polynomial matrices:
approximation and interpolation, quasi-linear GCD

Algorithmes Efficaces en Calcul Formel
Master Parisien de Recherche en Informatique
6 December 2022
- Introduction
- Shifted Reduced Forms
- Fast Algorithms
- Applications
outline

- introduction
  - rational approximation and interpolation
  - the vector case
  - pol. matrices: reminders and motivation
- shifted reduced forms
- fast algorithms
- applications
introduction

 ⇦ earlier in the course ⇦

 ⇦ in this lecture ⇦
addition $f + g$, multiplication $f \cdot g$

division with remainder $f = qg + r$

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

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

multipoint eval. $f \mapsto f(\alpha_1), \ldots, f(\alpha_d)$

interpolation $f(\alpha_1), \ldots, f(\alpha_d) \mapsto f$

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

minpoly of linearly recurrent sequence

in this lecture

earlier in the course
### Introduction

#### Earlier in the Course

- **$O(M(d))$**
  - Addition $f + g$, multiplication $f \times g$
  - Division with remainder $f = qg + r$
  - Truncated inverse $f^{-1} \mod X^d$
  - Extended GCD $uf + vg = \gcd(f, g)$

- **$O(M(d) \log(d))$**
  - Multipoint eval. $f \mapsto f(\alpha_1), \ldots, f(\alpha_d)$
  - Interpolation $f(\alpha_1), \ldots, f(\alpha_d) \mapsto f$
  - Padé approximation $f = \frac{p}{q} \mod X^d$
  - Minpoly of linearly recurrent sequence

#### In This Lecture
introduction

⇓ earlier in the course ⇓

\[ O(M(d)) \]

- addition \( f + g \), multiplication \( f \times g \)
- division with remainder \( f = qg + r \)
- truncated inverse \( f^{-1} \mod X^d \)
- extended GCD \( uf + vg = \gcd(f, g) \)

\[ O(M(d) \log(d)) \]

- multipoint eval. \( f \mapsto f(\alpha_1), \ldots, f(\alpha_d) \)
- interpolation \( f(\alpha_1), \ldownarrow \ldots, f(\alpha_d) \mapsto f \)
- Padé approximation \( f = \frac{p}{q} \mod X^d \)
- minpoly of linearly recurrent sequence

⇓ in this lecture ⇓

- Padé approximation, sequence minpoly, extended GCD
- \( O(M(d) \log(d)) \) operations in \( \mathbb{K} \)

matrix versions of these problems

- \( O(m^\omega M(d) \log(d)) \) operations in \( \mathbb{K} \)

or a tiny bit more for matrix-GCD
given power series $p(X)$ and $q(X)$ over $\mathbb{K}$ at precision $d$, with $q(X)$ invertible,
→ compute $\frac{p(X)}{q(X)} \mod X^d$
given power series $p(X)$ and $q(X)$ over $\mathbb{K}$ at precision $d$, with $q(X)$ invertible, 
→ compute $\frac{p(X)}{q(X)} \mod X^d$
given power series $p(X)$ and $q(X)$ over $\mathbb{K}$ at precision $d$, 
with $q(X)$ invertible, 
$\rightarrow$ compute $\frac{p(X)}{q(X)} \mod X^d$ 

given $M(X) \in \mathbb{K}[X]$ of degree $d > 0$, 
given polynomials $p(X)$ and $q(X)$ over $\mathbb{K}$ of degree $< d$, 
with $q(X)$ invertible modulo $M(X)$, 
$\rightarrow$ compute $\frac{p(X)}{q(X)} \mod M(X)$
given **power series** $p(X)$ and $q(X)$ over $\mathbb{K}$ at precision $d$, with $q(X)$ invertible, 
$\rightarrow$ compute $\frac{p(X)}{q(X)} \mod X^d$

*algo?? $O(??)$
*inv+mul: $O(M(d))$

---

given $M(X) \in \mathbb{K}[X]$ of degree $d > 0$,
given **polynomials** $p(X)$ and $q(X)$ over $\mathbb{K}$ of degree $< d$, with $q(X)$ invertible modulo $M(X)$, 
$\rightarrow$ compute $\frac{p(X)}{q(X)} \mod M(X)$

*algo?? $O(??)$
*xgcd+mul+rem: $O(M(d) \log(d))$
given power series \( p(X) \) and \( q(X) \) over \( \mathbb{K} \) at precision \( d \),
with \( q(X) \) invertible,
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod X^d \]
algo?? \( O(??) \)
inv+mul: \( O(M(d)) \)

given \( M(X) \in \mathbb{K}[X] \) of degree \( d > 0 \),
given polynomials \( p(X) \) and \( q(X) \) over \( \mathbb{K} \) of degree \( < d \),
with \( q(X) \) invertible modulo \( M(X) \),
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod M(X) \]
what does that mean?
algo?? \( O(??) \)
xgcd+mul+rem \( O(M(d) \log(d)) \)

given \( M(X) = (X - \alpha_1) \cdots (X - \alpha_d) \in \mathbb{K}[X] \),
for pairwise distinct \( \alpha_1, \ldots, \alpha_d \in \mathbb{K} \),
given polynomials \( p(X) \) and \( q(X) \) over \( \mathbb{K} \) of degree \( < d \),
with \( q(X) \) invertible modulo \( M(X) \),
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod M(X) \]
what does that mean?
algo?? \( O(??) \)
Introduction

rational approximation and interpolation

Given power series \( p(X) \) and \( q(X) \) over \( K \) at precision \( d \), with \( q(X) \) invertible,
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod X^d \]

Algorithm? \( O(??) \)

\[ \text{inv+mul: } O(M(d)) \]

Given \( M(X) \in K[X] \) of degree \( d > 0 \),
given polynomials \( p(X) \) and \( q(X) \) over \( K \) of degree \( < d \),
with \( q(X) \) invertible modulo \( M(X) \),
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod M(X) \]

What does that mean?
Algorithm? \( O(??) \)

\[ \text{xgcd+mul+rem } O(M(d \log d)) \]

Given \( M(X) = (X - \alpha_1) \cdots (X - \alpha_d) \in K[X] \),
for pairwise distinct \( \alpha_1, \ldots, \alpha_d \in K \),
given polynomials \( p(X) \) and \( q(X) \) over \( K \) of degree \( < d \),
with \( q(X) \) invertible modulo \( M(X) \),
\[ \rightarrow \text{compute } \frac{p(X)}{q(X)} \mod M(X) \]

What does that mean?
Algorithm? \( O(??) \)

\[ \text{eval+div+interp } O(M(d \log d)) \]
rational approximation and interpolation

rational fractions $\iff$ linearly recurrent sequences

reminders from lectures 4 and 5
Application: extension of recurrences

[Shoup, 1991]

Problem: Given \(r, N \in \mathbb{N}\), a linear recurrence with constant coefficients of order \(r\) for \((u_n)_n\) and the first \(r\) terms \(u_0, \ldots, u_{r-1}\), compute \(u_r, \ldots, u_N\)

Naive algorithm: unroll the recurrence \(O(rN) \subseteq O(N^2)\)

Idea: \(\sum_{i \geq 0} u_i x^i\) is rational \(A(x)/B(x)\), with \(B\) given by the input recurrence, and \(\deg(A) < \deg(B)\)

Example (Fibonacci): \(F_{i+2} = F_{i+1} + F_i\) \iff \(\sum_i F_i x^i = \frac{F_0 + (F_1 - F_0)x}{1 - x - x^2}\)

Algorithm:
- Compute \(A\) from \(B\) and \(u_0, \ldots, u_{r-1}\) \(O(M(r))\)
- Expand \(A/B\) modulo \(x^{N+1}\) \(O(M(N))\)
Computing the $N$-th coefficient of a rational function

**Duality lemma** (link between C-recursive sequences and rational functions)
Let $A(x) = \sum_{n \geq 0} u_n x^n \in \mathbb{K}[[x]]$ be the generating function of $(u_n)_{n \geq 0}$.
The following assertions are equivalent:

(i) $(u_n)_{n \geq 0}$ is C-recursive, having $\Gamma$ as characteristic polynomial of degree $d$;

(ii) $A(x)$ is rational, of the form $A = P / Q$ for some $P \in \mathbb{K}[x]_{<d}$, where $Q := \text{rev}_d(\Gamma) = \Gamma(\frac{1}{x})x^d$.

▷ The denominator of $A$ encodes a recurrence for $(u_n)_{n \geq 0}$; the numerator encodes initial conditions.

▷ Generating function of $(F_n)_{n \geq 0}$ given by $F_0 = a$, $F_1 = b$, $F_{n+2} = F_{n+1} + F_n$ is $(a + (b - a)x) / (1 - x - x^2)$. Here $\Gamma = x^2 - x - 1$ and $P = a + (b - a)x$.

