Mechanized Reasoning for Continuous Problem Domains (Extended Abstract)

R.D. Arthan

Lemma 1 Ltd.
2nd Floor, 31A Chain Street, Reading RG1 2HX, UK
& Department of Computer Science,
Queen Mary, University of London, London E1 4NS, UK
rda@lemma-one.com

Abstract. Specification and verification in continuous problem domains are key topics for the practical application of formal methods and mechanized reasoning. I discuss one approach to linear continuous control systems and consider the challenges and opportunities raised for mechanized reasoning. These include practical implementation and integration issues, algorithms in computational real algebraic geometry and hard open questions such as the Schanuel conjecture. I conclude with an overview of some recent new results on decidability and undecidability for vector spaces and related theories.

1 Introduction

For some years, I have been involved with tools used for formally specifying and verifying digital subsystems of avionics control systems [2]. The models used in this work typically have discrete time and continuous data. These discrete models emerge only at the end of a chain of refinements starting from a purely continuous top-level model of the overall system. To apply formal verification techniques earlier in the chain could offer significant benefits in the shape of increased dependability, early detection of defects, and reduction in validation costs. Practical techniques for mechanized reasoning about continuous problem will be a key factor in obtaining these benefits.

To understand the challenges that formal verification of continuous systems offers for mechanized reasoning, it is helpful to do some methodological thinking. In the first part of the talk, I give an overview of an approach to linear continuous systems that builds on the well-known ideas of Hoare logic that have proved so fruitful in program verification. It turns out that linearity makes this approach very tractable given adequate support for reasoning about the mathematical problem domains involved, namely vector spaces, typically with some additional structure such as an inner product or a norm.

However, some significant problems arise from this. While the first order theory of the real field is decidable, in practice, engineers will want to work with the kind of rich vocabulary supported by typical computer algebra systems; so even to deal with the field of scalars in our vector spaces, we may need to go well beyond the usual first order theory of the real numbers. Moreover, even if we have some solution to this problem or have an application in which a simple language for the scalars is adequate, we need methods for reasoning about vector spaces. In the second part of the talk, I will describe some new results on decidability and undecidability for various theories of inner product spaces and normed vector spaces (including Hilbert spaces and Banach spaces). It turns out that the very uniform geometric and algebraic properties of inner product spaces lead to decidable theories, while, with only trivial exceptions, theories of normed vector spaces are undecidable. Nonetheless, the universal fragment admits a decision procedure. I believe there is plenty of scope for interesting and useful further research in this area.

2 Reasoning about linear systems

Let us consider an approach to reasoning about linear systems proposed in [1]. By reusing some well-known ideas from software specification and verification, this approach is designed to be modular and scalable. It deals with a type of model supported by widely used tools such as Simulink. These tools allow a system to be expressed as a signal flow graph formed by wiring together primitive components.

As an example, Figure 1 represents a mechanical system in which a force f acts on a cart of mass m attached to a wall by a spring with spring constant, k. It is a graphical representation of the following differential equation:

$$m\ddot{x}(t) + kx(t) - f(t) = 0.$$

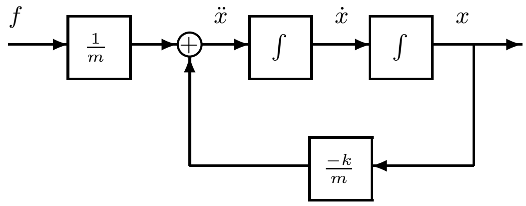

Fig. 1. A Linear Signal Flow Graph

The arrows in the diagram suggest a distinction between inputs and outputs that is missing from the differential equation. They let us view figure 1 as specifying the function mapping the force function f to the position function x. With this intensional viewpoint, the diagram might serve, for example. as a design for an analogue computer that simulates the mechanical system.

The lists of real-valued functions of time that appear as the lists of inputs and outputs to the primitive components in our diagram form vector spaces over the field $\mathbb{R}$ of real numbers. Moreover, the primitive components of the diagram represent linear transformations on those vector spaces (integration, scalar multiplication and addition). Such diagrams are called *linear signal flow graphs* and are very common in engineering practice. From now on we restrict our attention to linear signal flow graphs.

In the example of figure 1 the diagram happens to be a function, but, in general, a differential equation may not have a unique solution for a given initial condition. So in general a diagram denotes an input/output relation that is not necessarily total or single-valued. Rather than trying to ban partial or multi-valued relations, we will deal with them by borrowing some ideas from the world of relational specification of programs. This turns out to work particularly nicely given the algebraic structure we have to hand.

