1) Introduction to Hardware Verification
   • Formal Hardware Verification
   • Combinational and Sequential Circuit Verification
   • Equivalence and Property Checking
   • SAT and SMT-based Verification
   • Decision Diagrams
   • Datapath Verification Challenges
   • Motivation for Formal Verification using Computational Algebra and Algebraic Geometry

2) 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

3) Finite Fields and Cryptography Circuits
   • Finite Fields and Hardware Design
   • From $f : \mathbb{B}^k \to \mathbb{B}^k$ to $f : F_{2^k} \to F_{2^k}$
   • Applications in Public Key Cryptography
   • Formal Specification and Construction of Finite Field Circuits
   • The Verification Formulation
4) Ideals, Varieties, and Gröbner Bases
   - Polynomial Ideals and their Varieties
   - Gröbner Bases of Polynomial Ideals
   - Buchberger’s Algorithm
   - Ideal Membership Testing and Equivalence Checking

5) Nullstellensatz and Hardware Verification
   - The Weak and Strong Nullstellensatz
   - Radical Ideals and the I(V(\text{J}))
   - Nullstellensatz over Finite Fields
   - Application of Nullstellensatz to Equivalence Checking

6) Elimination Ideals and Design Abstraction
   - Elimination Ideals and Projection of Varieties
   - Application over Finite Fields
   - Word-Level Abstraction from Bit-Level Circuits

7) Improving Gröbner Basis based Hardware Verification
   - Efficient Term-ordering for Circuits
   - Faugère’s F₄ Algorithm
   - Applications to Circuit Verification

8) Reachability Analysis and Sequential Circuit Verification
   - Finite State Machines (FSMs)
   - State-Space Analysis and Sequential Circuit Verification
   - Reachability analysis using Algebraic Geometry
   - Property Directed Reachability and Gröbner Bases
   - Craig’s Interpolants in Algebraic Geometry

9) Testing VLSI Circuits for Manufacturing Defects
   - The Stuck-at Fault Model and ATPG
   - Fault Collapsing for ATPG
   - The D- and PODEM-algorithms for ATPG
   - Sequential Circuit Testing
   - Delay Fault ATPG

10) Conclusion of Course
    - Class Projects and Presentations