a consequence, the sensor values (and thus the control) are independent of value of variable x. We can therefore omit variable x in the abstraction.

- In order to establish that assertion (31) holds for all reachable state of $\mathcal{H}$ it suffices to prove that at least one sensor is on the tape in any reachable state in which the clock variable c has value 0:

$$c = 0 \;\Rightarrow\; PLS \in [-B, B] \vee PRS \in [-B, B] \tag{33}$$

  This observation allows us to omit variables *s1*, *s2*, *sample1* and *sample2* in the abstraction.

The abstraction of $\mathcal{H}$ that we consider is a transition system $\mathcal{A}$ with as states all valuations of two real valued variables y and θ, as initial states all valuations that satisfy formula (3), the initial state predicate of Chassis, and a transition relation defined in terms of the disjunction φ_{step} of four transition formulas, where each formula corresponds to one of the four control modes of the car:

$$\varphi_{step} \triangleq \varphi_{forward} \vee \varphi_{back} \vee \varphi_{left} \vee \varphi_{right} \tag{34}$$

$$\begin{aligned} \varphi_{forward} \triangleq\ & PLS \in [-B, B] \wedge PRS \in [-B, B] \\ & \wedge y' = y + V \sin(\theta) t_{sample} \\ & \wedge \theta' = \theta \end{aligned} \tag{35}$$

$$\begin{aligned} \varphi_{back} \triangleq\ & PLS \notin [-B, B] \wedge PRS \notin [-B, B] \\ & \wedge y' = y - V \sin(\theta) t_{sample} \\ & \wedge \theta' = \theta \end{aligned} \tag{36}$$

$$\begin{aligned} \varphi_{left} \triangleq\ & PLS \in [-B, B] \wedge PRS \notin [-B, B] \\ & \wedge y' = y \\ & \wedge \theta' = \theta + \frac{2V}{L} t_{sample} \end{aligned} \tag{37}$$

$$\begin{aligned} \varphi_{right} \triangleq\ & PLS \notin [-B, B] \wedge PRS \in [-B, B] \\ & \wedge y' = y \\ & \wedge \theta' = \theta - \frac{2V}{L} t_{sample} \end{aligned} \tag{38}$$

The theorem below relates hybrid I/O automaton $\mathcal{H}$ to the abstraction $\mathcal{A}$ via a *bisimulation relation* [12] between the states of the two automata. In the proof, we use the following global invariant of $\mathcal{H}$:

Lemma 3.1. *In all reachable states of* $\mathcal{H}$

$$c = 0 \Rightarrow [(sample1 = black \Leftrightarrow PLS \in [-B, B]) \wedge (sample2 = black \Leftrightarrow PRS \in [-B, B])]$$

Theorem 3.2. *Let* R *be the relation between reachable states of* $\mathcal{H}$ *and states of* $\mathcal{A}$ *given by:*

$$c_{\mathcal{H}} = 0 \ \wedge\ \theta_{\mathcal{H}} = \theta_{\mathcal{A}} \ \wedge\ y_{\mathcal{H}} = y_{\mathcal{A}}$$

For states s *and* s' *of* $\mathcal{H}$*, write* $s \rightsquigarrow s'$ *if there exists an execution fragment leading from* s *to* s' *that consists of a trajectory followed by a single discrete transition. For states* u *and* u' *of* $\mathcal{A}$*, write* $u \rightarrow u'$ *if there exists a transition from* u *to* u' *according to the transition predicate* φ_{step} *of* $\mathcal{A}$*. Then* R *is a bisimulation between* $\mathcal{H}$ *and* $\mathcal{A}$ *in the sense that:*

1. *Each initial state of* $\mathcal{H}$ *is related to an initial state of* $\mathcal{A}$*, and vice versa.*
2. *If* $(s, u) \in R$ *and* $s \rightsquigarrow s'$ *then there exists a state* u' *of* $\mathcal{A}$ *such that* $u \rightarrow u'$ *and* $(s', u') \in R$*.*
3. *If* $(s, u) \in R$ *and* $u \rightarrow u'$ *then there exists a state* s' *of* $\mathcal{H}$ *such that* $s \rightsquigarrow s'$ *and* $(s', u') \in R$*.*

4 Correctness

4.1 The Desired Properties

In this section we derive constraints which ensure that, starting from the initial state, the car always remains on the tape, either one of its sensors is on the tape, and its direction remains within the interval $[-\alpha, \alpha]$. More specifically, we prove that

$$\varphi_{safe} \triangleq \theta \in [-\alpha, \alpha] \wedge y \in [-B, B] \wedge (PLS \in [-B, B] \vee PRS \in [-B, B]) \tag{39}$$

is an invariant of $\mathcal{A}$, assuming certain constraints on the parameters.