We write $r : X \leftrightarrow Y$ to denote that r is a relation between the sets X and Y, i.e., a subset of $X \times Y$, and use $x \underline{r} y$ as a shorthand for $(x, y) \in r$. If r and s are relations, $(r; s)$ denotes the relational composition r followed by s, so that $x \underline{(r; s)} y$ iff there is a z with $x \underline{r} z$ and $z \underline{s} y$. If $r : X \leftrightarrow Y$, $r^{-1} : Y \leftrightarrow X$ is the relational inverse of r, defined by taking $x \underline{r^{-1}} y$ iff $y \underline{r} x$. We write Ar for the image of a set A under the relation r. So if $r : X \leftrightarrow Y$, then $\mathsf{dom}(r) = Yr^{-1}$ is the domain of r, $\mathsf{ran}(r) = Xr$ is its range and r acts as a relation between any sets A and B such that $\mathsf{dom}(r) \subseteq A$ and $\mathsf{ran}(r) \subseteq B$.

If $r : X \leftrightarrow Y$, $A \subseteq X$ and $B \subseteq Y$, a *Hoare triple*, $\{A\}\, r\, \{B\}$, is the logical judgement which holds whenever $A \subseteq \mathsf{dom}(r)$ and $Ar \subseteq B$. A and B are referred to as the *pre-condition* and *post-condition* respectively. Hoare triples may be characterised in terms of weakest pre-conditions: the *weakest pre-condition*, $\mathsf{wp}(r, B)$, of B through r is the set of all points in the domain of r whose image under r is contained entirely in B. As is easily verified, the Hoare triple $\{A\}\, r\, \{B\}$ holds, iff $A \subseteq \mathsf{wp}(r, B)$.

The weakest pre-condition $\mathsf{wp}(r, B)$ contrasts with the pre-image Br^{-1} of B under r comprising all points whose image under r meets B. In general $\mathsf{wp}(r, B)$ is a proper subset of Br^{-1}. But if r is a function (not necessarily total), one has that $\mathsf{wp}(r, B) = Br^{-1}$. It turns out that something quite similar holds for the input/output relations defined by linear signal flow graphs.

In fact, the input/output relation between vector spaces V and W determined by a a linear signal flow graph is what is called an *additive relation* [8], i.e., a non-empty relation $r : V \leftrightarrow W$ that forms a subspace of $V \times W$. Additive relations generalise linear transformations. Like a linear transformation, an additive relation has a *kernel*, $\mathsf{ker}(r) = \{v : V \mid v \underline{r} 0\}$, which one can view as a uniform measure of the information lost by r. Dually, r has an *indeterminacy*, $\mathsf{ind}(r) = \{v : V \mid 0 \underline{r} v\}$, which one can view as a uniform measure of the non-determinism of r: if $v \underline{r} w$, then the set of elements related to v by r is $w + \mathsf{ind}(r)$. It turns out that to form the weakest pre-condition $\mathsf{wp}(r, B)$, one simply discards from B any element w for which $w + \mathsf{ind}(r)$ is not contained in B, and then $\mathsf{wp}(r, B)$ is the the pre-image through r of what remains. I.e., putting $B_0 = \{b : B \mid b + \mathsf{ind}(r) \subseteq B\}$ one has that $\mathsf{wp}(r, B) = B_0 r^{-1}$.

In figure 2 we show a set of constructors for forming new signal flow graphs from old. We call a signal flow graph a *structured block diagram* if it is formed from primitive components using these constructors. In [1], we prove that structured block diagrams are complete in the sense that subject to reasonable assumptions on the set of primitive components the input/output relation of an arbitrary signal flow graph can be expressed as the input/output relation of a structured block diagram (cf., the Turing completeness of while programs).

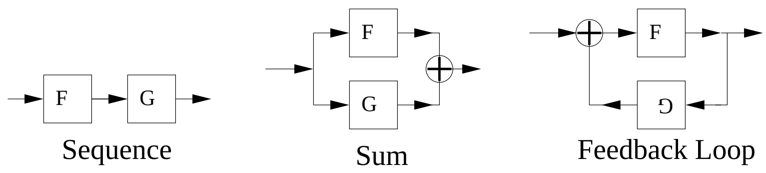

Fig. 2. Structured Block Diagram Constructors

Using the characterisation of the weakest pre-condition given above, we can then derive a Hoare logic for structured block diagrams. For example, we have the **linear combination rule**

$$\frac{\{A\}\,r\,\{B\} \quad \{A\}\,s\,\{B_1\}}{\{A\}\,\beta r + \gamma s\,\{\beta B + \gamma B_1\}}$$

Assuming we have a tractable characterisation of the primitive blocks, the Hoare logic reduces the problem of verifying any structured block diagram against given pre- and post-conditions reduces to a problem in the assertion language we are using to express the pre- and post-conditions.

