George Labahn, Wei Zhou — University of Waterloo, Canada

Vincent Neiger — Sorbonne University, France

Thi Xuan Vu — The Arctic University of Norway

Rank-sensitive computation of the **rank profile** of a **polynomial matrix**

ISSAC 2022
Villeneuve d'Ascq, France
5th July 2022

outline

- introduction
- context and motivations
- contribution

outline

introduction

- rank profile of a matrix
- rank-sensitive algorithms
- univariate polynomial matrices

context and motivations

contribution

rank profile of a matrix

$m \times n$ matrix $\mathbf{M}$ over some field $\mathbb{K}$

column rank profile of $\mathbf{M}$:
the list of indices $(j_1, \ldots, j_r)$ such that

- r is the rank of $\mathbf{M}$
- columns $1, 2, \ldots, j_i$ of $\mathbf{M}$ have rank i - - - - - → $1 \leqslant j_1 < \cdots < j_r \leqslant n$
- $j_1, \ldots, j_r$ is lexicographically minimal

rank profile of a matrix

$m \times n$ matrix $\mathbf{M}$ over some field $\mathbb{K}$

column rank profile of M:
the list of indices $(j_1, \ldots, j_r)$ such that

- r is the rank of $\mathbf{M}$
- columns $1, 2, \ldots, j_i$ of $\mathbf{M}$ have rank i → $1 \leqslant j_1 < \cdots < j_r \leqslant n$
- $j_1, \ldots, j_r$ is lexicographically minimal

column rank profile ⟷ pivot indices in row echelon form

$\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$, $m = 8$, $n = 8$, $r = 4$, column rank profile $(1, 3, 5, 6)$

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 \\ 2 & 4 & 0 & 1 & 1 & 0 & 0 & 3 \\ 4 & 3 & 2 & 1 & 1 & 4 & 4 & 3 \\ 4 & 3 & 1 & 4 & 4 & 3 & 4 & 1 \\ 0 & 0 & 3 & 1 & 1 & 1 & 1 & 3 \\ 3 & 1 & 3 & 0 & 3 & 3 & 2 & 0 \\ 1 & 2 & 1 & 0 & 4 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 3 \end{bmatrix} \longrightarrow \mathrm{rref}(\mathbf{A}) = \begin{bmatrix} 1 & 2 & 0 & 3 & 0 & 0 & 3 & 2 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 \end{bmatrix}$$

rank profile of a matrix

$m \times n$ matrix $\mathbf{M}$ over some field $\mathbb{K}$

column rank profile of $\mathbf{M}$:
the list of indices $(j_1, \dots, j_r)$ such that

- r is the rank of $\mathbf{M}$
- columns $1, 2, \dots, j_i$ of $\mathbf{M}$ have rank i ⟶ $1 \leqslant j_1 < \cdots < j_r \leqslant n$
- $j_1, \dots, j_r$ is lexicographically minimal

row rank profile ⟷ complemented of column rank profile of left kernel

row rank profile $(1, 2, 3, 4)$

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 \\ 2 & 4 & 0 & 1 & 1 & 0 & 0 & 3 \\ 4 & 3 & 2 & 1 & 1 & 4 & 4 & 3 \\ 4 & 3 & 1 & 4 & 4 & 3 & 4 & 1 \\ 0 & 0 & 3 & 1 & 1 & 1 & 1 & 3 \\ 3 & 1 & 3 & 0 & 3 & 3 & 2 & 0 \\ 1 & 2 & 1 & 0 & 4 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 3 \end{bmatrix} \longrightarrow \mathrm{lker}(\mathbf{A}) = \begin{bmatrix} 0 & 3 & 1 & 0 & 1 & 0 & 0 & 0 \\ 3 & 1 & 3 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 4 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 3 & 0 & 0 & 0 & 1 \end{bmatrix}$$

rank-sensitive algorithms

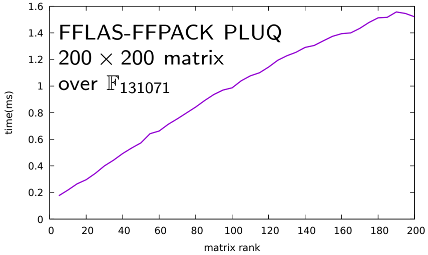
efficient algorithms:

