Termination of linear loops under commutative updates

Ruiwen Dong

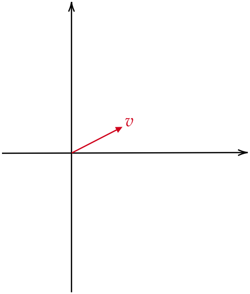
University of Oxford

July 2023

Let's play a game

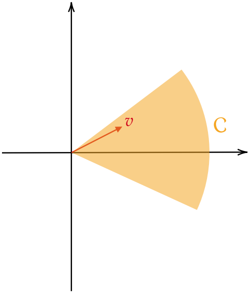
Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$



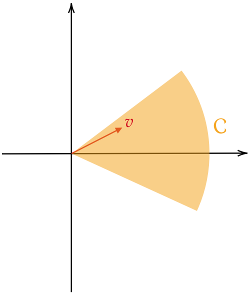
Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$



Let's play a game

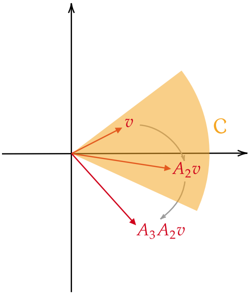
Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathsf{GL}(d, \mathbb{Q})$.



Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

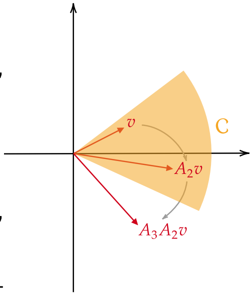
Objective: escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

Objective: escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

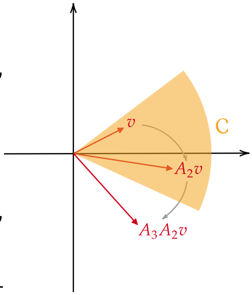
Input: $v \in \mathbb{R}^d$, polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

Output: does there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?
($\langle S \rangle$ denotes the semigroup generated by S.)

Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathsf{GL}(d, \mathbb{Q})$.

Objective: escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

Input: $v \in \mathbb{R}^d$, polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

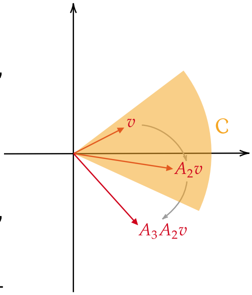
Output: does there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?
($\langle S \rangle$ denotes the semigroup generated by S.)

General case: undecidable.

Let's play a game

Set up: given a vector $v \in \mathbb{R}^d$, a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

Objective: escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

Input: $v \in \mathbb{R}^d$, polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

Output: does there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?
($\langle S \rangle$ denotes the semigroup generated by S.)

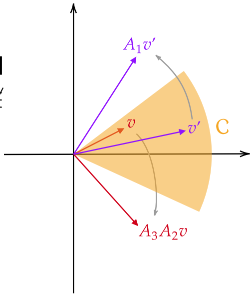
General case: undecidable.

Special case where $\mathrm{card}(S) = 1$: open, subsumes hard problems in Diophantine approximation. (Worrell, Ouaknine 2014)

A "universal" game

Set up: given ~~a vector $v \in \mathbb{R}^d$,~~ a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

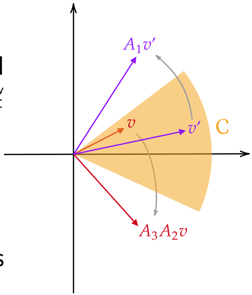
Objective: for every $v \in \mathcal{C}$, escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



A "universal" game

Set up: given ~~a vector $v \in \mathbb{R}^d$,~~ a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

Objective: for every $v \in \mathcal{C}$, escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

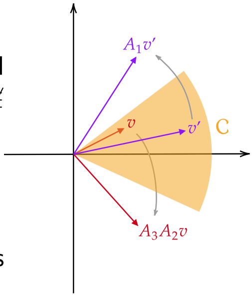
Input: polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

Output: whether for every $v \in \mathcal{C}$, there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?

A "universal" game

Set up: given ~~a vector $v \in \mathbb{R}^d$,~~ a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

Objective: for every $v \in \mathcal{C}$, escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

Input: polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

Output: whether for every $v \in \mathcal{C}$, there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?

