Queen Mary
UNIVERSITY OF LONDON

M.Sc. EXAMINATION BY COURSE UNIT

MTHM032 Advanced Algorithmic Mathematics

27 May 2004 10:00–13:00

The duration of this examination is 3 hours.

You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best four *questions answered will be counted.*

Calculators are NOT permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Show your calculations.

Throughout, $\mathbb{N}$ *denotes the set of non-negative integers and* F *denotes a field.*

1. (a) [6 marks] Define what is meant by a *partial order*, *total order* and *well-order* on a set S.

(b) [5 marks] Let $\leq$ be a total order on S. Prove that $\leq$ is a well-order on S if and only if there is no infinite strictly decreasing sequence $a_1 > a_2 > a_3 > \cdots$ of elements of S.

(c) [2 marks] Define what is meant by a *monomial order* for $F[x_1, \ldots, x_n]$.

(d) [4 marks] Define *lexicographic order* on $\mathbb{N}^n$, and, assuming that this order is a well-order, prove that it is a monomial order for $F[x_1, \ldots, x_n]$.

(e) [4 marks] Suppose $\leq$ is a monomial order for $F[x_1, \ldots, x_n]$. Prove that

$$(0, \ldots, 0) \leq \alpha$$

for all $\alpha \in \mathbb{N}^n$.

(f) [4 marks] Show that if $\leq$ is a monomial order for $F[x]$, then $x^0 < x^1 < x^2 < \cdots$.

2. (a) [4 marks] State precisely the input and output specifications of the algorithm `MultivariateDivision`.

(b) [6 marks] Apply the algorithm `MultivariateDivision` systematically to divide $x^2y + xy^2 + xy - y^3$ by $(y^2 - 1, xy - 1)$, using lexicographic order with $x >_{\text{lex}} y$.

[This question continues overleaf . . .]

(c) [6 marks] Define what is meant by an *ideal* of $F[x_1, \ldots, x_n]$, by the ideal $\langle S \rangle$ *generated by* $S \subseteq F[x_1, \ldots, x_n]$, and by a *monomial* ideal of $F[x_1, \ldots, x_n]$.

(d) [5 marks] Give an example, with justification, of $g, g_1, g_2 \in \mathbb{Q}[x]$, such that $g \in \langle g_1, g_2 \rangle \neq \mathbb{Q}[x]$, but multivariate division of g by (g_1, g_2) does not give remainder $r = 0$.

(e) [4 marks] Prove that $\langle x^2 - xy, xy + y^2, (x+y)^2 \rangle$ is a monomial ideal of $\mathbb{Q}[x, y]$.

3. (a) [2 marks] Define what is meant by a *Gröbner basis* for an ideal of $F[x_1, \ldots, x_n]$ (with respect to a fixed monomial order for $F[x_1, \ldots, x_n]$).

(b) [4 marks] Let $0 \neq f \in F[x_1, \ldots, x_n]$. Show that, with respect to any fixed monomial order, $\{f\}$ is a Gröbner basis for $\langle f \rangle$.

(c) [2 marks] Define what is meant by the *S-polynomial* of two polynomials in $F[x_1, \ldots, x_n]$.

(d) [3 marks] Let $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$ and $I = \langle f_1, \ldots, f_s \rangle$. Describe a method, making use of S-polynomials, to test whether or not $\{f_1, \ldots, f_s\}$ is a Gröbner basis for I (with respect to a fixed monomial order for $F[x_1, \ldots, x_n]$).

(e) [8 marks] Apply the algorithm `GröbnerBasis` to determine a Gröbner basis for the ideal $\langle xy - 1, xz - 1 \rangle$ of $\mathbb{Q}[x, y, z]$, with respect to lexicographic order with $x >_{\text{lex}} y >_{\text{lex}} z$.

(f) [6 marks] Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals of $F[x_1, \ldots, x_n]$. Prove that there exists an integer $N \geq 1$ such that $I_N = I_{N+1} = \cdots$. (You may assume that every ideal of $F[x_1, \ldots, x_n]$ has a Gröbner basis.)

4. (a) [7 marks] Let $f, f_1, \ldots, f_s, g_1, \ldots, g_t \in F[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_s \rangle$, and $J = \langle g_1, \ldots, g_t \rangle$. Explain precisely how to use Gröbner bases to determine:

(i) whether $f \in I$;

(ii) whether $I \subseteq J$;

(iii) whether $I = J$.

(b) [6 marks] Let I be an ideal of $F[x_1, \ldots, x_n]$ and $j \in \{0, \ldots, n-1\}$. Define what is meant by the *j-th elimination ideal* I_j, and prove that I_j is an ideal of $F[x_{j+1}, \ldots, x_n]$.

(c) [2 marks] Let $j \in \{1, \ldots, n-1\}$. Define what is meant by a monomial order for $F[x_1, \ldots, x_n]$ of *j-elimination type.*

(d) [10 marks] Let $j \in \{1, \ldots, n-1\}$ and let G be a Gröbner basis for an ideal I of $F[x_1, \ldots, x_n]$, with respect to a monomial order $\leq$ of j-elimination type. Prove that $G \cap F[x_{j+1}, \ldots, x_n]$ is a Gröbner basis for the j-th elimination ideal I_j (with respect to $\leq$ restricted to $F[x_{j+1}, \ldots, x_n]$).

[Next question overleaf]

5. Let $(v_1, \ldots, v_n)$ be a sequence of linearly independent vectors in $\mathbb{R}^n$.

(a) [2 marks] Define what is meant by the *lattice* with *basis* $(v_1, \ldots, v_n)$.

(b) [8 marks] Suppose L and M are lattices in $\mathbb{R}^n$, with respective bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_n)$. Let V be the $n \times n$ matrix whose rows are $v_1, \ldots, v_n$ and W be the $n \times n$ matrix whose rows are $w_1, \ldots, w_n$.

(i) Prove that if $L \subseteq M$ then there is an integer d such that $\det(V) = d \det(W)$.

(ii) Deduce that the *norm* of L, defined to be $|\det(V)|$, does not depend on the choice $(v_1, \ldots, v_n)$ of basis for L.

(c) [7 marks] State precisely how to determine the *Gram-Schmidt orthogonalization* (or *GSO*) $((v_1^*, \ldots, v_n^*), M)$ of $(v_1, \ldots, v_n)$, and state the main properties of this GSO.

(d) [8 marks] Suppose L is a lattice with basis $(v_1, \ldots, v_n)$, and let $((v_1^*, \ldots, v_n^*), M)$ be the GSO of $(v_1, \ldots, v_n)$. Prove that if $0 \neq v \in L$, then $|v| \geq \min\{|v_1^*|, \ldots, |v_n^*|\}$.

6. (a) [2 marks] Define what is meant by a *reduced* basis for a lattice.

(b) [6 marks] Suppose $(v_1, \ldots, v_n)$ is a reduced basis for a lattice L, and $0 \neq v \in L$. Prove that $|v_1| \leq 2^{(n-1)/2}|v|$. (You may assume the result of question 5(d) holds.)

(c) [5 marks] State precisely the input and output specifications of the algorithm `BasisReduction`.

(d) [12 marks] Describe the *subset sum problem*, and how the algorithm `BasisReduction` may be employed in an attempt to find a solution to this problem.

[End of examination paper]