▷ **Corollary:** $N$-th Taylor coeff. of $\frac{P}{Q} \in \mathbb{K}(x)_d$ in $\sim 3M(d) \log N$ ops. in $\mathbb{K}$
rational fractions $\leftrightarrow$ linearly recurrent sequences
reminders from lectures 4 and 5

\[
\text{expand } \frac{N}{\text{rev}(P)} \mod X^d
\]

numerator $N$ and charpoly $P$ $\quad$ first $d$ terms of the LRS $(u_n)_{n \in \mathbb{N}}$
Introduction

Rational approximation and interpolation

Rational fractions $\longleftrightarrow$ linearly recurrent sequences
Reminders from lectures 4 and 5

Numerator $N$ and charpoly $P$ \hspace{2cm} First $d$ terms of the LRS $(u_n)_{n \in \mathbb{N}}$

Expand $\frac{N}{\text{rev}(P)} \mod X^d$

Reconstruct from $A(X) \mod X^d \rightsquigarrow$ Padé approximation
Padé approximation:

given power series \( f(X) \) at precision \( d \),
\[ \rightarrow \] compute \( p(X), q(X) \) such that \( f = \frac{p}{q} \mod X^d \)
introduction

rational approximation and interpolation

**Padé approximation:**
given power series \( f(X) \) at precision \( d \),
→ compute \( p(X), q(X) \) such that \( f = \frac{p}{q} \mod X^d \)

opinions on this algorithmic problem?
Padé approximation:

given power series $f(X)$ at precision $d$,
given degree constraints $d_1, d_2 > 0$,
→ compute polynomials $(p(X), q(X))$ of degrees $< (d_1, d_2)$
and such that $f = \frac{p}{q} \mod X^d$
**Padé approximation:**

given power series \( f(X) \) at precision \( d \),
given degree constraints \( d_1, d_2 > 0 \),
→ compute polynomials \((p(X), q(X))\) of degrees < \((d_1, d_2)\)
and such that \( f = \frac{p}{q} \mod X^d \)

**Cauchy interpolation:**

given \( M(X) = (X - \alpha_1) \cdots (X - \alpha_d) \in \mathbb{K}[X] \),
for pairwise distinct \( \alpha_1, \ldots, \alpha_d \in \mathbb{K} \),
given degree constraints \( d_1, d_2 > 0 \),
→ compute polynomials \((p(X), q(X))\) of degrees < \((d_1, d_2)\)
and such that \( f = \frac{p}{q} \mod M(X) \)
Padé approximation:
given power series $f(X)$ at precision $d$,
given degree constraints $d_1, d_2 > 0$,
→ compute polynomials $(p(X), q(X))$ of degrees $< (d_1, d_2)$
and such that $f = \frac{p}{q} \mod X^d$

Cauchy interpolation:
given $M(X) = (X - \alpha_1) \cdots (X - \alpha_d) \in \mathbb{K}[X]$,
for pairwise distinct $\alpha_1, \ldots, \alpha_d \in \mathbb{K}$,
given degree constraints $d_1, d_2 > 0$,
→ compute polynomials $(p(X), q(X))$ of degrees $< (d_1, d_2)$
and such that $f = \frac{p}{q} \mod M(X)$

- degree constraints specified by the context
- usual choices have $d_1 + d_2 \approx d$ and existence of a solution
\[ K = \mathbb{F}_7 \]

\[ f = 2X^7 + 2X^6 + 5X^4 + 2X^2 + 4 \]

\[ d = 8, \quad d_1 = 3, \quad d_2 = 6 \]

→ look for \((p, q)\) of degree \(< (3, 6)\) such that \(f = \frac{p}{q} \mod X^8\)

\[
\begin{bmatrix}
q & p \\
-1 & 0
\end{bmatrix}
\begin{bmatrix}
f \\
1
\end{bmatrix}
= 0 \mod X^8
\]
\[ K = \mathbb{F}_7 \]
\[ f = 2X^7 + 2X^6 + 5X^4 + 2X^2 + 4 \]
\[ d = 8, \quad d_1 = 3, \quad d_2 = 6 \]
\[ \rightarrow \text{look for } (p, q) \text{ of degree } < (3, 6) \text{ such that } f = \frac{p}{q} \mod X^8 \]

\[
\begin{bmatrix}
q & p \\
-1 &
\end{bmatrix}
\begin{bmatrix}
f \\\
-1
\end{bmatrix}
= 0 \mod X^8
\]

\[
\begin{bmatrix}
4 & 0 & 2 & 0 & 5 & 0 & 2 & 2 \\
4 & 0 & 2 & 0 & 5 & 0 & 2 \\
4 & 0 & 2 & 0 & 5 & 0 \\
4 & 0 & 2 & 0 & 5 \\
4 & 0 & 2 \\
4 & 0 & 2 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
= 0
\]
\[ \mathbb{K} = \mathbb{F}_7 \]
\[ f = 2X^7 + 2X^6 + 5X^4 + 2X^2 + 4 \]
\[ d = 8, \, d_1 = 3, \, d_2 = 6 \]

→ look for \((p, q)\) of degree \(< (3, 6)\) such that \(f = \frac{p}{q} \mod X^8\)

\[
\begin{bmatrix}
q & p
\end{bmatrix}
\begin{bmatrix}
f \\
-1
\end{bmatrix}
= 0 \mod X^8
\]

\[
\begin{bmatrix}
[q_0 \, q_1 \, q_2 \, q_3 \, q_4 \, 1 \mid p_0 \, p_1 \, p_2]
\end{bmatrix}
= 0
\]
Sur la généralisation des fractions continues algébriques;

PAR M. H. PADÉ,

Docteur ès Sciences mathématiques,
Professeur au lycée de Lille.

[1894, Journal de mathématiques pures et appliquées]

INTRODUCTION.

M. Hermite s’est, dans un travail récemment paru (1), occupé de la généralisation des fractions continues algébriques. La question est de déterminer les polynômes $X_1, X_2, \ldots, X_n$, de degrés $\mu_1, \mu_2, \ldots, \mu_n$, qui satisfont à l’équation

$$S_1 X_1 + S_2 X_2 + \ldots + S_n X_n = S x^{\mu_1+\mu_2+\ldots+\mu_n+n-1},$$

$S_1, S_2, \ldots, S_n$ étant des séries entières données, et $S$ une série également entière. Ou plutôt, il s’agit d’obtenir un algorithme qui permette le calcul de proche en proche de ces systèmes de $n$ polynômes, et qui soit analogue à l’algorithme par lequel le numérateur et le dénominateur d’une réduite d’une fraction continue se déduisent des numérateurs et dénominateurs des réduites précédentes. D’élégantes considérations.
approximation and interpolation: the vector case

**Hermite-Padé approximation**

[Hermite 1893, Padé 1894]

**input:**
- polynomials $f_1, \ldots, f_m \in \mathbb{K}[X]$
- precision $d \in \mathbb{Z}_{>0}$
- degree bounds $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$

**output:**
polynomials $p_1, \ldots, p_m \in \mathbb{K}[X]$ such that
- $p_1 f_1 + \cdots + p_m f_m = 0 \mod X^d$
- $\text{cdeg}([p_1 \cdots p_m]) < (d_1, \ldots, d_m)$

(Padé approximation: particular case $m = 2$ and $f_2 = -1$)
M-Padé approximation / vector rational interpolation

[Cauchy 1821, Mahler 1968]

input:
- polynomials $f_1, \ldots, f_m \in K[X]$
- pairwise distinct points $\alpha_1, \ldots, \alpha_d \in K$
- degree bounds $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$

output:
- polynomials $p_1, \ldots, p_m \in K[X]$ such that
  - $p_1(\alpha_i)f_1(\alpha_i) + \cdots + p_m(\alpha_i)f_m(\alpha_i) = 0$ for all $1 \leq i \leq d$
  - $\text{cdeg}([p_1 \cdots p_m]) < (d_1, \ldots, d_m)$

(rational interpolation: particular case $m = 2$ and $f_2 = -1$)
in this lecture: modular equation and fast algebraic algorithms


input:
- polynomials $f_1, \ldots, f_m \in \mathbb{K}[X]$
- field elements $\alpha_1, \ldots, \alpha_d \in \mathbb{K}$  $\rightsquigarrow$ not necessarily distinct
- degree bounds $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$  $\rightsquigarrow$ general “shift” $s \in \mathbb{Z}^m$

output:
- polynomials $p_1, \ldots, p_m \in \mathbb{K}[X]$ such that
  - $p_1 f_1 + \cdots + p_m f_m = 0 \mod \prod_{1 \leq i \leq d} (X - \alpha_i)$
  - $\text{cdeg}([p_1 \cdots p_m]) < (d_1, \ldots, d_m)$  $\rightsquigarrow$ minimal $s$-row degree

