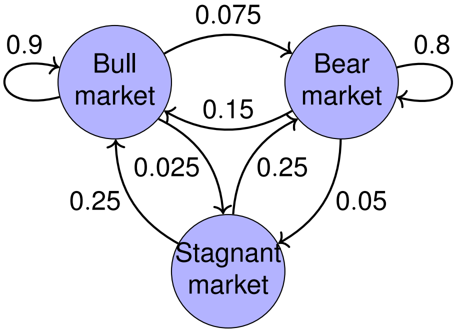
Linear Dynamical Systems

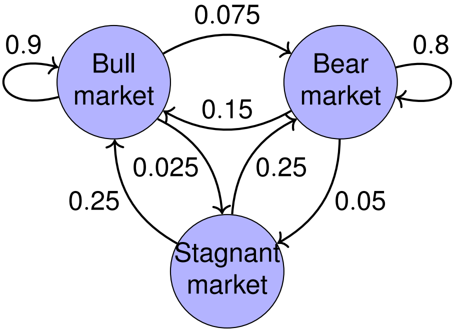
Amaury Pouly

Overview

Examples: while loop, Markov chain



Examples: while loop, Markov chain



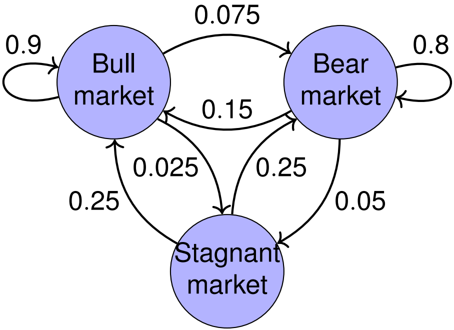
State: $X = (p_{bull}, p_{bear}, p_{stag}) \in [0,1]^3$
Transitions:

$$A = \begin{bmatrix} 0.9 & 0.15 & 0.25 \\ 0.075 & 0.8 & 0.25 \\ 0.025 & 0.05 & 0.5 \end{bmatrix}$$

$\rightarrow$ Linear dynamical system

$$X_{n+1} = AX_n$$

Examples: while loop, Markov chain



State: $X = (p_{bull}, p_{bear}, p_{stag}) \in [0,1]^3$
Transitions:

$$A = \begin{bmatrix} 0.9 & 0.15 & 0.25 \\ 0.075 & 0.8 & 0.25 \\ 0.025 & 0.05 & 0.5 \end{bmatrix}$$

$\rightarrow$ Linear dynamical system

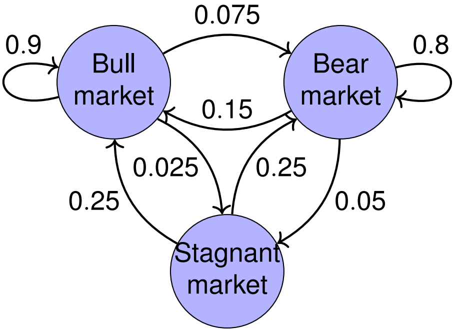
$$X_{n+1} = AX_n$$

Linear loop

$p_{bull} := 0$
$p_{bear} := 1$
$p_{stag} := 0$
while $p_{bull} \leqslant 1/2$ do

$$\begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix} := A \begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix}$$

Examples: while loop, Markov chain



State: $X = (p_{bull}, p_{bear}, p_{stag}) \in [0,1]^3$
Transitions:

$$A = \begin{bmatrix} 0.9 & 0.15 & 0.25 \\ 0.075 & 0.8 & 0.25 \\ 0.025 & 0.05 & 0.5 \end{bmatrix}$$

$\rightarrow$ Linear dynamical system

$$X_{n+1} = AX_n$$

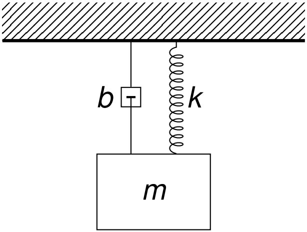
Linear loop

$p_{bull} := 0$
$p_{bear} := 1$
$p_{stag} := 0$
while $p_{bull} \leqslant 1/2$ do

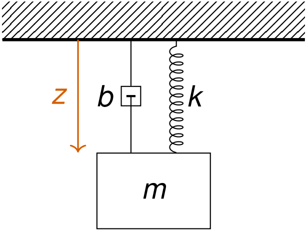
$$\begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix} := A \begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix}$$

The loop terminates if and only if the probability of a bull market is $> 1/2$.

Example: mass-spring-damper system



Example: mass-spring-damper system

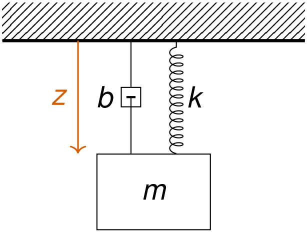


State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg$$

Example: mass-spring-damper system



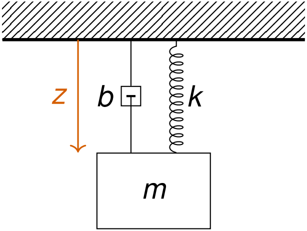
State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg$$

$\rightarrow$ Affine but not first order

Example: mass-spring-damper system



State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg$$

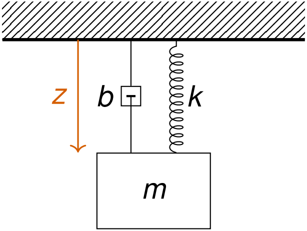
$\rightarrow$ Affine but not first order

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g \\ 0 \end{bmatrix}$$

Example: mass-spring-damper system



State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg$$

$\rightarrow$ Affine but not first order

State: $X = (z, z', 1) \in \mathbb{R}^3$

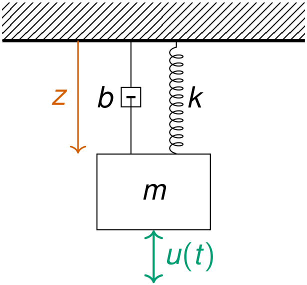
Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g \\ 0 \end{bmatrix}$$

$\rightarrow$ Linear dynamical system

$$X' = AX$$

Example: mass-spring-damper system



with external input $u(t)$.

State: $X = z \in \mathbb{R}$

Equation of motion:

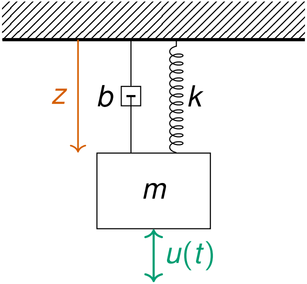
$$mz'' = -kz - bz' + mg + u$$

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g \\ 0 \end{bmatrix}$$

Example: mass-spring-damper system



with external input $u(t)$.

$\rightarrow$ Linear time invariant system

$$X' = AX + Bu$$

State: $X = z \in \mathbb{R}$

Equation of motion:

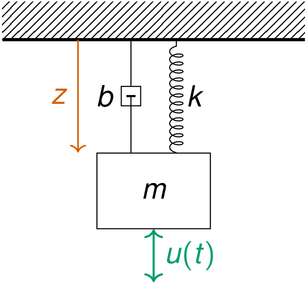
$$mz'' = -kz - bz' + mg + u$$

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{m} \\ 0 \end{bmatrix} u$$

Example: mass-spring-damper system



with external input $u(t)$.

$\rightarrow$ Linear time invariant system

$$X' = AX + Bu$$

State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg + u$$

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{m} \\ 0 \end{bmatrix} u$$

Can be used to model a car suspension.

Linear dynamical systems

Discrete case

$$x(n+1) = Ax(n)$$

- biology,
- software verification,
- probabilistic model checking,
- combinatorics,
- ....

Continuous case

$$x'(t) = Ax(t)$$

- biology,
- physics,
- probabilistic model checking,
- electrical circuits,
- ....

Typical questions

- reachability
- safety

Linear dynamical systems

Discrete case

$$x(n+1) = Ax(n) + Bu(n)$$

- biology,
- software verification,
- probabilistic model checking,
- combinatorics,
- ....

Continuous case

$$x'(t) = Ax(t) + Bu(t)$$

- biology,
- physics,
- probabilistic model checking,
- electrical circuits,
- ....

Typical questions

- reachability
- safety
- controllability

Linear dynamical systems

Discrete case

$$x(n+1) = Ax(n) + Bu(n)$$

- biology,
- software verification,
- probabilistic model checking,
- combinatorics,
- ....

Continuous case

$$x'(t) = Ax(t) + Bu(t)$$

- biology,
- physics,
- probabilistic model checking,
- electrical circuits,
- ....

Typical questions

- reachability
- safety
- controllability
- optimal control
- feedback control
- ...

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
    if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
    if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Very challenging to analyze!

- reachability is undecidable
- invariant* synthesis also hard

*Will be defined later, think "approximate reachability".

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
  if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
  else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$\rightsquigarrow$

Nondeterminic loop

$x := 2^{-10}$
$y := 1$
while true do
  non deterministically do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
  or
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Very challenging to analyze!

- reachability is undecidable
- invariant* synthesis also hard

*Will be defined later, think “approximate reachability”.

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
    if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$\rightsquigarrow$

Nondeterminic loop

$x := 2^{-10}$
$y := 1$
while true do
    non deterministically do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    or
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Very challenging to analyze!

- reachability is undecidable
- invariant* synthesis also hard

Overapproximate behaviours

- reachability still undecidable
- invariant synthesis possible

*Will be defined later, think “approximate reachability”.

Does this program halt?

Affine program

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

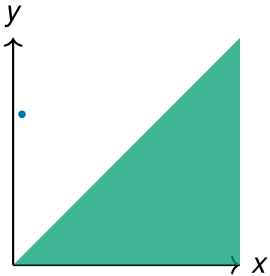
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Does this program halt?

Affine program

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

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

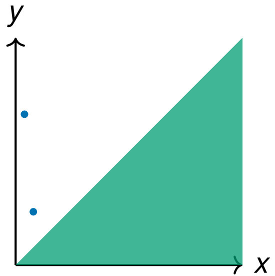


Does this program halt?

Affine program

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

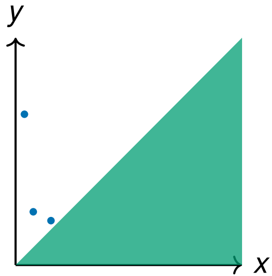
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

Affine program

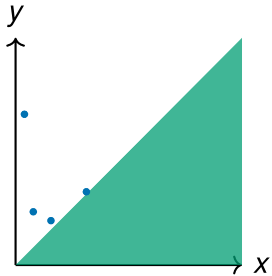
$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

Affine program

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

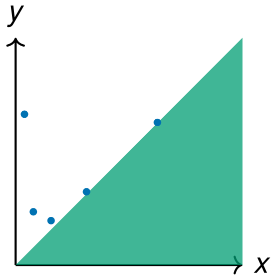


Does this program halt?

Affine program

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

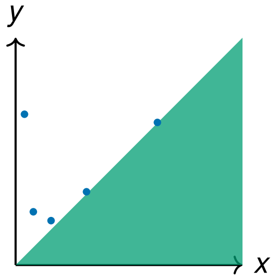
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



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:

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

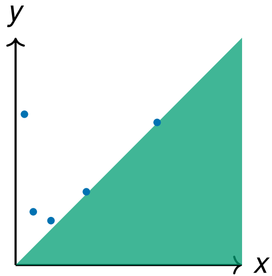
Does this program halt?

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:

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



- (2) is an invariant: it holds at every step

Does this program halt?

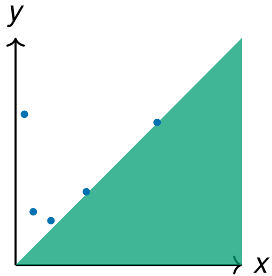
Affine program

$x := 2^{-10}$
$y := 1$
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:

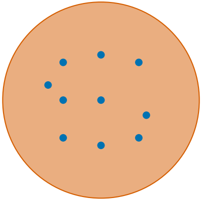
$$x^2 y - x^3 = \frac{1023}{1073741824} \tag{1}$$



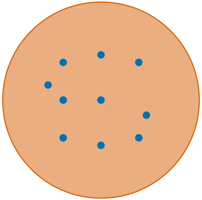
- (2) is an invariant: it holds at every step
- (2) implies the guard is true

Invariants

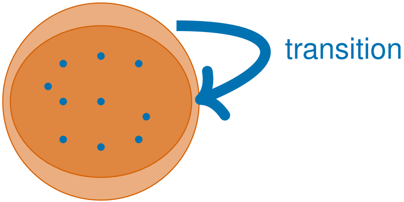
invariant = overapproximation of the reachable states



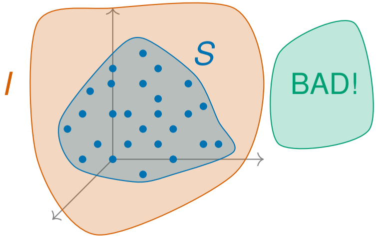
invariant = overapproximation of the reachable states



inductive invariant = invariant preserved by the transition relation



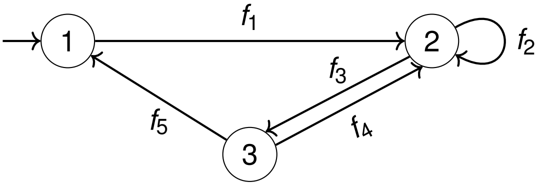
Why Invariants?



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.***

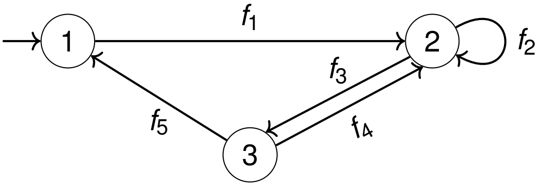
D. Beyer, T. Henzinger, R. Majumdar, and A. Rybalchenko
Invariant Synthesis for Combined Theories, 2007

Affine programs



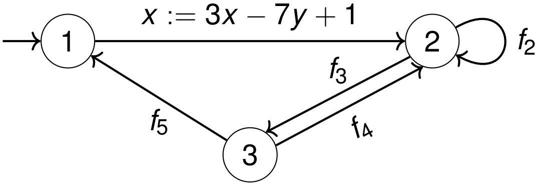
Affine programs

- Nondeterministic branching (no guards)



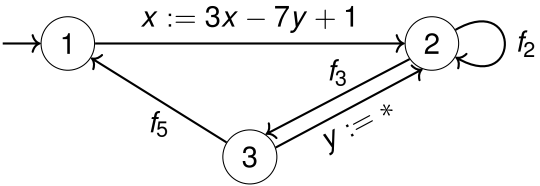
Affine programs

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



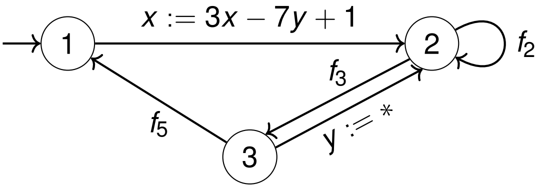
Affine programs

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



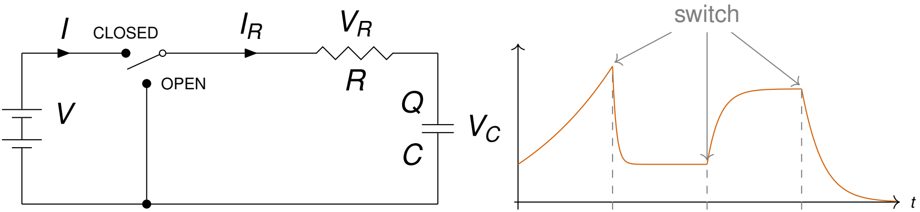
Affine programs

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

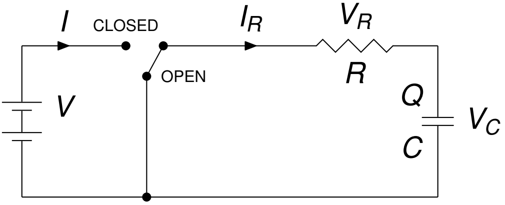


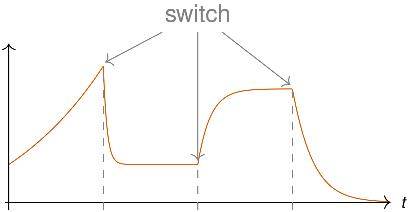
- Can overapproximate complex programs
- Covers existing formalisms:
  finite, probabilistic, quantum, quantitative automata

RC circuit



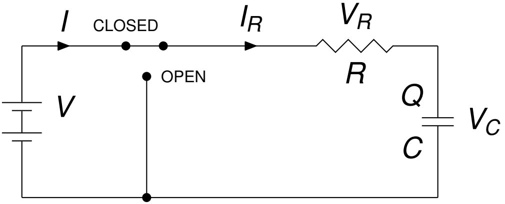
RC circuit

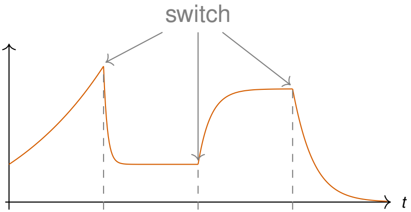




OPEN

$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$





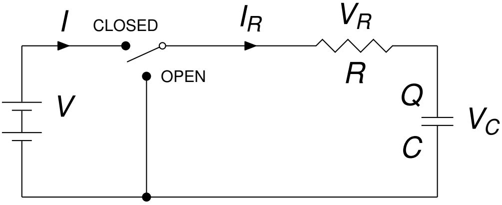
OPEN

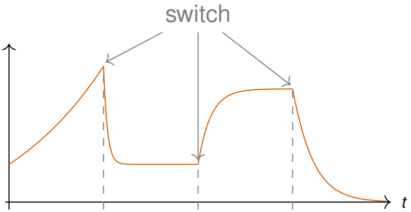
$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

