Solving Quantified Bit-Vectors using Invertibility Conditions

Aina Niemetz* **Mathias Preiner*** Andrew Reynolds†
Clark Barrett* Cesare Tinelli†

* Stanford University † The University of Iowa

CAV 2018
July 14-17, 2018
Oxford, UK

Motivation

Example: Prove unsatisfiability of ψ

$$\psi = \forall x \,.\, (x + s \not\approx t) \qquad\qquad x,\ s,\ t \ldots \text{bit-vectors of size } N$$

State of the Art in SMT: Quantifier instantiation-based techniques

Find conflicting ground instances of the formula

- Crucial to find good instantiation candidates

- Naive: Enumerate values for x (2^N possible instantiations)
- Better: Instantiate with symbolic term $t - s$

$$\underbrace{(t - s) + s \not\approx t}_{\text{UNSAT}}$$

  - Idea: Compute symbolic inverses of bit-vector operators

Symbolic Inverses

Inspired by propagation-based local search approach [CAV'16]

- Concrete values vs. symbolic terms

Example: $x + s \approx t$ (solve for x)

- Inverse: $x = t - s$

- Unconditional inverses not always possible

Example: $x \cdot s \approx t$ (solve for x)

- No inverse e.g., $x \cdot 2 \approx 3$
- Identify condition under which $x \cdot s \approx t$ is invertible

Invertibility Conditions

Exact condition under which a bit-vector operation is solvable for some x.

Example: $x \cdot s \approx t$ (solve for x)

- Invertibility condition: $((-s \mid s)\ \&\ t) \approx t$
- $((-s \mid s)\ \&\ t) \approx t \ \Leftrightarrow\ x \cdot s \approx t$

Invertibility conditions

- 162 ICs for: $\{\approx, \not\approx, <_u, \leq_u, >_u, \geq_u, <_s, \leq_s, >_s, \geq_s\}$
  $\times\{\sim, \&, \mid, \ll, \gg, \gg_a, -, +, \cdot, \mathsf{mod}, \div, \circ, [:]\}$
- 83 crafted manually
- 79 synthesized with SyGuS (syntax-guided synthesis)

Invertibility Conditions

$\ell[x]$	$\approx$	$\not\approx$
$x \cdot s \bowtie t$	$(-s \mid s)\ \&\ t \approx t$	$s \not\approx 0 \vee t \not\approx 0$
$x \bmod s \bowtie t$	$\sim(-s) \geq_u t$	$s \not\approx 1 \vee t \not\approx 0$
$s \bmod x \bowtie t$	$(t + t - s)\ \&\ s \geq_u t$	$s \not\approx 0 \vee t \not\approx 0$
$x \div s \bowtie t$	$(s \cdot t) \div s \approx t$	$s \not\approx 0 \vee t \not\approx \sim 0$
$s \div x \bowtie t$	$s \div (s \div t) \approx t$	$\begin{cases} s\ \&\ t \not\approx 0 & \text{for } \kappa(s) = 1 \\ \top & \text{otherwise} \end{cases}$
$x\ \&\ s \bowtie t$	$t\ \&\ s \approx t$	$s \not\approx 0 \vee t \not\approx 0$
$x \mid s \bowtie t$	$t \mid s \approx t$	$s \not\approx \sim 0 \vee t \not\approx \sim 0$
$x \gg s \bowtie t$	$(t \ll s) \gg s \approx t$	$t \not\approx 0 \vee s <_u \kappa(s)$
$s \gg x \bowtie t$	$\bigvee_{i=0}^{\kappa(s)} s \gg i \approx t$	$s \not\approx 0 \vee t \not\approx 0$
$x \gg_a s \bowtie t$	$(s <_u \kappa(s) \Rightarrow (t \ll s) \gg_a s \approx t) \wedge$ $(s \geq_u \kappa(s) \Rightarrow (t \approx \sim 0 \vee t \approx 0))$	$\top$
$s \gg_a x \bowtie t$	$\bigvee_{i=0}^{\kappa(s)} s \gg_a i \approx t$	$(t \not\approx 0 \vee s \not\approx 0) \wedge$ $(t \not\approx \sim 0 \vee s \not\approx \sim 0)$
$x \ll s \bowtie t$	$(t \gg s) \ll s \approx t$	$t \not\approx 0 \vee s <_u \kappa(s)$
$s \ll x \bowtie t$	$\bigvee_{i=0}^{\kappa(s)} s \ll i \approx t$	$s \not\approx 0 \vee t \not\approx 0$
$x \circ s \bowtie t$	$s \approx t[\kappa(s) - 1 : 0]$	$\top$
$s \circ x \bowtie t$	$s \approx t[\kappa(t) - 1 : \kappa(t) - \kappa(s)]$	$\top$