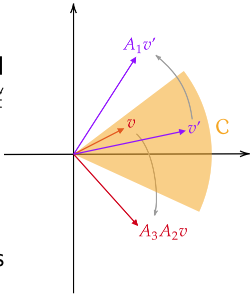
General case: open.

Special case where $\mathrm{card}(S) = 1$: easy using Jordan Normal Form.

A "universal" game

Set up: given ~~a vector $v \in \mathbb{R}^d$,~~ a polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, and a set of linear transformations $S = \{A_1, \ldots, A_n\} \subseteq \mathrm{GL}(d, \mathbb{Q})$.

Objective: for every $v \in \mathcal{C}$, escape $\mathcal{C}$ (find $B_1, \ldots, B_m \in S$, such that $B_1 B_2 \cdots B_m v \notin \mathcal{C}$).



As a decidability problem:

Input: polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d$, matrices $S = \{A_1, \ldots, A_n\}$.

Output: whether for every $v \in \mathcal{C}$, there exist $M \in \langle S \rangle$ such that $Mv \notin \mathcal{C}$?

General case: open.

Special case where card$(S) = 1$: easy using Jordan Normal Form.

Motivation: verify termination of linear programs.

Termination of linear loops

Let's consider the complement of the previous problem:

Definition

Termination of linear loops is the following decision problem.
Input: a closed polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d \setminus \{0^d\}$ generated by rational vectors, a set of matrices $S \subseteq \mathrm{GL}(d, \mathbb{Q})$.
Output: whether there exists $v \in \mathcal{C}$, such that $\langle S \rangle \cdot v \subseteq \mathcal{C}$?

Termination of linear loops

Let's consider the complement of the previous problem:

Definition

Termination of linear loops is the following decision problem.
Input: a closed polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d \setminus \{0^d\}$ generated by rational vectors, a set of matrices $S \subseteq \mathrm{GL}(d, \mathbb{Q})$.
Output: whether there exists $v \in \mathcal{C}$, such that $\langle S \rangle \cdot v \subseteq \mathcal{C}$?

Theorem

Termination of linear loops is decidable for **commuting matrices***.*

Termination of linear loops

Let's consider the complement of the previous problem:

Definition

Termination of linear loops is the following decision problem.
Input: a closed polyhedral cone $\mathcal{C} \subseteq \mathbb{R}^d \setminus \{0^d\}$ generated by rational vectors, a set of matrices $S \subseteq \mathrm{GL}(d, \mathbb{Q})$.
Output: whether there exists $v \in \mathcal{C}$, such that $\langle S \rangle \cdot v \subseteq \mathcal{C}$?

Theorem

Termination of linear loops is decidable for **commuting matrices***.*

In other words, let $S = \{A_1, \ldots, A_n\}$ be a set of pairwise commuting matrices. It is decidable whether there exists v, such that

$$A_1^{k_1} A_2^{k_2} \cdots A_n^{k_n} v \in \mathcal{C} \quad \text{for all } k_1, \ldots, k_n \in \mathbb{N}.$$

Proof idea. Step 1: dual problem

Suppose $\mathcal{C}$ is defined by

$$\{x \in \mathbb{R}^d \setminus \{0^d\} \mid c_1^\top x \geq 0, \ldots, c_m^\top x \geq 0\},$$

where $c_1, \ldots, c_m \in \mathbb{R}^d$.

Proof idea. Step 1: dual problem

Suppose $\mathcal{C}$ is defined by

$$\{x \in \mathbb{R}^d \setminus \{0^d\} \mid c_1^\top x \geq 0, \ldots, c_m^\top x \geq 0\},$$

where $c_1, \ldots, c_m \in \mathbb{R}^d$.

Termination of linear loops

$\iff$ there exists $v \in \mathbb{R}^d$, s.t. $A_1^{k_1} \cdots A_n^{k_n} v \in \mathcal{C}$ for all $k_1, \ldots, k_n \in \mathbb{N}$

Proof idea. Step 1: dual problem

Suppose $\mathcal{C}$ is defined by

$$\{x \in \mathbb{R}^d \setminus \{0^d\} \mid c_1^\top x \geq 0, \ldots, c_m^\top x \geq 0\},$$

where $c_1, \ldots, c_m \in \mathbb{R}^d$.

