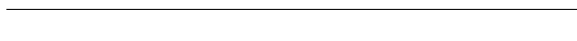


University of Bath

**DEPARTMENT OF COMPUTER SCIENCE  
EXAMINATION**



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?*

What is generally meant by ‘sparsity’ in computer algebra? Illustrate your answer with at least two different mathematical objects. [4]

*Bookwork: expecting polynomials and matrices.*

Explain the difference between *recursive* and *distributed* representations of polynomials, explaining what has to be known for the representations to be canonical. [6]

*Bookwork. In both cases, need canonical representations of coefficients. For recursive, need order on variables, whereas distributed needs order on monomials.*

Give, with brief reasons, *one* algorithm which is better suited for the *recursive* representation and *one* for the *distributed* representation. [4]

*Recursive, e.g. gcd; distributed, e.g. Buchberger.*

2. What is an *admissible* ordering on monomials? [1]

$1$  is the least monomial, and  $a < b \Rightarrow ac < bc$ .

Define a *lexicographical* ordering, and name and define two other common orderings. [5]

*Bookwork.*

Explain the sparse distributed representation of polynomials, showing how  $y(x^2 + 2) - x^3 + 3x^2z^5$  would be represented under the lexicographical ordering with  $x > y > z$ . [4]

*Bookwork.*

$$(-1) \cdot x^3y^0z^0 + 1 \cdot x^2y^1z^0 + 3 \cdot x^2y^0z^5 + 2 \cdot x^0y^1z^0.$$

State two definitions of a *Gröbner basis* with respect to an admissible ordering, one of which should be constructively testable. [4]

$\forall f, g \in G, S(f, g)$  reduces to 0 under  $G$  (constructive);

$(\text{lm}(G)) = (\text{lm}(\langle G \rangle))$ , or several others.

How is a lexicographical-order Gröbner base useful for solving a zero-dimensional set of polynomial equations? Illustrate your answer by solving

$$x(x^2 + 1)(x^3 - 1) = 0 \quad (1)$$

$$x(x^2 + 1)(y - 1) = 0 \quad (2)$$

$$x(y - 1)(y^2 - 2) = 0 \quad (3)$$

$$(y - 1)(y^2 - 2)(y^3 - 3) = 0 \quad (4)$$

(which is a Gröbner base for purely lexicographical ordering with  $x < y$ ).

How many solutions are there? [6]

*Bookwork: Gianni–Kalkbrener.*  $x$  must be a root of the first equation. If  $x$  is a root of  $x^3 - 1$ , then  $y - 1$  from the second (3 solutions). If  $x$  is a root of  $x^2 + 1$ , then  $y^2 = 2$  or  $y = 1$  from the third (2\*3 solutions). If  $x = 0$ , then  $y$  is a root of the last (6 solutions). Hence the answer is 15.

3. How does the ‘many small primes’ version of the modular gcd algorithm work for computing the g.c.d. of two polynomials in  $\mathbf{Z}[x]$ ? [20]

The following features should be mentioned.

- Which primes *must not* be used, and why?
- The rôle of the Landau–Mignotte bound (you *need not state* the precise bound) and how it can be improved during the algorithm.
- The process of verifying that you have actually computed a common divisor.
- Why this must be the *greatest* common divisor.

*Largely bookwork.* [10]

- *Those primes that divide both leading coefficients, because then they might divide the leading coefficient of the g.c.d., which would lead to a degree drop.* [2]
- *Tells us when we can stop, i.e. when  $\prod p > 2LM$ . Since the Landau–Mignotte bound for the height of a factor depends (monotonically!) on the degree of that factor, every time we improve this, we can improve the bound.* [3]
- *Trial division can be expensive if the divisor is wrong (e.g.  $x - 10$  into  $x^{100} - 10$ ) so use ‘early abort’.* [3]
- *It’s a common divisor, and the degree isn’t too small (because of first point), and the g.c.d. is the unique common divisor of that degree.* [2]

4. What form does the integral of a rational function of  $x$  take? Your answer should pay attention to the domain of definition of the various components. [4]

*rational function (in the same field as the integrand)  $+ \sum c_i \log v_i$ , where the  $c_i$  are constants (algebraic over the ground field  $K$ ) and the  $v_i$  are polynomials over  $K(c_i)$ .*

Outline an algorithm for computing the integral of a rational function in such a representation. You may assume the existence of sub-algorithms such as square-free decomposition. [10]

*Bookwork. Either Hermite or Horowitz–Ostrogradski (the latter probably simpler to state) followed by Trager–Rothstein.*

What obstacles lie in the way of extending this to higher functions? Your answer should mention logarithmic integrals, exponential integrals and go further. [6]

**Logarithmic** *The  $c_i$  produced by Trager–Rothstein might no longer be constants, as in  $\int \frac{1}{\log x}$ .*

**Exponential** *The Risch differential equation might not be soluble, as in  $\int \exp(-x^2)$ .*

**Further** *We might no longer have a Liouville principle, or it might be more complicated, as in erf.*