Internship report outline
(intended to the ENS staff)

Tahina Ramananandro
Daniel Jackson ?

July 24, 2006

1 Introduction

1.1 The VSR Project

Verified Software Repository, a level 6 Grand Challenge.

The VSR/NET workshops in England, with Jim Woodcock.

To share the same case study with many different methods. To seek proofs as automatically as possible. List of candidates. Why Coq, for instance, would not have suited.

1.2 The Mondex Case Study

The Mondex electronic purses. Abstract and Concrete protocols.

Introducing the Z specification language, in which the Mondex has been modeled and proved by hand.

2 The Alloy method

2.1 The Alloy specification language

Signature, relations, ... A short example of an Alloy model.

2.2 The Alloy Analyzer

Principles of model-finding. Finite scope. (Some screenshots.)

It interacts with the specification process to find bugs in the constraints.

3 The Mondex spec in Alloy

3.1 Constraints

Global and local constraints. Global constraints may make me miss some cases.

Many differences with Z, though. Some imprecisions with specifying in Z (operations and constraints).

3.2 Atom identification and canonicalization

Distinguishing identified (purses) and unidentified (PayDetails) objects.

Unidentified objects have to be canonicalized.

Notion does not exist in Z.

3.3 Results

The use of the Alloy Analyzer implementation raised technical issues which led to modifying the specification : why not use integers ?

Bugs found in the original specification.

Time of SAT-Solving.

How could it be improved with Kodkod (currently under development, but using the same method) ?

3.4 Limits to the method

The finite scope : results are valid only for a given scope. The higher, the longer time and the more resources.

So, finiteness properties ignored.

4 Extended analysis : Alloy and theorem proving

4.1 Translating Alloy to FOL.

Alloy semantics in FOL. Problem : transitive closures.

4.2 Results (in progress)

Which theorems have been proved from the existing specification ? How long time ?

4.3 Limits to the method

Transitive closures. Fortunately, the Mondex spec has none of them.

In general, does not solve how to tackle finiteness. In the Mondex spec in Z, there are some required properties. Dropped again.

Using proof assistants could help (cf. Prioni), but we lose automation. (Some failed example with Coq)

5 Conclusion and future work

In particular we would have shown that the Mondex specification can be fitted into FOL if finiteness properties are dropped.

The Alloy language has a high potential of use ; though, I would say Daniel's group should give a hand for other groups to use the Alloy spec language with other methods than model-finding. But on the contrary, I fear from the fact that the current evolution of Alloy, with scripting features, would enforce the use of the next Alloy/Kodkod model-finding analyzer.

For the Mondex case study in particular : I'll technically present my work on October 5-6th, and they'll decide how to use it. Probably to interact Alloy with other methods.