polynomial matrices: introduction, motivations, and basic algorithms
outline

introduction

matrices? polynomials?

polynomial matrices

reduced forms
introduction
- definitions and algebraic properties
- examples you already know
- three flagship applications

matrices? polynomials?

polynomial matrices

reduced forms
working over a base field \( K \)
\( K = \) finite field \( \mathbb{F}_q \), extension \( \mathbb{F}_q[X]/\langle f(X) \rangle \), rational numbers \( \mathbb{Q} \), …

considering polynomials in one indeterminate \( X \)
\( K[X] \) is a principal ideal domain (what does that mean?)

in \( K[X] \), many operations cost \( O(M(d)) \) or \( O(M(d) \log(d)) \) field ops.
where \( d \mapsto M(d) \) is a cost function for polynomial multiplication in degree \( d \)
polynomial matrices – introduction

definitions and algebraic properties

- working over a base field $\mathbb{K}$
  $\mathbb{K} = \text{finite field } \mathbb{F}_q$, extension $\mathbb{F}_q[X]/\langle f(X) \rangle$, rational numbers $\mathbb{Q}$, ...

- considering polynomials in one indeterminate $X$
  $\mathbb{K}[X]$ is a principal ideal domain (what does that mean?)

- in $\mathbb{K}[X]$, many operations cost $O(M(d))$ or $O(M(d) \log(d))$ field ops.
  where $d \mapsto M(d)$ is a cost function for polynomial multiplication in degree $d$

- addition $f + g$, multiplication $f \ast g$

- division with remainder $f = qg + r$

- truncated inverse $f^{-1} \mod X^d$

- extended GCD $uf + vg = \gcd(f, g)$

- multipoint eval. $f \mapsto f(x_1), \ldots, f(x_d)$

- interpolation $f(x_1), \ldots, f(x_d) \mapsto f$

- Padé approximation $f = \frac{p}{q} \mod X^d$

- minpoly of linearly recurrent sequence
polynomial matrices – introduction

definitions and algebraic properties

Working over a base field $\mathbb{K}$
$\mathbb{K} = \text{finite field } \mathbb{F}_q$, extension $\mathbb{F}_q[X]/\langle f(X) \rangle$, rational numbers $\mathbb{Q}$, ...

Considering polynomials in one indeterminate $X$
$\mathbb{K}[X]$ is a principal ideal domain (what does that mean?)

In $\mathbb{K}[X]$, many operations cost $O(M(d))$ or $O(M(d) \log(d))$ field ops.
where $d \mapsto M(d)$ is a cost function for polynomial multiplication in degree $d$

- addition $f + g$, multiplication $f \times g$
- division with remainder $f = qg + r$
- truncated inverse $f^{-1} \mod X^d$
- extended GCD $uf + vg = \gcd(f, g)$
- multipoint eval. $f \mapsto f(x_1), \ldots, f(x_d)$
- interpolation $f(x_1), \ldots, f(x_d) \mapsto f$
- Padé approximation $f = \frac{p}{q} \mod X^d$
- minpoly of linearly recurrent sequence
polynomial matrices – introduction

definitions and algebraic properties

\[ K[X]^{m \times n} = \text{set of } m \times n \text{ matrices over } K[X] \]

called polynomial matrices in what follows

\[
\begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3 \\
3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1
\end{bmatrix} \in K[X]^{3 \times 3}
\]
polynomial matrices – introduction

definitions and algebraic properties

\[ \mathbb{K}[X]^{m \times n} = \text{set of } m \times n \text{ matrices over } \mathbb{K}[X] \]

called polynomial matrices in what follows

\[
\begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3 \\
3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1
\end{bmatrix} \in \mathbb{K}[X]^{3 \times 3}
\]

▶ structure: matrices over \( \mathbb{K}[X] \) \( \longleftrightarrow \) “free” modules over \( \mathbb{K}[X] \)
similarly to: matrices over \( \mathbb{K} \) \( \longleftrightarrow \) vector spaces over \( \mathbb{K} \)

▶ basic operations: addition and multiplication
defined as usual (multiplication requires compatible dimensions)

▶ \( \mathbb{K}[X] \) is not a field
what does this change? what operations are allowed / not allowed?
polynomial matrices – introduction

definitions and algebraic properties

\[ \mathbb{K}[X]^{m \times n} = \text{set of } m \times n \text{ matrices over } \mathbb{K}[X] \]

called polynomial matrices in what follows

\[
\begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3 \\
3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1
\end{bmatrix} \in \mathbb{K}[X]^{3 \times 3}
\]

▶ structure: matrices over \( \mathbb{K}[X] \) \( \leftrightarrow \) “free” modules over \( \mathbb{K}[X] \)
similarly to: matrices over \( \mathbb{K} \) \( \leftrightarrow \) vector spaces over \( \mathbb{K} \)

▶ basic operations: addition and multiplication
defined as usual (multiplication requires compatible dimensions)

▶ \( \mathbb{K}[X] \) is not a field
what does this change? what operations are allowed / not allowed?

⇝ algorithms may work in \( \mathbb{K}(X)^{m \times n} \), but be careful with “degree explosion”!
polynomial matrices – introduction

examples you already know
polynomial matrices – introduction

examples you already know

large matrices with small degrees:
characteristic polynomial \( \det(XI_m - M) \in \mathbb{K}[X] \) of a matrix \( M \in \mathbb{K}^{m \times m} \)
\( \leadsto \) determinant of polynomial matrix \( XI_m - M \in \mathbb{K}[X]^{m \times m} \)

- fastest known algorithm uses this viewpoint [N.-Pernet, 2021]
- gradually transforms \( XI_m - M \) to smaller matrices with larger degrees
polynomial matrices – introduction

examples you already know

large matrices with small degrees:

characteristic polynomial $\det(\mathbf{X} \mathbf{I}_m - \mathbf{M}) \in \mathbb{K}[\mathbf{X}]$ of a matrix $\mathbf{M} \in \mathbb{K}^{m \times m}$

