

## 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

$\ell[x]$	=	≠	< <sub>u</sub>	> <sub>u</sub>	≤ <sub>u</sub>	≥ <sub>u</sub>
$-x \boxtimes t$	✓	✓	✓	✓	✓	✓
$\sim x \boxtimes t$	✓	✓	✓	✓	✓	✓
$x \& s \boxtimes t$	✓	✓	✓	✓	✓	✓
$x   s \boxtimes t$	✓	✓	✓	✓	✓	✓
$x \ll s \boxtimes t$	✓	✓	✓	✓	✓	✓
$s \ll x \boxtimes t$	✓	✓	✓	✓	✓	✓
$x \gg s \boxtimes t$	✓	✓	✓	✗	✓	✓
$s \gg x \boxtimes t$	✓	✓	✓	✓	✓	✓
$x \gg_a s \boxtimes t$	✓	✓	✓	✓	✓	✓
$s \gg_a x \boxtimes t$	✓	✓	✓	✓	✓	✓
$x + s \boxtimes t$	✓	✓	✓	✓	✓	✓

✓ Verified in Coq

✓ Verified in SMT

✓ Verified in Coq and SMT

✗ 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

- formalized a representative subset of the 162 invertibility equivalences in Coq
- extended a Coq bit-vector library to support these equivalences
- 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:  $\leq\leq$ ,  $\geq\geq$ ,  $\gg_a$

## Bitvector Representations

	SMTLib[CAV 18]	Encoding[CADE 19]	Coq Library(Our work)
<b>Bit-vector Representation:</b>	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
<b>Expressivity:</b>	n cannot be symbolic	Allows quantification over n	Bit-vectors dependent on n
<b>Verification:</b>	Automatic proofs using SMT solvers	Automatic proofs using SMT solvers	Manual proofs in Coq
<b>Results</b>	Verified all equivalences for n = 1 to 65	Verified ≈75% of equivalences	Verified 18 equivalences