(Hermite-Padé: $\alpha_1 = \cdots = \alpha_d = 0$; interpolation: pairwise distinct points)
application of vector rational interpolation:
given pairwise distinct points \{((\alpha_i, \beta_i), 1 \leq i \leq 8\}
\begin{align*}
&= \{(24, 80), (31, 73), (15, 73), (32, 35), (83, 66), (27, 46), (20, 91), (59, 64)\},
\end{align*}
compute a \textbf{bivariate} polynomial \(p(X, Y) \in \mathbb{K}[X, Y]\)
such that \(p(\alpha_i, \beta_i) = 0\) for \(1 \leq i \leq 8\)

\[
\begin{align*}
M(X) &= (X - 24) \cdots (X - 59) \\
L(X) &= \text{Lagrange interpolant}
\end{align*}
\]
\[\longrightarrow \text{solutions} = \text{ideal} \left\langle M(X), Y - L(X) \right\rangle\]

solutions of smaller \(X\)-degree: \(p(X, Y) = p_0(X) + p_1(X)Y + p_2(X)Y^2\)

\[
p(X, L(X)) = \begin{bmatrix} p_0 & p_1 & p_2 \end{bmatrix} \begin{bmatrix} 1 & \text{L} & \text{L}^2 \end{bmatrix} = 0 \mod M(X)
\]

\begin{itemize}
  \item instance of \textbf{univariate} rational vector interpolation
  \item with a \textbf{structured} input equation (powers of \(L \mod M\))
\end{itemize}
application of vector rational interpolation:
given pairwise distinct points \{(\alpha_i, \beta_i), 1 \leq i \leq 8\} = \{(24, 80), (31, 73), (15, 73), (32, 35), (83, 66), (27, 46), (20, 91), (59, 64)\},
compute a bivariate polynomial \(p(X, Y) \in \mathbb{K}[X, Y]\)
such that \(p(\alpha_i, \beta_i) = 0\) for \(1 \leq i \leq 8\).

add degree constraints: seek \(p(X, Y)\) of the form
\[
p_{00} + p_{01}X + p_{02}X^2 + p_{03}X^3 + p_{04}X^4 + (p_{10} + p_{11}X + p_{12}X^2)Y + p_{20}Y^2:
\]

\[
\begin{bmatrix}
P_{00} & P_{01} & P_{02} & P_{03} & P_{04} & P_{10} & P_{11} & P_{12} & P_{20}
\end{bmatrix}
\begin{bmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_8 \\
\alpha_1^2 & \alpha_2^2 & \cdots & \alpha_8^2 \\
\alpha_1^3 & \alpha_2^3 & \cdots & \alpha_8^3 \\
\alpha_1^4 & \alpha_2^4 & \cdots & \alpha_8^4 \\
\beta_1 & \beta_2 & \cdots & \beta_8 \\
\alpha_1\beta_1 & \alpha_2\beta_2 & \cdots & \alpha_8\beta_8 \\
\alpha_1^2\beta_1 & \alpha_2^2\beta_2 & \cdots & \alpha_8^2\beta_8 \\
\beta_1^2 & \beta_2^2 & \cdots & \beta_8^2
\end{bmatrix}
= 0
\]

- \(\mathbb{K}\)-linear system
- two levels of structure

\(p(X, Y) = (2X^4 + 56X^3 + 42X^2 + 48X + 15) + (72X^2 + 12X + 30)Y + Y^2\)
polyonomial matrices: reminder and motivation

why polynomial matrices here?
omitting degree constraints, the set of solutions is
\[ S = \{ (p_1, \ldots, p_m) \in \mathbb{K}[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \mod M \} \]

recall \( M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \)

why polynomial matrices here?

S is a free \( \mathbb{K}[X] \)-module of rank \( m \), meaning:

▶ stable under \( \mathbb{K}[X] \)-linear combinations
▶ admits a basis consisting of \( m \) elements
▶ basis = \( \mathbb{K}[X] \)-linear independence + generates all solutions
▶ \( S \subset \mathbb{K}[X]^m \Rightarrow S \) has rank \( \leq m \)
▶ \( M(X) \) \( \mathbb{K}[X]^m \subset S \Rightarrow S \) has rank \( \geq m \)

remark: solutions are not considered modulo \( M \) e.g. \((M, 0, \ldots, 0)\) is in \( S \) and may appear in a basis
omitting degree constraints, the set of solutions is
\[ S = \{(p_1, \ldots, p_m) \in \mathbb{K}[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \mod M\} \]

recall \( M(X) = \prod_{1 \leq i \leq d}(X - \alpha_i) \)

\( S \) is a “free \( \mathbb{K}[X] \)-module of rank \( m \)”, meaning:
- stable under \( \mathbb{K}[X] \)-linear combinations
- admits a basis consisting of \( m \) elements
- basis = \( \mathbb{K}[X] \)-linear independence + generates all solutions
introduction

polynomial matrices: reminder and motivation

why polynomial matrices here?

omitting degree constraints, the set of solutions is

\[ S = \{(p_1, \ldots, p_m) \in K[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \mod M\} \]

\[ \text{recall } M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \]

\( S \) is a “free \( K[X] \)-module of rank \( m \)”, meaning:

- stable under \( K[X] \)-linear combinations
- admits a basis consisting of \( m \) elements
- basis = \( K[X] \)-linear independence + generates all solutions

\[ \begin{align*}
\text{\( S \subset K[X]^m \Rightarrow S \) has rank} & \leq m \\
\text{\( M(X)K[X]^m \subset S \Rightarrow S \) has rank} & \geq m
\end{align*} \]

remark: solutions are not considered modulo \( M \)

e.g. \( (M, 0, \ldots, 0) \) is in \( S \) and may appear in a basis
omitting degree constraints, the set of solutions is
\[ S = \{ (p_1, \ldots, p_m) \in \mathbb{K}[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \mod M \} \]

recalling \( M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \)

basis of solutions:
- square nonsingular matrix \( P \) in \( \mathbb{K}[X]^{m \times m} \)
- each row of \( P \) is a solution
- any solution is a \( \mathbb{K}[X] \)-combination \( uP, u \in \mathbb{K}[X]^{1 \times m} \)

i.e. \( S \) is the \( \mathbb{K}[X] \)-row space of \( P \)
omitting degree constraints, the set of solutions is
\[ S = \{(p_1, \ldots, p_m) \in \mathbb{K}[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \mod M\} \]

recall \( M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \)

why polynomial matrices here?

basis of solutions:

- square nonsingular matrix \( P \) in \( \mathbb{K}[X]^{m \times m} \)
- each row of \( P \) is a solution
- any solution is a \( \mathbb{K}[X] \)-combination \( uP, u \in \mathbb{K}[X]^{1 \times m} \)

\[ \text{i.e. } S \text{ is the } \mathbb{K}[X]-\text{row space of } P \]

prove: \( \det(P) \) is a divisor of \( M(X)^m \)
omitting degree constraints, the set of solutions is
\[ S = \{(p_1, \ldots, p_m) \in K[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \pmod{M}\} \]

recall \( M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \)

**basis of solutions:**
- square nonsingular matrix \( P \) in \( K[X]^{m \times m} \)
- each row of \( P \) is a solution
- any solution is a \( K[X] \)-combination \( uP \), \( u \in K[X]^{1 \times m} \)

i.e. \( S \) is the \( K[X] \)-row space of \( P \)

**prove:** \( \det(P) \) is a divisor of \( M(X)^m \)

**prove:** any other basis is \( UP \) for \( U \in K[X]^{m \times m} \) with \( \det(U) \in K \setminus \{0\} \)
omitting degree constraints, the set of solutions is

\[ S = \{ (p_1, \ldots, p_m) \in K[X]^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \, \text{mod} \, M \} \]

recall \( M(X) = \prod_{1 \leq i \leq d} (X - \alpha_i) \)

**basis of solutions:**
- square nonsingular matrix \( P \) in \( K[X]^{m \times m} \)
- each row of \( P \) is a solution
- any solution is a \( K[X] \)-combination \( uP, u \in K[X]^{1 \times m} \)

i.e. \( S \) is the \( K[X] \)-row space of \( P \)

computing a **basis** of \( S \) with "minimal degrees"
- has many more applications than a single small-degree solution
- is in most cases the fastest known strategy anyway(!)

\( \leadsto \) degree minimality ensured via **shifted reduced forms**
**Introduction**

**Polynomial Matrices: Reminder and Motivation**

A = \[
\begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3 \\
3X^3 + X^2 + 5X + 3 & 6X + 5 & 2X + 1
\end{bmatrix}\] ∈ \(\mathbb{K}[X]^{3×3}\)

3 × 3 matrix of degree 3
with entries in \(\mathbb{K}[X] = \mathbb{F}_7[X]\)

operations in \(\mathbb{K}[X]_{d}^{m×m}\):

- combination of matrix and polynomial computations
- addition in \(O(m^2d)\), naive multiplication in \(O(m^3d^2)\)
- some tools shared with \(\mathbb{K}\)-matrices, others specific to \(\mathbb{K}[X]\)-matrices

[Cantor-Kaltofen’91]

multiplication in \(O(m^\omega d \log(d) + m^2d \log(d) \log \log(d))\)

\(∈ O(m^\omega M(d)) ⊂ O^\sim (m^\omega d)\)
introduction

polynomial matrices: reminder and motivation

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

3 × 3 matrix of degree 3 with entries in \( \mathbb{K}[X] = \mathbb{F}_7[X] \)

operations in \( \mathbb{K}[X]^{m \times m}_{<d} \):

- combination of matrix and polynomial computations
- addition in \( O(m^2d) \), naive multiplication in \( O(m^3d^2) \)
- some tools shared with \( \mathbb{K} \)-matrices, others specific to \( \mathbb{K}[X] \)-matrices

[Cantor-Kaltofen’91]

multiplication in \( O(m^\omega d \log(d) + m^2d \log(d) \log \log(d)) \)

\( \in O(m^\omega M(d)) \subset O^\sim(m^\omega d) \)

