Abstract: The long list of software failures over the past years calls for serious concerns in our digital society, creating bad reputation and adding huge economic burden on organizations, industries and governments. Improving software reliability is no more enough, ensuring software reliability is mandatory. Our ARTIST project complements other advances in the area and addresses this demand by turning first-order theorem proving into an alternative, yet powerful approach to ensuring software reliability. Saturation-based proof search is the leading technology for automated first-order theorem proving. The high-gain/high-risk aspect of our project comes from the development and use of saturation-based theorem proving as a unifying framework to reason about software technologies. We use first-order theorem proving methods not only to prove, but also to generate software properties that imply the absence of program errors at intermediate program steps. Generating and proving program properties call for new methods supporting reasoning with both theories and quantifiers. Our project extends saturation-based first-order theorem provers with domain-specific inference rules to keep reasoning efficient. This includes commonly used theories in software development, such as the theories of integers, arrays and inductively defined data types, and automation of induction within saturation-based theorem proving, contributing to the ultimate goal of generating and proving inductive software properties, such as invariants. Thanks to the full automation of our project, our results can be integrated and used in other frameworks, to allow end-users and developers of software technologies to gain from theorem proving without the need of becoming experts of it.

Free participation upon registration online by 8 March.

More information: bit.ly/PIStory2