For example, assume that we are working with finite-dimensional vector spaces $\mathbb{R}^m$, $m \in \mathbb{N}$ and that our primitive blocks are given by matrices with constant rational coefficients. Let us make assertions about vectors $(v_1, \ldots, v_m) \in \mathbb{R}^m$ using first order formulae in the language of the real field with free variables drawn from $v_1, \ldots v_m$. Then our approach automatically reduces any verification problem to a problem in the language of the real field. Thus, in contrast with the situation for programming languages, a large and natural class of signal flow graphs has a decidable verification problem, since, by a classic result of Tarski [11], the first order theory of the reals is decidable.

However, there are practical concerns: the time complexity of the decision procedure for the first order theory of the reals is provably doubly exponential in the number of bound variables in the formula (this theoretical bound being achieved by Collins' method of cylindrical algebraic decomposition [5]). The best known algorithms have the advantage of being at worst doubly exponential in the number of quantifier alternations [3], and that would be advantageous in the present context, but these have not yet been implemented.

As suggested in [1], if one restricts to so-called linear formulae, i.e., ones in which multiplication is restricted to have at least one operand constant, the more efficient method of Fourier-Motzkin-Hodes applies [7]. However, the restriction to linear formulae *and* rational coefficients would generally be too restrictive for practical use, since even simple properties such as $|v_1| < \sqrt{2}$ would not be expressible. Now Fourier-Motzkin elimination is effective over any subfield of the reals in which one can effectively compute. So one might consider linear formulae over arbitrary real algebraic numbers, but calculation with such numbers is possible but complex to implement [10]. Of course, engineers are also likely to want calculation with transcendental functions as well. Towards this, we have Macintyre and Wilkie's result that Schanuel's conjecture implies the decidability of the real exponential field [9]. So progress on a natural engineering problem may be contingent on a hard unsolved problem in pure mathematics!

3 Decidability for theories of vector spaces

A few years ago, on being asked by John Harrison about decidability for vector spaces, Robert M. Solovay promptly invented quantifier elimination procedures for a range of theories. Some special cases of these have so far been implemented and found very useful in practice [6]. Solovay also demonstrated that the theory of Banach spaces is undecidable. Since then Solovay, Harrison and I have simplified and extended these results and a full exposition is in preparation. Here I sketch some of the main results and methods.

We work in a two-sorted first order language with sorts $\mathcal{R}$ for scalars and $\mathcal{V}$ for vectors. The intended interpretation of the sort $\mathcal{R}$ is the set $\mathbb{R}$ of real numbers. We have function symbols $\_ + \_, \_ \times \_ : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ and $-\_ : \mathcal{R} \to \mathcal{R}$ which in the intended interpretations are the usual field operations on $\mathbb{R}$. We have function symbols $\_ + \_ : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$, $-\_ : \mathcal{V} \to \mathcal{V}$ and $\_ \times \_ : \mathcal{R} \times \mathcal{V} \to \mathcal{V}$ which in the intended interpretations make the set denoted by $\mathcal{V}$ into a real vector space. We have scalar constants $m/n : \mathcal{R}$ for each rational number m/n and we have the vector constant $\mathbf{0} : \mathcal{V}$ to be interpreted as the zero vector. The first order theory of real vector spaces is the set of sentences in our language that are valid in all the intended interpretations.

The theory of normed spaces is obtained by adding to the language a function symbol $||\_|| : \mathcal{V} \to \mathcal{R}$ whose intended interpretation is a norm on the vector space. A norm defines a metric on the set of vectors via $d(\mathbf{v}, \mathbf{w}) = ||\mathbf{v} - \mathbf{w}||$. Recall that a normed space is called a Banach space if it is complete with respect to this metric (i.e., if every Cauchy sequence converges).

The theory of inner product spaces is obtained by adding a function symbol $\langle \_, \_ \rangle : \mathcal{V} \times \mathcal{V} \to \mathcal{R}$ whose intended interpretation is an inner product. Recall that an inner product space that is also a Banach space under the norm defined by $||\mathbf{v}|| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ is called a Hilbert space.

