On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices

Klara Nosan, Amaury Pouly, Sylvain Schmitz, Mahsa Shirmohammadi and James Worrell

Université de Paris Cité, CNRS, IRIF
Department of Computer Science, Oxford University

18 october 2022

Motivation

Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do

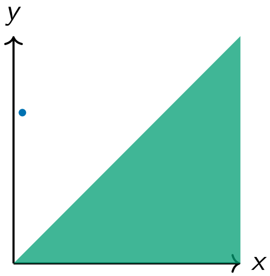
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do

$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

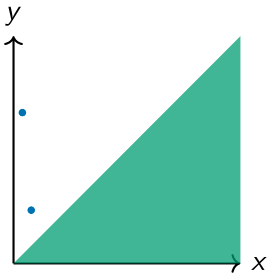


Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do

$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

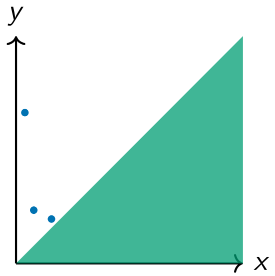


Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do

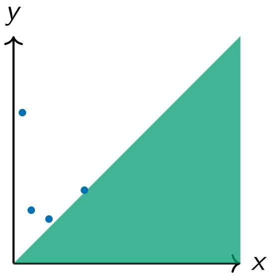
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

Affine program

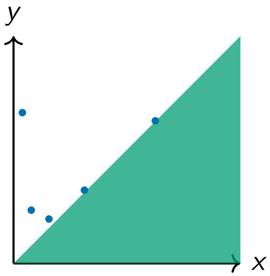
$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

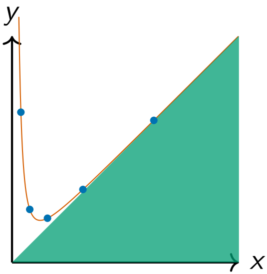
Affine program

$x := 2^{-10}$

$y := 1$

while $y \geqslant x$ do

$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Certificate of non-termination:

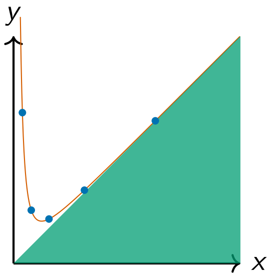
$$x^2 y - x^3 = \frac{1023}{1073741824} \tag{1}$$

- (1) is an invariant: it holds at every step
- (1) implies the guard is true

Does this program halt?

Affine program

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Certificate of non-termination:

$$x^2 y - x^3 = \frac{1023}{1073741824} \quad (1)$$

- (1) is an invariant: it holds at every step
- (1) implies the guard is true

Computing such invariants reduces to computing the **Zariski closure** of a semigroup of matrices.

Quantum automata

A matrix $U \in \mathbb{C}^{n \times n}$ is unitary if it is length preserving:

$$\|Ux\|_2 = \|x\|_2.$$

Quantum automata

A matrix $U \in \mathbb{C}^{n \times n}$ is unitary if it is length preserving:

$$\|Ux\|_2 = \|x\|_2.$$

A (measure once) quantum finite automaton (QFA):

- Σ: finite alphabet,
- $s \in \mathbb{C}^n$: vector of unit norm,
- $X_a \in \mathbb{C}^{n \times n}$: unitary transition matrix for each $a \in \Sigma$,
- $P \in \mathbb{C}^{n \times n}$: orthogonal projection matrix.

Quantum automata

A matrix $U \in \mathbb{C}^{n \times n}$ is unitary if it is length preserving:

$$\|Ux\|_2 = \|x\|_2.$$

A (measure once) quantum finite automaton (QFA):

- Σ: finite alphabet,
- $s \in \mathbb{C}^n$: vector of unit norm,
- $X_a \in \mathbb{C}^{n \times n}$: unitary transition matrix for each $a \in \Sigma$,
- $P \in \mathbb{C}^{n \times n}$: orthogonal projection matrix.

Value of a word $w \in \Sigma^*$:

$$\mathrm{Val}_{\mathcal{A}}(w) = \|PX_w s\|_2^2 \qquad \text{where } X_w = X_{w_{|w|}} \cdots X_{w_1}$$

Interpretation: the probability of observing the quantum state in the acceptance space after having applied the operator sequence X_{w_1} to $X_{w_{|w|}}$ to the initial quantum states.

Quantum automata problems

Given a QFA $\mathcal{A}$ and a threshold λ:

Emptiness Problem

$\exists w \in \Sigma^*$ such that $\text{Val}_{\mathcal{A}}(w) \geq \lambda$?

Undecidable*: proof by reduction from PCP.

*Derksen, Jeandel and Koiran, 2004

Quantum automata problems

Given a QFA $\mathcal{A}$ and a threshold λ:

Emptiness Problem

$\exists w \in \Sigma^*$ such that $\mathsf{Val}_{\mathcal{A}}(w) \geq \lambda$?

Undecidable*: proof by reduction from PCP.

Strict Emptiness Problem

$\exists w \in \Sigma^*$ such that $\mathsf{Val}_{\mathcal{A}}(w) > \lambda$?

Decidable*: reduces to computing the **Zariski closure** of a group of matrices

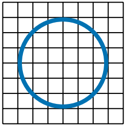
*Derksen, Jeandel and Koiran, 2004

The Problem

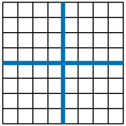
The Zariski topology

Algebraic set: set of common zeroes of a collection S of polynomials in $\mathbb{A}[x_1, \ldots, x_n]$:

$$V(S) = \{x \in \mathbb{A}^n : \forall p \in S, p(x) = 0\}$$



$x^2 + y^2 = c$



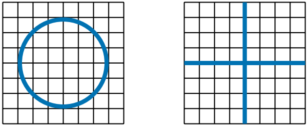
$xy = 0$

Hilbert's basis theorem: for any S, there exists S' **finite** s.t. $V(S) = V(S')$

The Zariski topology

Algebraic set: set of common zeroes of a collection S of polynomials in $\mathbb{A}[x_1, \ldots, x_n]$:

$$V(S) = \{x \in \mathbb{A}^n : \forall p \in S, p(x) = 0\}$$



$x^2 + y^2 = c$ $\qquad$ $xy = 0$

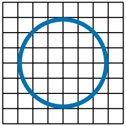
Hilbert's basis theorem: for any S, there exists S' **finite** s.t. $V(S) = V(S')$

Zariski topology: closed sets are algebraic sets.

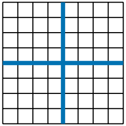
The Zariski topology

Algebraic set: set of common zeroes of a collection S of polynomials in $\mathbb{A}[x_1, \ldots, x_n]$:

$$V(S) = \{x \in \mathbb{A}^n : \forall p \in S, p(x) = 0\}$$



$x^2 + y^2 = c$

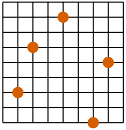


$xy = 0$

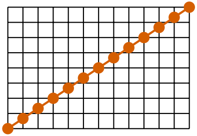
Hilbert's basis theorem: for any S, there exists S' **finite** s.t. $V(S) = V(S')$

Zariski topology: closed sets are algebraic sets.

