The “Push-Out” Approach to Refinement and Composition for High-Consequence Systems

Philip Johnson-Freyd

May 18, 2016

While High-Consequence Control Systems may end up being simpler than some other digital systems they frequently are still rather complicated. Challenges abound in formal modeling at scale. Specialized practices and tools are needed to build large scale specifications and formal models. Two particularly important techniques are refinement and composition. In a refinement based approach complex detailed models are constructed as refinements of simpler abstract models. In a composition based approach complex models are built out of smaller component models. These concepts can be instantiated in different ways in different modeling methodologies. In the Temporal Logic of Actions[3], for example, refinement is interpreted as logical implication and a basic form of composition is given by logical conjunction. We must be careful however in accounting for the fact that a single variable in abstract models may be implemented by multiple variables in a more concrete refined model and so we need to generalize the notions of refinement include a concept of refinement mapping[1]. Moreover, the formula composition is conjunction is complicated by concerns over sharing of variables and variable renaming.

In this tutorial style talk we show how, far from being completely separate concepts, refinement and composition are related. Taking an old idea from Goguen [2] we suggest an approach to viewing composition in terms of refinement using the concept of a “push-out” from category theory. In this approach refinements are proof relevant: we care not only that there exists a refinement but can depend on its structure. We show how the push-out approach generalizes other views and allows for a scalable approach to specification engineering. Finally, we discuss how the idea of the push-out is cleanly implemented in specific modeling methodologies like TLA.

References

[1] Abadi, M., and Lamport, L. The existence of refinement mappings. *Theor. Comput. Sci. 82*, 2 (May 1991), 253–284.

[2] Goguen, J. A. A categorical manifesto. *Mathematical structures in computer science 1*, 01 (1991), 49–67.

[3] Lamport, L. The temporal logic of actions. *ACM Trans. Program. Lang. Syst. 16*, 3 (May 1994), 872–923.