Applications of MetiTarski in the Verification of Control and Hybrid Systems

Behzad Akbarpour[1] and Lawrence C. Paulson[2]

[1] Concordia University, Montreal, Quebec, H3G 1M8, Canada
behzad@ece.concordia.ca
[2] Computer Laboratory, University of Cambridge, England
lp15@cam.ac.uk

Abstract. MetiTarski, an automatic proof procedure for inequalities on elementary functions, can be used to verify control and hybrid systems. We perform a stability analysis of control systems using Nichols plots, presenting an inverted pendulum and a magnetic disk drive reader system. Given a hybrid systems specified by a system of differential equations, we use Maple to obtain a problem involving the exponential and trigonometric functions, which MetiTarski can prove automatically.

1 Introduction

Most research into the verification of hybrid systems involves model checking and constraint solving. In this paper, we present preliminary results involving the use of automated theorem proving. Our approach delivers proofs of its claims, which can be checked by other tools or even examined by humans. These proofs are low-level and can be very long; for example, the proof of the collision avoidance problem (see Sect. 4.1) consists of nearly 2600 text lines and 162 logical inferences, some of which refer to decision procedures. Formal verification is typically used in applications that demand high assurance. Our methodology can produce documentation of every phase of the formal analysis of the design, from differential equations to proof.

MetiTarski [1–3] is a new automatic theorem prover for special functions over the real numbers. It consists of a resolution theorem prover (Metis) combined with a decision procedure (QEPCAD) for the theory of real closed fields. It can prove logical statements involving the functions ln, exp, sin, cos, arctan, sqrt, etc. We have applied it to hundreds of problems mainly of mathematical origin. In this paper, we report recent experiments in which we have applied MetiTarski to standard benchmark problems about hybrid and control systems.

Our workflow typically involves using a computer algebra system (Maple) to solve a differential equation. The result is a formula over the real numbers, which we supply to MetiTarski. For most problems that we have investigated, MetiTarski returns a proof in seconds. The entry of problems is currently manual, though it is not difficult, because the output of Maple can be pasted into MetiTarski, with modest further editing to put the problem into the right form. These tasks are routine and could be automated.

Paper outline. Section (§2) reviews some related work. Section (§3) describes the verification of control systems. Section (§4) describes the details of our approach for the verification of hybrid systems using illustrative case studies. Section (§5) concludes the paper and provides hints for future work directions.

2 Related Work

Control systems are traditionally analysed using numerical techniques, often involving the visual inspection of plots for a number of sample inputs and different values of parameters. Then we must assume that the results of this analysis also hold for any values of the input and the parameters. This assumption can lead to incorrect conclusions. Hardy [10] proposed a formal and symbolic technique to increase the reliability of the results, removing the possibility of erroneous results due to plotting errors and uncertain parameters. She examined the underlying mathematical representation of a particular form of control system requirements: Nichols plot requirements. These requirements were reduced to their most basic form and a decision procedure was developed for use in the analysis which can be used to decide the positivity or negativity of finitely inflective functions. The resulting tool, called Nichols plot Requirements Verifier (NRV), was developed in the Maple-PVS-QEPCAD system which exploits the symbolic computation provided by the computer algebra system Maple, the formal techniques provided by the theorem prover PVS and the quantifier elimination routines provided by QEPCAD. Hardy presented two case studies to demonstrate the practical application of the NRV system. In this paper, we achieve similar results by replacing the PVS-QEPCAD combination with MetiTarski. We still use Maple for initial calculations but we replace the semi-automatic proofs by PVS with fully automatic proofs of MetiTarski.

Several techniques for model checking of hybrid systems have been proposed. The most widely investigated is bounded model checking (BMC), which computes a set of reachable states that corresponds to an over-approximation of the solution of the system equations obtained for a bounded period of time. This approach provides the algorithmic foundations for the tools that are available for computer-aided verification of hybrid systems such as Checkmate [6], d/dt [5], PHaver [9], and HyTech [11]. On the other hand, there are some hybrid system verification tools such as Stefan Ratschan's HSolver [14], which are based on constraint solving techniques. The basic idea is to decompose the state space into hyperboxes according to a rectangular grid and then use interval constraint-propagation techniques to check the flow on the boundary between neighboring grid elements. This is done via an abstraction refinement framework in order to achieve precise results.

In this paper, we present a novel approach based on automatic theorem proving for hybrid system verification. We show how our tool MetiTarski assisted with Maple can be used to prove safety properties about hybrid systems. We have selected a set of case studies in real world applications collected from standard benchmarks [15] for evaluating and comparing tools for hybrid system design

and verification. Our current examples are restricted to linear systems for which we can solve the systems of ordinary differential equations (ODE) using methods like the Laplace transform to find the closed form solutions based on elementary functions. We have been able to prove safety properties of the systems such as Room Heating and Navigation, which cannot be verified by HSolver.[3] We are planning to extend our case studies to cover nonlinear cases by finding methods of solving systems of polynomial nonlinear ordinary differential equations analytically in terms of elementary and special functions. An example of such method is the Prelle-Singer procedure [12], extensions of which are also implemented in computer algebra systems such as REDUCE (the PSODE package [13]) and Maple (the PSsolver package [8]).

