Available online at www.sciencedirect.com

SCIENCE DIRECT®

Electronic Notes in Theoretical Computer Science

Electronic Notes in Theoretical Computer Science 151 (2006) 111–125

www.elsevier.com/locate/entcs

Interactions Between PVS and Maple in Symbolic Analysis of Control Systems

Ruth Hardy[1,2]

School of Computer Science
University of St Andrews
St Andrews, Scotland

Abstract

This paper presents a decision procedure for problems relating polynomial and transcendental functions. The procedure applies to functions that are continuously differentiable with a finite number of points of inflection in a closed convex set. It decides questions of the form 'is $f \sim 0$?', where $\sim \in \{=, >, <\}$. An implementation of the procedure in Maple and PVS exploits the existing Maple, PVS and QEPCAD connections. It is at present limited to those twice differentiable functions whose derivatives are rational functions (rationally differentiable). This procedure is particularly applicable to the analysis of control systems in determining important properties such as stability.

Keywords: reliable mathematics, formal methods, quantifier elimination, control systems, Maple-PVS, QEPCAD

1 Introduction

Many problems in the fields of mathematics, computer science and control engineering can be reduced to decision and quantifier elimination problems [7], [14], [20], often involving trigonometric and transcendental functions; problems such as algebraic surface intersection and display; robot motion planning

[1] Thanks go to Ursula Martin and Richard Boulton for their help and guidance, especially in the early stages of this work, also to Roy Dyckhoff and Steve Linton for their continuing help and guidance. Additional thanks go to John Hall, Rick Hyde and Yoge Patel for sharing their insights into control engineering, and to Rob Arthan, Tom Kelsey and Colin O'Halloran for many helpful discussions.

[2] Email: rh@dcs.st-and.ac.uk

doi:10.1016/j.entcs.2005.11.026

(where the aim is to determine whether a number of objects, whose physical attributes and range of motion can be described algebraically, can move from some initial configuration to reach some final configuration); stability analysis using the von Neumann condition for the stability of difference schemes. Quantifier elimination algorithms for real closed fields (RCF) have been developed [6], [17], [18] and various algorithms have been suggested for special types of problems involving trigonometric or transcendental functions [2], [21] but these are limited to very specific problems and often do not include support for inverse trigonometric or transcendental functions such as arctan or the natural logarithm, which are important in control engineering.

A problem arising in analysis of control systems is to decide if a given function is greater than another in an interval [10]. In this paper we present a decision procedure for problems of this type for functions $f : \mathbb{R}^2 \to \mathbb{R}$ that are continuously differentiable with a finite number of points of inflection in a closed convex set (a set such that every element that lies between two members of the set is a member of the set and the boundary points of the set are members of it). The procedure requires efficient reliable symbolic manipulation of mathematical formulae and exact numerical calculation. No existing individual tool has all of these qualities. Computer algebra systems (CASs) are excellent at symbolic manipulation and often provide powerful methods for numerical calculations, however, they cannot guarantee correct results; formal theorem provers (TPs) can guarantee correct results but are inefficient for automatic symbolic manipulation and numerical calculations. There has been much interest in the development of systems that provide the power of a CAS and the rigour of a TP. Systems of this type fall into two main categories; computational support for TPs and formal support for CASs. Systems such as Maple–HOL [11] and Maple–Isabelle [3] provide links between the TPs HOL and Isabelle and the CAS Maple, allowing the TPs to call upon the computational power of Maple under appropriate circumstance to increase efficiency of proof or proof search; Maple–PVS [1] provides a link between Maple and the TP PVS, allowing Maple to call upon the theorem proving power of PVS to increase reliability of its results; the Omega proof development system [15] supports the integration of computer algebra into mechanised reasoning systems at the proof planning stage; Redlog [8], Analytica [4] and Theorema [5] extend CASs with support for formal theorem proving. A prototype tool implementing the decision procedure has been developed in the Maple–PVS system, taking advantage of the reliable efficient mathematics it provides.

The formulae for which the decision procedure is applicable are classified in Section 2 of this paper, in terms of a fragment of a first order logic $\mathcal{L}$ for the reals. Various important geometric properties of curves are given in Section 3.

In Section 4 the procedure for deciding sentences of the language $\mathcal{L}$ based on the geometric properties of curves is described. In Section 5 the practical issues associated with the automation of the procedure are discussed and a prototype tool combining Maple, PVS and QEPCAD is presented to demonstrate how computer algebra, theorem proving and quantifier elimination systems can be combined to automate the procedure for sentences of $\mathcal{L}$ containing one quantified variable. Section 6 presents a simple example of the usage of this method in the analysis of a control system. Finally, conclusions and directions for further work are presented in Section 7.

