Verifying Bit-vector Invertibility Conditions in Coq

Burak Ekici[1] Arjun Viswanathan[2] Yoni Zohar[3] Clark Barrett[3] Cesare Tinelli[2]

[1] University of Innsbruck [2] University of Iowa [3] Stanford University

Invertibility Equivalence:

$$\forall s,t : BV_n.\ \underbrace{IC[s,t]}_{\text{Invertibility Condition}} \iff \exists x : BV_n.\ \ell[x,s,t]$$

- The CVC4 SMT-solver uses invertibility equivalences to solve quantified bit-vector formulas
- Proofs of these equivalences for arbitrary bit-widths certify the solver's results

Examples

$$\top \iff \exists x.\ x + s = t$$

$$t\ \&\ s = t \iff \exists x.\ x\ \&\ s = t$$

$$t <_u (\sim s \gg s) \iff \exists x.\ (x \gg s) <_u t$$

Results

$\ell[x]$	$=$	$\neq$	$<_u$	$>_u$	$\leq_u$	$\geq_u$
$-x \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$\sim x \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$x\ \&\ s \bowtie t$	$\color{blue}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$x \mid s \bowtie t$	$\color{blue}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$x \ll s \bowtie t$	$\color{blue}{\checkmark}$	$\color{blue}{\checkmark}$	$\color{green}{\checkmark}$	$\color{blue}{\checkmark}$	$\color{green}{\checkmark}$	$\color{blue}{\checkmark}$
$s \ll x \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$x \gg s \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{red}{\times}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$s \gg x \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$x \gg_a s \bowtie t$	$\color{blue}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$
$s \gg_a x \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{blue}{\checkmark}$	$\color{blue}{\checkmark}$	$\color{blue}{\checkmark}$	$\color{blue}{\checkmark}$
$x + s \bowtie t$	$\color{blue}{\checkmark}\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$	$\color{green}{\checkmark}$

$\color{blue}{\checkmark}$ Verified in Coq

$\color{green}{\checkmark}$ Verified in SMT

$\color{blue}{\checkmark}\color{green}{\checkmark}$ Verified in Coq and SMT

$\color{red}{\times}$ Verified in neither Coq nor SMT

Contributions

Previous Work

[Niemetz et al., CAV 2018]

- generated 162 invertibility equivalences
- proved them using SMT-solvers for bit-widths up to 65

[Niemetz et al., CADE 2019]

- encoded the equivalences in theories supported by SMT-solvers
- verified equivalences for parametric widths
- succeeded on ≈75% of the equivalences

This work

1. formalized a representative subset of the 162 invertibility equivalences in Coq
2. extended a Coq bit-vector library to support these equivalences
3. proved 18 of them for arbitrary bit-width

Bit-vector Library

Basic Signature

Arithmetic: $+,\ -,\ \cdot$

Shift: $\ll,\ \gg$

Bit-wise logical: $\&,\ |,\ \sim$

Concatenation: $\circ$

Comparison: $=,\ \neq,\ <_u,\ >_u,\ <_s,\ >_s$

Extended Signature

Comparison: $\leq_u,\ \geq_u$

Shift: $\gg_a$

Shifts redefined: $\underline{\ll},\ \underline{\gg},\ \underline{\gg_a}$

Bitvector Representations

	SMTLib[CAV 18]	Encoding[CADE 19]	Coq Library(Our work)
Bit-vector Representation:	Bit-vector of width n One sort for each n	Bit-vector of width n Translated to NIA and UF	Bit-vector of width n List of Booleans over 2 layers
Expressivity:	n cannot be symbolic	Allows quantification over n	Bit-vectors dependent on n
Verification:	Automatic proofs using SMT solvers	Automatic proofs using SMT solvers	Manual proofs in Coq
Results	Verified all equivalences for n = 1 to 65	Verified ≈75% of equivalences	Verified 18 equivalences