CLOSED

$$\boxed{\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

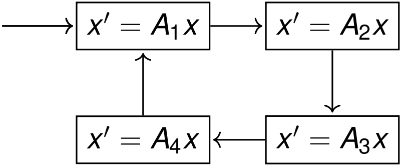
RC circuit





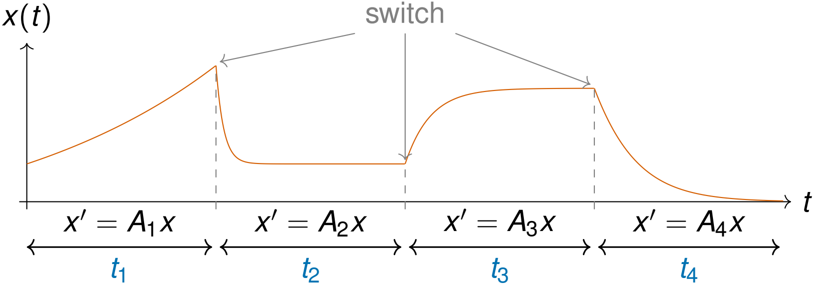
OPEN		CLOSED
$\dot I = 0$ $\dot I_R = -\frac{1}{RC} I_R$ $\dot V_R = -\frac{1}{C} I_R$ $\dot Q = I_R$ $\dot V_C = \frac{1}{C} I_R$	OPEN → CLOSED: $I := \frac{1}{R}(V - V_C)$, $I_R := \frac{1}{R}(V - V_C)$, $V_R := V - V_C$ CLOSED → OPEN: $I := 0$, $I_R := -\frac{1}{R} V_C$, $V_R := -V_C$	$\dot I = -\frac{1}{RC} I_R$ $\dot I_R = -\frac{1}{RC} I_R$ $\dot V_R = -\frac{1}{C} I_R$ $\dot Q = I_R$ $\dot V_C = \frac{1}{C} I_R$

Switching systems

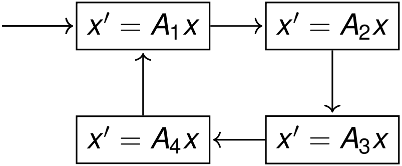


Restricted hybrid system:

- linear dynamics
- no guards (nondeterministic)
- no discrete updates

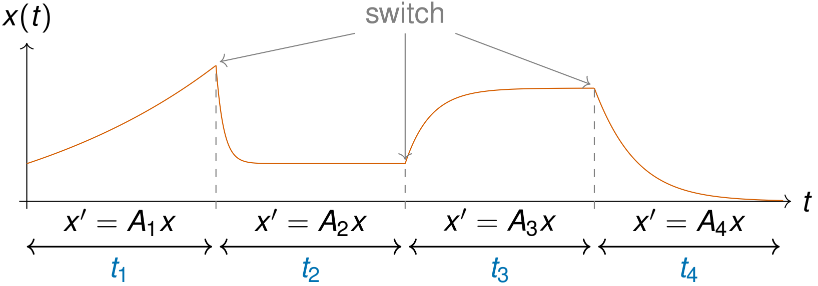


Switching systems



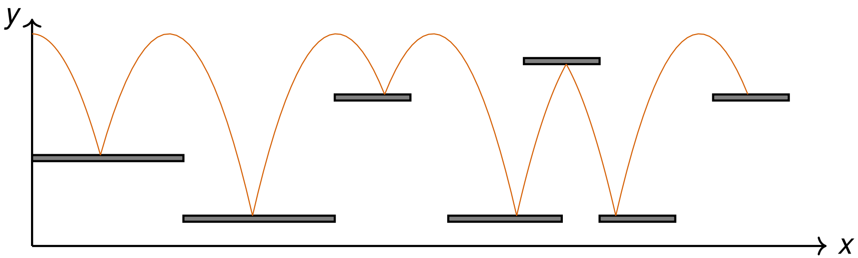
Restricted hybrid system:

- linear dynamics
- no guards (nondeterministic)
- no discrete updates

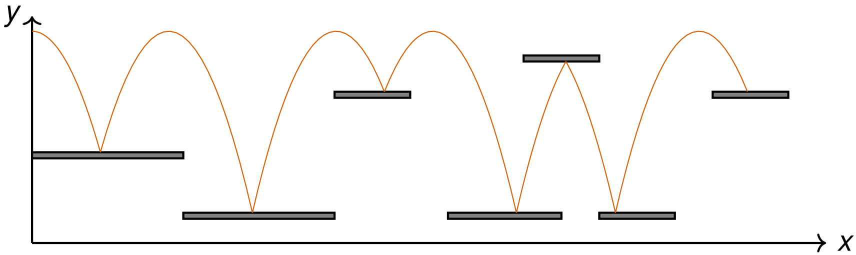


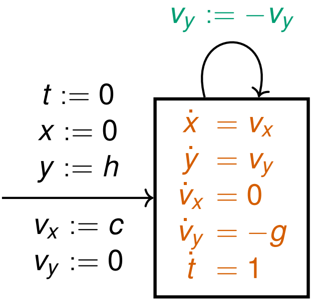
- reachability also undecidable
- invariant synthesis possible

Going hybrid: a bouncing ball



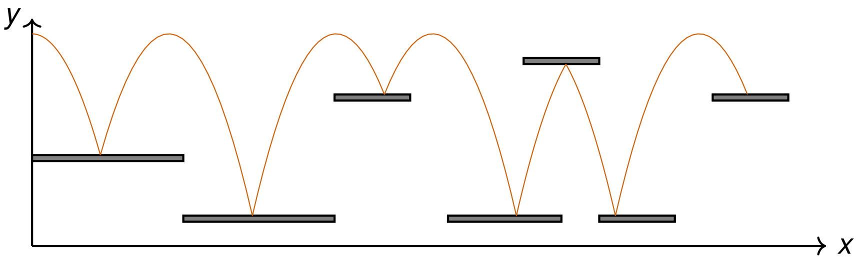
Going hybrid: a bouncing ball





- affine program: collision
- \+ linear differential equation: mechanics
- = linear hybrid automaton

Going hybrid: a bouncing ball



$$v_y := -v_y$$

$$t := 0 \quad x := 0 \quad y := h \quad v_x := c \quad v_y := 0$$

$$\begin{aligned} \dot{x} &= v_x \\ \dot{y} &= v_y \\ \dot{v}_x &= 0 \\ \dot{v}_y &= -g \\ \dot{t} &= 1 \end{aligned}$$

- affine program: collision
- \+ linear differential equation: mechanics
- = linear hybrid automaton

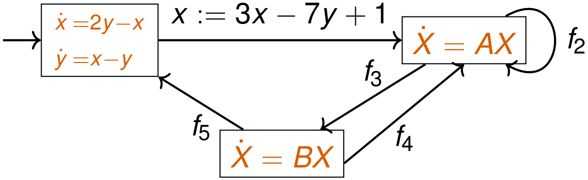
Invariants:

- $v_x = c$
- $x = tc$
- $v_y^2 + 2g(y - h) = 0$

recover conservation of energy!

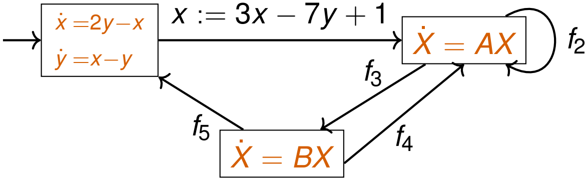
Linear Hybrid Automata

- Nondeterministic branching (no guards)
- All assignments are affine
- Linear differential equations in each location



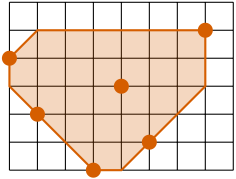
Linear Hybrid Automata

- Nondeterministic branching (no guards)
- All assignments are affine
- Linear differential equations in each location



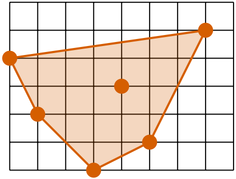
- More general than affine programs
- More general than linear differential equations

Which invariants?



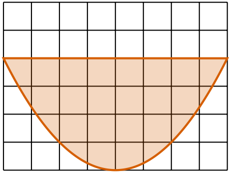
Octagons

$\leqslant$



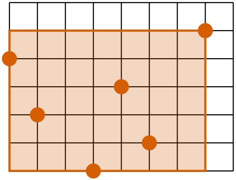
Polyhedrons

$\leqslant$

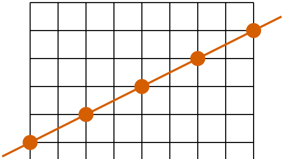


Semialgebraic sets

$\rotatebox{90}{$\leqslant$}$ $\rotatebox{90}{$\leqslant$}$ $\rotatebox{90}{$\leqslant$}$

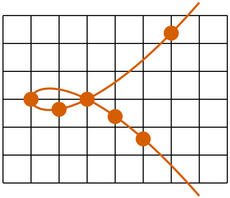


Intervals



Affine/linear sets

$\leqslant$



Algebraic sets =
polynomial equalities

Linear system with rounding

Rounding: $\lfloor \cdot \rceil$ = round to nearest integer

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix} x \\ y \end{pmatrix} \right\rceil = \begin{pmatrix} \lfloor x \rceil \\ \lfloor y \rceil \end{pmatrix}$$

Linear system with rounding

Rounding: $\lfloor \cdot \rceil$ = round to nearest integer

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix} x \\ y \end{pmatrix} \right\rceil = \begin{pmatrix} \lfloor x \rceil \\ \lfloor y \rceil \end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n \rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?

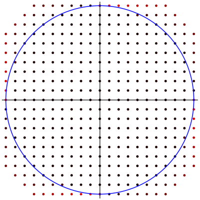
Linear system with rounding

Rounding: $\lfloor \cdot \rceil$ = round to nearest integer

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix} x \\ y \end{pmatrix} \right\rceil = \begin{pmatrix} \lfloor x \rceil \\ \lfloor y \rceil \end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n \rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?



$r = 10, \theta = \pi/42$

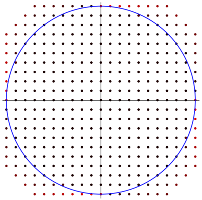
Linear system with rounding

Rounding: $\lfloor \cdot \rceil$ = round to nearest integer

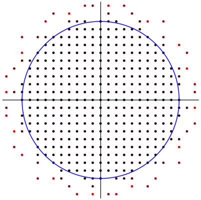
$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix} x \\ y \end{pmatrix} \right\rceil = \begin{pmatrix} \lfloor x \rceil \\ \lfloor y \rceil \end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n \rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?



$r = 10, \theta = \pi/42$



$r = 10, \theta = \frac{2^{0.4}\pi}{10}$

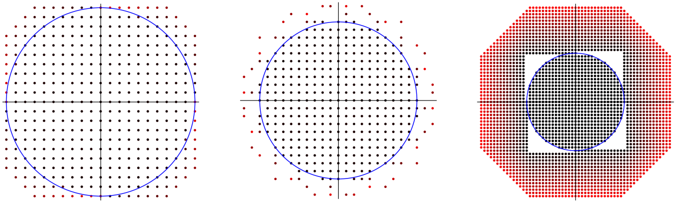
Linear system with rounding

Rounding: $\lfloor\cdot\rceil$ = round to nearest integer

$$A = \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix}x\\y\end{pmatrix}\right\rceil = \begin{pmatrix}\lfloor x\rceil\\ \lfloor y\rceil\end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n\rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?



$r = 10, \theta = \pi/42$ $\quad r = 10, \theta = \frac{2^{0.4}\pi}{10}$ $\quad r = 15, \theta = \pi/91$

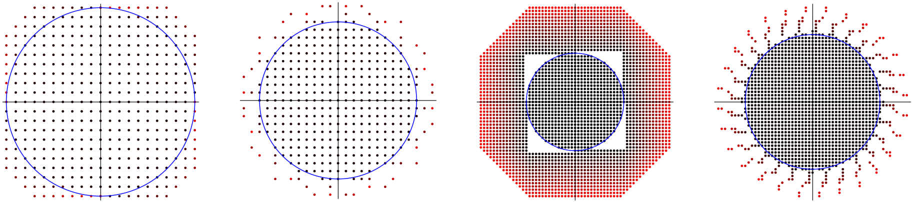
Linear system with rounding

Rounding: $\lfloor \cdot \rceil$ = round to nearest integer

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor \begin{pmatrix} x \\ y \end{pmatrix} \right\rceil = \begin{pmatrix} \lfloor x \rceil \\ \lfloor y \rceil \end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n \rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?



$r = 10, \theta = \pi/42$ $r = 10, \theta = \frac{2^{0.4}\pi}{10}$ $r = 15, \theta = \pi/91$ $r = 20, \theta = \pi/14$

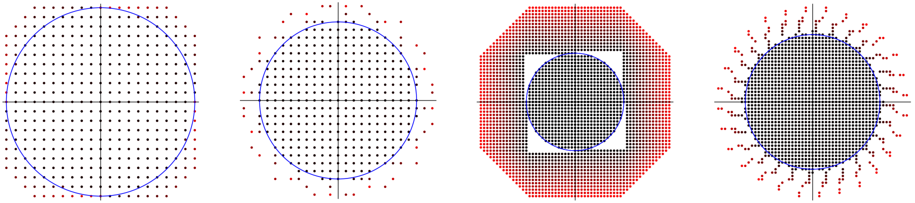
Linear system with rounding

Rounding: $\lfloor\cdot\rceil$ = round to nearest integer

$$A = \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix} \in \mathbb{Q}^{2\times 2}, \qquad \left\lfloor\begin{pmatrix}x\\y\end{pmatrix}\right\rceil = \begin{pmatrix}\lfloor x\rceil\\ \lfloor y\rceil\end{pmatrix}$$

Problem: given $X_0 \in \mathbb{Q}^2$, define $X_{n+1} = \lfloor AX_n\rceil$

- is reachability decidable ?
- is $(X_n)_n$ eventually periodic?
- what does the reachable set look like?



$r = 10, \theta = \pi/42$ $\quad r = 10, \theta = \frac{2^{0.4}\pi}{10}$ $\quad r = 15, \theta = \pi/91$ $\quad r = 20, \theta = \pi/14$

Open problems! Only known for a few specific values of θ.

Linear dynamical systems are ubiquitous...

... and lead to very interesting mathematics!

Interesting related mathematics

- Linear recurrent sequences (LRS)

$$x_{n+k} = a_{k-1}a_{n+k-1} + \cdots + x_0 x_n$$

Fibonacci: $F_{n+2} = F_{n+1} + F_n$

Interesting related mathematics

- Linear recurrent sequences (LRS)

$$x_{n+k} = a_{k-1} a_{n+k-1} + \cdots + x_0 x_n$$

  Fibonacci: $F_{n+2} = F_{n+1} + F_n$

- Skolem/Positivity problem (Open for more than 70 years!)
  decide if a given LRS has a zero/is always positive

Interesting related mathematics

- Linear recurrent sequences (LRS)

$$x_{n+k} = a_{k-1} a_{n+k-1} + \cdots + x_0 x_n$$

  Fibonacci: $F_{n+2} = F_{n+1} + F_n$

- Skolem/Positivity problem (Open for more than 70 years!)
  decide if a given LRS has a zero/is always positive

- Exponential polynomials:

$$f(t) = P_1(t) e^{\lambda_1 t} + \cdots + P_n(t) e^{\lambda_n t}$$

  Examples: polynomials, e^t, $\sin(t)$, $t^2 \sin(t) - e^{-t}$

Interesting related mathematics

- Linear recurrent sequences (LRS)

$$x_{n+k} = a_{k-1}a_{n+k-1} + \cdots + x_0 x_n$$

  Fibonacci: $F_{n+2} = F_{n+1} + F_n$

- Skolem/Positivity problem (Open for more than 70 years!)
  decide if a given LRS has a zero/is always positive

- Exponential polynomials:

$$f(t) = P_1(t)e^{\lambda_1 t} + \cdots + P_n(t)e^{\lambda_n t}$$

  Examples: polynomials, e^t, $\sin(t)$, $t^2 \sin(t) - e^{-t}$

- Continuous Skolem/Positivity (Also open)
  decide if an exponential polynomial has a zero/is always positive

Interesting related mathematics

- Linear recurrent sequences (LRS)

$$x_{n+k} = a_{k-1}a_{n+k-1} + \cdots + x_0 x_n$$

  Fibonacci: $F_{n+2} = F_{n+1} + F_n$

- Skolem/Positivity problem (Open for more than 70 years!)
  decide if a given LRS has a zero/is always positive

- Exponential polynomials:

$$f(t) = P_1(t)e^{\lambda_1 t} + \cdots + P_n(t)e^{\lambda_n t}$$

  Examples: polynomials, e^t, $\sin(t)$, $t^2 \sin(t) - e^{-t}$

- Continuous Skolem/Positivity (Also open)
  decide if an exponential polynomial has a zero/is always positive

Reachability often harder/reduces to of these problems!

Algebraic numbers and conjectures

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Algebraic numbers and conjectures

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Gelfond–Schneider theorem)

If a, b are algebraic numbers with $a \neq 0, 1$ and b irrational, then (any value of) a^b transcendental.

Example: $2^{\sqrt{2}}$ is transcendental.

Algebraic numbers and conjectures

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Gelfond–Schneider theorem)

If a, b are algebraic numbers with $a \neq 0, 1$ and b irrational, then (any value of) a^b transcendental.

Example: $2^{\sqrt{2}}$ is transcendental.

Why is this related to reachability?

- target is usually rational/algebraic
- reachability creates constraints between numbers

Example: given $a, b \in \mathbb{Q}$, $P \in \mathbb{Q}[X]$ polynomial, find t such that

$$P(t) = a \quad \text{and} \quad e^t = b$$

Algebraic numbers and conjectures

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Gelfond–Schneider theorem)

If a, b are algebraic numbers with $a \neq 0, 1$ and b irrational, then (any value of) a^b transcendental.

Example: $2^{\sqrt{2}}$ is transcendental.