- Newton truncated inversion, matrix-QuoRem → fast \( O^\sim(m^\omega d) \)
- inversion and determinant via evaluation-interpolation → medium \( O^\sim(m^{\omega+1}d) \)
- vector rational approximation & interpolation → ???
introduction

polynomial matrices: reminder and motivation

reductions of most problems to polynomial matrix multiplication

matrix \( m \times m \) of degree \( d \)

of “average” degree \( \frac{D}{m} \)

\[ \rightarrow O^\sim(m^{\omega d}) \]
\[ \rightarrow O^\sim(m^{\omega \frac{D}{m}}) \]

classical matrix operations

- multiplication
- kernel, system solving
- rank, determinant
- inversion \( O^\sim(m^3 d) \)

univariate specific operations

- truncated inverse, QuoRem
- Hermite-Padé approximation
- vector rational interpolation
- syzygies / modular equations

transformation to normal forms

- triangularization: Hermite form
- row reduction: Popov form
- diagonalization: Smith form
reductions of most problems to polynomial matrix multiplication
matrix $m \times m$ of degree $d$ \newline
of “average” degree $\frac{D}{m}$ → $O^\sim(m^{\omega}d)$ \newline
\newline
classical matrix operations
▶ multiplication
▶ kernel, system solving
▶ rank, determinant
▶ inversion $O^\sim(m^{3}d)$

univariate specific operations
▶ truncated inverse, QuoRem
▶ Hermite-Padé approximation
▶ vector rational interpolation
▶ syzygies / modular equations

transformation to normal forms
▶ triangularization: Hermite form
▶ row reduction: Popov form
▶ diagonalization: Smith form
reductions of most problems to polynomial matrix multiplication
matrix $m \times m$ of degree $d$
of “average” degree $\frac{D}{m}$

$\rightarrow O^\sim(m^\omega d)$
$\rightarrow O^\sim(m^\omega \frac{D}{m})$

---

**classical matrix operations**

- multiplication
- kernel, system solving
- rank, determinant
- inversion $O^\sim(m^3 d)$

**univariate specific operations**

- truncated inverse, QuoRem
- Hermite-Padé approximation
- vector rational interpolation
- syzygies / modular equations

---

**transformation to normal forms**

- triangularization: Hermite form
- row reduction: Popov form
- diagonalization: Smith form
introduction

polynomial matrices: reminder and motivation

reductions of most problems to polynomial matrix multiplication
matrix \( m \times m \) of degree \( d \) of “average” degree \( \frac{D}{m} \)

\[
\rightarrow \quad O^\sim(m^\omega d)
\]
\[
\rightarrow \quad O^\sim(m^\omega \frac{D}{m})
\]

classical matrix operations
- multiplication
- kernel, system solving
- rank, determinant
- inversion \( O^\sim(m^3 d) \)

univariate specific operations
- truncated inverse, QuoRem
- Hermite-Padé approximation
- vector rational interpolation
- syzygies / modular equations

transformation to normal forms
- triangularization: Hermite form
- row reduction: Popov form
- diagonalization: Smith form
outline

- introduction
  - rational approximation and interpolation
  - the vector case
  - pol. matrices: reminders and motivation
- shifted reduced forms
- fast algorithms
- applications
shifted reduced forms

reducedness: examples and properties

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

definition: (row-wise) leading matrix

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

equivalently, $X^{-d}A = \text{Im}(A) + \text{terms of strictly negative degree}$
shifted reduced forms

reducedness: examples and properties

notation:
let \( A \in \mathbb{K}[X]^{m \times n} \) with no zero row,
define \( d = (d_1, \ldots, d_m) = rdeg(A) \)
and \( \chi^d = \begin{bmatrix} \chi^{d_1} & & \\ & \ddots & \\ & & \chi^{d_m} \end{bmatrix} \in \mathbb{K}[X]^{m \times m} \)

definition: (row-wise) leading matrix
the leading matrix of \( A \) is the unique matrix \( \text{lm}(A) \in \mathbb{K}^{m \times n} \) such that
\[
A = \chi^d \text{lm}(A) + R \text{ with } rdeg(R) < d \text{ entry-wise}
\]
equivalently, \( \chi^{-d}A = \text{lm}(A) + \text{terms of strictly negative degree} \)

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
shifted reduced forms

reducedness: examples and properties

consider the following matrices, with $\mathbb{K} = \mathbb{F}_7$:

$$A_1 = \begin{bmatrix} 3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\ 5 & 5X^2 + 3X + 1 & 5X + 3 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 3X + 1 & 4X + 3 & 5X + 5 \\ 0 & 4X^2 + 6X & 5 \\ 4X^2 + 5X + 2 & 5 & 6X^2 + 1 \end{bmatrix}$$

$A_3 = \text{transpose of } A_1$

$A_4 = \text{transpose of } A_2$

answer the following, for $i \in \{1, 2, 3, 4\}$:
1. what is $\text{rdeg}(A_i)$?
2. what is $\text{Im}(A_i)$?
3. is $A_i$ reduced?
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 $i$, $r\text{deg}(uA) \geq r\text{deg}(A_{i,*})$
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 $i$, $\text{rdeg}(uA) \geq \text{rdeg}(A_{i,*})$

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

(v) degree minimality: $\text{rdeg}(A) \preceq \text{rdeg}(UA)$ 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.

(vi) predictable determinantal degree: $\deg \det(A) = |\text{rdeg}(A)|$ (only when $m = n$)
polynomial matrices in reduced form

reducedness: examples and 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 $i$, $r\deg(uA) \geq r\deg(A_{i,*})$

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

(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
polynomial matrices in reduced form

reducedness: examples and 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 $u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m}$, $r\text{deg}(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + r\text{deg}(A_{i,*}))$

(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

(v) predictable determinantal degree: $\deg \det(A) = |r\text{deg}(A)|$ (only when $m = n$)
shifted reduced forms

reducedness: examples and properties

recall the matrix, with $\mathbb{K} = \mathbb{F}_7$,
$$A = \begin{bmatrix}
3X + 1 & 4X + 3 & 5X + 5 \\
0 & 4X^2 + 6X & 5 \\
4X^2 + 5X + 2 & 5 & 6X^2 + 1
\end{bmatrix}$$

1. what is $\deg \det(A)$?

2. what is $rdeg([4X^2 + 1 \ 2X \ 4X + 5] A)$?

3. is it possible to find a matrix
$$P = \begin{bmatrix}
p_{00} & p_{01} & p_{02} \\
p_{10} & p_{11} & p_{12}
\end{bmatrix}$$
whose rank is 2, whose degree is 1, and which is a left-multiple of $A$?
shifted reduced forms

reducedness: examples and properties

recall the matrix, with $K = \mathbb{F}_7$,

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

1. what is $\text{deg det}(A)$?

2. what is $\text{rdeg}([4X^2 + 1 \ 2X \ 4X + 5] A)$?

3. is it possible to find a matrix

$$P = \begin{bmatrix}
p_{00} & p_{01} & p_{02} \\
p_{10} & p_{11} & p_{12}
\end{bmatrix}$$

whose rank is 2, whose degree is 1, and which is a left-multiple of $A$?

find a row vector $u$ of degree 1 such that $uA$ has degree 2, where

$$A = \begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3
\end{bmatrix}$$
keeping our problem in mind:

- **input:** $f_i$'s and $\alpha_i$'s and degree constraints $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$
- **output:** a solution $p$ satisfying the constraints $cdeg(p) < (d_1, \ldots, d_m)$

**obstacle:**
computing a reduced basis of solutions ignores the constraints

**exercise:** suppose we have a reduced basis $P \in K[X]^{m \times m}$ of solutions

- think of particular constraints $(d_1, \ldots, d_m)$ that can be handled via $P$
- give constraints $(d_1, \ldots, d_m)$ for which $P$ is “typically” not satisfactory
shifted reduced forms

shifted forms and degree constraints

keeping our problem in mind:

- input: $f_i$'s and $\alpha_i$'s and degree constraints $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$
- output: a solution $p$ satisfying the constraints $\text{cdeg}(p) < (d_1, \ldots, d_m)$

obstacle:
computing a reduced basis of solutions ignores the constraints

exercise: suppose we have a reduced basis $P \in K[X]^{m \times m}$ of solutions

- think of particular constraints $(d_1, \ldots, d_m)$ that can be handled via $P$
- give constraints $(d_1, \ldots, d_m)$ for which $P$ is “typically” not satisfactory

solution: compute $P$ in shifted reduced form
shifted reduced forms

shifted forms and degree constraints

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

using elementary row operations, transform \( A \) into...

