UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE FOUR

COMPUTER ALGEBRA

Monday 23 April 2001

14:00 to 15:30

Examiners:

Prof. K. Turner (External)

Prof. G. Plotkin (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. (a) Explain the use of hashing in Maple, covering:

   i. its implementation,

   ii. its use in the simplification table

   Include examples. [*8 marks*]

   (b) Recall that, by default, Maple represents polynomials as sums of products. Suppose, for the sake of definiteness, that we are dealing with polynomials in the indeterminates $x_1, x_2, \ldots, x_n$ with integer coefficients, represented as sums of products.

   i. Explain briefly what is meant by a sum of products representation; give an example. [*3 marks*]

   ii. Given such a representation one way to test if it represents the zero polynomial is to expand it. Explain why this can be a problematic approach and mention an illustrative example (you do not need to go into details here). [*4 marks*]

   iii. Given a sum of products representation, explain how to find efficiently a number d such that if the represented polynomial is non-zero then its total degree is at most d. (You are not required to include a runtime analysis.) [*4 marks*]

   iv. Suppose that $P(x_1, x_2, \ldots, x_n)$ is a non-zero polynomial of total degree at most d and S is a set of B distinct integers. It can be shown that if we pick $a_1, a_2, \ldots, a_n$ from S uniformly at random then the probability that $P(a_1, a_2, \ldots, a_n) = 0$ is at most d/B.
   Outline an algorithm for testing sums of products representations of polynomials for equality to zero which is such that:

   - it does not carry out any expansion,
   - if the algorithm returns 'non-zero' then this answer is correct,
   - if it returns 'zero' the probability that this answer is incorrect is strictly less than 1/1000.

   In your algorithm you may assume that we have an efficient method for choosing numbers from a given finite set uniformly at random. [*6 marks*]

2. Let x be an indeterminate over $\mathbb{Z}$ and suppose throughout the question that $A, B \in \mathbb{Z}[x]$ are both non-zero.

   (a) Recall that a polynomial H is said to be a *greatest common divisor (gcd)* of A, B if H divides both A and B and whenever G divides both A and B then G divides H.

   Prove that if H is a gcd of A, B then so is $-H$ and moreover this is the only other possibility. [*4 marks*]

   (b) Explain a simple condition that is used in order to make $\gcd(A, B)$ unique. [*2 marks*]

   (c) Assume that at least one of A, B is primitive. Prove that $\gcd(A, B)$ is the largest degree polynomial that divides both A and B (and, for uniqueness, satisfies the condition in (b) above). What goes wrong if neither of A, B is primitive?

   [**Note:** In this part you may assume standard facts about the factorization of polynomials. You may also assume without proof that $\gcd(A, B)$ is primitive.] [*6 marks*]

   (d) From now on

$$\begin{aligned} A &= 9x^3 - 3x^2 - 5x - 1, \\ B &= 9x^4 - 6x^3 - 2x - 1. \end{aligned}$$

   Suppose that we use the modular algorithm for finding $\gcd(A, B)$ with primes $2, 3, 5, 7, \ldots$. For a prime p we use A_p, B_p to denote the polynomials A, B when viewed as elements of $\mathbb{Z}_p[x]$ and set $G_p = \gcd(A_p, B_p)$. In fact we have:

$$\begin{aligned} G_2 &= x^3 + x^2 + x + 1, \\ G_3 &= x + 2, \\ G_5 &= x^2 + x + 3, \\ G_7 &= x^2 + 4x + 2. \end{aligned}$$

   i. Explain why 3 is a bad choice of prime and 2 is an unlucky prime. [*3 marks*]

   ii. From the given information what do we know about the primes 5 and 7 in terms of whether they are lucky or unlucky? At this stage do we have any reason to believe that either of them is unlucky (explain your answer briefly)? [*3 marks*]

   iii. In fact the coefficients of $\gcd(A, B)$ are all in the range $[-16, 17]$ and the leading coefficient of $\gcd(A, B)$ is 3. Assume that 5 and 7 are lucky and find $\gcd(A, B)$ from the information given above. What simple extra test could be used to verify the result?

