COMPUTER ALGEBRA FOR ELECTRICAL & COMPUTER ENGINEERS
FALL SEMESTER 2010

Instructor: Prof. Priyank Kalla
Electrical and Computer Engineering, University of Utah, USA
Email: kalla@ece.utah.edu; Web: www.ece.utah.edu/˜kalla

List of Topics to be covered in Class:

1. Commutative Algebra Basics
   - Preliminaries: Groups, Rings, Infinite and Finite Fields
   - Polynomials as Functions
   - Varieties, Ideals, and Ideal Generators
   - Univariate polynomials over $k[x]$
   - Division and Euclidean Algorithms
2. Gröbner Bases over $k[x_1, \ldots, x_n]$
   - Monomial Orderings and Monomial Ideals
   - Gröbner bases & their properties
   - S-Polynomials and Buchberger's Algorithm
   - Reduced Gröbner bases
3. Applications of Gröbner bases
   - Nullstellensatz
   - Elimination Ideals
   - Applications in logic design verification, cryptography, etc.
   - Other Improvements on Buchberger's Algorithm
4. Study of Finite Fields GF(p^m)
   - Construction of Finite Fields
   - Study of Properties of Finite Fields: additive and multiplicative group structure, order, primitive roots, primitive polynomials, existence and uniqueness of finite fields, etc.
   - Applications of Finite Fields in coding theory, cryptography, logic-circuit design etc.
   - Composite Field Arithmetic and Applications [relatively new concept]
   - Gröbner bases over Finite Fields and their applications
5. Polynomial functions and Gröbner Bases over Rings
   - Polynomial functions over Finite Integer Rings $f : Z_n \rightarrow Z_m$
   - Canonical Representations of polynomial functions and applications in arithmetic circuit/logic design
   - Gröbner bases over rings and applications
6. Case Studies [or Class project ideas]
   - Model checking using algebraic geometry
   - Recent work on verification of arithmetic circuits using Gröbner Bases techniques
   - Montgomery Multiplication and hardware/software-algorithm design for Crypto applications

- Hybrid system analysis
- Factorization-based polynomial system synthesis
- Constraint solvers using polynomial function theory and p-adid techniques
- Integer Programing using Gröbner Bases

Gröbner bases material can be found in [1] [2], among many others, while Finite field related fundamental topics can be found in [3]. The literature on polynomial functions over finite rings and composite field arithmetic will be provided as published papers and manuscripts. Papers describing applications of Gröbner bases will also be provided.

Computer Algebra Tools: We are interested in algorithmic study, implementation and applications of Gröbner bases over various problem domains. So it would be a good idea to implement these algorithms, and make use of Computer Algebra tools for this purpose. A lot of computer algebra systems are available in public domain, that can serve our purpose. We can make use of SINGULAR for our purpose, which can be accessed from: www.singular.uni-kl.de. There are other tools, such as COCOA (cocoa.dima.unige.it), that also allow Gröbner bases computations, but SINGULAR has recently implemented algorithms to compute Gröbner bases over finite rings, which might come in handy, particularly if you work on a class project on such topics.

REFERENCES

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics. American Mathematical Society, 1994.

[2] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms* An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer-Verlag, 1997.

[3] Robert J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.