Towards SMT-Style Reasoning about Floating-Point Arithmetic

Aleksandar Zeljić
Uppsala University

Philipp Rümmer
Uppsala University

Christoph Wintersteiger
MSR Cambridge

Workshop Progress in Decision Procedures
Belgrade
March 30^{th} 2013

Motivation

- Verification of software using FPA
- Provide tools for embedded systems development
- Reasoning about FPA
- SMT enables reasoning in various domains
- Apply the SMT approach to FPA

Some existing approaches

Interval reasoning [Haller et al., FMCAD '12]

- Interval propagation
- Abstract interpretation
- Uses generalization of conflict analysis algorithm
- Good for proving unsatisfiability
- Not good at computing models

Encoding as bit-vector arithmethic [Brillout et al., FMCAD '09]

- Translation to BVA uses knowledge of hardware implementations
- Uses bit-blasting to reduce BVA to propositional logic

Challenges

Bit-blasting

- Introduce new boolean variables
- Add constraints over introduced variables to the formula

- Bit-blasting is often time- and memory-consuming
- Multiplication can take 25000 variables
- Subsequent reasoning can be very quick by comparison

Approximations and Model refinement

- Use of approximations in encodings would be beneficial
- Generate a model that can be refined

Types of approximation

- Under-approximations
- Over-approximations
- Computation with reduced precision

Approximations and Model refinement

Refinement loop

```
while(1)
{
  bvProb = appFpa2bv(fpaProb,appLevel);
  propProb = bitBlast(bvProb);
  model = getModel(propProblem);
  if(!model || !satisfies(model,fpaProb))
     appLevel++;
  else
     output(model);
}
```

Approximating FP operations

- Division uses an iterative algorithm
- Over-approximate by fixing the number of iterations
- FPA is always performed with a given precision
- All operations can be performed with a smaller precision
- Removing rounding could also be a form of approximation

Future work

- Evaluate the outlined ideas
- Come up with different operation schemes
- Look into generation of robust models
- Investigate lazy assertion of constraints
- Implement a theory solver for FPA

Thanks for your attention!