Verifying real inequalities

Jeremy Avigad

Department of Philosophy

Carnegie Mellon University

http://www.andrew.cmu.edu/∼avigad

(joint work with Harvey Friedman)

A characterization of mathematics

For centuries, mathematics was viewed as the science of *quantity*:

- Geometry = study of magnitude (continuous quantities)
- Arithmetic = study of number (discrete quantities)

Comparisons between quantities are central to the subject.

We need better automated support for ordinary mathematical reasoning involving inequalities.

First example

Ramsey's theorem tells us that for every k there is an N large enough, so that no matter how one colors the edges of the complete graph on N vertices red and blue, there is a homogeneous subset of size k.

Here is a lower bound on N:

Theorem (Erdös) For all $k \geq 2$, if $N < 2^{k/2}$, there is a coloring of the complete graph on N vertices with no homogeneous subset of size k.

For $k = 2$ and $k = 3$ is it easy to check this by hand.

For $k \geq 4$, show that with nonzero probability, a random coloring has this property.

First example

For $k \geq 4$, suppose $N < 2^{k/2}$, and suppose we color each edge red with probability $1/2$.

The probability that any given subset of size k is homogeneous is $2^{-\binom{k}{2}+1}$.

So the probability of a homogeneous subset is at most $\binom{N}{k}2^{-\binom{k}{2}+1}$.

But $\binom{N}{k} = \frac{N(N-1)(N-2)\cdots(N-k+1)}{k(k-1)\cdots 1} \leq \frac{N^k}{2^{k-1}}$.

So we have

$$\binom{N}{k}2^{-\binom{k}{2}+1} \leq \frac{N^k}{2^{k-1}}2^{-\binom{k}{2}+1} < 2^{\frac{k^2}{2}-\binom{k}{2}-k+2} = 2^{-\frac{k}{2}+2} \leq 1.$$

Second example

Proposition. When $0 \leq x \leq 1/2$, we have $x - x^2 \leq \ln(1+x) \leq x$.

Let's do this without using the Maclaurin series! Suppose $0 \leq x \leq 1/2$.

From $e^x = 1 + x + x^2/2 + \ldots$, we have $e^x \geq 1 + x$ and hence $e^{x^2} \geq 1 + x^2$.

On the other hand, $e^x \leq 1 + x + x^2/2 + x^2/4 + x^2/8 + \ldots = 1 + x + x^2$. So we have

$$e^{x-x^2} = e^x / e^{x^2} \leq (1 + x + x^2)/(1 + x^2) \leq 1 + x,$$

by multiplying through.

Taking logarithms, we have $x - x^2 \leq \ln(1+x) \leq x$.

Third example

Here's an inequality that comes up in Shapiro's presentation of the Selberg proof of the prime number theorem.

Assuming

$$n \leq (K/2)x$$

$$0 < C$$

$$0 < \varepsilon < 1$$

we have

$$(1 + \frac{\varepsilon}{3(C+3)}) \cdot n < Kx$$

Reflection

Here's what these examples have in common:

- They are "typical."
- They are straightforward.
- They are quantifier-free.
- They rely on basic arithmetic inferences.
- Verifying them formally is (currently) a pain in the neck.

(Mild uses of quantifiers come in with phrases like "sufficiently large," or "choose $N >> x$.")

The challenge: figure out how to capture these automatically.

Real closed fields

Consider the first-order theory of $\langle \mathbb{R}, 0, 1, +, \times, < \rangle$.

Theorem (Tarski). T has *elimination of quantifiers*, that is, every sentence in the language is provably equivalent to one that is quantifier-free. Hence T is decidable.

Chronology:

- Alfred Tarski proved this around 1930 (finally published in 1948), based on Sturm's theorem.
- Abraham Robinson gave an easy model-theoretic proof in 1956, based on Artin-Schreier.
- George Collins gave a *practical* method in 1975.
- Sean McLaughlin and John Harrison have recently implemented a proof-producing version.

Real closed fields

But the story doesn't end here.

