Decision Problems in Geometry and Analysis

Rob Arthan

Lemma 1 Ltd./QMUL

Based on joint work with Robert M. Solovay and John Harrison

See `http://arxiv.org/abs/0904.3482`, submitted to APAL

PCV Seminar, University of Bath 3rd December 2009

0. Plan

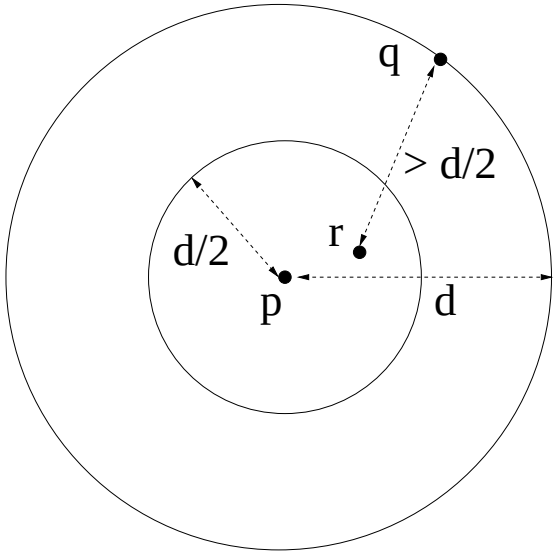
1. Introduction and Background
2. $\mathcal{L}_R$
3. $\mathcal{L}_M$
4. $\mathcal{L}_V$, $\mathcal{L}_I$ and $\mathcal{L}_N$
5. A little challenge problem
6. Concluding Remarks

1. Introduction: Background and Goals

- Mechanized theorem-proving:
  - Interactive HOL: HOL-IV, Isabelle, ProofPower, Coq, PVS etc.
  - Automatic: SMT systems, QEPCAD, etc.
  - Inside CAS: REDLOG, Chiron, etc.
- Applications:
  - Engineering: e.g., safety-critical control systems in avionics
  - Mathematics: e.g., Hales's Flyspeck project
- Continuous structures: e.g. metric spaces or real vector spaces
- What useful theories or fragments of theories are decidable?
- Undecidability results focus attention on useful fragments

Motivation: Formal Development of Analysis

- If p, q and r are in $\mathbb{R}$, standard automation will prove things like:
  $|p - q| = d \wedge |p - r| < d/2 \Rightarrow |q - r| > d/2$
- What if p, q and r are in $\mathbb{C}$?



- All that matters is that $\mathbb{C} = \mathbb{R}^2$, so what about $\mathbb{R}^n$ for any n?

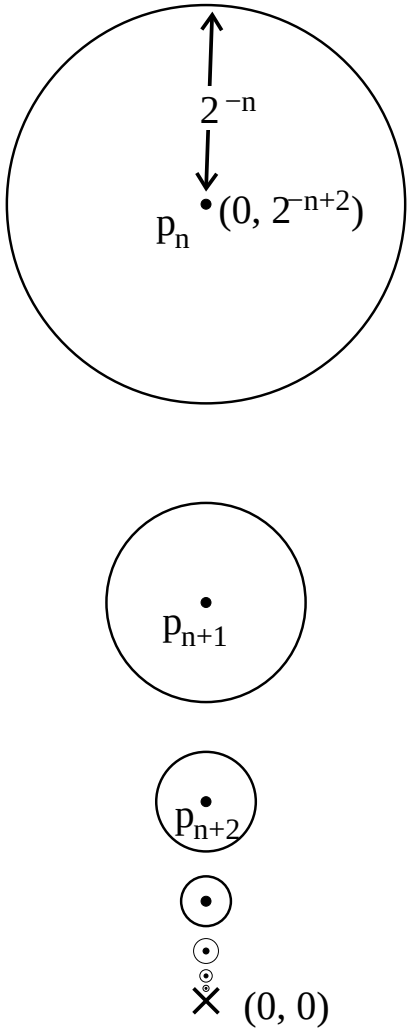
2. The First-Order Theory of the Reals

- Single-sorted first-order language $\mathcal{L}_R$ with a sort $\mathcal{R}$ and:
  - Field operations: $- : \mathcal{R} \to \mathcal{R}$, $+, \times : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$
  - Constants: m/n ($n \neq 0$, $m, n \in \mathbb{N}$) (or just 0 and 1)
  - Ordering: $<$
- Intended interpretation: the real numbers $\mathbb{R}$.
- The theory of the $\mathcal{L}_R$-structure $\mathbb{R}$ is decidable (Tarski 1930s).
- Practical implementations based on C.A.D. by Collins 1970s.
- Theory has many models, e.g., the field $\mathcal{A}$ of real algebraic numbers
- First-order language insensitive to metric completeness