3 Control Systems Verification

This section presents our methodology for using MetiTarski in the verification of control systems. Our approach can be briefly described as follows. We start from the open loop transfer function of the feedback control system in Laplace domain as a function of s (G (s)). Then we replace s with jw and switch to frequency domain. Then we calculate the gain and phase shift of $G(jw)$ according to Equation 1, as real valued functions over w, and plot them in the x/y plane and call it the Nichols plot. For stability, the Nichols plot of the system should lie outside an exclusion region which will be explained later. We describe this obligation as inequalities on special functions such as arctan and log over w, and prove them using MetiTarski. We use Maple to plot the Nichols plots, and also for some preliminary investigations about the intermediate expressions.

We illustrate our methodology using two moderately sized case studies, both based on examples that appear regularly in control engineering texts. In Section 3.2, an inverted pendulum system is analysed. The stability criteria are specified in terms of three intervals in which the Nichols plot of the system must not enter a given bounded region on the graph. We use MetiTarski to verify this system. We then alter the system and use MetiTarski to show that the system is now unstable. In both cases, the Nichols plot for the system lies too close to the exclusion region to be confirmed by visual inspection. In Section 3.3, a disk drive reader system is analysed with respect to stability. This system has an 'uncertain' parameter, whose value is known to lie within an interval. This type of problem is difficult to analyse using classical Nichols plot techniques as it is a three dimensional rather than two dimensional problem. The classical solution is to plot a suite of Nichols plots showing the system response for various values of the parameter. If the system meets its requirements in all of these plots the assumption is made that the system meets its requirements for all permissible values of the parameter. In this case study we provide symbolic analysis of the system for all permissible values of the parameter, generating a formal proof.

[3] See http://hsolver.sourceforge.net/benchmarks/

3.1 Nichols Plot Requirements

There are three main graphical analysis techniques used in the analysis of control systems in frequency or the complex plane: the Nyquist plot (complex plane), Bode diagrams (frequency domain), and Nichols plots (frequency domain). We will discuss in particular analysis using Nichols plots. The *Nichols plot* [7] (also known as *Nichols chart*) plots the gain (in decibels) against the phase-shift of the output sinusoid as the frequency varies. The gain and phase-shift of a system with transfer function G can be calculated explicitly using the following formulas:

$$\begin{aligned} y &= \text{gain} = 20\log_{10}(|G(jw)|) \\ x &= \text{phase-shift} = \text{argument}(G(jw)) \\ &= \begin{cases} \arctan(\frac{\Im(G(jw))}{\Re(G(jw))}) + k\pi & \text{if } \Re(G(jw)) \neq 0 \\ \frac{\pi}{2} + k\pi & \text{if } \Re(G(jw)) = 0 \end{cases} \end{aligned} \tag{1}$$

where $\Re$ ($\Im$) denotes the real (imaginary) part of a complex number, and k is an integer. When using arctan to calculate the value of phase-shift, we may have to adjust the range of arctan, which normally is restricted to $(-\frac{\pi}{2}, \frac{\pi}{2})$ in radians. If the shift in phase at w is greater than $\frac{\pi}{2}$ then $\arctan(\frac{\Im(G(jw))}{\Re(G(jw))})$ must be adjusted by an appropriate multiple k of π to give the phase-shift as in equation 1.

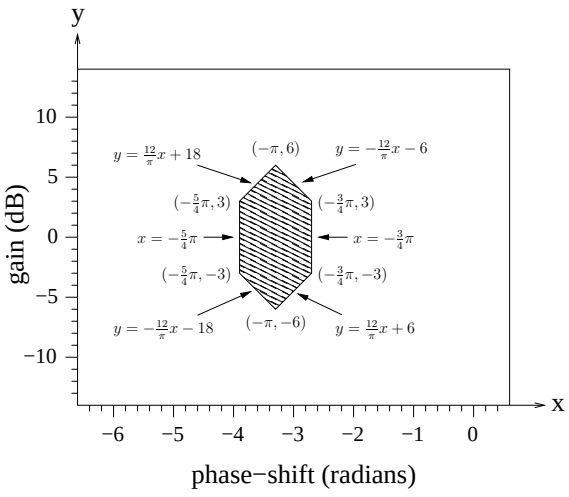

Fig. 1. Exclusion Region

Nichols plots often show *exclusion regions* that must be avoided to achieve stability and performance. In general, a system is considered stable if its Nichols plot does not enter a certain hexagonal region about the point $(-\pi, 0)$ as shown in Fig. 1. This requirement can be expressed in terms of the lines bounding the region in three intervals.

1. The Nichols plot for the system must lie below the line $y = -\frac{12}{\pi}x - 18$ between the points $(-\frac{5}{4}\pi, -3)$ and $(-\pi, -6)$, or above the line $(y = \frac{12}{\pi}x + 18)$ between the points $(-\frac{5}{4}\pi, 3)$ and $(-\pi, 6)$.
2. It must lie below the line $y = -\frac{12}{\pi}x - 6$ between the points $(-\pi, -6)$ and $(-\frac{3}{4}\pi, -3)$, or above the line $y = \frac{12}{\pi}x + 6$ between $(-\pi, 6)$ and $(-\frac{3}{4}\pi, 3)$.
3. It must lie to the left of line $x = -\frac{5}{4}\pi$ between the points $(-\frac{5}{4}\pi, -3)$ and $(-\frac{5}{4}\pi, 3)$, or to the right of line $x = \frac{-3}{4}\pi$ between $(-\frac{3}{4}\pi, -3)$ and $(-\frac{3}{4}\pi, 3)$.