Why is this related to reachability?

- target is usually rational/algebraic
- reachability creates constraints between numbers

Example: given $a, b \in \mathbb{Q}$, $P \in \mathbb{Q}[X]$ polynomial, find t such that

$$P(t) = a \quad \text{and} \quad e^t = b \qquad \rightsquigarrow \text{impossible unless } t = 0$$

Algebraic numbers and conjectures

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Gelfond–Schneider theorem)

If a, b are algebraic numbers with $a \neq 0, 1$ and b irrational, then (any value of) a^b transcendental.

Example: $2^{\sqrt{2}}$ is transcendental.

Why is this related to reachability?

- target is usually rational/algebraic
- reachability creates constraints between numbers

Example: given $a, b \in \mathbb{Q}$, $P \in \mathbb{Q}[X]$ polynomial, find t such that

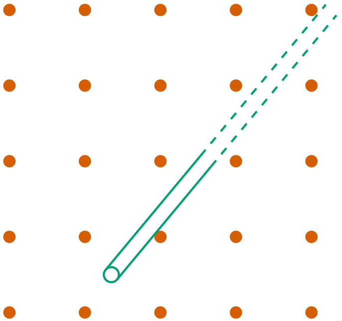
$$P(t) = a \quad \text{and} \quad e^t = b \qquad \rightsquigarrow \text{impossible unless } t = 0$$

Biggest open question in this field: Schanuel's conjecture

Transcendental number theory

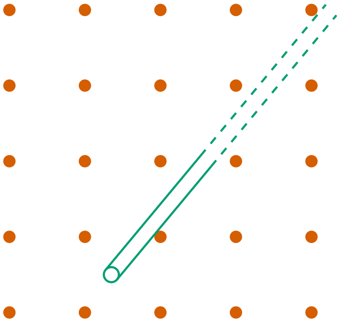
Many problems boil down to diophantine equations/approximations:

- Finding integer points in cones: Kronecker's theorem



Many problems boil down to diophantine equations/approximations:

- Finding integer points in cones: Kronecker's theorem



- Compare linear forms in logarithms: Baker's theorem

$$\sqrt{2} + \log\sqrt{3} - 3\log\sqrt{7} \overset{?}{=} 1 + \log 9 - \log \sqrt[42]{666}$$

(Semi-)group theory

Finitely generated matrix semigroup:

$A_1, \ldots, A_k \in \mathbb{Q}^{n \times n}$ generate a semigroup $S = \langle A_1, \ldots, A_k \rangle$

Example: $\mathsf{SL}_2(\mathbb{Z}) = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \right\rangle$

(Semi-)group theory

Finitely generated matrix semigroup:

$A_1, \dots, A_k \in \mathbb{Q}^{n\times n}$ generate a semigroup $S = \langle A_1, \dots, A_k \rangle$

Example: $\mathrm{SL}_2(\mathbb{Z}) = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \right\rangle$

Problems:

- finitness: is S finite ?
- mortality: does $0 \in S$?
- identity: does $I_n \in S$?
- membership: does $M \in S$ where $M \in \mathbb{Q}^{n\times n}$ is given as input ?

(Semi-)group theory

Finitely generated matrix semigroup:
$A_1, \dots, A_k \in \mathbb{Q}^{n \times n}$ generate a semigroup $S = \langle A_1, \dots, A_k \rangle$

Example: $\mathrm{SL}_2(\mathbb{Z}) = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \right\rangle$

Problems:

- finitness: is S finite ?
- mortality: does $0 \in S$?
- identity: does $I_n \in S$?
- membership: does $M \in S$ where $M \in \mathbb{Q}^{n \times n}$ is given as input ?

Undecidable in general, many decidable subclasses are known.
Equivalent to reachability of affine programs.

Algebraic geometry

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

$$\begin{aligned} x^2 + y^2 + z^2 - 1 = 0 \quad &\rightsquigarrow \quad \text{sphere in } \mathbb{R}^3 \\ x^2 + y^2 + z^2 = 1 \ \wedge \ x + y + z = 1 \quad &\rightsquigarrow \quad \text{"sliced" sphere in } \mathbb{R}^3 \\ x^2 + 1 = 0 \quad &\rightsquigarrow \quad \varnothing \text{ in } \mathbb{R} \\ x^2 + 1 = 0 \quad &\rightsquigarrow \quad \{i, -i\} \text{ in } \mathbb{C} \end{aligned}$$

Algebraic geometry

Study systems of multivariate polynomial equations using abstract algebraic techniques, with applications to geometry.

Examples

$$
\begin{aligned}
x^2+y^2+z^2-1=0 \quad &\rightsquigarrow \quad \text{sphere in } \mathbb{R}^3 \\
x^2+y^2+z^2=1 \ \wedge \ x+y+z=1 \quad &\rightsquigarrow \quad \text{“sliced” sphere in } \mathbb{R}^3 \\
x^2+1=0 \quad &\rightsquigarrow \quad \varnothing \text{ in } \mathbb{R} \\
x^2+1=0 \quad &\rightsquigarrow \quad \{i,-i\} \text{ in } \mathbb{C}
\end{aligned}
$$

The field $\mathbb{K}$ is very important:

- real algebraic geometry: more “intuitive” but more difficult, really requires the study of *semi-algebraic sets*
- mainstream algebraic geometry: $\mathbb{K}$ is algebraically closed†, e.g. $\mathbb{C}$

† $\mathbb{K}$ is algebraically closed if every non-constant polynomial has a root in $\mathbb{K}$.

First-order theory of the reals

Many questions expressible in first-order logical theories:

- $\mathfrak{R}_0 = (\mathbb{R}, 0, 1, <, +, \cdot)$: decidable

$$\forall x, y \in \mathbb{R} \; \frac{x+y}{2} \geqslant \sqrt{xy}$$

First-order theory of the reals

Many questions expressible in first-order logical theories:

- $\mathfrak{R}_0 = (\mathbb{R}, 0, 1, <, +, \cdot)$: decidable

$$\forall x, y \in \mathbb{R}\ \frac{x+y}{2} \geqslant \sqrt{xy}$$

- $\mathfrak{R}_{\exp} = (\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,1]})$: decidable subject to Schanuel's conjecture

$$\forall x \in \mathbb{R}\ x \neq 0 \Rightarrow t + te^{t} - 43e^{3t} \neq 1$$

First-order theory of the reals

Many questions expressible in first-order logical theories:

- $\mathfrak{R}_0 = (\mathbb{R}, 0, 1, <, +, \cdot)$: decidable

$$\forall x, y \in \mathbb{R}\ \frac{x+y}{2} \geqslant \sqrt{xy}$$

- $\mathfrak{R}_{\exp} = (\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,1]})$: decidable subject to Schanuel's conjecture

$$\forall x \in \mathbb{R}\ x \neq 0 \Rightarrow t + te^{t} - 43e^{3t} \neq 1$$

- Presburger arithmetic $(\mathbb{N}, 0, 1, <, +)$: decidable

$$\exists x \in \mathbb{N}^n\ Ax \geqslant b$$

Summary

Linear dynamical systems are ubiquitous and exact reachability questions lead to very interesting mathematical and logical questions.

Summary

Linear dynamical systems are ubiquitous and exact reachability questions lead to very interesting mathematical and logical questions.

But...

- some systems are fundamentally nonlinear

$$x_{n+1} = x_n^2$$

Summary

Linear dynamical systems are ubiquitous and exact reachability questions lead to very interesting mathematical and logical questions.

But...

- some systems are fundamentally nonlinear

$$x_{n+1} = x_n^2$$

- real programs manipulate data structures:

trees, arrays, ...

Summary

Linear dynamical systems are ubiquitous and exact reachability questions lead to very interesting mathematical and logical questions.

But...

- some systems are fundamentally nonlinear

$$x_{n+1} = x_n^2$$

- real programs manipulate data structures:

trees, arrays, ...

- some programs are not sequential / nondeterministic

probabilistic, concurrent/parallell, ...

Summary

Linear dynamical systems are ubiquitous and exact reachability questions lead to very interesting mathematical and logical questions.

But...

- some systems are fundamentally nonlinear

$$x_{n+1} = x_n^2$$

- real programs manipulate data structures:

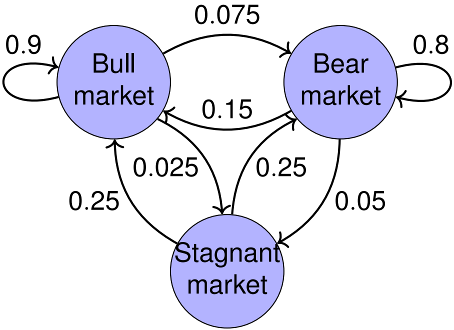
  trees, arrays, ...
- some programs are not sequential / nondeterministic

  probabilistic, concurrent/parallell, ...
- exact reachability is not the only approach

  testing, probabilistic model checking, incomplete algorithms, ...

Reachability

Examples: while loop, Markov chain



State: $X = (p_{bull}, p_{bear}, p_{stag}) \in [0,1]^3$
Transitions:

$$A = \begin{bmatrix} 0.9 & 0.15 & 0.25 \\ 0.075 & 0.8 & 0.25 \\ 0.025 & 0.05 & 0.5 \end{bmatrix}$$

$\to$ Linear dynamical system

$$X_{n+1} = AX_n$$

Linear loop

$p_{bull} := 0$
$p_{bear} := 1$
$p_{stag} := 0$
while $p_{bull} \leqslant 1/2$ do

$$\begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix} := A \begin{bmatrix} p_{bull} \\ p_{bear} \\ p_{stag} \end{bmatrix}$$

The loop terminates if and only if the probability of a bull market is $> 1/2$.

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x := 2^{-10}, y := 1$
until $\phi(x)$ do

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

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x := 2^{-10}, y := 1$
until $\phi(x)$ do

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\ A^n x_0 \in \mathcal{S}$.

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x := 2^{-10}, y := 1$

until $x = 42$ and $y = 36$ do

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\ A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:

$$\exists n \in \mathbb{N}\ A^n x_0 = y$$

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x := 2^{-10}, y := 1$
until $x = y$ do

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\ A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:

$$\exists n \in \mathbb{N}\ A^n x_0 = y$$

- affine subspace:

$$\exists n \in \mathbb{N}\ MA^n x_0 = b$$

Termination Linear Loops

Does this loop terminate?

Linear Loop

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

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}. A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:

$$\exists n \in \mathbb{N}\ A^n x_0 = y$$

- affine subspace:

$$\exists n \in \mathbb{N}\ M A^n x_0 = b$$

- polyhedron:

$$\exists n \in \mathbb{N}\ M A^n x_0 \geqslant b$$

Termination Linear Loops

Does this loop terminate?

Linear Loop

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

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\ A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:

$$\exists n \in \mathbb{N}\ A^n x_0 = y$$

- affine subspace:

$$\exists n \in \mathbb{N}\ M A^n x_0 = b$$

- polyhedron:

$$\exists n \in \mathbb{N}\ M A^n x_0 \geqslant b$$

- (semi-)algebraic sets

$$\exists n \in \mathbb{N}\ p(A^n x_0) \geqslant 0$$

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x := 2^{-10}, y := 1$
until $x^2 y \geqslant 1$ or $x = y$ do

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

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\ A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:

$$\exists n \in \mathbb{N}\ A^n x_0 = y$$

- affine subspace:

$$\exists n \in \mathbb{N}\ M A^n x_0 = b$$

- polyhedron:

$$\exists n \in \mathbb{N}\ M A^n x_0 \geqslant b$$

- (semi-)algebraic sets

$$\exists n \in \mathbb{N}\ p(A^n x_0) \geqslant 0$$

- boolean combinations

Termination Linear Loops

Does this loop terminate?

Linear Loop

$x \in [0,1], y \in [1,2]$
until $\phi(x)$ do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$\rightsquigarrow$

Reachability problem

Given

- initial point: $x_0 \in \mathbb{Q}^d$,
- transition matrix: $A \in \mathbb{Q}^{d \times d}$,
- target set: $\mathcal{S} \subseteq \mathbb{R}^d$

decide if $\exists n \in \mathbb{N}.\, A^n x_0 \in \mathcal{S}$.

Natural choices for $\mathcal{S}$:

- point:
$$\exists n \in \mathbb{N}\ A^n x_0 = y$$
- affine subspace:
$$\exists n \in \mathbb{N}\ MA^n x_0 = b$$
- polyhedron:
$$\exists n \in \mathbb{N}\ MA^n x_0 \geqslant b$$
- (semi-)algebraic sets
$$\exists n \in \mathbb{N}\ p(A^n x_0) \geqslant 0$$
- boolean combinations
- replace x_0 by an initial set $\mathcal{X}$
$$\exists x_0 \in \mathcal{X} \exists n \in \mathbb{N}\ A^n x_0 \in \mathcal{S}$$
$$\forall x_0 \in \mathcal{X} \exists n \in \mathbb{N}\ A^n x_0 \in \mathcal{S}$$

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

Theorem (Orbit problem; Kannan and Lipton 1980, 1986)

Decidable in polynomial time when $\mathcal{S}$ is a singleton.

Already nontrivial proof using algebraic number theory!

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

Theorem (Orbit problem; Kannan and Lipton 1980, 1986)

Decidable in polynomial time when $\mathcal{S}$ is a singleton.

Already nontrivial proof using algebraic number theory!

Theorem (Chonev, Ouaknine and Worrell, 2016)

Decidable (in $\mathrm{NP}^{\mathrm{RP}}$) when $\mathcal{S}$ is a linear subspace of dimension $\leqslant 3$.

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

Theorem (Orbit problem; Kannan and Lipton 1980, 1986)

Decidable in polynomial time when $\mathcal{S}$ is a singleton.

Already nontrivial proof using algebraic number theory!

Theorem (Chonev, Ouaknine and Worrell, 2016)

Decidable (in NP^{RP}) when $\mathcal{S}$ is a linear subspace of dimension $\leqslant 3$.
Decidable (in PSPACE) when $\mathcal{S}$ is a polytope of dimension $\leqslant 3$.

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

Theorem (Orbit problem; Kannan and Lipton 1980, 1986)

Decidable in polynomial time when $\mathcal{S}$ is a singleton.

Already nontrivial proof using algebraic number theory!

Theorem (Chonev, Ouaknine and Worrell, 2016)

Decidable (in NP^{RP}) when $\mathcal{S}$ is a linear subspace of dimension $\leqslant 3$.
Decidable (in PSPACE) when $\mathcal{S}$ is a polytope of dimension $\leqslant 3$.

Problem: given $\mathcal{X}$, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n \mathcal{X} \cap \mathcal{S} \neq \varnothing$.

Theorem (Almagor, Ouaknine and Worrell, 2017)

Decidable (in PSPACE) when $\mathcal{X}, \mathcal{S}$ are polytopes of dimension $\leqslant 3$.

What is decidable about linear loops?

Problem: given x_0, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n x_0 \in \mathcal{S}$.

Theorem (Orbit problem; Kannan and Lipton 1980, 1986)

Decidable in polynomial time when $\mathcal{S}$ is a singleton.

Already nontrivial proof using algebraic number theory!

Theorem (Chonev, Ouaknine and Worrell, 2016)

Decidable (in NP^{RP}) when $\mathcal{S}$ is a linear subspace of dimension $\leqslant 3$.
Decidable (in PSPACE) when $\mathcal{S}$ is a polytope of dimension $\leqslant 3$.

Problem: given $\mathcal{X}$, A and $\mathcal{S}$, decide if $\exists n \in \mathbb{N}$ such that $A^n \mathcal{X} \cap \mathcal{S} \neq \varnothing$.

Theorem (Almagor, Ouaknine and Worrell, 2017)

Decidable (in PSPACE) when $\mathcal{X}, \mathcal{S}$ are polytopes of dimension $\leqslant 3$.

Why do we need the dimension to be small?

From loops to recurrent sequences

Linear Loop

$x := x_0$
until $3x_1 - 7x_2 + 4x_3 = 0$ do
$x := Ax$

From loops to recurrent sequences

Linear Loop

$x := x_0$
until $y^T x = 0$ do $x := Ax$

$\rightsquigarrow$

Half-space reachability

Given $x, y \in \mathbb{Q}^d$, $A \in \mathbb{Q}^{d \times d}$,
decide if $\exists n \in \mathbb{N}.\, y^T A^n x_0 = 0$.

From loops to recurrent sequences

Linear Loop

$x := x_0$
until $y^T x = 0$ do $x := Ax$

$\rightsquigarrow$

Half-space reachability

Given $x, y \in \mathbb{Q}^d$, $A \in \mathbb{Q}^{d\times d}$,
decide if $\exists n \in \mathbb{N}.\, y^T A^n x_0 = 0$.

Consider the sequence $u_n = y^T A^n x$.

Lemma

There exists $a_0, \ldots, a_{d-1} \in \mathbb{Q}$ such that

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

In other words, $(u_n)_n$ is a linear recurrent sequence (LRS).

From loops to recurrent sequences

Linear Loop

$x := x_0$
until $y^T x = 0$ do $x := Ax$

$\rightsquigarrow$

Half-space reachability

Given $x, y \in \mathbb{Q}^d$, $A \in \mathbb{Q}^{d\times d}$,
decide if $\exists n \in \mathbb{N}.\, y^T A^n x_0 = 0$.

Consider the sequence $u_n = y^T A^n x$.

Lemma

There exists $a_0, \ldots, a_{d-1} \in \mathbb{Q}$ such that

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

In other words, $(u_n)_n$ is a linear recurrent sequence (LRS).

- Fibonacci: $F_{n+2} = F_{n+1} + F_n$
- Pell numbers: $P_{n+2} = 2P_{n+1} + P_n$
- very common in combinatorics

From loops to recurrent sequences

Linear Loop

$x := x_0$
until $y^T x = 0$ do $x := Ax$

$\rightsquigarrow$

Half-space reachability

Given $x, y \in \mathbb{Q}^d$, $A \in \mathbb{Q}^{d\times d}$,
decide if $\exists n \in \mathbb{N}.\, y^T A^n x_0 = 0$.

