Queen Mary
University of London

M. Sci. Examination 2006

MAS400 Advanced Algorithmic Mathematics

Duration: 3 hours

Date and time: 19th May 2006, 10:00–13:00

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 4 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, $\mathbb{N} = \{0, 1, \ldots\}$ *denotes the set of non-negative integers and* F *denotes an arbitrary field.*

Question 1 (25 marks)

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

(b) Define what is meant by a *monomial order* on $F[x_1,\ldots,x_n]$ (equivalently, on $\mathbb{N}^n$). [2]

(c) Define what is meant by the *lexicographic order* $\leqslant_{\text{lex}}$ on $\mathbb{N}^n$. [2]

(d) Show that $\leqslant_{\text{lex}}$ is a well-order and a monomial order on $\mathbb{N}^n$. You may assume that $\leqslant_{\text{lex}}$ is a total order. You may also assume that a set S is well-ordered if and only if it has no infinite strictly descending chains. [7]

(e) Prove that if $\leqslant$ is a monomial order on $\mathbb{N}^n$ then $(0,\ldots,0) \leqslant \alpha$ for all $\alpha \in \mathbb{N}^n$. [4]

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

Question 2 (25 marks)

(a) Write down the algorithm `MultivariateDivision`, stating the input and output precisely. [10]

(b) Show that the algorithm `MultivariateDivision` terminates, and produces the correct output. [8]

(c) Let $f, f_1, \ldots, f_s \in F[x_1,\ldots,x_n]$ with $f_i \neq 0$ for all i. Let $r = f \text{ rem } (f_1,\ldots,f_s)$. Show that the ideals $\langle f, f_1,\ldots,f_s\rangle$ and $\langle r, f_1,\ldots,f_s\rangle$ coincide. [2]

(d) Apply `MultivariateDivision` to divide $x^4y+x^3y+x^2y+xy+1$ by $\{f_1, f_2\} = \{x^3+y, x^2-xy\}$ (in that order), using the lexicographic order on $F[x,y]$ in which $x>y$. [5]

Question 3 (25 marks)
In this question $R = F[x_1, \ldots, x_n]$, and a monomial order $\leqslant$ on R is fixed.

(a) Let $A \subseteq \mathbb{N}^n$, let $I = \langle \underline{x}^\alpha : \alpha \in A \rangle$ be an ideal of R, and let $f \in R$. Show that $f \in I$ if and only if each term of f is divisible by $\underline{x}^\alpha$ for some $\alpha \in A$. [6]

(b) State Dickson's Lemma. [2]

(c) For $S \subseteq R$ define $\operatorname{lt} S$ (with respect to $\leqslant$). [1]

(d) Let I be an ideal of R and let $G \subseteq I$. State precisely what it means for G to be a Gröbner basis for I (with respect to $\leqslant$). [4]

(e) Show that I has a Gröbner basis. [2]

(f) Let G be a Gröbner basis for I. Show that I is generated by G. Deduce that I is finitely generated. [5]

(g) Show that R has no infinite strictly ascending chain of ideals. [5]

Question 4 (25 marks)
In parts (a)–(c), $R = F[x_1, \ldots, x_n]$, and a monomial order $\leqslant$ on R is fixed.

(a) Define the *S-polynomial* $S(f, g)$ for polynomials $f, g \in R$. [2]

(b) Let $0 \notin \{f_1, \ldots, f_s\} \subseteq R$, and let $I = \langle f_1, \ldots, f_s \rangle$. State a theorem involving S-polynomials that gives a necessary and sufficient condition for $\{f_1, \ldots, f_s\}$ to be a Gröbner basis of I (with respect to $\leqslant$). [3]

(c) Give pseudo-code for the algorithm `GröbnerBasis` that includes accurate descriptions of the input and output. [10]

(d) Let $R = F[x, y]$ be equipped with the monomial order $\leqslant_{\text{lex}}$ where $x >_{\text{lex}} y$. Let $f_1 = x^2y + 1$, $f_2 = xy^2 + y$, and $I = \langle f_1, f_2 \rangle$. Calculate $g := S(f_1, f_2)$, placing its leading term first, and determine $r_1 := f_1 \text{ rem } (g)$ and $r_2 := f_2 \text{ rem } (g)$. Show that $I = \langle r_1, r_2, g \rangle$. Determine the reduced Gröbner basis for I.
[Hint: Do not apply `GröbnerBasis` to the input $\{f_1, f_2\}$.] [8]

(e) Use any method to determine the affine variety $\mathbb{V}(x^2y + 1, xy^2 + y) \subseteq F^2$. [2]

Question 5 (25 marks)

(a) Let $(v_1, \ldots, v_r)$ be a sequence of $\mathbb{R}$-linearly independent vectors of $\mathbb{R}^n$ (where $r \leqslant n$, and you may assume that $r \geqslant 1$). State precisely how to determine the *Gram–Schmidt orthogonalisation*, or *GSO*, $((v_1^*, \ldots, v_r^*), (\mu_{ij}))$ of $(v_1, \ldots, v_r)$, and state the main properties of this GSO. [7]

(b) Prove that the vectors in $(v_1^*, \ldots, v_r^*)$ are indeed pairwise orthogonal. [5]

(c) Prove that $|v_i| \geqslant |v_i^*|$ for $1 \leqslant i \leqslant r$, where $|v|$ denotes $\sqrt{v \cdot v}$. [3]

(d) Let A be the $r \times n$ matrix whose i^{th} row is v_i, and define A^* similarly. Thus

$$A := \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} \quad \text{and} \quad A^* := \begin{pmatrix} v_1^* \\ \vdots \\ v_r^* \end{pmatrix}.$$

Show that A and A^* are related by $A = TA^*$, and describe the structure of T as fully as possible. [4]

(e) Hence prove Hadamard's inequality in the form

$$\left| \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right| \leqslant \prod_{i=1}^{n} |v_i|$$

by considering the above theory in the special case $r = n$. [6]

Question 6 (25 marks)

(a) State what is meant by the lattice generated by $v_1, \ldots, v_n$ ($v_i \in \mathbb{R}^n$ for all i). [2]

(b) State what is meant by a *reduced basis* of a lattice. [2]

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

(d) Let $L = \langle (1, -2), (4, -5) \rangle_{\mathbb{Z}}$.

 (i) Determine the norm $|L|$ of the lattice L. [2]

 (ii) Apply the algorithm `BasisReduction` to produce a reduced basis for L. Explain your calculations in terms of steps of the algorithm. [14]

 END OF EXAMINATION