We consider the theories of vector spaces, normed spaces, Banach spaces etc. with various restrictions on the dimension, e.g., the theory of all finite dimensional inner product spaces. We write IP, resp., $\mathsf{IP}^{\mathbb{F}}$, resp., IP^{∞} for the theories of real inner product spaces where the dimension is unconstrained, resp., constrained to be finite, resp., constrained to be infinite, and HS, $\mathsf{HS}^{\mathbb{F}}$ and HS^{∞} for the theories of Hilbert spaces with the corresponding constraints on the dimension. Completeness is guaranteed if the dimension is finite, so $\mathsf{IP}^{\mathbb{F}} = \mathsf{HS}^{\mathbb{F}}$.

A sentence in any of these languages that contains no vector-valued subexpressions is just a sentence in the first order language of the real field and its truth is independent of the interpretation of the vector sort. If we can eliminate all the vector quantifiers from a formula, then occurrences of the vector constant $\mathbf{0}$ can readily be eliminated to give an equivalent formula in the first order language of the real field.

If B is a basis for a vector space V, then we can define an inner product on V by requiring $\langle \mathbf{b}, \mathbf{b} \rangle = 1$ for $\mathbf{b} \in B$ and $\langle \mathbf{b}, \mathbf{c} \rangle = 0$ for $\mathbf{b}, \mathbf{c} \in B$ with $\mathbf{b} \neq \mathbf{c}$ and extending to V by bilinearity. Thus the theory of inner product spaces is a conservative extension of the theory of vector spaces and a decision procedure for the theory of inner product spaces is also a decision procedure for the theory of vector spaces.

The key to decidability for inner product spaces is the fact that it takes at most k degrees of freedom to decide a sentence containing k vector variables. I.e., a sentence P containing k vector variables is valid in all inner product spaces iff it is valid in $\mathbb{R}^n$ for $0 \leq n \leq k$. This is proved by considering a process that replaces vector quantifiers by blocks of scalar quantifiers. The process transforms a formula containing k vector variables into one which is equivalent in spaces of dimension at least k and in which vector variables only appear within arithmetic constraints on inner products $\langle \mathbf{v}, \mathbf{w} \rangle$, with $\mathbf{v}$, $\mathbf{w}$ free. Applying the process to a sentence P with k vector variables results in a sentence in the language of a real field which is equivalent in dimensions k or higher. From P one can effectively construct a sentence $P|_n$ containing no vector-valued subexpressions which is valid iff P is valid in $\mathbb{R}^n$. Writing D_n (resp. $D_{\leq n}$) for a sentence asserting that the dimension of the space is n (resp. at most n), one finds that P is equivalent to:

$$(D_0 \wedge P|_0) \vee (D_1 \wedge P|_1) \vee \ldots \vee (D_{k-1} \wedge P|_{k-1}) \vee (\neg D_{\leq (k-1)} \wedge P|_k)$$

Applying the quantifier elimination algorithm for the first order theory of the reals to the subformulae $P|_n$, this leads to the following result:

Theorem 1 *The theories* IP, $\mathsf{IP}^{\mathbb{F}}$, IP^{∞}, HS, $\mathsf{HS}^{\mathbb{F}}$ *and* HS^{∞} *are all decidable.*

When we consider decidability for normed spaces we find that even the theory of 2-dimensional spaces is undecidable and actually admits a primitive recursive reduction of second order arithmetic. The proof uses the following fact that is well-known to descriptive set theorists and others, but seems not to have appeared in the literature in quite the form we need.

Theorem 2 *Let K be a (many-sorted) first-order language including a sort $\mathcal{R}$, constants $0 : \mathcal{R}$ and $1 : \mathcal{R}$ and function symbols $\_ + \_, \_ \times \_ : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ whose intended interpretations form the field of the real numbers. Let $\mathcal{M}$ be some class of structures for K in which $\mathcal{R}$ and these symbols have their intended interpretations and let $\mathcal{T}$ be the theory of $\mathcal{M}$, i.e., the set of all sentences valid in every member of $\mathcal{M}$. If there is a formula $N(x)$ of K with one free variable x of sort $\mathcal{R}$ such that in some structure in the class $\mathcal{M}$, $N(x)$ defines the set of natural numbers (i.e., $\{x : \mathbb{R} \mid N(x)\} = \mathbb{N}$), then there is a primitive recursive reduction of second order arithmetic to $\mathcal{T}$.*