These conditions can be expressed as inequalities in arctan, ln, and square root.

Several different cases of curves can be identified depending on whether $y = f(x)$ is monotonic decreasing, or monotonic increasing and concave, or monotonic increasing and convex. These properties help to reduce the proofs to specific points instead of a whole range. A real-valued function f defined on an interval is *convex* if for any two points x and y in its domain and any t in $[0, 1]$, we have

$$f(tx + (1-t)y) \leq tf(x) + (1-t)f(y).$$

A function f is said to be *concave* if $-f$ is convex. A twice differentiable function of one variable is convex on an interval if and only if its second derivative is non-negative there; this gives a practical test for convexity. A *point of inflection* is a point on a curve at which the curvature changes sign; at this point, the graph of the function makes a smooth transition between convexity and strict concavity. These conditions can be easily checked using Maple.

3.2 Inverted Pendulum

This section focuses on the modeling and analysis of an inverted pendulum system. An *inverted pendulum* is a pendulum that has its mass above its pivot point, which is mounted on a cart that can move horizontally (Fig. 2). Whereas a normal pendulum is stable when hanging downwards, an inverted pendulum is inherently unstable, and must be actively balanced in order to remain upright by applying a horizontal force to the cart. The inverted pendulum is a classic problem in dynamics and control theory and is widely used as benchmark for testing control algorithms.

There are two outputs of interest: the displacement of the cart x and the angle of the pendulum θ. When concerned only with the angle of the pendulum, the behaviour of the system can be represented using the following transfer function

$$G(s) = \frac{ml(K_d s^2 + K_p s + K_i)}{(MI + Mml^2 + mI)s^3 + (bI + bml^2)s^2 - (Mmgl + m^2gl)s - bmgl}$$

Table 1 shows the values for the parameters of the system chosen for this example. The value of the mass of the pendulum m is left undecided.

Analysis of an Inverted Pendulum that Meets its Requirements Assuming that the mass of the pendulum is 0.2 kg, the open loop transfer function

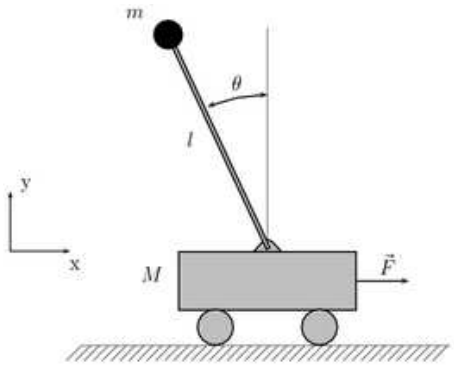

Fig. 2. Inverted Pendulum

Table 1. Values for parameters in an inverted pendulum system

Mass of cart	M	0.5 kg
Friction of the cart	b	0.1
Length to the pendulum's center of mass	l	0.3 m
Inertia of the pendulum	I	0.006 kgm^2
Gravitational acceleration	g	9.8 m/sec^2
Proportional coefficient	K_p	3.5
Integral coefficient	K_i	-1
Derivative coefficient	K_d	-1

for the inverted pendulum system is

$$G(s) = \frac{-25(2s^2 - 7s + 2)}{11s^3 + 2s^2 - 343s - 49}$$

and the gain and phase-shift can be calculated as follows:

$$y = 20 \log_{10} \left(\frac{25\sqrt{\begin{array}{c} 484w^{10} + 35161w^8 + 781414w^6 \\ + 4871449w^4 + 569821w^2 + 9604 \end{array}}}{121w^6 + 7550w^4 + 117845w^2 + 2401} \right)$$

$$x = \begin{cases} -\arctan(\frac{650w^3 - 1029w + 22w^5}{81w^4 + 24595w^2 - 98}) & \text{if } 0 \leq w < 0.198 \\ -\pi & \text{if } w = 0.198 \\ -\arctan(\frac{650w^3 - 1029w + 22w^5}{81w^4 + 24595w^2 - 98}) - \pi & \text{if } 0.198 < w \end{cases}$$

Next we use Maple and MetiTarski to analyse this system with respect to the exclusion region criteria and prove that it meets its requirements as follows:

1. We first calculate using Maple that the interval $[-\frac{5}{4}\pi, -\pi]$, in terms of x, corresponds to the interval $[\frac{157}{128}, \frac{129}{32}]$ in terms of w and then use MetiTarski

to show that

$$\forall w.\ \frac{157}{128} \geq w \vee w \geq \frac{129}{32} \Longrightarrow -\frac{5}{4}\pi \geq x \vee x \geq -\pi.$$

Analysis using Maple shows that within this interval there is one point of inflection, which lies in the interval $[\frac{569}{256}, \frac{1139}{512}]$. The curve is convex for $w \in [\frac{157}{128}, \frac{569}{256}]$ and concave for $w \in [\frac{1139}{512}, \frac{129}{32}]$. Then MetiTarski proves that the curve lies below $-\frac{12}{\pi}x - 18$ at $\frac{157}{128}$, $\frac{569}{256}$ and $\frac{1139}{512}$, and thus that it lies outside the exclusion region for $x \in [-\frac{5}{4}\pi, -\pi]$.

