Lightweight Verification of Formal Reasoning

Andrei Lapets

Background and Motivation

Many formal verification systems exist [Wie03]. Why are contemporary systems not adopted and used more widely?

Obstacles and Disincentives

- Unfamiliar syntax and/or environment.
- Unnatural, cumbersome bottom-up structure (fixed logic, emphasis on induction, limited libraries).
- Lack of flexibility to make use of features and benefits selectively (heavyweight or lightweight).

Our Approach

We forego the prevalent assumption that in order to be of any value, automated formal verification must guarantee absolute correctness w.r.t. a specific model.

In most real-world applications, formally verified claims are only as correct as the fidelity of the problem's representation within the model: only ***relative*** correctness is guaranteed.

Guiding Principles

- "Implicit arguments, explicit results."

  No model- or tool-specific annotations, pure "forward compatible" representation.
- Familiar concrete syntax.

  A strict subset of English, LaTeX, and MediaWiki markup, aiding with "backwards compatibility" in terms of usability and easy integration with new or existing editing/content management tools (e.g. http://www.safre.org).

Table 1: Example of a verifiably consistent argument.

First, we introduce some assumptions about integers and rational numbers.
Assume for any $i \in \mathbb{Z}$, there exists $j \in \mathbb{Z}$ s.t. $i = 2 \cdot j$ implies that i is even.
Assume for any $i \in \mathbb{Z}$, i^2 is even implies that i is even.
Assume for any $i \in \mathbb{Z}$, i is even implies that there exists $j \in \mathbb{Z}$ s.t. $i = 2 \cdot j$.
Assume that for any $q \in \mathbb{Q}$, there exist $n \in \mathbb{Z}, m \in \mathbb{Z}$ s.t. n and m have no common factors and $q = n/m$.
Assume for any $x, y, z \in \mathbb{R}$, if $z = x/y$ then $y \cdot z = x$.
Assume that if there exist $i, j \in \mathbb{Z}$ s.t. i is even, j is even, and i and j have no common factors then we have a contradiction.

Now, we present our main argument. We want to show that $\sqrt{2}$ is irrational. We will proceed by contradiction.
Assume that $\sqrt{2} \in \mathbb{Q}$.
Assert that there exist $n, m \in \mathbb{Z}$ s.t. n and m have no common factors and $\sqrt{2} = n/m$.
Therefore, $m \cdot \sqrt{2} = n$,
$(m \cdot \sqrt{2})^2 = n^2$,
$m^2 \cdot \sqrt{2}^2 = n^2$,
$m^2 \cdot 2 = n^2$,
$n^2 = m^2 \cdot 2$,
$n^2 = 2 \cdot m^2$, and so, n^2 is even. Thus, n is even.
Furthermore, there exists $j \in \mathbb{Z}$ s.t. $n = 2 \cdot j$,
$n^2 = (2 \cdot j)^2$,
$n^2 = 2^2 \cdot j^2$,
$n^2 = 4 \cdot j^2$,
$2 \cdot m^2 = 4 \cdot j^2$,
$m^2 = 2 \cdot j^2$,
m^2 is even and m is even.
Thus, we have a contradiction.

Verification Technique

Verification occurs with respect to a standard collection of symbolic logical inference rules found in propositional logic, FOL, HOL, etc.

Table 2: Template for logical inference rules.

$$[\text{Assumption}]\ \frac{e \in \Phi \quad FV(e) \subset \Delta}{\Delta;\Phi \vdash e}$$

$$[\Rightarrow\text{-Intro}]\ \frac{\Delta;\Phi \cup \{e_1\} \vdash e_2}{\Delta;\Phi \vdash e_1 \Rightarrow e_2} \qquad [\Rightarrow\text{-Elim}]\ \frac{\Delta;\Phi \vdash e_1 \Rightarrow e_2 \quad \Delta;\Phi \vdash e_1}{\Delta;\Phi \vdash e_2}$$

$$[\wedge\text{-Intro}]\ \frac{\Delta;\Phi \vdash e_1 \quad \Delta;\Phi \vdash e_2}{\Delta;\Phi \vdash e_1 \wedge e_2} \qquad [\wedge\text{-Elim-L}]\ \frac{\Delta;\Phi \vdash e_1 \wedge e_2}{\Delta;\Phi \vdash e_1} \qquad [\wedge\text{-Elim-R}]\ \frac{\Delta;\Phi \vdash e_1 \wedge e_2}{\Delta;\Phi \vdash e_2}$$

$$[\forall\text{-Intro}]\ \frac{\Delta, \overline{x}; \Phi \cap \{e \mid FV(e) \cap \overline{x} = \emptyset\} \vdash e}{\Delta;\Phi \vdash \forall \overline{x}.e} \qquad [\forall\text{-Elim}]\ \frac{\Delta;\Phi, \vdash \forall \overline{x}.e \quad |\overline{e}| = |\overline{x}| \quad \overline{e} \subset D \quad FV(\overline{e}) \subset \Delta}{\Delta;\Phi \vdash e[\overline{x} \mapsto \overline{e}]}$$

$$[\exists\text{-Intro}]\ \frac{\Delta;\Phi \vdash e[\overline{x} \mapsto \overline{e}] \quad |\overline{e}| = |\overline{x}| \quad \overline{e} \subset D \quad FV(\overline{e}) \subset \Delta}{\Delta;\Phi, \vdash \exists \overline{x}.e}$$

Relative Consistency: Specific models can be chosen by restricting the domain over which variables are quantified.

Small Context Assumption and Search

Assertions are verified by searching the local context Φ, which is typically small, to depth d:

$$O\Big(\big(|e| \cdot |e^*| \cdot |\Phi|\big)^d\Big).$$

Many common algebraic manipulations on expressions that contain pre-defined constant symbols (such as $+$, $\cdot$, $\cup$, $\cap$, etc.) are automatically checked using multiple, distinct normalization procedures.

References

[Wie03] Freek Wiedijk. Comparing mathematical provers. In *MKM '03: Proceedings of the Second International Conference on Mathematical Knowledge Management*, pages 188–202, London, UK, 2003. Springer-Verlag.

Advisor: Assaf Kfoury