In addition we want to ensure that transition $\varphi_{forward}$ will be taken infinitely often during the course of an infinite run of the system. For this it is sufficient to show that the following temporal logic formula, which expresses that during each execution infinitely often both sensors are on the tape, holds in $\mathcal{A}$:

$$\varphi_{live} \triangleq \Box\Diamond(PLS \in [-B, B] \wedge PRS \in [-B, B]) \tag{40}$$

The next lemma allows us to transfer our results from $\mathcal{A}$ to $\mathcal{H}$:

Lemma 4.1. *If φ_{safe} is an invariant of $\mathcal{A}$ and formula φ_{live} holds for $\mathcal{A}$, then assertion (31) is an invariant of $\mathcal{H}$ and liveness assertion (32) holds for $\mathcal{H}$.*

Proof. Use Lemma 3.2, Theorem 3.1 and (18). □

4.2 Parameter Constraints

Below we give the constraints on the parameters, and show by counterexamples that they are necessary to prove that φ_{safe} is preserved by the transitions of $\mathcal{A}$, and φ_{live} holds for $\mathcal{A}$. In the next subsection we will establish that the proposed constraints are also sufficient for correctness. The parameter constraints are:

$$\begin{aligned}
\varphi_1 &\triangleq a\cos(\alpha) + b\sin(\alpha) \geq V\sin(\alpha)t_{sample} \\
\varphi_2 &\triangleq 2a\cos(\alpha) \geq V\sin(\alpha)t_{sample} \\
\varphi_3 &\triangleq \frac{2V}{L}t_{sample} + \arctan(\frac{a}{b}) \leq \alpha \\
\varphi_4 &\triangleq a\cos(\frac{V}{L}t_{sample}) + b\sin(\frac{V}{L}t_{sample}) \leq B
\end{aligned}$$

Before explaining these constraints, we first give two simple technical lemma's:

Lemma 4.2. $\varphi_1 \Leftrightarrow \forall 0 \leq \beta \leq \alpha : a\cos(\beta) + b\sin(\beta) \geq V\sin(\beta)t_{sample}$.

Proof. Implication "$\Leftarrow$" is trivial, so we concentrate on implication "$\Rightarrow$". Assume that φ_1 holds. For all $0 \leq \beta \leq \alpha$:

$$\begin{aligned}
& a\cos(\beta) + b\sin(\beta) \geq V\sin(\beta)t_{sample} \\
\Leftrightarrow\ & a + b\tan\beta \geq V\tan(\beta)t_{sample} \\
\Leftrightarrow\ & a \geq (Vt_{sample} - b)\tan\beta
\end{aligned}$$

Observe that $\tan\beta \geq 0$. There are two cases. If $Vt_{sample} \leq b$ then the inequality $a \geq (Vt_{sample} - b)\tan\beta$ trivially holds and we are done. Otherwise, if $Vt_{sample} > b$, we use that $\tan$ is monotonic on $[0, \frac{\pi}{2})$ to derive:

$$a \geq (Vt_{sample} - b)\tan\alpha \geq (Vt_{sample} - b)\tan\beta$$

which again gives the desired inequality. □

Lemma 4.3. $\varphi_2 \Leftrightarrow \forall 0 \leq \beta \leq \alpha : 2a\cos(\beta) \geq V\sin(\beta)t_{sample}$.

Proof. Similar to the proof of Lemma 4.2. □

We will now try to give some intuitions why we need constraints $\varphi_1, \ldots, \varphi_4$.