$$y < -\frac{12}{\pi}x - 18 \text{ at } \frac{157}{128}, \frac{569}{256}, \text{ and } \frac{1139}{512}$$

2. Maple calculates that the interval $[-\pi, -\frac{3}{4}\pi]$, in terms of x, corresponds to the interval $[\frac{57}{128}, \frac{629}{512}]$ in terms of w and then MetiTarski proves that

$$\forall w.\ \frac{57}{128} \geq w \vee w \geq \frac{629}{512} \Longrightarrow -\pi \geq x \vee x \geq -\frac{3}{4}\pi$$

Within this interval there are no points of inflection. The curve is convex for $w \in [\frac{57}{128}, \frac{629}{512}]$. MetiTarski proves that the curve lies below $\frac{12}{\pi}x + 6$ at $\frac{57}{128}$ and $\frac{629}{512}$, and thus it lies outside the exclusion region for $x \in [-\pi, -\frac{3}{4}\pi]$.

$$y < \frac{12}{\pi}x + 6 \text{ at } \frac{57}{128} \text{ and } \frac{629}{512}$$

3. Maple calculates that the interval $[-3, 3]$, in terms of y, corresponds to the interval $[0, \frac{101}{512}]$ in terms of w and then MetiTarski proves that

$$\forall w.\ w \geq \frac{101}{512} \Longrightarrow -3 \geq y \vee y \geq 3$$

Within this interval there are no points of inflection. The curve is convex for $w \in [0, \frac{101}{512}]$. MetiTarski proves that the curve lies above $-\frac{3}{4}\pi$ at $\frac{101}{512}$ and thus that it lies outside the exclusion region for $y \in [-3, 3]$.

$$-\frac{3}{4}\pi < x \text{ at } \frac{101}{512}$$

Analysis of an Inverted Pendulum that Fails to Meet its Requirements Next a parameter of the inverted pendulum system is altered slightly and the system is re-analysed with respect to the same criteria. Given that the mass of the pendulum in the inverted pendulum system has the value 0.17, the open loop transfer function for the system is

$$G(s) = \frac{-4250(2s^2 - 7s + 2)}{1945s^3 + 355s^2 - 55811s - 8330}$$

and the gain and phase-shift can be calculated as follows:

$$y = 20\log_{10}\left(\frac{425\sqrt{0.1w^{10} + 10.2w^8 + 214.0w^6 + 1290.9w^4 + 153.2w^2 + 2.7}}{37.8w^6 + 2172.3w^4 + 31207.8w^2 + 693.8}\right)$$

$$x = \begin{cases} -\arctan(\frac{105247w^3 + 3890w^5 - 169932w}{14325w^4 + 406627w^2 - 16660}) & \text{if } 0 \leq w < 0.202 \\ -\pi & \text{if } w = 0.202 \\ -\arctan(\frac{105247w^3 + 3890w^5 - 169932w}{14325w^4 + 406627w^2 - 16660}) - \pi & \text{if } 0.202 < w \end{cases}$$

We use Maple and MetiTarski to analyse this system with respect to the exclusion region criteria and prove that it fails to meet its requirements by providing a counter example as follows:

1. We first calculate using Maple that the interval $[-\frac{5}{4}\pi, -\pi]$, in terms of x, corresponds to the interval $[\frac{79}{64}, \frac{517}{128}]$ in terms of w and then use MetiTarski to show that

$$\forall w.\ \frac{79}{64} \geq w \vee w \geq \frac{517}{128} \Longrightarrow -\frac{5}{4}\pi \geq x \vee x \geq -\pi$$

   Within this interval there is one point of inflection, which lies in the interval $[\frac{1059}{512}, \frac{265}{128}]$. The curve is convex for $w \in [\frac{79}{64}, \frac{1059}{512}]$ and concave for $w \in [\frac{256}{128}, \frac{517}{128}]$. MetiTarski proves that the curve lies below the line $-\frac{12}{\pi}x - 18$ at $\frac{79}{64}$ and $\frac{1059}{512}$.

$$y < -\frac{12}{\pi}x - 18 \text{ at } \frac{79}{64} \text{ and } \frac{1059}{512}$$

   MetiTarski then proves that at $\frac{265}{128}$ the curve lies within the exclusion region and thus the Nichols plot fails to meet its requirements for $x \in [-\frac{5}{4}\pi, -\pi]$.

$$y \geq -\frac{12}{\pi}x - 18 \wedge y \leq \frac{12}{\pi}x + 18 \text{ at } \frac{256}{128}$$

2. Maple calculates that the interval $[-\pi, -\frac{3}{4}\pi]$, in terms of x, corresponds to the interval $[\frac{231}{512}, \frac{633}{512}]$ in terms of w and then MetiTarski proves that

$$\forall w.\ \frac{231}{512} \geq w \vee w \geq \frac{633}{512} \Longrightarrow -\pi \geq x \vee x \geq -\frac{3}{4}\pi$$

   Within this interval there are no points of inflection. The curve is convex for $w \in [\frac{231}{512}, \frac{633}{512}]$. MetiTarski proves that at $\frac{57}{128}$ the curve lies within the exclusion region and thus the Nichols plot fails to meet its requirements for $x \in [-\pi, -\frac{3}{4}\pi]$.