Table 2. Conditions for the invertibility of bit-vector operators over (dis)equality. Those for $\cdot$, & and | are given modulo commutativity of those operators.

$\ell[x]$	$<_u$	$>_u$
$x \cdot s \bowtie t$	$t \not\approx 0$	$t <_u -s \mid s$
$x \bmod s \bowtie t$	$t \not\approx 0$	$t <_u \sim(-s)$
$s \bmod x \bowtie t$	$t \not\approx 0$	$t <_u s$
$x \div s \bowtie t$	$0 <_u s \wedge 0 <_u t$	$\sim 0 \div s >_u t$
$s \div x \bowtie t$	$0 <_u \sim(-t\ \&\ s) \wedge 0 <_u t$	$t <_u \sim 0$
$x\ \&\ s \bowtie t$	$t \not\approx 0$	$t <_u s$
$x \mid s \bowtie t$	$s <_u t$	$t <_u \sim 0$
$x \gg s \bowtie t$	$t \not\approx 0$	$t <_u \sim s \gg s$
$s \gg x \bowtie t$	$t \not\approx 0$	$t <_u s$
$x \gg_a s \bowtie t$	$t \not\approx 0$	$t <_u \sim 0$
$s \gg_a x \bowtie t$	$(s <_u t \vee s \geq_s 0) \wedge t \not\approx 0$	$s <_s (s \gg \sim t) \vee t <_u s$
$x \ll s \bowtie t$	$t \not\approx 0$	$t <_u \sim 0 \ll s$
$s \ll x \bowtie t$	$t \not\approx 0$	$\bigvee_{i=0}^{\kappa(s)} (s \ll i) >_u t$
$x \circ s \bowtie t$	$t_x \approx 0 \Rightarrow s <_u t_s$ where $t_x = t[\kappa(t) - 1 : \kappa(t) - \kappa(x)], t_s = t[\kappa(s) - 1 : 0]$	$t_x \approx \sim 0 \Rightarrow s >_u t_s$
$s \circ x \bowtie t$	$s \leq_u t_s \wedge (s \approx t_s \Rightarrow t_x \not\approx 0)$ where $t_x = t[\kappa(x) - 1 : 0], t_s = t[\kappa(t) - 1 : \kappa(t) - \kappa(s)]$	$s \geq_u t_s \wedge s \approx t_s \Rightarrow t_x \not\approx \sim 0$

Table 3. Conditions for the invertibility of bit-vector operators over unsigned inequality. Those for $\cdot$, & and | are given modulo commutativity of those operators.

$\ell[x]$	$<_u$	$>_u$	$<_s$	$>_s$	$\leq_u, \geq_u, \leq_s, \geq_s$
$x \bowtie t$					
$-x \bowtie t$	$t \not\approx 0$	$t \not\approx \sim 0$	$t \not\approx \min_s$	$t \not\approx \max_s$	$\top$
$\sim x \bowtie t$					
$x + s \bowtie t$					

Table 5. Conditions for the invertibility for $x \bowtie t$ and bit-vector operators $\{-, \sim, +\}$ over inequality. The one for $+$ given modulo commutativity of $+$.