$\leadsto$ determinant of polynomial matrix $\mathbf{X} \mathbf{I}_m - \mathbf{M} \in \mathbb{K}[\mathbf{X}]^{m \times m}$

- fastest known algorithm uses this viewpoint [N.-Pernet, 2021]
- gradually transforms $\mathbf{X} \mathbf{I}_m - \mathbf{M}$ to smaller matrices with larger degrees

small matrices with large degree:

extended GCD $u f + v g = \gcd(f, g)$ for polynomials $f, g \in \mathbb{K}[\mathbf{X}]_{\leq d}$

$\leadsto$ corresponds to a polynomial matrix transformation

$$
\begin{bmatrix}
u & v \\
u' & v'
\end{bmatrix}
\begin{bmatrix}f \\
g
\end{bmatrix}
= 
\begin{bmatrix}
gcd(f, g) \\
0
\end{bmatrix}
$$

with the leftmost (polynomial) matrix of determinant in $\mathbb{K} \setminus \{0\}$

- fastest known “half-gcd” algorithms use this viewpoint

[Knuth, 1970] [Schönhage, 1971] [Brent-Gustavson-Yun, 1980]
polynomial matrices – introduction

three flagship applications

1. operations on sparse matrices
   ▶ solving sparse linear systems over $\mathbb{K}$
   ▶ computing the minimal polynomial / Frobenius form
   ▶ introducing parallelism in these computations

[Wiedemann 1986]
[Coppersmith 1993]
[Villard 1997]

example of sparse matrix in $\mathbb{K}^{m \times m}$

typical case: $O(m)$ nonzero entries

uses polynomial matrix generator
of linearly recurrent matrix sequence
2. operations on structured matrices
▶ matrix-vector multiplication
▶ linear system solving
▶ nullspace computation

[Kailath-Kung-Morg 1979]
[Bostan et al. 2017]

example of Hankel matrix
⇝ block-Hankel matrices
⇝ Hankel-like matrices

uses polynomial matrix multiplication and matrix-Padé approximation / matrix-GCD
3. bivariate interpolation and multipoint evaluation

problem: given points \((\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)\) in \(K^2\),

- given \(p(x, y)\), compute \(p(\alpha_i, \beta_i)\) for \(1 \leq i \leq n\)
- find \(p(x, y)\) of small degree such that \(p(\alpha_i, \beta_i) = 0\)

\[\text{[Nüsken-Ziegler 2004]}\]
\[\text{[Neiger 2016]}\]

bivariate interpolation = main step in Reed-Solomon list-decoding (univariate interpolation with errors)

\[\text{[Guruswami-Sudan 1999]}\]

uses polynomial matrix multiplication and matrix rational reconstruction / algebraic approximants
Outline

- Introduction
  - Definitions and algebraic properties
  - Examples you already know
  - Three flagship applications

- Matrices? Polynomials?
  - Using matrix arithmetic
  - Using polynomial arithmetic
  - Limitations of these viewpoints

- Polynomial matrices

- Reduced forms
the matrix and the polynomial viewpoints

using matrix arithmetic

matrices in $\mathbb{K}[X]^{m\times n}$ are also in $\mathbb{K}(X)^{m\times n}$

(and $\mathbb{K}(X)$ is a field)

$\Rightarrow$ usual definition of addition, multiplication, determinant
these do not involve fractions anyway(?)

$\Rightarrow$ usual definition of inverse
but with inverse over $\mathbb{K}(X)$

$\Rightarrow$ usual definition of rank
... which one, by the way?
the matrix and the polynomial viewpoints

using matrix arithmetic

matrices in $\mathbb{K}[X]^{m \times n}$ are also in $\mathbb{K}(X)^{m \times n}$

(and $\mathbb{K}(X)$ is a field)

this point of view is hardly usable for algorithms:
it easily yields “garbage” cost bounds
e.g. addition in $\mathbb{K}[X]^{m \times n}$ costs $mn$ additions... in $\mathbb{K}(X)$

▶ what is the cost of naive addition in $\mathbb{K}[X]^{m \times m}$?
▶ what is the cost of naive multiplication in $\mathbb{K}[X]^{m \times m}$?
▶ let $2 < \omega < 3$ be such that we can multiply two $m \times m$ matrices
  over a commutative ring in $O(m^\omega)$ ring operations: what do you
  deduce about the cost of multiplying two matrices in $\mathbb{K}[X]^{m \times m}$?
the matrix and the polynomial viewpoints
using matrix arithmetic

**matrices in** $\mathbb{K}[X]^{m \times n}$ **are also in** $\mathbb{K}(X)^{m \times n}$
(and $\mathbb{K}(X)$ is a field)
	his point of view is hardly usable for algorithms:
it easily yields “garbage” cost bounds
e.g. addition in $\mathbb{K}[X]^{m \times n}$ costs $mn$ additions... in $\mathbb{K}(X)$

▶ what is the cost of naive addition in $\mathbb{K}[X]^{m \times m}$?
▶ what is the cost of naive multiplication in $\mathbb{K}[X]^{m \times m}$?
▶ let $2 < \omega < 3$ be such that we can multiply two $m \times m$ matrices
over a commutative ring in $O(m^\omega)$ ring operations: what do you
deduce about the cost of multiplying two matrices in $\mathbb{K}[X]^{m \times m}$?

for algorithms&complexity, considering the degrees of entries is essential
The matrix and the polynomial viewpoints

Using matrix arithmetic

Matrices in $\mathbb{K}[X]^{m \times n}$ are also in $\mathbb{K}(X)^{m \times n}$
(and $\mathbb{K}(X)$ is a field)

