Computing Submatrices of the Hermite Normal Form of a Structured Polynomial Matrix

Jérémy Berthomieu, Vincent Neiger, Hugo Passe

Sorbonne Université, CNRS, LIP6

17 July 2026, Oldenburg, Germany

Sylvester matrix

Given two polynomials

$$\begin{aligned} f_1 &= (x+72)y^4 + 23y^3 + 22x^3y + 39, \\ f_2 &= x^2y^3 + 25xy^2 + 43x^4y + (54x^4+60). \end{aligned}$$

Their Sylvester matrix:

$$S = \begin{array}{cc} & \begin{array}{ccccc} 1 & y & y^2 & y^3 & y^4 \end{array} \\ \begin{array}{c} f_1 \\ \\ f_2 \\ \\ \end{array} & \begin{bmatrix} 39 & 22x^3 & 0 & 23 & x+72 & & \\ & & & & & & \\ 54x^4+60 & 43x^4 & 25x & x^2 & 0 & & \\ & & & & & & \end{bmatrix} \end{array}$$

Sylvester matrix

Given two polynomials

$$\begin{aligned} f_1 &= (x+72)y^4 + 23y^3 + 22x^3y + 39, \\ f_2 &= x^2y^3 + 25xy^2 + 43x^4y + (54x^4+60). \end{aligned}$$

Their Sylvester matrix:

$$S = \begin{array}{r} \\ f_1 \\ y\,f_1 \\ y^2 f_1 \\ f_2 \\ y\,f_2 \\ y^2 f_2 \\ y^3 f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 \end{array} \\ \begin{bmatrix} 39 & 22x^3 & 0 & 23 & x+72 & 0 & 0 \\ 0 & 39 & 22x^3 & 0 & 23 & x+72 & 0 \\ 0 & 0 & 39 & 22x^3 & 0 & 23 & x+72 \\ 54x^4+60 & 43x^4 & 25x & x^2 & 0 & 0 & 0 \\ 0 & 54x^4+60 & 43x^4 & 25x & x^2 & 0 & 0 \\ 0 & 0 & 54x^4+60 & 43x^4 & 25x & x^2 & 0 \\ 0 & 0 & 0 & 54x^4+60 & 43x^4 & 25x & x^2 \end{bmatrix} \end{array}$$

Sylvester matrix

Given two polynomials

$$f_1 = (x+72)y^4 + 23y^3 + 22x^3y + 39,$$
$$f_2 = x^2y^3 + 25xy^2 + 43x^4y + (54x^4+60).$$

Their Sylvester matrix:

$$S = \begin{array}{r} \\ f_1 \\ y f_1 \\ y^2 f_1 \\ f_2 \\ y f_2 \\ y^2 f_2 \\ y^3 f_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 \end{array} \\ \begin{bmatrix} 39 & 22x^3 & 0 & 23 & x+72 & 0 & 0 \\ 0 & 39 & 22x^3 & 0 & 23 & x+72 & 0 \\ 0 & 0 & 39 & 22x^3 & 0 & 23 & x+72 \\ 54x^4+60 & 43x^4 & 25x & x^2 & 0 & 0 & 0 \\ 0 & 54x^4+60 & 43x^4 & 25x & x^2 & 0 & 0 \\ 0 & 0 & 54x^4+60 & 43x^4 & 25x & x^2 & 0 \\ 0 & 0 & 0 & 54x^4+60 & 43x^4 & 25x & x^2 \end{bmatrix} \end{array}$$

$$\det S = \mathrm{Res}_y(f_1, f_2) = 16x^{21} + 73x^{20} + 7x^{19} + 49x^{18} + 58x^{17} + 3x^{16} + 14x^{15} + \cdots$$

