Solving (radical) polynomial systems by eigenvectors of a multiplication matrix

December 7, 2022

Algorithm 1: Multivariate Polynomial Division Algorithm

Input: $f, F = (f_1, \ldots, f_s), \geq$ (monomial ordering)

Output: $(q_1, \ldots, q_s), r$ such that $f = \sum_{i=1}^{s} q_i f_i + r$, $\mathrm{LT}_{\geq}(r)$ is not divisible by any of $\mathrm{LT}_{\geq}(f_i)$ or $r = 0$

$q_1 \leftarrow \cdots \leftarrow q_s \leftarrow r \leftarrow 0$
$p \leftarrow f$
while $p \neq 0$ **do**
  $i \leftarrow 1$
  divisionoccured $\leftarrow FALSE$
  while $i \leq s$ **and** divisionoccured $= FALSE$ **do**
    if $\mathrm{LT}_{\geq}(f_i)$ divides $\mathrm{LT}_{\geq}(p)$ **then**
      $q_i \leftarrow q_i + \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)}$
      $p \leftarrow p - \frac{\mathrm{LT}_{\geq}(p)}{\mathrm{LT}_{\geq}(f_i)} f_i$
      divisionoccured $\leftarrow TRUE$
    else
      $i \leftarrow i + 1$
  if divisionoccured $= FALSE$ **then**
    $r \leftarrow r + \mathrm{LT}_{\geq}(p)$
    $p \leftarrow p - \mathrm{LT}_{\geq}(p)$
return $(q_1, \ldots, q_s), r$

Definition 1. *Let* $\mathbf{x}^{\boldsymbol{\alpha}}$ *and* $\mathbf{x}^{\boldsymbol{\beta}}$ *be two monomials. We say that* $\mathbf{x}^{\boldsymbol{\alpha}}$ *is greater or equal than* $\mathbf{x}^{\boldsymbol{\beta}}$ *w.r.t. the graded reverse lexicographic order, or, simply,*

$$\mathbf{x}^{\boldsymbol{\alpha}} \geq_{\mathrm{grevlex}} \mathbf{x}^{\boldsymbol{\beta}}$$

if

$$|\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i > |\boldsymbol{\beta}| = \sum_{i=1}^{n} \beta_i, or |\boldsymbol{\alpha}| = |\boldsymbol{\beta}| \text{ and the rightmost nonzero entry of } \boldsymbol{\alpha} - \boldsymbol{\beta} \text{ is negative.}$$

Example 1. *For the variable ordering* $x > y > z$*, the two monomials*

$$\mathbf{x}^{\boldsymbol{\alpha}} = xy^3z \geq_{\mathrm{grevlex}} x^2yz = \mathbf{x}^{\boldsymbol{\beta}}$$

since $|\boldsymbol{\alpha}| = 1 + 3 + 1 = 5 > |\boldsymbol{\beta}| = 2 + 1 + 1 = 4$*. Also,*

$$\mathbf{x}^{\boldsymbol{\alpha}} = x^2yz \geq_{\mathrm{grevlex}} xy^2z = \mathbf{x}^{\boldsymbol{\beta}}$$

since $|\boldsymbol{\alpha}| = 2 + 1 + 1 = 4 = |\boldsymbol{\beta}| = 1 + 2 + 1 = 4$ *and the rightmost nonzero entry of* $\boldsymbol{\alpha} - \boldsymbol{\beta} = (2, 1, 1) - (1, 2, 1) = (1, -1, 0)$ *is negative.*

Task 1. *Let us have a Gröbner basis* $G = (g_1, g_2, g_3)$ *with*

$$g_1 = x_1x_2 - \frac{4}{3}x_1 - \frac{4}{3}x_2 + \frac{4}{3}$$
$$g_2 = x_2^2 - \frac{2}{3}x_1 - \frac{5}{3}x_2 + \frac{2}{3}$$
$$g_3 = x_1^2 - \frac{5}{3}x_1 - \frac{2}{3}x_2 + \frac{2}{3}$$

w.r.t. grevlex monomial ordering for the variable ordering $x_1 > x_2$*. Construct a multiplication matrix* M_f *for* $f = 1 + x_1 - x_2$ *and extract the solutions to* G *from the eigenvectors of* $M_f^\top$*.*