- algebraic complexity → counting operations in the base field $\mathbb{K}$
- software performance → here: single-threaded, $\mathbb{K} = \mathbb{F}_p$ for word-size prime p
- exploit matrix multiplication → $m \times m$ in $O(m^\omega)$ operations in $\mathbb{K}$

rank-sensitive algorithms

efficient algorithms:

- algebraic complexity → counting operations in the base field $\mathbb{K}$
- software performance → here: single-threaded, $\mathbb{K} = \mathbb{F}_p$ for word-size prime p
- exploit matrix multiplication → $m \times m$ in $O(m^\omega)$ operations in $\mathbb{K}$



for **matrix decompositions** (LSP, PLUQ, ...)

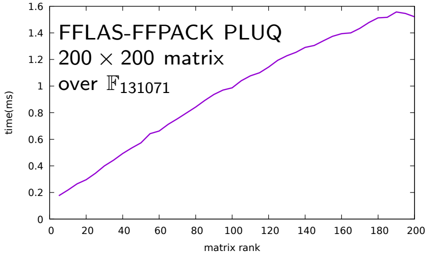
- naive Gaussian elimination $O(rmn)$
- exploiting `MatMul` $O(m^{\omega-1}n)$
- rank-sensitive algorithms $O(r^{\omega-2}mn)$

[Bunch-Hopcroft 1974] [Ibarra-Hui-Moran 1982]
[Storjohann 2000] [Jeannerod 2006]
[Jeannerod-Pernet-Storjohann 2013]
[Dumas-Pernet-Sultan 2015+2017]

rank-sensitive algorithms

efficient algorithms:

- algebraic complexity → counting operations in the base field $\mathbb{K}$
- software performance → here: single-threaded, $\mathbb{K} = \mathbb{F}_p$ for word-size prime p
- exploit matrix multiplication → $m \times m$ in $O(m^\omega)$ operations in $\mathbb{K}$



for **matrix decompositions** (LSP, PLUQ, ...)

- naive Gaussian elimination $O(rmn)$
- exploiting `MatMul` $O(m^{\omega-1}n)$
- rank-sensitive algorithms $O(r^{\omega-2}mn)$

[Bunch-Hopcroft 1974] [Ibarra-Hui-Moran 1982]
[Storjohann 2000] [Jeannerod 2006]
[Jeannerod-Pernet-Storjohann 2013]
[Dumas-Pernet-Sultan 2015+2017]

rank-sensitiveness for "Gauss-based" matrix operations
rank profile, echelon form, linear system, nullspace, ...

for finding the rank profile or solving linear systems: $(r^\omega + mn)^{1+o(1)}$
[H. Y. Cheung, T. C. Kwok, and L. C. Lau. 2013] [Storjohann Yang 2015]

univariate polynomial matrices

$$\mathbf{P} = \begin{bmatrix} 4x^2+3 & x^3+4x+1 & 3x+4 \\ 5x+3 & 5x^2+3x+1 & 5 \\ 2x+1 & 6x+5 & 3x^3+x^2+5x+3 \end{bmatrix} \in \mathbb{K}[x]^{3\times 3}$$

3×3 matrix of degree 3
with entries in $\mathbb{K}[x] = \mathbb{F}_7[x]$

operations on $\mathbb{K}[x]_{<d}^{m\times m}$

- combination of matrix and polynomial computations
- addition in $O(m^2 d)$, naive multiplication in $O(m^3 d^2)$

