

University of Bath

**DEPARTMENT OF COMPUTER SCIENCE  
EXAMINATION**

**CM30070: Computer Algebra**

---

---

No calculators may be brought in and used.

Full marks will be given for correct answers to **THREE** questions.  
Only the best three answers will contribute towards the assessment.

Examiners will attach importance to the number of  
well-answered questions.

1. What are meant by ‘normal’ and ‘canonical’ representations? [2]

*Normal: 0 has a unique representation. Canonical: every object has a unique representation.*

What is meant by ‘simplification’ in computer algebra (e.g. in Maple), and how does this relate to normal and canonical representations? [4]

*Simplification tends to mean “produce a short form”. If there are normal representations, simplification should produce 0 for zero objects, since this is the shortest representation. Canonical is much harder, and may not be possible. While we might not want  $\frac{x^{1000}-1}{x-1}$  expanded, could we reasonably expect the reverse?*

For each of the following polynomial representations, outline a representation of  $(x^2y^2+1)(xy-1)-x^3y^3$  (which may of course look nothing like this) and explain what choices need to be made to make this expression format normal and/or canonical (if possible). [14]

- (i) Recursive sparse.

- A. Note the polynomial is “really”  $-x^2y^2 - xy + 1$ . Therefore in LISP-speak (I actually think I’ll get box-and-arrow diagrams) I’d expect

```
(x (2 (y 2 -1))
  (1 (y 1 -1))
  (0 1))
```

or any of several variants. Even for normal, we need to expand and collect common terms (to kill the  $x^3y^3$  in the example), which means:

- fix an order on the variables;
- fix an order on the exponents (generally decreasing);
- collect common terms, deleting zero ones. [of which 4]

- (ii) Distributed sparse.

- A. Note the polynomial is “really”  $-x^2y^2 - xy + 1$ . Therefore in LISP-speak (I actually think I’ll get box-and-arrow diagrams) I’d expect

```
((x y) (2 2 -1)
  (1 1 -1)
  (0 0 1))
```

or any of several variants. Even for normal, we need to expand and collect common terms (to kill the  $x^3y^3$  in the example), which means:

- fix an order on the variables;
- fix an order on the monomials (generally admissible, but strictly this isn’t necessary);
- collect common terms, deleting zero ones. [of which 4]

*Question 1 continues on next page . . .*

*Question 1 continued . . .*

(iii) Factored (you may choose any representation for the factors)

A. One factor, being one of the above. If this is normal, we have normal, but to get canonical, we would need complete factorisation, which is prohibitive. [of which 3]

(iv) Straight-Line Program

A.  $L1 := x * y$   
 $L2 := L1 * L1$   
 $L3 := L2 - 1$   
 $L4 := L1 - 1$   
 $L5 := L3 * L4$   
 $L6 := L1 * L2$   
 $L7 := L5 - L6$

Generally not even normal, since this would imply expansion. [of which 3]

2. Give a computationally testable definition of what it means for a set of polynomials (with coefficients from a field) to be a Gröbner base, defining any terms you use which are specific to Gröbner base theory. [8]

*(This is the only constructive definition I gave: the rest all rely on ideals, which aren't testable without GB).*

*$G$  is a Gröbner base with respect to a particular admissible order  $>$  on monomials if and only iff*

$$\forall f, g \in G \quad S(f, g) \xrightarrow{*G} 0 \quad \text{where}$$

$$S(f, g) \text{ is } \frac{\text{lt}(g)}{\gcd(\text{lm}(f), \text{lm}(g))} f - \frac{\text{lt}(f)}{\gcd(\text{lm}(f), \text{lm}(g))} g$$

*lt( $f$ ) is the leading term of  $f$  (i.e. power product and coefficient)*

*lm( $f$ ) is the leading monomial of  $f$  (i.e. power product only)*

*$\xrightarrow{*G}$  is the result of carrying out  $\rightarrow^G$  until it is no longer possible*