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 $\leq d_2$

- 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 $\mathbb{K}[X]$

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

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

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

Matrices with determinant in $\mathbb{K} \setminus \{0\}$ are called unimodular
the matrix and the polynomial viewpoints

using polynomial arithmetic

$\mathbb{K}[X]^{m \times n}$ is isomorphic to $\mathbb{K}^{m \times n}[X]$ 
(as $\mathbb{K}[X]$-modules)

\[
\begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3 \\
3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1
\end{bmatrix}
= \begin{bmatrix}
4 & 1 & 3 \\
5 & 1 & 3 \\
3 & 5 & 1
\end{bmatrix}
+ \begin{bmatrix}
3 & 4 & 0 \\
0 & 3 & 5 \\
5 & 6 & 2
\end{bmatrix}X
+ \begin{bmatrix}
0 & 0 & 4 \\
0 & 5 & 0 \\
1 & 0 & 0
\end{bmatrix}X^2
+ \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
3 & 0 & 0
\end{bmatrix}X^3
\]
the matrix and the polynomial viewpoints

using polynomial arithmetic

\[ K[X]^{m \times n} \text{ is isomorphic to } K^{m \times n}[X] \]
(as \( K[X] \)-modules)

- natural notion of **degree** of a polynomial matrix
- **addition** of \( A, B \in K[X]^{m \times n} \) is in \( O(mnd) \) operations in \( K \)
  where \( d = \min(\deg(A), \deg(B)) \)
- **some** other polynomial operations available:
  truncation \( A \ \text{rem} \ X^N \), shift \( X^d A \), evaluation \( A(\alpha) \)

what is the complexity of evaluation?
what about Lagrange interpolation?
the matrix and the polynomial viewpoints

using polynomial arithmetic

\( \mathbb{K}[X]^{m \times n} \text{ is isomorphic to } \mathbb{K}^{m \times n}[X] \)

(as \( \mathbb{K}[X] \)-modules)

when \( m = n \), \( \mathbb{K}^{m \times m} \) is a (non-commutative) ring

- multiplication in \( \mathbb{K}[X]^{m \times m} \) seen as a product of polynomials complexity?

- truncated inversion via power series & Newton iteration condition for \( A \) to be invertible as a power series? complexity?

- fast Euclidean division with remainder does this make any sense?
On fast multiplication
of polynomials over arbitrary algebras

David G. Cantor\textsuperscript{1} and Erich Kaltofen\textsuperscript{2} *

\textsuperscript{1} Department of Mathematics, University of California, Los Angeles, CA 90024-1555, USA
\textsuperscript{2} Department of Computer Science, Rensselaer Polytechnic Institute, Troy, NY 12180-3590, USA

Received January 22, 1988 / May 10, 1991

1 Introduction

In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an arbitrary, not necessarily commutative, not necessarily associative, algebra $\mathcal{A}$. Our main result is an algorithm to multiply polynomials of degree $<n$ in $O(n \log n)$ algebra multiplications and $O(n \log n \log \log n)$ algebra additions/subtractions (we count a subtraction as an addition). The constant implied by the $"O"$ does not depend upon the algebra $\mathcal{A}$. The parallel complexity of our algorithm, i.e., the depth of the corresponding arithmetic circuit, is
On fast multiplication of polynomials over arbitrary algebras

David G. Cantor¹ and Erich Kaltofen ²

¹ Department of Mathematics, University of California, Los Angeles, CA 90024-1555, USA
² Department of Computer Science, Rensselaer Polytechnic Institute, Troy, NY 12180-3590, USA

Received January 22, 1988 / May 10, 1991

1 Introduction

In this paper we generalize the well-known Schönhage-Strassen algorithm for multiplying large integers to an algorithm for multiplying polynomials with coefficients from an arbitrary, not necessarily commutative, not necessarily associative, algebra $\mathcal{A}$. Our main result is an algorithm to multiply polynomials of degree $<n$ in $O(n \log n)$ algebra multiplications and $O(n \log n \log \log n)$ algebra additions/subtractions (we count a subtraction as an addition). The constant implied by the “$O$” does not depend upon the algebra $\mathcal{A}$. The parallel complexity of our algorithm, i.e., the depth of the corresponding arithmetic circuit, is...
the matrix and the polynomial viewpoints

using polynomial arithmetic

truncated inversion – reminder from October 11 & from AECF

Details on power series inversion

Algorithm (series inversion by Newton iteration)

Input Truncation $T$ to order $N \in \mathbb{N}_{>0}$ of a series $F \in \mathbb{K}[[x]]$ with $F(0) \neq 0$.

Output The truncation $S$ to order $N$ of the inverse series $F^{-1}$.

If $N = 1$, return $T(0)^{-1}$. Otherwise:
1. Recursively compute the truncation $G$ to order $\lceil N/2 \rceil$ of $T^{-1}$.
2. Return $S := G + \text{rem}((1 - GT)G, x^N)$.

Correctness proof Assume $T^{-1} = G + O(x^{\lceil N/2 \rceil})$ by induction. By Lemma,

$\mathcal{N}(G) - T^{-1} = O(x^{2\lceil N/2 \rceil}) = O(x^N)$.

Write $F = T + O(x^N) = T(1 + O(x^N))$ to observe $F^{-1} = T^{-1} + O(x^N)$. Then,

$F^{-1} - S = (F^{-1} - T^{-1}) + (T^{-1} - \mathcal{N}(G)) + (\mathcal{N}(G) - S) = O(x^N)$. 

the matrix and the polynomial viewpoints

using polynomial arithmetic

truncated inversion – reminder from October 11 & from AECF

<table>
<thead>
<tr>
<th><strong>Entrée</strong></th>
<th>Un entier $N &gt; 0$, $F \mod X^N$ une série tronquée.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sortie</strong></td>
<td>$F^{-1} \mod X^N$.</td>
</tr>
<tr>
<td></td>
<td>Si $N = 1$, alors renvoyer $f_0^{-1}$, où $f_0 = F(0)$.</td>
</tr>
<tr>
<td></td>
<td>Sinon :</td>
</tr>
<tr>
<td></td>
<td>1. Calculer récursivement l'inverse $G$ de $F \mod X^{[N/2]}$.</td>
</tr>
<tr>
<td></td>
<td>2. Renvoyer $G + (1 - GF)G \mod X^N$.</td>
</tr>
</tbody>
</table>

Algorithme 3.2 – Inverse de série par itération de Newton.