Constraint φ_1 is needed to maintain $y \in [-B, B]$ when moving forward. Suppose that the system is in a state satisfying φ_{safe}, the left sensor is just on the tape ($PLS = B$), the right sensor is also on the tape, and $\theta > 0$. This scenario is illustrated in Figure 4. We then

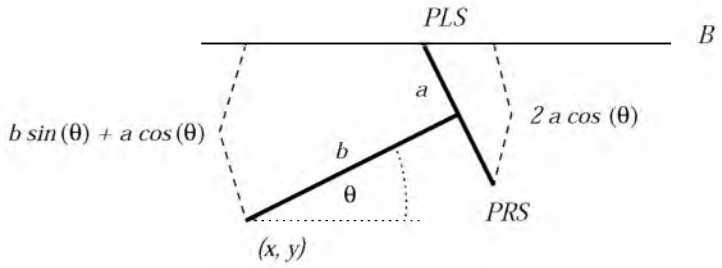

Figure 4: Illustration of the need for φ_1 and φ_2.

have that the distance from the central position to B is $a\cos(\theta) + b\sin(\theta)$. Since both sensors are on the the tape, the vehicle will move forward and during the next sampling interval the value of y will be incremented by $V\sin(\theta)t_{sample}$. If the distance $a\cos(\theta) + b\sin(\theta)$ is less than $V\sin(\theta)t_{sample}$, the center of the car will be off the tape after transition $\varphi_{forward}$, and the invariant property is violated.

Constraint φ_2 is needed to guarantee that at least one sensor remains on tape when moving forward. To illustrate this, we use the same scenario that we used for φ_1, see Figure 4. Since both sensors are assumed to be on the tape the car will move forward. If $2a\cos(\theta) < V\sin(\theta)t_{sample}$, then the position of the right sensor PRS will be above B after one sampling interval.

Constraint φ_3 is needed to keep the angle θ in the interval $[-\alpha, \alpha]$. Suppose that the system is in a state where the center of the car is right at the bottom of the tape ($y = -B$), the right sensor is just below the bottom of the tape ($PRS = -B - \epsilon$, for some small $\epsilon > 0$), and the left sensor is on the tape. The scenario is illustrated in Figure 5. In this scenario, θ is

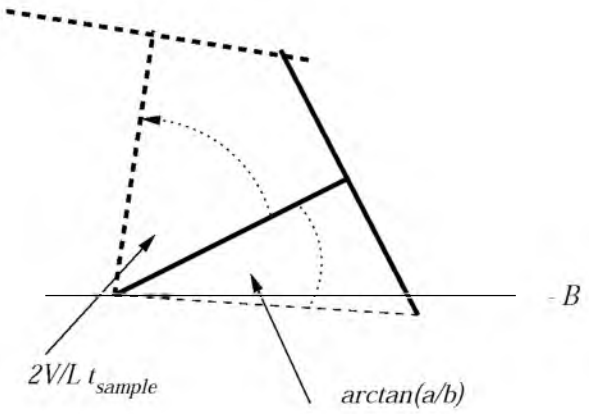

Figure 5: Illustration of the need for φ_3.

almost $\arctan(\frac{a}{b})$. Suppose that φ_3 does not hold and $\frac{2V}{L}t_{sample} + \arctan(\frac{a}{b}) > \alpha$. Since the left sensor is on the tape but the right sensor is not, the vehicle will turn left. Transition φ_{left} will then lead to an angle $\theta' = \theta + \frac{2V}{L}t_{sample} > \alpha$, which violates φ_{safe}.

Constraint φ_4 is needed to avoid infinite repetition between transitions φ_{right} and φ_{left}. Suppose that the center of the car is in the middle of the tape ($y = 0$), the angle θ equals

$\frac{V}{L}t_{sample}$, the right sensor is on the tape, and constraint φ_4 does not hold, i.e., $a\cos(\frac{V}{L}t_{sample})+b\sin(\frac{V}{L}t_{sample}) > B$. This scenario is illustrated in Figure 6. It follows from the inequality

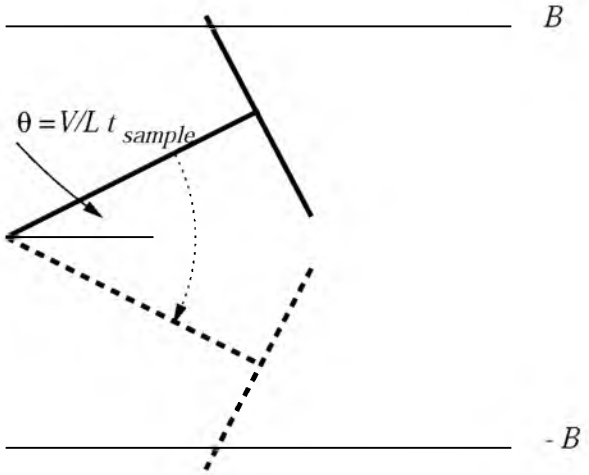

Figure 6: Illustration of the need for φ_4.