- RCF procedures are slow (and arguably misguided, for the types of inferences we are interested in).
- Worse: they do not extend to straightforward inferences with monotone functions, trigonometric functions, exponentiation and logarithm, etc.

Problem: nontrivial parts of mathematics are undecidable. Two options:

- Use full decision procedures in more restricted settings.
- Use "heuristic procedures" in more general settings.

Is there a middle ground? Let's consider some strategies.

Idea 1: work backwards

Work backwards, using, for example,

$$0 < s, 0 < t \Rightarrow 0 < st$$

and

$$0 < s < t \Rightarrow 1/t < 1/s.$$

But backchaining is nondeterministic. For example:

- We also have $s < 0, t < 0 \Rightarrow 0 < st$ and $s < t < 0 \Rightarrow 1/t < 1/s$.
- We can prove $s + t + u < r + v$ by proving $s + u < r$ and $t \leq v$.
- We can also prove $s + t + u < r + v$ by proving $s + u < r + 3$ and $t \leq v - 3$ or by proving $s < (r + v)/2$ and $t + u < (r + v)/2$.

Idea 2: work forwards

For example, from $n \leq (K/2)x$, $0 < C$, and $0 < \varepsilon < 1$, we have

- $C + 3 > 1$
- $3(C + 3) > 1$
- $\frac{\varepsilon}{3(C+3)} < 1$
- $1 + \frac{\varepsilon}{3(C+3)} < 2$

and hence

$$(1 + \frac{\varepsilon}{3(C+3)}) \cdot n < 2(K/2)x = Kx.$$

But clearly we need some guidance!

Idea 3: combine local procedures

Theorem. Suppose T_1 and T_2 are "stably infinite" and decidable. Suppose that the languages are disjoint, except for the equality symbol. Then the universal fragment of $T_1 \cup T_2$ is decidable.

In particular, if T_1 and T_2 have only infinite models, they are stably infinite.

This allows you to design decision procedures for individual theories and then put them together.

With additional hypotheses on the source theories, the decision procedures can be made efficient (Nelson-Oppen, Shostak, . . .).

Idea 3: combine local procedures

Theorem. The theory of $\langle \mathbb{R}, 0, +, < \rangle$ has quantifier-elimination, and so is decidable.

For universal formulas, Fourier-Motzkin is doubly exponential in principle, but works well in practice. More efficient methods are available (e.g. Weispfenning's "test point" method).

Theorem. The theory of $\langle \mathbb{R}, 1, \cdot, < \rangle$ has quantifier-elimination and so is decidable.

In fact, modulo case splits on the signs of terms, this reduces to the previous theorem.

Corollary. The universal fragment of the union of these two theories is decidable.

Idea 3: combine local procedures

The bad news: the union of the two theories just described doesn't include distributivity.

The good news: many inferences don't need it, except for constants (for example, $3(r + s) = 3r + 3s$).

The bad news: adding symbols for constants, or multiplication by constants, introduces nontrivial overlap between the languages. Nelson-Oppen methods break down.

General question: what happens when you combine local procedures, when the theories have nontrivial overlap?

A theory for real inequalities

Specifically: let $f_a(x) = ax$ for rational constants a.

Let $T_{add}[\mathbb{Q}]$ be the theory of $\langle \mathbb{R}, 0, 1, +, -, <, \ldots, f_a, \ldots \rangle$.

Let $T_{mult}[\mathbb{Q}]$ be the theory of $\langle \mathbb{R}, 0, 1, \times, \div, \sqrt[n]{\cdot}, <, \ldots, f_a, \ldots \rangle$.

Let $T_{common}[\mathbb{Q}] = T_{add}[\mathbb{Q}] \cap T_{mult}[\mathbb{Q}]$.

Let $T[\mathbb{Q}] = T_{add}[\mathbb{Q}] \cup T_{mult}[\mathbb{Q}]$. This theory seems to be very useful.

$T_{add}[\mathbb{Q}]$, $T_{mult}[\mathbb{Q}]$, $T_{common}[\mathbb{Q}]$ all have quantifier elimination.