3. Metric Spaces: Basic Concepts

- $\mathcal{L}_M$ is a two-sorted expansion of $\mathcal{L}_R$ with a sort $\mathcal{V}$ of *points*
- Metric function: $d : \mathcal{V} \times \mathcal{V} \to \mathcal{R}$
  - $\forall \mathbf{x}\ \mathbf{y} \cdot\ d(\mathbf{x}, \mathbf{y}) \geq 0 \wedge (d(\mathbf{x}, \mathbf{y}) = 0 \Leftrightarrow \mathbf{x} = \mathbf{y})$
  - $\forall \mathbf{x}\ \mathbf{y} \cdot\ d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$
  - $\forall \mathbf{x}\ \mathbf{y}\ \mathbf{z} \cdot\ d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.
- Recall the second-order notion of metric completencess:
  - Say $\mathbf{x}_n, n = 1, 2, \ldots$ is a Cauchy sequence if:
    $\forall \epsilon > 0 \cdot\ \exists N \cdot\ \forall m, n \cdot\ m > n > N \Rightarrow d(\mathbf{x}_m, \mathbf{x}_n) < \epsilon$
  - A space is *metric complete* if every Cauchy sequence converges
  - E.g., the usual metric in the plane $\mathbb{R}^2$.
- Metric completeness has first-order consequences

Metric Spaces: Consequences of Incompleteness



This metric space $\mathbb{M} \subseteq \mathbb{R}^2$ is incomplete.

Define a sequence $\mathbf{p}_n$, where $\mathsf{P}(2^{-n}, \mathbf{p}_n)$ with

$$\begin{aligned} \mathsf{P}(x, \mathbf{p}) \quad &:= \quad (\exists \mathbf{q} \cdot\, \mathbf{q} \neq \mathbf{p} \wedge d(\mathbf{p}, \mathbf{q}) = x) \\ &\wedge \quad (\forall \mathbf{q} \cdot\, \mathbf{q} \neq \mathbf{p} \Rightarrow d(\mathbf{p}, \mathbf{q}) \geq x). \end{aligned}$$

There is a sentence R in $\mathcal{L}_M$ which says:

"$\mathbf{p}_n$ is Cauchy and has no limit".

So R is true in $\mathbb{M}$,

. . . but not in its completion $\mathbb{M} \cup \{(0, 0)\}$,

. . . or in any complete metric space.

But metric completeness isn't axiomatisable.

Metric Spaces: A Decidable Fragment I

Theorem: Let P be an $\exists\forall$ sentence in the language $\mathcal{L}_M$ of metric spaces, say $P \equiv \exists x_1, \ldots, x_n \cdot Q$ where Q is a $\forall$ formula. Then P has a model iff it has a finite model with at most $\mathsf{max}\{n, 1\}$ points.

Proof (Cf. Bernays-Schönfinkel) Let $\mathbf{p}_1, \ldots, \mathbf{p}_m$ list the variables of sort $\mathcal{V}$ amongst the x_i. Can assume $1 \leq m \leq n$. If P has a model, then there is a metric space M containing points $\mathbf{p}_1, \ldots, \mathbf{p}_m$ such that Q holds of $\mathbf{p}_1, \ldots \mathbf{p}_m$. Because Q is a $\forall$ formula, the subspace $\{\mathbf{p}_1, \ldots, \mathbf{p}_m\}$ of M is also a model of P and it is finite and has at most $\mathsf{max}\{n, 1\}$ points. ■

Corollary: The set of satisfiable $\exists\forall$ sentences in $\mathcal{L}_M$ is decidable.

Proof. Let P and Q and $\mathbf{p}_1, \ldots, \mathbf{p}_m$ be as above. Q and the axioms for a metric space amount to a first-order system of constraints expressible in the language $\mathcal{L}_R$ on the m^2 quantities $d_{ij} = d(\mathbf{p}_i, \mathbf{p}_j)$. P is satisfiable iff this system of constraints is satisifiable and that is decidable by Tarski. ■

Metric Spaces: A Decidable Fragment II

Corollary: The $\forall\exists$ fragment of the theory of metric spaces is decidable.

