Computer Science at Kent

Implementation and Application of Functional Languages
19th International Symposium, IFL 2007

Olaf Chitil (Ed.)

Freiburg, Germany, 27th-29th September 2007

Technical Report No. 12-07
September 2007

Published by the Computing Laboratory,
University of Kent, Canterbury, Kent, CT2 7NF, UK

Preface

The 19th International Symposium on Implementation and Application of Functional Languages (IFL 2007) is held at Freiburg, Germany, on the 27th to the 29th September 2007. Local organiser is the Programming Languages Group of the Department of Computer Science of the University of Freiburg.

IFL brings together researchers active in the area of functional programming, with an emphasis on the implementation and application of the same. IFL provides an annual open forum for researchers who wish to present and discuss new ideas and concepts, work in progress, preliminary results, etc. IFL has been held throughout Europe in the Netherlands, United Kingdom, Germany, Sweden, Spain, Ireland and Hungary. This year for the first time IFL is co-located with the International Conference on Functional Programming (ICFP). A record number of 44 papers have been submitted for these draft proceedings. By the time of printing 73 researchers had registered for attendance at the symposium.

Following tradition, two proceedings are to be published: the draft proceedings used at the symposium (this document), released as a technical report of the Computing Laboratory of the University of Kent, and the post-symposium proceedings based on revised papers. The draft proceedings are un-refereed and provide a useful reference to the delegates at the symposium. All participants who give talks at the symposium are invited to submit revised papers for review after the symposium, to normal conference standards. The post-symposium proceedings of selected revised papers will be published by Springer-Verlag in its Lecture Notes in Computer Science (LNCS) series.

Olaf Chitil
Programme Chair
University of Kent
September 2007

Local Organisers

Markus Degen
Peter Thiemann
Stefan Wehr

Supported by Deutsche Forschungsgemeinschaft (DFG)

Table of Contents

Index

On the Validation of Specifications used in Model-Based Testing

Pieter Koopman, Peter Achten, and Rinus Plasmeijer

Software Technology, Nijmegen Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands
{pieter, p.achten, rinus}@cs.ru.nl

Abstract. In model-based testing the behavior of a system under test, sut, is compared automatically with the behavior of the specification. A significant fraction of issues found in testing appear to be caused by problems with the specification. In order to ensure that the specification prescribes the desired behavior, it has to be *validated* by a human. In this work we introduce a tool to support this validation. In addition to an interactive simulator of the specification, the tool is able to generate transition tables and diagrams of the observed behavior. In order to make simulation and the displaying of the observed behavior finite, we introduce equivalence of states, inputs and outputs.

Extended Abstract

In model-based testing the behavior of a system under test, sut, is compared automatically with the behavior of the specification. The specification is a state transition system that can be nondeterministic. Usually the number of states, inputs and outputs possible is infinite. The sut is also assumed to be a state transition system, but its state is hidden. One can only apply input to the system and observe the corresponding output. We have used model-based testing successfully to improve controllers, protocols, javacard applets and more.

For this comparison of behavior, the test system takes a specification and executes a user defined number of traces. For each trace the sut and the specification starts in their initial states. The test system selects an input that is covered by the specification, applies this input to the sut, and computes the allowed states of the specification. If no states are possible for the specification the sut has shown behavior that is not covered by the specification. The testers say that an *issue* is found.

Ideally, each issue indicates an error in the sut. However, in practice a significant fraction of issues appear to be caused by problems with the specification: the specification does not correctly capture the intentions of the users and the sut does something different. Although the fraction of issues caused by the specification differs with the kind of system and the amount of effort put in the correctness of the specification, we estimate that on average in about 25% of the issues found in model-based testing one has to blame the specification.

Incorrect specifications are a problem for several reasons. First, if an issue is found it is not clear whether we have to blame the specification or the sut. Finding and correcting errors in the specification takes time during the test phase of the project. This is not the right moment to create a correct specification. In many projects there is a significant time pressure during the testing phase of a system. Second, only behavior that is implemented differently by the sut can cause issues. All other errors in the specification are not found at all during model-based testing. Third, any change in the specification during the testing phase can cause significant implementation changes to the sut. Finally, any change in the specification invalidates in principle all previous test results (just like any change in the sut). This implies that errors in the specification can be very expensive and it is worthwhile to invest effort to ensure the quality of the specification.

In our model-based test system G∀st we use the functional language Clean as specification language. Due to the high abstraction level of this language it is possible to write concise specifications which contributes to their quality. The Clean compiler will check quality aspects like type correctness and consistent definition of identifiers used. We have shown that quality aspects such as the reachability of states, determinism and completeness of the specification, and the preservation of constraints can be checked by systematic testing.

However, this does not rule out the possibility that the specification prescribes the wrong behavior in a consistent way. In order to ensure that the specification prescribes the desired behavior, it has to be *validated* by a human. In this work we introduce tools to support this validation. First, a simulator enables the user to execute the specification. Such an interactive execution can be much more illustrative than looking at the code of the specification. Second, it is possible to record the traces of the specification executed in the simulator. The states visited and their transitions can be visualized in a table or a state transition diagram. Since the number of states, inputs and outputs can be infinite and different in each and every specification, this is not straightforward. The key to the solution is an operator to define equivalence of states, inputs and outputs. For instance, values that are handled by the same symbolic transition in the specification (function alternative in the specifying function) are usually considered to be equivalent. All states that are considered equivalent can be mapped to the same entry of the table or the same place in the transition diagram. Since the equivalence of values is problem dependent, some human input is required to define equivalence.