Convergence quadratique pour l'inverse d'une série formelle

**Lemme 3.2** Soient $A$ un anneau non nécessairement commutatif, $F \in A[[X]]$ une série formelle de terme constant inversible et $G$ une série telle que $G - F^{-1} = O(X^n)$ ($n \geq 1$). Alors la série

$$N(G) = G + (1 - GF)G$$

(3.2)

vérifie $N(G) - F^{-1} = O(X^{2n})$.

**Démonstration.** Par hypothèse, on peut définir $H \in A[[X]]$ par $1 - GF = X^nH$. Il suffit alors de récrire $F = G^{-1}(1 - X^nH)$ et d'inverser :

$$F^{-1} = (1 + X^nH + O(X^{2n}))G = G + X^nHG + O(X^{2n})G = N(G) + O(X^{2n})$$

Algorithme

**Lemme 3.3** L'Algorithme 3.2 d'inversion est correct.

**Démonstration.** La preuve est une récurrence sur les entiers. Pour $N = 1$ la propriété est claire. Pour $N \geq 2$, si la propriété est vraie jusqu'à l'ordre $N - 1$, alors elle l'est pour $N$.
consider a (square) polynomial matrix $A \in \mathbb{K}[X]^{m \times m}$

- $A$ is invertible as a power series
  $\iff$ its constant term $A(0) \in \mathbb{K}^{m \times m}$ is invertible

- if $A$ is invertible as a power series, computing its truncated inverse $A^{-1} \mod X^N$ costs

$$O(MM(m, N)) \in O(m^\omega N \log(N) + m^2 N \log(N) \log \log(N))$$

operations in $\mathbb{K}$
Euclidean division for polynomials

[Strassen, 1973]

**Pb:** Given $F, G \in \mathbb{K}[x]_{\leq N}$, compute $(Q, R)$ in Euclidean division $F = QG + R$

**Naive algorithm:** $O(N^2)$

**Idea:** look at $F = QG + R$ from infinity: $Q \sim_{+\infty} F/G$

Let $N = \deg(F)$ and $n = \deg(G)$. Then $\deg(Q) = N - n$, $\deg(R) < n$ and

$$F(1/x)x^N = G(1/x)x^n \cdot Q(1/x)x^{N-n} + R(1/x)x^\deg(R) \cdot x^{N-\deg(R)}$$

**Algorithm:**

- Compute $\text{rev}(Q) = \text{rev}(F)/\text{rev}(G) \mod x^{N-n+1}$ $O(M(N))$
- Recover $Q$ $O(1)$
- Deduce $R = F - QG$ $O(M(N))$
the matrix and the polynomial viewpoints

using polynomial arithmetic

**division with remainder**

**problem:**
given \( A, B \in K^{m \times m}[X] \),
compute \( Q, R \in K^{m \times m}[X] \) such that
\[
A = BQ + R \quad \text{and} \quad \deg(R) < \deg(B)
\]

... are we not missing an assumption?
the matrix and the polynomial viewpoints

using polynomial arithmetic

division with remainder

problem:
given \( A, B \in K^{m \times m}[X] \),
compute \( Q, R \in K^{m \times m}[X] \) such that
\[
A = BQ + R \quad \text{and} \quad \deg(R) < \deg(B)
\]

... are we not missing an assumption?

rule 1: dividing by zero is generally a bad idea
rule 2: if you think you need to divide by zero, refer to rule 1
rule 3: neglecting to check that something is not zero does not make it nonzero
etc. etc.
the matrix and the polynomial viewpoints

using polynomial arithmetic

division with remainder

problem:
given \( A, B \in \mathbb{K}^{m \times m}[X] \),
compute \( Q, R \in \mathbb{K}^{m \times m}[X] \) such that
\[
A = BQ + R \quad \text{and} \quad \deg(R) < \deg(B)
\]

... are we not missing an assumption?

for a polynomial \( p \in \mathcal{A}[X] \), over some ring \( \mathcal{A} \), division by \( p \) is feasible

- if \( p \) is monic (leading coefficient 1\( _\mathcal{A} \))
- and more generally if the leading coefficient of \( p \) is invertible in \( \mathcal{A} \)

assumption: the leading coefficient of \( B \) is invertible in \( \mathbb{K}^{m \times m} \)

recall \( B = B_0 + B_1X + \cdots + B_dX^d \) with \( B_i \in \mathbb{K}^{m \times m} \)
the matrix and the polynomial viewpoints

using polynomial arithmetic

division with remainder

problem:
given $A, B \in K^{m \times m}[X]$ with $\text{lc}(B)$ invertible,
compute $Q, R \in K^{m \times m}[X]$ such that
$A = BQ + R$ and $\deg(R) < \deg(B)$

example:
let $B = XI_m - M$ for some $M \in K^{m \times m}$
give a description of $R = A \text{ rem } B$
the matrix and the polynomial viewpoints

using polynomial arithmetic

division with remainder

problem:
given $A, B \in \mathbb{K}^{m \times m}[X]$ with $\text{lc}(B)$ invertible,
compute $Q, R \in \mathbb{K}^{m \times m}[X]$ such that
$A = BQ + R$ and $\deg(R) < \deg(B)$

device:

example:

let $B = XI_m - M$ for some $M \in \mathbb{K}^{m \times m}$
give a description of $R = A \text{ rem } B$

from $X^kI_m - M^k = (XI_m - M) \sum_{1 \leq i \leq k-1} M^i X^{k-i}$
we get $X^kI_m = M^k \text{ mod } B$, with $\deg(M^k) < 1$

then by linearity
$R = A \text{ rem } B = (A_0 + A_1X + A_2X^2 + \cdots + A_dX^d) \text{ rem } B$
$= A_0 + MA_1 + M^2A_2 + \cdots + M^dA_d$
the matrix and the polynomial viewpoints

using polynomial arithmetic

division with remainder

problem:
given $A, B \in \mathbb{K}^{m \times m}[X]$ with $\text{lc}(B)$ invertible,
compute $Q, R \in \mathbb{K}^{m \times m}[X]$ such that

$$A = BQ + R \quad \text{and} \quad \deg(R) < \deg(B)$$

- under this assumption, the usual fast Euclidean algorithm works
- recall:
  1. reverse the equation,
  2. compute quotient by truncated inverse,
  3. deduce remainder