*$f_1 \rightarrow^G f_2$  is  $f_2$  being the result of subtracting  $\frac{\text{lt}(f_1)}{\text{lt } g} g$  from  $f_1$  where  $g$  is any element of  $G$  with  $\text{lm}(g)$  dividing  $\text{lm}(f_1)$ .*

Explain how to convert your test into an algorithm (proof of termination is *not* required) to produce a Gröbner base, generating the same ideal, from a set of polynomials. [8]

*If any  $S(f, g) \xrightarrow{*G} h \neq 0$ , then  $h \in (G)$ , so add  $h$  to  $G$  and keep testing. If this terminates, the resultant  $G$  is a Gröbner base by the test above. This is Buchberger's algorithm.*

Given a Gröbner base of an ideal with respect to *some* ordering, what can you deduce from the leading monomials of this base? [4]

*Whether or not the ideal is zero-dimensional: every  $x_i$  must occur alone to some power as a leading monomial.*

*If zero-dimensional, the number (with multiplicity) of solutions of the set of polynomials. This is just the number of monomials irreducible under the ideal, i.e. all those less than (in our ordering) all the leading monomials of the ideal.*

3. Suppose you are given a procedure which, given two univariate polynomials  $f$  and  $g$  over the integers (i.e. in  $\mathbf{Z}[x]$ ) and a *small* prime  $p$ , returns the greatest common divisor of  $f \pmod{p}$  and  $g \pmod{p}$ . i.e.  $f$  and  $g$  viewed as polynomials modulo  $p$ . Outline **two** different methods you could use to compute the greatest common divisor of  $f$  and  $g$  over the integers, identifying any major common components of these solutions. Which would you choose, and why? [20]

**Common** *The Landau–Mignotte bound, which lets us state a bound  $M$  on the size of coefficients of  $\gcd(f, g)$ . Also, in both cases we must not use primes that divide  $\gcd(\text{lc}(f), \text{lc}(g))$ .*

**Modular** *I expect a description of the “several small primes” Chinese Remainder Theorem approach. Take several primes  $p_i$ , discarding any where the gcd modulo  $p_i$  is greater than that for any other prime, until  $\prod p_i > 2M$ , then use Chinese Remainder to reconstruct, regard the resulting polynomial  $h \pmod{\prod p_i}$  as a polynomial over the integers, and check it does divide  $f$  and  $g$ . If not, all the primes chosen were bad, and we start again.*

**$p$ -adic** *Choose a prime  $p$ , compute  $h_p = \gcd(f_p, g_p)$ . Use Hensle’s Lemma (either linear or quadratic) to lift  $f_p = h_p k_p$  (or with  $g$ : use whichever has smaller degree) to a split  $f_{2p} = h_{p^2} k_{p^2} \dots$  until we get  $f_{p^n} = h_{p^n} k_{p^n}$  with  $p^n > 2M$ . Then if this factorisation works over  $\mathbf{Z}$ ,  $h$  has to be the true gcd. Otherwise  $p$  was unlucky and we try with a different one.*

**Choice** *Probably modular, as with  $p$ -adic we can go all the way before we discover that our prime is bad. In other words, all the eggs are in one basket.*

4. Define the term “elementary function”, as used in integration in finite terms. [2]

*Bookwork. My notes read as follows.*

**Definition 1** Let  $K$  be a field of functions. The function  $\theta$  is an elementary generator over  $K$  if one of the following is satisfied:

- (a)  $\theta$  is algebraic over  $K$ , i.e.  $\theta$  satisfies a polynomial equation with coefficients in  $K$ ;
- (b)  $\theta$  is an exponential over  $K$ , i.e. there is an  $\eta$  in  $K$  such that  $\theta' = \eta'\theta$ , which is only an algebraic way of saying that  $\theta = \exp \eta$ ;
- (c)  $\theta$  is a logarithm over  $K$ , i.e. there is an  $\eta$  in  $K$  such that  $\theta' = \eta'/\eta$ , which is only an algebraic way of saying that  $\theta = \log \eta$ .