[Cantor-Kaltofen 1991] [Bostan-Schost 2005] [Harvey-van der Hoeven-Lecerf 2017]

multiplication in $\tilde{O}(m^\omega d)$ operations in $\mathbb{K}$

in general: $O(m^\omega d \log(d) + m^2 d \log(d) \log\log(d))$

univariate polynomial matrices

$$\mathbf{P} = \begin{bmatrix} 4x^2+3 & x^3+4x+1 & 3x+4 \\ 5x+3 & 5x^2+3x+1 & 5 \\ 2x+1 & 6x+5 & 3x^3+x^2+5x+3 \end{bmatrix} \in \mathbb{K}[x]^{3\times 3}$$

3×3 matrix of degree 3
with entries in $\mathbb{K}[x] = \mathbb{F}_7[x]$

operations on $\mathbb{K}[x]^{m\times m}_{<d}$

- combination of matrix and polynomial computations
- addition in $O(m^2 d)$, naive multiplication in $O(m^3 d^2)$

[Cantor-Kaltofen 1991] [Bostan-Schost 2005] [Harvey-van der Hoeven-Lecerf 2017]

multiplication in $O\tilde{~}(m^\omega d)$ operations in $\mathbb{K}$

in general: $O(m^\omega d \log(d) + m^2 d \log(d) \log\log(d))$

various utilizations:

- 2×2 matrices: XGCD, Padé approximation, Berlekamp-Massey, Toeplitz linear systems, ...
- $m \times m$: basis reduction, Hermite-Padé approximation, block-Wiedemann, block-Toeplitz, ...

- some notions and techniques shared with matrices over a field
- some notions and techniques specific to polynomial entries

univariate polynomial matrices

shared with $\mathbb{K}$

multiplication, determinant, rank, rank profile, ...
$\rightsquigarrow$ suitable for evaluation/interpolation

test of nonsingularity for $\mathbf{A} \in \mathbb{K}[x]^{m \times m}$

take random α, and test whether $\det(\mathbf{A}(\alpha)) \neq 0$

- requires large $\mathbb{K}$
- Monte Carlo, without false positives
- cheap, rank sensitive

$\det(\mathbf{A}(\alpha)) = \det(\mathbf{A})(\alpha)$

$O(\mathrm{size}(\mathbf{A}) + r^{\omega-2} m^2)$

specific to $\mathbb{K}[x]$

univariate polynomial matrices

shared with $\mathbb{K}$

multiplication, determinant, rank, rank profile, ...
$\rightsquigarrow$ suitable for evaluation/interpolation

rank profile for $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$

take random α, and return the rank profile of $\mathbf{A}(\alpha)$

- requires large $\mathbb{K}$
- Monte Carlo, no efficient verification
- cheap, rank sensitive

$O(\mathsf{size}(\mathbf{A}) + r^{\omega-2}mn)$

specific to $\mathbb{K}[x]$

univariate polynomial matrices

shared with $\mathbb{K}$

multiplication, determinant, rank, rank profile, ...
$\rightsquigarrow$ suitable for evaluation/interpolation

rank profile for $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$

take random α, and return the rank profile of $\mathbf{A}(\alpha)$

- requires large $\mathbb{K}$
- Monte Carlo, no efficient verification
- cheap, rank sensitive

$O(\mathsf{size}(\mathbf{A}) + r^{\omega-2}mn)$

specific to $\mathbb{K}[x]$

matrix factorizations $\Rightarrow$ divisions + degree growth

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

row operations

$$\begin{bmatrix} 4x^2+3 & x^3+4x+1 & 3x+4 \\ 0 & \frac{2x^4+4x^3+5x^2+5x}{x^2+6} & \frac{3x+1}{x+1} \\ 0 & 0 & \frac{3x^6+4x^4+3x^3+3x+5}{x^3+2x^2+6x+6} \end{bmatrix}$$

univariate polynomial matrices

shared with $\mathbb{K}$

multiplication, determinant, rank, rank profile, ...
$\rightsquigarrow$ suitable for evaluation/interpolation

rank profile for $\mathbf{A} \in \mathbb{K}[x]^{m \times n}$

take random α, and return the rank profile of $\mathbf{A}(\alpha)$

- requires large $\mathbb{K}$
- Monte Carlo, no efficient verification
- cheap, rank sensitive

