CAREER: Design Tools for Formal Specifications

Abstract

Formal specifications are a prerequisite for correct software, yet programmers ofter choose not to write them because tool support for designing specification lags far behind tools for designing code. Specifications can be wrong; tools must embrace this fact and encourage exploration and debugging. This proposal aims to uncover scientific principles to support the nimble design of formal specifications. It focuses on three target areas: type specifications for untyped programs, logic specifications for uncrewed aircraft routes, and models for reactive systems. The third domain will serve as the focus for outreach efforts. The PI will develop on online environment for system modeling and deploy it in an undergraduate course that gives students hands-on experience writing specifications and in K-12 activities through the University of Utah GREAT summer camp program. To engage students, the online environment will frame specification as a game between the specifier (student) and an adversary who invents a wrong system while obeying all rules from the specification.