Termination of linear loops

$\iff$ there exists $v \in \mathbb{R}^d$, s.t. $A_1^{k_1} \cdots A_n^{k_n} v \in \mathcal{C}$ for all $k_1, \ldots, k_n \in \mathbb{N}$

$\iff$ there exists $v \in \mathbb{R}^d$, s.t. $c_i^\top A_1^{k_1} \cdots A_n^{k_n} v \geq 0$ for all $i = 1, \ldots, m$, and $k_1, \ldots, k_n \in \mathbb{N}$

Proof idea. Step 1: dual problem

Suppose $\mathcal{C}$ is defined by

$$\{x \in \mathbb{R}^d \setminus \{0^d\} \mid c_1^\top x \geq 0, \ldots, c_m^\top x \geq 0\},$$

where $c_1, \ldots, c_m \in \mathbb{R}^d$.

$$\begin{aligned}
& \text{Termination of linear loops} \\
\iff & \text{there exists } v \in \mathbb{R}^d, \text{ s.t. } A_1^{k_1} \cdots A_n^{k_n} v \in \mathcal{C} \text{ for all } k_1, \ldots, k_n \in \mathbb{N} \\
\iff & \text{there exists } v \in \mathbb{R}^d, \text{ s.t. } c_i^\top A_1^{k_1} \cdots A_n^{k_n} v \geq 0 \text{ for all } i = 1, \ldots, m, \\
& \text{and } k_1, \ldots, k_n \in \mathbb{N} \\
\iff & {A_n^\top}^{k_n} \cdots {A_1^\top}^{k_1} c_i \text{ are in some closed } \textbf{halfspace } \mathcal{H} := \{x \mid v^\top x \geq 0\} \\
& \text{for all } i = 1, \ldots, m, k_1, \ldots, k_n \in \mathbb{N}
\end{aligned}$$

Proof idea. Step 1: dual problem

Suppose $\mathcal{C}$ is defined by

$$\{x \in \mathbb{R}^d \setminus \{0^d\} \mid c_1^\top x \geq 0, \ldots, c_m^\top x \geq 0\},$$

where $c_1, \ldots, c_m \in \mathbb{R}^d$.

Termination of linear loops

$\iff$ there exists $v \in \mathbb{R}^d$, s.t. $A_1^{k_1} \cdots A_n^{k_n} v \in \mathcal{C}$ for all $k_1, \ldots, k_n \in \mathbb{N}$

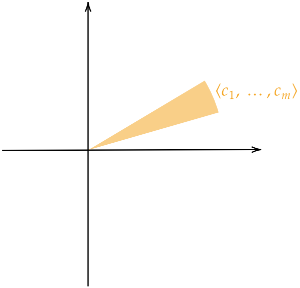
$\iff$ there exists $v \in \mathbb{R}^d$, s.t. $c_i^\top A_1^{k_1} \cdots A_n^{k_n} v \geq 0$ for all $i = 1, \ldots, m$, and $k_1, \ldots, k_n \in \mathbb{N}$

$\iff$ ${A_n^\top}^{k_n} \cdots {A_1^\top}^{k_1} c_i$ are in some closed **halfspace** $\mathcal{H} := \{x \mid v^\top x \geq 0\}$ for all $i = 1, \ldots, m, k_1, \ldots, k_n \in \mathbb{N}$

Let $S^\top := \{A_1^\top, \ldots, A_n^\top\}$. Denote by $\langle c_1, \ldots, c_m \rangle$ the cone generated by $c_1, \ldots, c_m$. It suffices to decide whether the orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace.

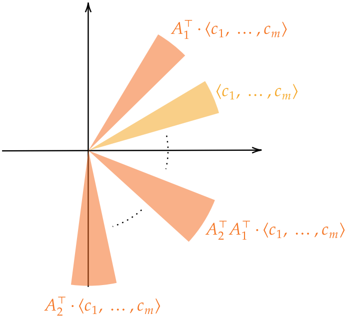
Proof idea. Step 2: halfspace

It suffices to decide whether the orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace.



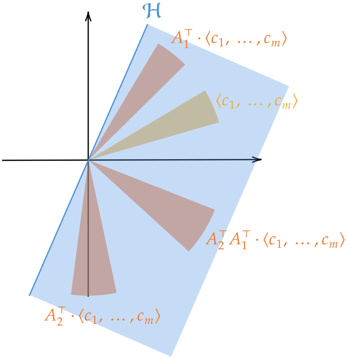
Proof idea. Step 2: halfspace

It suffices to decide whether the orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace.