But the presence of the new symbols in the common language makes the situation much more complex.

A theory for real inequalities

Think of $T[\mathbb{Q}]$ as:

- real-closed fields without distributivity (except for constants)
- a shotgun wedding of the additive and multiplicative theories.

It seems to cover very many "obvious" calculations.

Theorem. Let $f(x_1, \ldots, x_k)$ be a polynomial over $\mathbb{Q}$. Then f is nonzero on $[0, 1]^k$ if and only if $T[\mathbb{Q}]$ proves that fact.

This provides a lower bound on the strength of $T[\mathbb{Q}]$ on universal assertions. For an upper bound:

Theorem. $T[\mathbb{Q}]$ proves $\forall x \ (x^2 - 2x + 1 \geq \varepsilon)$ if and only if $\varepsilon < 0$.

In fact, the size of a minimal interpolant depends on ε.

A theory for real inequalities

Here are some of our results.

- $T[\mathbb{Q}]$ has good normal forms.
- Valid equations are independent of the ordering.
- $T[\mathbb{Q}]$ is undecidable.
- In fact, the $\forall\forall\forall\exists \ldots \exists$ fragment is complete r.e.
- Assuming that the solvability of Diophantine equations in the rationals is undecidable, then so is the existential fragment of $T[\mathbb{Q}]$.

Most important:

- The universal fragment of $T[\mathbb{Q}]$ *is* decidable.

More generally, we consider theories $T[F]$, for arbitrary computable subfields F of $\mathbb{R}$.

Decidability of the universal fragment

Let $\forall \vec{x}\ \varphi(\vec{x})$ be a universal formula of $T[F]$.

By introducing variables to name subterms, we can reprexpress this as

$$\varphi \equiv \forall \vec{x}\ (\varphi_{add}(\vec{x}) \vee \varphi_{mult}(\vec{x}))$$

where φ_{add} and φ_{mult} are in the languages of $T_{add}[F]$, $T_{mult}[F]$, respectively.

Theorem. $T[F]$ proves $\forall \vec{x}\ \varphi$ iff there is a quantifier-free "interpolant" $\theta(\vec{x})$ in the language of $T_{common}[F]$ such that

- $T_{add}[F] \cup \{\neg\varphi_{add}(\vec{x})\} \vdash \theta(\vec{x})$
- $T_{mult}[F] \cup \{\neg\varphi_{mult}(\vec{x})\} \vdash \neg\theta(\vec{x})$.

Decidability of the universal fragment

In the Nelson-Oppen setting, there are only finitely many possible interpolants.

The language of $T_{common}[F]$ has atomic formulas $x_i \leq ax_j$, $x_i < ax_j$. (We can assume each $x_i > 0$, and $x_1 = 1$.)

Difficulties:

- There are infinitely many constants.
- There is no a priori bound on the size of the interpolant.
- Constants come from the subfield, F.

Nonetheless, with work, one can develop an algorithm to determine whether there is such an interpolant.

Decidability of the universal fragment

Theorem. The following are equivalent:

1. $T[F]$ doesn't prove φ.
2. The union of $T_{add}[F] \cup \{\neg\varphi_{add}(\vec{x})\}$ and $T_{mult}[F] \cup \{\neg\varphi_{mult}(\vec{x})\}$ is consistent.
3. There is a complete type $\Gamma(\vec{x})$ in $T_{common}[F]$ such that
   - $T_{add}[F] \cup \{\neg\varphi_{add}(\vec{x})\} \cup \Gamma(\vec{x})$ and
   - $T_{mult}[F] \cup \{\neg\varphi_{mult}(\vec{x})\} \cup \Gamma(\vec{x})$

   are both consistent.

$T[F] \vdash \varphi$ iff for every complete type $\Gamma(\vec{x})$ in the language of $T_{common}[F]$, there is a finite subset $\Gamma'(\vec{x})$ such that either

$$\forall\vec{x}\ (\bigwedge \Gamma'(\vec{x}) \to \varphi_{add}(\vec{x})) \quad \text{or} \quad \forall\vec{x}\ (\bigwedge \Gamma'(\vec{x}) \to \varphi_{mult}(\vec{x}))$$

holds in the reals.