Relation with Gröbner bases

Generically, the lexicographic Gröbner basis of $\langle f_1, f_2 \rangle$ is

$$\mathcal{G}_{\text{lex}} = \{\text{Res}_y(f_1, f_2), y + p(x)\} \, .$$

Relation with Gröbner bases

Generically, the lexicographic Gröbner basis of $\langle f_1, f_2 \rangle$ is

$$\mathcal{G}_{\text{lex}} = \{\text{Res}_y(f_1, f_2), y + p(x)\}.$$

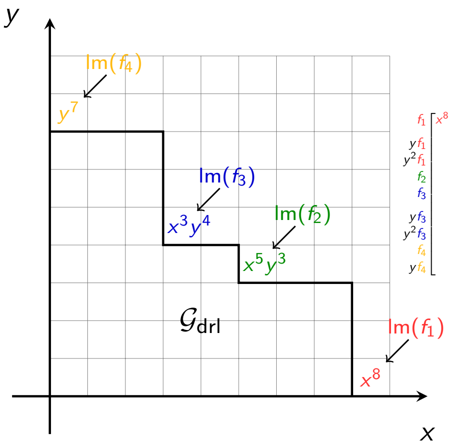
It can be computed via the Hermite normal form of S:

$$\text{HNF}(S) = \begin{array}{c} \\ g_1 \\ g_2 \\ \vdots \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & y & \cdots & \cdots & y^6 \end{array} \\ \begin{bmatrix} \text{Res}_y(f_1, f_2) & 0 & \cdots & \cdots & 0 \\ p(x) & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & \star & & & \\ & & & 1 & 0 \end{bmatrix} \end{array}$$

Change of ordering

Adapted construction from [Macaulay 1903]

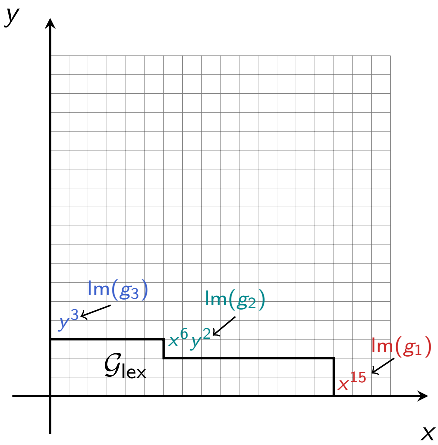
$$(f_1, \ldots, f_\ell) = \mathcal{G}_{\mathrm{drl}} \rightarrow M \in \mathbb{K}[x]^{n \times n} \rightarrow \mathrm{HNF}(M) \rightarrow \mathcal{G}_{\mathrm{lex}}$$



$$\begin{array}{c|ccccccccc}
 & 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 & y^8 \\
\hline
f_1 & x^8+\cdots & \star & \cdots & \cdots & \cdots & \cdots & \star & 0 & 0 \\
y f_1 & 0 & x^8+\cdots & & & & & & & 0 \\
y^2 f_1 & 0 & 0 & x^8+\cdots & \star & \cdots & \cdots & \cdots & \cdots & \star \\
f_2 & \star & \cdots & \star & x^5+\cdots & \star & \cdots & \cdots & \cdots & \star \\
f_3 & \star & \cdots & \cdots & \star & x^3+\cdots & \star & \star & 0 & 0 \\
y f_3 & 0 & & & & & x^3+\cdots & & & 0 \\
y^2 f_3 & 0 & 0 & \star & \cdots & \cdots & \star & x^3+\cdots & \star & \star \\
f_4 & \star & \cdots & \cdots & \cdots & \cdots & \cdots & \star & 1 & 0 \\
y f_4 & 0 & \star & \cdots & \cdots & \cdots & \cdots & \cdots & \star & 1
\end{array}$$

Matrix in $\mathbb{K}[x]^{9 \times 9}$

The 4×4-submatrix of the HNF reveals $\mathcal{G}_{\text{lex}}$



$$\begin{array}{c|ccccccccc}
 & 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 & y^8 \\
\hline
g_1 & x^{15}+\cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
y g_1 & 0 & x^{15}+\cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
g_2 & \star & \star & x^6+\cdots & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
g_3 & \star & \cdots & \star & 1 & 0 & \cdots & \cdots & \cdots & 0 \\
\vdots & \vdots & & & & \ddots & & & & \vdots \\
 & & & & & & & & & 0 \\
 & \star & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \star & 1
\end{array}$$

The other rows give redudant information on

the normal forms of $y^4, y^5, \ldots$

Hermite normal form

Definition

$H \in \mathbb{K}[x]^{n\times n}$ is in row Hermite normal form (HNF) **iff**

- Lower triangular;
- For all $0 \leq i < j < n$, $\deg(H_{i,i}) > \deg(H_{j,i})$.

H is in column HNF **iff** H^{T} is in row HNF.