Proof idea. Step 2: halfspace

It suffices to decide whether the orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace.



Proof idea. Step 3: salient cone

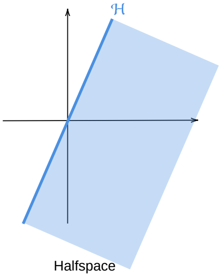
Instead of deciding whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace, we first decide whether it is **salient**.

Proof idea. Step 3: salient cone

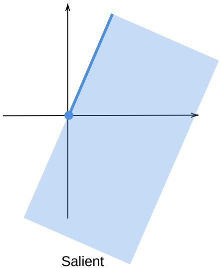
Instead of deciding whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace, we first decide whether it is **salient**.

Definition

A cone $C \subseteq \mathbb{R}^d$ is called *salient* if $x, -x \in \mathcal{C} \implies x = 0^d$.
A set $\mathcal{O} \subseteq \mathbb{R}^d$ is called *salient* if the cone it generates is salient.



Halfspace



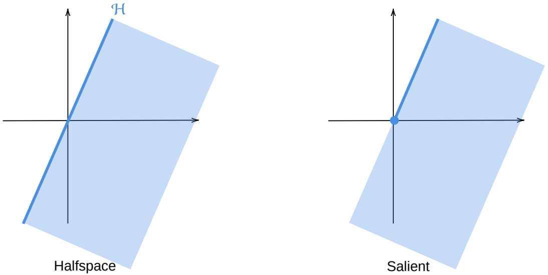
Salient

Proof idea. Step 3: salient cone

Instead of deciding whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ lies in a closed halfspace, we first decide whether it is **salient**.

Definition

A cone $C \subseteq \mathbb{R}^d$ is called *salient* if $x, -x \in \mathcal{C} \implies x = 0^d$.
A set $\mathcal{O} \subseteq \mathbb{R}^d$ is called *salient* if the cone it generates is salient.



Lemma

Suppose we have a procedure that decides whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is salient, then we can decide whether it is contained in a closed halfspace.

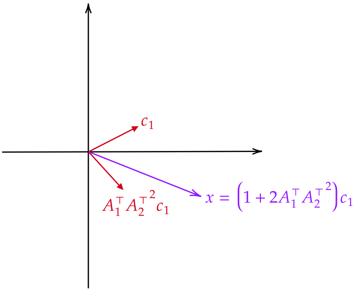
Step 4: from salient cone to positive polynomials

Now it suffices to whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is salient. That is, whether there exist $x \neq 0^d$ such that both x and $-x$ are in the cone generated by $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$.

Step 4: from salient cone to positive polynomials

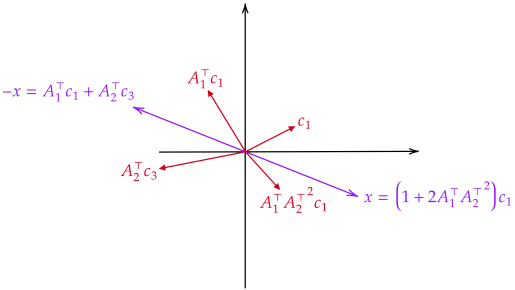
Now it suffices to whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is salient. That is, whether there exist $x \neq 0^d$ such that both x and $-x$ are in the cone generated by $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$.

Suppose such x exists, for example, $x = c_1 + 2A_1^\top {A_2^\top}^2 c_1$.



Now it suffices to whether $\langle S^\top \rangle \cdot \langle c_1, \dots, c_m \rangle$ is salient. That is, whether there exist $x \neq 0^d$ such that both x and $-x$ are in the cone generated by $\langle S^\top \rangle \cdot \langle c_1, \dots, c_m \rangle$.

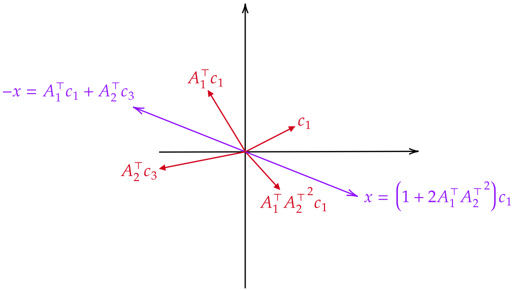
Suppose such x exists, for example, $x = c_1 + 2A_1^\top {A_2^\top}^2 c_1$.
Similarly, say, $-x = A_1^\top c_1 + A_2^\top c_3$.



