Foundations of Computer Algebra: Project 2 Proposals

Marc Moreno Maza
University of Western Ontario
CS 424b / CS556b – Winter 2005

January 7, 2008

1 Introduction

The proposed projects aim to enhance the computing performances of AXIOM or MAPLE by implementing algorithms for fast polynomial arithmetic. The details of these algorithms are in Chapters 5 and 10 of [GG99]

2 Guidelines

Date of postage. Wenesady 16th of March.

Due format. Similar as for Project 1:

- An AXIOM or MAPLE implementation of the chosen algorithm,
- a postscript or a PDF document reporting on your experiments. Slides would be perfect.
- Each student will present her(his) results during a short (about 15 min) presentation in the class on Wenesady 27th of April.

Project Choice. The students are proposed a variety of projects Wenesady 16th of March. On Wenesady 23rd of March, each student must notify the instructor which project she/he would like to realize. Ideally, it would be desirable that each of the first five projects could be chosen by at least one student and that no more than two students choose the same project. But no formal constrainsts are fixed.

3 Description of the Proposed Projects

Project 1 (Rational function reconstruction in MAPLE**)** A rational number n/d can be reduced modulo a prime p to an element $r \in \mathbb{Z}/p\mathbb{Z}$, provided that p does not divide d. Similarly, given a field k, a rational function $n(x)/d(x)$, where $n(x), d(x) \in k[x]$, can be reduced to $r \in k[x]$ modulo an irreducible polynomial $m(x)$ that does not divide $d(x)$. The question is how to retrieve $n(x)/d(x)$? The algorithm is described in Section 5.7 of [GG99]. The goal of this project is to implement this algorithm in MAPLE and realize benchmarks with $k = \mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$.

Project 2 (Rational function reconstruction in AXIOM**)** Similar to Project 1, but with an implementation in AXIOM.

Project 3 (FFT-based multiplication in $\mathbb{Z}/p\mathbb{Z}$ in AXIOM**)** The goal of this project is to implement in AXIOM the algorithms of the course for FFT-based multiplication in $\mathbb{Z}/p\mathbb{Z}[x]$. Benchmarks versus the Karatsuba and classical quadratic multiplication algorithms are needed for $p \in \{11, 101, 1009, 10007, 100003\}$.

Project 4 (Fast Interpolation in MAPLE**)** We have seen during the course how to perform interpolation with more than two moduli. Section 10.2 in [GG99] propose an elegant divide-and-conquer strategy to improve the performances of the interpolation Algorithm. The goal of this project is to implementation this algorithm in MAPLE and realize benchmarks with $k = \mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$.

Project 5 (Fast Chinese Remaindering in MAPLE**)** We have seen during the course how to perform Chinese Remaindering with more than two moduli. Section 10.3 in [GG99] propose an elegant divide-and-conquer strategy to improve the performances of the Chinese Remaindering Algorithm. The goal of this project is to implementation this algorithm in MAPLE and realize benchmarks with $k = \mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.

Project 6 (Fast Interpolation in AXIOM**)** Similar to Project 4, but with an implementation in AXIOM.

Project 7 (Fast Chinese Remaindering in AXIOM**)** Similar to Project 5, but with an implementation in AXIOM.

Project 8 (Project of your choice in Maple **or** AXIOM**)** During your reading of [GG99], you may have been seduced or puzzled by an algorithm. Please discuss it with the instrutor, to determine if it can be turned into a project.

References

[GG99] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.