Proof. If R is an $\forall\exists$ sentence, then $\neg R$ is logically equivalent to an $\exists\forall$ sentence that is unsatisfiable iff R is valid. ■

- The additive fragment of $\mathcal{L}_R$ can be decided quite efficiently.
- The metric space axioms don't introduce multiplication.
- Harrison has an implementation for the additive $\forall\exists$ fragment.

The *additive* fragment bans $\times$. In $\mathcal{L}_R$ this is often called *linear arithmetic*.

4. Vector Spaces, Hilbert Spaces etc.: Executive Summary

- Consider vector spaces often with a norm or an inner product
- Work with or without assumption of metric completeness:
  - Complete normed space = Banach space
  - Complete inner product space = Hilbert space
- . . . and with or without constraints on dimension:
  - IP, IP^n, $\mathsf{IP}^{\mathbb{F}}$, IP^∞, HS, HS^n, $\mathsf{HS}^{\mathbb{F}}$, HS^∞, NS, NS^n, $\mathsf{NS}^{\mathbb{F}}$, NS^∞, BS, BS^n, $\mathsf{BS}^{\mathbb{F}}$ & BS^∞
- Theories for inner product spaces and Hilbert spaces are all decidable.
- Apart from $\mathsf{NS}^1 = \mathsf{BS}^1 = \mathsf{IP}^1$, theories for normed spaces and Banach spaces are highly undecidable.

The Formal Languages $\mathcal{L}_V$, $\mathcal{L}_I$ and $\mathcal{L}_N$

- Expand $\mathcal{L}_R$ by adding a new sort $\mathcal{V}$ for *vectors*.
- $\mathcal{L}_V$ (vector spaces) adds group operations:
  $$- : \mathcal{V} \to \mathcal{V}, \quad + : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$$
  and scalar multiplication:
  $$\times : \mathcal{R} \times \mathcal{V} \to \mathcal{V}.$$
- $\mathcal{L}_N$ (normed spaces) adds to $\mathcal{L}_V$ a norm:
  $$||\_|| : \mathcal{V} \to \mathcal{R}.$$
- $\mathcal{L}_I$ (inner product spaces) adds to $\mathcal{L}_N$ an inner product:
  $$\langle \_, \_ \rangle : \mathcal{V} \times \mathcal{V} \to \mathcal{R}$$
  with the norm required to be euclidean: $||\mathbf{v}|| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$.
- View $\mathcal{L}_N$ and $\mathcal{L}_I$ as expansions of $\mathcal{L}_M$ by defining
  $$d(\mathbf{p}, \mathbf{q}) := ||\mathbf{p} - \mathbf{q}||.$$

Some Examples

- Models are vector spaces or inner product spaces or normed spaces over $\mathbb{R}$
- E.g., $\mathbb{R}^n$ where if $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$
  $-\mathbf{v} = (-v_1, \ldots, -v_n), \quad \mathbf{v} + \mathbf{w} = (v_1 + w_1, \ldots, v_n + w_n)$
  $\lambda\mathbf{v} = (\lambda v_1, \ldots, \lambda v_n), \quad \langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=1}^{n} v_i w_i.$
- Spaces of real-valued functions provide ∞-dimensional examples:
  E.g., $C = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ with
  $(-f)(x) = -f(x), \quad (f + g)(x) = f(x) + g(x),$
  $(\lambda f)(x) = \lambda(f(x))$
  - $\langle f, g \rangle = \int_0^1 f(x)g(x)dx$ gives an inner product on C
  - $||f|| = \mathsf{sup}\{|f(x)| \mid x \in [0,1]\}$ gives a non-euclidean norm on C.

What can $\mathcal{L}_V$ or $\mathcal{L}_I$ say about a space?

