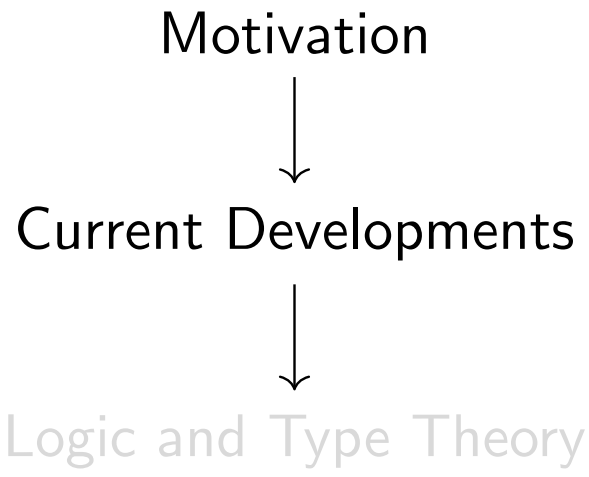
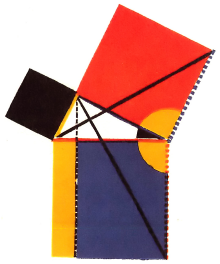
Rigour and Automated Theorem Proving

Hernán Ibarra


Motivation
Current Developments
Logic and Type Theory

I. Motivation

Why do you do mathematics?



IN *a right angled triangle*  *the ſquare on the hypotenuſe* —— *is equal to the ſum of the ſquares of the ſides,* (—— *and* ——).

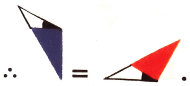
On ——, —— and —— deſcribe ſquares, (pr. 46.)

Draw ·····‖ - - - - - (pr. 31.)
alſo draw —— and ——.

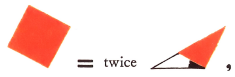
 ,

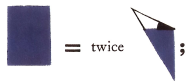
To each add  ∴  ,

—— = - - - - - and —— = ·····;

∴  .

Again, becauſe —— ‖ ·····

 ,

and  ;

∴  .

In the ſame manner it may be ſhown

that  ;

hence  .

Q. E. D.

be previously understood. And what are these fluxions? The velocities of evanescent increments? And what are these same evanescent increments? They are neither finite quantities, nor quantities infinitely small, nor yet nothing. May we not call them the ghosts of departed quantities?

$$\frac{\sin x}{x} = (1-\frac{x}{\pi})(1+\frac{x}{\pi})(1-\frac{x}{2\pi})(1+\frac{x}{2\pi})$$
$$(1-\frac{x}{3\pi})(1+\frac{x}{3\pi})\dots$$

COURS D'ANALYSE

DE

L'ÉCOLE ROYALE POLYTECHNIQUE;

PAR M. AUGUSTIN-LOUIS CAUCHY,

Ingénieur des Ponts et Chaussées, Professeur d'Analyse à l'École polytechnique,
Membre de l'Académie des sciences, Chevalier de la Légion d'honneur.

I.re PARTIE. *ANALYSE ALGÉBRIQUE.*

DE L'IMPRIMERIE ROYALE.

Chez DEBURE frères, Libraires du Roi et de la Bibliothèque du Roi,
rue Serpente, n.° 7.

1821.


-300
1687
1730
1821
1910

***54·43.** $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51·231] $\equiv . \iota`x \cap \iota`y = \Lambda .$

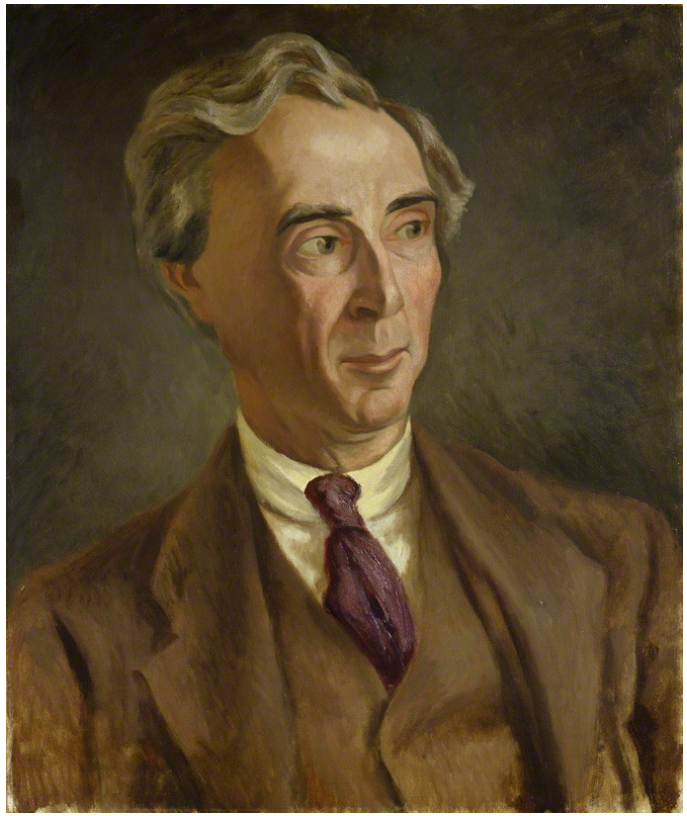
[*13·12] $\equiv . \alpha \cap \beta = \Lambda$ (1)