Hermite form

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

Popov form

\[ P = \begin{bmatrix} X^3 + 5X^2 + 4X + 1 & 2X + 4 & 3X + 5 \\ 1 & X^2 + 2X + 3 & X + 2 \\ 3X + 2 & 4X & X^2 \end{bmatrix} \]
shifted reduced forms

shifted forms and degree constraints

nonsingular \( A \in \mathbb{K}[X]^{m \times m} \)

elementary row transformations

Hermite form \([\text{Hermite, 1851}]\)

▷ triangular
▷ column normalized

\[
\begin{bmatrix}
16 & 0 \\
15 & 0 \\
15 & 0 \\
\end{bmatrix}
\quad \begin{bmatrix}
4 & 3 & 7 \\
3 & 1 & 5 & 3 \\
3 & 6 & 1 & 2 \\
\end{bmatrix}
\]
shifted reduced forms

shifted forms and degree constraints

nonsingular $A \in \mathbb{K}[X]^{m \times m}$

elementary row transformations

Hermite form [Hermite, 1851]
- triangular
- column normalized

<table>
<thead>
<tr>
<th>16</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

Popov form [Popov, 1972]
- row reduced/distinct pivots
- column normalized

<table>
<thead>
<tr>
<th>4</th>
<th>3</th>
<th>3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th>0</th>
<th>1</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
shifted reduced forms

shifted forms and degree constraints

nonsingular $A \in K[X]^{m \times m}$

elementary row transformations

Hermite form [Hermite, 1851]

- triangular
- column normalized

Popov form [Popov, 1972]

- row reduced/distinct pivots
- column normalized

$\begin{bmatrix}
16 & 0 \\
15 & 0 \\
15 & 0 \\
\end{bmatrix}$

$\begin{bmatrix}
4 & 7 \\
3 & 3 \\
1 & 2 \\
\end{bmatrix}$

$\begin{bmatrix}
4 & 3 & 3 & 3 \\
3 & 4 & 3 & 3 \\
3 & 3 & 4 & 3 \\
3 & 3 & 3 & 4 \\
\end{bmatrix}$

$\begin{bmatrix}
7 & 0 & 1 & 5 \\
0 & 1 & 0 \\
0 & 2 \\
6 & 0 & 1 & 6 \\
\end{bmatrix}$

$\begin{bmatrix}
15 \\
16 \\
15 \\
15 \\
\end{bmatrix}$

$\begin{bmatrix}
3 \\
1 \\
3 \\
3 \\
\end{bmatrix}$

$\begin{bmatrix}
3 \\
5 \\
6 \\
1 \\
2 \\
6 \\
0 \\
1 \\
6 \\
\end{bmatrix}$

$\begin{bmatrix}
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\leq \text{pot} \\
\end{bmatrix}$

$\leq \text{reduced Gröbner basis}$

$K[X]$-module $S \subset K[X]^{1 \times m}$ of rank $m$
**shifted reduced forms**

**shifted forms and degree constraints**

**nonsingular** \( \mathbf{A} \in \mathbb{K}[X]^{m \times m} \)

**elementary row transformations**

**Hermite form** [Hermite, 1851]
- triangular
- column normalized

\[
\begin{bmatrix}
16 & 0 \\
15 & 0 \\
15 & 0 \\
\end{bmatrix}
\begin{bmatrix}
4 & 7 \\
3 & 3 \\
1 & 5 \\
3 & 6 \\
\end{bmatrix}
\]

**Popov form** [Popov, 1972]
- row reduced/distinct pivots
- column normalized

\[
\begin{bmatrix}
4 & 3 & 3 & 3 \\
3 & 4 & 3 & 3 \\
3 & 3 & 4 & 3 \\
3 & 3 & 3 & 4 \\
\end{bmatrix}
\begin{bmatrix}
7 & 0 & 1 & 5 \\
0 & 1 & 0 & 0 \\
2 & & & \ \\
6 & 0 & 1 & 6 \\
\end{bmatrix}
\]

**Invariant:** \( D = \deg(\det(\mathbf{A})) = 4 + 7 + 3 + 2 = 7 + 1 + 2 + 6 \)
- **average** column degree is \( \frac{D}{m} \)
- **size** of object is \( mD + m^2 = m^2(\frac{D}{m} + 1) \)
shifted reduced forms

shifted forms and degree constraints

nonsingular \( A \in \mathbb{K}[X]^{m \times m} \)

elementary row transformations

Hermite form [Hermite, 1851]
- triangular
- column normalized

\[
\begin{bmatrix}
16 & 0 \\
15 & 0 \\
15 & 0
\end{bmatrix}
\quad \begin{bmatrix}
4 & 7 \\
3 & 7 \\
3 & 6
\end{bmatrix}
\]

Popov form [Popov, 1972]
- row reduced/distinct pivots
- column normalized

\[
\begin{bmatrix}
4 & 3 & 3 & 3 \\
3 & 4 & 3 & 3 \\
3 & 3 & 4 & 3 \\
3 & 3 & 3 & 4
\end{bmatrix}
\quad \begin{bmatrix}
7 & 0 & 1 & 5 \\
0 & 1 & 0 \\
2 \\
6 & 0 & 1 & 6
\end{bmatrix}
\]

[Beckermann-Labahn-Villard, 1999; Mulders-Storjohann, 2003]

shifted reduced form:

*arbitrary* degree constraints + **no** column column normalization

\( \approx \) minimal, non-reduced, \( \prec \)-Gröbner basis
## shifted reduced forms

**shift**: integer tuple \( s = (s_1, \ldots, s_m) \) acting as column weights

→ connects Popov and Hermite forms

<table>
<thead>
<tr>
<th>( s )</th>
<th>( \begin{bmatrix} 4 &amp; 3 &amp; 3 &amp; 3 \ 3 &amp; 4 &amp; 3 &amp; 3 \ 3 &amp; 3 &amp; 4 &amp; 3 \ 3 &amp; 3 &amp; 3 &amp; 4 \end{bmatrix} )</th>
<th>( \begin{bmatrix} 7 &amp; 0 &amp; 1 &amp; 5 \ 0 &amp; 1 &amp; 0 &amp; 0 \ 2 &amp; 2 &amp; 2 &amp; 2 \ 6 &amp; 0 &amp; 1 &amp; 6 \end{bmatrix} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s = (0, 0, 0, 0) )</td>
<td>Popov</td>
<td>s-Popov</td>
</tr>
<tr>
<td>( s = (0, 2, 4, 6) )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( s = (0, D, 2D, 3D) )</td>
<td>Hermite</td>
<td></td>
</tr>
</tbody>
</table>

- normal form, average column degree \( D/m \)
- shifted reduced form: same without normalization
- shifts arise naturally in algorithms (approximants, kernel, ...)
shifted reduced forms

shifted forms and degree constraints

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

For \( A = (a_{i,j}) \in K[X]^{m \times n} \), and \( s = (s_1, \ldots, s_n) \in \mathbb{Z}^n \),

\[
\text{rdeg}_s(A) = (\text{rdeg}_s(A_{1,*}), \ldots, \text{rdeg}_s(A_{m,*}))
\]

\[
= \left( \max_{1 \leq j \leq n} (\deg(A_{1,j}) + s_j), \ldots, \max_{1 \leq j \leq n} (\deg(A_{m,j}) + s_j) \right) \in \mathbb{Z}^m
\]

Example: for the matrix \( A = \begin{bmatrix}
3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\
5 & 5X^2 + 3X + 1 & 5X + 3
\end{bmatrix} \),
describe \( \text{rdeg}_{(0,0,0)}(A) \), \( \text{rdeg}_{(0,1,2)}(A) \), and \( \text{rdeg}_{(-1,-3,-2)}(A) \)
shifted reduced forms

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

for $A = (a_{i,j}) \in \mathbb{K}[X]^{m \times n}$, and $s = (s_1, \ldots, s_n) \in \mathbb{Z}^n$,

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

$$= \left( \max_{1 \leq j \leq n} (\deg(A_{1,j}) + s_j), \ldots, \max_{1 \leq j \leq n} (\deg(A_{m,j}) + s_j) \right) \in \mathbb{Z}^m$$

example: for the matrix $A = \begin{bmatrix} 3X + 4 & X^3 + 4X + 1 & 4X^2 + 3 \\ 5 & 5X^2 + 3X + 1 & 5X + 3 \end{bmatrix}$,

describe $rdeg_{(0,0,0)}(A)$, $rdeg_{(0,1,2)}(A)$, and $rdeg_{(-1,-3,-2)}(A)$

- $rdeg_s(A) = rdeg(AX^s)$
- $rdeg_s(A)$ only depends on $s$ and the degrees in $A$
- $rdeg_{s+(c,\ldots,c)}(A) = rdeg_s(A) + c$
shifted reduced forms

shifted forms and degree constraints

notation:
let \( A \in \mathbb{K}[X]^{m \times n} \) with no zero row, and \( s \in \mathbb{Z}^n \),
define \( d = (d_1, \ldots, d_m) = \text{rdeg}_s(A) \)
and \( X^d = \begin{bmatrix} X^{d_1} \\ \vdots \\ X^{d_m} \end{bmatrix} \in \mathbb{K}[X, X^{-1}]^{m \times m} \)

definition: s-leading matrix / s-reduced matrix
assuming \( s \geq 0 \),
- the s-leading matrix of \( A \) is \( \text{lm}_s(A) = \text{lm}(AX^s) \in \mathbb{K}^{m \times n} \)
- \( A \in \mathbb{K}[X]^{m \times n} \) is s-reduced if \( \text{lm}_s(A) \) has full row rank
shifted reduced forms

shifted forms and degree constraints

notation:

let $A \in \mathbb{K}[X]^{m \times n}$ with no zero row, and $s \in \mathbb{Z}^n$,

define $d = (d_1, \ldots, d_m) = \text{rdeg}_s(A)$

and $X^d = \begin{bmatrix} X^{d_1} & \cdots & \cdot & \cdots & X^{d_m} \end{bmatrix} \in \mathbb{K}[X, X^{-1}]^{m \times m}$

definition: $s$-leading matrix / $s$-reduced matrix

assuming $s \geq 0$,

- the $s$-leading matrix of $A$ is $\text{lm}_s(A) = \text{lm}(AX^s) \in \mathbb{K}^{m \times n}$
- $A \in \mathbb{K}[X]^{m \times n}$ is $s$-reduced if $\text{lm}_s(A)$ has full row rank