Consider the sequence $u_n = y^T A^n x$.

Lemma

There exists $a_0, \ldots, a_{d-1} \in \mathbb{Q}$ such that

$$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

In other words, $(u_n)_n$ is a linear recurrent sequence (LRS). Conversely,

Lemma

For any LRS $(u_n)_n$, there exists x_0, y and A such that $u_n = y^T A^n x_0$.

Skolem and posivity problems

Linear recurrent sequence (LRS) of order d:

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

Remark: entirely determined by $u_0, \ldots, u_{d-1}$ and $a_0, \ldots, a_{d-1}$

Skolem and posivity problems

Linear recurrent sequence (LRS) of order d:

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

Remark: entirely determined by $u_0, \ldots, u_{d-1}$ and $a_0, \ldots, a_{d-1}$

Skolem Problem

Given a LRS $(u_n)_n$, decide if $u_n = 0$ for some $n \in \mathbb{N}$.

This problem has been open for 70 years!

Skolem and posivity problems

Linear recurrent sequence (LRS) of order d:

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0 u_n, \qquad \forall n \in \mathbb{N}.$$

Remark: entirely determined by $u_0, \ldots, u_{d-1}$ and $a_0, \ldots, a_{d-1}$

Skolem Problem

Given a LRS $(u_n)_n$, decide if $u_n = 0$ for some $n \in \mathbb{N}$.

This problem has been open for 70 years!

Positivity Problem

Given a LRS $(u_n)_n$, decide if $u_n \geqslant 0$ for all $n \in \mathbb{N}$.

Harder than Skolem

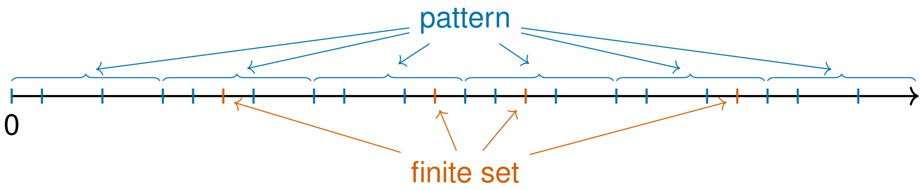
Skolem-Mahler-Lech theorem

Skolem Problem

Given a LRS $(u_n)_n$, decide if $u_n = 0$ for some $n \in \mathbb{N}$.

Theorem (Skolem, Mahler, and Lech, 1933, 1953, 1957)

The set $\{n \in \mathbb{N} : u_n = 0\}$ is a union of finitely arithmetic progression and a finite set.



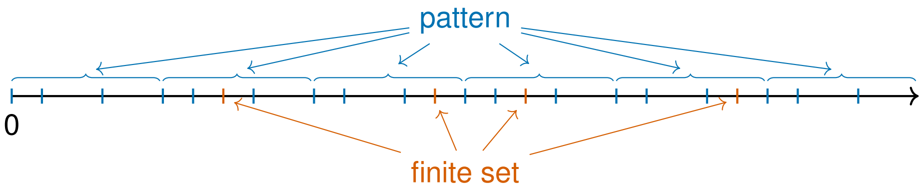
Skolem-Mahler-Lech theorem

Skolem Problem

Given a LRS $(u_n)_n$, decide if $u_n = 0$ for some $n \in \mathbb{N}$.

Theorem (Skolem, Mahler, and Lech, 1933, 1953, 1957)

The set $\{n \in \mathbb{N} : u_n = 0\}$ *is a union of finitely arithmetic progression and a finite set.*



The regular patterm is computable. Nothing is known about the finite set: the proof is nonconstructive and uses p-adic analysis.

Skolem in low dimension

Theorem (Mignotte, Shorey, Tijdeman; Vereshchagin, 1985)

The Skolem problem is decidable for LRS of order 4.

Skolem in low dimension

Theorem (Mignotte, Shorey, Tijdeman; Vereshchagin, 1985)

The Skolem problem is decidable for LRS of order 4.

Theorem (Blondel and Portier, 2002)

The Skolem problem is NP-hard.

Skolem in low dimension

Theorem (Mignotte, Shorey, Tijdeman; Vereshchagin, 1985)

The Skolem problem is decidable for LRS of order 4.

Theorem (Blondel and Portier, 2002)

The Skolem problem is NP-hard.

How can we show hardness without proving undecidability?

Skolem in low dimension

Theorem (Mignotte, Shorey, Tijdeman; Vereshchagin, 1985)

The Skolem problem is decidable for LRS of order 4*.*

Theorem (Blondel and Portier, 2002)

The Skolem problem is NP-hard.

For any $x \in \mathbb{R}$, the (homogeneous Diophantine approximation) type

$$L(x) = \inf\left\{c \in \mathbb{R} : \left|x - \frac{n}{m}\right| < \frac{c}{m^2} \text{ for some } n, m \in \mathbb{Z}\right\}.$$

Intuitively, if $L(x) > 0$ then x is badly approximable by rationals.

Skolem in low dimension

Theorem (Mignotte, Shorey, Tijdeman; Vereshchagin, 1985)

The Skolem problem is decidable for LRS of order 4.

Theorem (Blondel and Portier, 2002)

The Skolem problem is NP-hard.

For any $x \in \mathbb{R}$, the (homogeneous Diophantine approximation) type

$$L(x) = \inf \left\{ c \in \mathbb{R} : \left| x - \frac{n}{m} \right| < \frac{c}{m^2} \text{ for some } n, m \in \mathbb{Z} \right\}.$$

Intuitively, if $L(x) > 0$ then x is badly approximable by rationals. Almost nothing known for any concrete x except that $L(x) \in [0, 1/\sqrt{5}]$.

Theorem (Ouaknine and Worrell, 2013)

If Skolem is decidable at order 5 then one can approximate $L(x)$ *with arbitrary precision for a large class of numbers* x.

Positivity and eventual posivity

Positivity Problem

Given a LRS $(u_n)_n$, decide if $u_n \geqslant 0$ for all $n \in \mathbb{N}$.

Positivity and eventual posivity

Positivity Problem

Given a LRS $(u_n)_n$, decide if $u_n \geqslant 0$ for all $n \in \mathbb{N}$.

Theorem (Laohakosol and Tangsupphathawat, 2009)

The positivity problem is decidable at order 3.

Positivity and eventual posivity

Positivity Problem

Given a LRS $(u_n)_n$, decide if $u_n \geqslant 0$ for all $n \in \mathbb{N}$.

Theorem (Laohakosol and Tangsupphathawat, 2009)

The positivity problem is decidable at order 3*.*

Ultimate positivity Problem

Given a LRS $(u_n)_n$, decide if $\exists N \in \mathbb{N}$, such that $u_n \geqslant 0$ for all $n \geqslant N$.

Positivity and eventual posivity

Positivity Problem

Given a LRS $(u_n)_n$, decide if $u_n \geqslant 0$ for all $n \in \mathbb{N}$.

Theorem (Laohakosol and Tangsupphathawat, 2009)

The positivity problem is decidable at order 3*.*

Ultimate positivity Problem

Given a LRS $(u_n)_n$, decide if $\exists N \in \mathbb{N}$, such that $u_n \geqslant 0$ for all $n \geqslant N$.

Theorem (Ouaknine and Worrell, 2014)

The ultimate positivity problem is decidable for simple[‡] *LRS. It is at least as hard as deciding* $\exists\mathbb{R}$*.*

[‡] The associated characteristic polynomial has no repeated roots.

First-order queries on orbits

First-order orbit query (FOOQ): fully quantified first-order sentence whose atomic proposition are of the form

$$p(x) \geqslant 0, \qquad A^n x \in T \quad \text{(T semialgebraic set).}$$

First-order queries on orbits

First-order orbit query (FOOQ): fully quantified first-order sentence whose atomic proposition are of the form

$$p(x) \geqslant 0, \qquad A^n x \in T \quad \text{(T semialgebraic set).}$$

Examples: $\exists n \in \mathbb{N}$ such that...

- $A^n x = y$: $A^n x \in \{y\}$

First-order queries on orbits

First-order orbit query (FOOQ): fully quantified first-order sentence whose atomic proposition are of the form

$$p(x) \geqslant 0, \qquad A^n x \in T \quad \text{(T semialgebraic set).}$$

Examples: $\exists n \in \mathbb{N}$ such that...

- $A^n x = y$: $A^n x \in \{y\}$
- $A^n S \cap T \neq \varnothing$: $\exists x \in \mathbb{R}^d.\, x \in S \wedge A^n x \in T$

First-order queries on orbits

First-order orbit query (FOOQ): fully quantified first-order sentence whose atomic proposition are of the form

$$p(x) \geqslant 0, \qquad A^n x \in T \quad \text{(T semialgebraic set).}$$

Examples: $\exists n \in \mathbb{N}$ such that...

- $A^n x = y$: $A^n x \in \{y\}$
- $A^n S \cap T \neq \varnothing$: $\exists x \in \mathbb{R}^d . \, x \in S \wedge A^n x \in T$
- $A^n S \subseteq T$: $\forall x \in \mathbb{R}^d . \, x \in S \rightarrow A^n x \in T$

First-order queries on orbits

First-order orbit query (FOOQ): fully quantified first-order sentence whose atomic proposition are of the form

$$p(x) \geqslant 0, \qquad A^n x \in T \quad \text{(T semialgebraic set).}$$

Examples: $\exists n \in \mathbb{N}$ such that...

- $A^n x = y$: $A^n x \in \{y\}$
- $A^n S \cap T \neq \varnothing$: $\exists x \in \mathbb{R}^d .\, x \in S \wedge A^n x \in T$
- $A^n S \subseteq T$: $\forall x \in \mathbb{R}^d .\, x \in S \rightarrow A^n x \in T$

Theorem (Almagor, Ouaknine and Worrell, 2021)

Given A and $\Phi(n)$ a FOOQ, it is decidable whether $\exists n \in \mathbb{N}.\, \Phi(n)$ in dimension $\leqslant 3$.

MSO model-checking

Given $x \in \mathbb{Q}^d$ and $A \in \mathbb{Q}^{n \times n}$ and $\mathcal{T}_1, \ldots, \mathcal{T}_k \subseteq \mathbb{R}^d$ semialgebraic sets.

MSO model-checking

Given $x \in \mathbb{Q}^d$ and $A \in \mathbb{Q}^{n\times n}$ and $\mathcal{T}_1, \ldots, \mathcal{T}_k \subseteq \mathbb{R}^d$ semialgebraic sets.
Let $\Sigma = \{0,1\}^k$ and define $w \in \Sigma^{\mathbb{N}}$ by

$$w_n = \left(A^n x \in \mathcal{T}_1, \ldots, A^n x \in \mathcal{T}_k\right).$$

Intuition: w_n records to which sets $A^n x$ belongs to at eact step n.

MSO model-checking

Given $x \in \mathbb{Q}^d$ and $A \in \mathbb{Q}^{n \times n}$ and $\mathcal{T}_1, \ldots, \mathcal{T}_k \subseteq \mathbb{R}^d$ semialgebraic sets.
Let $\Sigma = \{0, 1\}^k$ and define $w \in \Sigma^{\mathbb{N}}$ by

$$w_n = \big(A^n x \in \mathcal{T}_1, \ldots, A^n x \in \mathcal{T}_k\big).$$

Intuition: w_n records to which sets $A^n x$ belongs to at eact step n.
Problem: given an MSO formula Ψ over $(\mathbb{N}, <)$, decide whether $w \models \Psi$.

Examples: $P_i(n)$ means $A^n x \in \mathcal{T}_i$

- $\mathcal{T}_i$ is reachable: $\exists n.\, P_i(n)$
- whenever $\mathcal{T}_i$ is visited $\mathcal{T}_j$ is visited some point later:

$$\forall n : P_i(n) \Rightarrow (\exists m > n : P_j(m))$$

MSO model-checking

Given $x \in \mathbb{Q}^d$ and $A \in \mathbb{Q}^{n \times n}$ and $\mathcal{T}_1, \dots, \mathcal{T}_k \subseteq \mathbb{R}^d$ semialgebraic sets.
Let $\Sigma = \{0,1\}^k$ and define $w \in \Sigma^{\mathbb{N}}$ by

$$w_n = \big(A^n x \in \mathcal{T}_1, \dots, A^n x \in \mathcal{T}_k\big).$$

Intuition: w_n records to which sets $A^n x$ belongs to at eact step n.
Problem: given an MSO formula Ψ over $(\mathbb{N}, <)$, decide whether $w \models \Psi$.

Examples: $P_i(n)$ means $A^n x \in \mathcal{T}_i$

- $\mathcal{T}_i$ is reachable: $\exists n.\, P_i(n)$
- whenever $\mathcal{T}_i$ is visited $\mathcal{T}_j$ is visited some point later:

$$\forall n : P_i(n) \Rightarrow (\exists m > n : P_j(m))$$

- in target $\mathcal{T}_i$ at every odd position:

$$\exists O \subseteq \mathbb{N} : \boxed{\text{formula to define odd numbers}} \wedge \forall x : x \in O \Rightarrow P_i(x)$$

MSO model-checking

Given $x \in \mathbb{Q}^d$ and $A \in \mathbb{Q}^{n\times n}$ and $\mathcal{T}_1, \ldots, \mathcal{T}_k \subseteq \mathbb{R}^d$ semialgebraic sets.
Let $\Sigma = \{0,1\}^k$ and define $w \in \Sigma^{\mathbb{N}}$ by

$$w_n = \big(A^n x \in \mathcal{T}_1, \ldots, A^n x \in \mathcal{T}_k\big).$$

Intuition: w_n records to which sets $A^n x$ belongs to at eact step n.
Problem: given an MSO formula Ψ over $(\mathbb{N}, <)$, decide whether $w \models \Psi$.

Theorem (Karimov, Lefaucheux, Ouaknine, Purser, Varonka, Whiteland, Worrell)

This is decidable if all $\mathcal{T}_i$ either have intrinsic dimension 1 or are included in a subspace of dimension 3.

Examples: $P_i(n)$ means $A^n x \in \mathcal{T}_i$

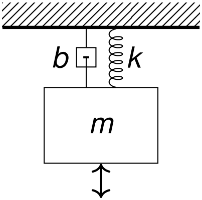
- $\mathcal{T}_i$ is reachable: $\exists n.\, P_i(n)$
- whenever $\mathcal{T}_i$ is visited $\mathcal{T}_j$ is visited some point later:

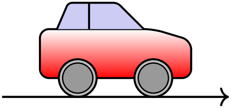
$$\forall n : P_i(n) \Rightarrow (\exists m > n : P_j(m))$$

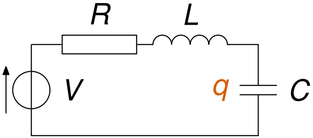
- in target $\mathcal{T}_i$ at every odd position:

$$\exists O \subseteq \mathbb{N} : \boxed{\text{formula to define odd numbers}} \wedge \forall x : x \in O \Rightarrow P_i(x)$$

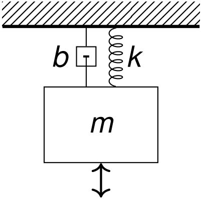
Continuous linear dynamical systems

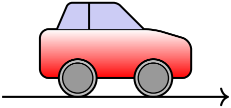


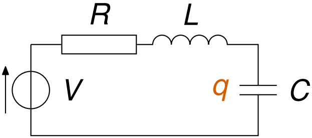




Continuous linear dynamical systems







Linear differential equation:

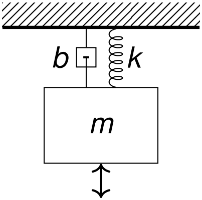
$$x'(t) = Ax(t) \qquad x(0) = x_0$$

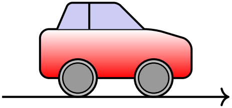
Example:

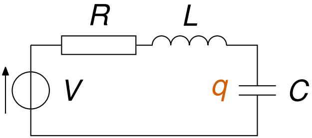
$$x'(t) = 7x(t)$$

$$\rightsquigarrow x(t) = e^{7t}$$

Continuous linear dynamical systems







Linear differential equation:

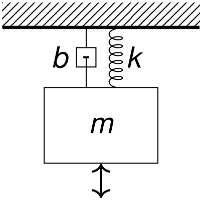
$$x'(t) = Ax(t) \qquad x(0) = x_0$$

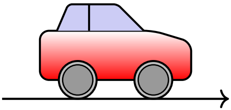
Example:

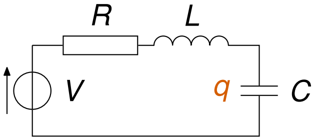
$$x'(t) = 7x(t) \qquad \begin{cases} x_1'(t) = x_2(t) \\ x_2'(t) = -x_1(t) \end{cases} \Leftrightarrow \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}' = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\rightsquigarrow x(t) = e^{7t} \qquad \rightsquigarrow \begin{cases} x_1(t) = \sin(t) \\ x_2(t) = \cos(t) \end{cases}$$

Continuous linear dynamical systems







Linear differential equation:

$$x'(t) = Ax(t) \qquad x(0) = x_0$$

General solution form:

$$x(t) = e^{At}x_0$$

$$\text{where } e^M = \sum_{n=0}^{\infty} \frac{M^n}{n!}$$

Continuous reachability

Continuous Skolem problem

Given x, y and A, decide if $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Continuous reachability

Continuous Skolem problem

Given x, y and A, decide if $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Bounded continuous Skolem problem

Given x, y and A, decide if $\exists t \in [0, 1]$ such that $x^T e^{At} y = 0$.

Continuous reachability

Continuous Skolem problem

Given x, y and A, decide if $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Bounded continuous Skolem problem

Given x, y and A, decide if $\exists t \in [0, 1]$ such that $x^T e^{At} y = 0$.

Continuous positivity Problem

Given x, y and A, decide whether $x^T e^{At} y \geqslant 0$ for all $t \geqslant 0$.