Solution: According to [1, Section 3.5.6], we have a well-defined linear map

$$\begin{aligned}\mathcal{M}_f\colon \mathbb{Q}\{1, x_1, x_2\} &\to \mathbb{Q}\{1, x_1, x_2\}\\ h &\mapsto fh \bmod G\end{aligned}$$

where $\mathbb{Q}\{1, x_1, x_2\}$ denotes the set of all linear combinations of $1, x_1, x_2$ with coefficients from $\mathbb{Q}$. We can thus see that $\mathbb{Q}\{1, x_1, x_2\}$ is a linear space of dimension 3. We can also see that $\mathcal{M}_f$ is a well-defined linear map since dividing any polynomial from $\mathbb{Q}[x_1, x_2]$ by G yields a polynomial with no monomial divisible by any of $\mathrm{LM}_\geq(g_1) = x_1x_2, \mathrm{LM}_\geq(g_2) = x_2^2, \mathrm{LM}_\geq(g_3) = x_1^2$. Hence, $\mathcal{M}_f$ has a matrix with respect to a basis $B = \{1, x_1, x_2\}$

$$M_f = \mathcal{M}_f(B)_B = \begin{bmatrix}\mathcal{M}_f(1)_B & \mathcal{M}_f(x_1)_B & \mathcal{M}_f(x_2)_B\end{bmatrix}$$

Also, we have

$$f\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G = \begin{bmatrix}\mathcal{M}_f(1)\\\mathcal{M}_f(x_1)\\\mathcal{M}_f(x_2)\end{bmatrix} = \begin{bmatrix}\mathcal{M}_f(1)_B^\top\\\mathcal{M}_f(x_1)_B^\top\\\mathcal{M}_f(x_2)_B^\top\end{bmatrix}\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} = M_f^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \iff f\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} + Q\begin{bmatrix}g_1\\g_2\\g_3\end{bmatrix} = M_f^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix}$$

where Q is a 3×3 matrix of quotient polynomials. Then for a solution (p_1, p_2) to G we have

$$f(p_1, p_2)\begin{bmatrix}1\\p_1\\p_2\end{bmatrix} = f(p_1, p_2)\begin{bmatrix}1\\p_1\\p_2\end{bmatrix} + Q(p_1, p_2)\underbrace{\begin{bmatrix}g_1(p_1, p_2)\\g_2(p_1, p_2)\\g_3(p_1, p_2)\end{bmatrix}}_{\mathbf{0}} = M_f^\top\begin{bmatrix}1\\p_1\\p_2\end{bmatrix}$$

Thus, the solutions to G may be recovered from the eigenvectors of $M_f^\top$. Also, since, for $f = a_0 + a_1x_1 + a_2x_2$ we have

$$M_f^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} = f\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G = (a_0 + a_1x_1 + a_2x_2)\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G = a_0\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} + a_1x_1\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} + a_2x_2\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G =$$

$$= \underbrace{a_0\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G}_{a_0\mathbf{I}\begin{bmatrix}1\\x_1\\x_2\end{bmatrix}} + \underbrace{a_1x_1\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G}_{a_1M_{x_1}^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix}} + \underbrace{a_2x_2\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G}_{a_2M_{x_2}^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix}} = (a_0\mathbf{I} + a_1M_{x_1}^\top + a_2M_{x_2}^\top)\begin{bmatrix}1\\x_1\\x_2\end{bmatrix}$$