2 Classification

A *closed convex set* is a subset of $\mathbb{R}^n$, such that every element that lies on the line between two members of the set is also a member of the set and all limit points of the set are also members of it. In the one dimensional case, a set $D \subseteq \mathbb{R}$ is a closed convex set if and only if D is a closed interval.

A *continuously differentiable* term is a function whose derivative exists and is continuous, i.e, it is an expression of the form $f(\mathbf{x})$ such that ∇f exists and is a vector of continuous terms. *Rational* terms are a specialised form of continuously differentiable terms and are quotients of polynomials in the variables x_i with real coefficients a_i. If these coefficients are non–algebraic then they are described in terms of intervals (a_{il}, a_{iu}) with real algebraic bounds, in which they lie. *Linear* terms are a specialised form of rational terms, such that they are linear in all variables, i.e, they are expressions of the form $a_0 + \sum_{i=0}^{n} a_i x_i$ where a_0, a_i are real algebraic numbers and x_i are real variables. A *rationally differentiable* term is a specialised form of continuously differentiable term, such that it is differentiable and all partial derivatives are rational terms, i.e, it is an expression of the form $f(\mathbf{x})$ such that ∇f exists and is a vector of rational terms. A *finitely inflective* term is a continuously differentiable term with a finite number of regions of convexity and/or concavity.

An atomic formula in the language $\mathcal{L}$ is an equation or inequality involving a finitely inflective term over some closed convex set, $\mathbf{x} \in D \Rightarrow f(\mathbf{x}) \sim 0$ where D is a closed convex set of $\mathbb{R}^n$, $f : \mathbb{R}^n \to \mathbb{R}$ and $\sim \in \{=, >, <\}$. Arbitrary formulae are obtained by iterated application of the propositional operators $\vee$, $\wedge$, $\neg$ and the quantifiers $\exists$, $\forall$ with respect to the variable x_i. Every formula can be rewritten in equivalent prenex normal form. If all occurrences of x in a formula ϕ are quantified then ϕ is a *closed formula* and, given the natural interpretation of formulae over reals, is either true or false.

3 Geometric Properties of Curves.

A function $f : \mathbb{R}^n \to \mathbb{R}$, where $\mathbf{dom} f$ is a convex set, is defined to be a convex function when:

$$f(\theta\mathbf{x} + (1-\theta)\mathbf{y}) \leq \theta f(\mathbf{x}) + (1-\theta)f(\mathbf{y}),\ \mathbf{x}, \mathbf{y} \in \mathbf{dom} f,\ 0 \leq \theta \leq 1$$

Various geometric properties can be inferred from this definition, for instance, the gradient of a convex curve in the direction of x_i does not decrease as x_i increases; [3] a convex curve lies on or above any tangent to it; in any direction the curve lies on or below the chord joining the curve at the boundary points. A linear term is both convex and concave and has an infinite number of points of inflection. Addition or subtraction of a linear function from a curve preserves the convexity/concavity of the curve.

4 Decision Procedure

The decision procedure described in this section was developed to take normal formulae in the language described in Section 2 and output the truth value of the input. Input is currently limited to functions of $\mathbb{R}$ or $\mathbb{R}^2$. The procedure was developed to be applied to the analysis of control systems and is applicable not only to sentences of real closed fields but also to any function whose derivative is a rational function. This encapsulates a range of functions that are not covered by any other decision procedure, including the natural logarithm and arctan, which are particularly significant functions in the field of control engineering.

The procedure relies on a set of conditions that allow the relative position of a curve $f : \mathbb{R}^2 \to \mathbb{R}$ and the plane $p : \mathbb{R}^2 \to \mathbb{R} = \mathbf{0}$ to be determined based on the examination of convexity properties (see Section 3) of the curve along with the examination of the curve and plane at a number of carefully determined points in a closed convex set.

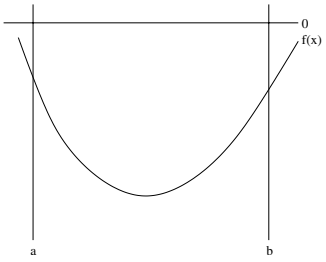
The set of conditions that the decision procedure uses for convex curves are detailed below and are illustrated for $f : \mathbb{R} \to \mathbb{R}$ in the interval $D = [a, b]$. Only the cases for a convex curve $f(\mathbf{x})$ in a convex set are detailed as all other cases are symmetric to this. Concave cases are a reflection of the convex cases and could be omitted by looking at $-f(\mathbf{x})$ in the appropriate regions.

Suppose the curve $f(\mathbf{x})$ is continuously differentiable and convex on the

[3] It should be noted that comparison of gradients is done not in terms of steepness (i.e, the norm of the gradient), but rather in terms of the actual value.

