zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Leino, K. Rustan M.; **Müller, Peter**

A verification methodology for model fields. (English) Zbl 1178.68348

Sestoft, Peter (ed.), Programming languages and systems. 15th European symposium on programming, ESOP 2006, held as part of the joint European conferences on theory and practice of software, ETAPS 2006, Vienna, Austria, March 27–28, 2006. Proceedings. Berlin: Springer (ISBN 3-540-33095-X/pbk). Lecture Notes in Computer Science 3924, 115-130 (2006).

Summary: Model fields are specification-only fields that encode abstractions of the concrete state of a data structure. They allow specifications to describe the behavior of object-oriented programs without exposing implementation details.

This paper presents a sound verification methodology for model fields that handles object-oriented features, supports data abstraction, and can be applied to a variety of realistic programs. The key innovation of the methodology is a novel encoding of model fields, where updates of the concrete state do not automatically change the values of model fields. Model fields are updated only by a special pack statement. The methodology guarantees that the specified relation between a model field and the concrete state of an object holds whenever the object is valid, that is, is known to satisfy its invariant.

The methodology also improves on previous work in three significant ways: First, the formalization of model fields prevents unsoundness, even if an interface specification is inconsistent. Second, the methodology fully supports inheritance. Third, the methodology enables modular reasoning about frame properties without using explicit dependencies, which are not handled well by automatic theorem provers.

For the entire collection see [Zbl 1103.68010].

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)
68N19 Other programming paradigms (object-oriented, sequential, concurrent, automatic, etc.)

Cited in **3** Documents

Software:

ESC/Java; JML; SIMPLIFY; Spec#

Full Text: DOI

© 2021 FIZ Karlsruhe GmbH