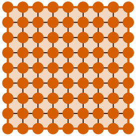
Zariski closure of a set X is the smallest algebraic set $\overline{X}$ that contains X.



$\overline{X} = X$ if X finite



$\overline{\mathbb{Z}} = \mathbb{A}$



$\overline{\mathbb{Z}}^2 = \mathbb{A}^2$

Zariski closure of finitely generated matrix semigroups

Given $A_1, \ldots, A_k \in \mathbb{A}^{n \times n}$, consider

$$\langle A_1, \ldots, A_k \rangle = \text{semigroup generated by the } A_i.$$

Problem: compute $\overline{\langle A_1, \ldots, A_k \rangle}$.

Zariski closure of finitely generated matrix semigroups

Given $A_1, \ldots, A_k \in \mathbb{A}^{n \times n}$, consider

$$\langle A_1, \ldots, A_k \rangle = \text{semigroup generated by the } A_i.$$

Problem: compute $\overline{\langle A_1, \ldots, A_k \rangle}$.

- $\overline{\langle A_1, \ldots, A_k \rangle}$ is an algebraic set, the output of the algorithm is a finite set of polynomials,
- view $\mathbb{A}^{n \times n}$ as $\mathbb{A}^{n^2}$ to make sense of the closure.

Zariski closure of finitely generated matrix semigroups

Given $A_1, \ldots, A_k \in \mathbb{A}^{n \times n}$, consider

$$\langle A_1, \ldots, A_k \rangle = \text{semigroup generated by the } A_i.$$

Problem: compute $\overline{\langle A_1, \ldots, A_k \rangle}$.

- $\overline{\langle A_1, \ldots, A_k \rangle}$ is an algebraic set, the output of the algorithm is a finite set of polynomials,
- view $\mathbb{A}^{n \times n}$ as $\mathbb{A}^{n^2}$ to make sense of the closure.

Example:

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \rightsquigarrow \qquad \langle S, T \rangle = \mathrm{SL}_2(\mathbb{Z})$$

then

$$\overline{\langle S, T \rangle} = SL_2(\overline{\mathbb{Z}}) = SL_2(\mathbb{A}) = \left\{ M \in \mathbb{A}^{n \times n} : \det(M) = 1 \right\}.$$

History of the problem

Given a finite set $S \subseteq \mathbb{A}^{n \times n}$ and $d \in \mathbb{N}$, define the "degree-d closure" as the smallest algebraic set that contains $\langle S \rangle$ and is defined by polynomials of total degree at most d.

History of the problem

Given a finite set $S \subseteq \mathbb{A}^{n \times n}$ and $d \in \mathbb{N}$, define the "degree-d closure" as the smallest algebraic set that contains $\langle S \rangle$ and is defined by polynomials of total degree at most d.

Theorem (Karr, 1974; Müller-Olm and Seidl, 2004)

There is an algorithm that computes, given S and d, the degree-d closure of $\langle S \rangle$, in time $O(|S| \cdot (n^2 + 1)^{3d})$.

There is even a randomized algorithm by Gulwani and Necula (2003).

History of the problem

Given a finite set $S \subseteq \mathbb{A}^{n \times n}$ and $d \in \mathbb{N}$, define the "degree-d closure" as the smallest algebraic set that contains $\langle S \rangle$ and is defined by polynomials of total degree at most d.

Theorem (Karr, 1974; Müller-Olm and Seidl, 2004)

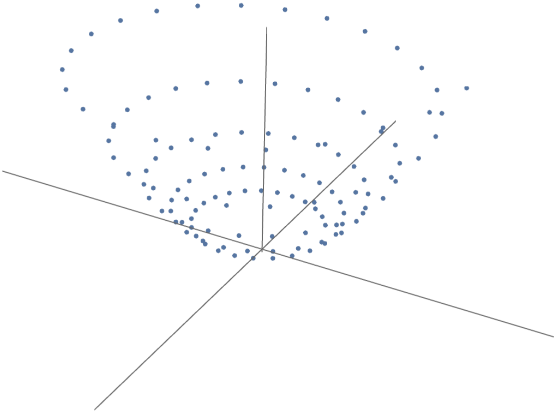
There is an algorithm that computes, given S and d, the degree-d closure of $\langle S \rangle$, in time $O(|S| \cdot (n^2 + 1)^{3d})$.

There is even a randomized algorithm by Gulwani and Necula (2003).

Remarks:

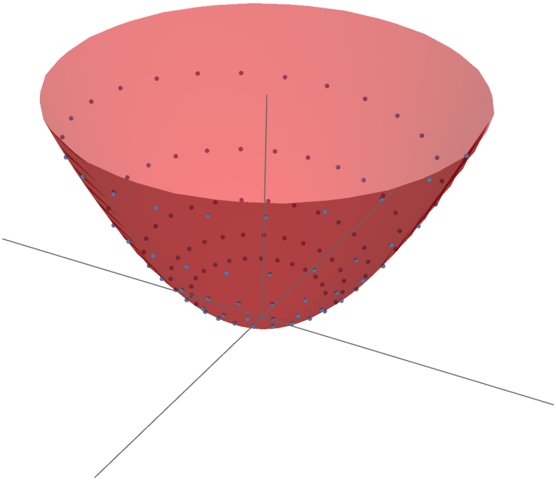
- most applications do **not** need the closure: a sufficiently good approximation is sufficient
- surely one can obtain an upper bound on d ?