$$y \geq \frac{12}{\pi}x + 6 \wedge y \leq -\frac{12}{\pi}x - 6 \text{ at } \frac{57}{128}$$

3. Maple calculates that the interval $[-3, 3]$, in terms of y, corresponds to the interval $[0, \frac{55}{256}]$ in terms of w and then MetiTarski proves that

$$\forall w.\ w \geq \frac{55}{256} \Longrightarrow -3 \geq y \vee y \geq 3$$

Within this interval there are no points of inflection. The curve is convex for $w \in [0, \frac{103}{512}]$ and concave for $w \in [\frac{13}{64}, \frac{55}{256}]$. MetiTarski proves that the curve lies above $-\frac{3}{4}\pi$ at $\frac{103}{512}$, $\frac{13}{64}$, and $\frac{55}{256}$, and thus that it lies outside the exclusion region for $y \in [-3, 3]$.

$$-\frac{3}{4}\pi < x \text{ at } \frac{103}{512}, \frac{13}{64}, \text{and } \frac{55}{256}$$

3.3 Magnetic Disk Drive Reader System

This section focuses on the modeling and analysis of a magnetic disk drive system [7] with respect to stability. Modern computers use magnetic disks to store data. A disk drive reader reads the data by positioning a reader head over a track on the disk. It consists of a controller (or amplifier), a motor, an arm and a read head. A metal spring (or flexure) holds the read head slightly above the disk. For a given set of parameter values, the open loop transfer function of the disk drive system is

$$G(s) = \frac{2.8 \times 10^{11} K_m}{(s + 1000)s(s + 20)(3s^2 + 30000 + 100000000).}$$

This system has an 'uncertain' parameter, namely the motor constant which is represented by the constant K_m and its value is known to lie within the interval $[120, 130]$. The gain and phase-shift of the system can be calculated as follows:

$$y = 20 \log_{10} \left(\frac{2.8 \times 10^{11} K_m}{\sqrt{9w^{10} + 3.09 \times 10^8 w^8 + 1.03 \times 10^{16} w^6 + 10^{22} w^4 + 4 \times 10^{24} w^2}} \right)$$

$$x = \begin{cases} -\arctan(\frac{-130660000w^2 + 3w^4 + 2 \times 10^{12}}{1140w(29w^2 - 90000000)}) - \pi & \text{if } 0 \leq w < 1761.6 \\ -\pi & \text{if } w = 1761.6 \\ -\arctan(\frac{-130660000w^2 + 3w^4 + 2 \times 10^{12}}{1140w(29w^2 - 90000000)}) - 2\pi & \text{if } 1761.6 < w \end{cases}$$

Following a similar approach to the inverted pendulum, we have used Maple and MetiTarski to provide a symbolic analysis and formal proof. The system meets its requirements for all permissible parameter values. The three Nichols plot exclusion zones (recall Sect. 3.1) give rise to the following proof obligations:

$$\forall w.\ \frac{15839}{128} \geq w \vee w \geq \frac{354991}{512} \Longrightarrow -\frac{5}{4}\pi \geq x \vee x \geq -\pi$$

$$y < -\frac{12}{\pi}x - 18 \text{ at } \frac{15839}{128} \text{ and } \frac{354991}{512} \text{ for } K_m = 120 \text{ and } K_m = 130$$

$$\forall w.\ \frac{9745}{512} \geq w \vee w \geq \frac{63357}{512} \Longrightarrow -\pi \geq x \vee x \geq -\frac{3}{4}\pi$$

$$y < \frac{12}{\pi}x + 6 \text{ at } \frac{9745}{512} \text{ and } \frac{63357}{512} \text{ for } K_m = 120 \text{ and } K_m = 130$$

$$\forall w.\ \frac{1347}{128} \geq w \vee w \geq \frac{9601}{512} \Longrightarrow -3 \geq y \vee y \geq 3$$
$$-\frac{3}{4}\pi < x \text{ at } \frac{1347}{128} \text{ for } K_m = 120 \text{ and } K_m = 130$$

4 Hybrid Systems Verification

In order to examine the feasibility of verifying hybrid systems using MetiTarski, we developed the following procedure. It involves a number of manual steps, but they are essentially mechanical and could be automated.

1. Derive the hybrid automaton model of the system under investigation as an state diagram, including the number of locations with the corresponding parameters, the transition relation between different locations, and the system of differential equations governing the system in each location.
2. Starting from any particular location, we supply its system of ODEs and initial condition to Maple, and apply a Laplace transform to find an expression for the state variables of the system as an output function of time.
3. Using the transition relations, we use Maple to find the switching time from the first location to the next location. At this calculated time, we determine the values of all state variables using the time-dependent analytical expressions determined in the previous step, to find the final values of the state variables in location 1, and use them as the initial condition for the next state. We continue this procedure until we cover all reachable locations taking non-singleton initial sets of states into account.
4. Formulate the verification question as a safety property involving inequalities over the real-valued special functions.
5. Supply this first-order formula in TPTP format, including the corresponding axioms, as an input file to MetiTarski.

If MetiTarski is successful, it delivers a proof. Otherwise, it will probably run until terminated.

