Mining-Based Invariant Extraction for Bounded Model Checking of Software
Xueqi Cheng and Michael S. Hsiao

• Motivation:
  • Software increasingly present in wireless systems
  • Software Bounded Model Checking (BMC): An automatic verification technique for checking whether the code satisfies a temporal property in paths with bounded length $k$

• Limitations in modern-day software SAT-based BMC
  • Lost high-level information when converting a program to propositional formula
  • Implications on variable relations and program structures are harder to discover at Boolean level than at high-level

• Novel Mining-based Software Model Checking Framework:
  • Use data mining to learn high-level invariants and add them to the original program
  • Fill in the gap between high-level programming language and Boolean-level SAT solving
  • Data mining is more flexible and cost-efficient compared to static program analysis

• Related Variables:
  Any variables that directly or indirectly contribute to the values of variables involved in the target assertion to be checked

• Must make tradeoffs between the invariants added and propositional formula size
  • Rank the value of each invariant through weight assignment
  • Weight is roughly determined by statement distance and variable distance between the invariant and target assertion

• Experimental Results:
  Optimization rules can effectively filter out the redundant and incorrect properties and lead to high rate of correctness

By adding the invariant(s) to the original program, the performance of bounded model checking can be significantly improved