Why fixed degree is not enough



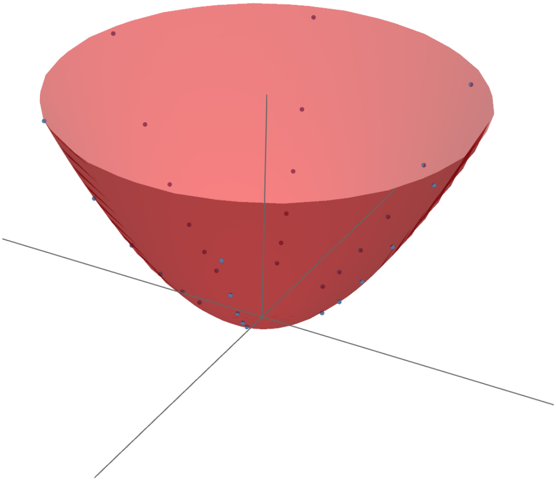
Why fixed degree is not enough

- Paraboloid $z = x^2 + y^2$



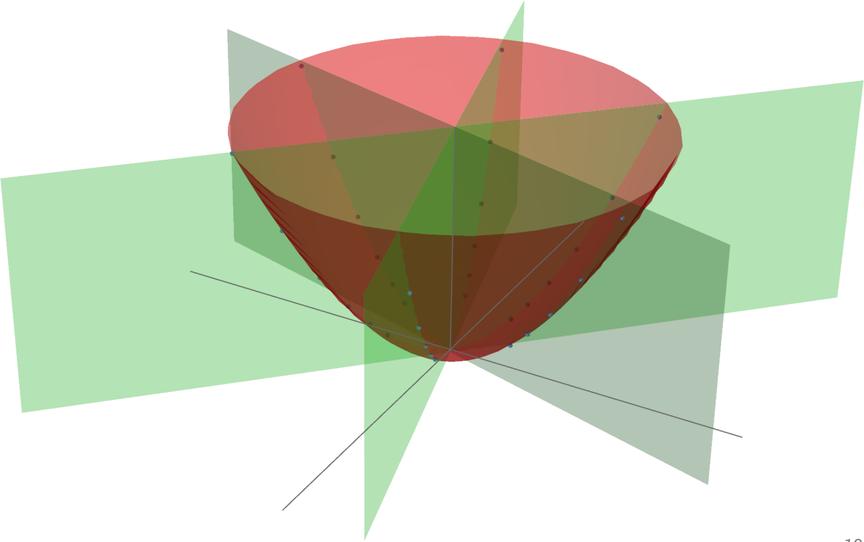
Why fixed degree is not enough

- Paraboloid $z = x^2 + y^2$



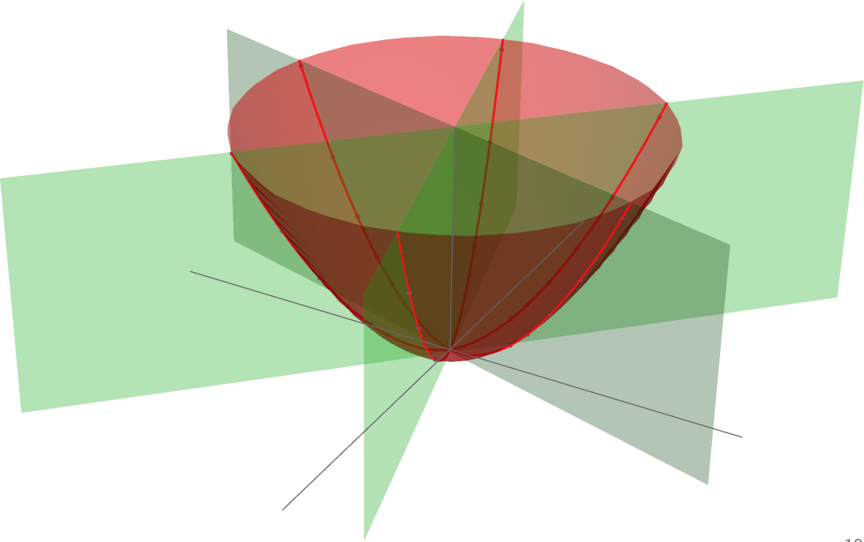
Why fixed degree is not enough

- Paraboloid $z = x^2 + y^2$
- Union of 3 hyperplanes $(x - y)(10y + x)(y + 10x) = 0$



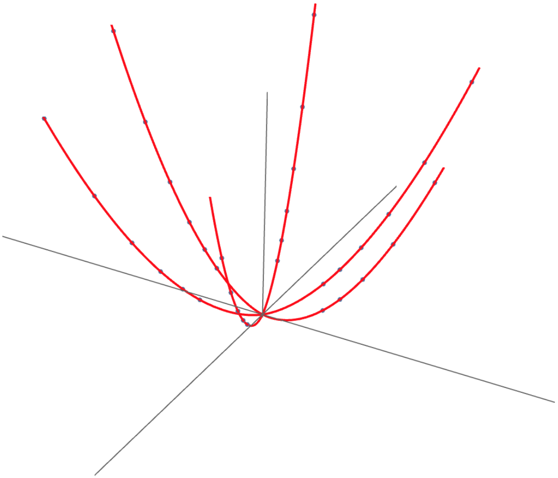
Why fixed degree is not enough

- Paraboloid $z = x^2 + y^2$
- Union of 3 hyperplanes $(x - y)(10y + x)(y + 10x) = 0$



Why fixed degree is not enough

- Paraboloid $z = x^2 + y^2$
- Union of 3 hyperplanes $(x - y)(10y + x)(y + 10x) = 0$



History of the problem (cont)

Quantum automata and algebraic groups

Harm Derksen[a], Emmanuel Jeandel[b], Pascal Koiran[b,*]

[a]*Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, United States*
[b]*Laboratoire de l'Informatique du Parallélisme, Ecole Normale Supérieure de Lyon, 69364, France*

Received 15 September 2003; accepted 1 November 2004

Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm that computes $\overline{\langle S \rangle}$ given a finite set S of invertible matrices.

History of the problem (cont)

Quantum automata and algebraic groups

Harm Derksen[a], Emmanuel Jeandel[b], Pascal Koiran[b,*]

[a] *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, United States*
[b] *Laboratoire de l'Informatique du Parallélisme, Ecole Normale Supérieure de Lyon, 69364, France*

Received 15 September 2003; accepted 1 November 2004

Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm that computes $\overline{\langle S \rangle}$ given a finite set S of invertible matrices.

Theorem (Hrushovski, Ouaknine, P., Worrell, 2018)

There is an algorithm that computes $\overline{\langle S \rangle}$ given a finite set S of matrices.

History of the problem (cont)

Quantum automata and algebraic groups

Harm Derksen[a], Emmanuel Jeandel[b], Pascal Koiran[b,*]

[a] *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, United States*
[b] *Laboratoire de l'Informatique du Parallélisme, Ecole Normale Supérieure de Lyon, 69364, France*

Received 15 September 2003; accepted 1 November 2004

Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm that computes $\overline{\langle S \rangle}$ given a finite set S of invertible matrices.

Theorem (Hrushovski, Ouaknine, P., Worrell, 2018)

There is an algorithm that computes $\overline{\langle S \rangle}$ given a finite set S of matrices.

None of these algorithms puts a bound on the degree of the closure!

Main result

We obtain a degree bound for invertible matrices:

Theorem (ISSAC 2022)

Given a finite set S of invertible matrices of dimension n, the algebraic group $G := \overline{\langle S \rangle}$ can be defined with equations of degree at most septuply exponential in n.

Main result

We obtain a degree bound for invertible matrices:

Theorem (ISSAC 2022)

Let $n \in \mathbb{N}$ and let $S \subseteq \mathsf{GL}_n(\mathbb{Q})$ be a finite set of matrices whose entries have height at most h. Then the Zariski closure of the group generated by S can be represented by finitely many polynomials of degree at most $(\log h)^{2^{|S|^{\exp^4(\mathrm{poly}(n))}}}$ with coefficients in $\mathbb{Q}$, forming a basis of the vanishing ideal of the group generated by S. Furthermore, if G contains only semisimple elements then the degree can be bounded by $(\log h)^{2^{|S|^{2^{\mathrm{poly}(n)}}}}$.

Main result

We obtain a degree bound for invertible matrices:

Theorem (ISSAC 2022)

Let $n \in \mathbb{N}$ and let $S \subseteq \mathsf{GL}_n(\mathbb{Q})$ be a finite set of matrices whose entries have height at most h. Then the Zariski closure of the group generated by S can be represented by finitely many polynomials of degree at most $(\log h)^{2^{|S|^{\exp^4(\mathrm{poly}(n))}}}$ with coefficients in $\mathbb{Q}$, forming a basis of the vanishing ideal of the group generated by S. Furthermore, if G contains only semisimple elements then the degree can be bounded by $(\log h)^{2^{|S|^{2^{\mathrm{poly}(n)}}}}$.

