Queen Mary
UNIVERSITY OF LONDON

M.Sci. EXAMINATION BY COURSE UNIT

MAS400 Advanced Algorithmic Mathematics

25 May 2005, 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) [2 marks] Define what is meant by an *ideal* of $F[x_1, \ldots, x_n]$.

(b) [5 marks] Let $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$. Define what is meant by $\langle f_1, \ldots, f_s \rangle$, and prove that $\langle f_1, \ldots, f_s \rangle$ is an ideal of $F[x_1, \ldots, x_n]$.

(c) [6 marks] Prove that if I is an ideal of $F[x]$ then $I = \langle g \rangle$ for some $g \in F[x]$.

(d) [4 marks] Let $f, g \in \mathbb{Q}[x]$. Describe a method (not using Gröbner bases) to determine whether or not $f \in \langle g \rangle$.

(e) [6 marks] Let $A \subseteq \mathbb{N}^n$, $I = \langle \underline{x}^\alpha \mid \alpha \in A \rangle \subseteq F[x_1, \ldots, x_n]$, and $f \in F[x_1, \ldots, x_n]$. Prove that $f \in I$ if and only if each term of f is divisible by $\underline{x}^\alpha$ for some $\alpha \in A$.

(f) [2 marks] State Dickson's Lemma.

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

(b) [3 marks] Fix a monomial order for $F[x_1, \ldots, x_n]$, and let $0 \neq f \in F[x_1, \ldots, x_n]$. Define, for f, what are meant by the *multidegree* $\mathrm{mdeg}(f)$, the *leading monomial* $\mathrm{lm}(f)$, and the *leading term* $\mathrm{lt}(f)$.

(c) [10 marks] State precisely the algorithm `MultivariateDivision`, including the input and output specifications.

(d) [4 marks] Explain why the algorithm `MultivariateDivision` must always terminate.

[This question continues overleaf . . .]

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

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

(c) [3 marks] Let $0 \neq f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$ and $I = \langle f_1, \ldots, f_s \rangle$. State a theorem which provides a method using 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 $F[x_1, \ldots, x_n]$).

(d) [4 marks] State precisely the input and output specifications of the algorithm `GröbnerBasis`.

(e) [6 marks] Explain why the algorithm `GröbnerBasis`, when it terminates, returns the correct output.

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

4. (a) [10 marks] Let G be a Gröbner basis for an ideal I of $F[x_1, \ldots, x_n]$, and let $f \in F[x_1, \ldots, x_n]$. Prove that there exist unique $h, r \in F[x_1, \ldots, x_n]$, such that

1. $f = h + r$,
2. $h \in I$, and
3. $r = 0$ or no term of r is divisible by any element of $\text{lt}(G)$.

(b) [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:

1. whether $f \in I$;
2. whether $I \subseteq J$;
3. whether $I = J$.

(c) [3 marks] Define what is meant by a *reduced Gröbner basis* for an ideal I of $F[x_1, \ldots, x_n]$.

(d) [5 marks] Let I be an ideal of $F[x_1, \ldots, x_n]$. Prove that $I = F[x_1, \ldots, x_n]$ if and only if $\{1\}$ is a reduced Gröbner basis for I.

[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) [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.

(c) [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 $\underline{0} \neq v \in L$, then $|v| \geq \min\{|v_1^*|, \ldots, |v_n^*|\}$.

(d) [8 marks] Let L be the lattice with basis $(v_1, \ldots, v_n)$, let $m \in \mathbb{Z}$, and $1 \leq j < i \leq n$. Prove that $(v_1, \ldots, v_{i-1}, v_i - mv_j, v_{i+1}, \ldots, v_n)$ is also a basis for L, and in addition, has the same Gram-Schmidt orthogonal basis as $(v_1, \ldots, v_n)$.

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

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

(c) Let $L = \langle (2, -1), (4, -3) \rangle_{\mathbb{Z}}$.

(i) [3 marks] Calculate the norm $|L|$ of the lattice L.

(ii) [15 marks] Apply the algorithm `BasisReduction` to determine a reduced basis for L. Explain your calculations in terms of the steps of the algorithm.

[End of examination paper]