polynomial matrices:
introduction, motivations, and basic algorithms

exercises and solutions

Algorithmes Efficaces en Calcul Formel
Master Parisien de Recherche en Informatique
4 November 2021
let $A \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leq d_1$

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

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

2. give an upper bound on $\deg \det(A)$

3. give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $U$

4. prove that $A^{-1} \in \mathbb{K}[X]^{m \times m} \iff \det(A) \in \mathbb{K} \setminus \{0\}$
let $A \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leq d_1$

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

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

2. give an upper bound on $\deg \det(A)$

3. give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $U$

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

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

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

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

let $A \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leq d_1$
let $V \in \mathbb{K}[X]^{m \times k}$ with all entries of degree $\leq d_2$

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

2. give an upper bound on $\text{deg} \det(A)$

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

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

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

. $\Delta = \det(A)$
. $U = C^T V$ which has polynomial entries
let $A \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leq d_1$

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

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

2. Give an upper bound on $\deg \det(A)$.

3. Give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $U$.

4. Prove that $A^{-1} \in \mathbb{K}[X]^{m \times m} \iff \det(A) \in \mathbb{K} \setminus \{0\}$

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

and the latter quantity is less than or equal to:

- $|\text{rdeg}(A)|$ (sum of row degrees)
- $|\text{cdeg}(A)|$ (sum of column degrees)
- $m \deg(A) \leq m d_1$
let $A \in \mathbb{K}[X]^{m \times m}$ be nonsingular with all entries of degree $\leq d_1$

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

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

2. give an upper bound on $\deg \det(A)$

3. give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $U$

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

according to 1, one can take $\Delta = \det(A)$ and $U = C^T V$.

$\implies$ we have the above bounds for $\deg(\Delta) = \deg \det(A)$

$\implies$ using $c_{i,j} = (-1)^{i+j} \det(A_{i,j})$, and similar bounds on $\det(A_{i,j})$, we obtain $\deg(C) \leq (m-1)d_1$, and $\deg(U) \leq (m-1)d_1 + d_2$

(there are refined bounds when considering row degrees or column degrees)

note: if there is a nonconstant divisor common to $\det(A)$ and all entries of $C$, then we may take another $\Delta$ and $U$ with smaller degrees
exercise: matrix equation $AU = V$

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

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

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

2. give an upper bound on $\deg \det(A)$

3. give an upper bound on $\deg(\Delta)$ and on the degrees of entries of $U$

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

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

1. adapting the evaluation-interpolation paradigm to matrices in \( K[X]^{m \times m} \),
   - give an explicit **multiplication** algorithm
   - give a **determinant** algorithm
   - give an **inversion** algorithm 🍌

computing the inverse over the fractions \( K(X) \)

2. for each of these algorithms,
   - give a required lower bound on the **cardinality of** \( K \)
   - 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**? 🍌フル
exercise: evaluation-interpolation based algorithms

**multiplication algorithm**

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

1. **pick points**: pairwise distinct $\alpha_1, \ldots, \alpha_{2d+1} \in \mathbb{K}$
   
2. **evaluate**: $A(\alpha_i)$ and $B(\alpha_i)$, for $i = 1, \ldots, 2d + 1$
   
3. **multiply**: $A(\alpha_i)B(\alpha_i)$, for $i = 1, \ldots, 2d + 1$

   \[ O(m^2 \Omega(d) \log(d)) \]

4. **interpolate**: find $C$ in $\mathbb{K}[X]^{m \times m}$ of degree $\leq 2d$ such that $C(\alpha_i) = A(\alpha_i)B(\alpha_i)$, for $i = 1, \ldots, 2d + 1$

   \[ O(m^2 \Omega(d) \log(d)) \]

5. **return** $C$

**excellent algorithm:**

- linear in $d$ in the term $m^\omega d$ (recall Cantor-Kaltofen: $m^\omega d \log(d)$)
- exponent $\omega$ of matrix multiplication
- the $m^2 \Omega(d) \log(d)$ term can be improved via points in geometric sequence
- downside: restriction on $\mathbb{K}$ (large degrees + small finite fields does happen)
given \( A \) in \( \mathbb{K}[X]^{m \times m} \) of degree \( \leq d \), we know that \( \Delta = \det(A) \) has degree at most \( md \), so:

1. **pick points**: pairwise distinct \( \alpha_1, \ldots, \alpha_{md+1} \in \mathbb{K} \)

2. **evaluate**: \( A(\alpha_i) \) for \( i = 1, \ldots, md + 1 \)

3. **determinant**: \( \beta_i = \det(A(\alpha_i)) \), for \( i = 1, \ldots, md + 1 \)

4. **interpolate**: find \( \Delta \) in \( \mathbb{K}[X] \) of degree \( \leq md \) such that \( \Delta(\alpha_i) = \beta_i \), for \( i = 1, \ldots, md + 1 \)

5. return \( \Delta \)

- quasi-linear in degree \( d \): fast for large \( d \), small \( m \)
- exponent \( > 3 \) on matrix dimension \( m \): slow for large \( m \)
- best known today: \( O^\sim(m^\omega d) \)
exercise: evaluation-interpolation based algorithms

inversion algorithm

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

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

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