- complexity is $O(\text{MM}(m, d))$ for $d = \max(\deg(A), \deg(B))$
the matrix and the polynomial viewpoints

limitations of these viewpoints

applying usual linear algebra algorithms to polynomial matrices:
▶ helps to understand some algebraic aspects
▶ leads too easily to computing in the fractions
▶ gives nonsensical complexity bounds

seeing polynomial matrices as polynomials with matrix coefficients
▶ allows direct use of some algorithms from polynomial arithmetic
▶ provides better control of the degree during computations
▶ remains restrictive and inefficient in many cases

▶ example for restrictive:
in division with remainder, the assumption “lc(B) invertible” can be relaxed into “B reduced” (and even to “B nonsingular”)

▶ example for inefficient:
for a matrix of degree d with many entries of degree ≪ d, we want to take the individual degrees into account
### outline

- **introduction**
  - definitions and algebraic properties
  - examples you already know
  - three flagship applications

- **matrices? polynomials?**
  - using matrix arithmetic
  - using polynomial arithmetic
  - limitations of these viewpoints

- **polynomial matrices**

- **reduced forms**
introduction

 matrices? polynomials?

 polynomial matrices

 reduced forms

- definitions and algebraic properties
- examples you already know
- three flagship applications

- using matrix arithmetic
- using polynomial arithmetic
- limitations of these viewpoints

- size and row/column degrees
- evaluation-interpolation-based algorithms
- partial linearization techniques
size of a polynomial matrix = number of coefficients from $K$ needed for its dense representation

for $A = (a_{i,j}) \in K[X]^{m \times n}$,

$$\text{size}(A) = \sum_{i,j} \text{size}(a_{i,j}) = \sum_{i,j} 1 + \max(0, \deg(a_{i,j}))$$
size and row/column degrees

**size** of a polynomial matrix = number of coefficients from $\mathbb{K}$ needed for its dense representation

For $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$,

$$\text{size}(A) = \sum_{i,j} \text{size}(a_{i,j}) = \sum_{i,j} 1 + \max(0, \deg(a_{i,j}))$$

Recall $\deg(AB) \leq \deg(A) + \deg(B)$,

however:

**in general the size is not compatible with matrix products**
mixing matrix and polynomial tools

size and row/column degrees

size of a polynomial matrix = number of coefficients from $\mathbb{K}$ needed for its dense representation

for $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$,

\[
\text{size}(A) = \sum_{i,j} \text{size}(a_{i,j}) = \sum_{i,j} 1 + \max(0, \deg(a_{i,j}))
\]

recall $\deg(AB) \leq \deg(A) + \deg(B)$,

however:

in general the size is not compatible with matrix products

considering the degree matrices:

\[
\begin{pmatrix}
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10
\end{pmatrix}
\begin{pmatrix}
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50
\end{pmatrix}
= 
\begin{pmatrix}
150 & 150 & 150 & 150 \\
150 & 150 & 150 & 150 \\
150 & 150 & 150 & 150 \\
150 & 150 & 150 & 150
\end{pmatrix}
\]

sizes of these three matrices?
mixing matrix and polynomial tools

size and row/column degrees

**size** of a polynomial matrix = number of coefficients from $\mathbb{K}$ needed for its dense representation

for $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$,

$\text{size}(A) = \sum_{i,j} \text{size}(a_{i,j}) = \sum_{i,j} 1 + \max(0, \deg(a_{i,j}))$

recall $\deg(AB) \leq \deg(A) + \deg(B)$,
however:

in general the size is not compatible with matrix products

but it may be, in some particular cases
mixing matrix and polynomial tools

size and row/column degrees

**size** of a polynomial matrix = number of coefficients from \( \mathbb{K} \) needed for its dense representation

For \( A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n} \),

\[
\text{size}(A) = \sum_{i,j} \text{size}(a_{i,j}) = \sum_{i,j} 1 + \max(0, \deg(a_{i,j}))
\]

Recall \( \deg(AB) \leq \deg(A) + \deg(B) \), however:

in general the size is not compatible with matrix products

but it may be, in some particular cases

\[
\begin{pmatrix}
100 & 100 & 100 & 100 \\
50 & 50 & 50 & 50 \\
40 & 40 & 40 & 40 \\
10 & 10 & 10 & 10
\end{pmatrix}
\begin{pmatrix}
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50 \\
50 & 50 & 50 & 50
\end{pmatrix}
= \begin{pmatrix}
150 & 150 & 150 & 150 \\
100 & 100 & 100 & 100 \\
90 & 90 & 90 & 90 \\
60 & 60 & 60 & 60
\end{pmatrix}
\]

sizes of these three matrices?
mixing matrix and polynomial tools

size and row/column degrees

**size** of a polynomial matrix = number of coefficients from $\mathbb{K}$ needed for its dense representation

for $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$,
size($A$) = $\sum_{i,j} $ size($a_{i,j}$) = $\sum_{i,j} 1 + \max(0, \deg(a_{i,j}))$

recall $\deg(AB) \leq \deg(A) + \deg(B)$,
however:

in general the size is not compatible with matrix products

but it may be, in some particular cases

- these particular cases include whole families of matrices
c.f. the degree profiles we just saw

- and they include *reduced matrices* often arising in algorithms
definition will come soon
**row degree** of a polynomial matrix

= the list of the maximum degree in each of its rows

for $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$,

$$\text{rdeg}(A) = (\text{rdeg}(A_{1,*}), \ldots, \text{rdeg}(A_{m,*}))$$

$$= \left( \max_{1 \leq j \leq n} \deg(A_{1,j}), \ldots, \max_{1 \leq j \leq n} \deg(A_{m,j}) \right) \in \mathbb{Z}^m$$
row degree of a polynomial matrix
= the list of the maximum degree in each of its rows

column degree of a polynomial matrix
= the list of the maximum degree in each of its columns
mixing matrix and polynomial tools

size and row/column degrees

**row degree** of a polynomial matrix
= the list of the maximum degree in each of its rows

**column degree** of a polynomial matrix
= the list of the maximum degree in each of its columns

average size \(\leq\) average row size
average column size \(\leq m n (1 + \deg(A))\)
row degree of a polynomial matrix
= the list of the maximum degree in each of its rows

column degree of a polynomial matrix
= the list of the maximum degree in each of its columns

average size \leq \text{average row size} \leq \text{average column size} \leq mn(1 + \deg(A))