- these notions are invariant under $s \rightarrow s + (c, \ldots, c)$
- they coincide with the non-shifted case when $s = (0, \ldots, 0)$
- $X^{-d}AX^s = \text{lm}_s(A) + \text{terms of strictly negative degree}$
exercise: for each of the matrices below, and each shift $s$,
1. give the $s$-leading matrix
2. deduce whether the matrix is $s$-reduced

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

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

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

$s = (0, 0, 0), \ s = (0, 5, 6), \ s = (-3, -2, -2)$
the characterizations generalize to the $s$-shifted case, using $s$-row degrees and $s$-leading matrices where appropriate

(proofs: direct, with: $A$ is $s$-reduced $\iff AX^s$ is reduced)

for example recall the predictable degree property:

$A$ is reduced if and only if for any $u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m}$,

$$rdeg(uA) = \max_{1 \leq i \leq m}(\deg(u_i) + rdeg(A_{i,*}))$$
the characterizations generalize to the $s$-shifted case, using $s$-row degrees and $s$-leading matrices where appropriate
(proofs: direct, with: $A$ is $s$-reduced $\iff AX^s$ is reduced)

for example recall the predictable degree property:

$A$ is reduced if and only if for any $u = [u_1 \ldots u_m] \in \mathbb{K}[X]^{1 \times m}$,

\[
\text{rdeg}(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + \text{rdeg}(A_i, *))
\]

- this means $\text{rdeg}(uA) = \text{rdeg}_t(u)$ where $t = \text{rdeg}(A)$
- i.e. $\text{rdeg}(uA) = \text{rdeg}(uX^{\text{rdeg}(A)})$, "no surprising cancellation"
- proof: let $\delta = \text{rdeg}_t(u)$, our goal is to show $\text{rdeg}(uA) = \delta$
  terms of $X^{-\delta}uA$ have degree $\leq 0$,
  and $X^{-\delta}uA = (X^{-\delta}uX^t)(X^{-t}A)$;
  the term of degree 0 is $\text{Im}_t(u)\text{Im}(A)$,
  it is nonzero since $\text{Im}(A)$ has full rank and $\text{Im}_t(u) \neq 0$
  (the case $u = 0$ is trivial)
the characterizations generalize to the \( s \)-shifted case, using \( s \)-row degrees and \( s \)-leading matrices where appropriate

(proofs: direct, with: \( A \) is \( s \)-reduced \( \iff \) \( AX^s \) is reduced)

for example recall the predictable degree property:

**A** is reduced if and only if for any \( u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m} \),

\[
\text{rdeg}(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + \text{rdeg}(A_{i,\ast}))
\]

**A** is \( s \)-reduced if and only if for any \( u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m} \),

\[
\text{rdeg}_s(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + \text{rdeg}_s(A_{i,\ast}))
\]

this means \( \text{rdeg}_s(uA) = \text{rdeg}_t(u) \), where \( t = \text{rdeg}_s(A) \)
the characterizations generalize to the \( s \)-shifted case, using \( s \)-row degrees and \( s \)-leading matrices where appropriate

(proofs: direct, with: \( A \) is \( s \)-reduced \( \iff \) \( AX^s \) is reduced)

for example recall the predictable degree property:

\( A \) is reduced if and only if for any \( u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m} \),
\[
\text{rdeg}(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + \text{rdeg}(A_{i,*}))
\]

\( A \) is \( s \)-reduced if and only if for any \( u = [u_1 \cdots u_m] \in \mathbb{K}[X]^{1 \times m} \),
\[
\text{rdeg}_s(uA) = \max_{1 \leq i \leq m} (\deg(u_i) + \text{rdeg}_s(A_{i,*}))
\]

this means \( \text{rdeg}_s(uA) = \text{rdeg}_t(u) \), where \( t = \text{rdeg}_s(A) \)

- \( s \)-reduced forms provide vectors of minimal \( s \)-degree in the module
- satisfying degree constraints \( (d_1, \ldots, d_m) \Rightarrow \) taking \( s = (-d_1, \ldots, -d_m) \)
- indeed \( \text{cdeg}([p_1 \cdots p_m]) < (d_1, \ldots, d_m) \)
  if and only if \( \text{rdeg}_{(-d_1,\ldots,-d_m)}([p_1 \cdots p_m]) < 0 \)
shifted reduced forms

stability under multiplication

algorithms based on polynomial matrix multiplication


▶ compute a first basis $P_1$ for a subproblem
▶ update the input instance to get the second subproblem
▶ compute a second basis $P_2$ for this second subproblem
▶ the output basis of solutions is $P_2 P_1$

we want $P_2 P_1$ to be reduced:
1. is it implied by “$P_1$ reduced and $P_2$ reduced”?
2. any idea of how to fix this?
shifted reduced forms

stability under multiplication

algorithms based on polynomial matrix multiplication

▷ compute a first basis \( P_1 \) for a subproblem
▷ update the input instance to get the second subproblem
▷ compute a second basis \( P_2 \) for this second subproblem
▷ the output basis of solutions is \( P_2 P_1 \)

we want \( P_2 P_1 \) to be reduced:
1. is it implied by “\( P_1 \) reduced and \( P_2 \) reduced”? 
2. any idea of how to fix this?

we want \( P_2 P_1 \) to be reduced
**theorem:** implied by “\( P_1 \) is reduced and \( P_2 \) is \( t \)-reduced”
where \( t = rdeg(P_1) \)
shifted reduced forms

stability under multiplication

algorithms based on polynomial matrix multiplication


▷ compute a first basis $P_1$ for a subproblem
▷ update the input instance to get the second subproblem
▷ compute a second basis $P_2$ for this second subproblem
▷ the output basis of solutions is $P_2 P_1$

we want $P_2 P_1$ to be reduced:
1. is it implied by “$P_1$ reduced and $P_2$ reduced”?
2. any idea of how to fix this?

we want $P_2 P_1$ to be $s$-reduced

**theorem:** implied by “$P_1$ is $s$-reduced and $P_2$ is $t$-reduced”
where $t = \text{rdeg}_s(P_1)$
let $M \subseteq M_1$ be two $K[X]$-submodules of $K[X]^m$ of rank $m$, let $P_1 \in K[X]^{m \times m}$ be a basis of $M_1$, let $s \in \mathbb{Z}^m$ and $t = \text{rdeg}_s(P_1)$,

- the rank of the module $M_2 = \{ \lambda \in K[X]^{1 \times m} \mid \lambda P_1 \in M \}$ is $m$

and for any basis $P_2 \in K[X]^{m \times m}$ of $M_2$, the product $P_2 P_1$ is a basis of $M$

- if $P_1$ is $s$-reduced and $P_2$ is $t$-reduced, then $P_2 P_1$ is $s$-reduced
shifted reduced forms

stability under multiplication

Let \( \mathcal{M} \subseteq \mathcal{M}_1 \) be two \( \mathbb{K}[X]\)-submodules of \( \mathbb{K}[X]^m \) of rank \( m \), let \( \mathbf{P}_1 \in \mathbb{K}[X]^{m \times m} \) be a basis of \( \mathcal{M}_1 \), let \( s \in \mathbb{Z}^m \) and \( t = \text{rdeg}_s(\mathbf{P}_1) \),

- the rank of the module \( \mathcal{M}_2 = \{ \lambda \in \mathbb{K}[X]^{1 \times m} \mid \lambda \mathbf{P}_1 \in \mathcal{M} \} \) is \( m \) and for any basis \( \mathbf{P}_2 \in \mathbb{K}[X]^{m \times m} \) of \( \mathcal{M}_2 \),
- the product \( \mathbf{P}_2 \mathbf{P}_1 \) is a basis of \( \mathcal{M} \)
- if \( \mathbf{P}_1 \) is \( s \)-reduced and \( \mathbf{P}_2 \) is \( t \)-reduced, then \( \mathbf{P}_2 \mathbf{P}_1 \) is \( s \)-reduced.

Let \( \mathbf{A} \in \mathbb{K}[X]^{m \times m} \) denote the adjugate of \( \mathbf{P}_1 \). Then, we have \( \mathbf{A} \mathbf{P}_1 = \det(\mathbf{P}_1)\mathbf{I}_m \).