$\ell[x]$	$\leq_u$	$\geq_u$
$x \cdot s \bowtie t$	$\top$	$-s \mid s \geq_u t$
$x \bmod s \bowtie t$	$\top$	$\sim(-s) \geq_u t$
$s \bmod x \bowtie t$	$\top$	$(t + t - s)\ \&\ s \geq_u t \vee t <_u s$
$x \div s \bowtie t$	$s \mid t \geq_u \sim(-s)$	$(s \cdot t) \div t\ \&\ s \approx s$
$s \div x \bowtie t$	$0 <_u \sim s \mid t$	$\top$
$x\ \&\ s \bowtie t$	$\top$	$s \geq_u t$
$x \mid s \bowtie t$	$t \geq_u s$	$\top$
$x \gg s \bowtie t$	$\top$	$(t \ll s) \gg s \approx t$
$s \gg x \bowtie t$	$\top$	$s \geq_u t$
$x \gg_a s \bowtie t$	$\top$	$\top$
$s \gg_a x \bowtie t$	$s <_u \min_s \vee t \geq_u s$	$s \geq_u \sim s \vee s \geq_u t$
$x \ll s \bowtie t$	$\top$	$\sim 0 \ll s \geq_u t$
$s \ll x \bowtie t$	$\top$	$\bigvee_{i=0}^{\kappa(s)} (s \ll i) \geq_u t$
$x \circ s \bowtie t$	$t_x \approx 0 \Rightarrow s \leq_u t_s$ where $t_x = t[\kappa(t) - 1 : \kappa(t) - \kappa(x)], t_s = t[\kappa(s) - 1 : 0]$	$t_x \approx \sim 0 \Rightarrow s \geq_u t_s$
$s \circ x \bowtie t$	$s \leq_u t_s$ where $t_x = t[\kappa(x) - 1 : 0], t_s = t[\kappa(t) - 1 : \kappa(t) - \kappa(s)]$	$s \geq_u t_s$

Table 6. Conditions for the invertibility of bit-vector operators over $\leq_u$ and $\geq_u$. Those for $\cdot$, & and | are given modulo commutativity of those operators.

