Constable, Robert L.; Moczydlowski, Wojciech

Extracting programs from constructive HOL proofs via IZF set-theoretic semantics. (English) [Zbl 1147.03013]


Summary: Church’s Higher Order Logic is a basis for influential proof assistants – HOL and PVS. Church’s logic has a simple set-theoretic semantics, making it trustworthy and extensible. We factor HOL into a constructive core plus axioms of excluded middle and choice. We similarly factor standard set theory, ZFC, into a constructive core, IZF, and axioms of excluded middle and choice. Then we provide the standard set-theoretic semantics in such a way that the constructive core of HOL is mapped into IZF. We use the disjunction, numerical existence and term existence properties of IZF to provide a program extraction capability from proofs in the constructive core. We can implement the disjunction and numerical existence properties in two different ways: one using Rathjen’s realizability for IZF and the other using a new direct weak normalization result for IZF by Moczydlowski. The latter can also be used for the term existence property.

MSC:
03B70 Logic in computer science
03B15 Higher-order logic; type theory (MSC2010)
03B35 Mechanization of proofs and logical operations
03E70 Nonclassical and second-order set theories
68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Keywords:
higher-order logic; intuitionistic set theory; constructive core of HOL; program extraction; weak normalization

Software:
Nuprl; PVS; MetaPRL

Full Text: DOI