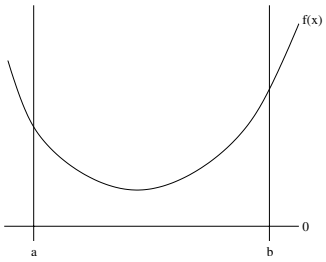
closed convex set D, then:

(i) The curve is negative on $\mathbf{x} \in D$ if and only if the curve is negative at the boundaries of D

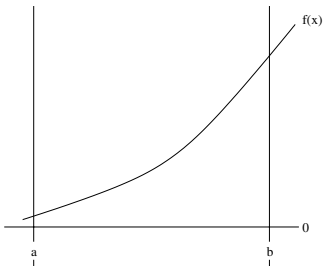


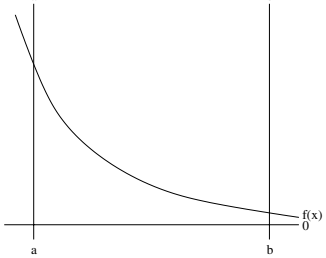
(ii) The curve is positive on $\mathbf{x} \in D$ if and only if one of the following mutually exclusive conditions holds:

(a) the gradient of the curve in any direction is equal to zero at any (extended) point within the region and the curve is positive at that point, i.e, $\nabla f(\mathbf{x}) = (0,\, f_1(\mathbf{x}))$ or $\nabla f(\mathbf{x}) = (f_2(\mathbf{x}),\, 0)$ and $f(\mathbf{x}) > 0$



(b) the gradient of the curve in any direction does not equal zero at any point within the region and the curve is positive at the region's boundaries, i.e, $\nabla f \neq (0,\, f_1)$ and $\nabla f \neq (f_2,\, 0)$ and $f(\text{boundary}(D)) > 0$





If none of the above conditions hold for a convex curve then there is at least one point within the region at which the curve is equal to zero.

For finitely inflective functions of one variable any interval of interest can be split into a finite number of intervals over which the curve is either convex or concave, however, for functions of multiple variables there may be regions over which the curve is neither convex nor concave (consider $z = x^2 - y^2$). These regions contain *saddle points* and must be treated separately. In these

regions the function is convex in some directions and concave in others. The maximum and minimum values for the function in these regions lie on the boundaries, and the sign of the function on these boundaries can be used to determine whether the curve is positive or negative in the region.

In order to use the conditions described here to decide sentences of the language described in Section 2 the closed convex set must be split into regions over which the curve is either convex, concave or contains a saddle point.

The decision procedure takes sentence ϕ in prenex normal form in the language described in Section 2 and performs the following steps:

Step 1: Convert existential quantification in ϕ to universal quantification giving ϕ'. This is a syntactic conversion to simplify the algorithm: $\exists x.P(x)$ becomes $\neg\forall x.\neg P(x)$
Step 2: Take each atomic formula $f_i \sim_i 0$ from ϕ' and determine the regions D_{ij} of convexity, concavity and those containing saddle points for f_i.
Step 3: For each of the regions D_{ij} within $\mathbf{dom} f_i$ apply the appropriate case from the set of conditions. If the correct conditions hold for all these regions then the i-th atomic formula has the value TRUE. If the condition fails to hold for any of the regions then the formula has the value FALSE.
Step 4: Construct the truth value for the sentence ϕ' (and thus ϕ) by applying the propositional operators within it to the truth values of Step 3.

The set of conditions presented in this section are applicable to functions that are finitely inflective, that is functions that are differentiable with a continuous derivative and a finite number of regions in which the curve is convex or concave. In practice this requirement is strengthened to finitely inflective rationally differentiable functions.

Proofs in PVS of coverage of these cases exists along with proof of termination of the procedure given that convexity is known and the number of regions in which the curve is convex or concave is finite in a closed convex set.

5 Implementation in Maple–PVS

In order to implement this procedure one must be able to reliably calculate the points of inflection of continuously differentiable functions, the convexity of the corresponding curve and the sign of the curve at given points. This requires not only powerful symbolic manipulation whose results are guaranteed correct but also validated numerical calculation.

Computer Algebra Systems (CASs) provide a powerful method for symbolic manipulation and analysis of mathematical formulae and are ideal for

performing the transformations and calculations required by the decision procedure of Section 4. However, they can not always guarantee correct results, often ignoring assumptions and side conditions and producing floating point errors during numerical calculation. Formal theorem provers provide powerful methods for formal analysis but lack the ability to perform symbolic manipulation or numerical calculations efficiently. The Maple-PVS [1] tool provides a link between the CAS Maple [16] and the theorem prover PVS [13]. This system allows the calculations performed by Maple to be formally verified by PVS, providing efficient and reliable mathematics. The onus is on Maple to formulate the lemmas to be proved and pass them to PVS along with the proof steps to be taken, usually by invoking some high level PVS strategies. The QEPCAD-PVS [19] tool provides a shared object file, which can be loaded by PVS to allow QEPCAD [12] routines to be accessed via foreign function calls. The results of these function calls are considered reliable by PVS. This system allows PVS to use powerful and efficient quantifier elimination within its proofs.

