Using computers to do maths for us!

Damiano Testa

University of Warwick

Tour of Mathematics, Term 1, 2020-21

Introduction

I chose to study maths, because I had an intuitive concept of what mathematics was and I was curious about it.

This initial concept evolved and changed as I kept studying.

And it keeps changing.

Formalizing mathematics

Today, I want to talk about formalization of mathematics.

In particular, I want to quickly review the role of sets.

We are used to stating mathematical questions in terms of sets.

However …

Using computers

Several automated proof checkers do NOT use sets.

They use *types*.

If we have time, we will see a demo with Lean,
one of these proof checkers.

Before going a little bit more in detail, I propose a riddle.

$1 = -1$

Why is the following argument incorrect?

$$1 = \sqrt{1} = \sqrt{(-1)^2} = \left(\sqrt{-1}\right)^2 = -1$$

We will come back to this later.

Foundations of mathematics

In the first years of study, I was taught how to formalize mathematics using sets.

The underlying principle is

EVERYTHING is a set.

Using sets

- The natural numbers $\mathbb{N}$ are a set: $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- The successor function

  $$\begin{array}{rccl} \mathrm{succ}\colon \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n+1 \end{array}$$

  is a set (of ordered pairs $(n, n+1)$).
- Ordered pairs are sets: we write $(a, b) \in A \times B$, and we encode it as the set $(a, b) \longleftrightarrow \big\{\{a\}, \{a, b\}\big\}$.
- Individual natural numbers themselves are encoded by sets!

$$\begin{tikzcd}
0 \arrow[d, leftrightarrow] & 1 \arrow[d, leftrightarrow] & 2 \arrow[d, leftrightarrow] & 3 \arrow[d, leftrightarrow] & \cdots \\
\emptyset & \{\emptyset\} & \Big\{\emptyset, \{\emptyset\}\Big\} & \Bigg\{\emptyset, \{\emptyset\}, \Big\{\emptyset, \{\emptyset\}\Big\}\Bigg\} & \cdots
\end{tikzcd}$$

Getting to the innermost set

Every statement in mathematics reduces to a statement about sets.

For instance:

- a sequence of real numbers is a function $a\colon \mathbb{N} \to \mathbb{R}$; i.e.
- a set of ordered pairs of a natural number and a real number;
- which is an equivalence class of subsets of rational numbers;
- which in turn are equivalence classes of pairs of integers;
- and integers are pairs of natural numbers;
- ah, of course natural numbers and pairs are themselves sets!
- I also missed out on spelling out that equivalence relations, order relations, equivalence classes,. . . are all sets.

Eventually all these sets will be sets of sets of . . . sets containing the empty set.

Confusion

If I ever unfolded all these definitions and
expressed everything in terms of sets,
I would probably be completely lost.

Let us try again!

Type theory

If you are familiar with set theory,
type theory is superficially very similar.

The basic concept in type theory is a *type*.
The closest analogue to a type in set theory is a set.

Besides types, in type theory there are *terms*.
The closest analogue to a term in set theory is an element of a set.

Type theory

Types are analogous to Sets.

Terms are analogous to Elements.

In type theory there are the types of

- the natural numbers $\mathbb{N}$;
- the integers $\mathbb{Z}$;
- the real numbers $\mathbb{R}$;
- and so on.

If n is a natural number, then we say that n is a term of type $\mathbb{N}$ and we write $n : \mathbb{N}$.

Terms have a unique type

A fundamental difference between types and sets is that

Every term has a *unique* type.

Once we say that $t : \mathbb{N}$, then t is a natural number.
We *cannot view t as an integer, as a real number, as a complex number, nor as any other kind of number.*

The symbol $t : \mathbb{N}$ commits us to the fact that t is a natural number.

We cannot revert or modify this choice.

We cannot identify or abuse notation and say that t is also an integer.

Back to the riddle – Sets

$$1 = \sqrt{1} = \sqrt{(-1)^2} \overset{\downarrow}{\underset{\uparrow}{=}} \left(\sqrt{-1}\right)^2 = -1$$

Explanation 1 (Sets).