4.1 Collision Avoidance

We consider a cruise control system with automatic collision avoidance [16]. Let gap, v_f, v and a respectively represent the gap between the two cars, the velocity of the leading car, and the velocity and acceleration of the rear car. Then, the set of differential equations governing the system is

$$\dot{v} = a,\ \dot{a} = -3a - 3(v - v_f) + (gap - (v + 10)),\ \dot{gap} = v_f - v$$

Assuming the variable v_f is a parameter (unchanging symbolic constant), the dynamics of the system can be written as $\dot{x} = Ax + B$, where

$$x = \begin{bmatrix} v \\ v_f \\ a \\ gap \end{bmatrix} \quad A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -4 & 3 & -3 & 1 \\ -1 & 1 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ -10 \\ 0 \end{bmatrix}$$

For the given set of initial states as $x_0 = (2, 2, -0.5, 1)^T$, the problem is to verify that rear car would never collide with the car in front, that is, always $gap > 0$.

Let X denote the Laplace transform of x ($X = \mathcal{L}\, x$), then $sX - x_0 = AX + \frac{B}{s}$, and solving for X we have $X = (sI - A)^{-1}(x_0 + \frac{B}{s})$. Using Maple we have

$$X = \begin{bmatrix} \dfrac{2s^3 + 5.5s^2 - 3s + 2}{s(s^3 + 3s^2 + 4s + 1.0)} \\ 2s^{-1} \\ \dfrac{-0.5s(22 + s)}{s^3 + 3s^2 + 4s + 1} \\ \dfrac{3s^2 + 4.5s + 12 + s^3}{s(s^3 + 3s^2 + 4s + 1)} \end{bmatrix}$$

Therefore, $gap = \mathcal{L}^{-1}\, \dfrac{3s^2 + 4.5s + 12 + s^3}{s\,(s^3 + 3s^2 + 4s + 1)}$, and using Maple for the inverse Laplace transform we have

$$gap = 12 - 14.2\mathrm{e}^{-0.318t} + 3.24\mathrm{e}^{-1.34t}\cos(1.16t) - 0.154\mathrm{e}^{-1.34t}\sin(1.16t).$$

MetiTarski proves that this expression is always greater than zero, and therefore the system is safe for the given initial conditions.

4.2 Navigation

This benchmark deals with an object (perhaps a vehicle, though the dynamics are not exactly vehicle dynamics) that moves in the $\mathbb{R}^2$ plane [9]. The desired velocity $\mathbf{v}_d$ is determined by the position of the object in an $n \times m$ grid, and the desired velocities may take values as follows:

$$\mathbf{v}_d = (v_{d1}(i), v_{d2}(i)) = (\sin(i \times \frac{\pi}{4}), \cos(i \times \frac{\pi}{4})),\ \text{for } i = 0, \ldots, 7$$

We assume that the length and the width of a cell is 1, and that the lower left corner of the grid is the origin. An example of a 3×3 grid is depicted in Fig. 3.a, where the label i in each cell refers to the desired velocity. In addition, the grid contains cells labelled **A** that have to be reached and cells labelled **B** that ought to be avoided.

Given $\mathbf{v}_d$ the behavior of the actual velocity $\mathbf{v}$ is determined by the differential equation $\dot{\mathbf{v}} = C(\mathbf{v} - \mathbf{v}_d)$, where $C \in \mathbb{R}^{2\times 2}$ is assumed to have eigenvalues with strictly negative real part. This guarantees that the velocity will converge to the desired velocity. Figure 3.b shows two trajectories, with $C = \begin{pmatrix} -1.2 & 0.1 \\ 0.1 & -1.2 \end{pmatrix}$. Both satisfy the property that **A** should be reached, and **B** avoided.

An instance of this benchmark is characterized by the initial condition on $\mathbf{x}$ and $\mathbf{v}$, by matrix C in the differential equation for $\mathbf{v}$ and by the map of the grid,

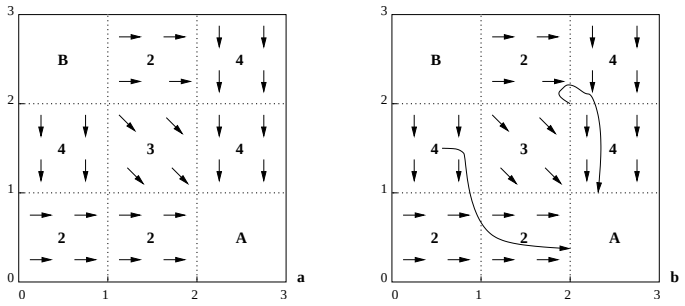

Fig. 3. a. The map determines the desired velocity of the moving object, depending on the position of the object. b. Two trajectories of objects moving in the plane. Both objects eventually reach cell **A** while avoiding **B**.

which can be represented as $n \times m$ matrix with elements from $\{0, \ldots, 7\} \cup \{\mathbf{A}, \mathbf{B}\}$. For the example in Fig. 3 this matrix is $\begin{pmatrix} \mathbf{B} & 2 & 4 \\ 4 & 3 & 4 \\ 2 & 2 & \mathbf{A} \end{pmatrix}$.