that the left sensor must be above the tape. The car will then take a φ_{right} transition, and θ' will be equal to $-\frac{V}{L}t_{sample}$. The new state is symmetric to the old one, but now $PRS = y - a\cos(\frac{V}{L}t_{sample}) - b\sin(\frac{V}{L}t_{sample})$, which is smaller than $-B$ by assumption. The next transition the car will take is φ_{left}, which will bring it back in its prior position, etc. This shows that if φ_4 does not hold there may be an infinite alternating sequence of φ_{right} and φ_{left} steps. This violates property φ_{live}.

4.3 Correctness Proof

The main technical result of this paper is that the four parameter constraints $\varphi_1, \ldots, \varphi_4$ are in fact sufficient to ensure invariance of φ_{safe}. In order to prove this, we need the following simple, trigonometric lemma.

Lemma 4.4.

1. $b\sin\beta + a\cos\beta = \sqrt{a^2+b^2}\,\sin(\beta + \arctan(\frac{a}{b}))$
2. $b\sin\beta - a\cos\beta = \sqrt{a^2+b^2}\,\sin(\beta - \arctan(\frac{a}{b}))$

Proof.

$$\begin{aligned} b\sin\beta + a\cos\beta &= \sqrt{a^2+b^2}\,(\frac{b}{\sqrt{a^2+b^2}}\sin\beta + \frac{a}{\sqrt{a^2+b^2}}\cos\beta) \\ &= \sqrt{a^2+b^2}\,(\cos(\arctan(\frac{a}{b}))\sin\beta + \sin(\arctan(\frac{a}{b}))\cos\beta) \\ &\quad (\text{use } \sin(\gamma+\delta) = \sin\gamma\cos\delta + \cos\gamma\sin\delta) \\ &= \sqrt{a^2+b^2}\,\sin(\beta + \arctan(\frac{a}{b})) \end{aligned}$$

The proof of (2) is similar and uses $\sin(\gamma - \delta) = \sin\gamma\cos\delta - \cos\gamma\sin\delta$. □

Theorem 4.5. *Assume that parameter constraints $\varphi_1, \ldots, \varphi_4$ hold. Then φ_{safe} is a stable property of $\mathcal{A}$, i.e., $\varphi_{safe} \wedge \varphi_{step} \Rightarrow \varphi'_{safe}$.*

Proof. It suffices to establish the following four implications:

1. $\varphi_{safe} \wedge \varphi_{forward} \Rightarrow \varphi'_{safe}$
2. $\varphi_{safe} \wedge \varphi_{back} \Rightarrow \varphi'_{safe}$
3. $\varphi_{safe} \wedge \varphi_{left} \Rightarrow \varphi'_{safe}$
4. $\varphi_{safe} \wedge \varphi_{right} \Rightarrow \varphi'_{safe}$

Ad 1 Assume $\varphi_{safe} \wedge \varphi_{forward}$.
Since $\theta \in [-\alpha, \alpha]$ and $\theta' = \theta$, trivially $\theta' \in [-\alpha, \alpha]$.
Assume without loss of generality that $\theta \geq 0$ (case $\theta \leq 0$ symmetric). Then

$$\begin{aligned} y' &= y + V\sin(\theta)t_{sample} \\ &\geq y \geq -B \\ y' &= y + V\sin(\theta)t_{sample} \quad \text{(use Lemma 4.2)} \\ &\leq y + a\cos\theta + b\sin\theta \\ &= PLS \leq B \end{aligned}$$

Hence $y' \in [-B, B]$.
Under the assumption $\theta \geq 0$ we now prove $PRS' \in [-B, B]$. (If $\theta \leq 0$ we prove $PLS' \in [-B, B]$ via a symmetric argument.)

$$\begin{aligned} PRS' &= y' + b\sin\theta' - a\cos\theta' \\ &= y + V\sin(\theta)t_{sample} + b\sin\theta - a\cos\theta \quad \text{(use Lemma 4.3)} \\ &\leq y + b\sin\theta + a\cos\theta \\ &= PLS \leq B \\ PRS' &= y + V\sin(\theta)t_{sample} + b\sin\theta - a\cos\theta \\ &\geq y + b\sin\theta - a\cos\theta \\ &= PRS \geq -B \end{aligned}$$

We conclude that φ'_{safe} holds.