Corollary

The algebraic closure of a finitely generated matrix group is computable in elementary (octuply exponential) time.

Summary

Motivation:

- certifying non-termination of linear loops
- analysing quantum automata

Problem: compute the Zariski closure of a finitely generated group of matrices

- computable
- we obtained a septuly exponential bound on the degree of the closure

Future work:

- improve bound using ideas from differential Galois group algorithms
- study special classes of groups
- extend to semigroups

Algebraic groups

General linear group: the set of all invertible matrices of dimension n with entries from $\mathbb{A}$, denoted $\mathrm{GL}_n(\mathbb{A})$.

Algebraic groups

General linear group: the set of all invertible matrices of dimension n with entries from $\mathbb{A}$, denoted $\mathrm{GL}_n(\mathbb{A})$.

Linear algebraic group: a subgroup of $\mathrm{GL}_n(\mathbb{A})$ that is an algebraic set.

Algebraic groups

General linear group: the set of all invertible matrices of dimension n with entries from $\mathbb{A}$, denoted $\mathsf{GL}_n(\mathbb{A})$.

Linear algebraic group: a subgroup of $\mathsf{GL}_n(\mathbb{A})$ that is an algebraic set.

$$\mathsf{GL}_n(\mathbb{A}) = \{(M, y) \in \mathbb{A}^{n^2+1} : \det(M) \cdot y = 1\}$$

$$\mathsf{SL}_n(\mathbb{A}) = \{(M, y) \in \mathbb{A}^{n^2+1} : \det(M) \cdot y = 1, \det(M) = 1\}$$

Algebraic groups

General linear group: the set of all invertible matrices of dimension n with entries from $\mathbb{A}$, denoted $\mathsf{GL}_n(\mathbb{A})$.

Linear algebraic group: a subgroup of $\mathsf{GL}_n(\mathbb{A})$ that is an algebraic set.

$$\mathsf{GL}_n(\mathbb{A}) = \{(M, y) \in \mathbb{A}^{n^2+1} : \det(M) \cdot y = 1\}$$

$$\mathsf{SL}_n(\mathbb{A}) = \{(M, y) \in \mathbb{A}^{n^2+1} : \det(M) \cdot y = 1, \det(M) = 1\}$$

Key fact: if $S \subseteq \mathsf{GL}_n(\mathbb{A})$ then $\overline{\langle S \rangle}$ is an algebraic group

We analyse the structure of algebraic groups that come from finitely generated groups.

Can we hope for better ?

A closely related topic is the computation of the Galois group of a linear differential equation which is a linear algebraic group.

Can we hope for better ?

A closely related topic is the computation of the Galois group of a linear differential equation which is a linear algebraic group.

- Ehud Hrushovski (2002): computable (no degree bound)
- Ruyong Feng (2015): sextuply exponential
- Mengxiao Sun (2018): triple exponential
- Amzallag, Minchenko, Pogudin (2021): single exponential

Can we hope for better ?

A closely related topic is the computation of the Galois group of a linear differential equation which is a linear algebraic group.

- Ehud Hrushovski (2002): computable (no degree bound)
- Ruyong Feng (2015): sextuply exponential
- Mengxiao Sun (2018): triple exponential
- Amzallag, Minchenko, Pogudin (2021): single exponential

Big difference: these bounds only depend on the dimension, ours also depend on the height of the entries (see next slide)

Can we hope for better ?

A closely related topic is the computation of the Galois group of a linear differential equation which is a linear algebraic group.

- Ehud Hrushovski (2002): computable (no degree bound)
- Ruyong Feng (2015): sextuply exponential
- Mengxiao Sun (2018): triple exponential
- Amzallag, Minchenko, Pogudin (2021): single exponential

Big difference: these bounds only depend on the dimension, ours also depend on the height of the entries (see next slide)

We use many ideas from the above papers to prove our result.

Future work: use the techniques of Amzallag, Minchenko and Pogudin to reduce our bound

Remarks on lower bounds

A difficulty in the proof is that the degree bound must depend on the height of the entries:

$$A = \mathrm{diag}(2^p, 1/2).$$

The height is $h = 2^p$.

Remarks on lower bounds

A difficulty in the proof is that the degree bound must depend on the height of the entries:

$$A = \mathrm{diag}(2^p, 1/2).$$

The height is $h = 2^p$. The vanishing ideal of $\langle A \rangle$ is generated by the multiplicative relations among the eigenvalues of A. Here there is only one:

$$(2^p)^1 \cdot (\tfrac{1}{2})^p = 1.$$

Remarks on lower bounds

A difficulty in the proof is that the degree bound must depend on the height of the entries:

$$A = \mathrm{diag}(2^p, 1/2).$$

The height is $h = 2^p$. The vanishing ideal of $\langle A \rangle$ is generated by the multiplicative relations among the eigenvalues of A. Here there is only one:

$$(2^p)^{1} \cdot (\tfrac{1}{2})^{p} = 1.$$

Therefore any polynomial that vanishes on $\langle A \rangle$ must also vanish on

$$\{\mathrm{diag}(x, y) : xy^p = 1\}$$

and thus be of degree at least $1 + p \geqslant \log(h)$.

Conclusion:

- even in dimension 2, the degree can be arbitrarily large and depends on the height.
- the exponential "lower bound" of Amzallag, Minchenko, Pogudin probably also works in our case

Chains of algebraic groups

The proof yields a potentially useful result on chains of algebraic groups:

Theorem

Let $n \in \mathbb{N}$, k be a number field, and $G_i = \overline{\langle S_i \rangle}$ for $S_i \subseteq \mathrm{GL}_n(k)$, $1 \leq i \leq \ell$, be such that $G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_\ell$. Then

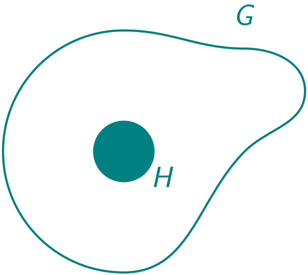
$$\ell \leq \exp\Big(\mathrm{poly}([k:\mathbb{Q}])\exp^3(\mathrm{poly}(n))\Big),$$

and $\ell \leq 2^{\mathrm{poly}(n[k:\mathbb{Q}])}$ if each G_i consists only of semisimple elements.

This may be useful to analyse the running time of algorithms.