The dynamics of the 4-dimensional state vector $(x_1, x_2, v_1, v_2)^T$ are given by

$$\begin{pmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{v_1} \\ \dot{v_2} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1.2 & 0.1 \\ 0 & 0 & 0.1 & -1.2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ v_1 \\ v_2 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ -1.2 & 0.1 \\ 0.1 & -1.2 \end{pmatrix} \begin{pmatrix} v_{d1}(i) \\ v_{d2}(i) \end{pmatrix}$$

The resulting time-deterministic hybrid system [4] is shown in Figure 4. The system has five locations.

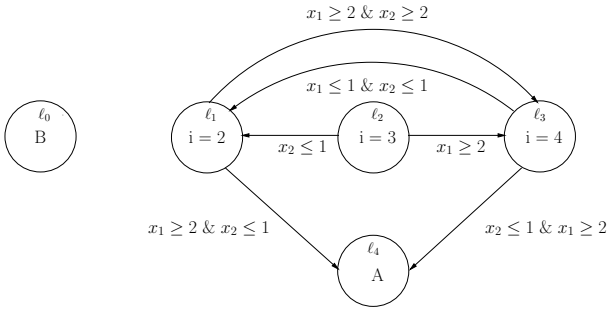

Fig. 4. The hybrid automaton model of the Navigation system.

1. Location ℓ_0, corresponds to cells labelled **B** that ought to be avoided.

2. Location ℓ_1, corresponds to $i = 2$ or $\mathbf{v}_d = (1, 0)$. Therefore, the differential equations of the system in this mode are

$$\dot{x_1} = v_1,\ \dot{x_2} = v_2,\ \dot{v_1} = -1.2v_1 + 0.1v_2 + 1.2,\ \dot{v_2} = 0.1v_1 - 1.2v_2 - 0.1. \quad (2)$$

3. Location ℓ_2, corresponds to $i = 3$ or $\mathbf{v}_d = (+0.707, -0.707)$. Therefore, the differential equations of the system in this mode are

$$\dot{x_1} = v_1,\ \dot{x_2} = v_2,\ \dot{v_1} = -1.2v_1 + 0.1v_2 + 0.919,\ \dot{v_2} = 0.1v_1 - 1.2v_2 - 0.919. \quad (3)$$

4. Location ℓ_3, corresponds to $i = 4$ or $\mathbf{v}_d = (0, -1)$. Therefore, the differential equations of the system in this mode are

$$\dot{x_1} = v_1,\ \dot{x_2} = v_2,\ \dot{v_1} = -1.2v_1 + 0.1v_2 + 0.1,\ \dot{v_2} = 0.1v_1 - 1.2v_2 - 1.2. \quad (4)$$

5. Location ℓ_4, corresponds to cells labelled **A** that have to be reached.

The transition relations between different locations are specified by logical formulas in Fig. 4. Now, suppose we start from the initial states defined by $(0.5, 1.5, 0.1, 0)^T$, which means we are initially in location ℓ_3, and the differential equations governing the system are those described in equation (4). Using the Laplace transform method as described before, we can solve this system of ODEs using Maple to get the following closed form formulas for x_1 and x_2

$$x_1 = -0.5\mathrm{e}^{-1.1t} + 0.654 + 0.346\mathrm{e}^{-1.3t}$$
$$x_2 = -0.5\mathrm{e}^{-1.1t} + 2.35 - 0.346\mathrm{e}^{-1.3t} - t$$

More analysis with Maple shows that at $t = 1.12$, $x_1 = 1$. At this point we switch to location ℓ_1 with $i = 2$. We also use Maple to calculate the value of the other state variables at this time as $x_2 = 0.588$, $v_1 = 0.057$, and $v_2 = -0.735$. Therefore, the new initial states can be defined by $(1, 0.588, 0.057, -0.735)^T$, and the differential equations governing the system are those described in equation (2). Using the Laplace transform method as described before, we can solve this system of ODEs using Maple to derive formulas for x_1 and x_2:

$$x_1 = 0.742\mathrm{e}^{-1.1t} - 0.252 + 0.0974\mathrm{e}^{-1.3t} + t$$
$$x_2 = 0.736\mathrm{e}^{-1.1t} + 0.317 - 0.0538\mathrm{e}^{-1.3t}$$

We used MetiTarski to prove that in the first mode, for all values of time in the range $0 \leq t \leq 1$, we have $x_2 \leq 2$, and in the second mode, for all values of time in the range $0 \leq t$, we have $x_2 \leq 1$, and therefore, we verified that **B** cannot be reachable.

We have similarly verified safety properties of other hybrid system case studies such as the Room Heating and Mutant systems.

5 Conclusions

Our experiments demonstrate that problems arising in real-world applications can be tackled using a suitable automatic theorem prover. Table 2 shows the problems and runtimes for three categories of case studies: inverted pendulum, disk drive reader, and hybrid systems. The runtimes were measured on a 2.66 GHz Mac Pro running Poly/ML.