Ad 2 This implication trivially holds since the left hand side is equivalent to false.

Ad 3 Assume $\varphi_{safe} \wedge \varphi_{left}$. Then in the state before the transition the left sensor is on the tape and the right sensor is off the tape. In fact, since

$$PRS = y + b\sin\theta - a\cos\theta \leq y + b\sin\theta + a\cos\theta = PLS \leq B,$$

we know that the right sensor is below the tape, i.e., $PRS < -B$. We use this fact to infer

$$b\sin\theta - a\cos\theta = PRS - y < -B - y \leq -B + B = 0$$

which in turn implies

$$\theta < \arctan(\frac{a}{b}) \tag{41}$$

We now prove φ'_{safe}.

$$\begin{aligned}
\theta' &= \theta + \frac{2V}{L} t_{sample} > \theta \geq -\alpha \\
\theta' &= \theta + \frac{2V}{L} t_{sample} \qquad \text{(use constraint } \varphi_3\text{)} \\
&\leq \theta + \alpha - \arctan(\frac{a}{b}) \qquad \text{(by (41)} \\
&< \alpha
\end{aligned}$$

Hence $\theta' \in [-\alpha, \alpha]$.

Since $y \in [-B, B]$ and $y' = y$, trivially $y' \in [-B, B]$.

Using Lemma 4.4 we infer

$$\begin{aligned}
PLS' &= y' + \sqrt{a^2 + b^2} \sin(\theta' + \arctan(\frac{a}{b})) \\
&= y + \sqrt{a^2 + b^2} \sin(\theta + \frac{2V}{L} t_{sample} + \arctan(\frac{a}{b}))
\end{aligned}$$

Let $\beta = \theta + \frac{2V}{L} t_{sample} + \arctan(\frac{a}{b})$. By φ_3 and since $\alpha < \frac{\pi}{2}$, $\beta < \pi$. If $\beta \geq 0$ then $PLS' \geq y \geq -B$. Otherwise, since $\theta \geq -\alpha$,

$$\begin{aligned}
PLS' &> y + \sqrt{a^2 + b^2} \sin(\theta + \arctan(\frac{a}{b})) \\
&= PLS \geq -B
\end{aligned}$$

Hence, independently of the value of β, $PLS' \geq -B$. Next we infer $PLS' \leq B$:

$$\begin{aligned}
PLS' &= y + \sqrt{a^2 + b^2} \sin(\theta + \frac{2V}{L} t_{sample} + \arctan(\frac{a}{b})) \quad \text{(use } PRS < -B\text{)} \\
&< -B + \sqrt{a^2 + b^2} \left[\sin(\theta + \frac{2V}{L} t_{sample} + \arctan(\frac{a}{b})) - \sin(\theta - \arctan(\frac{a}{b}))\right] \\
&\qquad \text{(use } \sin\gamma - \sin\delta = 2\sin\frac{1}{2}(\gamma - \delta)\ \cos\frac{1}{2}(\gamma + \delta)\text{)} \\
&= -B + 2\sqrt{a^2 + b^2} \sin(\frac{V}{L} t_{sample} + \arctan(\frac{a}{b}))\ \cos(\frac{V}{L} t_{sample} + \theta) \\
&\qquad \text{(by } \varphi_3 \text{ it follows that } 0 < \frac{V}{L} t_{sample} + \arctan(\frac{a}{b}) \leq \alpha < \frac{\pi}{2}\text{)} \\
&\leq -B + 2\sqrt{a^2 + b^2} \sin(\frac{V}{L} t_{sample} + \arctan(\frac{a}{b})) \\
&\qquad \text{(use } \varphi_4 \text{ rewritten according to Lemma 4.4)} \\
&\leq -B + 2B = B
\end{aligned}$$

We conclude that $PLS' \in [-B, B]$, and hence φ'_{safe} holds.