Decidability of the universal fragment

One can characterize all the complete types, $\Gamma(\vec{x})$, in terms of what they say about pairs $\{x_i, x_j\}$.

With work, the assertion above can be expressed by a restricted class of formulas in the language of real closed fields, with a predicate for F.

With more work, one can show that this class is decidable (assuming F is computable and $F \cap \mathbb{A}$ is decidable).

Undecidability

Theorem. There is a model of $T[F]$ where the solutions to the equation

$$x(1+x) = x + x^2$$

are exactly the $x \in F$.

Corollary. An existential sentence φ over F if and only if in any model of $T[F]$, φ has witnesses among the a with $a(1+a) = a + a^2$.

Corollary. If Diophantine equations in the rationals are unsolvable, then so is the set of existential consequences of $T[\mathbb{Q}]$.

Undecidability

Theorem. There is a model of $T[F]$ and elements μ, κ, λ such that solutions $x \in [1, \mu]$ to

$$(\kappa + x)(\lambda + x) = \kappa\lambda + \kappa x + \lambda x + x^2$$

are exactly the positive integers.

Corollary. Let φ be a Diophantine equation over the positive integers. Then φ has a solution in the positive integers if and only for every model $\mathcal{M}$ of $T[F]$, and every $\mu, \kappa, \lambda \in \mathcal{M}$, if

$$\{x \in [1, \mu] \mid (\kappa + x)(\lambda + x) = \kappa\lambda + \kappa x + \lambda x + x^2\}$$

contains 1 and is closed under $+1$, then φ has solutions in that set.

Corollary. The set of $\forall\forall\forall\exists \ldots \exists$ consequence of $T[F]$ is complete r.e.

Normal forms

One can simultaneously define normal forms and an ordering on terms in normal form.

$$4(1 + 3x_1 + 4x_1x_7)^2(x_1^2x_2^3 + 4x_3^2x_9^2)^3$$

Two terms are provably equal if and only if they have the same normal form.

In that case, they are provably equal in the theory without the ordering.

Heuristic procedures

Our decidability results are not practical. But the proofs provide ideas and guidelines.

We propose the following strategy: given a sequent

$$r_1 < s_1, r_2 \leq s_2, \ldots, r_k < s_k \Rightarrow t < u,$$

put all terms in normal form, and try to refute

$$r_1 < s_1, r_2 \leq s_2, \ldots, r_k < s_k, u \leq t.$$

To do this, you need to find an interpolant.

Iteratively use the additive and multiplicative parts to derive new inequalities, $p < aq$ or $p \leq aq$, between "subterms."

Heuristic procedures

Disadvantages:

- The procedure is not complete (need disjunctions).
- The procedure may not terminate.
- Need to consider arbitrary pairs of subterms.

Advantages:

- The method has the right flavor: forward reasoning, but focusing on "potentially useful" comparisons.
- It includes arithmetic and multiplicative decision procedures.
- It works on the kinds of examples I described above.

We expect that the method will work well in practice, but experimentation is needed.

Heuristic procedures

The method is, furthermore, open-ended and extensible:

- One can judiciously incorporate distributivity.
- One can judiciously incorporate disjunctions (case splits).
- One can add rules for e^x, $\ln x$, sin, cos, ...
- One can add general rules for monotone functions.

There are:

- interesting implementation issues
- interesting theoretical issues

Conclusions

Formally verified mathematics is becoming increasingly important:

- Proofs are getting very complex.
- Proofs rely on extensive computations.

New approaches are needed:

- Interesting fragments of mathematics are undecidable.
- Heuristic procedures are brittle, hard to extend, and unpredictable.

What we need are *principled* search procedures:

- Build heuristics on sound theory.
- Pay attention to data, and develop more useful classifications of mathematical contexts.

The work holds many engineering and theoretical challenges.