Proof verification within Set Theory: Exploiting a new way of modeling graphs

Eugenio G. Omodeo

University of Trieste (Italy), DMG/DMI

This talk illustrates proof-verification technology based on set theory, also reporting on experiments carried out with ÆtnaNova, aka Ref (see [6, 4]).

The said verifier processes script files consisting of definitions, theorem statements and proofs of the theorems. Its underlying deductive system—mainly first-order, but with an important second-order construct enabling one to package definitions and theorems into reusable proofware components—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 alike proof-assistants (cf., e.g., [2, 1]), are that Ref relies only marginally on predicate calculus and that types play no prominent role, in it, as a foundation.

The selection of examples, mainly referred to graphs, to be discusses in this talk, reflects today's tendency [5] to bring Ref's use closer to algorithm-correctness verification. To achieve relatively short, formally checked, proofs of properties enjoyed by claw-free graphs, we took advantage of novel results [3] about representing their (undirected) edges via membership.

Acknowledgements. *Partial funding was granted by the INdAM/GNCS 2013 project "*Specifica e verifica di algoritmi tramite strumenti basati sulla teoria degli insiemi*".*

References

1. C. E. Brown. Combining type theory and untyped set theory. In Ulrich Furbach and Natarajan Shankar, editors, *IJCAR*, volume 4130 of *Lecture Notes in Computer Science*, pages 205–219. Springer, 2006.
2. R. Matuszewski and P. Rudnicki. Mizar: the first 30 years. *Mechanized Mathematics and its Applications*, 4(1):3–24, 2005.
3. M. Milanič and A. I. Tomescu. Set graphs. I. Hereditarily finite sets and extensional acyclic orientations. *Discrete Applied Mathematics*, 161(4-5):677–690, 2013.
4. E. G. Omodeo. The Ref proof-checker and its "common shared scenario". In Martin Davis and Ed Schonberg, editors, *From Linear Operators to Computational Biology: Essays in Memory of Jacob T. Schwartz*, pages 121–167. Springer, 2012. With an appendix, *Claw-free graphs as sets*, co-authored by A. I. Tomescu.

5. E. G. Omodeo and A. I. Tomescu. Set graphs. III. Proof Pearl: Claw-free graphs mirrored into transitive hereditarily finite sets. *Journal of Automated Reasoning*, 52(1):1–29, 2014.
6. J.T. Schwartz, D. Cantone, and E.G. Omodeo. *Computational Logic and Set Theory - Applying Formalized Logic to Analysis*. Springer, 2011.