$\ell[x]$	$<_s$	$>_s$
$x \cdot s \bowtie t$	$\sim(-t)\ \&\ (-s \mid s) <_s t$	$t <_s t - ((s \mid t) \mid -s)$
$x \bmod s \bowtie t$	$\sim t <_s (-s \mid -t)$	$(s >_s 0 \Rightarrow t <_s \sim(-s)) \wedge$ $(s \leq_s 0 \Rightarrow t \not\approx \max_s) \wedge$ $(t \not\approx 0 \vee s \not\approx 1)$
$s \bmod x \bowtie t$	$s <_s t \vee 0 <_s t$	$(s \geq_s 0 \Rightarrow s >_s t) \wedge$ $(s <_s 0 \Rightarrow ((s - 1) \gg 1) >_s t)$
$x \div s \bowtie t$	$t \leq_s 0 \Rightarrow \min_s \div s <_s t$	$\sim 0 \div s >_s t \vee \max_s \div s >_s t$
$s \div x \bowtie t$	$s <_s t \vee t \geq_s 0$	$\begin{cases} s >_s t & \text{for } \kappa(s) = 1 \\ (s \geq_s 0 \Rightarrow s >_s t) \wedge & \text{otherwise} \\ (s <_s 0 \Rightarrow s \gg 1 >_s t) \end{cases}$
$x\ \&\ s \bowtie t$	$\sim(-t)\ \&\ s <_s t$	$t <_s s\ \&\ \max_s$
$x \mid s \bowtie t$ $s \mid x \bowtie t$	$\sim(s - t) \mid s <_s t$	$t <_s (s \mid \max_s)$
$x \gg s \bowtie t$	$\sim(-t) \gg s <_s t$	$t <_s (\max_s \ll s) \gg s$
$s \gg x \bowtie t$	$s <_s t \vee 0 <_s t$	$(s <_s 0 \Rightarrow s \gg 1 >_s t) \wedge$ $(s \geq_s 0 \Rightarrow s >_s t)$
$x \gg_a s \bowtie t$	$\min_s \gg_a s <_s t$	$t <_s \max_s \gg s$
$s \gg_a x \bowtie t$	$s <_s t \vee 0 <_s t$	$t <_s s\ \&\ \max_s \wedge t <_s s \mid \max_s$
$x \ll s \bowtie t$	$(\min_s \gg s) \ll s <_s t$	$t <_s (\max_s \ll s)\ \&\ \max_s$
$s \ll x \bowtie t$	$\min_s \ll s <_u t + \min_s$	$\bigvee_{i=0}^{\kappa(s)} (s \ll i) >_s t$
$x \circ s \bowtie t$	$t_x \approx \min_s \Rightarrow s <_u t_s$ where $t_x = t[\kappa(t) - 1 : \kappa(t) - \kappa(x)], t_s = t[\kappa(s) - 1 : 0]$	$t_x \approx \max_s \Rightarrow s >_u t_s$
$s \circ x \bowtie t$	$(s \leq_s t_s) \wedge (s \approx t_s \Rightarrow t_x \not\approx 0)$ where $t_x = t[\kappa(x) - 1 : 0], t_s = t[\kappa(t) - 1 : \kappa(t) - \kappa(s)]$	$(s \geq_s t_s) \wedge (s \approx t_s \Rightarrow t_x \not\approx \sim 0)$

Table 7. Conditions for the invertibility of bit-vector operators over $<_s$ and $>_s$. Those for $\cdot$, & and | are given modulo commutativity of those operators.

$\ell[x]$	$\leq_s$	$\geq_s$
$x \cdot s \bowtie t$	$\sim(s \approx 0 \wedge t <_s s)$	$(-s \mid s)\ \&\ \max_s \geq_s t$
$x \bmod s \bowtie t$	$\sim 0 <_s -s\ \&\ t$	$t <_s s \vee 0 \geq_s s$
$s \bmod x \bowtie t$	$t <_u \min_s \vee t \geq_s s$	$(s \geq_s 0 \Rightarrow s \geq_s t) \wedge$ $((s <_s 0 \wedge t \geq_s 0) \Rightarrow s - t >_u t)$
$x \div s \bowtie t$	$((s \cdot t) \div s \approx t) \vee$ $(t \leq_s 0 \Rightarrow \min_s \div s <_s t)$	$(\sim 0 \div s \geq_s t) \vee (\max_s \div s \geq_s t)$
$s \div x \bowtie t$	$t \geq_s \sim 0 \vee t \geq_s s$	$(s \geq_s 0 \Rightarrow s \geq_s t) \wedge$ $(s <_s 0 \Rightarrow s \gg 1 \geq_s t)$
$x\ \&\ s \bowtie t$	$s \geq_u t\ \&\ \min_s$	$s\ \&\ t \approx t \vee t <_s (t - s)\ \&\ s$
$x \mid s \bowtie t$	$t \geq_s s \mid \min_s$	$s\ \&\ t$
$x \gg s \bowtie t$	$t \geq_s t \gg s$	$s \not\approx 0 \Rightarrow \sim 0 \gg s \geq_s t$
$s \gg x \bowtie t$	$t <_u \min_s \vee t \geq_s s$	$(s <_s 0 \Rightarrow s \gg 1 \geq_s t) \wedge$ $(s \geq_s 0 \Rightarrow s \geq_s t)$
$x \gg_a s \bowtie t$	$t \geq_s \sim(\max_s \gg s)$	$\max_s \gg s \geq_s t$
$s \gg_a x \bowtie t$	$t \geq_s 0 \vee t \geq_s s$	$t \geq_u \sim t \vee s \geq_s t$
$x \ll s \bowtie t$	$t \gg (t \gg s) <_u \min_s$	$(\max_s \ll s)\ \&\ \max_s \geq_s t$
$s \ll x \bowtie t$	$t \gg s <_u \min_s$	$\bigvee_{i=0}^{\kappa(s)} (s \ll i) \geq_s t$
$x \circ s \bowtie t$	$t_x \approx \min_s \Rightarrow s \leq_u t_s$ where $t_x = t[\kappa(t) - 1 : \kappa(t) - \kappa(x)], t_s = t[\kappa(s) - 1 : 0]$	$t_x \approx \max_s \Rightarrow s \geq_u t_s$
$s \circ x \bowtie t$	$s \leq_s t_s$ where $t_x = t[\kappa(x) - 1 : 0], t_s = t[\kappa(t) - 1 : \kappa(t) - \kappa(s)]$	$s \geq_s t_s$