Table 2. Problems with Runtimes in Seconds

IPM-1-1	8.4
IPM-1-2	0.2
IPM-1-3	0.4
IPM-1-5-w	0.4
IPM-2-1	0.1
IPM-2-2	5.3
IPM-2-3	0.4
IPM-2-5-w	0.4
IPM-3-1	0.1
IPM-3-2	0.2
IPF-1-1	29.4
IPF-1-2	0.2
IPF-1-3	0.6
IPF-1-5-w	2.7
IPF-2-1	0.2
IPF-2-2	23.3
IPF-2-3	0.6
IPF-3-1	0.1
IPF-3-2	0.2
Inverted Pendulum	

DDR-1-1	0.8
DDR-1-2	6.8
DDR-1-3	0.2
DDR-1-5	0.8
DDR-1-6-w	0.3
DDR-1-7-w	0.4
DDR-1-8-w	0.3
DDR-2-1	1.0
DDR-2-2	0.2
DDR-2-5-w	0.4
DDR-2-6-w	0.4
DDR-2-7-w	0.4
DDR-2-8-w	0.4
DDR-3-1	0.1
DDR-3-2	0.1
Disk Drive Reader	

Collision Avoidance	5.1
Room Heating	0.8
Navigation-1	0.2
Navigation-2	0.4
Mutant-1	0.1
Mutant-2	12.9
Mutant-3	67.9
Hybrid Systems	

As can be seen from Table 2, there are different versions of the IPM and DDR problems which are related to the three intervals specifying the stability criteria of the Nichols plot of the systems. In each interval, we have proved several problems to guarantee that it meets or fails to meet its requirements. Different versions of a hybrid systems problem correspond to different modes of operation for the corresponding system.

The formulas to be proved are complicated, containing many occurrences of special functions. On the other hand, and in contrast to our earlier problems from the world of mathematics, they often have great margins of error. Therefore, they can be tackled even if we use fairly crude approximations, which in turn makes proofs less taxing than they would be otherwise.

We still need to investigate how well our work scales to larger and nonlinear problems. There will clearly still be a place for the competitive approaches based on model checking and constraint solving. Nevertheless, a theorem proving approach is a suitable alternative, particularly when we require proofs and not merely claims of correctness.

Acknowledgements. The research was supported by the Engineering and Physical Sciences Research Council [grant number EP/C013409/1]. Ruth (Hardy) Letham, Hanne Gottliebsen, and Ursula Martin helped with the control systems

problems. Stefan Ratschan, Zhikun She, and Mohamed Zaki helped with the hybrid systems problems. Figure 2 is obtained from http://en.wikipedia.org/wiki/Inverted_pendulum, and other figures are obtained from the corresponding references noted in each section.

References

1. B. Akbarpour and L. Paulson. Towards Automatic Proofs of Inequalities Involving Elementary Functions. In *Pragmatics of Decision Procedures in Automated Reasoning (PDPAR)*, pages 27–37, 2006.
2. B. Akbarpour and L. Paulson. Extending a Resolution Prover for Inequalities on Elementary Functions. In *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR)*, LNCS 4790, pages 47–61. Springer-Verlag, 2007.
3. B. Akbarpour and L. Paulson. Metitarski: An Automatic Prover for the Elementary Functions. In *Intelligent Computer Mathematics*, LNCS 5144, pages 217–231. Springer-Verlag, 2008.
4. R. Alur, C. Courcoubetis, N. Halbwaches, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olibero, J. Sifakis, and S. Yovine. The Algorithmic Analysis of Hybrid Systems. *Theoretical Computer Science*, 138:3–34, 1995.
5. E. Asarin, T. Dang, and O. Maler. The d/dt Tool for Verification of Hybrid Systems. In *Computer Aided Verification*, LNCS 2404, pages 365–370. Springer-Verlag, 2002.
6. A. Chutianan and B. H. Krogh. Computational Techniques for Hybrid System Verification. *IEEE Transactions on Automatic Control*, 48(1):64–75, 2003.
7. R. C. Dorf and R. H. Bishop. *Modern Control Systems*. Prentice-Hall, 2001.
8. L. Duarte, S. Duarte, L. da Mota, and J. Skea. An Extension of the Prelle-Singer Method and a Maple Implementation. *Computer Physics Communications*, 144(1):46–62, March 2002.
9. G. Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. In *Hybrid Systems: Computation and Control (HSCC)*, LNCS 3414, pages 258–273. Springer-Verlag, 2005.
10. R. Hardy. *Formal Methods for Control Engineering: A Validated Decision Procedure for Nichols Plot Analysis*. PhD thesis, St. Andrews University, 2006.
11. T. A. Henzinger, P. H. Ho, and H. Wong-Ti. HyTech: A Model Checker for Hybrid Systems. *Software Tools for Technology Transfer*, 1(1-2):110–122, 1997.
12. M. S. M. Prelle. Elementary First Integrals of Differential Equations. *Transactions of the American Mathematical Society*, 279(1):215–229, Sep. 1983.
13. Y. Man. Computing closed form solutions of first order odes using the prelle-singer procedure. *J. Symb. Comput.*, 16(5):423–443, 1993.
14. S. Ratschan and Z. She. Safety Verification of Hybrid Systems by Constraint Propagation-Based Abstraction Refinement. *ACM Transactions on Embedded Computing Systems*, 6(1), 2007.
15. S. Ratschan, Zhikun She. Benchmarks for Safety Verification of Hybrid Systems. http://hsolver.sourceforge.net/benchmarks, June 13, 2008.
16. A. Tiwari. Approximate Reachability for Linear Systems. In *Hybrid Systems: Computation and Control (HSCC)*, LNCS 2623, pages 514–525. Springer-Verlag, 2003.