Computing Elementary Vectors over Integral Domains

Marcus S. Aichmayr
aichmayr@mathematik.uni-kassel.de
joint work with Georg Regensburger

Algorithmic Algebra and Discrete Mathematics
University of Kassel

June 3rd, 2025

UNIKASSEL
VERSITÄT

Motivation

Elementary vectors? $\longrightarrow$ Support-minimal vectors

Applications

- Linear inequality systems
- Division-free kernel matrix
- Sparse basis problem
- Oriented & Linear matroids
- Reaction networks
- $\dots$

Elementary vectors (EVs)

- Integral domain $\mathcal{R}$
- For $x \in \mathcal{R}^n$,

$$\operatorname{supp} x = \{i \in [n] : x_i \neq 0\}.$$

$$[n] = \{1, \dots, n\}$$

$$\operatorname{supp} \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} = \{1, 3\}$$

- Subspace $\mathcal{V}$ (of $\mathcal{R}^n$)

Definition

$v \in \mathcal{V} \setminus \{0\}$ is EV (of $\mathcal{V}$) if for all $x \in \mathcal{V} \setminus \{0\}$,

$$\operatorname{supp} x \subseteq \operatorname{supp} v \implies \operatorname{supp} x = \operatorname{supp} v.$$

$\rightarrow$ Unique up to multiples
  - EVs with $\operatorname{supp} x = \operatorname{supp} y \rightarrow x$, y multiples
  - Finitely many!
- Computation? $\rightarrow$ Maximal minors

Maximal minors

$$P = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix} \to \det \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} = 4 = P(\{2,3\})$$

- $P = (p_1, \dots, p_n) \in \mathcal{R}^{d \times n}$
- $J = \{j_1, \dots, j_d\} \subseteq [n]$ with $j_1 < \dots < j_d$
- Maximal minor:

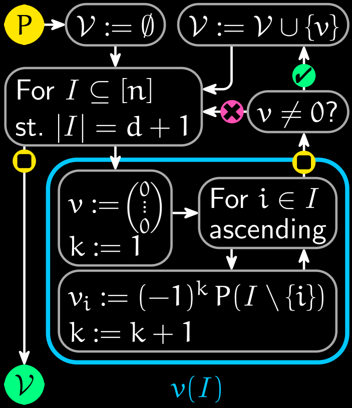
$$P(J) = \det(p_{j_1}, \dots, p_{j_d})$$

→ Compute EVs!

J	$P(J)$
$\{1,2\}$	1
$\{1,3\}$	2
$\{1,4\}$	3
$\{2,3\}$	4
$\{2,4\}$	6
$\{3,4\}$	0

Computing EVs

- $P \in \mathcal{R}^{d \times n}$ with rank d
- $\varepsilon(i) = \pm 1$



Theorem

For $I \subseteq [n]$ with $|I| = d + 1$, $v \in \mathcal{R}^n$:

$$v_i = \begin{cases} \varepsilon(i)\, P(I \setminus \{i\}), & \textit{if } i \in I, \\ 0, & \textit{else.} \end{cases}$$

If $v \neq 0$, then $v \in \ker P$ is EV.

$\rightarrow v(I)$

- How many? $\rightarrow \binom{n}{d+1}$ Finite!

$$P = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

I	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,3,4\}$	$\{2,3,4\}$
$v(I)$	$\begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 6 \\ -3 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ -3 \\ 2 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ -6 \\ 4 \end{pmatrix}$

J	$P(J)$
$\{1,2\}$	1
$\{1,3\}$	2
$\{1,4\}$	3
$\{2,3\}$	4
$\{2,4\}$	6
$\{3,4\}$	0

Parameters

- $P = \begin{pmatrix} 1 & 2 & a & 0 \\ 0 & 1 & 2 & b \end{pmatrix}$
- $a, b \in \mathbb{Z}$

