Towards the Automation of Proofs in Real Analysis

Luís Cruz-Filipe

July 12, 2002

University of Nijmegen, The Netherlands
Centro de Lógica e Computação, Portugal

Overview

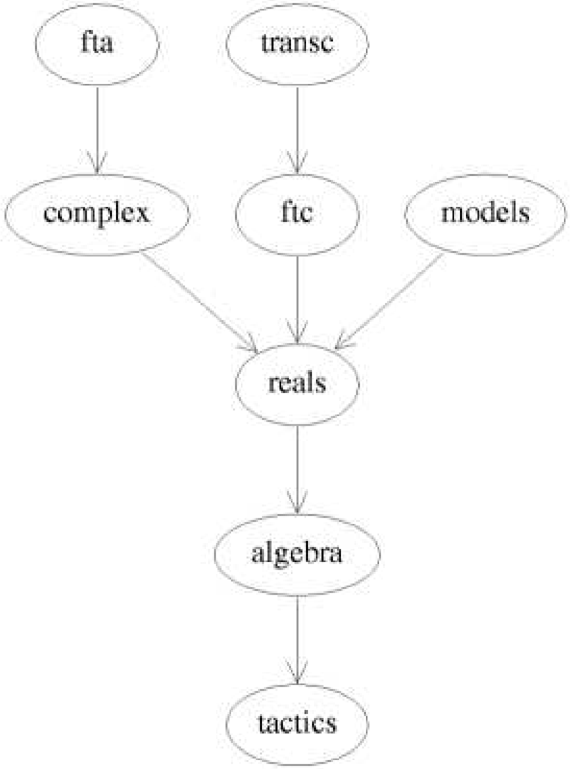
1. Introduction

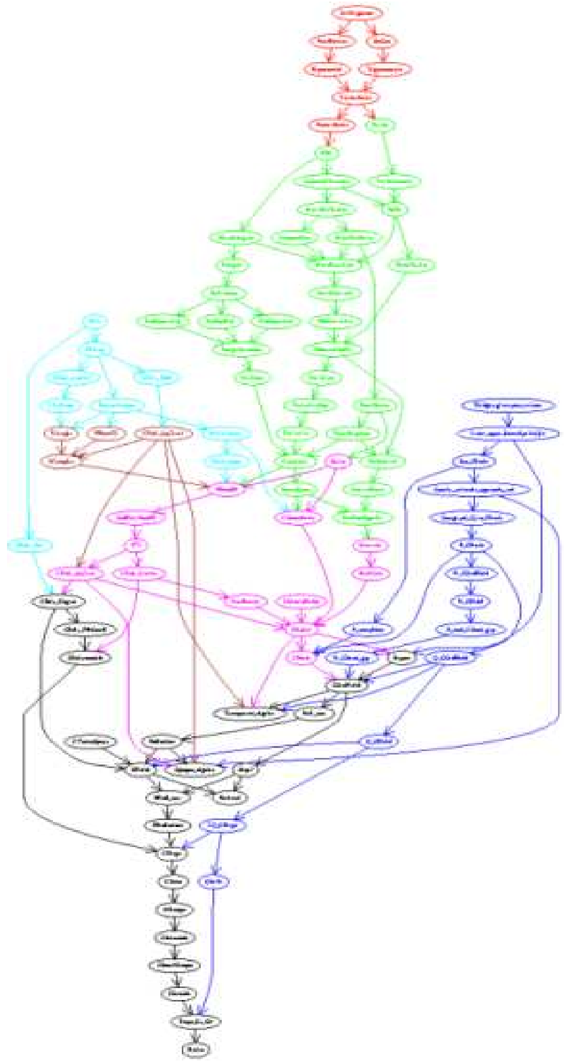
2. The Library of Real Analysis

3. The `Hints` mechanism

4. The Reflection mechanism

5. Conclusions and Future Work


fta
transc
complex
ftc
models
reals
algebra
tactics



Goal: $\forall_{x \in \mathbb{R}} \sin(2x) = (\cos(x) + \sin(x))^2 - 1$

$$\begin{aligned}
\sin(2x) &= 2\sin(x)\cos(x) \\
&= 2\sin(x)\cos(x) + 1 - 1 \\
&= 2\sin(x)\cos(x) + (\cos^2(x) + \sin^2(x)) - 1 \\
&= (\cos^2(x) + \sin^2(x) + 2\cos(x)\sin(x)) - 1 \\
&= (\cos(x) + \sin(x))^2 - 1
\end{aligned}$$

