Queen Mary
University of London

M. Sc. Examination 2007

MTHM032 Advanced Algorithmic Mathematics

Duration: 3 hours

Date and time: 29th May 2007, 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) For each of the three cases below give, with a very brief justification, examples $(S, <)$ such that:

(i) $<$ is a partial order but not a total order on the set S;

(ii) $<$ is a total order but not a well-order on the set S;

(iii) $<$ is a well-order on the set S. [3]

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

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

(e) Show that $\leqslant_{\text{lex}}$ is a total order, a well-order and a monomial order on $\mathbb{N}^n$. You may assume that a set S is well-ordered if and only if it has no infinite strictly descending chains. [12]

Question 2 (25 marks)

(a) Write down the algorithm `MultivariateDivision`, stating the input and output precisely. [9]

(b) Show that the algorithm `MultivariateDivision` terminates. [3]

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

(d) Let $A \subseteq \mathbb{N}^n$, let $I = \langle \underline{x}^\alpha : \alpha \in A \rangle$ be an ideal of $R = F[x_1, \ldots, x_n]$, 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]

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

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

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

(b) 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]

(c) What does it mean for G to be a reduced Gröbner basis for the ideal it generates? [3]

(d) Let G be a Gröbner basis for an ideal I of R and let $f \in R$. Show that there exist unique $h, r \in R$ 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 $\operatorname{lt} G$. [10]

(e) Let $f, f_1, \dots, f_s, g_1, \dots, g_t \in R$, with ideals $I = \langle f_1, \dots, f_s \rangle$ and $J = \langle g_1, \dots, g_t \rangle$. Explain precisely how to determine:

(i) whether $f \in I$;

(ii) whether $I \subseteq J$; and

(iii) whether $I = J$. [7]

Question 4 (25 marks)
In parts (a)–(c), $R = F[x_1, \dots, x_n]$, 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 $0 \notin \{f_1, \dots, f_s\} \subseteq R$, and let $I = \langle f_1, \dots, f_s \rangle$. State a theorem involving S-polynomials that gives a necessary and sufficient condition for $\{f_1, \dots, f_s\}$ 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) Find a Gröbner basis for the ideal $I = \langle f_1, f_2 \rangle \leqslant F[x, y]$, where $f_1 = x^3 + y^3$ and $f_2 = x^2 + y^2$, under the lexicographic monomial ordering in which $x >_{\text{lex}} y$. Hence, or otherwise, determine the affine variety $\mathbb{V}(x^3 + y^3, x^2 + y^2) \subseteq F^2$. (Note that the answers do depend on the field F, in particular on whether $2 = 0$ holds in F.) [10]

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

(c) Suppose that $v = \sum_{i=1}^n a_i v_i$ for some $a_1,\ldots,a_n \in \mathbb{Z}$. Show that if $v \neq 0$ then $|v| \geqslant \min\{|v_1^*|,\ldots,|v_n^*|\}$. [6]

(d) The algorithm `BasisReduction` sometimes requires one to swap two adjacent basis vectors, and to update the resulting GSO. So let $2 \leqslant i \leqslant n$, and let $w_{i-1} = v_i$, $w_i = v_{i-1}$ and $w_j = v_j$ whenever $1 \leqslant j \leqslant n$ and $j \notin \{i-1,i\}$. Let $((w_1^*,\ldots,w_n^*),(\xi_{kl}))$ be the GSO of $(w_1,\ldots,w_n)$. Determine the differences between $((v_1^*,\ldots,v_n^*),(\mu_{kl}))$ and $((w_1^*,\ldots,w_n^*),(\xi_{kl}))$, and explain how you would calculate $((w_1^*,\ldots,w_n^*),(\xi_{kl}))$ efficiently given $((v_1^*,\ldots,v_n^*),(\mu_{kl}))$.

Do *not* calculate w_i^*, $\xi_{k,i}$ or $\xi_{k,i-1}$ for $k \geqslant i$; the other w_j^* and ξ_{kl} should be determined in terms of the v_j^* and μ_{kl}. [9]

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 $L = \langle(1,-3),(3,-7)\rangle_{\mathbb{Z}}$.

(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