I	$v(I)$	$b = 0$	$a = 4$, $b = 0$
$\{1,2,3\}$	$\begin{pmatrix} 4-a \\ -2 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 4-a \\ -2 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \end{pmatrix}$
$\{1,2,4\}$	$\begin{pmatrix} 2b \\ -b \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
$\{1,3,4\}$	$\begin{pmatrix} ab \\ 0 \\ -b \\ 2 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}$
$\{2,3,4\}$	$\begin{pmatrix} 0 \\ ab \\ -2b \\ 4-a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 4-a \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

J	$P(J)$	$b = 0$	$a = 4$, $b = 0$
$\{1,2\}$	1	1	1
$\{1,3\}$	2	2	2
$\{1,4\}$	b	0	0
$\{2,3\}$	$4-a$	$4-a$	0
$\{2,4\}$	$2b$	0	0
$\{3,4\}$	ab	0	0

$\rightarrow$ Ring of matrix entries

- Algebraic numbers $\overline{\mathbb{Q}}$
- Field extensions $\mathbb{Q}(\sqrt{2})$
- Polynomial rings

- Prevent multiples?

$\rightarrow$ Zero minors!

EVs sharing a maximal minor

$$\mathrm{P} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

- $\mathrm{P} \in \mathcal{R}^{d\times n}$ with rank d
- For $J \subseteq [n]$ with $|J| = d$,

$$\mathcal{V}(J) = \{v(J \cup \{i\}) : i \notin J\} \subseteq \ker \mathrm{P}.$$

J	$\mathrm{P}(J)$
$\{1,2\}$	1
$\{1,3\}$	2
$\{1,4\}$	3
$\{2,3\}$	4
$\{2,4\}$	6
$\{3,4\}$	0

$\mathrm{P}(J) \neq 0$

- $\mathcal{V}(J)$ linearly independent
- $\mathrm{P}(\{1,3\}) = 2 \neq 0$

$$\begin{array}{c|cc} I & \{1,2,3\} & \{1,3,4\} \\ v(I) & \begin{pmatrix} 4 \\ -2 \\ 1 \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ -3 \\ 2 \end{pmatrix} \end{array}$$

→ Sparse basis of $\ker \mathrm{P}$

→ Division-free kernel matrix

$\mathrm{P}(J) = 0$

- $\mathcal{V}(J)$ multiples
- $\mathrm{P}(\{3,4\}) = 0$

$$\begin{array}{c|cc} I & \{1,3,4\} & \{2,3,4\} \\ v(I) & \begin{pmatrix} 0 \\ 0 \\ -3 \\ 2 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ -6 \\ 4 \end{pmatrix} \end{array}$$

→ Prevent multiples!

- Algorithm? → GP identity

Grassmann-Plücker identity

- $P \in \mathcal{R}^{d \times n}$

Theorem
$K, I \subseteq [n]$ *with* $|K| = d - 1$ *and* $|I| = d + 1$. *Then,*

$$\sum_{i \in I \setminus K} \varepsilon(i)\, P(K \cup \{i\})\, P(I \setminus \{i\}) = 0.$$

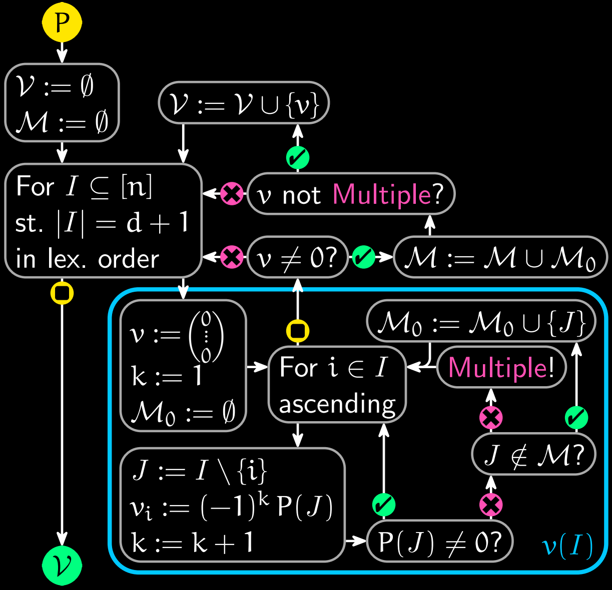
- Proof?
  - For fields?!