The Maple-PVS system has been extended to allow the automatic loading of the QEPCAD shared object file into PVS (see Figure 1). This allows QEPCAD routines to be invoked via PVS strategies.

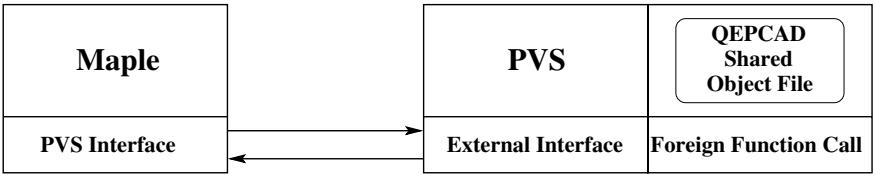


Fig. 1. Maple-PVS-QEPCAD.

The prototype tool is implemented in the Maple-PVS-QEPCAD system to allow the application of the decision procedure described in Section 4 in a formal and symbolic setting.

The prototype tool for the decision procedure is designed specifically for use in the field of control engineering. During *Nichols plot* analysis [9] it must be determined whether a parametric function remains within some bounded region on the plane. The user is required to provide the prototype tool with a parametric function and a representation of region; a list B of tuples each containing an interval $x \in [a_i, b_i]$, all of which are disjoint, and a list L_i of lines l_{ij} and inequality signs $\sim_{ij}$. Each element of L_i represents a constraint on the range of the parametric function. Each tuple represents the disjunction of the constraints in L_i in the domain $x \in [a_i, b_i]$. The list B represents the conjunction of the constraints represented by the tuples.

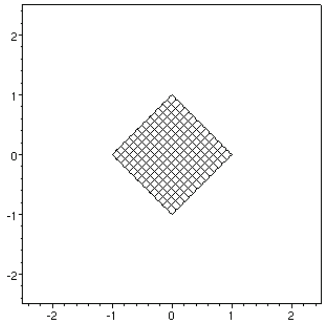


Fig. 2. Undesirable region around the origin.

Example 5.1 The input

$$y = Y(\omega),\ x = X(\omega)$$
$$B = [x \in [-1, 0],\ [-1 - x, >],\ [1 + x, <]],$$
$$[x \in [0, 1],\ [1 - x, <],\ [-1 + x, >]]$$

represents the constraint

$$\forall \omega.\, (X(\omega) \in [-1, 0] \Rightarrow -1 - X(\omega) > Y(\omega) \ \vee\ 1 + X(\omega) < Y(\omega))$$
$$\wedge\, (X(\omega) \in [0, 1] \Rightarrow 1 - X(\omega) < Y(\omega) \vee -1 + X(\omega) > Y(\omega)$$

in other words, the parametric curve must not enter a diamond region about the origin (see Figure 2).

In order to apply the decision procedure to the input a certain amount of pre–processing is required to correctly formulate the problem. This requires both symbolic manipulation of the input and numerical calculation and is a task ideally suited to Maple, which provides the front end of the prototype tool via Maplets. These provide a Java applet–like graphical user interface in which the input is entered and any results or error messages are displayed. A simple type check mechanism ensures that the input is of the correct type and format. Maple processes the input to form the appropriate sentences for use in the decision procedure and invokes PVS, which in turn may invoke QEPCAD, to perform the required verification. Once the process is complete Maple displays the results of the decision procedure and a plot showing the bounding lines for the specified region along with the plot of the curve.

The following describes the steps taken by the prototype tool when considering a parametric equation for a curve $y = Y(\omega)$ and $x = X(\omega)$ and a list B of tuples containing an interval $x \in [a_i, b_i]$ and a list L_i of lines l_{ij} and inequality signs $\sim_{ij}$. Let $f_{ij}(\omega) = Y(\omega) - l_{ij}(X(\omega))$

(i) The user supplied input is type checked and if it is not of the correct format an error message is produced and the prototype tool halts.

(ii) Maple calculates, rewrites and simplifies the derivative and second derivative of the parametric equation with respect to x. Since the decision procedure relies upon the convexity of the curve and thus the sign of the second derivative it is important to confirm that Maple has calculated this correctly and has not ignored any important side conditions. Maple calls PVS to confirm that the function is well defined and is twice differentiable. If PVS fails to provide the required proof then the prototype tool produces an appropriate error message and halts.

