

Fundamental subroutine: linear system of homogeneous polynomial equations

Proposition 1: given system of homogeneous equations $\sum_{j=1}^s f_{ij} g_j = 0 \quad i \in [r], \quad f_{ij} \in K[\bar{x}],$ one can construct a $K[\bar{x}]$ -module basis for the solutions $(g_1, \dots, g_s) \in K[\bar{x}]^s$.

Moreover there is a bound $\lambda(n, r, d) \leq 2 \cdot (2dr)^{2^n}$, such that a basis of solutions exists with $\deg g_i \leq \lambda(n, r, d)$. In particular this yields a bound $\Lambda(n, r, d)$ on the number of operations (in K) needed to construct such basis.

Proof: We can assume K infinite, otherwise let u be new variable and suppose $(g_i(u, \bar{x}))_{i=1}^s$ is a solution over $K(u)[\bar{x}]$.

Clearing denominators we can assume $g_i(u, \bar{x}) \in K[u, \bar{x}]$ now, by taking the coefficients of any power of u we get a solution over K .

Hence from a basis of solutions over $K(u)$ one gets a basis of solutions over K .

Let $M := (f_{ij})_{i \in [r], j \in [s]}$. Since $\text{rank}_{K(\bar{x})} M = r$, w.l.o.g.

$N := (f_{ij})_{i,j=1}^r$ is nonsingular (over $K(\bar{x})$) and let

$\Delta := \det N$. ($\because \Delta \neq 0$)

Since K is infinite, after an appropriate linear transformation we can assume Δ monic in x_n (i.e. regular in $\bar{x}$).

Let $\tilde{N} := \text{adj}(N) \therefore \tilde{N}N = \Delta \cdot I_r$ and we have

$$M \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix} = 0 \Leftrightarrow 0 = \tilde{N}M \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix} = (\Delta I_r | -Q) \begin{pmatrix} g_1 \\ \vdots \\ g_s \end{pmatrix}$$

$$\Leftrightarrow \Delta g_i = Q_{i(n+1)} g_{n+1} + \dots + Q_{is} g_s \quad i \in [r]$$

where $Q \in K[\bar{x}]^{r \times (s-r)}$.

We have the following set of "special" solutions:

$$(p_{i1}, \dots, p_{in}, \underbrace{0, \dots, 0}_{i-1}, \Delta, 0, \dots, 0) =: v_i$$

In particular, for any solution $(a_1, \dots, a_s)$, by monic division by Δ we can write

$$(a_1, \dots, a_s) = (a'_1, \dots, a'_s) + \sum_{i=1}^r t_i \cdot v_i \quad \text{where } t_i \in K[\bar{x}]$$

and $\deg_n a'_i < \deg_n \Delta$ for $r < i \leq s$.

So we can construct a basis by starting with $v_1, \dots, v_{r-1}$ and then adding solutions $(a_1, \dots, a_s)$ with $\deg_n a_i < \deg_n \Delta$ for $r < i$ (this also bounds $\deg_n a_i < \deg_n \Delta + d$ for $i \in [r]$).

In particular, these solutions can be found by analyzing the following system in $n-1$ variables (i.e. $(x_1, \dots, x_{n-1})$):

$$\text{write } f_{ij} = \sum_{k=0}^d f_{ijk} x_n^k \quad g_i = \sum_{k=0}^{D_n} g_{ik} x_n^k$$

$\uparrow$ these are the new unknowns

and our system becomes (collecting powers of x_n):

$$\sum_{j=1}^s \sum_{k=0}^d f_{ijk} g_{j(n-k)} = 0 \quad i \in [r], \quad 0 \leq k \leq D_n$$

which has $\underbrace{r \cdot (D_n + 1)}_{\tilde{r}}$ equations in $\underbrace{s \cdot D_n}_{\tilde{s}}$ unknowns.

Since $D_n + 1 := \deg_n \Delta + d \leq 2rd$, we have

$$\lambda(n, r, d) \leq 2dr + \lambda(n-1, 2dr^2, d)$$

in particular, if we define by x_k the upper bound on the rank of the linear system when we have k variables we have the following recurrence:

$$x_{n-1} \leq 2dr^2 \Leftrightarrow 2dr_{n-1} \leq (2dx_n)^2$$

$\therefore$ the general recurrence is given by $2dx_{n-k-1} \leq (2dx_{n-k})^2$

$$\Rightarrow 2dx_{n-k} \leq (2dx_n)^{2^k} = (2dx)^{2^{2^k}}$$

$$\Rightarrow \lambda(n, r, d) \leq \sum_{j=0}^n 2dx_{n-j} \leq 2 \cdot (2dx)^{2^n}$$

To get the recurrence just note by the above argument that $x_{n-k-1} \leq x_{n-k} \cdot D_{n-k}$ and $D_{n-k} \leq 2d \cdot x_{n-k}$.

□