$O(\text{size}(\mathbf{A}) + r^{\omega-2}mn)$

specific to $\mathbb{K}[x]$

matrix factorizations $\Rightarrow$ divisions + degree growth

- echelonization = Hermite normal form
- column rank profile = pivot positions

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

row operations

$$\begin{bmatrix} 4x^2+3 & x^3+4x+1 & 3x+4 \\ 0 & \frac{2x^4+4x^3+5x^2+5x}{x^2+6} & \frac{3x+1}{x+1} \\ 0 & 0 & \frac{3x^6+4x^4+3x^3+3x+5}{x^3+2x^2+6x+6} \end{bmatrix}$$

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

outline

- introduction
  - rank profile of a matrix
  - rank-sensitive algorithms
  - univariate polynomial matrices
- context and motivations
- contribution

outline

introduction

- rank profile of a matrix
- rank-sensitive algorithms
- univariate polynomial matrices

context and motivations

- polynomial matrices: complexity
- state of the art
- rank-sensitive rank profile: motivations

contribution

polynomial matrices: complexity

reductions of most problems to polynomial matrix multiplication

matrix $m \times m$ of degree d $\rightarrow$ $O\tilde{}(m^\omega d)$

of "**average degree**" $\frac{D}{m}$ $\rightarrow$ $O\tilde{}(m^\omega \frac{D}{m})$

classical matrix operations

- multiplication
- inversion $O\tilde{}(m^3 d)$
- linear system solving
- determinant, rank profile

univariate relations

- syzygies, kernel basis
- Hermite-Padé approximation
- vector rational interpolation
- truncated inverse, QuoRem

transformation to **normal forms**

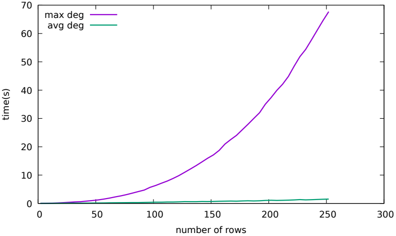
- echelonization: Hermite form
- basis reduction: Popov form
- diagonalization: Smith form

polynomial matrices: complexity

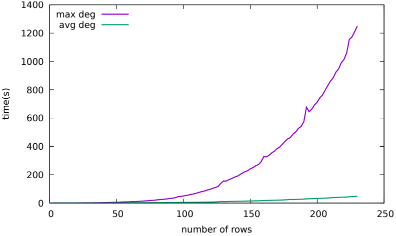
reductions of most problems to polynomial matrix multiplication

matrix $m \times m$ of degree d $\rightarrow$ $O\tilde{}(m^\omega d)$

of "**average degree**" $\frac{D}{m}$ $\rightarrow$ $O\tilde{}(m^\omega \frac{D}{m})$



- Hermite-Padé approximation of $m \times 1$ vector at order 4096
- partial linearization of [Storjohann 2006] and algorithm of [Giorgi-Jeannerod-Villard 2003]
- prototype implementation in PML



- for linear system solving: kernel basis of $2m \times m$ matrix with row degrees $(d, \ldots, d, md)$
- algorithm of [Zhou-Labahn-Storjohann 2012]
- implementation in PML

state of the art

complexity bounds, roughly summarized:

square, nonsingular matrices

- complexity $\approx$ matrix multiplication
- refined with average degree
- arbitrary normal forms

shifted reduced form, shifted Popov form

rectangular or rank-deficient matrices

- cost bounds mostly not rank-sensitive
- degrees are more difficult to control
- main tool: kernel basis

[Zhou-Labahn-Storjohann 2012]

$\mathbf{U}$ unimodular $\Rightarrow [\mathbf{U} \quad \mathbf{I}] \xrightarrow{\text{HNF}} [\mathbf{I} \quad \mathbf{U}^{-1}]$

state of the art

complexity bounds, roughly summarized:

square, nonsingular matrices

- complexity ≈ matrix multiplication
- refined with average degree
- arbitrary normal forms

shifted reduced form, shifted Popov form

rectangular or rank-deficient matrices

- cost bounds mostly not rank-sensitive
- degrees are more difficult to control
- main tool: kernel basis