Table 8. Conditions for the invertibility of bit-vector operators over $\leq_s$ and $\geq_s$. Those for $\cdot$, & and | are given modulo commutativity of those operators.

Synthesizing Invertibility Conditions

Formulate as SyGuS problem

$$\exists C \forall s \forall t. ((\exists x. x \diamond s \bowtie t) \Leftrightarrow C(s,t))$$

Operators: $\diamond \in \{\&, |, \ll, \gg, \gg_a, \cdot, \mathsf{mod}, \div, \circ\}$
Relations: $\bowtie \in \{\approx, \not\approx, <_u, \leq_u, >_u, \geq_u, <_s, \leq_s, >_s, \geq_s\}$

Expand innermost $\exists$ quantifier (4-bit)

$$\exists C \forall s \forall t. (\bigvee_{i=0}^{15} i \diamond s \bowtie t) \Leftrightarrow C(s,t)$$

Results

- Synthesized 118 conditions (out of 140) with CVC4
- Verified correctness of 94.6% the 162 ICs for bit-width 1 to 65

From Invertibility Conditions to Symbolic Instantiations

Hilbert choice functions $\varepsilon x.\, \varphi[x]$

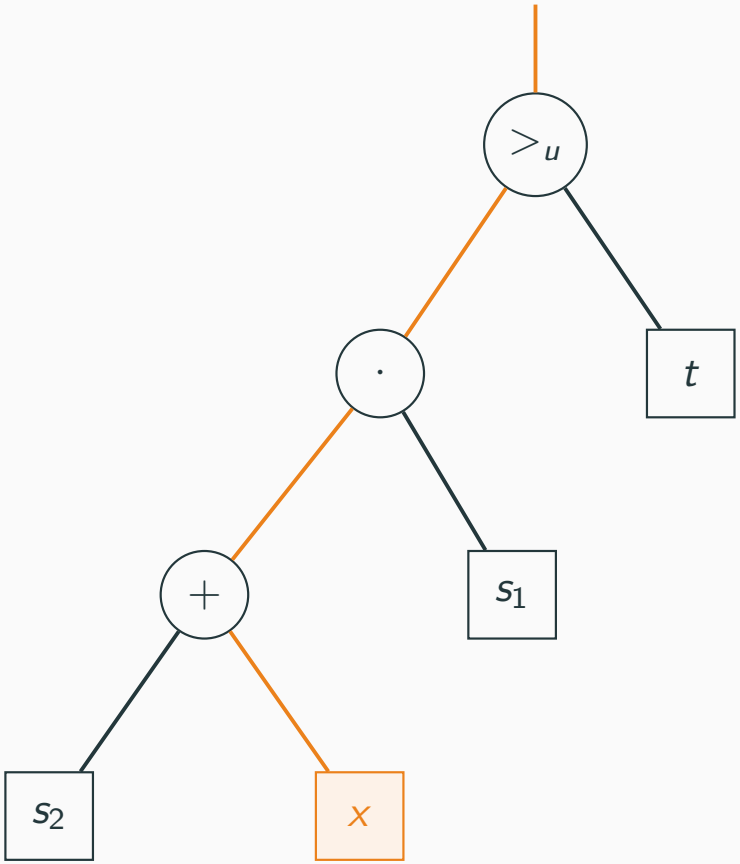
- Represents a solution for $\varphi[x]$ if there is one
- Represents arbitrary value otherwise

