Archived Design Steps in Temporal Logic

Pertti Kellomäki[1] and Tommi Mikkonen[2]

[1] Tampere University of Technology, Finland, pk@cs.tut.fi,
[2] Nokia Telecommunications, Finland, Tommi.Mikkonen@nokia.com

We demonstrate how solutions to recurring problems in the design of nonterminating reactive systems can be archived and verified in an abstract form using the DisCo specification method [1, 3].

DisCo is based on incremental development of temporal logic specifications using *superposition*. Superposition is a form of refinement in which new state variables and operations on them are added layerwise to a specification.

An archived specification $\mathcal{L}_1 + \mathcal{L}_2$ is applied to a specification S as depicted in Fig. 1. The "+" symbol denotes superposition, and "$\leq$" denotes refinement.

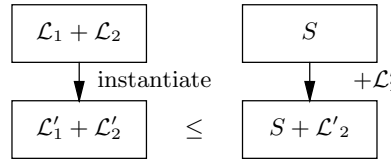

Fig. 1. Applying an archived step.

The archived specification is first instantiated with concrete classes, types and functions, yielding the specification $\mathcal{L}'_1 + \mathcal{L}'_2$. The layer $\mathcal{L}'_2$ is then superimposed on S, yielding the specification $S + \mathcal{L}_2$. Establishing that $S + \mathcal{L}_2$ is a refinement of $\mathcal{L}_1 + \mathcal{L}_2$ also establishes that $S + \mathcal{L}_2$ has the safety properties verified for the archived specification. Establishing the refinement incurs proof obligations, but these are relatively trivial because of the superposition methodology.

In an archived specification, $\mathcal{L}_1$ represents a problem and its context, and $\mathcal{L}_2$ a solution to the problem. They thus embody formally some of the information contained in behavioral *design patterns* [2]. Assumptions about the behavior of the context are formalized in an operational manner using the same formalism used for specifying the solution.

This research was supported by the Academy of Finland, project 757473.

References

[1] The DisCo project WWW page. http://www.cs.tut.fi/ohj/DisCo/.
[2] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design Patterns*. Addison Wesley, Reading, MA, 1995.
[3] Reino Kurki-Suonio. Fundamentals of object-oriented specification and modeling of collective behaviors. In H. Kilov and W. Harvey, editors, *Object-Oriented Behavioral Specifications*, pages 101–120. Kluwer Academic Publishers, 1996.

J. Wing, J. Woodcock, J. Davies (Eds.): FM'99, Vol. II, LNCS 1709, pp. 1858–1858, 1999.