Proof Preservation in Component Generalization

Anamaria Martins Moreira

Universidade Federal do Rio Grande do Norte (UFRN) — DIMAp
59078-970 Natal, RN, Brazil
`http://www.dimap.ufrn.br/∼anamaria`

Abstract. Formal specifications can provide significant support for software component reuse, as they allow tools to “understand” the semantics of the components they are manipulating. For instance, they can be of great help on the generation of reusable components through the parameterization of more specific ones, supporting the process of creation and maintenance of libraries of reusable components.

In this work[1], we concentrate on the generalization of algebraic specification components by their parameterization. Knowing that highly specific components have small chances of being reused, but that, on the other hand, if a component is too general, its reuse will often be useless; we try to preserve some set of semantic properties of a component that are considered “important” somehow. So, we propose means to identify the requirements that a formal parameter should satisfy in order to preserve part of the original component semantics in the generalization. To reach this goal, we may (or may not) consider proofs for these properties in the original context and identify the conditions under which these proofs are reproducible after generalization. In our PhD Thesis, we considered both cases; here, we concentrate in the case of known proofs. When these known proofs are rewrite proofs, a set of equations can be extracted from them and added to the formal parameter so that they are preserved in the process. This simple technique provides sufficient conditions for the validity of the considered properties in the models of the more general specification, with the advantage of being easily computed by a simple algorithm that we propose. This algorithm is to be applied in conjunction with a generalization operator that safely effectivates the generalization transformations in the component. This combination provides the means to obtain a more general specification component from which the original one is a specialization and that still satisfies a given set of equational properties with their rewrite proofs.

We have also shown that more complex proofs can benefit from this result, although only partially. One of the next steps in this work is to improve the treatement of these other kinds of proofs.

Keywords. algebraic specifications, component parameterization and reuse, proof generalization.

---

[1] A full version of this article may be found in the author’s URL.

J. Wing, J. Woodcock, J. Davies (Eds.): FM’99, Vol. II, LNCS 1709, pp. 1866–1866, 1999.