The fallacy in the argument above arises from $\sqrt{(-1)^2} = \left(\sqrt{-1}\right)^2$.

There is no square-root function $\sqrt{\ } : \mathbb{C} \to \mathbb{C}$ satisfying, for all complex numbers a, b, the identity $\sqrt{ab} = \sqrt{a}\sqrt{b}$.

We can prove this statement by fiddling around with complex numbers and their arguments: it is not hard, but does require some effort.

Back to the riddle – Types

$$1 \overset{\downarrow}{\underset{\uparrow}{=}} \sqrt{1} = \sqrt{(-1)^2} = \left(\sqrt{-1}\right)^2 = -1$$

Explanation 2 (Types).

Now, we must be careful about what is the type of each term.
Assume $(1 : \mathbb{N})$, that is, the first "1" is a natural number.
The square root is then a function $\sqrt{\ } : \mathbb{N} \to \mathbb{R}$.
We deduce that the term $\sqrt{1}$ has type $\mathbb{R}$.
The equality $1 = \sqrt{1}$ asserts that the term 1, of type $\mathbb{N}$, also has type $\mathbb{R}$.

We are in violation of the only requirement for terms:

every term must have a unique type!

Back to the riddle – Types

$$1 = \underset{\uparrow}{\overset{\downarrow}{\sqrt{1}}} = \sqrt{(-1)^2} = \left(\sqrt{-1}\right)^2 = -1$$

Explanation 3 (Types).

Assume $(1 : \mathbb{R})$, that is, the first "1" is a real number.

Then, the square root must be a function $\sqrt{\ } : \mathbb{R} \to ??$

Oh, scrap that: the square root function is not defined on all of $\mathbb{R}$!

Back to the riddle – Types

$$1 = \sqrt{1} = \sqrt{(\overset{\downarrow}{\underset{\uparrow}{-}}1)^2} = \left(\sqrt{-1}\right)^2 = -1$$

Explanation 4 (Types).

Assume $(1 : \mathbb{R}_+)$, that is, the first "1" is a non-negative real number.

Then, the square root is the function $\sqrt{\ } : \mathbb{R}_+ \to \mathbb{R}_+$.

$(-1)^2$ is the result of multiplying together the number -1 with itself. It is therefore a value of the multiplication function

$$- \cdot - : \mathbb{R} \times \mathbb{R} \to \mathbb{R}.$$

We would like to take the square root of $(-1)^2$, but the type of $(-1)^2$ is $\mathbb{R}$ and $\sqrt{\ }$ takes terms of type $\mathbb{R}_+$. Again, we find a type mismatch.

Back to the riddle – Types

$$1 = \sqrt{1} = \sqrt{(-1)^2} = \left(\underset{\uparrow}{\overset{\downarrow}{\sqrt{-1}}}\right)^2 = -1$$

Explanation 5 (Types). Assume:

- $(1 : \mathbb{R}_+)$, that is, the first "1" is a non-negative real number;
- the square root is the function $\sqrt{} : \mathbb{R}_+ \to \mathbb{R}_+$;
- the multiplication is defined on the negative reals alone

$$- \cdot - : \mathbb{R}_- \times \mathbb{R}_- \to \mathbb{R}_+.$$

The problem shifts further to the right!
We now need to compute the square root of a negative number.
Once more, there is an issue with types.

Conclusions

Type theory requires us to be more careful about our definitions.

We are often forced to be quite pedantic.

Yet, we resolved our riddle only checking that types did not match.

This is a much "softer" reason than having to make an argument about products of square-roots of complex numbers.

Computers can take care of "type-checking" efficiently.

Moreover, a large part of the type-checking can be automated: we can be sloppy with our types and the computer will try to fill in the gaps.

Of course, as soon as some type does not match, it will let us know!

Infinitude of primes

You can watch a short video by Scott Morrison on how to formalize Euclid's proof of the infinitude of primes in Lean.

If you want to learn more about Lean, you can play the

Natural Numbers Game

by Kevin Buzzard and Mohammad Pedramfar.

Questions?