Step 4: from salient cone to positive polynomials

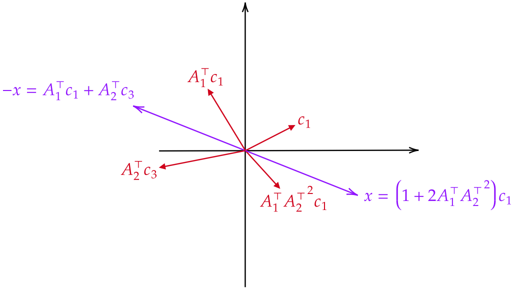
Now it suffices to whether $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is salient. That is, whether there exist $x \neq 0^d$ such that both x and $-x$ are in the cone generated by $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$.

Suppose such x exists, for example, $x = c_1 + 2A_1^\top {A_2^\top}^2 c_1$.
Similarly, say, $-x = A_1^\top c_1 + A_2^\top c_3$.



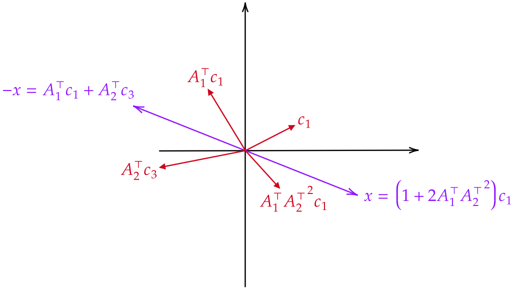
Then $0^d = (1 + A_1^\top + 2A_1^\top {A_2^\top}^2) \cdot c_1 + A_2^\top \cdot c_3$.

Step 4: from salient cone to positive polynomials



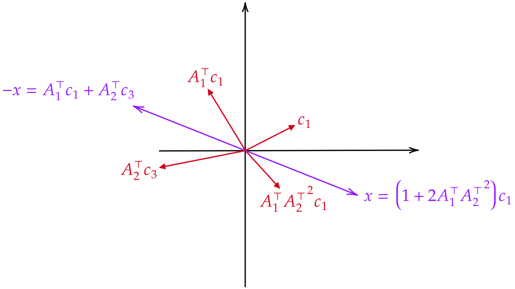
Then $0^d = (1 + A_1^\top + 2A_1^\top {A_2^\top}^2) \cdot c_1 + A_2^\top \cdot c_3$.

Step 4: from salient cone to positive polynomials



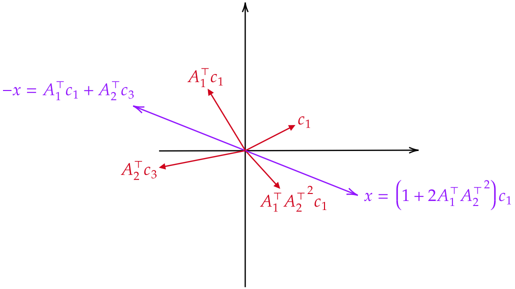
Then $0^d = \underbrace{(1 + A_1^\top + 2A_1^\top {A_2^\top}^2)}_{\text{polynomials over } A_1^\top,\, A_2^\top} \cdot c_1 + \underbrace{A_2^\top} \cdot c_3$.

Step 4: from salient cone to positive polynomials



Then $0^d = \underbrace{(1 + A_1^\top + 2A_1^\top {A_2^\top}^2)}_{\text{polynomials over } A_1^\top, A_2^\top \text{ with \textbf{positive} coefficients}} \cdot c_1 + \underbrace{A_2^\top} \cdot c_3.$

Step 4: from salient cone to positive polynomials



Then $0^d = \underbrace{\left(1 + A_1^\top + 2A_1^\top {A_2^\top}^2\right)}_{\text{polynomials over } A_1^\top, A_2^\top \text{ with positive coefficients}} \cdot c_1 + \underbrace{A_2^\top} \cdot c_3.$

Proposition

The orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is not salient if and only if there exist "positive polynomials" $f_1, \ldots, f_m \in \mathbb{R}_{\geq 0}[X_1, \ldots, X_n]$, not all zero, such that $0^d = f_1(A_1^\top, \ldots, A_n^\top) \cdot c_1 + \cdots + f_m(A_1^\top, \ldots, A_n^\top) \cdot c_m$.