Ad 4 Analogous to the previous case. □

Corollary 4.6. *Assume that parameter constraints $\varphi_1, \ldots, \varphi_4$ hold. Then φ_{safe} is an invariant of $\mathcal{A}$, i.e., φ_{safe} holds in all reachable states of $\mathcal{A}$.*

Proof. Immediate from Theorem 4.5 and the fact that φ_{safe} is implied by the initial condition of $\mathcal{A}$. □

Theorem 4.7. *Assume that parameter constraints $\varphi_1, \ldots, \varphi_4$ hold. Then φ_{live} holds for $\mathcal{A}$.*

Proof. By the above corollary, φ_{safe} holds in all reachable states of $\mathcal{A}$. This implies that no execution of $\mathcal{A}$ will contain a φ_{back} step. The proof of Theorem 4.5 shows that if a φ_{left} transition is taken, the left sensor will be on the tape in the target state, and the right sensor will be on the tape or still below it. Hence from the target state the system will either take another φ_{left} transition or a $\varphi_{forward}$ transition. Since each φ_{left} transition increases angle θ with $\frac{2V}{L}t_{sample}$, we only may have a finite number of consecutive φ_{left} transitions so that eventually we must reach a state in which both sensors are on the tape. By a symmetric argument we may infer that each φ_{right} transition will be either followed by another φ_{right} transition or by a $\varphi_{forward}$ transition. Also, we may only have a finite number of consecutive φ_{right} transitions. As a result, each infinite execution will contain infinitely many $\varphi_{forward}$ transitions. □

5 Adding Disturbances

Using Lemma 4.4, we can sligthly simplify constraints $\varphi_1, \ldots, \varphi_4$ and rewrite them in the following form:

$$\begin{aligned}
\psi_1 &\triangleq a \geq (Vt_{sample} - b)\tan\alpha \\
\psi_2 &\triangleq 2a \geq Vt_{sample}\tan\alpha \\
\psi_3 &\triangleq \frac{2Vt_{sample}}{L} + \arctan(\frac{a}{b}) \leq \alpha \\
\psi_4 &\triangleq \sqrt{a^2+b^2}\sin(\frac{Vt_{sample}}{L} + \arctan(\frac{a}{b})) \leq B
\end{aligned}$$

One can easily check that all four constraints hold for the specific values of the parameters measured on the physical car that were given at the beginning of Section 2. In fact, we can even slightly increase the maximal initial angle α to 0.88 radians (approximately 50 degrees).

More interesting is to see what are the maximal allowable tolerances on the parameter values. Suppose that we pick the value for a from an interval $[a_{\min}, a_{\max}]$, b from $[b_{\min}, b_{\max}]$, t_{sample} from $[t_{\min}, t_{\max}]$, V from $[V_{\min}, V_{\max}]$, L from $[L_{\min}, L_{\max}]$, α from $[\alpha_{\min}, \alpha_{\max}]$ and B from $[B_{\min}, B_{\max}]$. Then, in order to ensure that the parameter constraints hold, the following inequalities should be satisfied:

$$\begin{aligned}
&a_{\min} \geq (V_{\max}t_{\max} - b_{\min})\tan\alpha_{\max} \\
&2a_{\min} \geq V_{\max}t_{\max}\tan\alpha_{\max} \\
&\frac{2V_{\max}t_{\max}}{L_{\min}} + \arctan(\frac{a_{\max}}{b_{\min}}) \leq \alpha_{\min} \\
&\sqrt{a_{\max}^2 + b_{\max}^2}\sin(\frac{V_{\max}t_{\max}}{L_{\min}} + \arctan(\frac{a_{\max}}{b_{\min}})) \leq B_{\min}
\end{aligned}$$

Since $t_{\min}$, $V_{\min}$, $L_{\max}$ and $B_{\max}$ do not occur in these constraints, it follows that in any parameter valuation which satisfies the parameter constraints we can (1) decrease the values of t_{sample} and V, and (2) increase the values of L and B, all with an arbitrary amount, without violating the constraints. For instance, the parameter constraints hold for any (positive)

parameter valuation satisfying

$$\begin{aligned} a &\in [0.75, 0.85] \\ b &\in [2.15, 2.25] \\ t_{sample} &\leq 0.11 \\ V &\leq 13.5 \\ L &\geq 10.2 \\ \alpha &= \frac{\pi}{4} \\ B &\geq 1.25 \end{aligned}$$

It is not possible to increase the size of the intervals much more since this will lead to violation of the second constraint.