[Zhou-Labahn-Storjohann 2012]

$\mathbf{U}$ unimodular $\Rightarrow [\mathbf{U} \quad \mathbf{I}] \xrightarrow{\text{HNF}} [\mathbf{I} \quad \mathbf{U}^{-1}]$

- [Mulders-Storjohann 2003] $O(rmnd^2)$
  weak Popov form + rank profile

no fast MatMul or PolMul

- [Storjohann-Villard 2005] $\tilde{O}(r^{\omega-2}mnd)$
  small degree nullspace basis + rank

Las Vegas + no rank profile

- [Zhou 2012] $\tilde{O}(r^{\omega-2}mn\frac{D}{m})$
  ideas for column rank profile

some gaps and missing ingredients

rank-sensitive rank profile: motivations

general impact on polynomial matrices

- faster rank, rank profile, nonsingularity test, ...
- faster kernel basis and linear system solving
- faster row space basis

rank-sensitive rank profile: motivations

general impact on polynomial matrices

- faster rank, rank profile, nonsingularity test, ...
- faster kernel basis and linear system solving
- faster row space basis

impact on normal form computation

- efficient reduction from rank-deficient to full rank
- Hermite normal form: reduction to square, nonsingular
- extension to arbitrary normal forms?
  $\rightsquigarrow$ would require more general pivot profile computation

to each normal form we can associate a specific pivot profile
(for Hermite normal form: pivot profile = column rank profile)
finding the pivot profile = big step towards finding the normal form

rank-sensitive rank profile: motivations

general impact on polynomial matrices

- faster rank, rank profile, nonsingularity test, ...
- faster kernel basis and linear system solving
- faster row space basis

impact on normal form computation

- efficient reduction from rank-deficient to full rank
- Hermite normal form: reduction to square, nonsingular
- extension to arbitrary normal forms?
  $\rightsquigarrow$ would require more general pivot profile computation

specific applications

- verification protocols:
  locate nonsingular $r \times r$ submatrix
- recurrent sequences over $\mathbb{K}[x]/\langle x^\delta \rangle$:
  approximant basis of rank-deficient $m \times km$ matrix

outline

introduction

- rank profile of a matrix
- rank-sensitive algorithms
- univariate polynomial matrices

context and motivations

- polynomial matrices: complexity
- state of the art
- rank-sensitive rank profile: motivations

contribution

outline

introduction

- rank profile of a matrix
- rank-sensitive algorithms
- univariate polynomial matrices

context and motivations

- polynomial matrices: complexity
- state of the art
- rank-sensitive rank profile: motivations

contribution

- improved minimal kernel basis
- rank-sensitive rank profile
- conclusion | perspectives

improved minimal kernel basis

left kernel basis of $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$

- computes $\mathbf{s}$-weak Popov basis $\mathbf{K}$ for $\mathbf{s} = \text{rdeg}(\mathbf{F})$ and column rank profile + r independent rows of $\mathbf{F}$
- complexity $O\tilde{}(m^{\omega-1} n \frac{D}{m})$ when $m \in O(n)$
- support rank-deficient $\mathbf{F}$ and interpolant bases

red = new features compared to [Zhou-Labahn-Storjohann 2012]

improved minimal kernel basis

left kernel basis of $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$

- computes s-weak Popov basis $\mathbf{K}$ for $s = \mathrm{rdeg}(\mathbf{F})$ and column rank profile + r independent rows of $\mathbf{F}$
- complexity $O\tilde{~}(m^{\omega-1} n \frac{D}{m})$ when $m \in O(n)$
- support rank-deficient $\mathbf{F}$ and interpolant bases

red = new features compared to [Zhou-Labahn-Storjohann 2012]