   [**Note:** You may assume the following special case of the Chinese Remainder Theorem: let m_1, m_2 be coprime integers. Choose b_1, b_2 such that $b_1 m_2 = 1$ in $\mathbb{Z}_{m_1}$ and $b_2 m_1 = 1$ in $\mathbb{Z}_{m_2}$. Then $a = r_1$ in $\mathbb{Z}_{m_1}$ and $a = r_2$ in $\mathbb{Z}_{m_2}$ if and only if $a = r_1 b_1 m_2 + r_2 b_2 m_1$ in $\mathbb{Z}_{m_1 m_2}$. Note that for $m_1 = 5$ and $m_2 = 7$ we have $b_1 = b_2 = 3$.] [*7 marks*]

3. This question is concerned with Gröbner bases of ideals of polynomials in the indeterminates $x_1, x_2, \ldots, x_n$ and with coefficients from a field k.

   (a) Recall that an *admissible order* on power products is a total order $<$ such that 1 is the smallest power product and whenever $u < v$ then $uw < vw$ for all power products u, v, w. Why are these two conditions required in the context of Gröbner bases? [*4 marks*]

   (b) Explain what is meant by a lexicographic order on power products.

   Suppose we have such a lexicographic order with $x_1 > x_2 > \cdots > x_n$ and p is a non-zero polynomial whose leading power product is of the form x_i^e where $1 \leq i \leq n$. What can we say about the other power products (if any) that occur in p? [*4 marks*]

   (c) Let $f_1, f_2, \ldots, f_m \in k[x_1, x_2, \ldots, x_n]$ where k is an algebraically closed field and let G be a Gröbner basis of $f_1, f_2, \ldots, f_m$ with respect to a fixed lexicographic order.

      i. Explain how we can decide from the elements of G if $f_1, f_2, \ldots, f_m$ have finitely many or infinitely many solutions.
      Does the method work if k is not algebraically closed? (Give a simple counterexample if the method fails.) [*6 marks*]

      ii. Prove that if there are finitely many solutions then there are at most $d_1 d_2 \cdots d_n$ of them where $d_1, d_2, \ldots, d_n$ are natural numbers obtained from certain polynomials in G.
      [**Note:** You may assume without proof the fact that a non-zero univariate polynomial with coefficients from k of degree d has at most d roots in k.] [*6 marks*]

      iii. Let $u_1, u_2, \ldots, u_r$ be new indeterminates over k and suppose that we have $g_1, g_2, \ldots, g_n \in k[u_1, u_2, \ldots, u_r]$. These define the subset S of k^n given by

      $$S = \{\, (g_1(a_1, \ldots, a_r), \ldots, g_n(a_1, \ldots, a_r)) \mid a_1, \ldots, a_r \in k \,\}.$$

      The *implicitization problem* is to find $f_1, f_2, \ldots, f_m \in k[x_1, x_2, \ldots, x_n]$ such that $S \subseteq \mathbf{V}(f_1, f_2, \ldots, f_m)$ and this is the smallest variety that contains S (i.e., $\mathbf{V}(f_1, f_2, \ldots, f_m) \subseteq W$ whenever W is a variety such that $S \subseteq W$). Let I be the ideal of $k[x_1, \ldots, x_n, u_1, \ldots, u_r]$ generated by the polynomials $x_1 - g_1, x_2 - g_2, \ldots, x_n - g_n$. It can be shown that we can take for $f_1, f_2, \ldots, f_m$ any set of generators of $I \cap k[x_1, x_2, \ldots, x_n]$. Describe an algorithm for finding $f_1, f_2, \ldots, f_m$ (you are not required to prove its correctness). [*5 marks*]