Goal: $\forall_{x \in \mathbb{R}} \sin(2x) = (\cos(x) + \sin(x))^2 - 1$

$$
\begin{aligned}
\sin(2x) &= 2\sin(x)\cos(x) \\
&= 2\sin(x)\cos(x) + 0 \\
&= 2\sin(x)\cos(x) + (1 + (-1)) \\
&= 2\sin(x)\cos(x) + 1 + (-1) \\
&= 2\sin(x)\cos(x) + 1 - 1 \\
&= 2\sin(x)\cos(x) + (\cos^2(x) + \sin^2(x)) - 1 \\
&= 2(\sin(x)\cos(x)) + (\cos^2(x) + \sin^2(x)) - 1 \\
&= 2(\cos(x)\sin(x)) + (\cos^2(x) + \sin^2(x)) - 1 \\
&= 2\cos(x)\sin(x) + (\cos^2(x) + \sin^2(x)) - 1 \\
&= (\cos^2(x) + \sin^2(x) + 2\cos(x)\sin(x)) - 1 \\
&= (\cos(x) + \sin(x))^2 - 1
\end{aligned}
$$

Goal: $\forall_{x\in\mathbb{R}} \mathrm{ch}^2(x) - \mathrm{sh}^2(x) = 1$

$$
\begin{aligned}
\mathrm{ch}^2(x) - \mathrm{sh}^2(x) &= \left(\frac{e^x + e^{-x}}{2}\right)^2 - \left(\frac{e^x - e^{-x}}{2}\right)^2 \\
&= \frac{\left(e^x + e^{-x}\right)^2}{2^2} - \frac{\left(e^x - e^{-x}\right)^2}{2^2} \\
&= \frac{\left(e^x + e^{-x}\right)^2 - \left(e^x - e^{-x}\right)^2}{2^2} \\
&= \frac{\left[(e^x)^2 + \left(e^{-x}\right)^2 + 2e^x e^{-x}\right] - \left[(e^x)^2 + \left(e^{-x}\right)^2 - 2e^x e^{-x}\right]}{4} \\
&= e^x e^{-x} \\
&= 1
\end{aligned}
$$

Reflection

Aim Solve through symbolic computation decision problems, that is, given a domain $\mathbb{D}$ and a predicate $P : \mathbb{D}^n \rightarrow \mathbf{Prop}$ automatically prove goals of the form $P(x_1, \ldots, x_n)$.

Process

1. Encoding in an (inductive) type $\mathbb{S}$;
2. Interpretation $[\![\cdot]\!] : \mathbb{S} \rightarrow \mathbb{D}$;
3. Decision function $f : \mathbb{S}^n \rightarrow \{0, 1\}$;
4. Lemma $L : \forall_{e_1,\ldots,e_n : \mathbb{S}} [(f(e_1, \ldots, e_n) = 1) \rightarrow P([\![e_1]\!], \ldots, [\![e_n]\!])]$.