Step 5: positive polynomial in a module

Let $\mathcal{M}$ be the $\mathbb{R}[X_1, \dots, X_n]$-submodule of $\mathbb{R}[X_1, \dots, X_n]^m$ consisting of all tuples $(f_1, \dots, f_m)$ such that

$$0^d = f_1(A_1^\top, \dots, A_n^\top) \cdot c_1 + \cdots + f_m(A_1^\top, \dots, A_n^\top) \cdot c_m.$$

Step 5: positive polynomial in a module

Let $\mathcal{M}$ be the $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$ consisting of all tuples $(f_1, \ldots, f_m)$ such that

$$0^d = f_1(A_1^\top, \ldots, A_n^\top) \cdot c_1 + \cdots + f_m(A_1^\top, \ldots, A_n^\top) \cdot c_m.$$

Proposition

The orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is not salient if and only if

$$\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n])^m \neq \{0^m\}.$$

Step 5: positive polynomial in a module

Let $\mathcal{M}$ be the $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$ consisting of all tuples $(f_1, \ldots, f_m)$ such that

$$0^d = f_1(A_1^\top, \ldots, A_n^\top) \cdot c_1 + \cdots + f_m(A_1^\top, \ldots, A_n^\top) \cdot c_m.$$

Proposition

The orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ *is not salient if and only if*

$$\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n])^m \neq \{0^m\}.$$

Proposition ("multivariate", "*m*-dimensional" Cayley-Hamilton theorem)

A finite set of generators for $\mathcal{M}$ *can be effectively computed.*

Step 5: positive polynomial in a module

Let $\mathcal{M}$ be the $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$ consisting of all tuples $(f_1, \ldots, f_m)$ such that

$$0^d = f_1(A_1^\top, \ldots, A_n^\top) \cdot c_1 + \cdots + f_m(A_1^\top, \ldots, A_n^\top) \cdot c_m.$$

Proposition

The orbit $\langle S^\top \rangle \cdot \langle c_1, \ldots, c_m \rangle$ is not salient if and only if

$$\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n])^m \neq \{0^m\}.$$

Proposition ("multivariate", "m-dimensional" Cayley-Hamilton theorem)

A finite set of generators for $\mathcal{M}$ can be effectively computed.

Proof idea: the characteristic polynomials of $A_1^\top, \ldots, A_n^\top$ are in $\mathcal{M}$. The module $\mathbb{R}[X_1, \ldots, X_n]^m$ becomes finite dimensional $\mathbb{R}$-linear space after quotient by these characteristic polynomials, the rest is linear algebra.

Step 6: local-global principle by Einsiedler et al.

It suffices to decide whether $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty.

Step 6: local-global principle by Einsiedler et al.

It suffices to decide whether $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty.

Example: suppose polynomials are univariate and $\mathcal{M}$ is the solution set of the linear equation

$$0 = f_1 \cdot (2X^2 - 1) + f_2 \cdot (X + 2). \tag{1}$$

i.e. does (1) have solution $f_1, f_2 \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$?

Step 6: local-global principle by Einsiedler et al.

It suffices to decide whether $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty.

Example: suppose polynomials are univariate and $\mathcal{M}$ is the solution set of the linear equation

$$0 = f_1 \cdot (2X^2 - 1) + f_2 \cdot (X + 2). \tag{1}$$

i.e. does (1) have solution $f_1, f_2 \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_1(1) + 3f_2(1)$. No solution over $\mathbb{R}_{>0}$.

Step 6: local-global principle by Einsiedler et al.

It suffices to decide whether $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty.

Example: suppose polynomials are univariate and $\mathcal{M}$ is the solution set of the linear equation

$$0 = f_1 \cdot (2X^2 - 1) + f_2 \cdot (X + 2). \tag{1}$$

i.e. does (1) have solution $f_1, f_2 \in \mathbb{R}_{\geq 0}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_1(1) + 3f_2(1)$. No solution over $\mathbb{R}_{>0}$.

