Verifying OCL Specifications of UML Models

Tool Support and Compositionality

The Unified Modelling Language (UML) and the Object Constraint Language (OCL) serve as specification languages for embedded and real-time systems used in a safety-critical environment.

In this dissertation class diagrams, object diagrams, and OCL constraints are formalised. The formalisation serves as foundation for a translation of class diagrams, state machines, and constraints into the theorem prover PVS. This enables the formal verification of models defined in a subset of UML using the interactive theorem prover.

The type system of OCL makes writing specifications difficult while the model is still under development. To overcome this difficulty a new type system is proposed, based on intersection types, union types, and bounded operator abstraction.

To reduce the complexity of the model and to increase the structure of the specification, compositional reasoning is used. The introduction of history variables allows compositional specifications. Proof rules support compositional reasoning.

The feasibility of the presented approach is demonstrated by two case-studies. The first one is the "Sieve of Eratosthenes" and the second one is a part of the medium altitude reconnaissance system (MARS) deployed in F-16 fighters of the Royal Dutch Air Force.

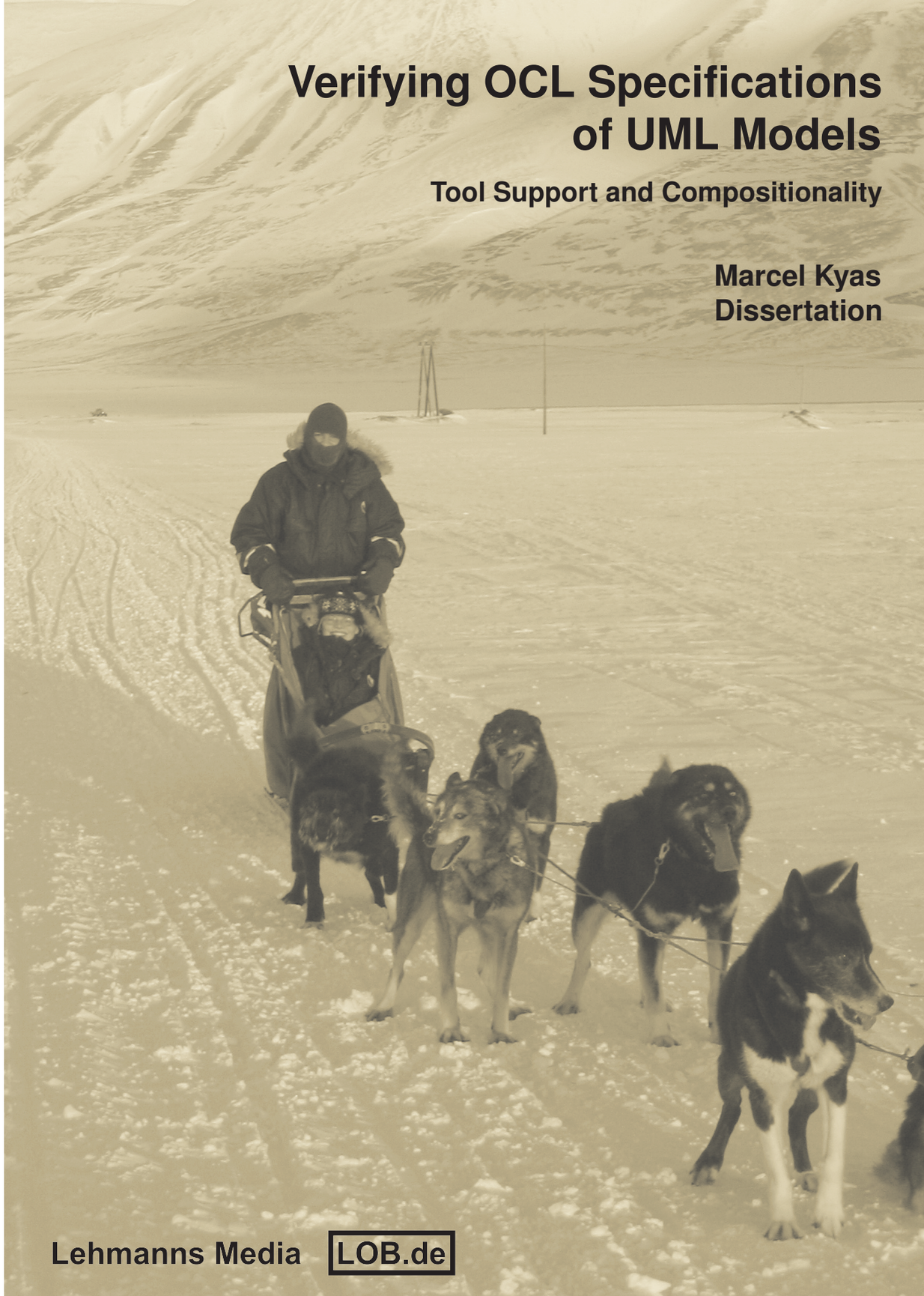
Lehmanns Media LOB.de

ISBN 3-86541-142-8

Marcel Kyas

Verifying OCL Specifications of UML Models

Tool Support and Compositionality



Verifying OCL Specifications of UML Models

Tool Support and Compositionality

Marcel Kyas
Dissertation

Lehmanns Media LOB.de