MATH 800 – Computer Algebra – FALL 2023

Instructor : Michael Monagan: mmonagan@sfu.ca

A course on algorithms for algebraic computation and tools for computing with multivariate polynomials, polynomial ideals, matrices and algebraic numbers. Tools include the Fast Fourier Transform, Groebner bases, and the Schwartz-Zippel Lemma. We will use Maple as a calculator and as a programming language to implement algorithms. Instruction in Maple usage and Maple programming will be provided.

Prerequisites (1) An undergraduate degree in mathematics and basic programming skills or, (2) an undergraduate degree in computer science and an algebra course, or, (3) permission of the instructor.

Maple

We will be using Maple for implementing algorithms and running experiments and as a symbolic calculator. If you don't have access to Maple at your university you may buy a personal license for Maple from Maplesoft, the company that develops and sells Maple. I have obtained a discount for the student version of Maple. This is the full version of Maple which you can keep on your computer "forever" but it does not come with free updates nor with tech support – I will be your tech support. The normal price is $149 + taxes. The discounted price is $99 + taxes. Go to https://webstore.maplesoft.com, select Student, and enter the product code M800-SFU-M2023

Course Outline

1. Getting Started (2 weeks)

   Programming in Maple tutorial. Analysis of algorithms tutorial. The extended Euclidean algorithm. Algorithms for polynomial interpolation.

2. Algorithms for Linear Algebra (2 weeks)

   Computing $\det(A)$ and solving $Ax = b$ over a field using Gaussian elimination. Fraction-free algorithms for computing $\det(A)$ and solving $Ax = b$. The Berkowitz division free algorithm for computing $\det(A - \lambda I)$. Solving $Ax = b$ over $\mathbb{Q}$ using p-adic lifting and rational number reconstruction.

3. The Fast Fourier Transform (1.5 weeks)

   Fast polynomial multiplication, fast division and fast multi-point evaluation.

4. Computing with multivariate polynomials (1.5 weeks)

   Data structures for multivariate polynomials. Term orderings.
   Multiplication and division using repeated merging and binary heaps.

5. Groebner bases and applications (2 weeks)

   Ideals in polynomial rings. Monomial orderings. Ideal membership and polynomial division. The Hilbert basis theorem. Groebner bases. Buchberger's algorithm. The elimination theorem. Applications of Groebner bases. Groebner bases in Maple.

6. Computing with algebraic numbers (1.5 weeks)

   Computing in $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$. Primitive elements, norms and resultants. Factoring polynomials over $\mathbb{Q}(\alpha)$.

7. Sparse polynomial interpolation (1.5 weeks)

   Sparse polynomials. Black box representations. The Schwartz-Zippel Lemma. Zippel's sparse interpolation. Ben-Or Tiwari interpolation.

Grading

15% Assignment 1
65% Assignments 2–7 (best 5 of 6 assignments, one per topic).
20% Course Project

Assignments and Lecture Notes

Assignments will partly be on paper and partly in Maple. I will post the assignments and solutions, lecture notes, handouts and links to recordings of the lectures on Canvas and also under `http://www.cecm.sfu.ca/~mmonagan/teaching/MATH8002023`

If you are registered for MATH 800 through SFU or the PIMS network, you will upload your assignments to Crowdmark and you will have access to the Canvas folder. If you are not registered through SFU or the PIMS network you can Email me your assignment solutions and will not have access to the Canvas folder.