Manuel Kauers
RISC-Linz

Hagenberg, January 18, 2003

Computer Algebra Exercises
Solution 8

Ex. (36) Let $\leq_1, \leq_2$ be admissible orderings. We have to show that also $\leq := \mathrm{prod}(\leq_1, \leq_2)$ is admissible. This means that 1 is its minimum and $a \leq b$ implies $ac \leq bc$ for all a, b, c.

1 is the minimum of $\leq$: Let $t_1 \in [x_1, \ldots, x_i]$ and $t_2 \in [x_{i+1}, \ldots, x_n]$. Then

$$1 \leq t_1 t_2 \iff 1 <_1 t_1 \vee (1 =_1 t_1 \wedge 1 \leq_2 t_2)$$

Since $\leq_1$ is an admissible order, $1 <_1 t_1$ or $1 =_1 t_1$ must be true. In the first case, we are done, and in the second case, we have $1 \leq_2 t_2$ which is asserted by the admissibility of $\leq_2$.

$\leq$ is monotonous: Let $a = a_1 a_2$, $b = b_1 b_2$ and $c = c_1 c_2$ be such that $a \leq b$. Then, by definition,

$$a_1 <_1 b_1 \vee (a_1 =_1 b_1 \wedge a_2 \leq_2 b_2)$$

which by the admissibility of $\leq_1$ and $\leq_2$ and some other trivial properties ("monotonicity" of $=_1$ and $\neq_1$) also implies

$$a_1 c_1 <_1 b_1 c_1 \vee (a_1 c_1 =_1 b_1 c_1 \wedge a_2 c_2 \leq_2 b_2 c_2),$$

i.e. $ac \leq bc$.

This completes the proof.

Ex. (37) To prove:
Any admissible ordering on $[X] = [x_1, \ldots, x_n]$ is noetherian, i.e. any strictly descending sequence is finite.

Assume that $s_1, s_2, \ldots$ is in strictly descending sequence. The admisibility of the order asserts that none of the s_i can lie in the intersection of the cones spanned by the s_j $(j < 1)$, because the elements of the cone with corner s_i are of the form $s = s_i \cdot t$ and hence $s \geq s_i$.

In order to be outside the the cone of s_1, the term s_2 must have a strictly lower exponent in at least one variable. It is clear by inspection that there are only finitely many terms in the square spanned by $\gcd(s_1, s_2)$, s_1 and s_2. We can ignore them and find that the next term, say s_3, has to be strictly less than $\gcd(s_1, s_2)$, i.e. it cannot lie in its cone, i.e. it must have at least one variable with strictly smaller exponent.

We see that a strictly decreasing sequence of terms induces strictly decreasing sequences on the exponents. But the exponents live in the natural numbers, so each of them finally has to be finite. Since there are only finitely many variables, all of the exponent sequences have to be finished at some point. This completes the "proof."

Ex. (38) Let $f_1 = x^2y + xy + 1, f_2 = y^2 + x + y \in \mathbb{Z}_3[x, y]$. We compute a Grö bner basis of $\langle f_1, f_2\rangle$ wrt. graduated lexicographical ordering where $x > y$ by Bruno's algorithm.

$$
\begin{aligned}
f_1 &= \boldsymbol{x^2y} + xy + 1 \\
f_2 &= \boldsymbol{y^2} + x + y \\
S(f_1, f_2) &= xy^2 + y - \boldsymbol{x^3} - x^2y \\
&\xrightarrow{-xf_2} -\boldsymbol{xy^2} - x^2 - xy \\
&\xrightarrow{+f_1} -\boldsymbol{x^3} + y - x^2 + 1 =: f_3 \\
S(f_1, f_3) &= x + \boldsymbol{y^2} - y \\
&\xrightarrow{-f_2} 0 \\
S(f_2, f_3) &= -\boldsymbol{x^4} - x^3y + y^2x^2 - y^3 - y^2 \\
&\xrightarrow{-xf_3} -\boldsymbol{x^3y} + y^2x^2 - y^3 - y^2 + x^3 - xy - x \\
&\xrightarrow{-yf_3} -\boldsymbol{2x^3y} + y^2x^2 - y^3 + x^3 - xy - x - x^2y + y \\
&\xrightarrow{-2yf_3} \boldsymbol{y^2x^2} - y^3 + x^3 - xy - x + x^2y - y - 2y^2 \\
&\xrightarrow{-x^2f_2} -\boldsymbol{y^3} - xy - x - y - 2y^2 \\
&\xrightarrow{+yf_2} -x - \boldsymbol{y^2} - y \\
&\xrightarrow{+f_2} 0.
\end{aligned}
$$

