Sequential Circuit Verification at Word Level using Algebraic Geometry

Xiaojun Sun

Ph.D Candidate
Electrical and Computer Engineering, University of Utah
xiaojuns@ece.utah.edu

Ph.D's Dissertation Proposal

Agenda

- Focus
  - Implicitly analyze the reachability of a sequential circuit at word level
  - Use algebraic geometry to assist in sequential circuits abstraction refinement
- Motivation
  - Bit-level to word-level abstraction, BFS traversal of FSMs
- Target problems
  - Given a sequential FSM, with k-bit state variables, perform an implicit state enumeration at word level, i.e. use word-level variables from $\mathbb{F}_{2^k}$ to represent reachable states
  - Extract UNSAT cores efficiently from a given set of CNF clauses
- Approach: **Algebraic geometry techniques**
  - Gröbner basis methods + Elimination ordering + BFS traversal
  - Challenge: Discover efficient algorithmic techniques to implement image computations, set operations, UNSAT proofs, etc. at word level
  - Proposed Contribution: Polynomial abstraction as well as algebraic geometry techniques is applied to reachability analysis; A new algorithm based on Gröbner basis computation is explored to extract UNSAT cores

Motivation

- Importance of reachability analysis in sequential circuits verification
  - Circuits $\rightarrow$ state machines; errors $\rightarrow$ bad states
  - Bad states are reachable *implies* errors affect circuit behavior
- Advantages exploiting word-level verification
  - Many circuit datapaths/system models are described at word level
  - Reduce state space, avoid "bit-blasting"
- Why use algebraic geometry?
  - Provide a symbolic representation for both bit and word level variables in one unified framework
  - Recent work shows it is practical to apply algebraic geometry to circuit verification