Embed invertibility conditions into Hilbert choice functions

- BV literal: $l[x] := x \diamond s \bowtie t$
- Inv. cond.: $IC(s,t) \;\Leftrightarrow\; l[x]$
- Symbolic term: $\varepsilon y.\, (IC(s,t) \;\Rightarrow\; l[y])$

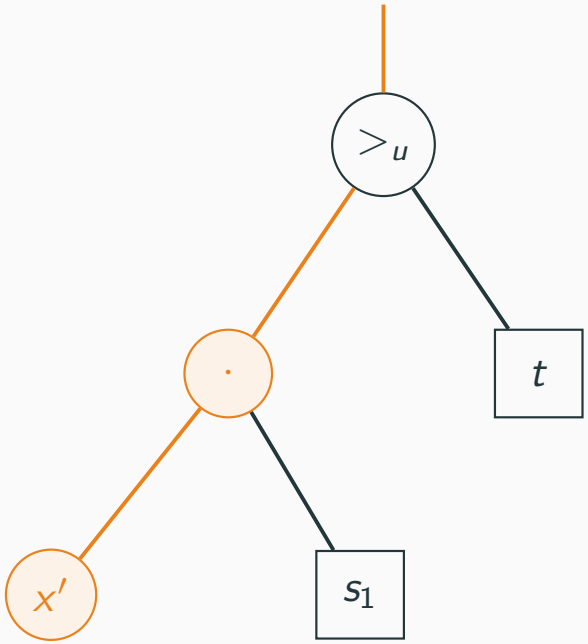
▶ Choice functions express all conditional solutions in one symbolic term

Example: $\forall x.\, (s_2 + x) \cdot s_1 >_u t$



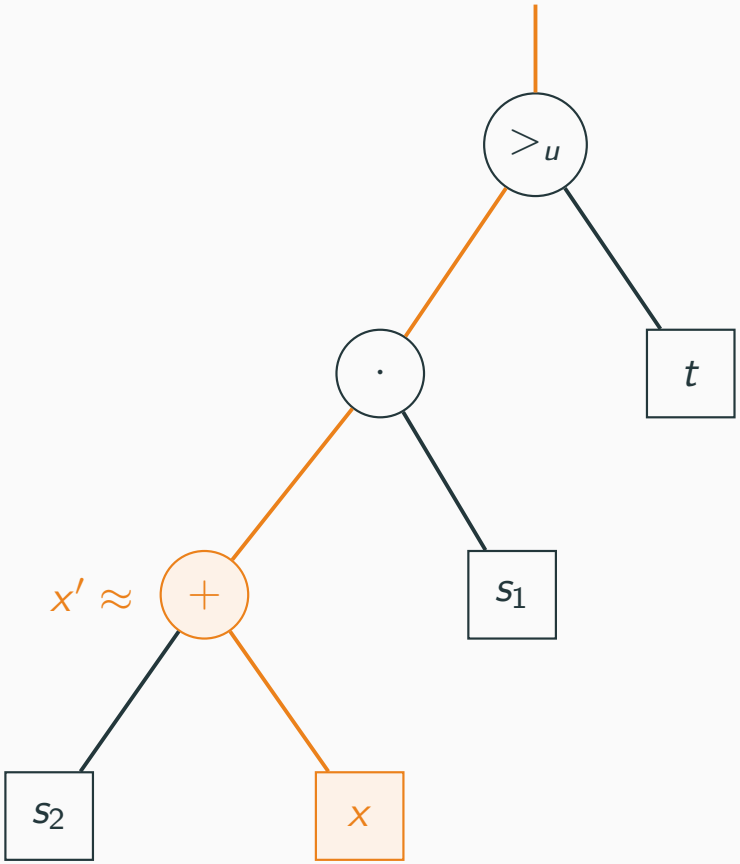
1. Pick variable to solve for (x)
2. Compute inverse/invertibility conditions along path to x

