Animation
Implementing Z in Isabelle

Ina Kraan and Peter Baumann

Department of Computer Science, University of Zürich
8057 Zürich, Switzerland
inak,baumann@ifi.unizh.ch

Abstract. We present work in progress on a deep semantic embedding of the specification language Z and its deductive system (as defined by the draft Z standard) in the theorem prover Isabelle. Z is based on Zermelo-Fraenkel set theory and first-order predicate logic, extended by a notion of schemas. Isabelle supports a fragment of higher-order predicate logic, in which object logics such as Z can be encoded as theories. This paper gives an overview of Z-in-Isabelle, including some example proofs, and discusses some of the major issues involved in formalizing Z in Isabelle.

1 Introduction

We are implementing the language Z and a deductive system for Z in the generic theorem proving tool Isabelle. The implementation is based on Z and its deductive system as defined in the draft Z standard [2]. It is a deep embedding of Z, i.e., both the syntax and a deductive system are formalized within Isabelle's meta-logic.

Implementations of Z can be roughly divided into two categories. First, there are the direct implementations, including, for instance, the tool Balzac [4, 6]. Second, there are the embeddings of Z in other logics and in logical frameworks. Most such implementations have been shallow rather than deep embeddings, including ProofPower [5], Z in HOL [1], and Z in LEGO [7]. The distinction between shallow and deep is not always clear-cut, but in principle, the deeper the embedding, the more properties of the language can be proven in the embedding. Deep embeddings of Z in logical frameworks include Jigsaw [8] and our system Z-in-Isabelle. Jigsaw is based on the deductive system of Woodcock and Brien [13] and implemented in 2OBJ [3]. Despite being deep embeddings within logical frameworks, the two systems are quite different. A comparison can be found in section 7.

An embedding within a logical framework has the advantage that one can prove faithfulness and adequacy more easily (for an example of such proofs for first-order logic in Isabelle, see [9]). A deep embedding, while involving much more effort than a shallow one, has a number of advantages. First, it can be used to rigorously derive, as theorems in the meta-logic, new rules of inference for the object logic (one of the example proofs presented is the derivation of such a rule). These may be more desirable because they are simpler to use, or because they facilitate the automation of proofs. Second, one can prove properties of the language being embedded, e.g., properties such as commutativity or associativity of operators. Our experience with Isabelle has shown that it is a suitable

1 Where it is incomplete, we have referred to the logic of Woodcock and Brien [13].