Proof verification within set theory

Eugenio G. Omodeo

Dipartimento Matematica e Geoscienze sez. Matematica e Informatica,
Università degli Studi di Trieste

Abstract. The proof-checker ÆtnaNova, aka Ref, processes proof scenarios to establish whether or not they are formally correct. A scenario, typically written by a working mathematician or computer scientist, consists of definitions, theorem statements and proofs of the theorems. There is a construct enabling one to package definitions and theorems into reusable proofware components. The deductive system underlying Ref mainly first-order, but with an important second-order feature: the packaging construct just mentioned is a variant of the Zermelo-Fraenkel set theory, ZFC, with axioms of regularity and global choice. This is apparent from the very syntax of the language, borrowing from the set-theoretic tradition many constructs, e.g. abstraction terms. Much of Ref's naturalness, comprehensiveness, and readability, stems from this foundation; much of its effectiveness, from the fifteen or so built-in mechanisms, tailored on ZFC, which constitute its inferential armory. Rather peculiar aspects of Ref, in comparison to other proof-assistants (Mizar to mention one), are that Ref relies only marginally on predicate calculus and that types play no significant role, in it, as a foundation.
This talk illustrates the state-of-the-art of proof-verification technology based on set theory, by reporting on 'proof-pearl' scenarios currently under development and by examining some small-scale, yet significant, examples of use of Ref. The choice of examples will reflect today's tendency to bring Ref's scenarios closer to algorithm-correctness verification, mainly referred to graphs. The infinity axiom rarely plays a role in applications to algorithms; nevertheless the availability of all resources of ZFC is important in general: for example, relatively unsophisticated argumentations enter into the proof that the Davis-Putnam-Logemann-Loveland satisfiability test is correct, but in order to prove the compactness of propositional logic or Stone's representation theorem for Boolean algebras one can fruitfully resort to Zorn's lemma.