Consider \( A \) and \( B \) with respective degree matrices:

\[
A = \begin{pmatrix}
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10 \\
100 & 50 & 40 & 10 \\
\end{pmatrix}
\quad \text{and} \quad
B = \begin{pmatrix}
100 & 100 & 100 & 100 \\
50 & 50 & 50 & 50 \\
40 & 40 & 40 & 40 \\
10 & 10 & 10 & 10 \\
\end{pmatrix}
\]

row degree and column degree of these two matrices?
Exercise: multiplication, determinant, inversion

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
- Could your complexity bounds take into account degree measures that refine the matrix degree such as the average row or column degree?
- For inversion, assume you can do quasi-linear Cauchy interpolation
5.8. Cauchy interpolation

The polynomial interpolation problem is, given a collection of sample values $v_i = f(u_i) \in F$ for $0 \leq i < n$ of an unknown function $f:F \rightarrow F$ at distinct points $u_0, \ldots, u_{n-1}$ of a field $F$, to compute a polynomial $g \in F[x]$ of degree less than $n$ that interpolates $g$ at those points, so that $g(u_i) = v_i$ for all $i$. We saw in Section 5.2 that such a polynomial always exists uniquely and learned how to compute it using the Lagrange interpolation formula.

A more general problem is **Cauchy interpolation** or rational interpolation, where furthermore $k \in \{0, \ldots, n\}$ is given and we are looking for a rational function $r/t \in F(x)$, with $r, t \in F[x]$, such that

$$t(u_i) \neq 0 \text{ and } \frac{r(u_i)}{t(u_i)} = v_i \text{ for } 0 \leq i < n, \quad \deg r < k, \quad \deg t \leq n - k. \quad (20)$$

[von zur Gathen, Gerhard, Modern Computer Algebra]

see also [AECF, Definition 7.1] (in French)

we will describe a quasi-linear algorithm later in this course which does not rely on polynomial matrix inversion...
mixing matrix and polynomial tools

partial linearization techniques

reduce **unbalanced** degrees to the **average** degree

where degree means row degree, column degree, or related refined measures

[Storjohann 2006] [Zhou-Labahn 2012] [Jeannerod-Neiger-Villard 2020]

typical properties:
from a matrix $A \in K[X]^{m \times m}$ with $D = |\text{rdeg}(A)| \ll m \deg(A)$ construct a matrix $\bar{A} \in K[X]^{m' \times m'}$ with

- a slight increase of matrix dimension: $m \leq m' \leq 2m$
- a strong decrease of matrix degree: $\deg(\bar{A}) \leq 2 \frac{D}{m}$
- preservation of the features targeted by our computations

examples:
- product $AB$ easily deduced from product $\bar{A}\bar{B}$
- preservation of the determinant $\det(A) = \det(\bar{A})$
- inverse of $\bar{A}$ contains inverse of $A$ as submatrix
- ...
mixing matrix and polynomial tools

partial linearization techniques

reduce unbalanced degrees to the average degree

basic illustration:

- let $A \in \mathbb{K}[X]^{m \times m}$ of degree $< d$,
- let $u \in \mathbb{K}[X]^{m \times 1}$ of degree $< md$,

then the matrix-vector product $Au$ can be computed in $\text{MM}(m, d) + O(m^2d)$ operations in $\mathbb{K}$.

what would be the cost of the "naive" multiplication?

algorithm:
mixing matrix and polynomial tools

partial linearization techniques

reduce unbalanced degrees to the average degree

basic illustration:
- let $A \in \mathbb{K}[X]^{m \times m}$ of degree $< d$,
- let $u \in \mathbb{K}[X]^{m \times 1}$ of degree $< md$,
then the matrix-vector product $Au$ can be computed in $\text{MM}(m, d) + O(m^2 d)$ operations in $\mathbb{K}$

what would be the cost of the “naive” multiplication?

algorithm:

\[
\begin{bmatrix}
A
\end{bmatrix}
\begin{bmatrix}
u
\end{bmatrix}
= 
\begin{bmatrix}
A
\end{bmatrix}
\begin{bmatrix}
\bar{u}
\end{bmatrix}
\begin{bmatrix}
1 \\
X^d \\
X^{2d}
\vdots
\end{bmatrix}
\]

where the columns of $\bar{u} \in \mathbb{K}[X]^{m \times m}$ form the $X^d$-adic expansion of $u$

$\Rightarrow$ here $\deg(\bar{u}) < d$
Introduction

- Definitions and algebraic properties
- Examples you already know
- Three flagship applications

Matrices? Polynomials?

- Using matrix arithmetic
- Using polynomial arithmetic
- Limitations of these viewpoints

Polynomial Matrices

- Size and row/column degrees
- Evaluation-interpolation-based algorithms
- Partial linearization techniques

Reduced Forms
<table>
<thead>
<tr>
<th>Outline Section</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>introduction</td>
<td>definitions and algebraic properties</td>
</tr>
<tr>
<td></td>
<td>examples you already know</td>
</tr>
<tr>
<td></td>
<td>three flagship applications</td>
</tr>
<tr>
<td>matrices? polynomials?</td>
<td>using matrix arithmetic</td>
</tr>
<tr>
<td></td>
<td>using polynomial arithmetic</td>
</tr>
<tr>
<td></td>
<td>limitations of these viewpoints</td>
</tr>
<tr>
<td>polynomial matrices</td>
<td>size and row/column degrees</td>
</tr>
<tr>
<td></td>
<td>evaluation-interpolation-based algorithms</td>
</tr>
<tr>
<td></td>
<td>partial linearization techniques</td>
</tr>
<tr>
<td>reduced forms</td>
<td>motivations</td>
</tr>
<tr>
<td></td>
<td>leading matrix and reducedness</td>
</tr>
<tr>
<td></td>
<td>characterizations and main properties</td>
</tr>
</tbody>
</table>
polynomial matrices in reduced form

motivations

the above degree measures and techniques
- yield faster algorithms in some cases
- but leave many remaining questions

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on \(\text{lc}(\mathbf{B})\) for QuoRem
3. can we get even faster determinant and inversion?
polynomial matrices in reduced form

motivations

the above degree measures and techniques
● yield faster algorithms in some cases
● but leave many remaining questions

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on $\text{lc}(B)$ for QuoRem
3. can we get even faster determinant and inversion?