**Definition 2** Let  $K$  be a field of functions. An overfield  $K(\theta_1, \dots, \theta_n)$  of  $K$  is called a field of elementary functions over  $K$  if every  $\theta_i$  is an elementary generator over  $K$ . A function is elementary over  $K$  if it belongs to a field of elementary functions over  $K$ . If  $K$  is omitted, we understand  $\mathbf{C}(x)$ : the field of rational functions.

State Liouville’s Theorem on integration in finite terms. [4]

*Bookwork. My notes read as follows.*

**Theorem 1 (Liouville’s Principle)** Let  $f$  be a function from some function field  $K$ . If  $f$  has an elementary integral over  $K$ , it has an integral of the following form:

$$\int f = v_0 + \sum_{i=1}^n c_i \log v_i,$$

where  $v_0$  belongs to  $K$ , the  $v_i$  belong to  $\hat{K}$ , an extension of  $K$  by a finite number of constants algebraic over  $K$ , and the  $c_i$  belong to  $\hat{K}$  and are constant.

Another way of putting this is to say that, if  $f$  has an elementary integral over  $K$ , then  $f$  has the following form:

$$f = v_0' + \sum_{i=1}^n \frac{c_i v_i'}{v_i}.$$

Why is Liouville’s Theorem so important for the theory of integration in computer algebra? [4]

*It gives limits on where we need to look for elementary functions in the integral, i.e. those in the integrand plus some new logs, and those only with constant coefficients.*

Restricting ourselves to the integration of *transcendental* algebraic functions, state two developments of Liouville’s Theorem that further help the construction of algorithms for integration in computer algebra. [4]

*Question 4 continues on next page ...*

*Question 4 continued ...*

*Several possibilities. The two most obvious ones are the following (from my notes). Let  $\theta$  be a (transcendental) logarithm over  $K$ .*

**Lemma 1 (Decomposition Lemma (logarithmic))**  *$f \in K(\theta)$  can be written uniquely as  $p + q/r$ , where  $p$ ,  $q$  and  $r$  are polynomials of  $K[\theta]$ ,  $q$  and  $r$  are relatively prime, and the degree of  $q$  is less than that of  $r$ . If  $f$  has an elementary integral over  $K$ , then  $p$  and  $q/r$  each possess an elementary integral over  $K$ . Let  $\theta$  be a (transcendental) exponential over  $K$ .*

**Lemma 2 (Decomposition Lemma (exponential))**  *$f \in K(\theta)$  can be written uniquely as  $p + q/r$ , where  $p$  is a generalised (or Laurent) polynomial (that is  $\sum_{i=-m}^n a_i \theta^i$ ),  $q$  and  $r$  are polynomials of  $K[\theta]$  such that  $\theta$  does not divide  $r$ ,  $q$  and  $r$  are relatively prime, and the degree of  $q$  is less than that of  $r$ . If  $f$  has an elementary integral over  $K$ , then each of the terms of  $p$ , and also  $q/r$ , have an elementary integral over  $K$ .*

If we were to go beyond elementary functions, in the sense of wishing to integrate elementary functions but with a wider class of answer, what sort of extra theorems would we need in order to have a satisfactory integration theory? [6]

You may use the dilogarithm function, defined by  $\text{dilog}(x) = \int \frac{\log x}{1-x}$ , as your example of a wider class of functions, but you are *not* expected to know any dilog-specific results.

*We would certainly need an analogy of Liouville's Theorem, to say that the only new functions were dilogs with constant coefficients **if true**. Similarly, we would need a decomposition lemma. We would then need to know what dilog functions could actually appear: presumably  $\text{dilog}(f)$  for every  $\log(f)$  in the integrand, but is this clear?*