With k vector variables you can specify the dimension is at most k:

$$D_{\leq k} := \exists \mathbf{v}_1, \ldots, \mathbf{v}_k \cdot \forall \mathbf{v} \cdot \exists a_1, \ldots, a_k \cdot \mathbf{v} = \sum_{i=1}^{k} a_i \mathbf{v}_i$$

or at least k:

$$D_{\geq k} := \exists \mathbf{v}_1, \ldots, \mathbf{v}_k \cdot \forall a_1, \ldots, a_k \cdot \sum_{i=1}^{k} a_i \mathbf{v}_i = \mathbf{0} \Rightarrow \bigwedge_{i=1}^{n} a_i = 0$$

Theorem A sentence of $\mathcal{L}_V$ or $\mathcal{L}_I$ containing k vector variables has a model iff it has a finite-dimensional model of dimension $\leq k$

Proof. A kind of quantifier elimination. See SA&H.■

It follows with a little more work that any sentence is equivalent to a propositional combination of the various $D_{\leq k}$ and $D_{\geq k}$.

Inner Product Spaces and Hilbert Spaces are Decidable

Corollary The theories IP, $\mathsf{IP}^{\mathbb{F}}$, IP^{∞}, HS, $\mathsf{HS}^{\mathbb{F}}$ & HS^{∞} are all decidable.

Proof To decide a sentence with k vector variables, test it in $\mathbb{R}^n$ for $0 \leq n \leq k$ using coordinates to reduce to $\mathcal{L}_R$ ■

E.g., to decide: $\forall \mathbf{p}, \mathbf{q} \cdot \langle \mathbf{p}, \mathbf{p} \rangle = \langle \mathbf{q}, \mathbf{q} \rangle = \langle \mathbf{p} + \mathbf{q}, \mathbf{p} + \mathbf{q} \rangle / 4 \Rightarrow \mathbf{p} = \mathbf{q}$,

i.e., $\forall \mathbf{p}, \mathbf{q} \cdot ||\mathbf{p}|| = ||\mathbf{q}|| = ||(\mathbf{p} + \mathbf{q})/2|| \Rightarrow \mathbf{p} = \mathbf{q}$,

for $\mathbb{R}^0$ test: $0 = 0 = 0 \Rightarrow 0 = 0$,

for $\mathbb{R}^1$ test: $p_1^2 = q_1^2 = (p_1 + q_1)^2/4 \Rightarrow p_1 = q_1$,

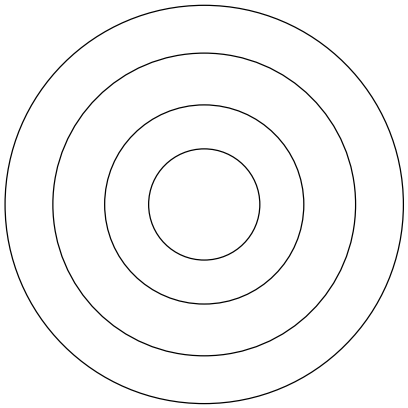
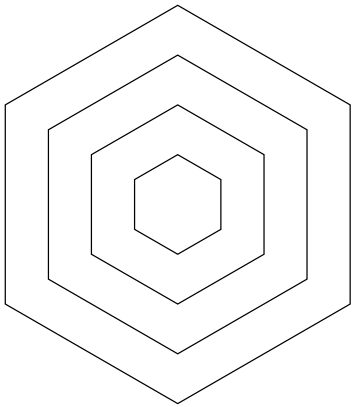
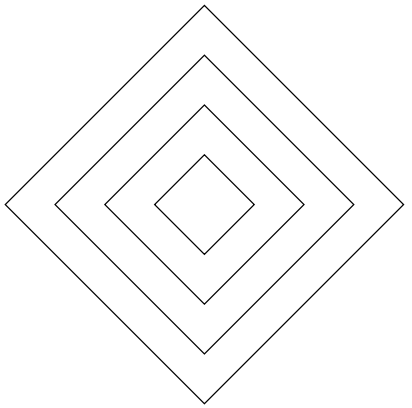
& for $\mathbb{R}^2$ test: $p_1^2 + p_2^2 = q_1^2 + q_2^2 = ((p_1 + q_1)^2 + (p_2 + q_2)^2)/4$

$\Rightarrow p_1 = q_1 \wedge p_2 = q_2$,

where $p_1, p_2, q_1, q_2 \in \mathbb{R}$.