Thus, \( p \mathbf{A} \mathbf{P}_1 = \det(\mathbf{P}_1) p \in \mathcal{M} \) for all \( p \in \mathcal{M} \), and therefore \( \mathcal{M} \mathbf{A} \subseteq \mathcal{M}_2 \). Now, the nonsingularity of \( \mathbf{A} \) ensures that \( \mathcal{M} \mathbf{A} \) has rank \( m \); this implies that \( \mathcal{M}_2 \) has rank \( m \) as well (see e.g. [Dummit-Foote 2004, Sec. 12.1, Thm. 4]). The matrix \( \mathbf{P}_2 \mathbf{P}_1 \) is nonsingular since \( \det(\mathbf{P}_2 \mathbf{P}_1) \neq 0 \). Now let \( p \in \mathcal{M} \); we want to prove that \( p \) is a \( \mathbb{K}[X] \)-linear combination of the rows of \( \mathbf{P}_2 \mathbf{P}_1 \). First, \( p \in \mathcal{M}_1 \), so there exists \( \lambda \in \mathbb{K}[X]^{1 \times m} \) such that \( p = \lambda \mathbf{P}_1 \). But then \( \lambda \in \mathcal{M}_2 \), and thus there exists \( \mu \in \mathbb{K}[X]^{1 \times m} \) such that \( \lambda = \mu \mathbf{P}_2 \). This yields the combination \( p = \mu \mathbf{P}_2 \mathbf{P}_1 \).
shifted reduced forms

stability under multiplication

Let \( M \subseteq M_1 \) be two \( \mathbb{K}[X] \)-submodules of \( \mathbb{K}[X]^m \) of rank \( m \),
let \( P_1 \in \mathbb{K}[X]^{m \times m} \) be a basis of \( M_1 \),
let \( s \in \mathbb{Z}^m \) and \( t = \text{rdeg}_s(P_1) \),

- the rank of the module \( M_2 = \{ \lambda \in \mathbb{K}[X]^{1 \times m} \mid \lambda P_1 \in M \} \) is \( m \)
and for any basis \( P_2 \in \mathbb{K}[X]^{m \times m} \) of \( M_2 \),
the product \( P_2P_1 \) is a basis of \( M \)
- if \( P_1 \) is \( s \)-reduced and \( P_2 \) is \( t \)-reduced,
then \( P_2P_1 \) is \( s \)-reduced

Let \( d = \text{rdeg}_t(P_2) \); we have \( d = \text{rdeg}_s(P_2P_1) \) by the predictable degree property. Using \( X^{-d}P_2P_1X^s = X^{-d}P_2X^tX^{-t}P_1X^s \), we obtain that \( \text{Im}_s(P_2P_1) = \text{Im}_t(P_2)\text{Im}_s(P_1) \). By assumption, \( \text{Im}_t(P_2) \) and \( \text{Im}_s(P_1) \) are invertible, and therefore \( \text{Im}_s(P_2P_1) \) is invertible as well; thus \( P_2P_1 \) is \( s \)-reduced.
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

input: vector $F = \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix}$, points $\alpha_1, \ldots, \alpha_d \in K$, shift $s = (s_1, \ldots, s_m) \in \mathbb{Z}^m$

1. $P = \begin{bmatrix} -p_1 \\ \vdots \\ -p_m \end{bmatrix}$ = identity matrix in $K[X]^{m \times m}$

2. for $i$ from 1 to $d$:
   a. evaluate updated vector $\begin{bmatrix} (p_1 \cdot F)(\alpha_i) \\ \vdots \\ (p_m \cdot F)(\alpha_i) \end{bmatrix} = (P \cdot F)(\alpha_i)$
   b. choose pivot $\pi$ with smallest $s_\pi$ such that $(p_\pi \cdot F)(\alpha_i) \neq 0$
      update pivot shift $s_\pi = s_\pi + 1$
   c. eliminate: $\forall j \neq \pi, (p_j \cdot F)(\alpha_i) = 0$
      
      for $j \neq \pi$ do $p_j \leftarrow p_j - \frac{(p_j \cdot F)(\alpha_i)}{(p_\pi \cdot F)(\alpha_i)} p_\pi$; $p_\pi \leftarrow (X - \alpha_i) p_\pi$

after $i$ iterations: $P$ is an $s$-reduced basis of solutions for $(\alpha_1, \ldots, \alpha_i)$
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \), \( m = 4 \), \( s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( F = [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]^{T} \)

iteration: \( i = 1 \), point: \( 24, 31, 15, 32, 83, 27, 20, 59 \)

shift \( \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \)

basis \( \begin{bmatrix} 0 & 2 & 4 & 6 \end{bmatrix} \)

values \( \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 80 & 73 & 73 & 35 & 66 & 46 & 91 & 64 \\ 95 & 91 & 91 & 61 & 88 & 79 & 36 & 22 \\ 34 & 47 & 47 & 1 & 85 & 45 & 75 & 50 \end{bmatrix} \)
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \), \( m = 4 \), \( s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( F = [1 \ L \ L^2 \ L^3]^T \)

iteration: \( i = 1 \)  
point: \( 24, 31, 15, 32, 83, 27, 20, 59 \)

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 2 & 4 & 6 \\
80 & 73 & 73 & 35 & 66 & 46 & 91 & 64 \\
95 & 91 & 91 & 61 & 88 & 79 & 36 & 22 \\
34 & 47 & 47 & 1 & 85 & 45 & 75 & 50 \\
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( F_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \(F = [1 \quad L \quad L^2 \quad L^3]^{T}\)

iteration: \( i = 1 \)  \hspace{1cm} point: \(24, 31, 15, 32, 83, 27, 20, 59\)

\[
\begin{align*}
\text{shift} & \quad [0 \quad 2 \quad 4 \quad 6] \\
\text{basis} & \quad \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
17 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
63 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix} \\
\text{values} & \quad \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 90 & 90 & 52 & 83 & 63 & 11 & 81 & 0 \\
0 & 93 & 93 & 63 & 90 & 81 & 38 & 24 & 0 \\
0 & 13 & 13 & 64 & 51 & 11 & 41 & 16 & 0 \\
\end{bmatrix}
\end{align*}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters:  \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \(F = [1 \ L \ L^2 \ L^3]^T\)

iteration: \(i = 1\)  
point: \(24, 31, 15, 32, 83, 27, 20, 59\)

shift

\[
\begin{bmatrix}
X + 73 \\
17 \\
2 \\
63
\end{bmatrix}
\]

basis

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

values

\[
\begin{bmatrix}
0 & 7 & 88 & 8 & 59 & 3 & 93 & 35 \\
0 & 90 & 90 & 52 & 83 & 63 & 11 & 81 \\
0 & 93 & 93 & 63 & 90 & 81 & 38 & 24 \\
0 & 13 & 13 & 64 & 51 & 11 & 41 & 16
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \(d = 8\), \(m = 4\), \(s = (0, 2, 4, 6)\), base field \(\mathbb{F}_{97}\)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \(\mathbb{F} = \begin{bmatrix} 1 & L & L^2 & L^3 \end{bmatrix}^T\)

iteration: \(i = 2\)  
point: \(24, 31, 15, 32, 83, 27, 20, 59\)

shift

\[
\begin{bmatrix}
X + 73 & 0 & 0 & 0 \\
17 & 1 & 0 & 0 \\
2 & 0 & 1 & 0 \\
63 & 0 & 0 & 1 \\
\end{bmatrix}
\]

values

\[
\begin{bmatrix}
0 & 7 & 88 & 8 & 59 & 3 & 93 & 35 \\
0 & 90 & 90 & 52 & 83 & 63 & 11 & 81 \\
0 & 93 & 93 & 63 & 90 & 81 & 38 & 24 \\
0 & 13 & 13 & 64 & 51 & 11 & 41 & 16 \\
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( \mathbf{F} = [1 \quad L \quad L^2 \quad L^3]^T \)

iteration: \( i = 2 \)  
point: \( 24, 31, 15, 32, 83, 27, 20, 59 \)

shift \[ [1 \quad 2 \quad 4 \quad 6] \]

basis
\[
\begin{bmatrix}
X + 73 & 0 & 0 & 0 \\
X + 90 & 1 & 0 & 0 \\
56X + 16 & 0 & 1 & 0 \\
12X + 66 & 0 & 0 & 1 \\
\end{bmatrix}
\]

values
\[
\begin{bmatrix}
0 & 7 & 88 & 8 & 59 & 3 & 93 & 35 \\
0 & 0 & 81 & 60 & 45 & 66 & 7 & 19 \\
0 & 0 & 74 & 26 & 96 & 55 & 8 & 44 \\
0 & 0 & 2 & 63 & 80 & 47 & 90 & 48 \\
\end{bmatrix}
\]
**fast algorithms**

