Queen Mary
UNIVERSITY OF LONDON

B.Sc. EXAMINATION

MAS400 Advanced Algorithmic Mathematics

Friday 18 May 2001, 2:30 pm – 5:30 pm

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.*

Show your calculations.

The symbol $\mathbb{K}$ *denotes a field.*

1. (a) [6 marks] Define what is meant by *partially ordered*, *totally ordered* and *well ordered* sets.
[3 marks] Give one example in each case, with a brief explanation, of a set that is:

(i) partially but not totally ordered;
(ii) totally but not well ordered;
(iii) well ordered.

(b) [4 marks] Define what is meant by *monomial ordering* and by *lexicographic ordering* on the ring $\mathbb{K}[x_1, \ldots, x_n]$ of multivariate polynomials.
[12 marks] Prove that lexicographic ordering is a monomial ordering.

2. [10 marks] Give an algorithm to divide one multivariate polynomial by a sequence of multivariate polynomials in $\mathbb{K}[x_1, \ldots, x_n]$, specifying the input and output precisely.

[8 marks] Sketch a proof that the algorithm terminates and, by using a loop invariant, that it is correct.

[5 marks] Apply the algorithm systematically to divide $f = x^2y + xy^2 + xy + y^2$ by $f_1 = xy + 1, f_2 = x + 1$ (in that order) using lexicographic ordering with $x > y$.

[2 marks] State a condition under which the result of this division algorithm is independent of the order of the polynomials in the divisor sequence.

3. (a) [5 marks] Define what is meant by:

(i) an *ideal* of $\mathbb{K}[x_1, \ldots, x_n]$,

(ii) a *generating set* for an ideal of $\mathbb{K}[x_1, \ldots, x_n]$,

(iii) a *monomial ideal*.

(b) [8 marks] Define a *Gröbner Basis* for an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. Prove that any finite basis of monomials for a monomial ideal is a Gröbner Basis for that ideal.

(c) [2 marks] Define what is meant by an *S-polynomial*.
[7 marks] State Buchberger's Algorithm, specifying the input and output precisely.

(d) [3 marks] Prove that $\{xy - 1, y^2 + 1\} \subseteq \mathbb{Q}[x, y]$ is *not* a Gröbner Basis for the ideal it generates in some appropriate ordering, which you must specify.

4. (a) [5 marks] Explain precisely how to use Gröbner Bases to determine:

(i) whether $f \in \mathbb{K}[x_1, \ldots, x_n]$ is in an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$;

(ii) whether $I = J$, where I, J are ideals of $\mathbb{K}[x_1, \ldots, x_n]$.

(b) [2 marks] Define the term *Principal Ideal Domain* (PID).
[8 marks] Prove that $\mathbb{K}[x]$ is a PID and that $\mathbb{K}[x_1, \ldots, x_n]$ is not a PID if $n > 1$.

(c) [2 marks] Define the term *reduced* when applied to a Gröbner Basis.

(d) [8 marks] Let $I = \langle x^2+1, x^3-x^2+x-1, x^4+2x^2+1\rangle$, $J = \langle x^2, x^3+x^2+x+1, x^4-1\rangle$ be ideals of $\mathbb{K}[x]$. Find (in any way you wish) *reduced* Gröbner Bases for I and J. Determine, with brief explanations, which of the following statements are true: $I = J$; $x^3 + x \in I$; $x \in J$.

5. [5 marks] Let $V = \boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ be a non-empty linearly independent sequence of vectors in $\mathbb{R}^n$. State the Gram-Schmidt orthogonalization process, which generates a new sequence $V^* = \boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_r^*$ of pairwise orthogonal vectors.

[5 marks] Prove that the vectors in V^* above are indeed pairwise orthogonal.

[5 marks] Prove that $|\boldsymbol{v}_i^*| \leq |\boldsymbol{v}_i|$ for $i = 1, \ldots, r$, where $|\boldsymbol{v}|$ denotes $\sqrt{\boldsymbol{v} \cdot \boldsymbol{v}}$.

[5 marks] Show that V and V^* are related, as columns of row vectors, by $V = T\,V^*$, and give the structure of the matrix T as fully as possible.

[5 marks] Hence, prove Hadamard's inequality, in the form

$$\left| \det \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix} \right| \leq \prod_{i=1}^{n} |\boldsymbol{v}_i|$$

by considering the above theory for the special case $r = n$.

6. (a) [9 marks] Let $\boldsymbol{v}_1 = (1, -2, 3)$, $\boldsymbol{v}_2 = (2, 5, -3)$, and let L be the lattice with basis $\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$. Apply the LLL algorithm to $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ to determine an LLL-reduced ordered basis for the lattice L. Explain your calculations briefly in terms of the steps of the algorithm.

[8 marks] Compute the determinant of the lattice L and use this determinant to make a partial check on the correctness of your basis reduction computation.

(b) [8 marks] Let L be a lattice with ordered basis $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$ and let $m \in \mathbb{Z}$. Prove that the sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_i - m\boldsymbol{v}_j, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_r)$ with $1 \leq j < i \leq r$ is an ordered basis for L having the same Gram-Schmidt orthogonalization as $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$.

 [End of examination paper.]