Certifying Solvability of Linear Inequality Systems with Elementary Vectors

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

Algorithmic Algebra and Discrete Mathematics
University of Kassel

September 4th, 2024

Theorems of the alternative

(1) $\boxed{\begin{aligned} Ax &= b \\ x &\geq 0 \end{aligned}}$ *Is (1) solvable?* (2) $\boxed{\begin{aligned} A^\top u &\geq 0 \\ b^\top u &< 0 \end{aligned}}$

- Compute solution
- What if no solution? Certificate?
  - → Dual system

Theorem (Farkas 1902)

Not constructive!

Either (1) or (2) has a solution.

Not both: $0 \overset{(1)(2)}{\leq} x^\top (A^\top u) = (Ax)^\top u \overset{(1)}{=} b^\top u \overset{(2)}{<} 0$ ↯

→ Either (1) or (2) has no solution

- Certify nonexistence for either system
  - → Certify existence!
    - With elementary vectors

Elementary vectors

- $x \in R^n$ with integral domain R

$$\operatorname{supp} x = \{i \mid x_i \neq 0\}$$

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

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

Definition

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

$$\operatorname{supp} x \subseteq \operatorname{supp} v \quad \Longrightarrow \quad \operatorname{supp} x = \operatorname{supp} v.$$

→ Unique up to multiples
  - EVs with $\operatorname{supp} x = \operatorname{supp} y \Longrightarrow x,\ y$ multiples
  - Finitely many EVs (up to multiples)

- *Computation?*

Elementary vectors – Computation

$M = \begin{pmatrix} 1 & \boxed{2} & \boxed{0} & 0 \\ 0 & \boxed{1} & \boxed{2} & 3 \end{pmatrix} \in \mathbb{R}^{d \times n}$

with rank d

Find EVs in $\ker M$*!*

J	$\det M_J$
$\{1,2\}$	1
$\{1,3\}$	2
$\{1,4\}$	3
$\boxed{\{2,3\}}$	$\boxed{4}$
$\{2,4\}$	6
$\{3,4\}$	$\boxed{0}$

Cramer's Rule

I: $\{1,2,3\}$ $\{1,2,4\}$ $\{1,3,4\}$ $\{2,3,4\}$

EV: $\begin{pmatrix} \boxed{4} \\ -2 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 6 \\ -3 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} \boxed{0} \\ 0 \\ -3 \\ 2 \end{pmatrix} \begin{pmatrix} 0 \\ \boxed{0} \\ 6 \\ \boxed{-4} \end{pmatrix}$

Proposition

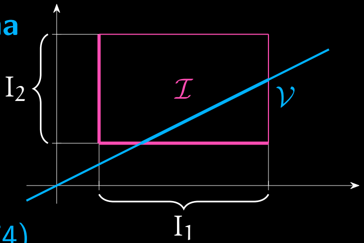
Define $v \in \mathbb{R}^n$ *for* $I \subseteq \{1, \dots, n\}$ *with* $|I| = d + 1$ *by*

$$v_i = \begin{cases} (-1)^{|\{k \in I : k < i\}|} \det M_{I \setminus \{i\}}, & \text{if } i \in I, \\ 0, & \text{else.} \end{cases}$$

Then, $v \in \ker M$ *is EV if* $\operatorname{rank} M_I = d$.

- *How many?* → $\binom{n}{d+1}$ Finitely many!
- Algorithm? → Iterate over all I
- Multiples? → $\boxed{\text{Zero minor}}$ *Prevent multiples?*

Minty's Lemma



- Subspace $\mathcal{V}$
- Intervals $\mathcal{I} = I_1 \times \cdots \times I_m$
- $y \in \mathcal{V} \cap \mathcal{I}$?

Theorem (Rockafellar 1969, Minty 1974)

(1) *Either* $y \in \mathcal{V} \cap \mathcal{I}$ *exists,*

(2) *or EV* $v \in \mathcal{V}^{\perp}$ *exists with* $z^{\top} v \neq 0$ *for all* $z \in \mathcal{I}$.

- *Decide solvability?*
  - Iterate over EVs
  - Certify nonexistence ✓
- *Subspace $\mathcal{V}$?*
  - Use matrix: $\mathcal{V} = \operatorname{im} M$

$$y \in \mathcal{V} \cap \mathcal{I} \longrightarrow Mx \in \mathcal{I}$$

Example

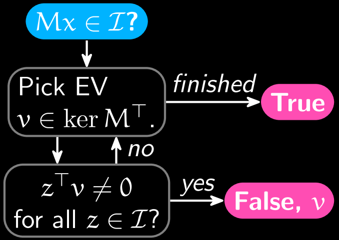
$$\left.\begin{array}{rcrl} -1 \leq x_1 & + & 2x_2 & < 3 \\ 3 < x_1 & - & x_2 & \leq 4 \\ & & x_2 & > 0 \end{array}\right\} \longrightarrow \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix}}_{M} x \in \underbrace{[-1,3) \times (3,4] \times (0,\infty)}_{\mathcal{I}}$$

Minty's Lemma – Algorithm

Corollary

(1) *Either* $Mx \in \mathcal{I}$ *has a solution,*

(2) *or* *EV* $v \in \ker M^\top$ *exists with* $z^\top v \neq 0$ *for all* $z \in \mathcal{I}$.



$$M = \begin{pmatrix} 1 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$\mathcal{I} = [-1, 3) \times (3, 4] \times (0, \infty)$$

```
sage: from vectors_in_intervals import *
sage: exists_vector(M, I)
False
```

```
sage: exists_vector(M, I, certify=True)
(False, (1, -1, -3))
```

Certificate ✓

$$\mathcal{I} = [-1, 3) \times (2, 4] \times (0, \infty)$$

```
sage: exists_vector(M, I)
True
```

Certify existence?