Geometry of Normed Spaces

- Many norms on $\mathbb{R}^n$, e.g., the 1-norm or Manhattan taxi norm:
  $||\mathbf{v}||_1 = \sum_{i=1}^{n} |v_i|$
- Think of the norm as "cost of travel" in each direction
- The *unit disc* or *sphere* in a normed space is $\{\mathbf{v} \mid ||\mathbf{v}|| \leq 1\}$.
  - Circular disc in $\mathbb{R}^2$ under the standard norm
  - Meets each line through $\mathbf{0}$ in $[-\mathbf{p}, +\mathbf{p}]$ for some $\mathbf{p} \neq \mathbf{0}$
  - Any convex set with the above property determines a norm

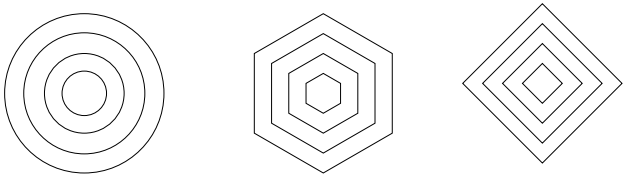




Expressive power of $||\_||$

- In a general normed space, points on the unit circle need not be extreme points:

$$\begin{aligned}\mathsf{E}(\mathbf{v}) \quad := \quad & ||\mathbf{v}|| = 1 \wedge \\ & \forall \mathbf{u}\ \mathbf{w}\cdot\, ||\mathbf{u}|| \leq 1 \wedge ||\mathbf{w}|| \leq 1 \wedge \mathbf{v} = (\mathbf{u}+\mathbf{w})/2 \Rightarrow \mathbf{u} = \mathbf{w}\end{aligned}$$

- If the dimension is finite, the Krein-Milman theorem implies that the unit disc is the convex hull of its extreme points.



- But the following sentence has models:

$$\mathsf{Inf} := (\exists \mathbf{v}\cdot\, \mathbf{v} \neq \mathbf{0}) \wedge (\forall \mathbf{v}\cdot\, \neg \mathsf{E}(\mathbf{v})).$$

A method for proving undecidability I

Work in some language $\mathcal{L}$ including $\mathcal{L}_R$. An $\mathcal{L}$-structure is *standard* if it interprets $\mathcal{R}$ as $\mathbb{R}$. Given a formula $N(x)$ in $\mathcal{L}$ $x : \mathcal{R}$ as its only free variable, define:

$$\begin{aligned} \mathsf{Peano} \quad := \quad & N(0) \wedge \\ & (\forall x \cdot\, N(x) \Rightarrow x \geq 0 \wedge N(x+1)) \wedge \\ & (\forall x\ y \cdot\, N(x) \wedge N(y) \wedge x \neq y \Rightarrow |x - y| \geq 1) \end{aligned}$$

Let A be a standard $\mathcal{L}$-structure satisfying Peano. Then $N(x)$ holds in A iff x is interpreted as a natural number. Let $Q(x_1, \ldots, x_n)$ be any quantifier-free formula in the language $\mathcal{L}_A$ of natural number arithmetic. Then

$$\mathbb{N} \models \exists x_1 \ldots x_n \cdot\, Q(x_1, \ldots, x_n)$$

iff

$$A \models \exists x_1 \ldots x_n \cdot\, N(x_1) \wedge \ldots N(x_n) \wedge Q(x_1, \ldots, x_n)$$

A method for proving undecidability II

- To prove undecidability of the theory of a class of structures $\mathcal{C}$, need just **one** structure A in which some $N(x)$ in $\mathcal{L}$ defines $\mathbb{N}$. For then:

$$\mathbb{N} \models \exists x_1 \ldots x_n \cdot Q(x_1, \ldots, x_n)$$

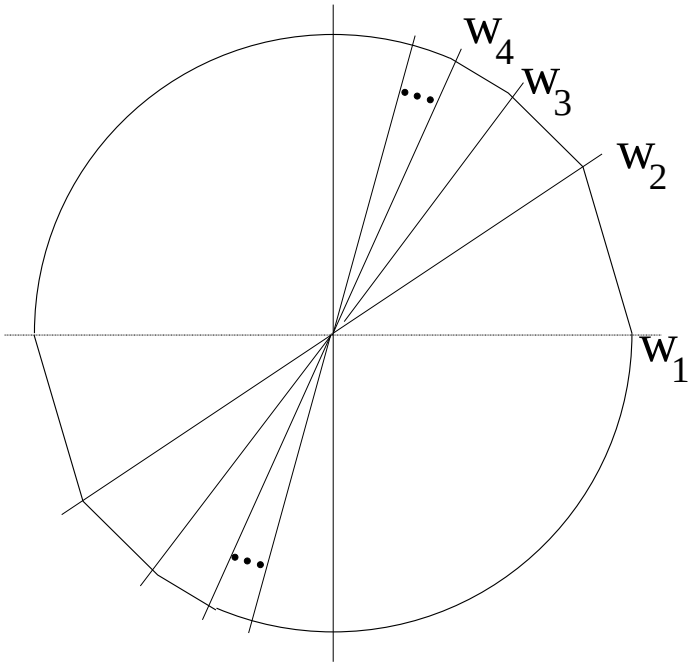
iff

$$\mathcal{C} \models \mathsf{Peano} \Rightarrow \exists x_1 \ldots x_n \cdot N(x_1) \wedge \ldots N(x_n) \wedge Q(x_1, \ldots, x_n)$$

  and satisfiability for quantifier-free formulas in $\mathcal{L}_A$ is undecidable by the famous resolution of Hilbert's 10^{th} problem by Matiyasevich.

- E.g., metric spaces are undecidable: take $A = \mathbb{N}$.
- The same data and a more involved argument give a reduction of second-order arithmetic to the theory of the class of structures $\mathcal{C}$.
- Can we define $\mathbb{N}$ in a normed space?

Can we define $\mathbb{N}$? ... Yes, we can!



Choose $\mathbf{w}_i$ so that $||\mathbf{w}_i - \mathbf{w}_{i-1}|| = \frac{1}{i!}$
Then $i+1 = \frac{||\mathbf{w}_i - \mathbf{w}_{i-1}||}{||\mathbf{w}_{i+1} - \mathbf{w}_i||}$,
$||\mathbf{w}_i - \mathbf{w}_1|| < \sum_{j=2}^{\infty} \frac{1}{j!} = e - 2 < 1$,
and $x \in \mathbb{N}$ iff $N(x)$ where:

$$N(x) :=$$
$$x = 0 \vee x = 1 \vee x = 2 \vee$$
$$\exists \mathbf{u}\ \mathbf{v}\ \mathbf{w} \cdot\ \mathbf{v} \neq \mathbf{w} \wedge$$
$$3 \leq x = \frac{||\mathbf{v}-\mathbf{u}||}{||\mathbf{w}-\mathbf{v}||} \wedge$$
$$\mathsf{E}(\mathbf{u}) \wedge \mathsf{E}(\mathbf{v}) \wedge \mathsf{E}(\mathbf{w}) \wedge$$
$$||(\mathbf{u}+\mathbf{v})/2|| = ||(\mathbf{v}+\mathbf{w})/2|| = 1$$

So $\mathsf{NS}^2 = \mathsf{BS}^2$, $\mathsf{NS}^{\mathbb{F}} = \mathsf{BS}^{\mathbb{F}}$, NS, BS and (with a bit more work) NS^n and BS^n for $n > 2$ are all undecidable.

Decidable fragments for Normed Spaces

- The $\exists$ fragment of NS is decidable but rather trivial.
- The $\exists\forall$ and $\forall\exists$ fragments are undecidable.

Theorem The set of $\forall$ sentences in the theory NS is decidable.

Proof (highlights): Every satisfiable $\exists$ formula is satisfiable in a normed space whose unit sphere is a polyhedron; Existence of the polyhedron reduces to a system of constraints expressible in $\mathcal{L}_R$. ■