In other words,

$$M_f = a_0\mathbf{I} + a_1M_{x_1} + a_2M_{x_2}$$

So, it is sufficient to compute M_{x_1} and M_{x_2}:

$$M_{x_1}^\top\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} = x_1\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \bmod G = \begin{bmatrix}x_1\\x_1^2\\x_1x_2\end{bmatrix} \bmod G = \begin{bmatrix}0 & 1 & 0\\-\frac{2}{3} & \frac{5}{3} & \frac{2}{3}\\-\frac{4}{3} & \frac{4}{3} & \frac{4}{3}\end{bmatrix}\begin{bmatrix}1\\x_1\\x_2\end{bmatrix} \Rightarrow M_{x_1}^\top = \begin{bmatrix}0 & 1 & 0\\-\frac{2}{3} & \frac{5}{3} & \frac{2}{3}\\-\frac{4}{3} & \frac{4}{3} & \frac{4}{3}\end{bmatrix}$$

$$M_{x_2}^\top \begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} = x_2 \begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} \mod G = \begin{bmatrix} x_2 \\ x_1x_2 \\ x_2^2 \end{bmatrix} \mod G = \begin{bmatrix} 0 & 0 & 1 \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \\ -\frac{2}{3} & \frac{5}{3} & \frac{2}{3} \end{bmatrix} \begin{bmatrix} 1 \\ x_1 \\ x_2 \end{bmatrix} \Rightarrow M_{x_2}^\top = \begin{bmatrix} 0 & 0 & 1 \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{5}{3} \end{bmatrix}$$

Thus,

$$M_f^\top = 1 \cdot \mathbf{I} + 1 \cdot M_{x_1}^\top + (-1) \cdot M_{x_2}^\top = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ -\frac{2}{3} & \frac{5}{3} & \frac{2}{3} \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \end{bmatrix} - \begin{bmatrix} 0 & 0 & 1 \\ -\frac{4}{3} & \frac{4}{3} & \frac{4}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{5}{3} \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 \\ \frac{2}{3} & \frac{4}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{2}{3} \end{bmatrix}$$

The characteristic polynomial of $M_f^\top$ is

$$p(\lambda) = \det(\lambda\mathbf{I} - M_f^\top) = \det \begin{bmatrix} \lambda - 1 & -\frac{2}{3} & \frac{2}{3} \\ -1 & \lambda - \frac{4}{3} & \frac{1}{3} \\ -1 & \frac{2}{3} & \lambda - \frac{5}{3} \end{bmatrix} = \lambda^3 - 3\lambda^2 + 2\lambda = \lambda(\lambda - 1)(\lambda - 2)$$

The eigenvectors of $M_f^\top$ are:

1. $\lambda_1 = 0:$
$$(0 \cdot \mathbf{I} - M_f^\top)\mathbf{v}_1 = \mathbf{0}$$
$$\begin{bmatrix} -1 & -1 & 1 \\ -\frac{2}{3} & -\frac{4}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & -\frac{2}{3} \end{bmatrix} \mathbf{v}_1 = \mathbf{0} \Rightarrow \mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

2. $\lambda_2 = 1:$
$$(1 \cdot \mathbf{I} - M_f^\top)\mathbf{v}_2 = \mathbf{0}$$
$$\begin{bmatrix} 0 & -1 & 1 \\ -\frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{bmatrix} \mathbf{v}_2 = \mathbf{0} \Rightarrow \mathbf{v}_2 = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$$

3. $\lambda_3 = 2:$
$$(2 \cdot \mathbf{I} - M_f^\top)\mathbf{v}_3 = \mathbf{0}$$
$$\begin{bmatrix} 1 & -1 & 1 \\ -\frac{2}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{4}{3} \end{bmatrix} \mathbf{v}_3 = \mathbf{0} \Rightarrow \mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

The solutions can be extracted from $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ by looking at the last 2 coordinates:

$$S = \{(0, 1), (2, 2), (1, 0)\}.$$

□

References

[1] Tomas Pajdla, *Elements of geometry for robotics*, `https://cw.fel.cvut.cz/b221/_media/courses/pkr/pro-lecture-2021.pdf`.