Motzkin's Transposition Theorem

Theorem (Motzkin 1936)

Either (1) or (2) has a solution:

$$(1)\ \boxed{\begin{array}{c} Ax > 0 \\ Bx \geq 0 \\ Cx = 0 \end{array}} \qquad (2)\ \boxed{\begin{array}{cc} \multicolumn{2}{c}{A^\top u + B^\top v + C^\top w = 0} \\ u, v \geq 0, & u \neq 0 \end{array}}$$

$\rightarrow$ General: Linear inequality system $\xrightarrow{\text{homogenize}}$ (1)

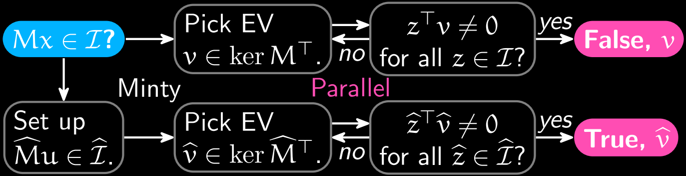
- *Certify?* ◦ Translate (1) and (2).
  ◦ Apply Minty twice!

$$(1')\ \boxed{\begin{pmatrix} A \\ B \\ C \end{pmatrix} x \in (0,\infty)^p \times [0,\infty)^q \times \{0\}^r} \qquad Mx \in \mathcal{I}$$

$$(2')\ \boxed{\begin{pmatrix} A^\top & B^\top & C^\top \\ \mathrm{Id} & 0 & 0 \\ 0 & \mathrm{Id} & 0 \\ 1^\top & 0 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} \in \{0\}^n \times [0,\infty)^{p+q} \times (0,\infty)} \quad \widehat{M} \begin{pmatrix} u \\ v \\ w \end{pmatrix} \in \widehat{\mathcal{I}}$$

Algorithm?

Certifying solvability



- *Pick which EV?*
  - → Iterate over all? – Order?
  - → Random?

Example

```
sage: S = Alternatives(M, I)
sage: S.one.matrix
[ 1  2]
[ 1 -1]
[ 0  1]
sage: S.one.intervals
[[-1, 3), (2, 4], (0, +oo)]
```

```
sage: S.two.matrix
[ 0  0  1  1  1  1]
[ 1  0  0  0  0  0]
[ 0  1  0  0  0  0]
[ 0  0  1  0  0  0]
[ 0  0  0  1  0  0]
[ 0  0  0  0  1  0]
[ 0  0  0  0  0  1]
[-1  1  1 -1  0  0]
[-2 -1  2  1 -1  0]
[-1 -4 -3  2  0 -1]
```

```
sage: S.two.intervals
[(0, +oo),
 [0, +oo),
 [0, +oo),
 [0, +oo),
 [0, +oo),
 [0, +oo),
 [0, +oo),
 {0},
 {0},
 {0}]
```

```
sage: S.certify()
(True, (1, 19, 9, 0, 0, 0, 4, 12, 1, 5), 39)
sage: S.certify(random=True)
(True, (1, 19, 9, 0, 0, 0, 4, 12, 1, 5), 7)
```

Certifying solvability – Analysis

- Where do we compute?
  - Elementary vectors $\longrightarrow$ Determinants
    - Ring of entries of matrices
    - No division!
  - ≥ 0, > 0

$\longrightarrow$ Computable ordered field/ring
  - Integers $\mathbb{Z}$
  - Rationals $\mathbb{Q}$
  - Field extensions, e.g. $\mathbb{Q}(\sqrt{2})$
  - Real algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$
- Runtime
  - High dimensions $\longrightarrow$ Number of minors/EVs explodes
    - 20 variables
  - Number of certificates
  - Order of EVs
  - Parallel

Other approaches?

Other approaches

$$(1)\ \boxed{\begin{aligned} Ax &> 0 \\ Bx &\geq 0 \\ Cx &= 0 \end{aligned}}$$

Is (1) solvable?

$$(2)\ \boxed{\begin{gathered} A^\top u + B^\top v + C^\top w = 0 \\ u, v \geq 0, \qquad u \neq 0 \end{gathered}}$$

- ✓ Certify with EVs
- → Compute solution to certify existence!
  - For either system
- Quantifier elimination
  - MATHEMATICA `Reduce`
    - Crashes (at around 7 variables)
- MATHEMATICA `FindInstance`
  - Fast
  - Heuristics → Unreliable
- Polytopes
  - No strict inequalities – Really?
  - SAGEMATH Polytopes (Polymake)
    - Very fast (over $\mathbb{Q}$) ✓
    - No real algebraic numbers...

$$(1')\ \boxed{\begin{aligned} Ax &\geq 1 \\ Bx &\geq 0 \\ Cx &= 0 \end{aligned}}$$

Summary and outlook

- Certifying linear inequality systems
  - Theorems of the alternative
  - EVs
  - Certificates in ring of matrix entries
- Solution?
  - → (Conformal) sum of EVs?
- Upcoming preprint
- SageMath Package
  - Documentation
  - Examples
  - Elementary vectors
  - Linear inequality systems
  - Sign vectors, oriented matroids:

https://github.com/MarcusAichmayr/elementary_vectors