Continuous reachability

Continuous Skolem problem

Given x, y and A, decide if $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Bounded continuous Skolem problem

Given x, y and A, decide if $\exists t \in [0, 1]$ such that $x^T e^{At} y = 0$.

Continuous positivity Problem

Given x, y and A, decide whether $x^T e^{At} y \geqslant 0$ for all $t \geqslant 0$.

Continuous positivity is inter-reducible with continuous Skolem.

The decidability of all these problems is also open!

A link with number theory

Some reachability questions look like this :

$$\exists t \in \mathbb{R}.\ 42t^7 = 56 \ \wedge\ e^{3t} - e^t = 9$$

A link with number theory

Some reachability questions look like this (P, Q polynomials):

$$\exists t \in \mathbb{R}.\ P(t) = 0 \land Q(e^t) = 0$$

A link with number theory

Some reachability questions look like this (P, Q polynomials):

$$\exists t \in \mathbb{R}.\ P(t) = 0 \wedge Q(e^t) = 0$$

Claim: impossible except possibly for $t = 0$ (easy to check)

A link with number theory

Some reachability questions look like this (P, Q polynomials):

$$\exists t \in \mathbb{R}.\ P(t) = 0 \wedge Q(e^t) = 0$$

Claim: impossible except possibly for $t = 0$ (easy to check)

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

A link with number theory

Some reachability questions look like this (P, Q polynomials):

$$\exists t \in \mathbb{R}.\ P(t) = 0 \wedge Q(e^t) = 0$$

Claim: impossible except possibly for $t = 0$ (easy to check)

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Special case of Lindemann–Weierstrass)

If t is a nonzero algebraic number then e^t is transcendental.

A link with number theory

Some reachability questions look like this (P, Q polynomials):

$$\exists t \in \mathbb{R}.\ P(t) = 0 \wedge Q(e^t) = 0$$

Claim: impossible except possibly for $t = 0$ (easy to check)

Algebraic number: root of polynomial with integer coefficients
Transcendental number: not algebraic, e.g. e, π

Theorem (Special case of Lindemann–Weierstrass)

If t is a nonzero algebraic number then e^t is transcendental.

- $P(t) = 0$ so t is algebraic (by definition)
- Lindemann–Weierstrass: e^t transcendental (unless $t = 0$)
- hence $Q(e^t) \neq 0$ (except maybe if $t = 0$)

Exponential polynomial

In general,

$$x^T e^{At} y = \sum_{i=1}^{d} P_i(t) e^{\lambda_i t}$$

where P_i polynomial, $\lambda_i \in \mathbb{C}$ eigenvalues of A.

Exponential polynomial

In general,

$$x^T e^{At} y = \sum_{i=1}^{d} P_i(t) e^{\lambda_i t}$$

where P_i polynomial, $\lambda_i \in \mathbb{C}$ eigenvalues of A.

Lindemann–Weierstrass's theorem is not enough to solve the continuous Skolem problem.

Exponential polynomial

In general,

$$x^T e^{At} y = \sum_{i=1}^{d} P_i(t) e^{\lambda_i t}$$

where P_i polynomial, $\lambda_i \in \mathbb{C}$ eigenvalues of A.

Lindemann–Weierstrass's theorem is not enough to solve the continuous Skolem problem.

Theorem (Wilkie and MacIntyre)

If Schanuel's conjecture is true, then, for each $k \in \mathbb{N}$, the first-order theory of the structure $(\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,k]}, \sin\restriction_{[0,k]})$ is decidable.

- algorithm always correct, only termination requires the conjecture

Exponential polynomial

In general,

$$x^T e^{At} y = \sum_{i=1}^{d} P_i(t) e^{\lambda_i t}$$

where P_i polynomial, $\lambda_i \in \mathbb{C}$ eigenvalues of A.

Lindemann–Weierstrass's theorem is not enough to solve the continuous Skolem problem.

Theorem (Wilkie and MacIntyre)

If Schanuel's conjecture is true, then, for each $k \in \mathbb{N}$, the first-order theory of the structure $(\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,k]}, \sin\restriction_{[0,k]})$ is decidable.

- algorithm always correct, only termination requires the conjecture
- this makes many problem (inc. continuous Skolem) decidable!

Exponential polynomial

In general,

$$x^T e^{At} y = \sum_{i=1}^{d} P_i(t) e^{\lambda_i t}$$

where P_i polynomial, $\lambda_i \in \mathbb{C}$ eigenvalues of A.

Lindemann–Weierstrass's theorem is not enough to solve the continuous Skolem problem.

Theorem (Wilkie and MacIntyre)

If Schanuel's conjecture is true, then, for each $k \in \mathbb{N}$, the first-order theory of the structure $(\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,k]}, \sin\restriction_{[0,k]})$ is decidable.

- algorithm always correct, only termination requires the conjecture
- this makes many problem (inc. continuous Skolem) decidable!

What is Schanuel's conjecture?

Schanuel's conjecture

Schanuel's conjecture

If $z_1, \ldots, z_n$ that are linearly independent over $\mathbb{Q}$, then at least n numbers among $z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}$ are algebraically independent.

Schanuel's conjecture

Schanuel's conjecture

If $z_1, \ldots, z_n$ that are linearly independent over $\mathbb{Q}$, then at least n numbers among $z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}$ are algebraically independent.

Example: π and e are algebraically independent

$$z_1 = i\pi, z_2 = 1 \qquad \rightsquigarrow \qquad e^{z_1} = -1, e^{z_2} = e.$$

Schanuel's conjecture

Schanuel's conjecture

If $z_1, \ldots, z_n$ that are linearly independent over $\mathbb{Q}$, then at least n numbers among $z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}$ are algebraically independent.

Example: π and e are algebraically independent

$$z_1 = i\pi, z_2 = 1 \qquad \rightsquigarrow \qquad e^{z_1} = -1, e^{z_2} = e.$$

Clearly z_1 and z_2 are linearly independent over $\mathbb{Q}$. So at least 2 of $i\pi, 1, -1, e$ are algebraically independent. But 1 is algebraic so π and e are algebraically independent.

Schanuel's conjecture

Schanuel's conjecture

If $z_1, \ldots, z_n$ that are linearly independent over $\mathbb{Q}$, then at least n numbers among $z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}$ are algebraically independent.

Example: π and e are algebraically independent

$$z_1 = i\pi, z_2 = 1 \qquad \rightsquigarrow \qquad e^{z_1} = -1, e^{z_2} = e.$$

Clearly z_1 and z_2 are linearly independent over $\mathbb{Q}$. So at least 2 of $i\pi, 1, -1, e$ are algebraically independent. But 1 is algebraic so π and e are algebraically independent.

Summary:

- Schanuel implies that π, e, $\pi + e$, $e\pi$, ... are transcendental.
- π and e are known to be transcendental
- $\pi + e$ is **not known** to be transcendental

Continuous reachability

Bounded continuous Skolem problem: given x, y and A, decide if

- unbounded: $\exists t \in [0, 1]$ such that $x^T e^{At} y = 0$.
- bounded: $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Theorem (Chonev, Ouaknine and Worrell, 2016)

The bounded continuous Skolem Problem is decidable subject to Schanuel's conjecture.

Continuous reachability

Bounded continuous Skolem problem: given x, y and A, decide if

- unbounded: $\exists t \in [0,1]$ such that $x^T e^{At} y = 0$.
- bounded: $\exists t \in \mathbb{R}$ such that $x^T e^{At} y = 0$.

Theorem (Chonev, Ouaknine and Worrell, 2016)

The bounded continuous Skolem Problem is decidable subject to Schanuel's conjecture.

Theorem (Chonev, Ouaknine and Worrell, 2016)

If the (unbounded) continuous Skolem Problem is decidable then the Diophantine-approximation types of all real algebraic numbers is computable.

In other words: it requires new mathematics...

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
  if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
  else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
    if $y \geqslant 2x$ then
        $\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$
    else
        $\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

Reachability is trivially undecidable by simulating two counter automata

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
  if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
  else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$\rightsquigarrow$

Nondeterminic loop

$x := 2^{-10}$
$y := 1$
while true do
  non deterministically do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
  or
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Reachability is trivially undecidable by simulating two counter automata

More complicated programs

Linear loop with if

$x := 2^{-10}$
$y := 1$
while $y \geqslant x$ do
    if $y \geqslant 2x$ then
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    else
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$\rightsquigarrow$

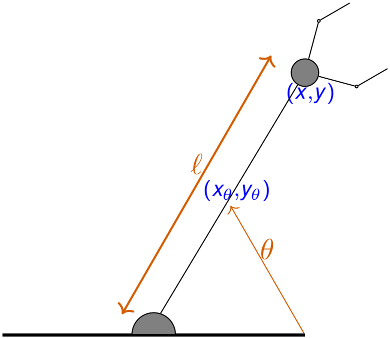
Nondeterminic loop

$x := 2^{-10}$
$y := 1$
while true do
    non deterministically do
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$
    or
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 3 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Reachability is trivially undecidable by simulating two counter automata

- Overapproximate behaviours
- Nondeterminic

Example: 2D robot



State: $\vec{u} = (x_\theta, y_\theta, x, y)$

Discretized actions:

- rotate arm by ψ
- change arm length by δ

$\rightsquigarrow$ Linear transformations

Rotate arm by ψ:

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\begin{pmatrix} x_\theta \\ y_\theta \end{pmatrix} \leftarrow \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \begin{pmatrix} x_\theta \\ y_\theta \end{pmatrix}$$

Change arm length by δ:

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} x \\ y \end{pmatrix} + \delta \begin{pmatrix} x_\theta \\ y_\theta \end{pmatrix}$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d \times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C \quad ?$

Example: $\exists n \in \mathbb{N}$ such that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 100 \\ 0 & 1 \end{bmatrix} \quad ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Example: $\exists n \in \mathbb{N}$ such that

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^n = \begin{bmatrix}1 & 100\\ 0 & 1\end{bmatrix} \quad ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$?

✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$?

Example: $\exists n, m \in \mathbb{N}$ such that

$$\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix}^m = \begin{bmatrix} 1 & 60 \\ 0 & 1 \end{bmatrix} \quad ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$? ✓ Decidable

Example: $\exists n, m \in \mathbb{N}$ such that

$$\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix}^m = \begin{bmatrix} 1 & 60 \\ 0 & 1 \end{bmatrix} \quad ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$? ✓ Decidable

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n_1, \ldots, n_k \in \mathbb{N}$ such that $\prod_{i=1}^{k} A_i^{n_i} = C$?

Example: $\exists n, m, p \in \mathbb{N}$ such that

$$\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix}^m \begin{bmatrix} 2 & 5 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} 81 & 260 \\ 0 & 1 \end{bmatrix} ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$? ✓ Decidable

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n_1, \ldots, n_k \in \mathbb{N}$ such that $\prod_{i=1}^{k} A_i^{n_i} = C$?
✓ Decidable if A_i commute × Undecidable in general

Example: $\exists n, m, p \in \mathbb{N}$ such that

$$\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix}^m \begin{bmatrix} 2 & 5 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} 81 & 260 \\ 0 & 1 \end{bmatrix} ?$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$? ✓ Decidable

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n_1, \ldots, n_k \in \mathbb{N}$ such that $\prod_{i=1}^{k} A_i^{n_i} = C$?
✓ Decidable if A_i commute × Undecidable in general

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $C \in \langle$semigroup generated by $A_1, \ldots, A_k\rangle$?

Semigroup: $\langle A_1, \ldots, A_k\rangle$ = all finite products of $A_1, \ldots, A_k$
Examples:

$$A_1A_3A_2 \quad A_1A_2A_1A_2 \quad A_3^8A_2A_1^3A_3^{42}$$

Matrix problems

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n \in \mathbb{N}$ such that $A^n = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n, m \in \mathbb{N}$ such that $A^n B^m = C$? ✓ Decidable

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists n_1, \ldots, n_k \in \mathbb{N}$ such that $\prod_{i=1}^{k} A_i^{n_i} = C$?
✓ Decidable if A_i commute × Undecidable in general

Input: $A_1, \ldots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $C \in \langle$semigroup generated by $A_1, \ldots, A_k\rangle$?
✓ Decidable if A_i commute × Undecidable in general

Semigroup: $\langle A_1, \ldots, A_k\rangle$ = all finite products of $A_1, \ldots, A_k$
Examples:

$$A_1A_3A_2 \quad A_1A_2A_1A_2 \quad A_3^8A_2A_1^3A_3^{42}$$

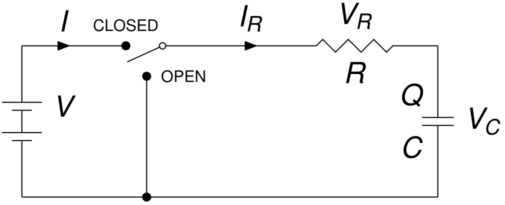
Discrete reachability problems

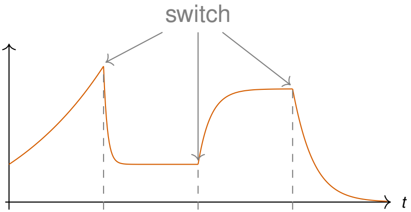
Every nontrivial extension of simple linear loops seems to lead to undecidable problems.

Discrete reachability problems

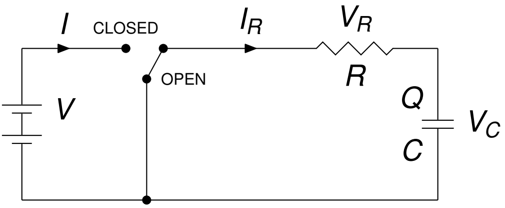
Every nontrivial extension of simple linear loops seems to lead to undecidable problems. What about the continuous setting?

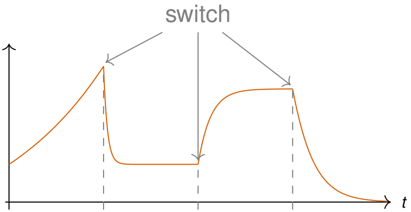
RC circuit





RC circuit

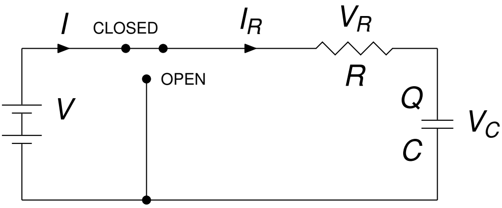


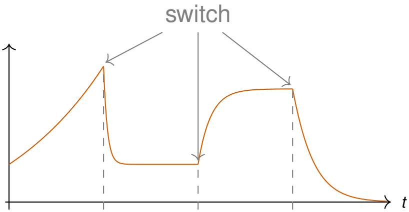


OPEN

$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

RC circuit





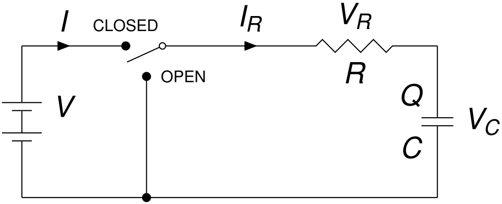
OPEN

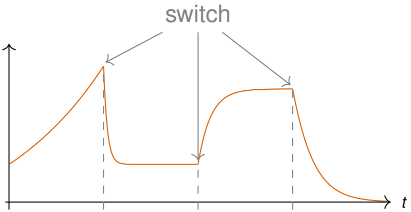
$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

CLOSED

$$\boxed{\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

RC circuit





OPEN

$$\begin{aligned}\dot{I} &= 0\\ \dot{I}_R &= -\frac{1}{RC} I_R\\ \dot{V}_R &= -\frac{1}{C} I_R\\ \dot{Q} &= I_R\\ \dot{V}_C &= \frac{1}{C} I_R\end{aligned}$$

OPEN → CLOSED:

$$\begin{aligned}I &:= \frac{1}{R}(V - V_C)\\ I_R &:= \frac{1}{R}(V - V_C)\\ V_R &:= V - V_C\end{aligned}$$

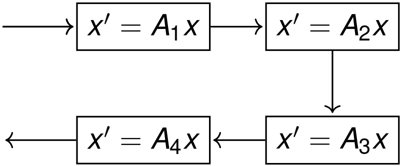
CLOSED → OPEN:

$$\begin{aligned}I &:= 0\\ I_R &:= -\frac{1}{R} V_C\\ V_R &:= -V_C\end{aligned}$$

CLOSED

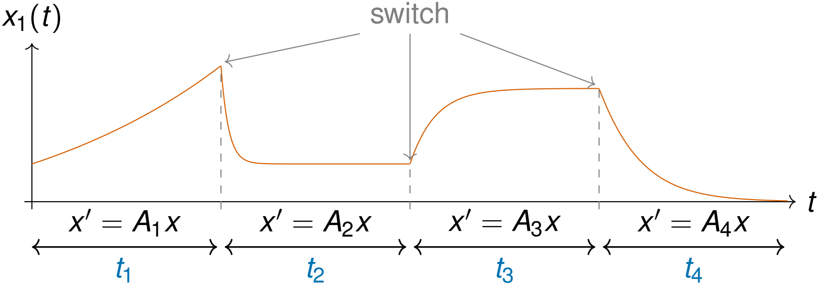
$$\begin{aligned}\dot{I} &= -\frac{1}{RC} I_R\\ \dot{I}_R &= -\frac{1}{RC} I_R\\ \dot{V}_R &= -\frac{1}{C} I_R\\ \dot{Q} &= I_R\\ \dot{V}_C &= \frac{1}{C} I_R\end{aligned}$$

Switching systems

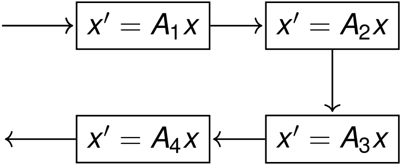


Restricted hybrid system:

- linear dynamics
- no guards (nondeterministic)
- no discrete updates

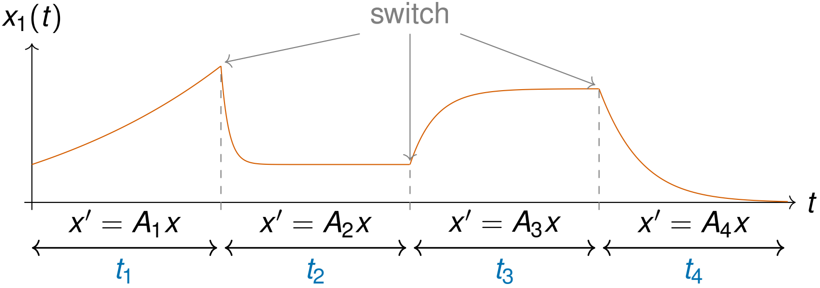


Switching systems



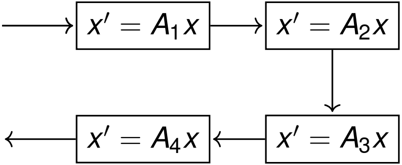
Restricted hybrid system:

- linear dynamics
- no guards (nondeterministic)
- no discrete updates



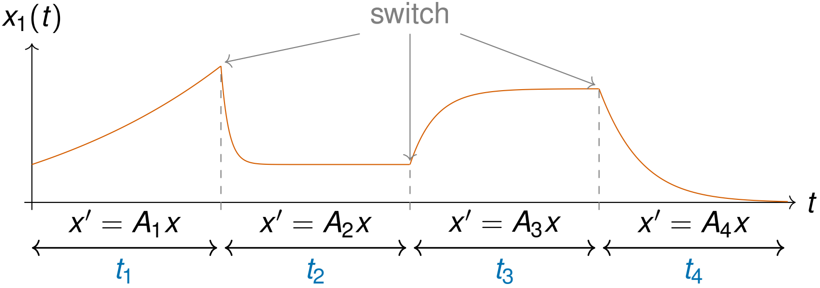
Dynamics:

$$e^{A_4 t_4} e^{A_3 t_3} e^{A_2 t_2} e^{A_1 t_1}$$



Restricted hybrid system:

- linear dynamics
- no guards (nondeterministic)
- no discrete updates



Problem:

$$e^{A_4 t_4} e^{A_3 t_3} e^{A_2 t_2} e^{A_1 t_1} = C \quad ?$$

What we control: $t_1, t_2, t_3, t_4 \in \mathbb{R}_{\geqslant 0}$

Related work in the continuous case

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t \in \mathbb{R}$ such that $e^{At} = C$?