In the case of some parameters, such as a and b, we may not be sure about their exact value due to measurement inaccuracies, but their value will not change significantly during operation of the car. For other parameters, such as V and t_{sample}, we do not know their exact values but in addition these values may change during operation (car slows down since batteries are almost dead; drift and jitter of hardware clock, etc.). Interestingly, we can use the verification results that we obtained in the previous section for a model in which the values of the parameters are fixed, to establish correctness for a variation of the model in which disturbances are allowed.

Theorem 4.5, specialized to the parameter intervals given above, states that:

$$\forall a \in [a_{\min}, a_{\max}], b \in [b_{\min}, b_{\max}], \alpha \in [\alpha_{\min}, \alpha_{\max}], B \geq B_{\min} :$$

$$\forall t_{sample} \leq t_{\max} \forall V \leq V_{\max} \forall L \geq L_{\min} : \varphi_{safe} \wedge \varphi_{step} \Rightarrow \varphi'_{safe}$$

As t_{sample}, V and L do not occur (free) in assertion φ_{safe}, we can apply the laws of predicate logic to rewrite this formula to:

$$\forall a \in [a_{\min}, a_{\max}], b \in [b_{\min}, b_{\max}], \alpha \in [\alpha_{\min}, \alpha_{\max}], B \geq B_{\min} : \varphi_{safe} \wedge \psi_{step} \Rightarrow \varphi'_{safe}$$

where

$$\psi_{step} \triangleq \exists t_{sample} \leq t_{\max} \exists V \leq V_{\max} \exists L \geq L_{\min} : \varphi_{step}$$

The predicate ψ_{step} corresponds to the transition relation of a variant of transition system $\mathcal{A}$ where each time before taking a transition we may choose new values of t_{sample}, V and L satisfying the specified inequalities. The resulting transition system $\mathcal{A}'$ can be viewed as an abstraction of a variant $\mathcal{H}'$ of $\mathcal{H}$ in which

- the lower bound constraint $c \geq t_{sample}$ in the predicate for the $tick$ transition (17) is replaced by $c > 0$ and t_{sample} is set to $t_{\max}$.
- rather than parameters, V and L are taken to be internal variables of the HIOA Plant. Within trajectories, V and L may behave as arbitrary continuous functions satisfying $V \leq V_{\max}$ resp. $L \geq L_{\min}$.

It is routine to prove variations of Lemma 3.1 and Theorem 3.2 in which $\mathcal{H}$ and $\mathcal{A}$ have been replaced by $\mathcal{H}'$ and $\mathcal{A}'$, respectively. Hence, our correctness results extend to a setting in which we allow disturbances to alter the values of t_{sample}, V and L.

6 Future Work

Even though our model appears to be rather accurate, it can of course still be made more realistic in several ways. For instance:

1. We only consider the case in which the tape is straight and has a uniform width. What happens to our constraints when the tape may be curved?
2. We do not allow for disturbances to modify the values of parameters a, b and B.
3. In the real car the positions of the two sensors are not exactly symmetric: the left sensor is slightly further away from the center of the car than the right sensor.
4. The car has two motors, one for each of the caterpillar treads. As a result, one caterpillar tread may move slightly faster than the other one. To model the resulting dynamics will be considerably more complex than the simple case which we consider in this paper.
5. The sensors will not be perfect: especially when they get very close to the the edge of the tape, the sensed value need not be correct.

The parameter constraints that we derive in this paper are sufficient for correctness, but not necessary. In fact, we believe that it will be possible to further relax the parameter constraints, especially if one is willing to strengthen the initial condition (for instance, by requiring that the distance between the center of the car and the tape edge is at least a).