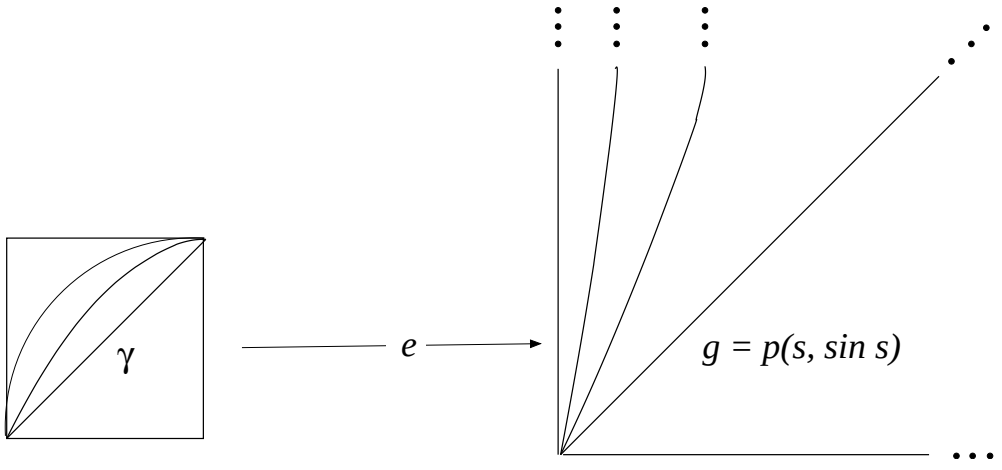
- The additive $\forall$ fragment is particularly tractable via a parametrised linear programming technique.
- Harrison has an implementation in HOL Light that can solve many of the motivating problems

Zero-th Order Real Number Theorem Proving

Interesting and of practical relevance to consider expanding the set of constants available in $\mathcal{L}_R$ to larger effective subfields of $\mathbb{R}$:

- $\mathbb{Q}$, $\mathbb{Q}[\sqrt{p/q} \mid p, q \in \mathbb{N}, q \neq 0]$ — easy
- $\mathcal{A} = \mathbb{Q}[\mathsf{RealRoots}(f) \mid f \in \mathbb{Q}[X]]$
  the ring of all algebraic numbers – doable, hard-ish
- $\mathcal{A} = \mathcal{A}[\mathsf{RealRoots}(f) \mid f \in \mathcal{A}[X]]$ — doable, harder
- $\mathbb{Q}[e]$, $\mathbb{Q}[\pi]$ — doable, hard-ish
- $\mathcal{A}[e]$, $\mathcal{A}[\pi]$ — doable, harder still
- $\mathbb{Q}[e, \pi]$ — very difficult open question: Schanuel's conjecture

5. A Little Challenge. Can we encode sin in a bounded concave γ?

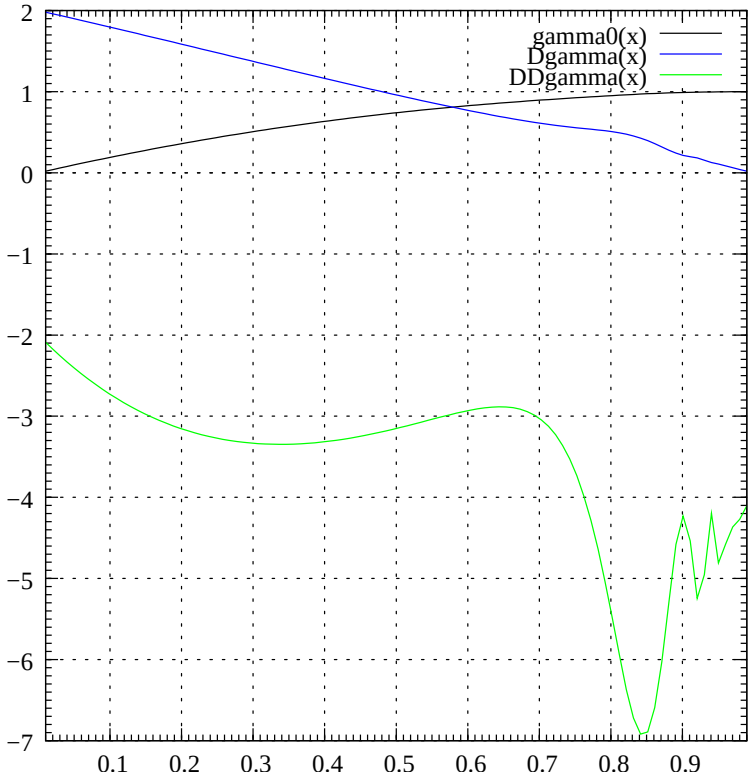


$$
\begin{array}{lrcl}
 & e(x,y) & = & (\frac{x}{1-x}, \frac{y}{1-y}) \\
\text{so} & \gamma(x) & = & q(g(p(x))) \\
\text{where} & p(x) & = & \frac{x}{1-x}, \quad q(s) = \frac{s}{1+s} \\
\text{and} & g(s) & = & Ks + s^2 + \frac{1}{M}\sin s
\end{array}
$$

Question: do any K and M in $\mathbb{N}_{>0}$ make γ concave?