If $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty, such "certificate" always exists!

Theorem (Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ if and only if:

1. *For every $r \in \mathbb{R}^n_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^m_{>0}$.*
2. *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f}_v \in \mathcal{M}$, whose initial polynomial $\mathrm{in}_v(\boldsymbol{f}_v)$ is in $(\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$.*

Step 6: local-global principle by Einsiedler et al.

Theorem (Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ if and only if:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^m_{>0}$.*
2. *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f}_v \in \mathcal{M}$, whose initial polynomial $\mathrm{in}_v(\boldsymbol{f}_v)$ is in $(\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$.*

Step 6: local-global principle by Einsiedler et al.

Theorem (Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ if and only if:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^m_{>0}$.*
2. *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f}_v \in \mathcal{M}$, whose initial polynomial $\mathrm{in}_v(\boldsymbol{f}_v)$ is in $(\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$.*

Condition 1 can be checked using the first order theory of the reals.

Step 6: local-global principle by Einsiedler et al.

Theorem (Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{R}[X_1, \ldots, X_n]$-submodule of $\mathbb{R}[X_1, \ldots, X_n]^m$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ if and only if:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^m_{>0}$.*
2. *For every $v \in (\mathbb{R}^n)^*$, there exists $\boldsymbol{f}_v \in \mathcal{M}$, whose initial polynomial $\mathrm{in}_v(\boldsymbol{f}_v)$ is in $(\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$.*

Condition 1 can be checked using the first order theory of the reals.

Condition 2 only needs to be checked for a finite number of v (consider the Newton polytopes of a Gröbner basis of $\mathcal{M}$).

Corollary

Given a finite set of generators for the $\mathbb{R}[X_1, \ldots, X_n]$-submodule $\mathcal{M}$ of $\mathbb{R}[X_1, \ldots, X_n]^m$, it is decidable whether $\mathcal{M} \cap (\mathbb{R}_{\geq 0}[X_1, \ldots, X_n]^*)^m$ is empty.

Conclusion

Termination of linear loops with commuting matrices $\longleftrightarrow$ whether a submodule $\mathcal{M}$ of $\mathbb{R}[X_1, \ldots, X_n]^m$ contains a "positive" element.

Theorem

Termination of linear loops with commuting matrices is decidable.

Conclusion

Termination of linear loops with commuting matrices $\longleftrightarrow$ whether a submodule $\mathcal{M}$ of $\mathbb{R}[X_1, \ldots, X_n]^m$ contains a "positive" element.

Theorem

Termination of linear loops with commuting matrices is decidable.

What about non-commuting matrices?

Conclusion

Termination of linear loops with commuting matrices $\longleftrightarrow$ whether a submodule $\mathcal{M}$ of $\mathbb{R}[X_1, \ldots, X_n]^m$ contains a "positive" element.

Theorem

Termination of linear loops with commuting matrices is decidable.

What about non-commuting matrices?
Let $\mathbb{R}\langle X_1, \ldots, X_n \rangle$ denote the ring of non-commutative polynomials.

Open Problem

Given the generators of a left submodule $\mathcal{M}$ of $\mathbb{R}\langle X_1, \ldots, X_n \rangle^m$, can we decide whether $\mathcal{M}$ contains an element with only positive coefficients?

Conclusion

Termination of linear loops with commuting matrices $\longleftrightarrow$ whether a submodule $\mathcal{M}$ of $\mathbb{R}[X_1, \ldots, X_n]^m$ contains a "positive" element.

Theorem

Termination of linear loops with commuting matrices is decidable.

What about non-commuting matrices?
Let $\mathbb{R}\langle X_1, \ldots, X_n \rangle$ denote the ring of non-commutative polynomials.

Open Problem

Given the generators of a left submodule $\mathcal{M}$ of $\mathbb{R}\langle X_1, \ldots, X_n \rangle^m$, can we decide whether $\mathcal{M}$ contains an element with only positive coefficients?

Open Problem (Interesting special cases)

- Given $f \in \mathbb{R}\langle X_1, \ldots, X_n \rangle$, decide if there exists $g \neq 0$ such that $g \cdot f$ has only positive coefficients?
- Let G be a 2-step nilpotent group, decide if a left ideal of $\mathbb{R}[G]$ contains an element of $\mathbb{R}_{\geq 0}[G]^*$.