In experiments with the Lego car we observed that even when the initial angle of the car is close to α (or $-\alpha$), after hitting the tape edge once, the absolute value of the angle always gets very small and subsequently remains very small, i.e., the car almost moves in the direction of the tape. We can use our analysis results to explain this phenomenon. In Theorem 4.5, we establish that if parameter constraints $\varphi_1, \ldots, \varphi_4$ hold, this implies that

$$\varphi_{safe} \stackrel{\Delta}{=} \theta \in [-\alpha, \alpha] \wedge y \in [-B, B] \wedge (PLS \in [-B, B] \vee PRS \in [-B, B])$$

is a stable property, i.e., if the property holds and we take a transitions then the property will also hold in the target state. Now suppose that at some point during a run of the car φ_{safe} holds and $\theta \in [-\beta, \beta]$ for some $\beta < \alpha$. Now if the parameter constraints still hold if we assign to α the value β, stability of φ_{safe} implies that θ will *always* remain in the interval $[-\beta, \beta]$. As a result of this mechanism, θ will after some time typically be contained in an interval $[-\alpha_{\min}, \alpha_{\min}]$, where $\alpha_{\min}$ is the smallest value for α for which the parameter constraints still hold (given the values of the other parameters). For the values of the parameters that we measured on the Lego car, $\alpha_{\min}$ is 0.60 radians (appr. 34 degrees). We expect that further analysis of our model may give rise to an even smaller value for $\alpha_{\min}$.

Finally, we think it will be interesting to investigate whether our use of abstractions and our way to handle disturbances can also be applied in other examples.

References

[1] E. Dolginova and N.A. Lynch. Safety verification for automated platoon maneuvers: A case study. In O. Maler, editor, *Proceedings International Workshop on Hybrid and Real-Time Systems (HART'97)*, Grenoble, France, volume 1201 of *Lecture Notes in Computer Science*, pages 154–170. Springer-Verlag, March 1997.

[2] A. Fehnker. Automotive control revisited — linear inequalities as approximation of reachable sets. In Henzinger and Sastry [5], pages 110–125.

[3] Ansgar Fehnker. *Citius, Vilius, Melius: Guiding and Cost-Optimality in Model Checking of Timed and Hybrid Systems.* PhD thesis, University of Nijmegen, April 2002.

[4] C. Heitmeyer and N.A. Lynch. The generalized railroad crossing — a case study in formal verification of real-time systems. In *Proceedings 15th IEEE Real-Time Systems Symposium,* San Juan, Puerto Rico, pages 120–131, December 1994.

[5] T.A. Henzinger and S. Sastry, editors. *Proceedings First International Workshop on Hybrid Systems: Computation and Control (HSCC'98),* Berkeley, California, volume 1386 of *Lecture Notes in Computer Science.* Springer-Verlag, April 1998.

[6] Jeroen Kratz. *A case study in PLC control: two ways of verifying PLC control software for a LEGO plant.* Master thesis, Department of Computing Science, University of Nijmegen, November 1999.

[7] J. Lygeros and N.A. Lynch. On the formal verification of the TCAS conflict resolution algorithms. In *Proceedings 36th IEEE Conference on Decision and Control,* San Diego, CA, pages 1829–1834, December 1997. Extended abstract.

[8] J. Lygeros and N.A. Lynch. Strings of vehicles: Modeling and safety conditions. In Henzinger and Sastry [5], pages 273–288.

[9] N.A. Lynch, R. Segala, and F.W. Vaandrager. Hybrid I/O automata revisited. In M.D. Di Benedetto and A.L. Sangiovanni-Vincentelli, editors, *Proceedings Fourth International Workshop on Hybrid Systems: Computation and Control (HSCC'01),* Rome, Italy, volume 2034 of *Lecture Notes in Computer Science,* pages 403–417. Springer-Verlag, March 2001.

[10] N.A. Lynch, R. Segala, and F.W. Vaandrager. Hybrid I/O automata. *Information and Computation,* 2003. To appear. Available as Technical Report MIT-LCS-TR-827d, MIT Laboratory for Computer Science, Cambridge, MA 02139, January 13, 2003. A preliminary version appeared as [9].

[11] Sayan Mitra, Yong Wang, Nancy Lynch, and Eric Feron. Safety verification of model helicopter controller using hybrid input/output automata. In *Hybrid Systems: Computation and Control (HSCC'03),* Prague, the Czech Republic, pages 259–273. Lecture Notes in Computer Science, Springer-Verlag, 2003.

[12] D.M.R. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, 5^{th} *GI Conference,* volume 104 of *Lecture Notes in Computer Science,* pages 167–183. Springer-Verlag, 1981.