| | |
|---|---|
| Title | CafeOBJによるB-抽象機械モデルの検証法に関する研究 |
| Author(s) | 梅原，伸年 |
| Citation | |
| Issue Date | 1998-03 |
| Type | Thesis or Dissertation |
| Text version | author |
| URL | http://hdl.handle.net/10119/1147 |
| Rights | |
| Description | Supervisor:二木 厚吉，情報科学研究科，修士 |

# Verification Method of B-Abstract Machine Model in CafeOBJ

Nobutoshi Umehara
School of Information Science,
Japan Advanced Institute of Science and Technology

February 13, 1998

keywords:
B-Technology, internal consistency, hidden algebra, refinement, projection

## Abstract

We verify the consistency of B Abstract Machine specification in CafeOBJ. We propose a guideline for descriptions of formal specifications of large systems that are based on algebraic specification techniques.

Recently, software is getting larger and more complex. Therefore, software engineers are faced with the difficulty to describe the target systems correctly. Formal methods are available to solve this problem. The formal methods are based on mathematically techniques for the describing system properties. The Z, VDM, *B-Technology* (hereafter, 'B') are famous as formal specification languages in model-oriented. The OBJ, CafeOBJ are also famous as in property-oriented. The model oriented formal specification languages are used to describe specifications. They use the concrete primitives, for example, set, list, and function. In contrast, the property oriented formal specification languages are used to describe specifications. They use axioms that represent required properties of specifications. In these formal languages, However, B gained support from developers to adopt techniques for the specification, design of software components known such as Abstract Machine, object based approach, Case Studies, etc. Now, there are various systems that we can treat as the states and their operations. The Abstract Machine consists of the states and their operations. An object based approach is easy to understand for the developers. The Case Studies on B is useful rather than on the other formal methods. The B-Technology consists of the Abstract Machine Notation, the B-Method and the B-Toolkit[1]. The B-Method is a methodology to proof *internal consistency* of the Abstract Machine and the Refinement (which refined Abstract Machine). This method provides specifications which contain no error. The B-Toolkit supports this method in various

[1] The B Toolkit is a trademark of B-Core (UK) Ltd.

stages on software development. We select B on the above points and to refer to the techniques of specification development.

The CafeOBJ is a formal specification language based on many sorted algebra, order sorted algebra, *hidden algebra* and rewriting logic. CafeOBJ can naturally cope with abstract data types. It copes with respectively data and operations of the data with sort and sorted functions. Therefore, CafeOBJ can cope with an object as a unit of specification. The concepts of rewriting logic and hidden algebra give the user the ability to describe object based specifications. CafeOBJ has also a feature as an executable language. We can prove the specification automatically using CafeOBJ. These features are similar to B. More over, CafeOBJ has many techniques such as projection and refinement. These points contribute to reduce verification steps.

# 1 The First Stage

We must consider how to express the Abstract Machine to obtain specification has wide applicability. Some features in the Abstract Machine Notation are the variables, the invariant, the constants and the sets for describing the state. Some features are parameters and pre-condition for describing the operations. Other features are sees, uses, includes and refinement for structuring specifications.

We provide a basic table to convert the Abstract Machine which consists of the above features to a specification in CafeOBJ. Then we consider the conversion of import commands of the Abstract Machine in practical sense. Since the operations clauses of B specification can deal with various internal states without declaration, we cannot obtain the accurate information of the affection of the operations on the internal states. To handle this problem, we propose a guideline recommends to set a new sort to an internal state.

# 2 Second Stage

We can use formal methods to describe a specification of safety critical system. This means formal methods provide us high reliability. The B-Method prescribes how to check the specification for consistency. The proof for internal consistency is *1*)parameter existence, *2*)constants and sets existence, *3*)non-emptiness of machine state, *4*)initialisation and *5*)invariant preservation. We make an equivalent proof in CafeOBJ with a proof provided in B-Method.

The Refinement is the process from high abstract specifications to low abstract ones (concrete specifications). Using refinement, we can preserve the properties of specifications based on the behaviours. The proof for refinement consistency is *1*)non-emptiness of joint state, *2*)initialisation refinement and *3*)operation refinement.

The *Refinement* on CafeOBJ needs signature map and proof that satisfy equations defined in abstract specification. We make also a proof of this in CafeOBJ.

# 3 Lift System Example

B supports Case Studies for training. The following lift system is one of them.

We describe abstract specifications of this lift system. The first specification is single lift for personal use. The second one is a single lift for personal use with more operations. We provide a proof score using the executable feature of CafeOBJ. This proof shows a correctness of refinement using above two specifications. The primary point of this example is that operation refinement is the map from one abstract operation to compositional concrete operations. We explain this composition of operations to use derived operator. The proof of this refinement is to prove that the concrete specification preserves all mapped equations.

The third one is a multi-lift. We describe a multi-lift specification by composing the above single lift specifications. The *Projection* is a useful methodology for describing concurrent systems. The projection operator is a map from the multi-lift system to the single lift systems. This multi-lift system is a concurrent system without synchronization. Using projection operator, we can give a simple verification on the multi-lift system. We verify that the execution order of two operations that generate transitions makes no influence with regard to the behaviour. This verification is based on hidden algebra. By using hidden algebra, we can specify encapsulated objects, and can handle behavioural specification.

The above specifications are part of the whole specification of the lift system. We described the whole specification in CafeOBJ actually.

# 4 Conclusion

We selected B to refer the techniques describing specification in this research.

We can summarize our work as the follows.

*1*) We considered how to describe B Abstract Machine specification in CafeOBJ. *2*) We made a useful reference table to transform B into CafeOBJ. *3*) We proposed to use new sort for represent internal state, to obtain the accurate information of the operations. *4*)We showed proof scores for internal consistency and refinement consistency of CafeOBJ specifications. *5*)We also showed a possibility of simple verification to use the concepts of refinement and projection by using examples such as lift systems.

An algebraic specification is a suitable specification for describing objects which consist of state and their operations. Then the abstraction of specifications is useful for verification in required aspect of behaviours. We showed a parallel property of operation on the multi-lift example, but this system has no synchronization. CafeOBJ is also based on rewrite logic. Thus we can cope with concurrency and non-deterministic choice by using rewrite logic. Our future work is to verify the above systems.