ECE/CS 5745/6745: Testing and Verification of Digital Circuits

Subtitle: Hardware Verification using Symbolic Computation

Mon-Wed, 1:25pm - 2:45pm, WEB 1230

Office Hours: Tue: 12pm - 1pm, or by appointment

Instructor: Priyank Kalla
Department of Electrical and Computer Engineering
University of Utah, Salt Lake City, UT 84112

Office: MEB 4112
Email: kalla@ece.utah.edu
Phone: 7-7617

Course Description: The course will cover VLSI Testing and Formal Hardware Verification techniques. This is a fundamental problem in digital circuit/RTL design validation, where it is important to verify whether or not a given circuit implementation is equivalent to its functional specification. This is called 'Equivalence Checking', and this fundamental problem is a foundation for most other VLSI Testing and formal verification techniques. The course will cover both conventional and advanced formal (mathematical) tools, algorithms and technologies that are employed as core computational platforms to verify such implementations.

We will also cover basic concepts of Automatic Test Pattern Generation Techniques to test VLSI circuits for fabrication defects.

Here is a list of topics that we will cover in class:

1) **Introduction to Hardware Verification**
   - Formal Hardware Verification
   - Combinational and Sequential Circuit Verification
   - Equivalence and Property Checking
2) **Boolean Operations and Data Structures for Test & Verification**
   - Boolean operations for Test & Verification
   - Binary Decision Diagrams (BDDs)
3) **SAT Solving and Test & Verification**

- SAT and SMT-based Verification
- Automatic Rectification of Buggy Designs

4) **Testing VLSI Circuits for Manufacturing Defects**
   - The Stuck-at Fault Model and ATPG
   - Fault Collapsing for ATPG
   - Sequential Circuit Testing
   - Design-for-Test (DFT) Techniques, Partial Scan
5) **Introduction to Commutative Algebra and Algebraic Geometry**
   - Rings and Fields
   - Modulo Arithmetic
   - Finite Fields
   - Polynomials, Polynomial Rings and Polynomial Functions
   - Hardware Modeling using Polynomial Functions
6) **Finite Fields and Cryptography Circuits**
   - Finite Fields and Hardware Design
   - From $f : \mathbb{B}^k \to \mathbb{B}^k$ to $f : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$
   - Applications in Public Key Cryptography
   - Formal Specification and Construction of Finite Field Circuits
   - The Verification Formulation
7) **Ideals Varieties and Gröbner Bases**
   - Polynomial Ideals and their Varieties
   - Gröbner Bases of Polynomial Ideals
   - Buchberger's Algorithm
   - Ideal Membership Testing and Equivalence Checking
8) **Nullstellensatz and Hardware Verification**
   - The Weak and Strong Nullstellensatz
   - Radical Ideals and the $I(V(J))$
   - Nullstellensatz over Finite Fields
   - Application of Nullstellensatz to Equivalence Checking
9) **Verification and Rectification of Integer Arithmetic Circuits**
   - Verification of Integer Arithmetic Circuits over $\mathbb{Q}$
   - Rectification of Integer Arithmetic Circuits over $\mathbb{Q}$
   - Computational Challenges for Verification of Integer Arithmetic
10) **Elimination Ideals and Design Abstraction** (Time Permitting)
    - Elimination Ideals and Projection of Varieties
    - Application over Finite Fields

- Word-Level Abstraction from Bit-Level Circuits

11) **Reachability Analysis and Sequential Circuit Verification**

- Finite State Machines (FSMs)
- State-Space Analysis and Sequential Circuit Verification

12) **Conclusion of Course**

- Class Projects and Presentations