→ Laplace expansion!

  - Commutative rings

→ Prevent multiples!

Computing EVs without multiples



Duality

- $P \in \mathcal{R}^{d \times n}$ with rank d

$$\begin{array}{c|cccc} K & \{1\} & \{2\} & \{3\} & \{4\} \\ w(K) & \begin{pmatrix} 0 \\ -1 \\ -2 \\ -3 \end{pmatrix} & \begin{pmatrix} 1 \\ 0 \\ -4 \\ -6 \end{pmatrix} & \begin{pmatrix} 2 \\ 4 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 3 \\ 6 \\ 0 \\ 0 \end{pmatrix} \end{array}$$

Theorem (Row space)

For $K \subseteq [n]$ with $|K| = d - 1$, $w \in \mathcal{R}^n$:

$$w_i = \begin{cases} 0, & \text{if } i \in K, \\ \varepsilon(i)\, P(K \cup \{i\}), & \text{else.} \end{cases}$$

If $w \neq 0$, then $w \in \operatorname{row} P$ is EV.

- Row space? $\rightarrow$ Q with $\ker Q = \operatorname{row} P$

$$P = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix} \rightarrow Q = \begin{pmatrix} 4 & -2 & 1 & 0 \\ 0 & 0 & -3 & 2 \end{pmatrix}$$

J	$P(J)$	$Q([n] \setminus J)$
$\{1,2\}$	1	2
$\{1,3\}$	2	-4
$\{1,4\}$	3	6
$\{2,3\}$	4	8
$\{2,4\}$	6	-12
$\{3,4\}$	0	0

- Maximal minors?
  $\rightarrow$ $P(J) = \varepsilon(J)\, c\, Q([n] \setminus J)$
- Use P directly!

Linear inequality systems

- Matrix A
- Vector x
    - $x > 0$ if all $x_i > 0$.
    - $x \geq 0$ if all $x_i \geq 0$.

Theorem

(1) *Either $Ax > 0$ has a solution; or*

(2) *there is EV $v \in \ker A^\top$ with $v \geq 0$.*

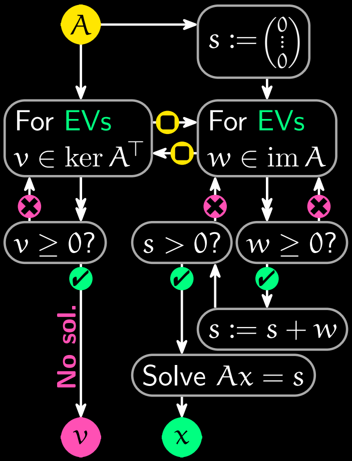
- Can *both* hold?

$$0 = (\underbrace{v^\top A}_{=0})x = \underbrace{v^\top}_{\geq 0}(\underbrace{Ax}_{>0}) > 0 \lightning$$

→ Certificate v

- Compute x? → Sum of EVs
- Parallel (↠)

→ One hash table for minors in $\ker A^\top$ and $\operatorname{im} A$



- No division!
- General systems?

Summary & Outlook

- Elementary vectors
- Applications
  - ✓ Sparse basis problem
  - ✓ Division-free kernel matrix
  - ✓ Linear inequality systems
  - ◦ ...
- Upcoming paper
- SageMath Package
  - ◦ Documentation
  - ◦ Examples
  - → Linear inequality systems
  - → Sign vectors
  - → Oriented matroids

  https://github.com/MarcusAichmayr/elementary_vectors
- Reaction networks

  https://github.com/MarcusAichmayr/sign_vector_conditions