

# Verifying Bit-vector Invertibility Conditions in Coq

Burak Ekici<sup>1</sup> Arjun Viswanathan<sup>2</sup> Yoni Zohar<sup>3</sup> Clark Barrett<sup>3</sup> Cesare Tinelli<sup>2</sup>

<sup>1</sup> University of Innsbruck 

<sup>2</sup> University of Iowa 

<sup>3</sup> Stanford University

# Invertibility Equivalence:

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

- 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

### Results

$\ell[x]$	=	$\neq$	$<_u$	$>_u$	$\leq_u$	$\geq_u$
$-x \bowtie t$	<b>~</b>	<b>√</b>	✓	✓	✓	✓
$\sim x\bowtie t$	<b>V</b>	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
$x \ \& \ s \bowtie t$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
$x \mid s \bowtie t$	$\checkmark$	$\checkmark$	✓	$\checkmark$	$\checkmark$	$\checkmark$
$x <\!\!< s \bowtie t$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
$s <\!\!< x \bowtie t$	<b>V</b>	$\checkmark$	✓	$\checkmark$	$\checkmark$	$\checkmark$
$x \gg s \bowtie t$	<b>V</b>	$\checkmark$	$\checkmark$	×	$\checkmark$	$\checkmark$
$s >\!\!> x \bowtie t$	<b>V</b>	<b>√</b>	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
$x \gg_a s \bowtie t$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	✓
$s \gg_a x \bowtie t$	<b>V</b>	<b>√</b>	✓	$\checkmark$	$\checkmark$	$\checkmark$
$x + s \bowtie t$	<b>√√</b>	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	✓

- √ Verified in Coq
- √ Verified in SMT
- √ Verified in Coq and SMT
- imes Verified in neither Coq nor SMT

#### **Contributions**

#### **Previous Work**

[Niemetz et al., CAV 2018]

- generated 162 invertibility equivalences
- proved them using SMT-solvers for bitwidths 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:  $\leq$ ,  $\geq$ ,  $\geq$ a

# **Bitvector Representations**

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	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 =	Verified ≈75% of equivalences	Verified 18 equivalences				