(iii) The intervals $[a_i, b_i]$ are in term of x but the procedure will require these intervals to be in terms of ω, i,e. $[a_i, b_i] = [X(\omega_{ik}), X(\omega_{ik+1})]$. To calculate these intervals in terms of ω all real solutions to $a_i = X(\omega_{ik})$ or $b_i = X(\omega_{ik})$ must be found, then by looking at a point between each ω_{ik} and ω_{ik+1} the corresponding intervals can be determined. Since Maple does this using numerical calculation it can suffer from the problem of inexact arithmetic caused by floating point error and may fail to find all solutions.

To ensure that all solutions have been found it must be shown that the solutions found by Maple actually are approximate solutions and that there are no other solutions within the intervals $[a_i, b_i]$. Letting D_i represent small intervals around each of Maple's solution the decision procedure is applied to

$$\exists \omega .\, \omega \in D_i \Rightarrow X(\omega) = a_i \vee X(\omega) = b_i \tag{1}$$

to ensure that there are solutions in the intervals and

$$\forall \omega_1, \omega_2 .\, \omega_1 \in D_i \wedge \omega_2 \in D_i \Rightarrow \tag{2}$$
$$(X(\omega_1) = a_i \vee X(\omega_1) = b_i) \wedge (X(\omega_2) = a_i \vee X(\omega_2) = b_i) \Rightarrow \omega_1 = \omega_2$$

to ensure that there is only one solution in each intervals. The decision procedure is also applied to

$$\forall \omega .\, \omega \notin D \Rightarrow X(\omega) \neq a_i \wedge X(\omega) \neq b_i \tag{3}$$

where D is the set of reals x such that $x \in D_0 \vee x \in D_1 \vee \ldots$, to ensure that there are no solutions other than those found by Maple. If this fails the prototype tool produces an appropriate error message and halts.

To compensate for Maple's inexact arithmetic the solutions are adjusted by a small value to give 'safe' bounds for the interval for example if Maple calculates ω_{ik} and ω_{ik+1} such that $[a_i, b_i] \simeq [X(\omega_{ik}), X(\omega_{ik+1})]$ then Maple adjust by some δ such that $[a_i, b_i] \subseteq [X(\omega_{ik}-\delta), X(\omega_{ik+1}+\delta)]$. It is important that this condition holds so Maple calls PVS to verify the solutions. If PVS fails to provide the required proof then the prototype tool produces an appropriate error message and halts.

(iv) Maple calculates the points of inflection of f_{ij}, including any points at which it becomes vertical, in the intervals $[\omega_{ik} - \delta, \omega_{ik+1} + \delta]$. This is achieved using numerical methods to find points at which the second derivative of f_{ij} in terms of x (which is the same as the second derivative of the parametric curve calculated in Step ii) is zero and as a consequence is subject to errors due to inexact arithmetic. To avoid this problem Maple calculates small intervals $[p_{ikm} - \delta, p_{ikm} + \delta]$ in which these points lie (referred to as *intervals of inflection*). PVS is called to confirm not only that these intervals contain true points of inflection rather than points of zero curvature between two regions both strictly convex or concave but also that each of these points is the only point of inflection in $[p_{ikm} - \delta, p_{ikm} + \delta]$ and that the derivative of f_{ij} does not equal zero in $[p_{ikm} - \delta, p_{ikm} + \delta]$ unless it is exactly at the point of inflection. This is a relatively difficult problem for PVS to solve but since the derivative and second derivative of f_{ij} are rational it is ideal for quantifier elimination. PVS uses the QEPCAD-PVS link to invoke the QEPCAD strategies to verify Maple's results. If PVS fails to provide the required proof then the prototype tool produces an appropriate error message and halts.

(v) The intervals $[\omega_{ik} - \delta, \omega_{ik+1} + \delta]$ are split into $[\omega_{ik} - \delta, p_{ikm} - \delta]$ $[p_{ikm} - \delta, p_{ikm} + \delta]$ $[p_{ikm} + \delta, \omega_{ik+1} + \delta]$ over which the curve is either convex or concave, or is an interval of inflection.

(vi) Maple formulates the lemmas to be solved by PVS in the form $\lambda\omega \in [a, b]$. $f_{ij}(\omega) \sim_{ij} 0$ using the inequality sign $\sim_{ij}$ and the intervals calculated in the previous step. PVS is called by Maple to prove these lemmas and in essence determine whether the desired case from the set of conditions holds. In the case of intervals of inflection the truth of the sentence is not found using one of the cases of Section 4 but is determined, if necessary, by examining the bounds of the interval, since due to the nature of these intervals the maximum and minimum of f_{ij} must lie on the bounds. The truth value for atomic formula $f_{ij} \sim_{ij} 0$ is built up from the conjunction of each of the truth values of the corresponding lemmas.