Example: $\exists t \in \mathbb{R}$ such that

$$\exp\left(\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} t\right) = \begin{bmatrix}1 & 100\\ 0 & 1\end{bmatrix} \quad ?$$

Related work in the continuous case

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t \in \mathbb{R}$ such that $e^{At} = C$?   ✓ Decidable (PTIME)

Example: $\exists t \in \mathbb{R}$ such that

$$\exp\left(\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} t\right) = \begin{bmatrix}1 & 100\\ 0 & 1\end{bmatrix} \quad ?$$

Related work in the continuous case

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t \in \mathbb{R}$ such that $e^{At} = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t, u \in \mathbb{N}$ such that $e^{At}e^{Bu} = C$?

Example: $\exists t, u \in \mathbb{R}$ such that

$$\exp\left(\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix} t\right) \exp\left(\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix} u\right) = \begin{bmatrix} 1 & 60 \\ 0 & 1 \end{bmatrix} \quad ?$$

Related work in the continuous case

Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t \in \mathbb{R}$ such that $e^{At} = C$? ✓ Decidable (PTIME)

Input: $A, B, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t, u \in \mathbb{N}$ such that $e^{At}e^{Bu} = C$? × Unknown

Example: $\exists t, u \in \mathbb{R}$ such that

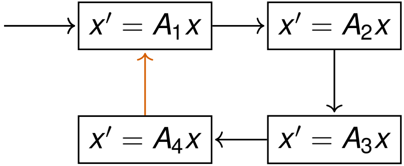
$$\exp\left(\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix} t\right) \exp\left(\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix} u\right) = \begin{bmatrix} 1 & 60 \\ 0 & 1 \end{bmatrix} \quad ?$$

Switching system

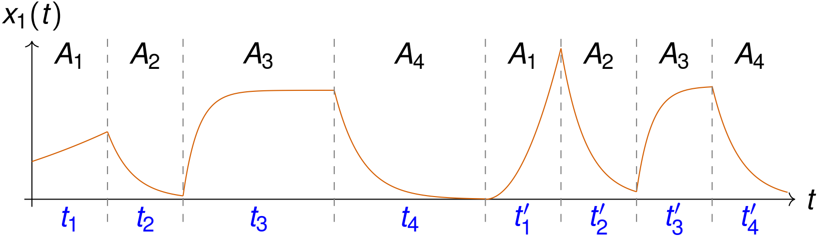
$$\begin{tikzcd}
\arrow[r] & \boxed{x' = A_1 x} \arrow[r] & \boxed{x' = A_2 x} \arrow[d] \\
& \boxed{x' = A_4 x} \arrow[u] & \boxed{x' = A_3 x} \arrow[l]
\end{tikzcd}$$

What about a loop ?

Switching system



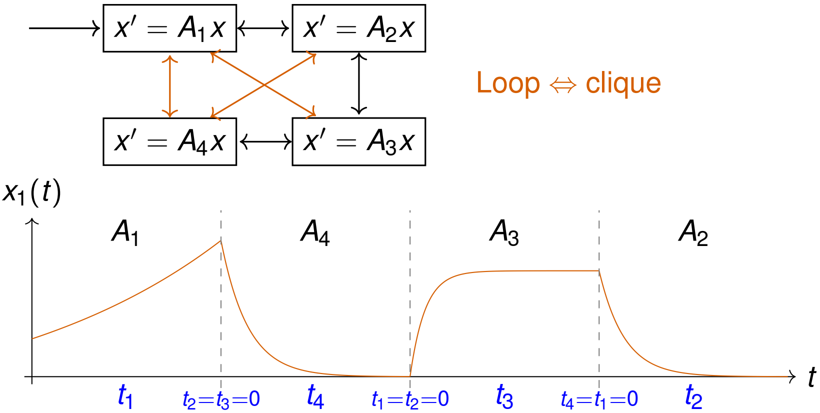
What about a loop ?



Dynamics:

$$e^{A_4 t'_4} e^{A_3 t'_3} e^{A_2 t'_2} e^{A_1 t'_1} e^{A_4 t_4} e^{A_3 t_3} e^{A_2 t_2} e^{A_1 t_1}$$

Switching system

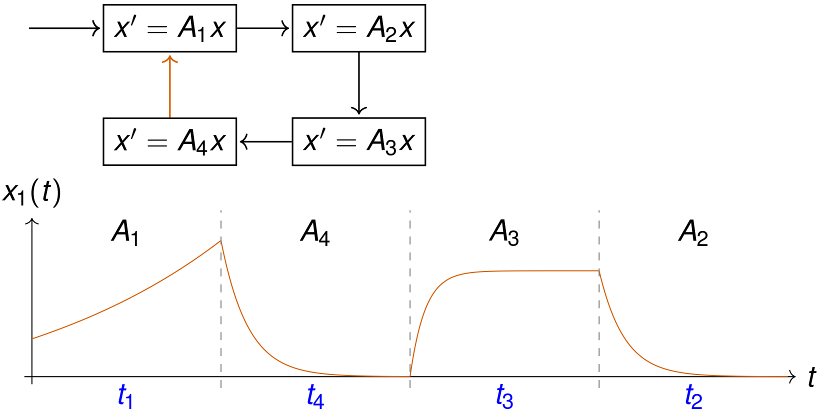


Loop $\Leftrightarrow$ clique

Remark:

zero time dynamics ($t_i = 0$) are allowed

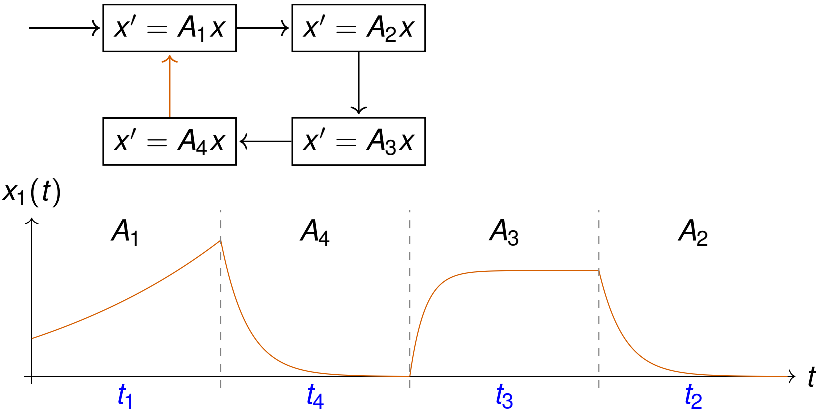
Switching system



Dynamics:

any finite product of $e^{A_i t}$ $\rightsquigarrow$ semigroup!

Switching system



Problem:

$$C \in \mathcal{G} \quad ?$$

where $\qquad \mathcal{G} = \langle \text{semigroup generated by } e^{A_i t} \text{ for all } t \geqslant 0 \rangle$

Reachability for switching systems

Input: $A_1, \dots, A_k, C \in \mathbb{Q}^{d \times d}$ matrices
Output: $\exists t_1, \dots, t_k \geqslant 0$ such that

$$\prod_{i=1}^{n} e^{A_i t_i} = C \quad ?$$

Input: $A_1, \dots, A_k, C \in \mathbb{Q}^{d \times d}$ matrices
Output:

$$C \in \langle \text{semigroup generated by } e^{A_1 t}, \dots, e^{A_k t} : t \geqslant 0 \rangle \quad ?$$

Theorem (Ouaknine, P, Sous-Pinto, Worrell)

Both problems are:

- *Undecidable in general*
- Decidable *when all the A_i commute*

Some words about the proof (commuting case)

Product Problem

$\exists t_1, \ldots, t_k \geqslant 0$ s.t. $\prod_{i=1}^{n} e^{A_i t_i} = C \quad ?$

equivalent

Semigroup Problem

$C \in \langle e^{A_1 t}, \ldots, e^{A_k t} : t \geqslant 0 \rangle \quad ?$

reduce

Integer Linear Programming

$\exists n \in \mathbb{Z}^d$ s.t. $\pi B n \leqslant s$

Some words about the proof (commuting case)

Product Problem

$\exists t_1, \ldots, t_k \geqslant 0$ s.t. $\prod_{i=1}^{n} e^{A_i t_i} = C$?

equivalent

Semigroup Problem

$C \in \langle e^{A_1 t}, \ldots, e^{A_k t} : t \geqslant 0 \rangle$?

reduce

Integer Linear Programming

$\exists n \in \mathbb{Z}^d$ s.t. $\pi B n \leqslant s$

⚠ s of the form:

$$a_0 + \log(a_1) + \cdots + \log(a_k)$$

✓ $B, a_0, \ldots, a_k$ are algebraic

Some words about the proof (commuting case)

Product Problem

$\exists t_1, \ldots, t_k \geqslant 0$ s.t.
$\prod_{i=1}^{n} e^{A_i t_i} = C \quad ?$

equivalent

Semigroup Problem

$C \in \langle e^{A_1 t}, \ldots, e^{A_k t} : t \geqslant 0 \rangle \quad ?$

reduce

Integer Linear Programming

$\exists n \in \mathbb{Z}^d$ s.t. $\pi B n \leqslant s$

⚠ s of the form:

$$a_0 + \log(a_1) + \cdots + \log(a_k)$$

✓ $B, a_0, \ldots, a_k$ are algebraic

How did we get from reals to integers with π ?

$$e^{it} = \alpha \quad \Leftrightarrow \quad t \in \log(\alpha) + 2\pi\mathbb{Z}$$

Integer Linear Programming

$$\exists n \in \mathbb{Z}^d \text{ such that } \pi B n \leqslant s \quad ?$$

where s is a linear form in logarithms of algebraic numbers

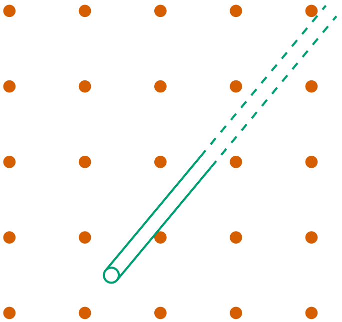
Integer Linear Programming

$$\exists n \in \mathbb{Z}^d \text{ such that } \pi B n \leqslant s \quad ?$$

where s is a linear form in logarithms of algebraic numbers

Key ingredient: Diophantine approximations

- Finding integer points in cones: Kronecker's theorem



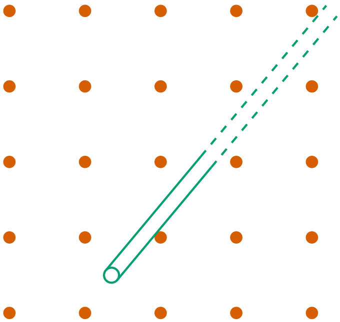
Integer Linear Programming

$$\exists n \in \mathbb{Z}^d \text{ such that } \pi B n \leqslant s \quad ?$$

where s is a linear form in logarithms of algebraic numbers

Key ingredient: Diophantine approximations

- Finding integer points in cones: Kronecker's theorem



- Compare linear forms in logs: Baker's theorem

$$\sqrt{2} + \log\sqrt{3} - 3\log\sqrt{7} \quad \stackrel{?}{=} \quad 1 + \log 9 - \log \sqrt[42]{666}$$

Some words about the proof (general case)

Product Problem

$\exists t_1, \ldots, t_k \geqslant 0$ s.t. $\prod_{i=1}^{n} e^{A_i t_i} = C \quad ?$

reduce $\rightarrow$

Semigroup Problem

$C \in \langle e^{A_1 t}, \ldots, e^{A_k t} : t \geqslant 0 \rangle \quad ?$

reduce $\uparrow$

Hilbert's Tenth Problem

$\exists n \in \mathbb{Z}^d$ s.t. $p(n) = 0$

Theorem (Matiyasevich)

Hilbert's Tenth Problem is undecidable

Summary on reachability

Exact reachability is hard:

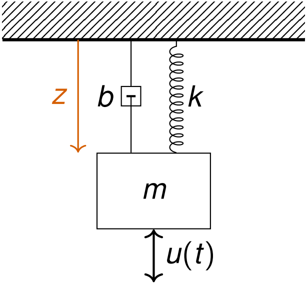
- Skolem/Positivity problem for linear loops (Open for 70 years)
- Every mild extension is undecidable
- Decidability requires very strong assumptions (commuting matrices)

Continuous vs discrete setting

- similar results
- different techniques
- continuous setting can leverage powerful results/conjectures

Control Theory

Example: mass-spring-damper system



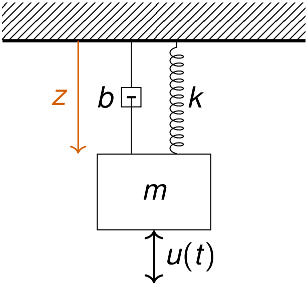
State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg + u$$

Model with external input $u(t)$

Example: mass-spring-damper system



State: $X = z \in \mathbb{R}$

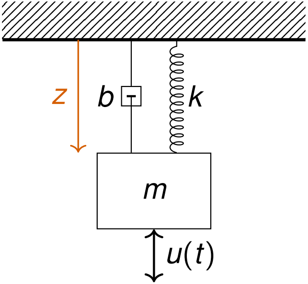
Equation of motion:

$$mz'' = -kz - bz' + mg + u$$

$\rightarrow$ Affine but not first order

Model with external input $u(t)$

Example: mass-spring-damper system



Model with external input $u(t)$

State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg + u$$

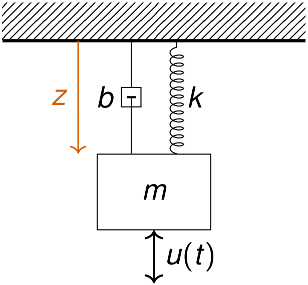
$\rightarrow$ Affine but not first order

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g + \frac{1}{m}u \\ 0 \end{bmatrix}$$

Example: mass-spring-damper system



Model with external input $u(t)$
$\rightarrow$ Linear time invariant system

$$X' = AX + Bu$$

with some constraints on u.