Hence,

$$\{\boldsymbol{x^2y} + xy + 1, \boldsymbol{y^2} + x + y, -\boldsymbol{x^3} + y - x^2 + 1\}$$

is a Gröbner basis of $\langle f_1, f_2\rangle$.

Ex. (39) We use Gröbner basis computations to find solutions of the system

$$
\begin{aligned}
f_1(x, y, z) &= 2xy - yz + 2z \\
f_2(x, y, z) &= x^2 + yz - 1 \\
f_3(x, y, z) &= xz + yz - 2x
\end{aligned}
$$

Using a lexicographic ordering with $x > y > z$, Maple gives us the following (reduced) Gröbner basis:

$$
\begin{gathered}
\{56z^3 - 72z^2 + 32z - 16 + 2z^5 - 21z^4, \\
-96 - 194z^2 - 6z^4 + 67z^3 + 56y + 224z, \\
112x + 10z^4 - 93z^3 + 146z^2 - 84z - 8\}
\end{gathered}
$$

A factorisation shows that the first polynomial is irreducible in $\mathbb{Q}$. Let α be an algebraic number that is a root of this polynomial. We know that every solution of the system must have $z = \alpha$. We plug $z = \alpha$ into the second equation and get

$$y = \tfrac{3}{28}\alpha^4 - \tfrac{67}{56}\alpha^3 + \tfrac{97}{28}\alpha^2 - 4\alpha + \tfrac{12}{7}.$$

We can do the same with the last polynomial and get

$$x = \tfrac{3}{4}\alpha - \tfrac{5}{56}\alpha^4 + \tfrac{93}{112}\alpha^3 - \tfrac{73}{56}\alpha^2 + \tfrac{1}{14}.$$

Summarizing, we got the point

$$(x, y, z) = (\tfrac{3}{4}\alpha - \tfrac{5}{56}\alpha^4 + \tfrac{93}{112}\alpha^3 - \tfrac{73}{56}\alpha^2 + \tfrac{1}{14}, \tfrac{3}{28}\alpha^4 - \tfrac{67}{56}\alpha^3 + \tfrac{97}{28}\alpha^2 - 4\alpha + \tfrac{12}{7}, \alpha)$$

as solution to the original system. This was pretty easy!

Ex. (40) Now consider the system

$$\begin{aligned} f_1(x, y, z) &= xz - xy^2 - 4x^2 - \tfrac{1}{4} \\ f_2(x, y, z) &= y^2 z + 2x + \tfrac{1}{2} \\ f_3(x, y, z) &= x^2 z + y^2 + \tfrac{1}{2}x. \end{aligned}$$

We compute a Gröbner basis wrt. lexicographic ordering with $x > y > z$. This gives us

$$\begin{gathered} G := \{5z^5 + 8z^4 + 3z^3 - 26z^2 - 102z + 60, \\ 33\,134 + 1\,388y^2 + 6\,295z - 2\,405z^2 - 3\,017z^3 - 1\,445z^4, \\ 2\,776x + 705z^4 + 1\,538z^3 + 1\,219z^2 - 3\,656z - 16\,646\} \end{gathered}$$

The first polynomial is again irreducible over $\mathbb{Q}$, let α be a root of it, and solve the second polynomial over $\mathbb{Q}(\alpha)$. This leads to another algebraic number β, and the last polynomial is linear in $\mathbb{Q}(\alpha, \beta)[x]$.

Hence, the solution is

$$(x, y, z) = (-\tfrac{5}{56}\alpha^4 + \tfrac{93}{112}\alpha^3 - \tfrac{73}{56}\alpha^2 + \tfrac{3}{4}\alpha + \tfrac{1}{14}, \beta, \alpha),$$

as it was on the previous sheet.