Certifying solvability of linear inequality systems using elementary vectors

Marcus S. Aichmayr
joint work with Georg Regensburger

Algorithmische Algebra und Diskrete Mathematik
Universität Kassel

1st June 2023

Introduction

- system of linear inequalities
- existence of solution?
- prove that no solution exists? certificate?
- theorems of the alternative

Theorem ([Farkas, 1902])

Let $A \in \mathbb{R}^{m \times n}$ *and* $b \in \mathbb{R}^{n}$*. Exactly one of the following holds:*

(1) *There is* $x \in \mathbb{R}^{n}$ *with* $Ax = b$ *and* $x \geq 0$*.*

(2) *There is* $u \in \mathbb{R}^{m}$ *with* $A^{\top}u \geq 0$ *and* $b^{\top}u < 0$*.*

- algorithmic approach?
  - find certificate?
- over which (computable) field?

Overview

- algorithmic theorem
  - [Rockafellar, 1969], [Minty, 1974]
  - certify non-existence of solution
  - with elementary vectors
- apply to general theorem of the alternative
  - certify existence or non-existence of solution
  - algorithm
  - implementation in SageMath
- construction of solution
  - recursive algorithm

Elementary vectors

R integral domain, $\mathcal{V}$ subspace of R^n

Definition

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

$$\operatorname{supp} y \subseteq \operatorname{supp} x \quad \text{implies} \quad \operatorname{supp} y = \operatorname{supp} x.$$

- uniquely determined by support
- unique up to multiples $\rightsquigarrow$ finitely many EVs
- computation by maximal minors and Cramer's Rule

Example

Given $M = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix}$. Find all EVs in $\ker(M)$.

(1) Compute maximal minors:

$$M_{\{1,2\}} = \det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1, \quad M_{\{2,3\}} = \det\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} = -2,$$

$$M_{\{1,3\}} = \det\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1, \quad M_{\{2,4\}} = \det\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} = 0,$$

$$M_{\{1,4\}} = \det\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = 2, \quad M_{\{3,4\}} = \det\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} = 4$$

(2) Use Cramer's Rule: $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$, $\{2,3,4\}$

EVs: $\begin{pmatrix} -2 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 0 \\ -2 \end{pmatrix} \in \ker(M)$

Constructing elementary vectors

R integral domain, $M \in R^{m \times n}$ with rank m,

Proposition

Let $I \subseteq \{1, \ldots, n\}$ *with* $|I| = m + 1$. *Define* $v \in R^n$ *by*

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

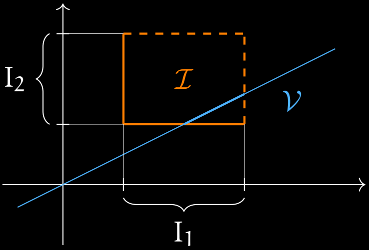
(1) $v \in \ker(M)$. *(Cramer's Rule)*

(2) *If* $\operatorname{rank}(M_I) = m$, *then* v *is EV.*

- compute all EVs
  - iterate over each I
- compute minors once
  - $\binom{n}{m}$ maximal minors
- if all minors non-zero $\rightsquigarrow$ $\binom{n}{m+1}$ EVs (generic case)
- sparse matrices $\rightsquigarrow$ many zero minors $\rightsquigarrow$ less EVs

Minty's Lemma

- computable ordered field $\mathcal{K}$
- subspace $\mathcal{V}$ of $\mathcal{K}^m$
- intervals $\mathcal{I} = I_1 \times \cdots \times I_m \subseteq \mathcal{K}^m$



Is there $x \in \mathcal{V} \cap \mathcal{I}$?

Theorem ([Rockafellar, 1969], [Minty, 1974])

Exactly one of the following holds:

(1) *There is* $x \in \mathcal{V} \cap \mathcal{I}$.

(2) *There is EV* $v \in \mathcal{V}^\perp$ *with* $z^\top v > 0$ *for all* $z \in \mathcal{I}$.

- linear inequality system?

Applying Minty's Lemma

Write linear inequality system as

$$Mx \in \mathcal{I} \qquad \text{with } M \in \mathcal{K}^{m\times n} \text{ and } \mathcal{I} = I_1 \times \cdots \times I_m.$$

Example

$a, b \in \mathcal{K}^n$, $c, d \in \mathcal{K}$

$$\left.\begin{aligned} a^\top x &\le c \\ b^\top x &< d \end{aligned}\right\} \quad \rightsquigarrow \quad \underbrace{\begin{pmatrix} a^\top \\ b^\top \end{pmatrix}}_{M} x \in \underbrace{(-\infty, c] \times (-\infty, d)}_{\mathcal{I}}$$

Corollary

Exactly one of the following holds:

(1) *There is* $x \in \mathcal{K}^n$ *with* $Mx \in \mathcal{I}$.

(2) *There is EV* $v \in \ker(M^\top)$ *with* $z^\top v > 0$ *for all* $z \in \mathcal{I}$.

- EV certifies that no solution exists
- certify existence of solution?