State: $X = z \in \mathbb{R}$

Equation of motion:

$$mz'' = -kz - bz' + mg + u$$

$\rightarrow$ Affine but not first order

State: $X = (z, z', 1) \in \mathbb{R}^3$

Equation of motion:

$$\begin{bmatrix} z \\ z' \\ 1 \end{bmatrix}' = \begin{bmatrix} z' \\ -\frac{k}{m}z - \frac{b}{m}z' + g + \frac{1}{m}u \\ 0 \end{bmatrix}$$

A very simple example

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

A very simple example

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

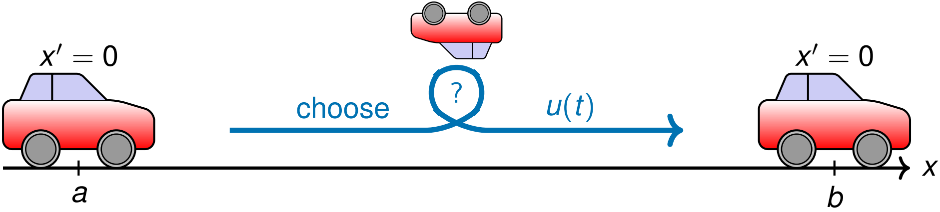
Starting at $x(0) = a$, want to reach and stop at $x = b$:

A very simple example

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

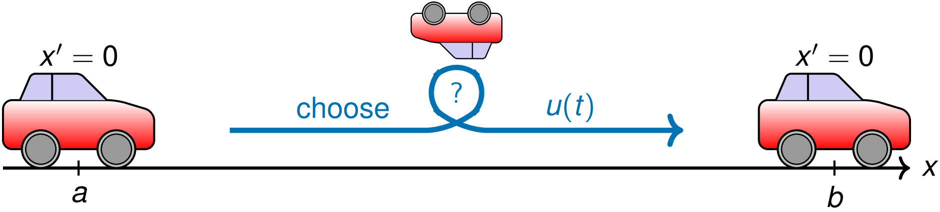
Starting at $x(0) = a$, want to reach and stop at $x = b$:



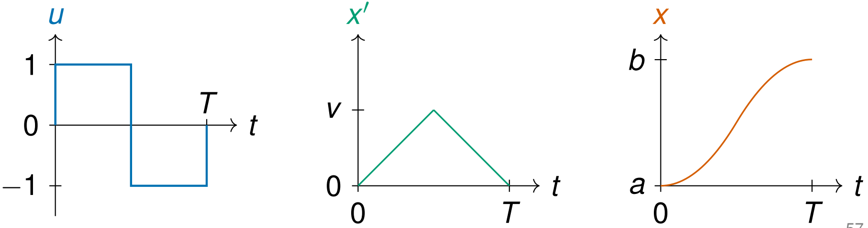
A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

Starting at $x(0) = a$, want to reach and stop at $x = b$:



Possible solution:

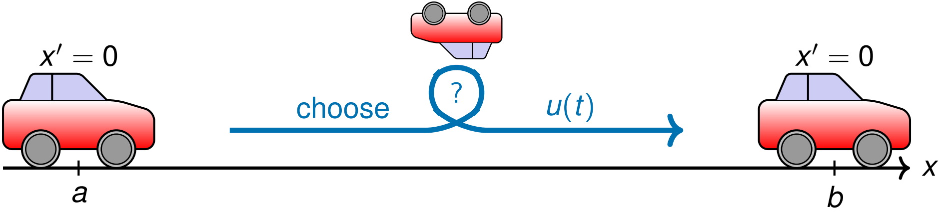


A very simple example

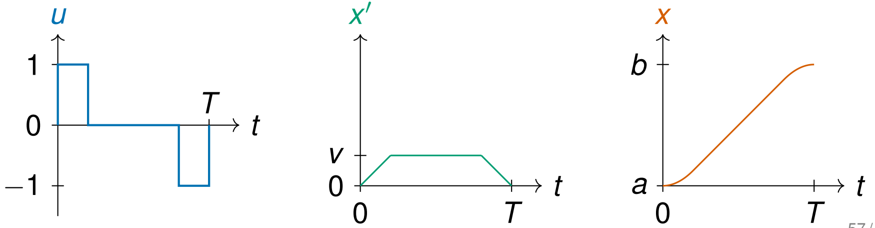
A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

Starting at $x(0) = a$, want to reach and stop at $x = b$:



More realistic solution:

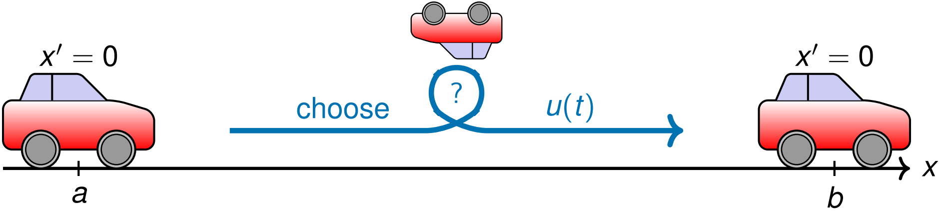


A very simple example

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

Starting at $x(0) = a$, want to reach and stop at $x = b$:



Rephrasing the problem:

$$\begin{cases} x' = y \\ y' = u \end{cases} \Leftrightarrow \begin{bmatrix} x \\ y \end{bmatrix}' = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ u \end{bmatrix} \Leftrightarrow X' = AX + U$$

Starting from $(x, y) = (a, 0)$, try to reach $(x, y) = (b, 0)$.

This is a point-to-point reachability problem.

The problem

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

The problem

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Warning: u **does not need to be "describable"**, *e.g.* piecewise polynomial. Otherwise, completely changes the nature of the problem.

Bigger picture

Continuous Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition function f,
- a set of controls $U \subseteq \mathbb{R}^m$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = f(t, x(t), u(t)) \quad \text{for } t \in [0, T].$$

Bigger picture

Continuous Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition function f,
- a set of controls $U \subseteq \mathbb{R}^m$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = f(t, x(t), u(t)) \quad \text{for } t \in [0, T].$$

Generally undecidable:

- for nonlinear systems, even without control ($U = \{0\}$)
- piecewise constant derivative systems (PCD), still *no control*
- linear saturated systems (at least for discrete systems), no control

LTI systems probably form the most useful class that is not undecidable.

Bigger picture

Continuous Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition function f,
- a set of controls $U \subseteq \mathbb{R}^m$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = f(t, x(t), u(t)) \quad \text{for } t \in [0, T].$$

Generally undecidable:

- for nonlinear systems, even without control ($U = \{0\}$)
- piecewise constant derivative systems (PCD), still *no control*
- linear saturated systems (at least for discrete systems), no control

LTI systems probably form the most useful class that is not undecidable.

But do they really?

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a target $z \in \mathbb{Q}^n$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability
- can **all points** $y \in \mathbb{R}^n$ tend to $z = 0$? asymptotic null-controllability

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability
- can **all points** $y \in \mathbb{R}^n$ tend to $z = 0$? asymptotic null-controllability
- can **all points** $y \approx 0$ reach $z = 0$? local null-controllability

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability
- can **all points** $y \in \mathbb{R}^n$ tend to $z = 0$? asymptotic null-controllability
- can **all points** $y \approx 0$ reach $z = 0$? local null-controllability
- is the trajectory bounded when u is bounded? stability

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability
- can **all points** $y \in \mathbb{R}^n$ tend to $z = 0$? asymptotic null-controllability
- can **all points** $y \approx 0$ reach $z = 0$? local null-controllability
- is the trajectory bounded when u is bounded? stability
- approximate the set of reachable points from y reach set

Existing work

LTI Reachability problem

- a source $y \in \mathbb{Q}^n$,
- a target $z \in \mathbb{Q}^n$,
- a transition matrix $A \in \mathbb{Q}^{n \times n}$,
- a set of controls $U \subseteq \mathbb{R}^n$,

decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ *measurable* such that $x(T) = z$ where

$$x(0) = y, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Many variants (applies to non-LTI systems):

- can **all points** $y \in \mathbb{R}^n$ reach $z = 0$? global null-controllability
- can **all points** $y \in \mathbb{R}^n$ tend to $z = 0$? asymptotic null-controllability
- can **all points** $y \approx 0$ reach $z = 0$? local null-controllability
- is the trajectory bounded when u is bounded? stability
- approximate the set of reachable points from y reach set

But also:

- assumptions on A (typically spectral)
- assumptions on U
- restrictions on acceptable u

Two known extreme cases

- When we have no control:

$$U = \{0\} \quad \text{and} \quad x'(t) = Ax + u(t) \qquad \Leftrightarrow \qquad x(t) = e^{At}x(0).$$

Two known extreme cases

- When we have no control:

$$U = \{0\} \quad \text{and} \quad x'(t) = Ax + u(t) \qquad \Leftrightarrow \qquad x(t) = e^{At}x(0).$$

Theorem (Hainry'08)

Given $y, z \in \mathbb{Q}^n$ and $A \in \mathbb{Q}^{n \times n}$, it is decidable whether $\exists t \geqslant 0$ such that

$$z = e^{At}y.$$

Two known extreme cases

- When we have no control:

$$U = \{0\} \quad \text{and} \quad x'(t) = Ax + u(t) \qquad \Leftrightarrow \qquad x(t) = e^{At}x(0).$$

Theorem (Hainry'08)

Given $y, z \in \mathbb{Q}^n$ and $A \in \mathbb{Q}^{n\times n}$, it is decidable whether $\exists t \geqslant 0$ such that

$$z = e^{At}y.$$

- When we can control in a vector space:

$$U = B\mathbb{R}^m \quad \text{and} \quad x'(t) = Ax + u(t) \quad \Rightarrow \quad x(t) \in \operatorname{span}[B, AB, \dots, A^{n-1}B]$$

Two known extreme cases

- When we have no control:

$$U = \{0\} \quad \text{and} \quad x'(t) = Ax + u(t) \qquad \Leftrightarrow \qquad x(t) = e^{At}x(0).$$

Theorem (Hainry'08)

Given $y, z \in \mathbb{Q}^n$ and $A \in \mathbb{Q}^{n\times n}$, it is decidable whether $\exists t \geqslant 0$ such that

$$z = e^{At}y.$$

- When we can control in a vector space:

$$U = B\mathbb{R}^m \quad \text{and} \quad x'(t) = Ax + u(t) \quad \Rightarrow \quad x(t) \in \operatorname{span}[B, AB, \dots, A^{n-1}B]$$

Theorem (Folklore)

Given $y, z \in \mathbb{Q}^n$ and $A \in \mathbb{Q}^{n\times n}$, $B \in \mathbb{Q}^{n\times m}$, it is decidable whether $\exists T \geqslant 0$ and $u : [0, T] \to B\mathbb{R}^m$ measurable such that $x(0) = y$ and $x(T) = z$ where

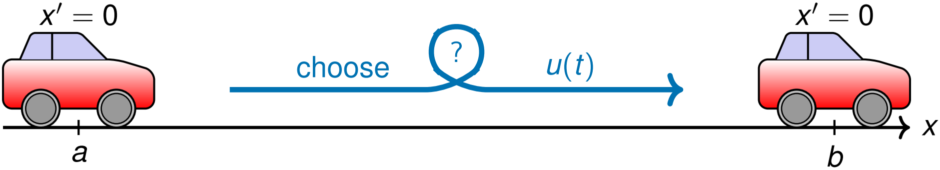
$$x'(t) = Ax(t) + u(t)$$

Back to the future

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

Starting at $x(0) = a$, want to reach and stop at $x = b$:



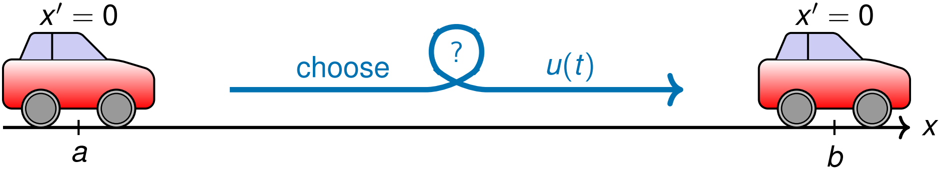
Reality: acceleration/braking is not infinite $\rightsquigarrow$ u is bounded!

Back to the future

A simplified one-dimensional car: control acceleration $u(t)$

$$x''(t) = u(t)$$

Starting at $x(0) = a$, want to reach and stop at $x = b$:



Reality: acceleration/braking is not infinite $\rightsquigarrow$ u is bounded!

Very few decidability results in the literature in this case.

Our results: decidability

LTI Zonotope Null-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U = B[-1,1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

Our results: decidability

LTI Zonotope Null-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U = B[-1, 1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*

Our results: decidability

LTI Zonotope Null-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U = B[-1,1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*
- *A is real diagonalizable, eigenvalues $\subseteq \alpha\mathbb{Q}$ for some $\alpha \in \overline{\mathbb{Q}}$,*

Our results: decidability

LTI Zonotope Null-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U = B[-1,1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*
- *A is real diagonalizable, eigenvalues $\subseteq \alpha\mathbb{Q}$ for some $\alpha \in \overline{\mathbb{Q}}$,*
- *A only has one eigenvalue which is real, B is a column,*

Our results: decidability

LTI Zonotope Null-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U = B[-1, 1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*
- *A is real diagonalizable, eigenvalues $\subseteq \alpha\mathbb{Q}$ for some $\alpha \in \overline{\mathbb{Q}}$,*
- *A only has one eigenvalue which is real, B is a column,*
- *dimension $n = 2$, B is a column and A has real eigenvalues.*

Our results: decidability

LTI Zonotope Null-Reachability problem

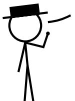
Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U = B[-1, 1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*
- *A is real diagonalizable, eigenvalues $\subseteq \alpha\mathbb{Q}$ for some $\alpha \in \overline{\mathbb{Q}}$,*
- *A only has one eigenvalue which is real, B is a column,*
- *dimension $n = 2$, B is a column and A has real eigenvalues.*



Our results: decidability

LTI Zonotope Null-Reachability problem

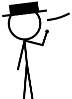
Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U = B[-1, 1]^m$, a target $z \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) = z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A is real diagonal, B is a column with at most 2 nonzero entries,*
- *A is real diagonalizable, eigenvalues $\subseteq \alpha\mathbb{Q}$ for some $\alpha \in \overline{\mathbb{Q}}$,*
- *A only has one eigenvalue which is real, B is a column,*
- *dimension $n = 2$, B is a column and A has real eigenvalues.*



Well, that was underwhelming...

Are you sure you cannot do better?

Our results: conditional decidability

Schanuel's conjecture

A deep conjecture in transcendental number theory. Widely believed to be true and totally open.

Our results: conditional decidability

Schanuel's conjecture

A deep conjecture in transcendental number theory. Widely believed to be true and totally open.

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A has real eigenvalues,*

Our results: conditional decidability

Schanuel's conjecture

A deep conjecture in transcendental number theory. Widely believed to be true and totally open.

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A has real eigenvalues,*
- *in dimension $n = 2$,*

Our results: conditional decidability

Schanuel's conjecture

A deep conjecture in transcendental number theory. Widely believed to be true and totally open.

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A has real eigenvalues,*
- *in dimension $n = 2$,*
- *we bound the time to reachability.*

and Schanuel's conjecture is true.

Our results: conditional decidability

Schanuel's conjecture

A deep conjecture in transcendental number theory. Widely believed to be true and totally open.

Theorem (Dantam, P.)

The LTI Zonotope Null-Reachability problem is decidable if one of:

- *A has real eigenvalues,*
- *in dimension $n = 2$,*
- *we bound the time to reachability.*

and Schanuel's conjecture is true.

Theorem (Wilkie and MacIntyre)

If Schanuel's conjecture is true, then, for each $k \in \mathbb{N}$, the first-order theory of the structure $(\mathbb{R}, 0, 1, <, +, \cdot, \exp, \cos\restriction_{[0,k]}, \sin\restriction_{[0,k]})$ is decidable.

Hardness

Study generalization:

Hardness

Study generalization:

LTI Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U \subseteq \mathbb{R}^n$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Hardness

Study generalization:

LTI Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U \subseteq \mathbb{R}^n$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

This is trivially hard for $U = \{0\}$ and $Z = \{\text{hyperplane}\}$ because:

Hardness

Study generalization:

LTI Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U \subseteq \mathbb{R}^n$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

This is trivially hard for $U = \{0\}$ and $Z = \{\text{hyperplane}\}$ because:

Continuous Skolem problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$ and $c, x_0 \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$ such that $c^T e^{At} x_0 = 0$.

Hardness

Study generalization:

LTI Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U \subseteq \mathbb{R}^n$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

This is trivially hard for $U = \{0\}$ and $Z = \{\text{hyperplane}\}$ because:

Continuous Skolem problem

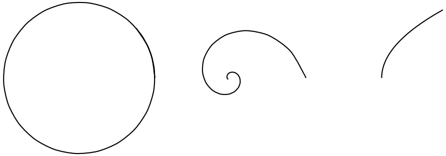
Given a matrix $A \in \mathbb{Q}^{n \times n}$ and $c, x_0 \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$ such that $c^T e^{At} x_0 = 0$.

This is a well-known “hard” problem.

Hardness (cont.)

Taking $U = \{0\}$ is cheating:

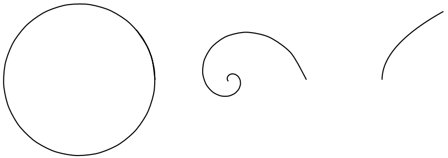
- when $U = \{0\}$, reachable set is closed (or closed minus a point)



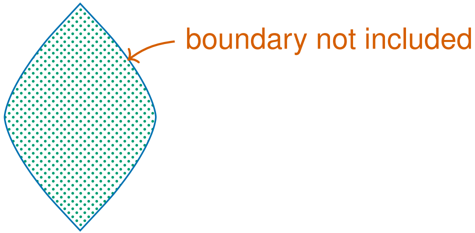
Hardness (cont.)

Taking $U = \{0\}$ is cheating:

- when $U = \{0\}$, reachable set is closed (or closed minus a point)



- when $U = B[-1, 1]^m$, reachable set is open



This is completely different!

Our results: hardness

LTI Zonotope Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n \times n}$, a set of controls $U = B[-1, 1]^m$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0, T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0, T].$$

Our results: hardness

LTI Zonotope Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U = B[-1,1]^m$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

Theorem (Dantam, P.)

The Continuous Nontangential Skolem problem reduces to this problem with a single input ($m = 1$), A stable and Z a hyperplane or a convex compact set of dimension $n-1$.

Our results: hardness

LTI Zonotope Null-Set-Reachability problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$, a set of controls $U = B[-1,1]^m$, a set $Z \subseteq \mathbb{R}^n$, decide if $\exists T \geqslant 0$, $u : [0,T] \to U$ such that $x(T) \in Z$ where

$$x(0) = 0, \qquad x'(t) = Ax(t) + u(t) \quad \text{for } t \in [0,T].$$

Theorem (Dantam, P.)

The Continuous Nontangential Skolem problem reduces to this problem with a single input ($m = 1$), A stable and Z a hyperplane or a convex compact set of dimension $n-1$.

Continuous Nontangential Skolem problem

Given a matrix $A \in \mathbb{Q}^{n\times n}$ and $c, x_0 \in \mathbb{Q}^n$, decide if $\exists T \geqslant 0$ such that $f(t) = 0$ and $f'(t) \neq 0$ where $f(t) = c^T e^{At} x_0 = 0$.

