

Polynomial matrices

approximation, interpolation, XGCD

Exercises for lecture 7

Recall the problem of *Vector rational interpolation* studied in last lecture:

Input:	<ul style="list-style-type: none"> • vector of polynomials $\mathbf{F} = [f_1 \ \cdots \ f_m]^\top \in \mathbb{K}[X]^{m \times 1}$; • points $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d) \in \mathbb{K}^d$; • shift $\mathbf{s} = (s_1, \dots, s_m) \in \mathbb{Z}^m$.
Output:	matrix $\mathbf{P} \in \mathbb{K}[X]^{m \times m}$ such that \mathbf{P} is \mathbf{s} -reduced and the rows of \mathbf{P} form a basis of the $\mathbb{K}[X]$ -module $\mathcal{I}(\boldsymbol{\alpha}, \mathbf{F})$.

Here, the $\mathbb{K}[X]$ -submodule of $\mathbb{K}[X]^{1 \times m}$ is defined as:

$$\mathcal{I}(\boldsymbol{\alpha}, \mathbf{F}) = \left\{ \mathbf{p} \in \mathbb{K}[X]^{1 \times m} \mid \mathbf{p}\mathbf{F} = 0 \bmod \prod_{1 \leq i \leq d} (X - \alpha_i) \right\}.$$

Recall that “ \mathbf{P} is a basis of $\mathcal{I}(\boldsymbol{\alpha}, \mathbf{F})$ ” means that each row of \mathbf{P} is in $\mathcal{I}(\boldsymbol{\alpha}, \mathbf{F})$, and that any $\mathbf{p} \in \mathcal{I}(\boldsymbol{\alpha}, \mathbf{F})$ is a $\mathbb{K}[X]$ -linear combination of the rows of \mathbf{P} .

Note that in most cases of application, the input satisfies $\deg(\mathbf{F}) < d$; if needed, this can be ensured via fast modular reduction.

Exercise 1. Shifted reduced forms.

Easy exercises for getting familiar with definitions. This will not be corrected in class; but you can use SageMath to verify your answers and you can ask about it during the exercise/revision session in November.

For each of the matrices below, and for each of the three shifts $\mathbf{s} = (0, 0, 0)$, $\mathbf{s} = (0, 5, 6)$, and $\mathbf{s} = (-3, -2, -2)$,

1. give the \mathbf{s} -leading matrix,
2. deduce whether the matrix is \mathbf{s} -reduced.

$$\mathbf{A} = \begin{bmatrix} 3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\ 5 & 5X^2 + 3X + 1 & 5X + 3 \\ 3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1 \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} X^6 + 6X^4 + X^3 + X + 4 & 0 & 0 \\ 5X^5 + 5X^4 + 6X^3 + 2X^2 + 6X + 3 & X & 0 \\ 3X^4 + 5X^3 + 4X^2 + 6X + 1 & 5 & 1 \end{bmatrix}$$

$$\mathbf{P} = \begin{bmatrix} X^3 + 5X^2 + 4X + 1 & 2X + 4 & 3X + 5 \\ 4X^2 + 1 & X^2 + 2X + 3 & X + 2 \\ 2X^2 + 3X + 2 & 4X & X^2 \end{bmatrix}$$

Exercise 2. Vector rational interpolation — some specific cases.

1. *Zero input matrix* [solved during lecture 6]. Assuming $\mathbf{F} = \mathbf{0}$, give a basis $\mathbf{P} \in \mathbb{K}[X]^{m \times m}$ of $\mathcal{I}(\alpha, \mathbf{F})$. Verify that this basis is \mathbf{s} -reduced for any \mathbf{s} .
2. *Hermite-Padé approximation*. Assuming $\alpha = (0, \dots, 0) \in \mathbb{K}^d$ as well as $f_1(0) \neq 0$, prove that the following matrix:

$$\mathbf{P} = \begin{bmatrix} X^d & & & \\ h_2 & 1 & & \\ \vdots & & \ddots & \\ h_{m-1} & & & 1 \end{bmatrix} \in \mathbb{K}[X]^{m \times m},$$

where $h_i = -f_i/f_1 \bmod X^d$, is the basis of $\mathcal{I}(\mathbf{0}, \mathbf{F})$ in Hermite form.

Note: a square, nonsingular matrix is in Hermite form if it is lower triangular, it has monic diagonal entries, and its entries below the diagonal have degree strictly less than the diagonal entry in the same column.