- n small: use fast approximation/interpolation algorithms

⇝ yields at least half the kernel efficiently

⇝ column rank profile is preserved

since $\mathbf{PF} \approx \begin{bmatrix} \mathbf{K}_1\mathbf{F} \\ \mathbf{QF} \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{QF} \end{bmatrix}$

if $n \leqslant \frac{m}{2}$:
  $\mathbf{P} \leftarrow$ approximant/interpolant basis of $\mathbf{F}$ at suitable order
  $\mathbf{K}_1, \mathbf{Q} \leftarrow$ rows of $\mathbf{P}$ which are in $\ker(\mathbf{F})$ / which are not in $\ker(\mathbf{F})$
  $\mathbf{K}_2, (j_1, \ldots, j_r) \leftarrow$ recursive call on $\mathbf{QF}$
  return $\begin{bmatrix} \mathbf{K}_1 \\ \mathbf{K}_2 \end{bmatrix}$ and $(j_1, \ldots, j_r)$

improved minimal kernel basis

left kernel basis of $\mathbf{F} \in \mathbb{K}[x]^{m \times n}$

- computes s-weak Popov basis $\mathbf{K}$ for $s = \text{rdeg}(\mathbf{F})$ and column rank profile + r independent rows of $\mathbf{F}$
- complexity $O\tilde{}(m^{\omega-1} n \frac{D}{m})$ when $m \in O(n)$
- support rank-deficient $\mathbf{F}$ and interpolant bases

red = new features compared to [Zhou-Labahn-Storjohann 2012]

- n large: divide and conquer on n

⇝ classical approach of residual + basis multiplication

⇝ combine rank profiles by concatenation

if $n > \frac{m}{2}$:

$\mathbf{K}_1, (i_1, \ldots, i_r) \leftarrow$ recursive call on first $\frac{n}{2}$ columns of $\mathbf{F}$

$\mathbf{G} \leftarrow$ multiply $\mathbf{K}_1 \cdot$ (last $\frac{n}{2}$ columns of $\mathbf{F}$)

$\mathbf{K}_2, (j_1, \ldots, j_{\hat{r}}) \leftarrow$ recursive call on $\mathbf{G}$

return $\mathbf{K}_2 \mathbf{K}_1$ and $(i_1, \ldots, i_r, \frac{n}{2} + j_1, \ldots, \frac{n}{2} + j_{\hat{r}})$

rank-sensitive rank profile

$$\begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 \\ 2 & 4 & 4 & 4 & 2 & 0 & 4 & 2 \\ 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 \\ 1 & 2 & 3 & 4 & 0 & 0 & 3 & 2 \\ 2 & 4 & 4 & 4 & 2 & 0 & 4 & 2 \\ 1 & 2 & 1 & 0 & 3 & 4 & 3 & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 & 1 & 4 \\ 1 & 2 & 2 & 2 & 3 & 3 & 1 & 1 \\ 4 & 3 & 1 & 4 & 3 & 1 & 1 & 4 \\ 1 & 2 & 4 & 1 & 4 & 1 & 1 & 2 \\ 2 & 4 & 2 & 0 & 3 & 1 & 0 & 0 \\ 3 & 1 & 1 & 1 & 2 & 2 & 1 & 2 \\ 4 & 3 & 4 & 0 & 3 & 3 & 0 & 2 \\ 0 & 0 & 3 & 1 & 4 & 2 & 0 & 4 \end{bmatrix}$$

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  $+$ same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
2	4	4	4	2	0	4	2
1	2	2	2	1	0	2	1
1	2	3	4	0	0	3	2
2	4	4	4	2	0	4	2
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  + same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
2	4	4	4	2	0	4	2
1	2	2	2	1	0	2	1
1	2	3	4	0	0	3	2
2	4	4	4	2	0	4	2
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  + same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	2	2	1	0	2	1
1	2	3	4	0	0	3	2
2	4	4	4	2	0	4	2
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  $+$ same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	3	4	0	0	3	2
2	4	4	4	2	0	4	2
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix
- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  $+$ same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	3	4	0	0	3	2
2	4	4	4	2	0	4	2
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  + same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  + same number of new rows