**iterative algorithm** [van Barel-Bultheel / Beckermann-Labahn]

parameters: \(d = 8\) \(m = 4\) \(s = (0, 2, 4, 6)\), base field \(\mathbb{F}_{97}\)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \(F = [1\ \ L\ \ L^2\ \ L^3]^T\)

iteration: \(i = 2\) point: \(24, 31, 15, 32, 83, 27, 20, 59\)

shift \(\begin{bmatrix} 2 & 2 & 4 & 6 \end{bmatrix}\)

basis \[
\begin{bmatrix}
X^2 + 42X + 65 & 0 & 0 & 0 \\
X + 90 & 1 & 0 & 0 \\
56X + 16 & 0 & 1 & 0 \\
12X + 66 & 0 & 0 & 1
\end{bmatrix}
\]

values \[
\begin{bmatrix}
0 & 0 & 47 & 8 & 61 & 85 & 44 & 10 \\
0 & 0 & 81 & 60 & 45 & 66 & 7 & 19 \\
0 & 0 & 74 & 26 & 96 & 55 & 8 & 44 \\
0 & 0 & 2 & 63 & 80 & 47 & 90 & 48
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \), \( m = 4 \), \( s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: (24, 31, 15, 32, 83, 27, 20, 59) and \( F = [1 \ L \ L^2 \ L^3]^T \)

iteration: \( i = 3 \) point: 24, 31, 15, 32, 83, 27, 20, 59

\[
\begin{align*}
\text{shift} & \quad [2 \ 2 \ 4 \ 6] \\
\text{basis} & \quad \begin{bmatrix}
X^2 + 42X + 65 & 0 & 0 & 0 \\
X + 90 & 1 & 0 & 0 \\
56X + 16 & 0 & 1 & 0 \\
12X + 66 & 0 & 0 & 1 \\
\end{bmatrix} \\
\text{values} & \quad \begin{bmatrix}
0 & 0 & 47 & 8 & 61 & 85 & 44 & 10 \\
0 & 0 & 81 & 60 & 45 & 66 & 7 & 19 \\
0 & 0 & 74 & 26 & 96 & 55 & 8 & 44 \\
0 & 0 & 2 & 63 & 80 & 47 & 90 & 48 \\
\end{bmatrix}
\end{align*}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \( (24, 31, 15, 32, 83, 27, 20, 59) \) and \( \mathbf{F} = [1 \ L \ L^2 \ L^3]^T \)

iteration: \( i = 3 \) \quad point: 24, 31, \textbf{15}, 32, 83, 27, 20, 59

shift

\[
\begin{bmatrix}
3 & 2 & 4 & 6
\end{bmatrix}
\]

basis

\[
\begin{bmatrix}
X^3 + 27X^2 + 17X + 92 & 0 & 0 & 0 \\
54X^2 + 38X + 11 & 1 & 0 & 0 \\
17X^2 + 91X + 54 & 0 & 1 & 0 \\
66X^2 + 68X + 88 & 0 & 0 & 1
\end{bmatrix}
\]

values

\[
\begin{bmatrix}
0 & 0 & 0 & 39 & 74 & 50 & 26 & 52 \\
0 & 0 & 0 & 7 & 41 & 0 & 55 & 74 \\
0 & 0 & 0 & 65 & 66 & 45 & 77 & 20 \\
0 & 0 & 0 & 9 & 32 & 31 & 84 & 29
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( \mathbf{F} = [1 \quad \mathbf{L} \quad \mathbf{L}^2 \quad \mathbf{L}^3]^T \)

iteration: \( i = 4 \)  

point: \( 24, 31, 15, 32, 83, 27, 20, 59 \)

shift

\[
[3 \quad 2 \quad 4 \quad 6]
\]

basis

\[
\begin{bmatrix}
X^3 + 27X^2 + 17X + 92 & 0 & 0 & 0 \\
54X^2 + 38X + 11 & 1 & 0 & 0 \\
17X^2 + 91X + 54 & 0 & 1 & 0 \\
66X^2 + 68X + 88 & 0 & 0 & 1
\end{bmatrix}
\]

values

\[
\begin{bmatrix}
0 & 0 & 0 & 39 & 74 & 50 & 26 & 52 \\
0 & 0 & 0 & 7 & 41 & 0 & 55 & 74 \\
0 & 0 & 0 & 65 & 66 & 45 & 77 & 20 \\
0 & 0 & 0 & 9 & 32 & 31 & 84 & 29
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \quad \text{base field } \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( F = [1 \quad L \quad L^2 \quad L^3]^T \)

iteration: \( i = 4 \)  \quad point: \( 24, 31, 15, 32, 83, 27, 20, 59 \)

shift \[
\begin{bmatrix}
[3 & 3 & 4 & 6]
\end{bmatrix}
\]

basis \[
\begin{bmatrix}
X^3 + 31X^2 + 27X + 3 & 36 & 0 & 0 \\
54X^3 + 56X^2 + 56X + 36 & X + 65 & 0 & 0 \\
56X^2 + 43X + 35 & 60 & 1 & 0 \\
52X^2 + 33X + 60 & 68 & 0 & 1
\end{bmatrix}
\]

values \[
\begin{bmatrix}
0 & 0 & 0 & 0 & 95 & 50 & 66 & 0 \\
0 & 0 & 0 & 0 & 54 & 0 & 19 & 58 \\
0 & 0 & 0 & 0 & 4 & 45 & 79 & 95 \\
0 & 0 & 0 & 0 & 7 & 31 & 41 & 17
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( F = [1 \quad L \quad L^2 \quad L^3]^T \)

iteration: \( i = 5 \) \quad point: \(24, 31, 15, 32, 83, 27, 20, 59\)

\[
\begin{bmatrix}
X^4 + 45X^3 + 73X^2 + 90X + 42 & 36X + 19 & 0 & 0 \\
81X^3 + 20X^2 + 9X + 20 & X + 67 & 0 & 0 \\
2X^3 + 21X^2 + 41 & 35 & 1 & 0 \\
52X^3 + 15X^2 + 79X + 22 & 0 & 0 & 1
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 13 & 13 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 89 & 55 & 58 \\
0 & 0 & 0 & 0 & 0 & 48 & 17 & 95 \\
0 & 0 & 0 & 0 & 0 & 0 & 12 & 78 & 17
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \( (24, 31, 15, 32, 83, 27, 20, 59) \) and \( \mathbf{F} = [1 \quad L \quad L^2 \quad L^3]^T \)

iteration: \( i = 6 \)  

point: 24, 31, 15, 32, 83, 27, 20, 59

\[
\begin{bmatrix}
X^4 + 19X^3 + 57X^2 + 44X + 26 & 74X + 43 & 0 & 0 \\
81X^4 + 64X^3 + 51X^2 + 68X + 42 & X^2 + 40X + 34 & 0 & 0 \\
3X^3 + 44X^2 + 54X + 64 & 6X + 49 & 1 & 0 \\
28X^3 + 45X^2 + 44X + 52 & 50X + 52 & 0 & 1
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 66 & 70 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 13 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 56 & 55 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & 7
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \), \( m = 4 \), \( s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \( \mathbf{F} = [1 \ L \ L^2 \ L^3]^T \)

iteration: \( i = 7 \)  
point: \(24, 31, 15, 32, 83, 27, 20, 59\)

shift \[ \begin{bmatrix} 5 & 4 & 4 & 6 \end{bmatrix} \]

basis
\[
\begin{bmatrix}
X^5 + 96X^4 + 65X^3 + 68X^2 + 19X + 62 & 74X^2 + 18X + 13 & 0 & 0 \\
6X^4 + 94X^3 + 44X^2 + 66X + 32 & X^2 + 19X + 10 & 0 & 0 \\
55X^4 + 78X^3 + 75X^2 + 49X + 39 & 2X + 86 & 1 & 0 \\
13X^4 + 81X^3 + 10X^2 + 34X + 2 & 42X + 29 & 0 & 1
\end{bmatrix}
\]

values
\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 14 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 25 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 44
\end{bmatrix}
\]
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

parameters: \( d = 8 \quad m = 4 \quad s = (0, 2, 4, 6) \), base field \( \mathbb{F}_{97} \)

input: \((24, 31, 15, 32, 83, 27, 20, 59)\) and \(F = [1 \quad L \quad L^2 \quad L^3]^T\)

iteration: \(i = 8\) \quad point: \(24, 31, 15, 32, 83, 27, 20, 59\)

shift \[
\begin{bmatrix}
5 & 5 & 4 & 6 \\
X^5 + 12X^4 + 10X^3 + 34X^2 + 65X + 2 & 60X^2 + 43X + 67 & 0 & 0 \\
6X^5 + 31X^4 + 27X^3 + 89X^2 + 18X + 52 & X^3 + 57X^2 + 53X + 89 & 0 & 0 \\
2X^4 + 56X^3 + 42X^2 + 48X + 15 & 72X^2 + 12X + 30 & 1 & 0 \\
40X^4 + 19X^3 + 14X^2 + 40X + 49 & 53X^2 + 79X + 74 & 0 & 1 \\
\end{bmatrix}
\]

basis \[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

values
fast algorithms

iterative algorithm [van Barel-Bultheel / Beckermann-Labahn]

to be continued...
outline

introduction
- rational approximation and interpolation
- the vector case
- pol. matrices: reminders and motivation

shifted reduced forms
- reducedness: examples and properties
- shifted forms and degree constraints
- stability under multiplication

fast algorithms
- iterative algorithm and output size
- base case: modulus of degree 1
- recursion: residual and basis multiplication

applications
outline

- **introduction**
  - rational approximation and interpolation
  - the vector case
  - pol. matrices: reminders and motivation

- **shifted reduced forms**
  - reducedness: examples and properties
  - shifted forms and degree constraints
  - stability under multiplication

- **fast algorithms**
  - iterative algorithm and output size
  - base case: modulus of degree 1
  - recursion: residual and basis multiplication

- **applications**
  - minimal kernel bases and linear systems
  - fast gcd and extended gcd
  - perspectives
summary

introduction
- rational approximation and interpolation
- the vector case
- pol. matrices: reminders and motivation

shifted reduced forms
- reducedness: examples and properties
- shifted forms and degree constraints
- stability under multiplication

fast algorithms
- iterative algorithm and output size
- base case: modulus of degree 1
- recursion: residual and basis multiplication

applications
- minimal kernel bases and linear systems
- fast gcd and extended gcd
- perspectives