Example: $\forall x.\,(s_2 + x) \cdot s_1 >_u t$



1. Pick variable to solve for (x)
2. Compute inverse/invertibility conditions along path to x
3. $x' \cdot s_1 >_u t$
   - $IC_{x'} = t <_u -s \mid s$
   - $x' = \varepsilon y.\,(IC_{x'} \Rightarrow y \cdot s_1 >_u t)$

Example: $\forall x.\,(s_2 + x) \cdot s_1 >_u t$



1. Pick variable to solve for (x)
2. Compute inverse/invertibility conditions along path to x
3. $x' \cdot s_1 >_u t$
   - $IC_{x'} = t <_u -s \mid s$
   - $x' = \varepsilon y.\,(IC_{x'} \Rightarrow y \cdot s_1 >_u t)$
4. $s_2 + x \approx x'$
   - $IC_x = \top$
   - $x = x' - s_2$

Instantiation for x: $\varepsilon y.\,(t <_u -s \mid s \Rightarrow s_1 \cdot y >_u t) - s_2$

Multiple Variable Occurrences

Non-linear constraints (multiple occurrences of a variable)

- Try to linearize with rewriting/normalization
  e.g., $x + x + s \approx t \to 2 \cdot x + s \approx t$
- Else: Replace all but one occurrence with value in current model $\mathcal{I}$
  e.g., $x \cdot x + s \approx t \to x \cdot x^{\mathcal{I}} + s \approx t$

- Future work: Use SyGuS to synthesize ICs for non-linear cases

Unit linear invertible formulas

- If $\forall x.\, \varphi[x]$ is linear in x (only one occurrence of x)

- Quantifier elimination: reduce to quantifier-free bit-vector formula

Experiments

	CVC4$_{\text{base}}$	**Q3B**	**Boolector**	**Z3**	**CVC4$_{\text{ic}}$**
keymaera (4035)	3823	3805	4025	**4031**	3993
psyco (194)	**194**	99	193	193	190
scholl (374)	239	214	**289**	271	246
tptp (73)	**73**	**73**	72	**73**	**73**
uauto (284)	112	256	180	190	**274**
wintersteiger (191)	168	**184**	154	162	168
Total (5151)	4609	4631	4913	4920	**4944**

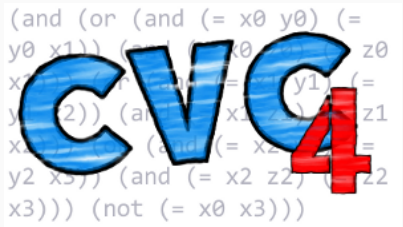
Limits: 300 seconds CPU time limit, 100G memory limit

CVC4$_{\text{ic}}$ won division BV at SMT-COMP 2018

Conclusion

Summary

- 162 invertibility conditions for various bit-vector operators
- SyGus really useful for synthesizing ICs
- Leverage ICs to compute symbolic quantifier instantiations
- Quantifier elimination for unit linear invertible class of formulas
  ▷ Applies to 25.6% of benchmarks
- All techniques implemented in CVC4
  `https://github.com/cvc4/cvc4`



Future Work

- ICs for non-linear literals/multiple constraints
- Bit-width independent correctness proofs for ICs

References i


Aina Niemetz and Mathias Preiner and Armin Biere. Precise and Complete Propagation Based Local Search for Satisfiability Modulo Theories. CAV, Pages 199-217. 2018