The idea behind of our proof

G has a normal subgroup of finite index H:



Good properties

- we know $|G/H|$,
- we have degree bounds on H

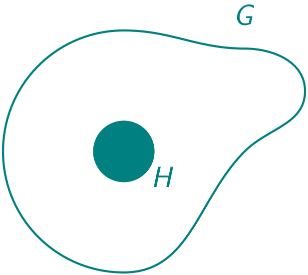
The idea behind of our proof

G has a normal subgroup of finite index H: G is the union of $|G/H|$ copies of H

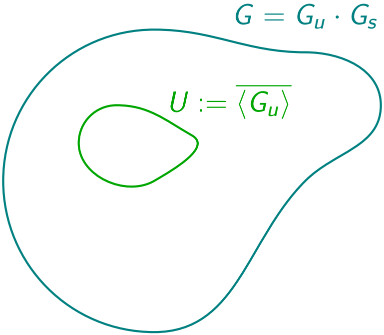
$\rightsquigarrow$ we can write equations for G from that of H and $|G/H|$.

Good properties

- we know $|G/H|$,
- we have degree bounds on H

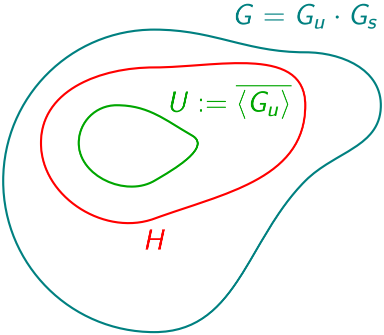


More details



U is a normal subgroup of G, and we have a bound on the degree of defining equations.

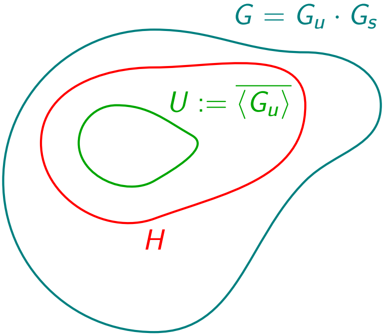
More details



U is a normal subgroup of G, and we have a bound on the degree of defining equations.

How can we use it to obtain a normal subgroup of finite index?

More details



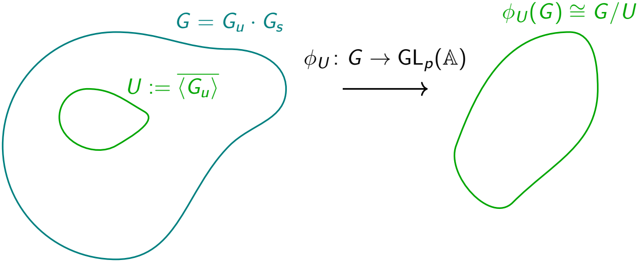
U is a normal subgroup of G, and we have a bound on the degree of defining equations.

How can we use it to obtain a normal subgroup of finite index?

The quotient G/U is an algebraic group consisting only of semisimple elements.

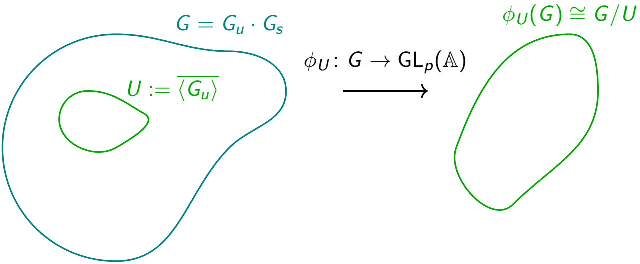
We can use this to reduce to the case of semisimple matrices!

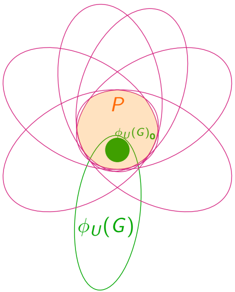
The construction



→ $U \lhd G$
→ $\phi_U(G) \cong G/U$ semisimple
→ Bound on U
→ Bound on the degree of equations defining ϕ_U **[Feng'15]**

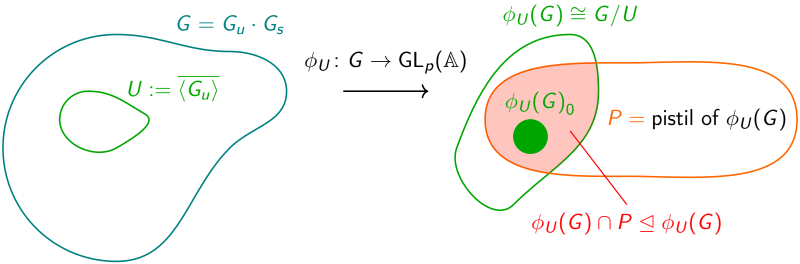
The construction

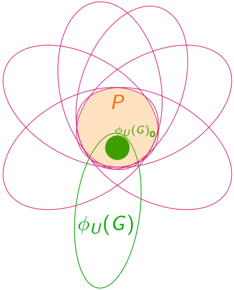




- $\to$ Pistil P of $\phi_U(G)$
- $\to$ $\phi_U(G) \triangleleft (\phi_U(G) \cap P) \triangleleft \phi_U(G)$
- $\to$ $\phi_U(G) \cap P$ finite index in $\phi_U(G)$
- $\to$ P commutative
- $\to$ P bounded by 1

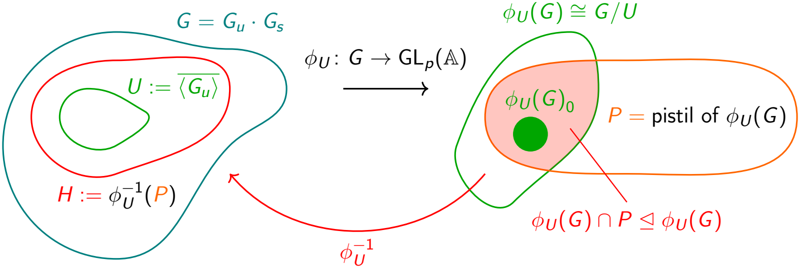
The construction





- → Pistil P of $\phi_U(G)$
- → $\phi_U(G) \triangleleft (\phi_U(G) \cap P) \triangleleft \phi_U(G)$
- → $\phi_U(G) \cap P$ finite index in $\phi_U(G)$
- → P commutative
- → P bounded by 1

The construction



- → $U \lhd H \lhd G$
- → $\phi_U(G) \cong G/U$ semisimple
- → Bound on U
- → Bound on the degree of equations defining ϕ_U
- → Bound on H
- → H finite index in G
- → H/U commutative

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

Note: if such a word exists, it is a finite certificate. Enumerate!

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

Note: if such a word exists, it is a finite certificate. Enumerate!

Our aim is to construct a finite certificate of non-existence.

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

Our aim is to construct a finite certificate of non-existence.

$$\mathcal{X} = \{X_w : w \in \Sigma^*\} = \langle X_a : a \in \Sigma \rangle$$

$$f(X) = \|sXP\|^2$$

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

Our aim is to construct a finite certificate of non-existence.

$$\mathcal{X} = \{X_w : w \in \Sigma^*\} = \langle X_a : a \in \Sigma \rangle$$

$$f(X) = \|sXP\|^2$$

Observation:

(i) $\mathsf{Val}_{\mathcal{A}}(w) = f(X_w)$,

(ii) f is an Euclidean-continuous polynomial map.