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

- sketch the strategy on constant matrix

- main subroutine: use left kernel basis to find subset of rows of maximal rank
- apply to current subset of rows
  + same number of new rows

- complexity of one step: $O\tilde{~}(\rho^{\omega-1} n \frac{\Delta}{\rho})$
for ρ the current number of rows
and Δ the current total row degree

- first sort rows by increasing degrees,
then complexity remains controlled
$\rightsquigarrow$ large ρ: fast progression towards $\rho = r$
$\rightsquigarrow$ small ρ: small cost of one step

rank-sensitive rank profile

1	2	2	2	1	0	2	1
[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
1	2	1	0	3	4	3	0
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

→

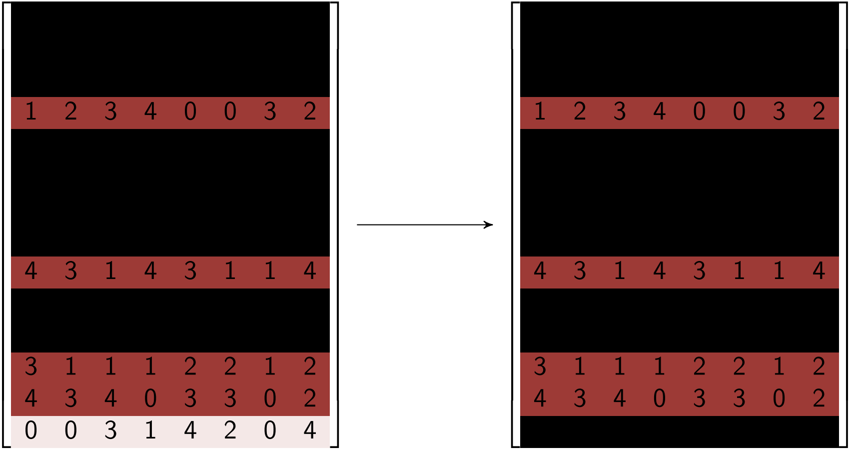
[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

rank-sensitive rank profile

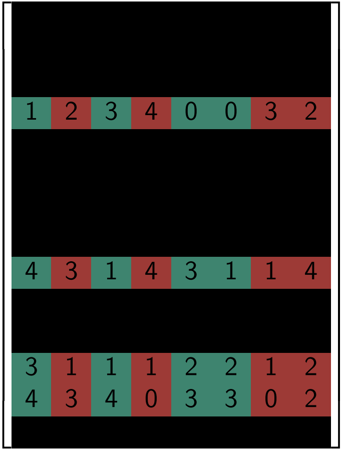
[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
4	3	1	4	3	1	1	4
[redacted]							
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

[redacted]							
1	2	3	4	0	0	3	2
[redacted]							
0	0	0	0	2	4	1	4
1	2	2	2	3	3	1	1
4	3	1	4	3	1	1	4
1	2	4	1	4	1	1	2
2	4	2	0	3	1	0	0
3	1	1	1	2	2	1	2
4	3	4	0	3	3	0	2
0	0	3	1	4	2	0	4

rank-sensitive rank profile



total complexity $\tilde{O}(r^{\omega-2} mn \frac{D}{m})$



column rank profile $(1, 3, 5, 6)$
independent rows $(3, 8, 11, 12)$

- rank-sensitive algorithms bring significant gains
both on complexity and software performance

- generalization of core tool: minimal kernel bases
based on [Zhou-Labahn-Storjohann 2012], not rank sensitive
provides column rank profile + independent rows

- deterministic, rank-sensitive algorithm for the rank profile

summary

conclusion

perspectives

- optimized software implementation
PML: `https://github.com/vneiger/pml`
LinBox: `https://github.com/linbox-team/linbox`

- rank-sensitive row space basis and Hermite normal form

- more generally, shifted Popov forms or pivot profiles?