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

Hermite normal form

Definition

$H \in \mathbb{K}[x]^{n \times n}$ is in row Hermite normal form (HNF) **iff**

- Lower triangular;
- For all $0 \leq i < j < n$, $\deg(H_{i,i}) > \deg(H_{j,i})$.

H is in column HNF **iff** H^{T} is in row HNF.

Theorem

For all $M \in \mathbb{K}[x]^{n \times n}$ there exist

- $U \in \mathbb{K}[x]^{n \times n}$ unimodular,
- $H \in \mathbb{K}[x]^{n \times n}$ in row HNF,

Such that $UM = H$.

Same goes in columns: $MV = H'$.

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

$$\downarrow$$

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

Hermite normal form: complexity

Theorem

For $M \in \mathbb{K}[x]^{n \times n}$, computing $\mathrm{HNF}(M)$ costs $\tilde{O}(n^{\omega} \deg M)$.

[Gupta, Storjohann 2011]
[Labahn, Neiger, Zhou 2017]

Hermite normal form: complexity

Theorem

For $M \in \mathbb{K}[x]^{n \times n}$, computing $\mathrm{HNF}(M)$ costs $\tilde{O}(n^\omega \deg M)$.

[Gupta, Storjohann 2011]
[Labahn, Neiger, Zhou 2017]

Theorem

For $M \in \mathbb{K}[x]^{n \times n}$, computing $\det M$ costs $\tilde{O}(n^\omega \deg M)$.

Hermite normal form: complexity

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\mathrm{HNF}(M)$ costs $\tilde{O}(n^\omega \deg M)$.

[Gupta, Storjohann 2011]
[Labahn, Neiger, Zhou 2017]

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\det M$ costs $\tilde{O}(n^\omega \deg M)$.

Generic case

$$\mathrm{HNF}(M) = \begin{bmatrix} \det M & 0 & \cdots & 0 \\ \star & & & \\ \vdots & & \mathrm{Id}_{n-1} & \\ \star & & & \end{bmatrix}$$

No reason for improvement in general case

Hermite normal form: complexity

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\mathrm{HNF}(M)$ costs $\tilde{O}(n^\omega \deg M)$.

[Gupta, Storjohann 2011]
[Labahn, Neiger, Zhou 2017]

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\det M$ costs $\tilde{O}(n^\omega \deg M)$.

Generic case

$$\mathrm{HNF}(M) = \begin{bmatrix} \det M & 0 & \cdots & 0 \\ \star & & & \\ \vdots & & \mathrm{Id}_{n-1} & \\ \star & & & \end{bmatrix}$$

No reason for improvement in general case

What about structured matrices?

Hermite normal form: complexity

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\mathrm{HNF}(M)$ costs $\tilde{O}(n^\omega \deg M)$.

[Gupta, Storjohann 2011]
[Labahn, Neiger, Zhou 2017]

Theorem

For $M \in \mathbb{K}[x]^{n\times n}$, computing $\det M$ costs $\tilde{O}(n^\omega \deg M)$.

Generic case

$$\mathrm{HNF}(M) = \begin{bmatrix} \det M & 0 & \cdots & 0 \\ \star & & & \\ \vdots & & \mathrm{Id}_{n-1} & \\ \star & & & \end{bmatrix}$$

No reason for improvement in general case

Sylvester matrices
$\tilde{O}(n^2 \deg M)$
[von zur Gathen, Gerhard 1999]
$\tilde{O}(n^{2-\frac{1}{\omega}} \deg M)$
[Villard 2018]

What about structured matrices? General Macaulay matrices?

Structured matrices

We define the matrices

$$Z_0 = \begin{bmatrix} & & & 0 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix}, \quad Z_1^\mathsf{T} = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}$$

and the displacement operator

$$\varphi : M \mapsto Z_0 M - M Z_1^\mathsf{T}.$$

Theorem

The operator φ is invertible.

Corollary

If $\mathrm{rank}(\varphi(M)) = \alpha$, then $\varphi(M) = S^\mathsf{T} T$ with S, T of size $\alpha \times n$.

S and T allow to represent M in $O(\alpha n)$.

Structured matrices

Definition

$\alpha = \mathrm{rank}(\varphi(M))$ is the displacement rank of M and S, T are displacement generators.