1. more general partial linearizations

**Theorem 3.7.** Let $A \in \mathbb{K}[x]^{m \times n}$, $s$ a shift with entries bounding the column degrees of $A$ and $\xi$, a bound on the sum of the entries of $s$. Let $B \in \mathbb{K}[x]^{n \times k}$ with $k \in O(m)$ and the sum $\theta$ of its $s$-column degrees satisfying $\theta \in O(\xi)$. Then we can multiply $A$ and $B$ with a cost of $O^\sim(nm^{2\xi})$.

[Zhou-Labahn-Storjohann 2012]

shift $s$? s-column degree?
polynomial matrices in reduced form

motivations

the above degree measures and techniques
▶ yield faster algorithms in some cases
▶ but leave many remaining questions

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on \( \text{lc}(B) \) for \( \text{QuoRem} \)
3. can we get even faster determinant and inversion?

2. more general division with remainder
is it reasonable to have an algorithm
which is not able to perform the division
\( A = BQ + R \) when \( B \) is the diagonal
matrix \( B = \text{diag}(X^{d_1}, \ldots, X^{d_m}) \)?
polynomial matrices in reduced form

motivations

▶ yield **faster algorithms** in some cases
▶ but leave **many remaining questions**

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on \( \text{lc}(B) \) for \( \text{QuoRem} \)
3. can we get even faster determinant and inversion?

---

2. more general division with remainder

is it reasonable to have an algorithm which is not able to perform the division \( A = BQ + R \) when \( B \) is the diagonal matrix \( B = \text{diag}(X^{d_1}, \ldots, X^{d_m}) \)?

[Neiger-Vu 2017]

[Algorithm 1: PM-QuoRem]

**Input:**
- \( M \in \mathbb{K}[x]^{n \times n} \) column reduced,
- \( F \in \mathbb{K}[x]^{n \times n} \),
- \( \delta \in \mathbb{Z}_{>0} \) such that \( \text{cdeg}(F) < \text{cdeg}(M) + (\delta, \ldots, \delta) \).

**Output:** the quotient \( \text{Quo}(F, M) \), the remainder \( \text{Rem}(F, M) \).

1. */ reverse order of coefficients */
   \( (d_1, \ldots, d_n) \leftarrow \text{cdeg}(M) \)
   \( M_{\text{rev}} = M(x^{-1}) \text{diag}(x^{d_1}, \ldots, x^{d_n}) \)
   \( F_{\text{rev}} = F(x^{-1}) \text{diag}(x^{\delta+d_1-1}, \ldots, x^{\delta+n-1}) \)
2. */ compute quotient via expansion */
   \( Q_{\text{rev}} \leftarrow F_{\text{rev}}M_{\text{rev}}^{-1} \mod x^\delta \)
   \( Q \leftarrow x^{\delta-1}Q_{\text{rev}}(x^{-1}) \)
3. Return \( (Q, F - QM) \)
polynomial matrices in reduced form

motivations

the above degree measures and techniques
- yield faster algorithms in some cases
- but leave many remaining questions

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on $\text{lc}(B)$ for QuoRem
3. can we get even faster determinant and inversion?

3. even faster algorithms

for $A \in K[X]^{m \times m}$ of degree $d$, evaluation-interpolation yields determinant and inverse algorithms in $O^\sim(m^{\omega+1}d)$ ops.

how does this compare to the size of $A$?
if you were to search for faster algorithms, what would you pick as your target complexity bound?
polynomial matrices in reduced form

motivations

the above degree measures and techniques
▶ yield **faster algorithms** in some cases
▶ but leave **many remaining questions**

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on $\text{lcm}(B)$ for QuoRem
3. can we get even faster determinant and inversion?

3. **even faster algorithms**

for $A \in \mathbb{K}[X]^{m \times m}$ of degree $d$, evaluation-interpolation yields determinant and inverse algorithms in $O^\sim(m^{\omega+1}d)$ ops.

how does this compare to the size of $A$?
if you were to search for faster algorithms, what would you pick as your target complexity bound?

$\leadsto$ cost $O^\sim(m^{\omega \frac{D}{m}})$ achieved using operations on **reduced matrices**

polynomial matrices in reduced form

motivations

the above degree measures and techniques
▷ yield faster algorithms in some cases
▷ but leave many remaining questions

1. row and column degrees not compatible with multiplication
2. does not lift the restrictive assumption on $\text{lcm}(B)$ for QuoRem
3. can we get even faster determinant and inversion?

4. bonus: predictable degrees

in the two cases below,
▷ can you predict $\deg \det(A)$?
▷ can you predict the degrees in $BA$ from the degrees in $B$?