$\vdash . (1) . *11{\cdot}11{\cdot}35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda$ (2)

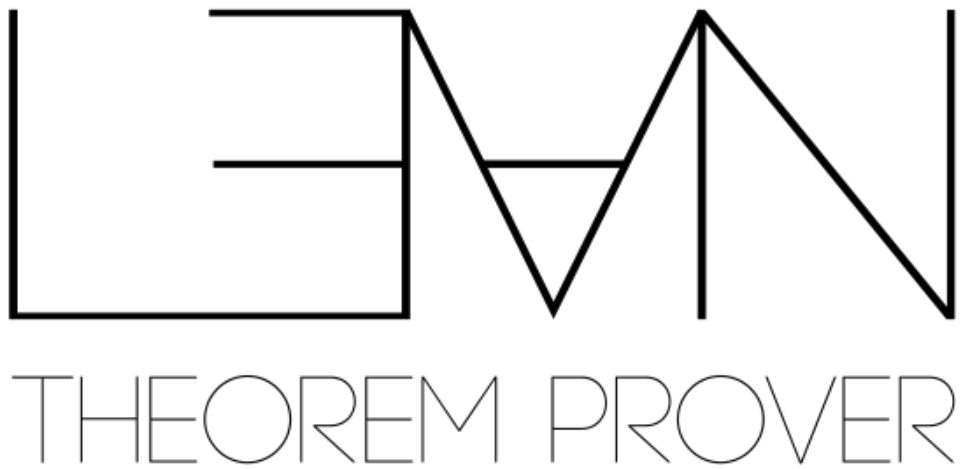
$\vdash . (2) . *11{\cdot}54 . *52{\cdot}1 . \supset \vdash .$ Prop

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.



Bertrand Russell, *Portraits from Memory*, Reflections on my Eightieth Birthday

II. Current Developments



The Future: Interactive Theorem Provers

- Review process
- Pedagogy
- Projects

The Future: Automatic Theorem Provers

III. Logic and Type Theory

III. Logic and Type Theory

- Set Theory: "Everything is a set"
- Category Theory: "Everything is an arrow"
- Type Theory: "Everything has a type"

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} \\
2 &:= \{0, 1\} \\
3 &:= \{0, 1, 2\} \\
&\vdots
\end{aligned}
$$

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} \\
2 &:= \{0, 1\} \\
3 &:= \{0, 1, 2\} \\
&\vdots
\end{aligned}
$$

$$(x, y) := \{x, \{x, y\}\}$$

Pop Quiz

1. $14 \in 66$
2. $1 \in 0$
3. For all x and y, $x \in (x, y)$
4. For all x and y, $y \in (x, y)$
5. $2 = (0, 0)$
6. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$

Pop Quiz

1. $14 \in 66$ T
2. $1 \in 0$ F
3. For all x and y, $x \in (x, y)$ T
4. For all x and y, $y \in (x, y)$ F
5. $2 = (0, 0)$ T
6. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ F

$$3 : \mathbb{N}$$

$$\pi : \mathbb{R}$$

$$3 : \mathbb{N}$$

$$\pi : \mathbb{R}$$

$$\mathbb{N}, \mathbb{R} : \textsc{Type}$$

If A and B are types

$$A \to B$$

If A and B are types

$$A \times B$$

comes with

$$\begin{aligned} p_1 : A \times B &\to A \\ (a, b) &\mapsto a \end{aligned}$$

and

$$\begin{aligned} p_2 : A \times B &\to B \\ (a, b) &\mapsto b \end{aligned}$$

```
In [1]: 5 + [1,2,3]
Traceback (most recent call last):

  File "<ipython-input-1-32e08cac139a>", line 1, in <module>
    5 + [1,2,3]

TypeError: unsupported operand type(s) for +: 'int' and 'list'
```

If P proposition then $P : \textsc{Prop}$

If P proposition then $P : \mathrm{PROP}$

If p is a proof of P then $p : P$

Let $P, Q : \mathrm{PROP}$ with $p : P$ and $q : Q$.

Let $P, Q : \mathrm{PROP}$ with $p : P$ and $q : Q$.

What is $P \to Q$?

Let $P, Q : \textsc{Prop}$ with $p : P$ and $q : Q$.

What is $P \to Q$?

Ans: "If P then Q"

Let $P, Q : \mathrm{PROP}$ with $p : P$ and $q : Q$.

What is $P \times Q$?

Let $P, Q : \mathrm{PROP}$ with $p : P$ and $q : Q$.

What is $P \times Q$?

Ans: "P and Q"

Concluding remarks

Theorem provers are interesting because

- History
- Type Theory
- The future