(vii) The truth of the formulae represented by each L_i is built up from the disjunction of the truth values of each $f_{ij} \sim_{ij} 0$. The truth of the formula represented by B is then built up from the conjunction of the truth values of each L_i. The prototype tool produces an appropriate message stating whether the formula is true or false.

(viii) Maple produces a plot of the lines and the parametric plot of the curve.

PVS uses custom built libraries containing lemmas concerning the differentiability of various functions important in control system analysis, such as

arctan, natural logarithm, logarithm to the base 10, arbitrary rational functions and parametric functions, along with high level strategies and external function calls to QEPCAD to provide the proofs required in the prototype tool. These libraries contain definitions of the natural logarithm and arctan as Taylor series, which allows bounds on the value of these functions for any given input to be defined.

6 A Simple Example

In this section we present a simple example of how one might use the decision procedure presented in Section 4 and the implementation presented in Section 5 to determine formally whether a curve meets a line. The given example is representative of the form that arise in Nichols Plot analysis of control systems. It is a particularly interesting example as the curve contains intervals of convexity and concavity, points at which the curve is vertical and multiple intervals in terms of ω corresponding to a single interval in terms of x.

Consider the following bounding lines and parametric equation (see Figure 3):

$$B = x \in [-1.5,\ 0.5], [[55 + 8x, >], [65 - 12x, <]]$$

$$Y(\omega) = \frac{10\ln(p) - 20\ln(\omega^6 + 5\omega^4 + 60\omega^2 + 16)}{\ln(10)}$$

$$X(\omega) = \arctan\left(\frac{797\omega^6 + 14382\omega^4 + 755\omega^2 - 3194}{800\omega^8 + 4803\omega^6 + 12054\omega^4 - 1597\omega^2 + 55}\right)$$

where $\omega \geq 0$, and

$$p = 640000\omega^{16} + 7684800\omega^{14} + 42990418\omega^{12} + 136160432\omega^{10}$$
$$338091528\omega^8 - 21346562\omega^6 - 87425842\omega^4 - 4998610\omega^2 + 10204661$$

Maple calculates the derivative f' and second derivative f'' of the given parametric function. Considering $\ln(10)$ as some real constant in the range $(2.302585090, 2.302585100)$, both the derivative and second derivative are rational functions. Maple calls PVS to confirm that the parametric function is twice differentiable and that the derivatives are as specified by Maple. This is a relatively simple task for PVS, which uses the custom built libraries and powerful general purpose simplification and rewrite strategies such as *GRIND* to provide the relevant proofs.

The next step is to determine the intervals over ω that correspond to $X(\omega) \in [-1.5, 0.5]$. Maple calculates all solutions for $X(\omega_{1j}) = -1.5$ and $X(\omega_{1j}) = 0.5$ discarding all non–real solutions and all those that are not in the domain of the parametric function (in this case negative solutions).

This leaves three solutions $\omega_{1,1} = 0.4231452940$, $\omega_{1,2} = 0.7664324880$ and $\omega_{1,3} = 1.631039454$, giving four potential corresponding intervals:

$$[-\infty, \omega_{1,1}], [\omega_{1,1}, \omega_{1,2}], [\omega_{1,2}, \omega_{1,3}], [\omega_{1,3}, \infty]$$

Maple confirms that these are indeed approximate solutions and that they are the only solutions in the domain of the function by letting $\delta = 0.001$ and applying the decision procedure to

$$\exists \omega . \omega \in [\omega_{1,i} - \delta, \omega_{1,i} + \delta] \Rightarrow X(\omega) = -1.5 \vee X(\omega) = 0.5$$

to determine the existence of solutions,

$$\forall \omega_1, \omega_2 . \omega_1 \in [\omega_{1,i} - \delta, \omega_{1,i} + \delta] \wedge \omega_2 \in [\omega_{1,i} - \delta, \omega_{1,i} + \delta] \Rightarrow$$
$$(X(\omega_1) = -1.5 \vee X(\omega_1) = 0.5) \wedge (X(\omega_2) = -1.5 \vee X(\omega_2) = 0.5)$$
$$\Rightarrow \omega_1 = \omega_2$$

to determine the uniqueness of each solution in each interval and

$$\forall \omega . \omega \geq 0 \wedge \omega \notin [\omega_{1,1} - \delta, \omega_{1,1} + \delta] \wedge \omega \notin [\omega_{1,2} - \delta, \omega_{1,2} + \delta] \wedge$$
$$\omega \notin [\omega_{1,3} - \delta, \omega_{1,3} + \delta] \Rightarrow X(\omega) \neq -1.5 \wedge X(\omega) \neq 0.5$$

to determine that all solutions were found. Since none of these problems involve parametric equations the application of the decision procedure is much simpler and does not require the application of step iii in Section 5. Also, since there are no points of inflection in the first two problems (nor are there likely to be in most cases since the intervals of interest are so small) the application of the procedure is again simplified requiring no splitting of the intervals into subinterval as described in steps iv and v in Section 5.

