polynomial matrices:
introduction, motivations, and basic algorithms

exercises and solutions

Algorithmes Efficaces en Calcul Formel
Master Parisien de Recherche en Informatique
18 November 2024

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m \times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg \det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m \times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m \times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg \det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m \times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$

the solution is based on Cramer's rule / Laplace formula:

$$\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})}\mathbf{C}^{\mathsf{T}}$$

where $\mathbf{C} \in \mathbb{K}[X]^{m \times m}$ is the matrix of cofactors of $\mathbf{A}$, that is, $(-1)^{i+j}c_{i,j}$ is the determinant of $\mathbf{A}$ after removing row i and column j

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m \times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg \det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m \times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$

1▸ Cramer's rule: $\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})}\mathbf{C}^\mathsf{T}$, with $c_{i,j} = (-1)^{i+j} \det(\mathbf{A}_{i,j})$
so $\mathbf{A}^{-1}\mathbf{V} = \frac{1}{\det(\mathbf{A})}\mathbf{C}^\mathsf{T}\mathbf{V}$, and one can take:

. $\Delta = \det(\mathbf{A})$
. $\mathbf{U} = \mathbf{C}^\mathsf{T}\mathbf{V}$ which has polynomial entries

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m\times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m\times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m\times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg\det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m\times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K}\setminus\{0\}$

2▸ $\deg\det(\mathbf{A}) = \deg\left(\sum_{\pi\in S_m} \pm \prod_i a_{i,\pi(i)}\right) \leqslant \max_{\pi\in S_m} \sum_i \deg(a_{i,\pi(i)})$

and the latter quantity is less than or equal to:

. $|\mathrm{rdeg}(\mathbf{A})|$ (sum of row degrees)
. $|\mathrm{cdeg}(\mathbf{A})|$ (sum of column degrees)
. $m\deg(\mathbf{A}) \leqslant m d_1$

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m \times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg \det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m \times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$

3▸ according to 1, one can take $\Delta = \det(\mathbf{A})$ and $\mathbf{U} = \mathbf{C}^\mathsf{T}\mathbf{V}$.

$\Rightarrow$ we have the above bounds for $\deg(\Delta) = \deg \det(\mathbf{A})$
$\Rightarrow$ using $c_{i,j} = (-1)^{i+j} \det(\mathbf{A}_{i,j})$, and similar bounds on $\det(\mathbf{A}_{i,j})$, we obtain $\deg(\mathbf{C}) \leqslant (m-1)d_1$, and $\deg(\mathbf{U}) \leqslant (m-1)d_1 + d_2$
(there are refined bounds when considering row degrees or column degrees ☕)

note: if there is a nonconstant divisor common to $\det(\mathbf{A})$ and all entries of $\mathbf{C}$, then we may take another Δ and $\mathbf{U}$ with smaller degrees

exercise: matrix equation $\mathbf{A}\mathbf{U} = \mathbf{V}$

let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leqslant d_1$

let $\mathbf{V} \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leqslant d_2$

1▸ show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[X]^{m \times k}$ and denominator a polynomial Δ in $\mathbb{K}[X]$

2▸ give an upper bound on $\deg \det(\mathbf{A})$

3▸ give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$

4▸ prove that $\mathbf{A}^{-1} \in \mathbb{K}[X]^{m \times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$

4▸ we prove both directions:
. from $\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})}\mathbf{C}^{\mathsf{T}}$, it follows that if $\det(\mathbf{A})$ is constant, then $\mathbf{A}^{-1}$ has polynomial entries
. from $\det(\mathbf{A})\det(\mathbf{A}^{-1}) = \det(\mathbf{A}\mathbf{A}^{-1}) = 1$, it follows that if $\mathbf{A}^{-1}$ has polynomial entries, then $\det(\mathbf{A}^{-1})$ is a polynomial and therefore $\det(\mathbf{A})$ must be constant

exercise: evaluation-interpolation based algorithms

1. adapting the evaluation-interpolation paradigm to matrices in $\mathbb{K}[X]^{m \times m}$,

▸ give an explicit **multiplication** algorithm

▸ give a **determinant** algorithm

▸ give an **inversion** algorithm ☕
computing the inverse over the fractions $\mathbb{K}(X)$

2. for each of these algorithms,

▸ give a required lower bound on the **cardinality of $\mathbb{K}$**

▸ state and prove an upper bound on the **complexity**

directions and hints:
▸ use known degree bounds on the output
▸ for inversion, assume you can do quasi-linear Cauchy interpolation

further perspective:
▸ could your complexity bounds take into account degree measures that refine the matrix degree such as the average row or column degree? ☕☕

exercise: evaluation-interpolation based algorithms

multiplication algorithm

given $\mathbf{A}$ and $\mathbf{B}$ in $\mathbb{K}[X]^{m\times m}$ of degree $\leqslant d$,
we know that $\mathbf{C} = \mathbf{A}\mathbf{B}$ has degree at most $2d$, so:

1. pick points: pairwise distinct $\alpha_1, \ldots, \alpha_{2d+1} \in \mathbb{K}$ — $\mathrm{Card}(\mathbb{K}) \geqslant 2d+1$
2. evaluate: $\mathbf{A}(\alpha_i)$ and $\mathbf{B}(\alpha_i)$, for $i = 1, \ldots, 2d+1$ — $O(m^2 \mathsf{M}(d)\log(d))$
3. multiply: $\mathbf{A}(\alpha_i)\mathbf{B}(\alpha_i)$, for $i = 1, \ldots, 2d+1$ — $O(m^\omega d)$
4. interpolate: find $\mathbf{C}$ in $\mathbb{K}[X]^{m\times m}$ of degree $\leqslant 2d$ such that
$\mathbf{C}(\alpha_i) = \mathbf{A}(\alpha_i)\mathbf{B}(\alpha_i)$, for $i = 1, \ldots, 2d+1$ — $O(m^2 \mathsf{M}(d)\log(d))$
5. return $\mathbf{C}$

excellent algorithm:
. linear in d in the term $m^\omega d$ (recall Cantor-Kaltofen: $m^\omega d \log(d)$)
. exponent ω of matrix multiplication
. the $m^2\mathsf{M}(d)\log(d)$ term can be improved via points in geometric sequence
. downside: restriction on $\mathbb{K}$ (large degrees + small finite fields do arise)

exercise: evaluation-interpolation based algorithms

determinant algorithm

given $\mathbf{A}$ in $\mathbb{K}[X]^{m \times m}$ of degree $\leqslant d$,
we know that $\Delta = \det(\mathbf{A})$ has degree at most md, so:

1. pick points: pairwise distinct $\alpha_1, \ldots, \alpha_{md+1} \in \mathbb{K}$ — $\mathrm{Card}(\mathbb{K}) \geqslant md + 1$
2. evaluate: $\mathbf{A}(\alpha_i)$ for $i = 1, \ldots, md + 1$ — $O(m^3 M(d) \log(d))$
3. determinant: $\beta_i = \det(\mathbf{A}(\alpha_i))$, for $i = 1, \ldots, md + 1$ — $O(m^{\omega+1} d)$
4. interpolate: find Δ in $\mathbb{K}[X]$ of degree $\leqslant md$ such that $\Delta(\alpha_i) = \beta_i$, for $i = 1, \ldots, md + 1$ — $O(M(md) \log(md))$
5. return Δ

- quasi-linear in degree d: fast for large d, small m
- exponent > 3 on matrix dimension m: slow for large m
- best known today: $\tilde{O}(m^\omega d)$

exercise: evaluation-interpolation based algorithms

inversion algorithm

given $\mathbf{A}$ in $\mathbb{K}[X]^{m\times m}$ of degree $\leqslant d$,
we know that $\mathbf{C} = \mathbf{A}^{-1} = \frac{1}{\Delta}\mathbf{U}$ with
$\deg(\Delta) \leqslant md$ and $\deg(\mathbf{U}) \leqslant (m-1)d$, so:

0. set $n = (2m-1)d + 1$ — $n = \Theta(md)$
1. pick points: pairwise distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ — $\mathrm{Card}(\mathbb{K}) \geqslant (2m-1)d+1$
2. evaluate: $\mathbf{A}(\alpha_i)$, for $i = 1, \ldots, n$ — $O(m^3 M(d)\log(d))$
3. invert: $\mathbf{A}(\alpha_i)^{-1}$, for $i = 1, \ldots, n$ — $O(m^{\omega+1}d)$
4. interpolate: using Cauchy interpolation find $\mathbf{C}$ in $\mathbb{K}(X)^{m\times m}$ with all numerators of degree $\leqslant (m-1)d$ and all denominators of degree $\leqslant md$ such that $\mathbf{C}(\alpha_i) = \mathbf{A}(\alpha_i)^{-1}$, for $i = 1, \ldots, n$ — $O(m^2 M(md)\log(md))$
5. return $\mathbf{C}$

- quasi-linear in degree d: fast for large d, small m
- exponent > 3 on dimension m but recall size of $\mathbf{A}^{-1}$ is typically $\Theta(m^3 d)$
- best known today: $\tilde{O}(m^3 d)$, and even $\tilde{O}(m^\omega d)$ for factorized form
- note: one could compute $\det(\mathbf{A})$ to avoid Cauchy interpolation