

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

Contributions

- 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
- 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