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

$$f(X) \leq \lambda \text{ for all } X \in \mathcal{X}$$

$$\Updownarrow$$

$$f(X) \leq \lambda \text{ for all } X \text{ in the Euclidian closure of } \mathcal{X}$$

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

$$f(X) \leq \lambda \text{ for all } X \in \mathcal{X}$$

$$\Updownarrow$$

$$f(X) \leq \lambda \text{ for all } X \text{ in the Euclidian closure of } \mathcal{X}$$

Crucial fact: the Euclidian closure of $\mathcal{X}$ is algebraic.

Deciding Strict Emptiness for QFA

Strict Emptiness

Given a QFA $\mathcal{A}$ and a threshold λ:

$$\exists w \in \Sigma^* \text{ s.t. } \mathsf{Val}_{\mathcal{A}}(w) > \lambda \text{ ?}$$

$$f(X) \leq \lambda \text{ for all } X \in \mathcal{X}$$

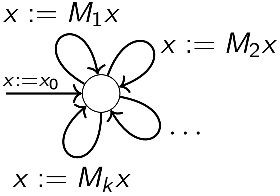
$$\Updownarrow$$

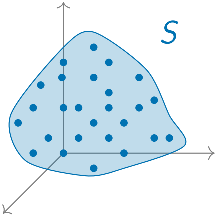
$$f(X) \leq \lambda \text{ for all } X \text{ in the Euclidian closure of } \mathcal{X}$$

Crucial fact: the Euclidian closure of $\mathcal{X}$ is algebraic.

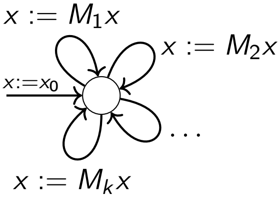
Finite certificate: $\overline{\mathcal{X}}$ can be finitely represented and is computable.
[Derksen et al.'05]

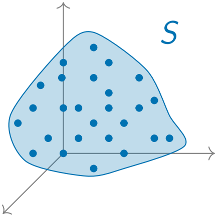
At the edge of decidability





At the edge of decidability

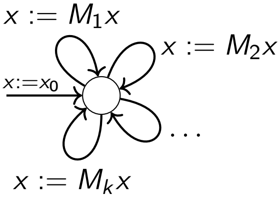


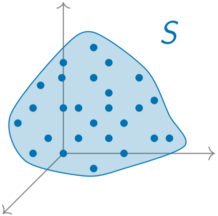


Theorem (Markov 1947)

There is a fixed finite set of 6×6 *integer matrices* S *such that the problem of deciding whether* $A \in \langle S \rangle$ *for a given* A *is undecidable.*

At the edge of decidability





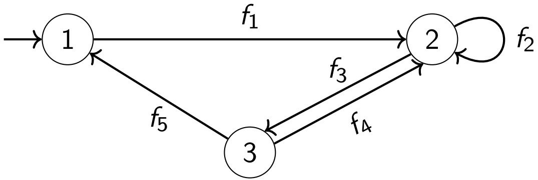
Theorem (Markov 1947)

There is a fixed finite set of 6×6 *integer matrices* S *such that the problem of deciding whether* $A \in \langle S \rangle$ *for a given* A *is undecidable.*

Theorem (Paterson 1970)

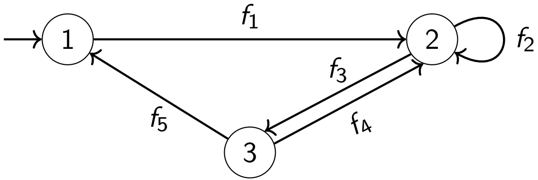
The problem of deciding, given $M_1, \ldots, M_k$*, whether* $0 \in \langle M_1, \ldots, M_k \rangle$ *is undecidable for* 3×3 *matrices.*

Affine programs



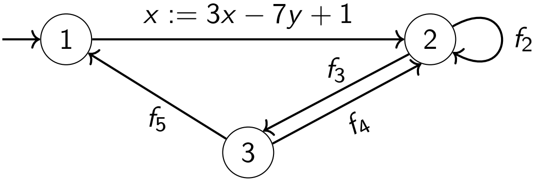
Affine programs

- Nondeterministic branching (no guards)



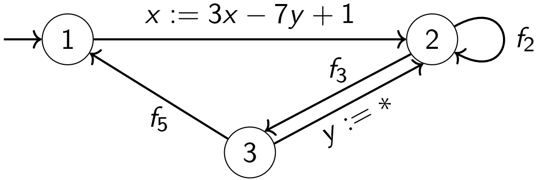
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine



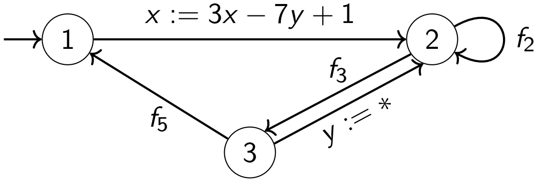
Affine programs

- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := *$)



Affine programs

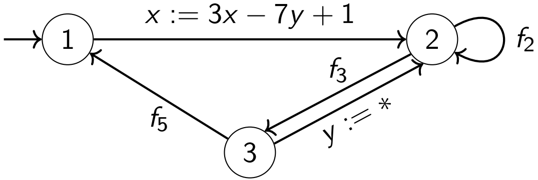
- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := *$)



- Can overapproximate complex programs

Affine programs

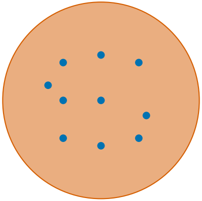
- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := *$)



- Can overapproximate complex programs
- Covers existing formalisms:
  probabilistic, quantum, quantitative automata

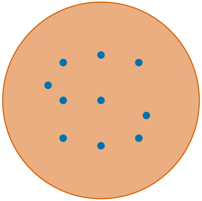
Invariants

invariant = overapproximation of the reachable states

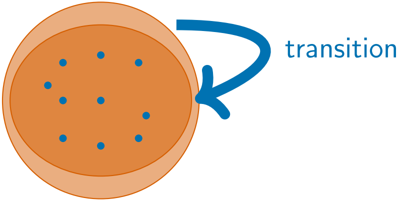


Invariants

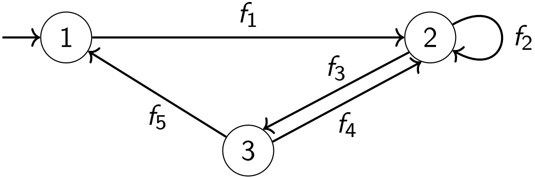
invariant = overapproximation of the reachable states



inductive invariant = invariant preserved by the transition relation

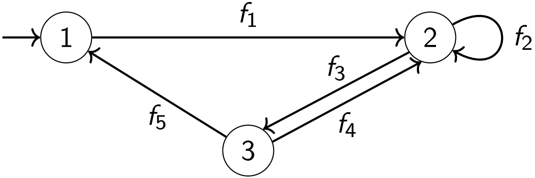


Inductive invariants: example



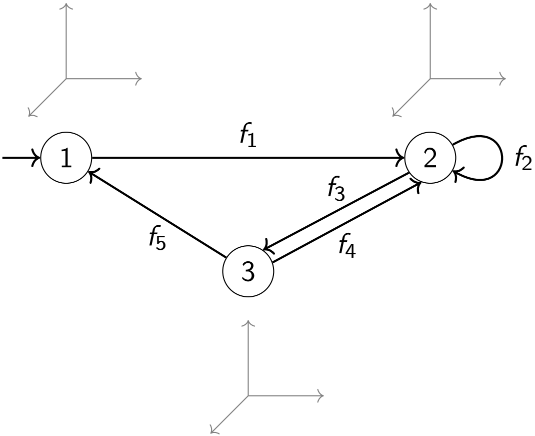
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\quad$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