Here is a sketch of the proof: one can write down a sentence Nat which asserts that the subset of the reals defined by $N(x)$ satisfies the Peano axioms, and then, in any structure for the language in which the reals have their intended interpretation, Nat holds iff $N(x)$ does indeed define the natural numbers. Now if P is any sentence in the language of Peano arithmetic, we may view P as a sentence in the first order language of the reals and then construct a new sentence P^* by relativizing all quantifiers to $N(x)$ (i.e., $\forall x \cdot Q$ is replaced by $\forall x \cdot N(x) \Rightarrow Q$ and $\exists x \cdot Q$ is replaced by $\exists x \cdot N(x) \wedge Q$). But then the sentence $\mathsf{Nat} \Rightarrow P^*$ is in $\mathcal{T}$ iff it P is valid in arithmetic. This gives a reduction of first order arithmetic to $\mathcal{T}$. A reduction of second order arithmetic is obtained in a similar way using real numbers to represent sets of natural numbers, e.g., using n-ary expansions.

So, for example, this gives a very simple proof that the first order theory of metric spaces is undecidable: in the metric space Z whose elements are the integers with the distance defined by $d(\mathbf{p}, \mathbf{q}) = |\mathbf{p} - \mathbf{q}|$, we can clearly define the natural numbers by the formula $N(x) := \exists \mathbf{p}\ \mathbf{q} \cdot x = d(\mathbf{p}, \mathbf{q})$. By the above theorem, the theory of metric spaces must therefore admit a primitive recursive reduction of second order arithmetic and hence is undecidable.

Write NS, resp., NS^n, resp., $\mathsf{NS}^{\mathbb{F}}$, resp., NS^{∞} for the theories of normed spaces where the dimension is unconstrained, resp., constrained to be n, resp., constrained to be finite, resp., constrained to be infinite, and write BS, BS^n etc. for the theories of Banach spaces with the corresponding constraints on the dimension. We have the following theorem which implies that with the exception of $\mathsf{NS}^1 = \mathsf{BS}^1$ (which is the same as the the theory of the real field) all of these theories are undecidable.

Theorem 3 *There is a primitive recursive reduction of second order arithmetic to each of the theories BS, BS^{∞}, NS, $\mathsf{NS}^n = \mathsf{BS}^n$, $\mathsf{NS}^{\mathbb{F}} = \mathsf{BS}^{\mathbb{F}}$, and NS^{∞} $(n \geq 2)$.*

The proof is based on a construction of a 2-dimensional normed space X in which a certain first order formula defines the natural numbers as a subset of the field of scalars. By theorem 2, this immediately gives the result for $\mathsf{NS}^2 = \mathsf{BS}^2$ and $\mathsf{NS}^{\mathbb{F}} = \mathsf{BS}^{\mathbb{F}}$. The other parts of the result follow by considering the cartesian product of X and a Hilbert space of appropriate dimension. X is constructed by taking the norm whose unit disc is the "infinigon" D shown in figure 3. D is the convex hull of the set comprising the two vectors $\pm\mathbf{e}_1$ together with the unit vectors $\pm\mathbf{v}_i$ on the lines through the origin and the points $(i, 1)$, $i \in \mathbb{Z}$.

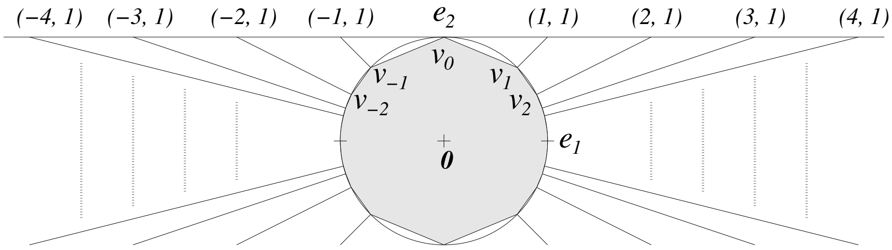

Fig. 3. The unit disc in the space X

Observing that the points $\pm\mathbf{v}_i$ are the isolated extreme points of the unit disc, while the only non-isolated extreme points are the points $\pm\mathbf{e}_1$, one finds that the language of normed spaces is sufficiently expressive for us to characterise the set of points $(i, 1)$ for $i \in \mathbb{Z}$ and then it is easy to give a formula $N(x)$ which defines the natural numbers in X.