When $\alpha \ll n$, M is said to be structured.

$$
\begin{array}{c|ccccccccc|}
 & 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 & y^8 \\
f_1 & x^8+\cdots & \star & & & & & \star & 0 & 0 \\
y f_1 & 0 & x^8+\cdots & & & & & & & 0 \\
y^2 f_1 & 0 & 0 & x^8+\cdots & \star & & & & & \star \\
f_2 & \star & & \star & x^5+\cdots & \star & & & & \star \\
f_3 & \star & & & \star & x^3+\cdots & \star & \star & 0 & 0 \\
y f_3 & 0 & & & & & x^3+\cdots & & & 0 \\
y^2 f_3 & 0 & 0 & \star & & & \star & x^3+\cdots & \star & \star \\
f_4 & \star & & & & & & \star & 1 & 0 \\
y f_4 & 0 & \star & & & & & & \star & 1
\end{array}
$$

$\alpha = 4$

Structured matrices

Definition

$\alpha = \mathrm{rank}(\varphi(M))$ is the displacement rank of M and S, T are displacement generators.

When $\alpha \ll n$, M is said to be structured.

Theorem [Bostan, Mouilleron, Jeannerod, Schost 2017]

Standard linear algebra operations for $n \times n$-matrices of displacement rank α over a field can be done in $\tilde{O}(\alpha^{\omega-1} n)$.

$$
\begin{array}{c}
\\ f_1 \\ y f_1 \\ y^2 f_1 \\ f_2 \\ f_3 \\ y f_3 \\ y^2 f_3 \\ f_4 \\ y f_4
\end{array}
\begin{array}{c}
\begin{array}{ccccccccc} 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 & y^8 \end{array} \\
\left[\begin{array}{ccccccccc}
x^8+\cdots & \star & & & & & \star & 0 & 0 \\
0 & x^8+\cdots & & & & & & & 0 \\
0 & 0 & x^8+\cdots & \star & & & & & \star \\
\star & & \star & x^5+\cdots & \star & & & & \star \\
\star & & & \star & x^3+\cdots & \star & \star & 0 & 0 \\
0 & & & & & x^3+\cdots & & & 0 \\
0 & 0 & \star & & & \star & x^3+\cdots & \star & \star \\
\star & & & & & & \star & 1 & 0 \\
0 & \star & & & & & & \star & 1
\end{array}\right]
\end{array}
$$

$\alpha = 4$

Main contribution

Theorem [B., Neiger, Passe 2026]

Computing a $m \times m$-submatrix of the HNF of an $n \times n$-matrix M with displacement rank α costs

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right)$$

Main contribution

Theorem [B., Neiger, Passe 2026]

Computing a $m \times m$-submatrix of the HNF of an $n \times n$-matrix M with displacement rank α costs

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right)$$

- Δ a degree bound on $\deg\det M + \deg\operatorname{adj} M$

Main contribution

Theorem [B., Neiger, Passe 2026]

Computing a $m \times m$-submatrix of the HNF of an $n \times n$-matrix M with displacement rank α costs

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right)$$

- Δ a degree bound on $\deg \det M + \deg \operatorname{adj} M$
- Las Vegas algorithm

Main contribution

Theorem [B., Neiger, Passe 2026]

Computing a $m \times m$-submatrix of the HNF of an $n \times n$-matrix M with displacement rank α costs

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right)$$

- Δ a degree bound on $\deg \det M + \deg \operatorname{adj} M$
- Las Vegas algorithm
- Structured algorithms: rows / columns of M^{-1}

Main contribution

Theorem [B., Neiger, Passe 2026]

Computing a $m \times m$-submatrix of the HNF of an $n \times n$-matrix M with displacement rank α costs

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right)$$

- Δ a degree bound on $\deg \det M + \deg \operatorname{adj} M$
- Las Vegas algorithm
- Structured algorithms: rows / columns of M^{-1}
- Relation basis over $\mathbb{K}[x]_{\leq \Delta}^{m \times n}$

Algorithm overview

Input:

- Displacement generators $S, T \in \mathbb{K}[x]^{\alpha \times n}$ that represent nonsingular $M \in \mathbb{K}[x]^{n \times n}$
- Degree bounds $D \geq \deg \det M$ and $\bar{D} \geq \deg \operatorname{adj} M$
- $J \subseteq \{1, \ldots, n\}$

Output:

