PROOF COMPLEXITY

JAN KRAJICEK

In many parts of mathematics one finds statements asserting that a finite object with a particular, feasibly verifiable, property does not exist. Such statements include, for example, the unsolvability of an equation, the non-existence of a combinatorial pattern or of an algebraic object, or the non-existence of a computation solving a problem.

A universal statement of this form is a statement that a propositional formula cannot be satisfied by any truth assignment or, equivalently, that the negation of the formula is a tautology. The qualification "universal" means, in particular, that proving statements about the non-existence of particular finite objects can be reduced to proving that particular propositional formulas are tautologies.

The ultimate goal of "proof complexity" is to show that there is no universal propositional proof system allowing for efficient proofs of all tautologies. This is equivalent to showing that the computational complexity class NP is not closed under the complementation (and it implies the famous conjecture that P differs from NP).

By the universality propositional proof systems subsume methods from other parts of mathematics used for proving the non-existence statements. Because of this, even the partial results known at present (lower bounds for some specific proof systems) revealed interesting links of proof complexity to logic, algebra, combinatorics, computational complexity,... .

I shall attempt to explain the basic points of proof complexity in a coherent manner accessible to any mathematician.