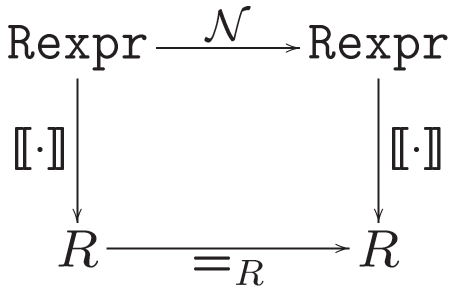
Example: Equality in Rings

```
Rexpr : Set := Rvar : nat->Rexpr
             | Rint : Z->Rexpr
             | Rplus : Rexpr->Rexpr->Rexpr
             | Rmult : Rexpr->Rexpr->Rexpr
```

- Interpretation as expected;

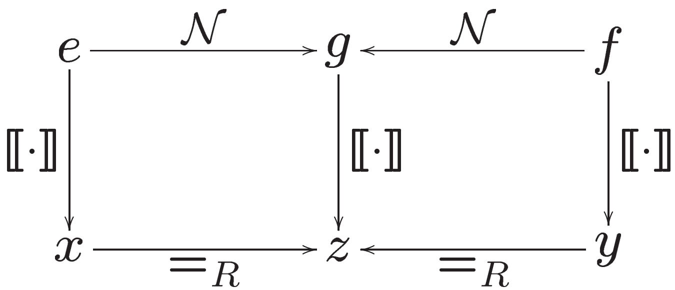
- Normalization function $\mathcal{N} : \texttt{Rexpr} \to \texttt{Rexpr}$;

- Lemma: $\forall_{e:\texttt{Rexpr}} [\![e]\!] =_R [\![\mathcal{N}(e)]\!]$.



Given $x, y : R$,

- find $e, f :$ `Rexpr` s. t. $[\![e]\!] = x$, $[\![f]\!] = y$;
- supposing that $\mathcal{N}(e) = \mathcal{N}(f) = g$ s. t. $[\![g]\!] = z$,



Lemma: $\forall_{e_1, e_2 : \texttt{Rexpr}} (\mathcal{N}(e_1) = \mathcal{N}(e_2)) \rightarrow [\![e_1]\!] =_R [\![e_2]\!]$

Partial Reflection

- $[\![\cdot]\!]$ is partial (functional relation);

- The lemma now reads:

$$
\begin{aligned}
L : \forall_{e_1,\ldots,e_n:\mathbb{S}} \quad & ([\![e_1]\!]\downarrow) \to \ldots \to ([\![e_n]\!]\downarrow) \to \\
& [(f(e_1,\ldots,e_n) = 1) \to P([\![e_1]\!],\ldots,[\![e_n]\!])]
\end{aligned}
$$

Sometimes we can internalize the proofs in the expressions:

- $\overline{\mathbb{S}} = \left\{\overline{\mathbb{S}}_d : d \in \mathbb{D}\right\}$;
- a forgetful map $|\cdot| : \overline{\mathbb{S}} \to \mathbb{S}$;
- a *total* interpretation $[\![\cdot]\!]' : \overline{\mathbb{S}} \to \mathbb{D}$

such that

- for every $e : \overline{\mathbb{S}}$, $[\![|e|]\!]\downarrow$ and $[\![|e|]\!] = [\![e]\!]'$;
- for every $e : \overline{\mathbb{S}}_d$ we have $[\![e]\!]' = d$.

Given $x_1, \ldots, x_n : \mathbb{D}$

- find $e_1 \in \overline{\mathbb{S}}_{x_1}, \ldots, e_n \in \overline{\mathbb{S}}_{x_n}$;
- then $[\![|e_1|]\!] \downarrow, \ldots, [\![|e_n|]\!] \downarrow$;
- and $[\![e_1]\!]' = x_1, \ldots, [\![e_n]\!]' = x_n$;
- compute $f(|e_1|, \ldots, |e_n|)$;
- apply L.

Applications:

$\rightarrow$ Equality in Fields;

$\rightarrow$ Given partial functions f, g, prove that $f' = g$

Conclusion

The best way to prove equalities is by an intelligent combination of both mechanisms.

Future Work

- New tactic `RealEq` to prove equalities between real numbers

  This tactic should know about:

  $$|\cdot|, \exp, \log, x^y, \sin, \cos, \arcsin, \arccos, \ldots$$

- Improve tactics for reasoning in real analysis (continuity proofs, derivative relation);

- Automatically integrate rational functions.