Queen Mary
UNIVERSITY OF LONDON

M.Sci. EXAMINATION

MAS400 Advanced Algorithmic Mathematics

Tuesday 27 May 2003, 10:00 am – 1:00 pm

The duration of this examination is three *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. Show your calculations.*

Calculators are not *permitted in this examination.*

$\mathbb{N}$ *denotes the set of non-negative integers,* $\mathbb{K}$ *denotes a field, and* $|\boldsymbol{v}|$ *denotes the (Euclidean) length of a vector* $\boldsymbol{v}$*.*

1. (a) [6 marks] Write down an algorithm to divide a multivariate polynomial by a sequence of multivariate polynomials. Include precise specifications of the input and output.

(b) [7 marks] From this algorithm, *deduce* an algorithm to divide one univariate polynomial by another, including precise specifications of the input and output. Outline the steps in your deduction.

(c) [5 marks] Divide $x^5 + x^2$ by $2x^2 + x - 1$ in $\mathbb{Q}[x]$.

(d) [7 marks] Divide $x^5y^2 + x^3y + 2x^2 + xy + 1$ by $xy + 1, x + y$ in $\mathbb{Q}[x, y]$ using lexicographic ordering with $x >_{\text{lex}} y$.

2. (a) [2 marks] Define what is meant by a *basis* for an ideal.

(b) [2 marks] Define what is meant by a *monomial ideal.*

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

(d) [5 marks] Let $A \subseteq \mathbb{N}^n$, $I = \langle x^\alpha \mid \alpha \in A\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$, and $\beta \in \mathbb{N}^n$. Prove that $x^\beta \in I$ if and only if x^α divides x^β for some $\alpha \in A$.

(e) [1 mark] State Dickson's Lemma.

(f) [2 marks] Define what is meant by a *Gröbner Basis* for an ideal.

(g) [4 marks] Prove that every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ has a Gröbner Basis.

(h) [5 marks] Prove that a Gröbner Basis for an ideal is a basis for that ideal. [Hint: prove that the remainder vanishes in an appropriate generalized polynomial division.]

3. (a) [2 marks] Define what is meant by the *S-polynomial* of two multivariate polynomials.

(b) [2 marks] State a condition in terms of S-polynomials for a basis to be a Gröbner Basis.

(c) [5 marks] State Buchberger's Algorithm to compute a Gröbner Basis. Include precise specifications of the input and output.

(d) Working in $\mathbb{Q}[x, y, z]$ and using lexicographic ordering with $x >_{\text{lex}} y >_{\text{lex}} z$:

(i) [3 marks] prove that $\{x - y, y^2 + z\}$ is a Gröbner Basis for the ideal I that it generates;

(ii) [8 marks] compute a Gröbner Basis for $J = \langle x - y, xy - z \rangle$.

(e) [5 marks] With I and J defined as above, determine whether $I = J$ and briefly explain your reasoning.

4. (a) [8 marks] Define what is meant by the *affine variety* $\mathbb{V}(F)$ of a set F of multivariate polynomials and define what is meant by the *affine variety* $\mathbb{V}(I)$ of a multivariate polynomial ideal I. If I is generated by F, prove that $\mathbb{V}(I) = \mathbb{V}(F)$.

(b) [6 marks] Define the term *elimination ideal* and define what it means for a monomial ordering to be of *j-elimination type.*

(c) [3 marks] Prove that lexicographic ordering is of *j-elimination type* for all (meaningful) values of j.

(d) [3 marks] State the *Elimination Theorem* for Gröbner Bases of elimination ideals.

(e) [5 marks] Given that, using lexicographic ordering with $x >_{\text{lex}} y >_{\text{lex}} z$, the set $\{x - y, y^2 + z\}$ is a Gröbner Basis for the ideal $I \subseteq \mathbb{R}[x, y, z]$ that it generates, use the elimination ideal approach to determine $\mathbb{V}(I)$ explicitly. Explain your reasoning.

[Next question overleaf]

5. (a) [2 marks] Define what is meant by a *lattice of rank* r in $\mathbb{R}^n$.

(b) [3 marks] Define what is meant by a *Gram matrix* and define what is meant by the *determinant of a lattice.*

(c) [5 marks] Prove that the determinant of a lattice depends only on the lattice and not on its representation.

(d) [5 marks] State the *Gram-Schmidt orthogonalization process* and define what is meant by the *Gram-Schmidt coefficients.*

(e) Let $V = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$ be a sequence of vectors in $\mathbb{R}^n$ and let $V^* = (\boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_r^*)$ be its Gram-Schmidt orthogonalization.

(i) [3 marks] Prove that $|\boldsymbol{v}_i^*| \leq |\boldsymbol{v}_i|$.

(ii) [3 marks] Express the relationship between V and V^* in the form of a matrix equation and state the structure of the matrices involved.

(iii) [2 marks] Deduce a bound on the determinant of the Gram matrix of V.

(iv) [2 marks] State and prove Hadamard's inequality for the determinant of an arbitrary square matrix.

6. (a) [5 marks] Let L be a lattice of rank r in $\mathbb{R}^n$ and let $(\boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_r^*)$ be the Gram-Schmidt orthogonalization of the lattice basis. Prove that each nonzero vector $\boldsymbol{v} \in L$ satisfies $|\boldsymbol{v}| \geq |\boldsymbol{v}_s^*|$ for some s, $1 \leq s \leq r$, and hence prove that $\min\{|\boldsymbol{v}| : \boldsymbol{0} \neq \boldsymbol{v} \in L\} \geq \min\{|\boldsymbol{v}_i^*| : 1 \leq i \leq r\}$.

(b) [5 marks] Define what is meant by (i) a *weakly reduced* basis, and (ii) an *LLL-reduced* basis, for a lattice.

(c) If $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r)$ is an LLL-reduced basis for a lattice L with Gram-Schmidt orthogonalization $(\boldsymbol{v}_1^*, \ldots, \boldsymbol{v}_r^*)$, prove that:

(i) [5 marks] $|\boldsymbol{v}_i^*|^2 \geq \frac{1}{2}|\boldsymbol{v}_{i-1}^*|^2$;

(ii) [2 marks] $|\boldsymbol{v}_i^*|^2 \geq 2^{1-i}|\boldsymbol{v}_1|^2$;

(iii) [4 marks] $|\boldsymbol{v}_1| \leq 2^{(r-1)/2} \min\{|\boldsymbol{v}| : \boldsymbol{0} \neq \boldsymbol{v} \in L\}$;

(iv) [4 marks] $|\boldsymbol{v}_1| \leq 2^{(r-1)/4} \sqrt[r]{\prod_{i=1}^{r} |\boldsymbol{v}_i^*|}$.

[End of examination paper]