Once it has been confirmed that the Solutions found by Maple are indeed correct a point within each of the intervals is examined, determining that $[\omega_{1,1}, \omega_{1,2}]$, and $[\omega_{1,3}, \infty]$ correspond to the interval $X(\omega) \in [-1.5, 0.5]$. To ensure the bounds on these intervals are 'safe' Maple adjusts them by $\delta = 0.01$; lower bounds are reduced by δ, upper bounds are increased by δ. At this point Maple calls PVS to confirm its calculations are correct, i.e, that $[-1.5, 0.5] \subseteq [X(\omega_{1,1} - \delta), X(\omega_{1,2} + \delta)]$ and that $[\lim_{\omega \to \infty} X(\omega), 0.5] \subseteq [\lim_{\omega \to \infty} X(\omega), X(\omega_{1,3} + \delta)]$. PVS uses custom built libraries and calls to QEPCAD to ensure this safety property.

Maple calculates the points of inflection of the parametric function, including points at which it becomes vertical by determining points at which the denominator and numerator of the second derivative equal zero. Discarding all points not within any interval of interest leaves a single point $\omega_{1,3,1} = 1.894587409$ within the interval $[\lim_{\omega \to \infty} X(\omega), X(\omega_{1,3} + \delta)]$. Maple calculates the interval of inflection $[\omega_{1,3,1} - \delta, \omega_{1,3,1} + \delta]$ and invokes PVS, which uses the QEPCAD strategies to prove that there is only one point of inflection

in the interval and that there is no point at which the derivative is equal to zero

$$\exists\omega \in [\omega_{1,3,1} - \delta,\, \omega_{1,3,1} + \delta].\forall\omega_2 \in [\omega_{1,3,1} - \delta,\, \omega_{1,3,1} + \delta].$$
$$(f''(\omega) = 0 \wedge f''(\omega_2) = 0) \Rightarrow \omega = \omega_2$$
$$\forall\omega \in [\omega_{1,3,1} - \delta,\, \omega_{1,3,1} + \delta].\, f'(\omega) - 8 \neq 0$$
$$\forall\omega \in [\omega_{1,3,1} - \delta,\, \omega_{1,3,1} + \delta].\, f'(\omega) + 12 \neq 0$$

Maple then formulates the appropriate lemmas

$$\lambda\omega \in [\omega_{1,1} - \delta,\, \omega_{1,2} + \delta]. \tag{4}$$
$$Y(\omega) - l_{1,1}(X(\omega)) \sim_{1,1} 0 \vee Y(\omega) - l_{1,2}(X(\omega)) \sim_{1,2} 0$$
$$\lambda\omega \in [\omega_{1,3} - \delta,\, \omega_{1,3,1} - \delta]. \tag{5}$$
$$Y(\omega) - l_{1,1}(X(\omega)) \sim_{1,1} 0 \vee Y(\omega) - l_{1,2}(X(\omega)) \sim_{1,2} 0$$
$$\lambda\omega \in [\omega_{1,3,1} - \delta,\, \omega_{1,3,1} + \delta]. \tag{6}$$
$$Y(\omega) - l_{1,1}(X(\omega)) \sim_{1,1} 0 \vee Y(\omega) - l_{1,2}(X(\omega)) \sim_{1,2} 0$$
$$\lambda\omega \in [\omega_{1,3,1} + \delta,\, \infty]. \tag{7}$$
$$Y(\omega) - l_{1,1}(X(\omega)) \sim_{1,1} 0 \vee Y(\omega) - l_{1,2}(X(\omega)) \sim_{1,2} 0$$

Each of these lemmas correspond either to one of the cases used in the decision procedure or to an interval of inflection. For lemmas 4, 5 and 7 PVS uses the appropriate case from the decision procedure to form a proof, the proof of lemma 6 follows directly from the truth of lemmas 5 and 7. This completes the calculations for the decision procedure.

Maple displays the truth of this formula along with a plot of the lines and the parametric curve as shown in Figure 3.

7 Conclusions and future work

The decision procedure presented in this paper allows one to determine the truth of sentences concerning finitely inflective functions in a closed convex sets. This encapsulates a range of functions not covered by existing decision procedures and has a wide variety of applications in mathematics, computer science and control engineering. The procedure requires symbolic manipulation, numerical calculation and formal mathematical analysis. A prototype tool implementing the procedure takes advantage of the existing Maple-PVS link to provide reliable mathematics and the QEPCAD-PVS link to utilise existing quantifier elimination techniques.