We say a formula is *additive* if the left operand of all multiplications in the formula are rational constants. With a little care one can arrange for the formula $N(x)$ above to be additive and then with a little more geometric effort, one can give an additive formula $M(x, y, z)$ that in X defines the graph of the multiplication function $\_ \times \_ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. A variant of theorem 2 can then be used to show that the that even the purely additive fragments of the various theories of normed spaces and Banach spaces are undecidable.

On the positive side for normed spaces, we have the following result on the existence of norms:

Theorem 4 *Let $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be vectors in a real vector space V and $b_1, \ldots, b_n$ be real numbers. Then there exists a norm $||\_||$ on V such that $||\mathbf{x}_i|| = b_i$ for all $1 \leq i \leq n$ iff:*

- *For all $1 \leq i \leq n$, $b_i \geq 0$.*
- *For all $1 \leq i \leq n$, if $b_i = 0$ then $\mathbf{x}_i = 0$*
- *For each $1 \leq k \leq n$ there are no real numbers $c_1, \ldots, c_n$ such that some $\mathbf{x}_k = \sum_{i=1}^{n} c_1 \mathbf{x}_i$ with $\sum_{i=1}^{n} |c_i| b_i < b_k$.*

Now a quantifier-free formula P in the language of normed spaces containing k free vector variables has a model iff it has a model of dimension k (since in any model the subspace W spanned by the interpretations of the free vector variables is again a model of dimension $n \leq k$ and then $W \times \mathbb{R}^{k-n}$ gives a model of dimension k). From this observation and theorem 4, one can effectively transform P into a formula in the first order language of the real field that is satisfiable iff P is. This gives a decision procedure for purely universal formulae in the language of normed spaces. For purely additive formulae, there is a more efficient procedure which uses a parametrised linear programming algorithm to reduce the problem to linear real arithmetic. An implementation of the latter procedure in HOL Light has proved to be a useful tool.

4 Concluding Remarks

The approach to specification and verification of linear systems presented in section 2 is simple and natural. But even in the simple case of finite-dimensional inner product spaces, there are difficult issues to be addressed for mechanized proof support. The decision procedures of section 3 give a starting point, but our undecidability results show that there is much to be done in identifying useful tractable fragments of theories and good heuristics. There are many fascinating challenges ahead for mechanized reasoning in continuous problem domains.

Acknowledgments

I thank Colin O'Halloran and Nick Tudor of QinetiQ for encouraging and informing my interest in control systems. The approach to reasoning about linear systems is joint work with Ursula Martin, Erik Arne Mathiesen and Paulo Oliva and was supported by EPSRC grants GR/M98340 and GR/L48256. The work on decidability and undecidability for vector spaces is joint work with Robert M. Solovay and John Harrison.

References

1. R. D. Arthan, U. Martin, E. A. Mathiesen, and P. Oliva. Reasoning About Linear Systems. In *SEFM'07*. IEEE Press, 2007.
2. R.D. Arthan, P. Caseley, C. O'Halloran, and A.Smith. ClawZ: Control Laws in Z. In *3rd International Conference on Formal Engineering Methods (ICFEM 2000)*. IEEE, 2000.
3. Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2006.
4. H. Brakhage, editor. *Second GI Conference on Automata Theory and Formal Languages*, volume 33 of *LNCS*. Springer-Verlag, 1976.
5. G. E. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. In Brakhage [4], pages 134–183.
6. John Harrison. A HOL Theory of Euclidean Space. In Joe Hurd and Thomas F. Melham, editors, *Proceedings of TPHOLs 2005*, volume 3603 of *Lecture Notes in Computer Science*, pages 114–129. Springer, 2005.
7. Louis Hodes. Solving Problems by Formula Manipulation in Logic and Linear Inequalities. *Proceedings of the 4th International Joint Conference on Artificial Intelligence*, pages 553–559, 1971.
8. S. Mac Lane. *Homology*, volume 114 of *Der Grundlehren der mathematischen Wissenschaften*. Springer, 1975.
9. A. J. Macintyre and A. J. Wilkie. On the Decidability of the Real Exponential Field. In Piergiorgio Odifreddi, editor, *Kreiseliana: About and Around Georg Kreisel*, pages 441–467. A. K. Peters, 1996.
10. Renaud Rioboo. Towards Faster Real Algebraic Numbers. *J. Symb. Comput.*, 36(3-4):513–533, 2003.
11. Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.