Encoding sin in a bounded concave γ. II

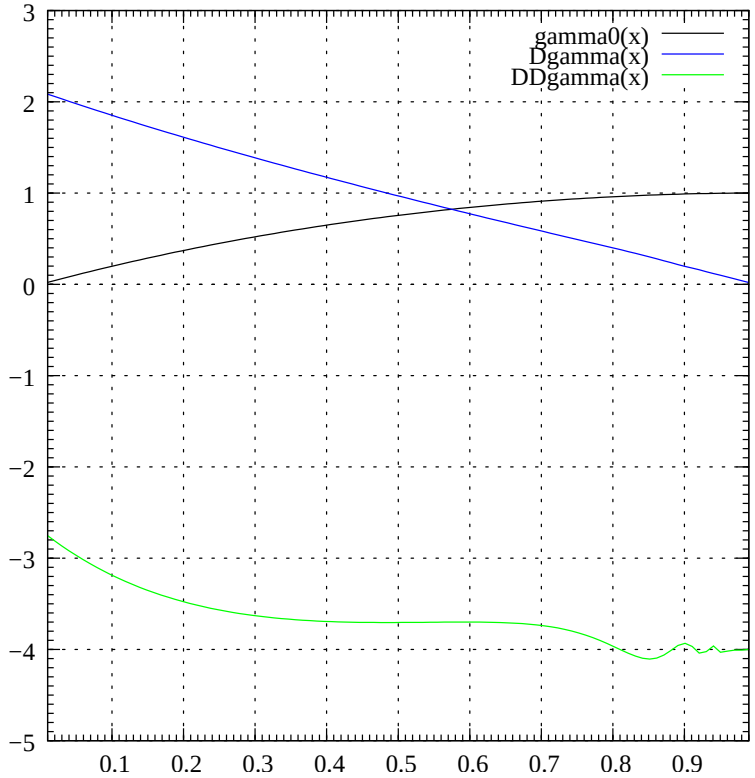
Answer: yes! Here are γ, γ' and γ'' for $K = M = 1$:



Can you **prove** $\gamma'' < 0$?

Encoding sin in a bounded concave γ. III

Answer: ah! well, I have a pen & paper proof for $K = 2$ and $M \geq 9$:



Challenge: is there any automation to help out there?

The challenge problem as a trigonometric polynomial

- γ is a trigonometric rational function.
- With $s = \frac{x}{1+x}$, $\gamma''(x)$ has the same sign as $h(s)$ where

$$\begin{aligned} h(s) &= (1 + Ks + s^2 + \tfrac{\sin s}{M})[(1+s)(2 - \tfrac{\sin s}{M}) + 2K + 4s + \tfrac{2\cos s}{M}] \\ &\quad - 2(1+s)(K + 2s + \tfrac{\cos s}{M})^2. \end{aligned}$$

- Solved by Tobias Nipkow for s in $(0, c)$ for reasonably large c using a procedure of Johannes Hölzl in Isabelle based on interval arithmetic.
- Solved by Amine Chaieb for s in (c, ∞) for large enough c using a procedure of his in Isabelle based on sums-of-squares.
- Larry Paulson's MetiTarski which combines resolution with QEPCAD is a contender but encounters some unresolved problems in parts of the range.

6. Concluding Remarks: Some More Undecidable Theories

TFTAU:

- Vector spaces over $\mathbb{R}$ equipped with an endomorphism.
- Ditto but even with scalars in $\mathbb{C}$ and the endomorphism unitary.
- Banach algebras (MacIntyre 1971)*.
- Finite-dimensional associative algebras over $\mathbb{R}$.
- Finite-dimensional Lie algebras over $\mathbb{R}$.

* The other claims are all fairly straightforward exercises and some follow from results proved or cited by MacIntyre (Annals of Mathematical Logic, 3(3). 1971).

Final Remarks

- Good to see real progress on proof automation.
- I hope this work will inform future practical and theoretical work — there are lots of interesting problems out there.
- An interesting possibility is weaker logics, e.g., the continuous logics that are in vogue in the model theory of Banach spaces.

Thank you!

Slides available at
`http://www.lemma-one.com/papers/papers.html`