The procedure is currently applicable to functions of $\mathbb{R}^2$ while the prototype tool implements the decision procedure for functions of $\mathbb{R}$ in formulae containing a single quantified variable. Future work includes extending the

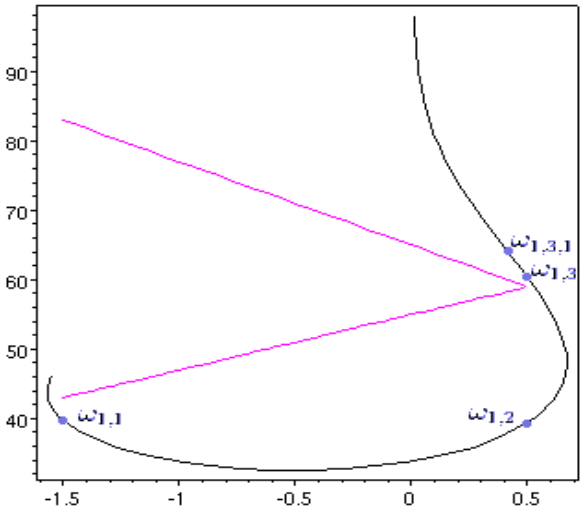


Fig. 3. Parametric plot of Y against X showing lines $l_{1,1}$ and $l_{1,2}$.

decision procedure to functions of higher dimensions, improving efficiency of the current prototype tool and extending its capabilities to include deciding sentences involving functions of higher dimensions with a larger number of quantified variables.

References

[1] A Adams, M Dunstan, H Gottliebsen, T Kelsey, U Martin, and S Owre. Computer algebra meets automated theorem proving: Integrating Maple and PVS. In R. J Boulton and P. B Jackson, editors, *Proceedings of the 14th International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2001)*, volume 2152 of *Lecture Notes in Computer Science*, pages 27–42. Springer-Verlag, 2001.

[2] H Anai and V Weispfenning. Deciding linear–trigonometric problems. In C Traverso, editor, *ISSAC '00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation*, pages 14–22. ACM Press, 2000.

[3] C Ballarin, K Homann, and J Calmet. Theorems and algorithms: an interface between isabelle and maple. In A. H. M Levelt, editor, *ISSAC '95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 150–157. ACM Press, 1995.

[4] A Bauer, E Clark, and X Zhao. Analytica – an experiment in combining theorem proving and symbolic computation. *Journal of Automated Reasoning*, 21(3):295–325, 1998.

[5] B Buchberger, T Jebelean, F Kriftner, M Marin, E Tomuta, and D Vasaru. A survey of the theorema project. In W Kuechlin, editor, *ISSAC '97: Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, pages 384–391. ACM Press, 1997.

[6] B. F Caviness and J. R Johnson, editors. *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Springer Wien NewYork, 1998.

[7] A Dolzmann. Solving geometric problems with real quantifier elimination. Technical Report Rep. MIP-9903, Universität Passau, 1999.

[8] A Dolzmann and T Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, 1997.

[9] R. C Dorf and R. H Bishop. *Modern Control Systems*. Prentice-Hall, ninth edition, 2001.

[10] Action Group FM(AG08). Robust flight control design challenge problem formulation and manual: the high incidence research model (HIRM). Technical Report TP-088-4, version 3, Group for Aeronautical Research and Technology in Europe (GARTEUR), 1997.

[11] J Harrison and L Théry. Reasoning about the reals: the marriage of HOL and maple. In A Voronkov, editor, *Logic programming and automated reasoning: proceedings of the 4th international conference, LPAR '93*, volume 698 of *Lecture Notes in Computer Science*, pages 351–359. Springer-Verlag, 1993.

[12] H Hong. Qepcad. Available at http://www.cs.usna.edu/~qepcad/B/QEPCAD.html.

[13] SRI International. PVS. Available at http://pvs.csi.sri.com.

[14] M Jirstrand. Nonlinear control system design by quantifier elimination. *Journal of Symbolic Computation*, 24(2):137–152, 1997.

[15] M Kerber, M Kohlhase, and V Sorge. Integrating computer algebra into proof planning. *Journal of Automated Reasoning*, 21(3):327–355, 1998.

[16] Maplesoft. Maple. Available at http://www.maplesoft.com/products/maple/.

[17] A Seidenberg. A new decision method for elementary algebra. *Annals of Math*, 60:365–374, 1954.

[18] A Tarski. *A Decision method for elementary algebra and geometry*. University of California Press, 1951.

[19] A Tiwari. PVS-QEPCAD. Available at http://www.csl.sri.com/users/tiwari/qepcad.html.

[20] V Weispfenning. Simulation and optimization by quantifier elimination. *Journal of Symbolic Computation*, 24(2):189–208, 1997.

[21] V Weispfenning. Deciding linear-exponential problems. *SIGSAM Bullettin*, 34(1):30–31, 2000.