

Automated Theorem Proving

*Automated Theorem Proving (ATP) deals with the development of computer programs that show that some statement (the conjecture) is a logical consequence of a set of statements (the axioms and hypotheses).*¹

What is it?

Automated theorem proving (currently the most important subfield of *automated reasoning*) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. For the frequent case of propositional logic, the problem is decidable but NP-complete, and hence only exponential time algorithms are believed to exist.

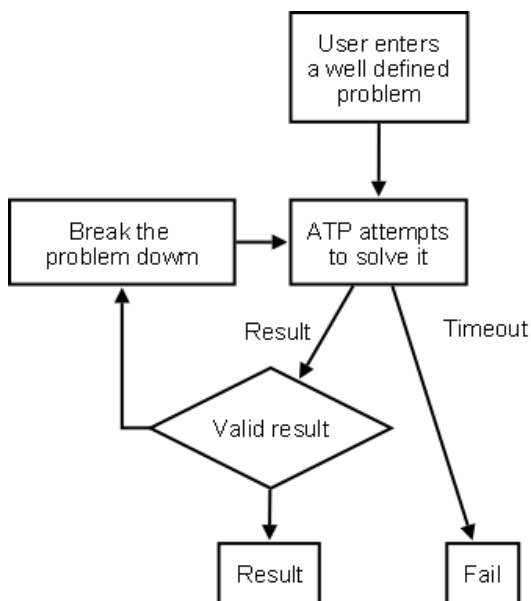


Figure 1 – The flow of an automated theorem prover

How it works

Figure 1 shows the basic flow of an ATP. It starts off with a description of the problem or theorem in some form of logic and then attempts to solve/prove it. It then either gives a result or times out (may happen if the problem can't be solved or a statement is invalid). If the result is wrong, it may be broken down into a set of smaller problems, or entered into the system in a different way.

Real world uses

Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification. Since the Pentium FDIV bug, the complicated floating point units of modern microprocessors have been designed with extra scrutiny. In the latest processors from AMD, Intel, and others, automated theorem proving has been used to verify that division and other operations are correct.²

The role of domain experts

ATP systems are enormously powerful computer programs, capable of solving immensely difficult problems. Because of this extreme capability, their application and operation sometimes needs to be guided by an expert in the domain of application, in order to solve problems in a reasonable amount of time. Thus ATP systems, despite the name, are often used by domain experts in an interactive way. The interaction may be at a very detailed level, where the user guides the inferences made by the system, or at a much higher level where the user determines intermediate lemmas to be proved on the way to the proof of a conjecture.³

Existing implementations

The following is a list of just some of the available implementations of automated theorem provers⁴:

- E
- Otter
- SETHEO
- Vampire
- Waldmeister

¹ <http://www.encyclopedia.com/doc/1G1-84804959.html> - 30/09/2009

² http://www.statemaster.com/encyclopedia/Automated-theorem-proving#Industrial_uses - 30/09/2009

³ <http://www.cs.miami.edu/~tptp/OverviewOfATP.html> - 30/09/2009

⁴ http://www.experiencefestival.com/a/Automated_theorem_proving/id/1923369 - 30/09/2009