# Invited Talk: AVR: Word-Level Verification by Equality Abstraction of Data State

Karem A. Sakallah

*Computer Science and Engineering*
*Universityy of Michigan, 2260 Hayward Ave. Ann Arbor, MI, 48109, USA*

## Abstract

AVR is, primarily, an IC3/PDR-style model checker for safety properties of word-level hardware. It scales to large designs by automatically abstracting the state space of word-level variables such that only equality and dis-equality among the variables are preserved regardless of their exact bit-precise assignments. The abstraction is parameterized by a user-specified bit width threshold $w$ which can range from 1 to the largest bit width in the design. Reachability queries employ EUF logic for word-level variables whose width is larger than $w$ and BV logic for variables whose width is less than or equal to $w$. This provides for a range of data abstractions that enable AVR to successfully handle a diverse set of benchmarks. AVR produces compact word-level inductive invariants for safe designs or counterexamples for unsafe designs. AVR was the overall winner of the 2020 Hardware Model Checking Competition. In this talk I will analyze AVR's performance on the 2020 HWMCC benchmarks under a variety of bit width thresholds. I will also compare its IC3/PDR mode with an option for $k$-induction and discuss the advantages and limitations of these approaches for different benchmark families.

*SMT'21: 19th International Workshop on Satisfiability Modulo Theories, July 18–19, 2021, Online*

karem@umich.edu (K. A. Sakallah)
https://web.eecs.umich.edu/~karem/ (K. A. Sakallah)
0000-0002-5819-9089 (K. A. Sakallah)