Verifying Bit-vector Invertibility Conditions in Coq

Burak Ekici, Arjun Viswanathan, Yoni Zohar, Clark Barrett, Cesare Tinelli

Introduction

- Bit-vectors are useful for many verification tasks
- Many applications require reasoning about quantified bit-vectors
- SMT solvers deal with quantified formulas using quantifier-instantiation techniques
- CVC4 uses invertibility conditions as part of a quantifier instantiation technique for bit-vectors

$$\forall s, t : BV_n.\ IC[s,t] \iff \exists x : BV_n.\ \ell[x,s,t]$$

Previous Work

- Niemetz et al. [CAV 2018] generated 162 invertibility equivalences and verified them automatically for bit-widths up to 65
- Niemetz et al. [CADE 2019] encoded these equivalences in UFNIA to verify 75% of the equivalences for arbitrary bit-width

Contributions

- We proved 11 equivalences from the rest of the 25% of the equivalences in the Coq proof assistant for arbitrary bit-width
- We used a Coq library originally used for SMTCoq developed by Ekici et al. [CAV 2017] and extended its signature

Invertibility Conditions

An *invertibility condition* for a variable x in a bit-vector literal

$$\ell\,[\,x\;,\;s\;,\;t\,]$$

is a formula

$$IC\,[\,s\;,\;t\,]$$

s.t. the following *invertibility equivalence* is valid in the theory of bit-vectors:

$$\forall s, t : BV_n.\ IC[s,t] \iff \exists x : BV_n.\ \ell[x,s,t]$$

Result Summary

$\ell[x]$	$=$	$\neq$	$<_u$	$>_u$	$\leq_u$	$\geq_u$
$-x \bowtie t$	✓✓	✓	✓	✓	✓	✓
$\sim x \bowtie t$	✓✓	✓	✓	✓	✓	✓
$x \ \& \ s \bowtie t$	✓	✓	✓	✓	✓	✓
$x \mid s \bowtie t$	✓	✓	✓	✓	✓	✓
$x \ll s \bowtie t$	✓	✓	✓	✓	✓	✓
$s \ll x \bowtie t$	✓✓	✓	✓	✓	✓	✓
$x \gg s \bowtie t$	✓✓	✓	✓	✗	✓	✓
$s \gg x \bowtie t$	✓✓	✓	✓	✓	✓	✓
$x \gg_a s \bowtie t$	✓	✓	✓	✓	✓	✓
$s \gg_a x \bowtie t$	✓✓	✓	✓	✓	✓	✓
$x + s \bowtie t$	✓✓	✓	✓	✓	✓	✓

✓ Verified in Coq

✓ Verified in SMT

✓✓ Verified in Coq and SMT

✗ Verified in neither Coq nor SMT

Future Work

$\ell[x]$	$=$	$\neq$	$<_u$	$>_u$	$\leq_u$	$\geq_u$	$<_s$	$>_s$	$\leq_s$	$\geq_s$
$-x \bowtie t$	✓✓	✓	✓	✓	✓	✓				
$\sim x \bowtie t$	✓✓	✓	✓	✓	✓	✓				
$x \;\&\; s \bowtie t$	✓	✓	✓	✓	✓	✓				
$x \mid s \bowtie t$	✓	✓	✓	✓	✓	✓		...		...
$x \ll s \bowtie t$	✓	✓	✓	✓	✓	✓				
$s \ll x \bowtie t$	✓✓	✓	✓	✓	✓	✓		...		...
$x \gg s \bowtie t$	✓✓	✓	✓	✗	✓	✓		...		...
$s \gg x \bowtie t$	✓✓	✓	✓	✓	✓	✓				
$x \gg_a s \bowtie t$	✓	✓	✓	✓	✓	✓				
$s \gg_a x \bowtie t$	✓✓	✓	✓	✓	✓	✓				
$x + s \bowtie t$	✓✓	✓	✓	✓	✓	✓				
$x \cdot s \bowtie t$										
$x \text{ div } s \bowtie t$				...		...		...		
$s \text{ div } x \bowtie t$				...		...		...		
$x \text{ mod } s \bowtie t$										
$s \text{ mod } x \bowtie t$										

✓ Verified in Coq

✓ Verified in SMT

✓✓ Verified in Coq and SMT

✗ Verified in neither Coq nor SMT