. case 1: $A = XI_m - M$, with $M \in \mathbb{K}^{m \times m}$
. case 2: $A = X^dL + R$, with $\deg(R) < d$ and $L \in \mathbb{K}^{m \times m}$
polynomial matrices in reduced form

leading matrix and reducedness

notation:

let \( A \in \mathbb{K}[X]^{m \times n} \) with no zero row,
define \( d = (d_1, \ldots, d_m) = \text{rdeg}(A) \)

and \( X^d = \begin{bmatrix} X^{d_1} & \cdots & \cdots & X^{d_m} \end{bmatrix} \in \mathbb{K}[X]^{m \times m} \)

definition: (row-wise) leading matrix

the leading matrix of \( A \) is the unique matrix \( L \in \mathbb{K}^{m \times n} \)
such that \( A = X^dL + R \) with \( \text{rdeg}(R) < d \) entry-wise

equivalently, \( X^{-d}A = L + \text{terms of strictly negative degree} \)
notation: 
let \( A \in \mathbb{K}[X]^{m \times n} \) with no zero row,
define \( d = (d_1, \ldots, d_m) = \text{rdeg}(A) \)
and \( X^d = \begin{bmatrix} X^{d_1} \\ \vdots \\ X^{d_m} \end{bmatrix} \in \mathbb{K}[X]^{m \times m} \)

definition: (row-wise) leading matrix 
the leading matrix of \( A \) is the unique matrix \( L \in \mathbb{K}^{m \times n} \)
such that \( A = X^dL + R \) with \( \text{rdeg}(R) < d \) entry-wise

equivalently, \( X^{-d}A = L + \text{terms of strictly negative degree} \)

. what is the leading matrix of \( \begin{bmatrix} 3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\ 5 & 5X^2 + 3X + 1 & 5X + 3 \end{bmatrix} \)?

. what is the leading matrix of \( A = XI_m - M \) of \( A = X^dL + R \)?
polynomial matrices in reduced form

leading matrix and reducedness

notation:
let $A \in \mathbb{K}[X]^{m \times n}$ with no zero row,
we write $\text{lm}(A)$ for the leading matrix of $A$

definition: (row-wise) reduced matrix
$A \in \mathbb{K}[X]^{m \times n}$ is said to be reduced
if $\text{lm}(A)$ has full row rank

what does this imply on $m$ and $n$?
notation:
let $A \in \mathbb{K}[X]^{m \times n}$ with no zero row,
we write $\text{lm}(A)$ for the leading matrix of $A$

**definition: (row-wise) reduced matrix**
$A \in \mathbb{K}[X]^{m \times n}$ is said to be **reduced**
if $\text{lm}(A)$ has full row rank

what does this imply on $m$ and $n$?

- is the matrix
  $\begin{bmatrix}
  3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
  5 & 5X^2 + 3X + 1 & 5X + 3
  \end{bmatrix}$ reduced?

- is $A = X I_m - M$ row-wise reduced? column-wise reduced?

- is “$A = X^d L + R$ is reduced” equivalent to “$L$ is invertible”? 
polynomial matrices in reduced form

characterizations and main properties

let $A \in \mathbb{K}[X]^{m \times n}$ with $m \leq n$, the following are equivalent:

(i) $A$ is reduced (i.e. $\text{Im}(A)$ has full rank)
let $A \in \mathbb{K}[X]^{m \times n}$ with $m \leq n$, the following are equivalent:

(i) $A$ is reduced (i.e. $\text{Im}(A)$ has full rank)

(ii) for any vector $u = [u_1 \ 1 \ u_2] \in \mathbb{K}[X]^{1 \times m}$ with 1 at index $i$, $r\text{deg}(uA) \geq r\text{deg}(A_{i,\ast})$
polynomial matrices in reduced form

characterizations and main properties

let $A \in \mathbb{K}[X]^{m \times n}$ with $m \leq n$,

the following are equivalent:

(i) $A$ is reduced (i.e. $\text{Im}(A)$ has full rank)

(ii) for any vector $u = [u_1 \ 1 \ u_2] \in \mathbb{K}[X]^{1 \times m}$ with 1 at index $i$,

$r\text{deg}(uA) \geq r\text{deg}(A_{i,\ast})$

(iii) predictable degree: for any vector $u = [u_1 \ldots u_m] \in \mathbb{K}[X]^{1 \times m}$,

$r\text{deg}(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + r\text{deg}(A_{i,\ast}))$
polynomial matrices in reduced form

characterizations and main properties

let $A \in \mathbb{K}[X]^{m \times n}$ with $m \leq n$, the following are equivalent:

(i) $A$ is reduced (i.e. $\text{Im}(A)$ has full rank)

(ii) for any vector $u = [u_1 \ 1 \ u_2] \in \mathbb{K}[X]^{1 \times m}$ with 1 at index $i$,
    $r\text{deg}(uA) \geq r\text{deg}(A_{i,*})$

(iii) predictable degree: for any vector $u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m}$,
    $r\text{deg}(uA) = \max_{1 \leq i \leq m}(\text{deg}(u_i) + r\text{deg}(A_{i,*}))$

(iv) degree minimality: $r\text{deg}(A) \preceq r\text{deg}(UA)$ holds for any nonsingular matrix $U \in \mathbb{K}[X]^{m \times m}$, where $\preceq$ sorts the tuples in nondecreasing order and then uses lexicographic comparison
polynomial matrices in reduced form

characterizations and main properties

let \( A \in \mathbb{K}[X]^{m \times n} \) with \( m \leq n \),
the following are equivalent:

(i) \( A \) is reduced (i.e. \( \text{Im}(A) \) has full rank)

(ii) for any vector \( u = [u_1 \quad 1 \quad u_2] \in \mathbb{K}[X]^{1 \times m} \) with 1 at index \( i \),
\( r\deg(uA) \geq r\deg(A_{i,*}) \)

(iii) predictable degree: for any vector \( u = [u_1 \ldots u_m] \in \mathbb{K}[X]^{1 \times m} \),
\( r\deg(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + r\deg(A_{i,*})) \)

(iv) degree minimality: \( r\deg(A) \preceq r\deg(UA) \) holds for any nonsingular matrix \( U \in \mathbb{K}[X]^{m \times m} \),
where \( \preceq \) sorts the tuples in nondecreasing order and then uses lexicographic comparison

(v) predictable determinantal degree: \( \deg \det(A) = |r\deg(A)| \)
(only when \( m = n \))
summary

introduction
- definitions and algebraic properties
- examples you already know
- three flagship applications

matrices? polynomials?
- using matrix arithmetic
- using polynomial arithmetic
- limitations of these viewpoints

polynomial matrices
- size and row/column degrees
- evaluation-interpolation-based algorithms
- partial linearization techniques

reduced forms
- motivations
- leading matrix and reducedness
- characterizations and main properties