Let H be the row-HNF of M, then the algorithm returns $H_{J,J}$

(Under some mild assumption on J and D)

Algorithm overview: rows of the inverse

Evaluation interpolation

Fast structured linear algebra over a field

$$F = [M^{-1}]_{J,\star} \bmod A(x)$$

Componentwise rational reconstruction

$$q_{i,j} F_{i,j} = p_{i,j} \bmod A(x)$$

Finally, we obtain q, P such that

$$[M^{-1}]_{J,\star} = \frac{1}{q} P.$$

Algorithm overview: relation basis

Definition

For $\mu \in \mathbb{K}[x] \setminus \{0\}$ and $F \in \mathbb{K}[x]^{n\times m}$ the relation module is

$$\mathcal{R}(\mu, F) = \left\{p \in \mathbb{K}[x]^{1\times m} | pF = 0 \bmod \mu\right\}.$$

$\mathcal{R}(\mu, F)$ is a free module of rank m. A basis of $\mathcal{R}(\mu, F)$ is called a relation basis.

With the notations $[M^{-1}]_{J,\star} = \frac{1}{q}P$, B **a relation basis** of $\mathcal{R}(q, P)$,

$$BP = 0 \bmod q \Leftrightarrow BP = Qq \Leftrightarrow B\frac{1}{q}P = Q \Leftrightarrow B = QM_{\star,J}$$

Theorem

If $UM = H$ is the HNF of M, then the HNF of B is $H_{J,J}$.

Contribution with generic properties

Complexity of the algorithm

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right), \qquad \Delta \geq \deg\det M + \deg\operatorname{adj} M$$

$\mathcal{H}_{\mathrm{col}}$: generic column HNF	$\mathcal{H}_{\mathrm{row}}$: generic row HNF
$MV = \begin{bmatrix} \bar{h}_0 & \bar{h}_1 & \cdots & \bar{h}_{n-1} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$	$UM = \begin{bmatrix} h_0 & & & \\ h_1 & 1 & & \\ \vdots & & \ddots & \\ h_{n-1} & & & 1 \end{bmatrix}$

Contribution with generic properties

Complexity of the algorithm

$$\tilde{O}\left(\left(\alpha^{\omega-1} + m^{\omega-1}\right) n\Delta\right), \qquad \Delta \geq \deg\det M + \deg\operatorname{adj} M$$

$\mathcal{H}_{\text{col}}$: generic column HNF	$\mathcal{H}_{\text{row}}$: generic row HNF
$MV = \begin{bmatrix} \bar{h}_0 & \bar{h}_1 & \cdots & \bar{h}_{n-1} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$	$UM = \begin{bmatrix} h_0 & & & \\ h_1 & 1 & & \\ \vdots & & \ddots & \\ h_{n-1} & & & 1 \end{bmatrix}$

Whenever the algorithm detects

- $\mathcal{H}_{\text{row}}$ and $\mathcal{H}_{\text{col}}$, $\tilde{O}(\alpha^{\omega-1} n\Delta)$
- $\mathcal{H}_{\text{col}}$ only, $\tilde{O}(\alpha^{\omega-1} n\Delta + m^{\omega-1} D)$, $\quad D = \deg\det M$
- $\mathcal{H}_{\text{row}}$ only, $\tilde{O}((\alpha^{\omega-1} + m\alpha^{\omega-2}) n\Delta)$

Conclusion and future work

Future work

- Use randomization to tackle rectangular matrices $M \in \mathbb{K}[x]^{n_1 \times n_2}$.
- Use randomization to compute a relation basis of $\mathcal{R}(\mu, F)$ with $F \in \mathbb{K}[x]^{m \times m}$ instead of $\mathbb{K}[x]^{m \times n}$.
- Instead of computing a rational reconstruction $M^{-1}_{J,\star}$, continue working modulo A with smaller degree.

Conclusion and future work

Future work

- Use randomization to tackle rectangular matrices $M \in \mathbb{K}[x]^{n_1 \times n_2}$.
- Use randomization to compute a relation basis of $\mathcal{R}(\mu, F)$ with $F \in \mathbb{K}[x]^{m \times m}$ instead of $\mathbb{K}[x]^{m \times n}$.
- Instead of computing a rational reconstruction $M_{J,\star}^{-1}$, continue working modulo A with smaller degree.

Thank you for your attention!