Mathematics and Algorithms for Computer Algebra

Part 1 © 1992 Dr Francis J. Wright – CBPF, Rio de Janeiro

July 9, 2003

Examination

The duration of this examination is 2 hours.

There are four question which carry equal marks. You may attempt as many as you wish, but marks will be awarded only for the best three *solutions. Therefore, if you attempt more than three questions, your worst solution will not contribute to your final mark.*

Please write carefully and legibly.

1. Explain how a long integer may be represented in a computer, in such a way that it can in principle use as much memory as necessary. Describe two specific representations, one in which the whole integer is contained within a single block of memory (range of addresses), and one in which the integer can be distributed throughout memory as necessary in order to use all memory that is free. Discuss the advantages and disadvantages of these two representations.

Explain carefully the relationship between the size (in terms of the number of bits in its binary representation) of the base used to represent the long integer and the computer word size or sizes (i.e. the sizes of integers on which the hardware can directly perform arithmetic). Consider separately the efficiency of (a) addition and (b) multiplication of long integers. (You need not consider representation of sign.)

Apart from the integers, state three other number domains that are important in computer algebra.

Give a (recursive) definition of the structure or “syntax” of a multivariate rational expression, i.e. a quotient of two polynomials in one or more variables (represented by identifiers, and not involving anything more structured). With the aid of one or more diagrams, show how this definition translates into a computer representation similar to that used for long integers. Give a diagram showing the representation of the specific rational expression

$$\frac{(y+1)x^2 + (3y)x + 2}{z}.$$

Discuss briefly sparse, dense, canonical and normal representations, and give the main requirements that ensure that a multivariate polynomial representation is canonical.

2. A function to return the sign of a number may be defined as follows:

$$\operatorname{sign}(x) = \begin{cases} +1 & \text{if } x > 0, \\ 0 & \text{if } x = 0, \\ -1 & \text{if } x < 0. \end{cases}$$

Assuming that both this function and normal arithmetic are supplied for small integers, that B, m, n are small integers, and that two long integers a, b represented in base B have respectively m and n digits, give algorithms that perform the following tasks and return representations of long integers with digits in the range $[0, B-1]$:

(a) compare two long integers a, b by returning the value of $\operatorname{sign}(a-b)$;

(b) add two positive long integers a, b;

(c) subtract a smaller positive long integers b from a larger positive long integers a.

Assuming that the sign function of a single long integer is provided, show how to compute the sum of two long integers of arbitrary sign using the addition and subtraction algorithms discussed above together with the long integer sign function. Hence, show how to perform subtraction of two long integers of arbitrary sign.

3. Let $u(x), v(x)$ be two univariate polynomials over a field, which are therefore elements of a Euclidean domain. The Euclidean Division Theorem states that, if $v(x) \neq 0$, there exist *unique* polynomials $q(x)$ and $r(x)$ such that

$$u(x) = q(x)v(x) + r(x), \quad \deg(r) < \deg(v).$$

Prove that these polynomials are unique (e.g. by assuming the contrary and finding a contradiction).

Give a Euclidean Division algorithm that constructs the quotient and remainder polynomials $q(x), r(x)$, by performing arithmetic on polynomial coefficients (rather than complete polynomials).

Now suppose that the polynomial coefficients are elements of a ring and not a field, and that only ring division can be performed. Explain why, in general, $q(x) = 0$, and give two cases in which this is not so and a non-trivial quotient exists. Explain the principle of pseudo-division and give, with justification, the simplest possible pseudo-division rule. (You need not give a full algorithm.) Explain why more sophisticated pseudo-division algorithms are generally to be preferred, and indicate briefly what they are.

4. Define the *Greatest Common Divisor* (GCD) of two elements of an integral domain. Discuss uniqueness of gcds, giving examples for gcds of integers and univariate polynomials over a field.

Derive Euclid's algorithm to compute a gcd in a Euclidean domain, and its extension to compute the coefficients s, t in the representation

$$\gcd(a, b) = sa + tb,$$

giving the extended Euclidean algorithm in detail for the integers.

Explain the relationship between Euclid's algorithm and Sturm sequences, and explain how the latter are used to solve polynomial equations. Show in detail how the technique would be used to solve the equation

$$4x^2 - 1 = 0$$

starting from a root bound of 1.