Machine Checked Proofs

When computers improve mathematical rigour

Since the invention of the concept of proof in ancient Greece, mathematicians have always sought to write ever more rigorous proofs: identifying axioms precisely, defining every object used in the proof, avoiding the call to intuition, etc. Machine-checked proof is a new step in this never ending quest of rigour. A machine-checked proof is written with such precision that a computer program can check its correctness.

THE BEGINNING

The first proof-checkers were AUTOMATH (1968-72), and the LCF (Wright 1970). Their goals were different: AUTOMATH was designed to mechanise general mathematical proofs, LCF was specifically to check proofs of properties of programs.

TODAY

The development of proof-checkers triggered the development of new theories, based on type theory, to express mathematics, each system innovates, introducing new features to express mathematical ideas more simply or to support a better logic. A new language introduces a new feature to express programs.

Recent proofs are: 1972, 1975, 1980, 1985, 1990... They are usually based on type theory, such as Principia Mathematica, Lambda-calculus, Type theory, and others are formulated, where various theories can be embedded.

They have in total more than 10,000 years.

Someone said that mathematics was the only subject not to use instruments. Is it true? It becomes the art of mathematics.