General theorem of the alternative

$A \in \mathcal{K}^{p \times n}$, $B \in \mathcal{K}^{q \times n}$, $C \in \mathcal{K}^{r \times n}$

Theorem (Motzkin's Transposition Theorem [Motzkin, 1936])

Exactly one of the following holds:

(1) *There is* $x \in \mathcal{K}^n$ *with*

$$Ax > 0, \quad Bx \geq 0, \quad Cx = 0.$$

(2) *There is* $(u, v, w) \in \mathcal{K}^{p+q+r}$ *with*

$$A^\top u + B^\top v + C^\top w = 0 \quad \textit{and} \quad u, v \geq 0,\ u \neq 0.$$

- represent linear inequality system as in 1.
- apply Minty's Lemma

Algorithmic theorem of the alternative

$A \in \mathcal{K}^{p\times n}$, $B \in \mathcal{K}^{q\times n}$, $C \in \mathcal{K}^{r\times n}$

Corollary

Exactly one of the following holds:

(1) *There is* $x \in \mathcal{K}^n$ *with*

$$\underbrace{\begin{pmatrix} A \\ B \\ C \end{pmatrix}}_{M} x \in \underbrace{(0,\infty)^p \times [0,\infty)^q \times \{0\}^r}_{\mathcal{I}}.$$

(2) *There is* $(u, v, w) \in \mathcal{K}^{p+q+r}$ *with*

$$\underbrace{\begin{pmatrix} A^\top & B^\top & C^\top \\ \mathrm{Id}_p & 0 & 0 \\ 0 & \mathrm{Id}_q & 0 \\ 1^\top & 0 & 0 \end{pmatrix}}_{\hat{M}} \begin{pmatrix} u \\ v \\ w \end{pmatrix} \in \underbrace{\{0\}^n \times [0,\infty)^{p+q} \times (0,\infty)}_{\hat{\mathcal{I}}}.$$

Certifying solvability

$$
\begin{tikzcd}
 & \text{matrices } A, B, C \arrow[dl] \arrow[dr] & \\
M, \mathcal{I} \arrow[d] & & \hat{M}, \hat{\mathcal{I}} \arrow[d] \\
\text{for all EVs } v \in \ker(M^\top) \arrow[d] & & \text{for all EVs } v \in \ker(\hat{M}^\top) \arrow[d] \\
\text{if } \forall z \in \mathcal{I}\colon z^\top v \neq 0 \arrow[d] & & \text{if } \forall z \in \hat{\mathcal{I}}\colon z^\top v \neq 0 \arrow[d] \\
\boxed{\texttt{False}, v} & & \boxed{\texttt{True}, v}
\end{tikzcd}
$$

Discussing the implementation

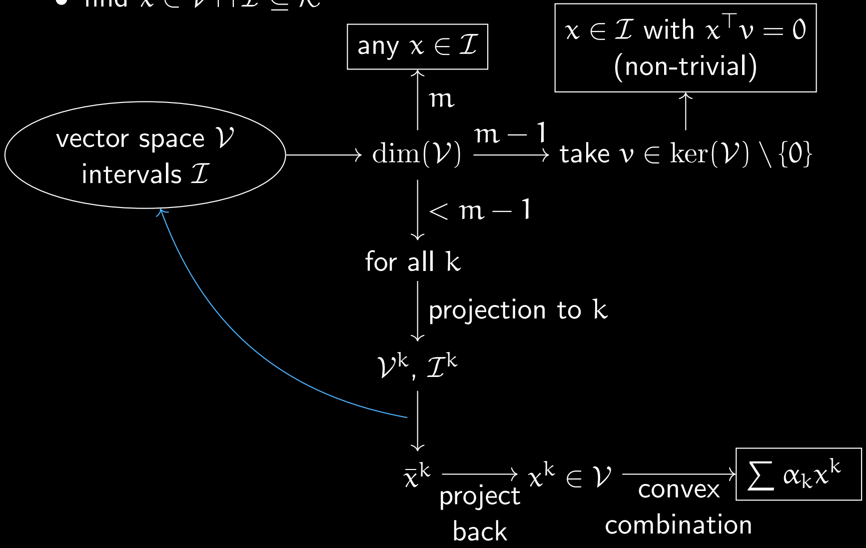
- systems are independent $\rightsquigarrow$ run them in parallel
- exactly one system yields certificate and terminates algorithm
- verify that returned EV certifies result
- works for strict inequalities
- don't compute all EVs
- don't compute all minors
- works over every computable ordered field
- implementation in SageMath
    - runtime depends on
        - dimensions
        - computation of minors
    - upper bound for number of elementary vectors
    - for all implemented ordered fields (e.g. algebraic extensions)
    - fast for rationals
    - `https://github.com/MarcusAichmayr/elementary_vectors`

Other approaches

- difficult to compare directly
- polytopes
  - very fast
  - no strict inequalities
- quantifier elimination (e.g. CAD)
  - either solution or “There is no solution.” (without certificate)
  - apply to both systems
  - Redloq `rlqea`
    - fast
    - certificate (solution) depends on variables
  - Mathematica `Reduce`
    - only for small systems
- Mathematica `FindInstance`
  - heuristics
  - also for larger problems
  - comparable time

Construction of a solution

- constructive proof of Minty's Lemma $\rightsquigarrow$ recursive algorithm
- find $x \in \mathcal{V} \cap \mathcal{I} \subseteq \mathcal{K}^m$



Outlook

- other ways to compute elementary vectors
  - double description method
    - efficient for sparse systems
    - oriented matroids
- improvements of certifying algorithm
  - randomly iterate over elementary vectors
  - use threads to run in parallel
- improvements of recursive algorithm
  - less recursive calls
  - simpler solutions
  - certifying is easier/faster
- `https://github.com/MarcusAichmayr/elementary_vectors`