Foundations of Computer Algebra: Assignment 1

Marc Moreno Maza
University of Western Ontario
CS424b – Winter 2005

Posted: Wednesday, February 2, 2005
Due: Wednesday, March 2, 2005

1 Guidelines

Date of postage. Wednesday, February 2, 2005

Normal date for submission. Wednesday, February 23, 2005

Due format. The assignment can be returned to the instructor by email in a form of a postscript, PDF or text file. Alternatively, a printed version can be delivered to his mail box in the Computer Science Department.

Collaboration. You are expected to do this assignment on your own without assistance from anyone else in the class.

Marking. This assignment will be marked out of 40. Each exercise is worth 10 points.

2 Exercise 1

2.1 Statement

Let $p \in \mathbb{N}$ and $n = 2^p$. Let A and B be two square matrices of order n and with coefficients in $\mathbb{Z}$. The classical algorithm for computing the matrix product $A\,B$ uses $\mathcal{O}(n^3)$ operations in $\mathbb{Z}$. The *Strassen* algorithm provides the lower asymptotic upper bound $\mathcal{O}(n^{2{,}81})$. As for the *Karatsuba* algorithm, the trick relies on a smart use of distributivity:

(1) If $n = 1$ the matrices A et B are of the form (a) et (b) where $a, b \in \mathbb{Z}$, such that $A\,B$ equals $(a\,b)$.

(2) If $n > 1$ the matrices A and B can be decomposed as

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \; B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix},$$

where A_{ij} and B_{ij} are square matrices of order $n/2$. Them, one computes the following 8 sums.

$$\begin{array}{ll} S_1 = A_{21} + A_{22} & T_1 = B_{12} - B_{11} \\ S_2 = S_1 - A_{11} & T_2 = B_{22} - T_1 \\ S_3 = A_{11} - A_{21} & T_3 = B_{22} - B_{12} \\ S_4 = A_{12} - S_2 & T_4 = T_2 - B_{21} \end{array}$$

(3) Next, one computes the following 7 matrix products by recursive calls to the algorithm.

$$\begin{array}{ll} P_1 = A_{11}\,B_{11} & P_5 = S_1\,T_1 \\ P_2 = A_{12}\,B_{21} & P_6 = S_2\,T_2 \\ P_3 = S_4\,B_{22} & P_7 = S_3\,T_3 \\ P_4 = A_{22}\,T_4 & \end{array}$$

(4) Finally, one computes the following 7 sums:

$$\begin{array}{ll} U_1 = P_1 + P_2 & U_5 = U_4 + P_3 \\ U_2 = P_1 + P_6 & U_6 = U_3 - P_4 \\ U_3 = U_2 + P_7 & U_7 = U_3 + P_5 \\ U_4 = U_2 + P_5 & \end{array}$$

and one returns:

$$\begin{pmatrix} U_1 & U_5 \\ U_6 & U_7 \end{pmatrix}.$$

2.2 Questions

(1) Using AXIOM or MAPLE check that the above formulas are correct. Your answer must be an AXIOM input file or a MAPLE worksheet.

(2) Use the results of the first chapter to retrieve the asymptotic upper bound given above.

3 Exercise 2

3.1 Statement

Let a, b, m be three integers such that $m > 1$ and $a \neq 0$. We are interested in solving in $\mathbb{Z}/m\mathbb{Z}$ the equation

$$ax = \ b \tag{1}$$

Let g be the gcd of a and m in $\mathbb{Z}$.

3.2 Questions

(1) Show that if $g = 1$ holds then Equation (1) admits a unique solution.

(2) Give all the solutions of Equation (1) in case $g > 1$ holds.

4 Exercise 3

4.1 Statement

Let $\mathbb{K}$ be a field. Let $a, b, c \in \mathbb{K}[x]$ be three non-zero univariate polynomials in x with coefficients in $\mathbb{K}$. We are interested in computing the polynomials $u, v \in \mathbb{K}[x]$ such that

$$au + bv = c \tag{2}$$

holds. Let $g \in \mathbb{K}[x]$ be the gcd of a, b and let $s, t \in \mathbb{K}[x]$ be such that

$$as + bt = g \tag{3}$$

holds. Remember that g, s, t can be computed by the Extended Euclidean Algorithm.

4.2 Questions

(1) Show that Equation (2) has a solution if and only if g divides c.

(2) Assume that g divides c. Show that Equation (2) may admit several solutions (u, v).

(3) Assume that g divides a and that $\deg(a) + \deg(b) - \deg(g) > \deg(c)$. Show that Equation (2) admits a unique solution (u, v) such that $\deg(u) < \deg(a) - \deg(g)$ and $\deg(v) < \deg(b) - \deg(g)$ both hold.

5 Exercise 4

5.1 Statement

We consider the ring of the univariate polynomials in x with coefficients in $\mathbb{Z}$. We assume that these polynomials are represented in a computer program using expression trees, as in MAPLE.

5.2 Questions

(1) Design an algorithm that will decide whether two polynomials of $\mathbb{Z}[x]$, represented using expression trees, are equal.

(2) Give an asymptotic upper bound for your algorithm.

References

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