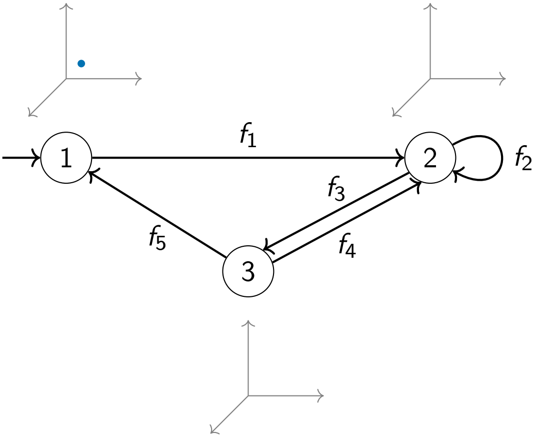
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



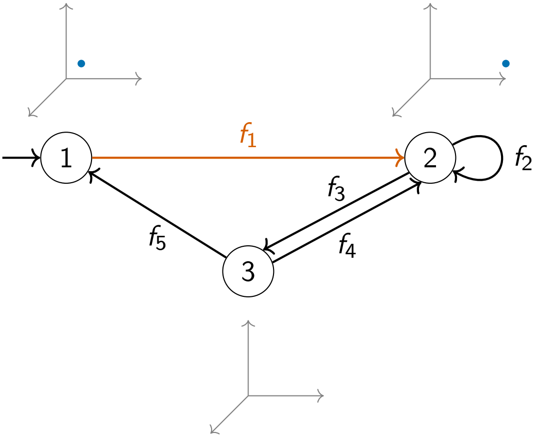
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\quad$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



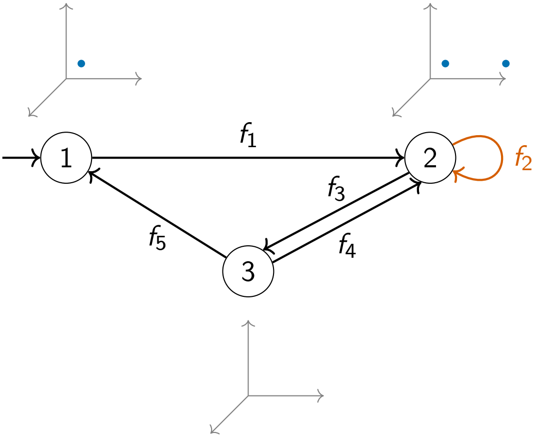
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



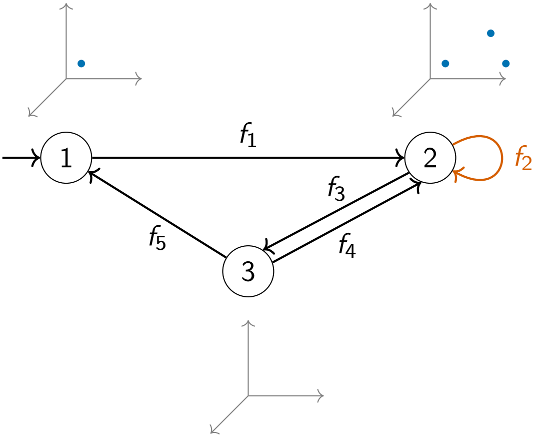
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



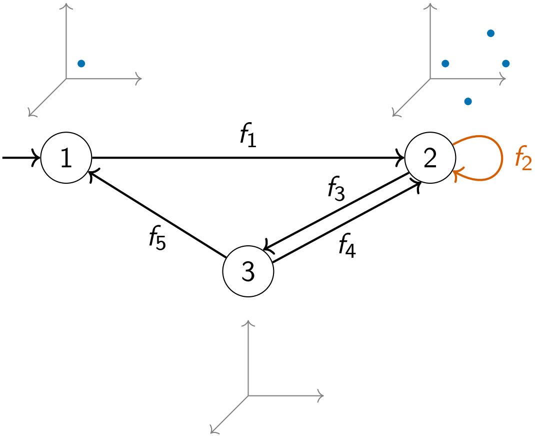
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



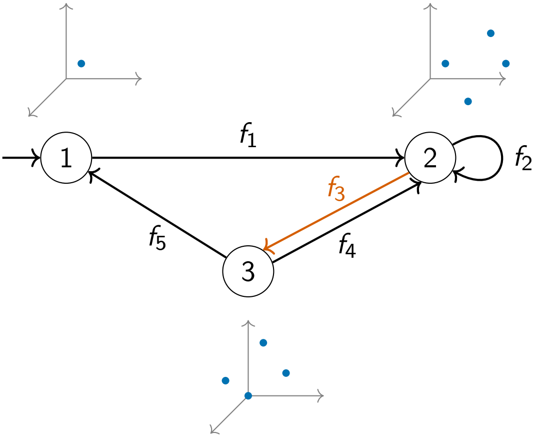
x, y, z range over $\mathbb{Q}$

$f_i : \mathbb{R}^3 \to \mathbb{R}^3$



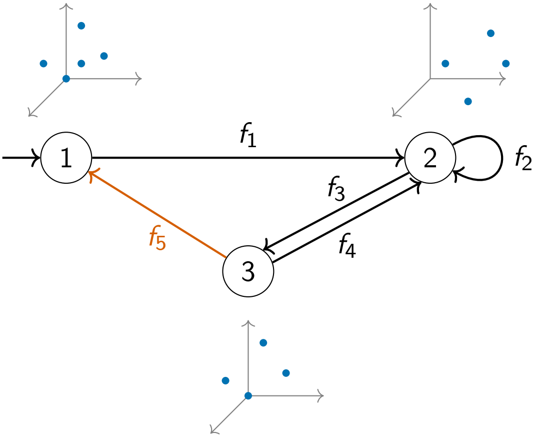
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



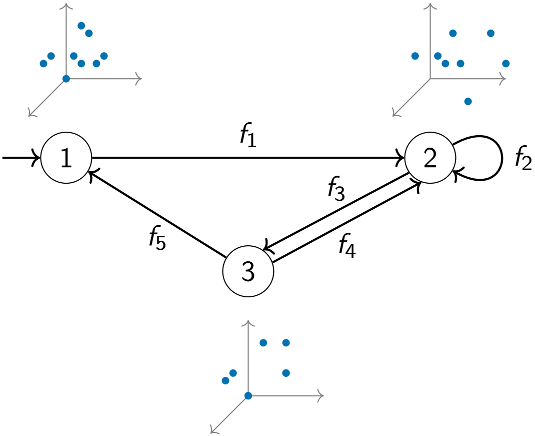
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



