Position Statement

Tim Sauerwein

Galois Connections Inc.
3875 SW Hall Blvd.
Beaverton, OR 97005 USA
tim@galconn.com

At Galois Connections, our business includes the construction of high-assurance software using formal methods. Our primary formal method is to program in modern functional programming languages, such as Haskell. These languages have powerful type systems that prevent certain classes of errors and promote intellectual control. Moreover, good functional programs have traits such as being declarative, using high levels of abstraction, using small, embedded domain-specific languages at appropriate points, and adopting a mathematical bias. We have found by experience that functional programming is a very effective industrial technique, one that lies in the "sweet spot" on the terrain that stretches between formal methods theory and industrial practice.

We are also starting to explore theorem-proving technology in one of our projects. At present, we are formalizing a few small portions of the project, with the hope of proving a few important properties that will raise confidence in the design. How best to apply theorem-proving technologies to large functional programs is an open research question. We intend to make some progress toward answering this question in practice, but without engaging in the sort of open-ended exploration that is more appropriate in an academic setting. The project will try a variety of different approaches, striving at first for small successes and learning from experience. We see theorem proving as a technology that will become gradually more and more important during the next decade.

To be really practical, the world of formalized reasoning needs an automatic and reliable link to the world of programming. Moreover, it is essential to find ways of structuring the program development to make proof construction more efficient. The nature of this link is not clear to me at present, but I am sure that those working in logic-based program synthesis have thought deeply about this problem. My interest in the symposium lies in its opportunities to find out what the experts have been doing and thinking. I am particularly interested in assessing what may be ready for practical application now, and what may become so in the future. I may be able to offer some opinions about what is practical and what is not, but I am coming to the symposium primarily to learn.