

Bitvector Support in the Theta Formal Verification Framework

The verification of safety-critical software systems has many challenges, such as the complex language constructs in embedded software. This paper addresses the verification problem of software systems using bitwise operations, and we present an extension to the Theta open-source formal verification framework. Our goal is to integrate bitvectors and bitwise operations in the abstraction-refinement-based formal verification methods in Theta. Supporting bitvectors is a step towards the verification of industrial embedded software systems. We extended the language support in Theta with formal semantics. In addition, the new language constructs and operators are transformed into the formal language inside Theta. We also need new algorithms to solve the verification problem: we implemented Newton-style refinement algorithms in Theta to verify software with bitvectors and bitwise operators efficiently.