Simpler proof assistants via bounded arithmetic

Paweł Balawender
University of Warsaw

Modern proof assistants are very powerful. This is generally considered an advantage, as we ultimately want their underlying theories to be capable of proving difficult theorems.

However, this strength also has disadvantages. In particular, it becomes difficult to reason about the actual expressive power of their formal systems. It is not even straightforward to specify all the subtle effects introduced into the theory by the features of a proof assistant. More importantly, this additional expressive power adds complexity to both proof checking and proof search, which is not always necessary. We propose that, for verifying simple proofs, much simpler proof systems could be used. Such systems would have kernels that are easier to verify and would facilitate proof search procedures that are easier to automate.

Results from the field of reverse mathematics suggest that most theorems used on a daily basis can be proved in very weak systems. Bounded arithmetic studies some of the weakest systems considered in reverse mathematics. In their remarkable work Logical Foundations of Proof Complexity (2010), Cook and Nguyen provide an exhaustive study of a hierarchy of formal systems V^i, the weakest of which (V^0) corresponds to the small circuit class AC^0, and the stronger correspond to TC^k, NC^k, L, P, and more. The authors include proofs that the weakest systems cannot prove theorems such as Kőnig's lemma or the totality of the exponential function. They also discuss connections between the V^i hierarchy and the formal system I\Delta_0, which has already been extensively studied in reverse mathematics.

It appears possible to implement the V^i systems on an actual computer, possibly within a setting such as Isabelle/Pure, an approach the author has already begun to explore. This could lead to the creation of a very simple yet expressive proof assistant, whose strength would be well-understood and precisely controllable at the level of individual theorems.

The existence of Witness theorems for V^0 and V^1 is a hint that code extraction from proof might be possible to implement, although the current proofs of them don’t seem to correspond to computationally feasible procedures.