3. *Case $d = 1$* [solved during lecture 6]. For $\alpha = (\alpha) \in \mathbb{K}^1$ (i.e. $d = 1$), and assuming all entries of $\mathbf{F}(\alpha)$ are nonzero, give an \mathbf{s} -reduced basis of $\mathcal{I}(\alpha, \mathbf{F})$ for each of the shifts $\mathbf{s} = \mathbf{0}$, $\mathbf{s} = (2, \dots, 2, 0)$, and $\mathbf{s} = (3, 0, 2, \dots, 2)$. (We assume m sufficiently large for these shifts to make sense.)

Exercise 3. Using products of bases.

1. For $\alpha = \mathbf{0} \in \mathbb{K}^{2d}$ (Hermite-Padé approximation at order $2d$), assume the following, where $\beta = \mathbf{0} \in \mathbb{K}^d$ (note the d):
 - (a) \mathbf{P}_1 is a basis of $\mathcal{I}(\beta, \mathbf{F})$;
 - (b) $\mathbf{G} = (X^{-d}\mathbf{P}_1\mathbf{F}) \bmod X^d$;
 - (c) \mathbf{P}_2 is a basis of $\mathcal{I}(\beta, \mathbf{G})$.

Prove that $\mathbf{P}_2\mathbf{P}_1$ is a basis of $\mathcal{I}(\alpha, \mathbf{F})$.

2. [solved during lecture 6] Give an example of matrices $\mathbf{P}_1 \in \mathbb{K}[X]^{m \times m}$ and $\mathbf{P}_2 \in \mathbb{K}[X]^{m \times m}$ which are both reduced (for the shift $\mathbf{0}$) but such that $\mathbf{P}_2\mathbf{P}_1$ is not reduced.
3. 🍷 Prove that if two nonsingular matrices $\mathbf{P}_1, \mathbf{P}_2 \in \mathbb{K}[X]^{m \times m}$ are such that \mathbf{P}_1 is \mathbf{s} -reduced and \mathbf{P}_2 is \mathbf{t} -reduced, for $\mathbf{t} = \text{rdeg}_{\mathbf{s}}(\mathbf{P}_1)$, then the product $\mathbf{P}_2\mathbf{P}_1$ is \mathbf{s} -reduced.

Exercise 4. Fast GCD.

Let f and g be two univariate polynomials in $\mathbb{K}[X]$ of respective degrees m and n ; in what follows we assume $n > m > 0$. Let $h = \gcd(f, g)$, and let ℓ be the degree of h , which satisfies $\ell \leq m$. We also define $\bar{f} = f/h$ and $\bar{g} = g/h$, which are polynomials in $\mathbb{K}[X]$ of respective degrees $m - \ell$ and $n - \ell$.

1. Show that the row vector $[-\bar{g} \ \bar{f}] \in \mathbb{K}[X]^{1 \times 2}$ is a basis of the left kernel of $\mathbf{F} = \begin{bmatrix} f \\ g \end{bmatrix}$, that is, of the $\mathbb{K}[X]$ -module

$$\{[p \ q] \in \mathbb{K}[X]^{1 \times 2} \mid pf + qg = 0\}.$$

2. 🍷 Take arbitrary (not necessarily pairwise distinct) points $\alpha \in \mathbb{K}^{m+n+1}$. Prove that any (m, n) -reduced basis of $\mathcal{I}(\alpha, \mathbf{F})$ has the form

$$\mathbf{P} = \begin{bmatrix} * & * \\ -c\bar{g} & c\bar{f} \end{bmatrix} \quad \text{or} \quad \mathbf{P} = \begin{bmatrix} -c\bar{g} & c\bar{f} \\ * & * \end{bmatrix},$$

for some constant $c \in \mathbb{K} \setminus \{0\}$.

3. What was the complexity seen in class for computing such a basis \mathbf{P} ? From \mathbf{P} , how much does it cost to deduce the sought GCD $h(x)$?
4. Observe that if some nontrivial lower bound on ℓ is known, say $\ell \geq \delta$ for some known $\delta > 0$, one can actually take fewer than $n + m + 1$ points.

Remark: similar techniques can be used to retrieve not only the GCD of f and g , but solve the extended GCD. Recall that in this XGCD problem we further compute cofactors (u, v) such that $uf + vg = h$. It is a classical result that there exists a unique pair of polynomials (u, v) in $\mathbb{K}[X]^2$ such that

$$\begin{cases} uf + vg = h, \\ \deg(u) < n - \ell \quad \text{and} \quad \deg(v) < m - \ell. \end{cases}$$