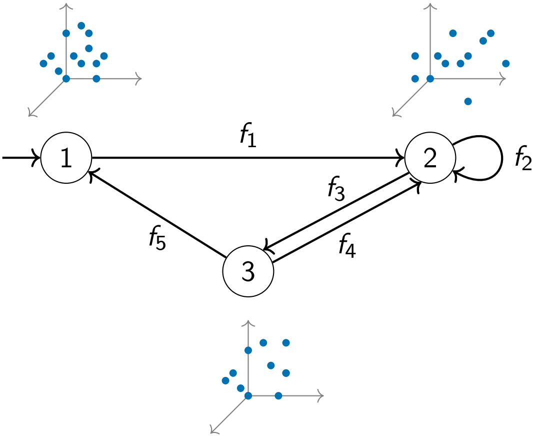
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



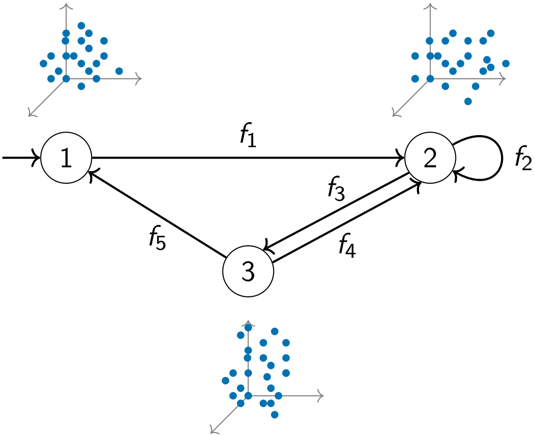
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



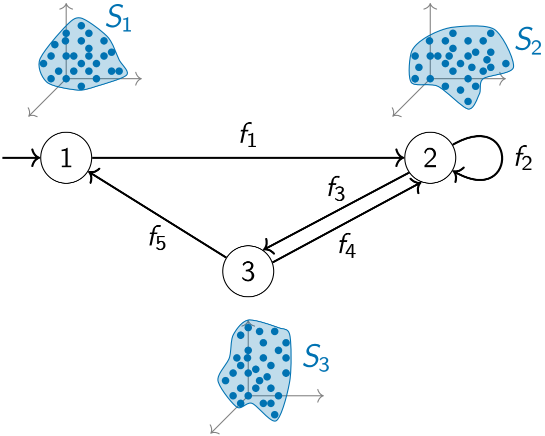
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



Inductive invariants: example

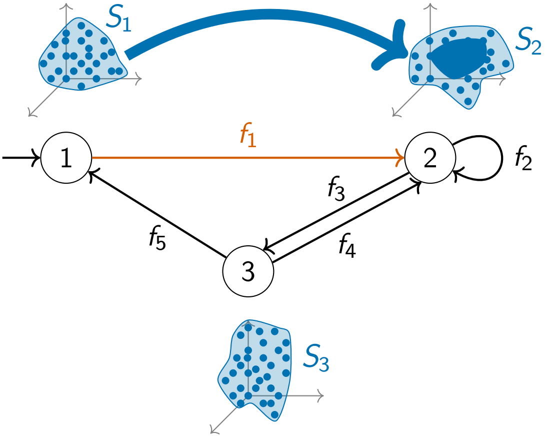
x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



S_1,S_2,S_3 are the reachable states

Inductive invariants: example

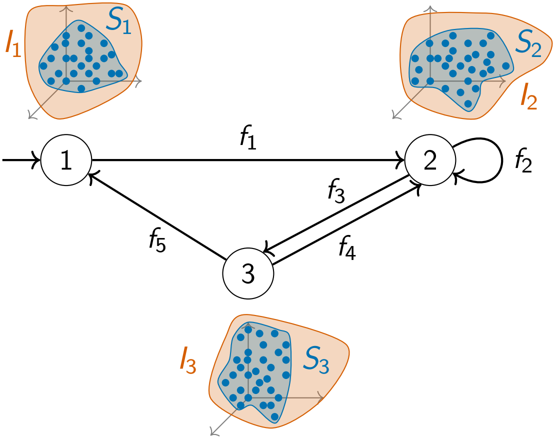
x, y, z range over $\mathbb{Q}$ $\qquad$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



S_1, S_2, S_3 is also an inductive invariant

Inductive invariants: example

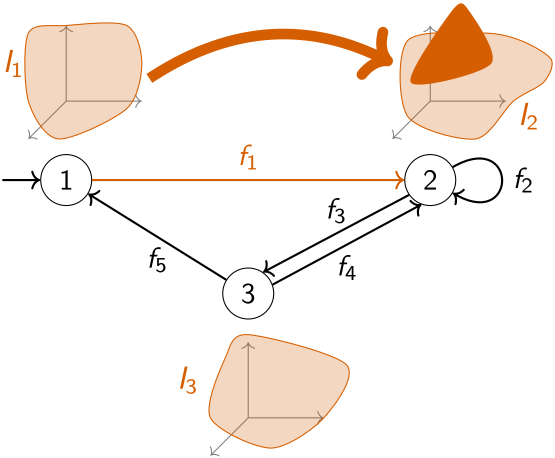
x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



I_1, I_2, I_3 is an invariant

Inductive invariants: example

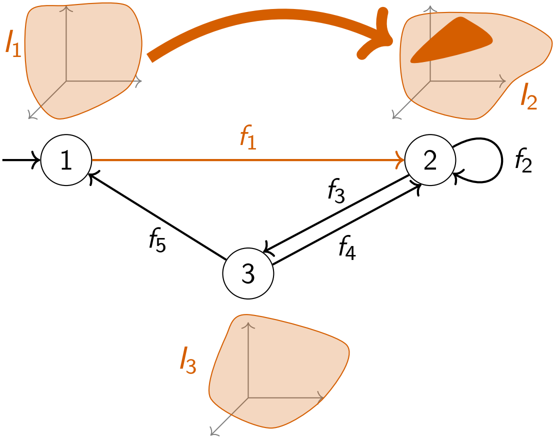
x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



I_1, I_2, I_3 is **NOT** an inductive invariant

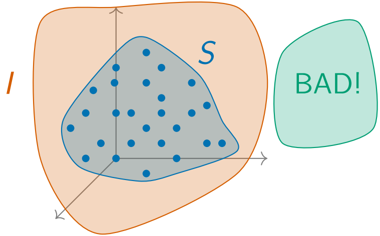
Inductive invariants: example

x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



I_1, I_2, I_3 is an inductive invariant

Why Invariants?



The classical approach to the verification of temporal safety properties of programs requires the construction of ***inductive invariants*** *[...].* ***Automation of this construction is the main challenge in program verification.***

D. Beyer, T. Henzinger, R. Majumdar, and A. Rybalchenko
Invariant Synthesis for Combined Theories, 2007

Which invariants?