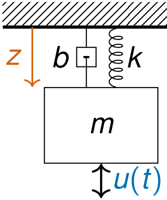
It is essentially as hard as the Continuous Skolem problem.

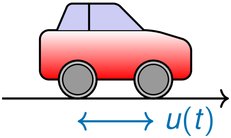
Conclusion (continuous case)

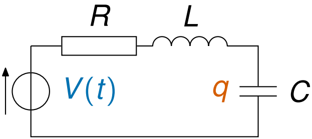
LTI reachability problem: find T and u such that

$$x(0) = 0, \qquad x'(t) = Ax(t) + Bu(t), \qquad u(t) \in [-1, 1]^m$$

satisfies $x(T) = $ target. Very natural problem in control theory.







Point reachability is

- decidable in dimension 2 or with spectral constraints,
- conditionally decidable with real eigenvalues,
- conditionally decidable in bounded time,

Set reachability is Nontangential Continuous Skolem hard.

The continuous case is much harder than expected. What about the discrete case?

The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

s $\qquad$ t

The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}$, $u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

$x_0 = s$ $\qquad$ t

The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

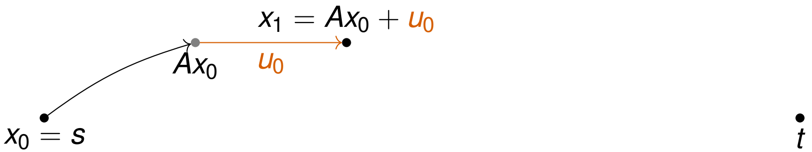
The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$



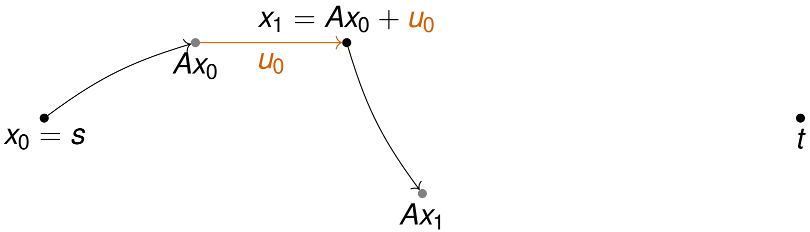
The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \dots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$



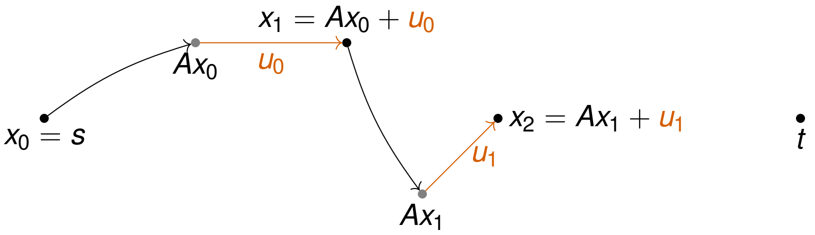
The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$



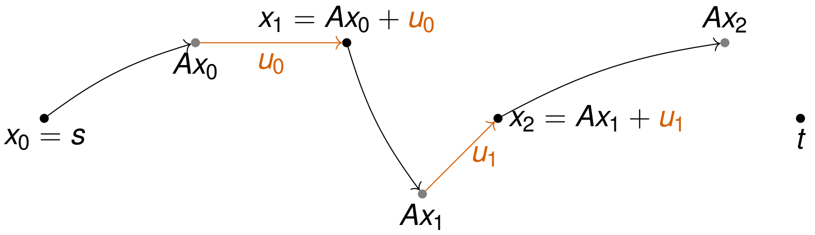
The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$



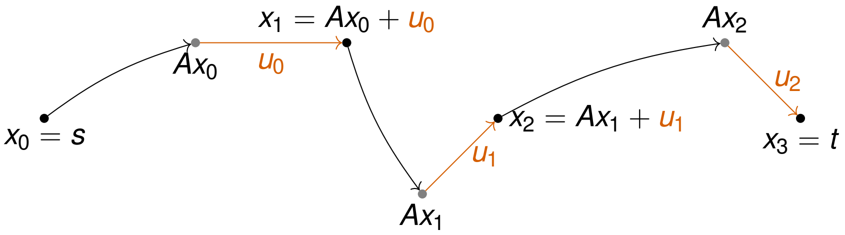
The problem

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}$, $u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$



Decidability (1)

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

Decidability (1)

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}$, $u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

Theorem (Lipton and Kannan, 1986)

LTI-REACHABILITY is decidable if U is an affine subspace of $\mathbb{R}^d$.

Decidability (1)

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

Theorem (Lipton and Kannan, 1986)

LTI-REACHABILITY is decidable if U is an affine subspace of $\mathbb{R}^d$.

Almost no exact results for other classes of U

Decidability (1)

LTI-REACHABILITY

- a source $s \in \mathbb{Q}^d$,
- a target $t \in \mathbb{Q}^d$,
- a transition matrix $A \in \mathbb{Q}^{d \times d}$,
- a set of controls $U \subseteq \mathbb{R}^d$,

decide if $\exists T \in \mathbb{N}, u_0, \ldots, u_{T-1} \in U$ such that $x_T = t$ where

$$x_0 = s, \qquad x_{n+1} = Ax_n + u_n.$$

Theorem (Lipton and Kannan, 1986)

LTI-REACHABILITY is decidable if U is an affine subspace of $\mathbb{R}^d$.

Almost no exact results for other classes of U in particular when U is bounded (which is the most natural case).

Hardness

Hardness

Theorem (Fijalkow, Ouaknine, P. Sousa-Pinto, Worrell)

$\mathit{LTI\text{-}REACHABILITY}$ is

- ***undecidable*** *if U is a finite union of affine subspaces.*

Hardness

Theorem (Fijalkow, Ouaknine, P. Sousa-Pinto, Worrell)

$\mathit{LTI\text{-}REACHABILITY}$ is

- ***undecidable*** *if U is a finite union of affine subspaces.*
- ***Skolem-hard*** *if $U = \{0\} \cup V$ where V is an affine subspace*

Since we cannot solve Skolem/Positivity, we need some strong assumptions for decidability.

Hardness

Theorem (Fijalkow, Ouaknine, P. Sousa-Pinto, Worrell)

$\mathit{LTI\text{-}REACHABILITY}$ *is*

- ***undecidable*** *if* U *is a finite union of affine subspaces.*
- ***Skolem-hard*** *if* $U = \{0\} \cup V$ *where* V *is an affine subspace*
- ***Positivity-hard*** *if* U *is a convex polytope*

Since we cannot solve Skolem/Positivity, we need some strong assumptions for decidability.

A positive result

A LTI system (s, A, t, U) is simple if $s = 0$ and

A positive result

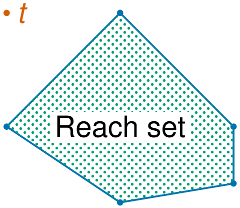
A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,

A positive result

A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,
- the spectral radius of A is less than 1 (stability),

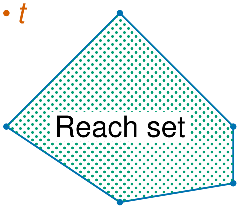


Assumptions imply that the reachable set is an open convex bounded set,

A positive result

A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,
- the spectral radius of A is less than 1 (stability),

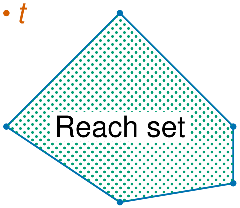


Assumptions imply that the reachable set is an open convex bounded set, but not always a polytope!

A positive result

A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,
- the spectral radius of A is less than 1 (stability),
- some positive power of A has exclusively real spectrum.



Assumptions imply that the reachable set is an open convex bounded set, but not always a polytope!

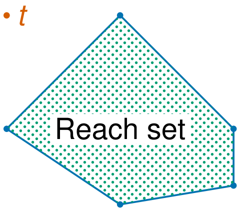
A positive result

A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,
- the spectral radius of A is less than 1 (stability),
- some positive power of A has exclusively real spectrum.

Theorem (Fijalkow, Ouaknine, P. Sousa-Pinto, Worrell)

LTI-REACHABILITY is decidable for simple systems.



Assumptions imply that the reachable set is an open convex bounded set, but not always a polytope!

A positive result

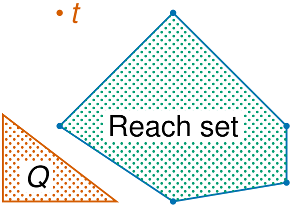
A LTI system (s, A, t, U) is simple if $s = 0$ and

- U is a bounded polytope that contains 0 in its (relative) interior,
- the spectral radius of A is less than 1 (stability),
- some positive power of A has exclusively real spectrum.

Theorem (Fijalkow, Ouaknine, P. Sousa-Pinto, Worrell)

LTI-REACHABILITY is decidable for simple systems.

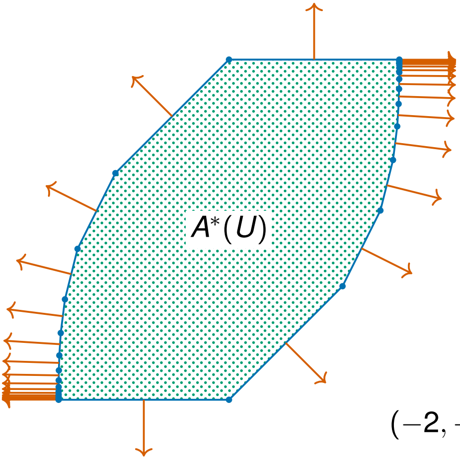
Remark: in fact we can decide reachability to a convex polytope Q.



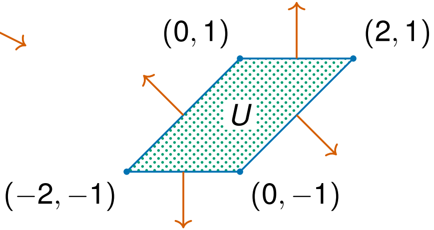
Assumptions imply that the reachable set is an open convex bounded set, but not always a polytope!

Why is this problem hard

The reachable set $A^*(U)$ can have **infinitely** many faces.

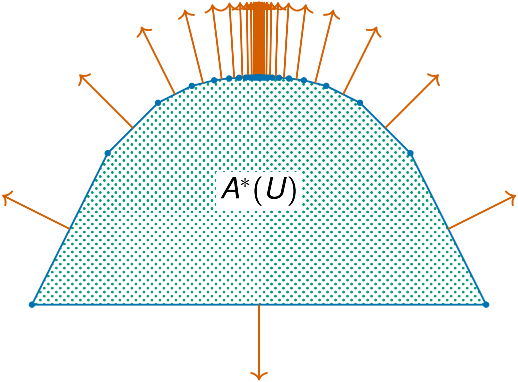


$$A = \begin{bmatrix} \frac{1}{3} & 0 \\ 0 & \frac{2}{3} \end{bmatrix}$$

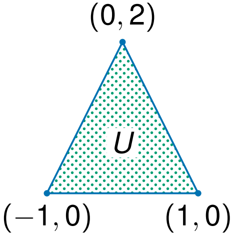


Why is this problem hard

The reachable set $A^*(U)$ can have **faces of lower dimension**: the "top" extreme point does not belong to any facet.



$$A = \begin{bmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{bmatrix}$$



Why is this problem hard

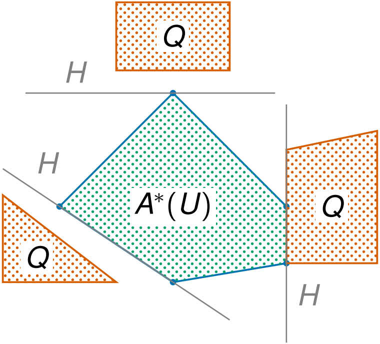
Approach: two semi-decision procedures

- reachability: under-approximations of the reachable set
- non-reachability: **separating hyperplanes**

Why is this problem hard

Approach: two semi-decision procedures

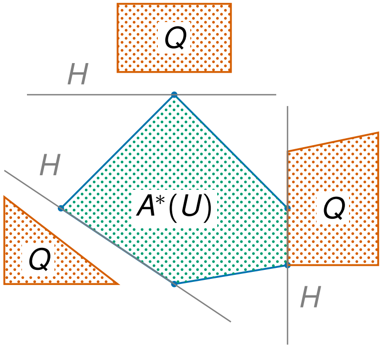
- reachability: under-approximations of the reachable set
- non-reachability: **separating hyperplanes**



Why is this problem hard

Approach: two semi-decision procedures

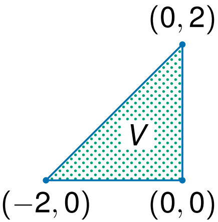
- reachability: under-approximations of the reachable set
- non-reachability: **separating hyperplanes**

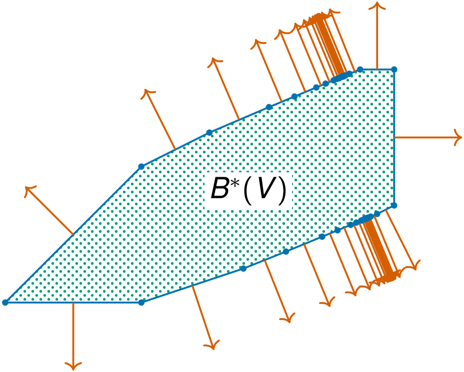


Further difficulty: a separating hyperplane may not be supported by a facet of either $A^*(U)$ or Q.

Why is this problem hard

$$B = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 \end{bmatrix}$$

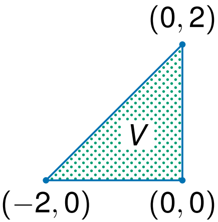


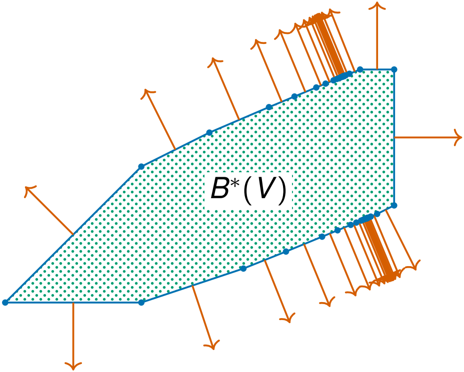


Even more difficulty: $B^*(V)$ has two extreme points that do not belong to any facet and have rational coordinates, but whose (unique) separating hyperplane requires the use of algebraic irrationals

Why is this problem hard

$$B = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 \end{bmatrix}$$





Even more difficulty: $B^*(V)$ has two extreme points that do not belong to any facet and have rational coordinates, but whose (unique) separating hyperplane requires the use of algebraic irrationals

Theorem (Non-reachable instances)

There is a separating hyperplane with algebraic coefficients.

Conclusion on control

Exact reachability for LTI systems:

- decidability crucially depends on the shape of the control set
- even with convex bounded inputs, the problem is very hard (Skolem/Positivity, open for 70 years)
- we can recover decidability using strong spectral assumptions

Conclusion on control

Exact reachability for LTI systems:

- decidability crucially depends on the shape of the control set
- even with convex bounded inputs, the problem is very hard (Skolem/Positivity, open for 70 years)
- we can recover decidability using strong spectral assumptions

Despite an extensive literature in control theory, the decidability control problems is still very open.

Invariant Synthesis

Does this program halt?

Affine program

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

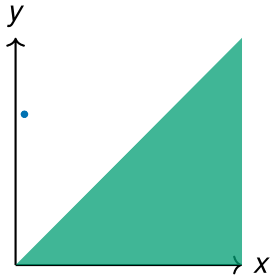
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Does this program halt?

Affine program

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

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

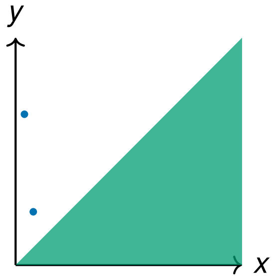


Does this program halt?

Affine program

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

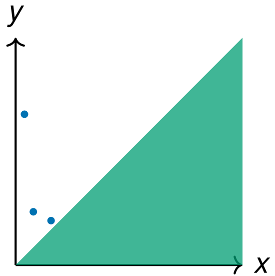
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



Does this program halt?

Affine program

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

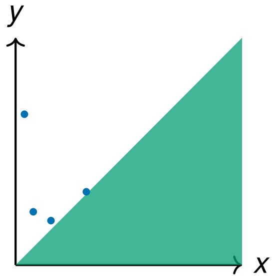


Does this program halt?

Affine program

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

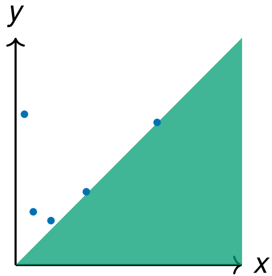
$$\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 2 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$



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?

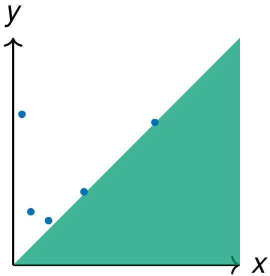
Affine program

$x := 2^{-10}$
$y := 1$
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:

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



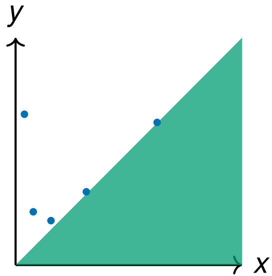
Does this program halt?

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:

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



- (2) is an invariant: it holds at every step

Does this program halt?

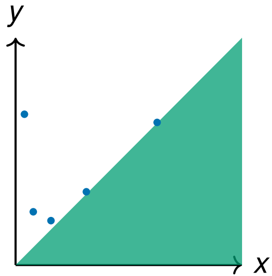
Affine program

$x := 2^{-10}$
$y := 1$
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:

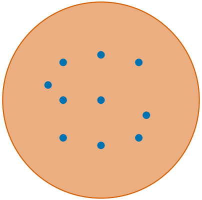
$$x^2 y - x^3 = \frac{1023}{1073741824} \qquad (2)$$



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

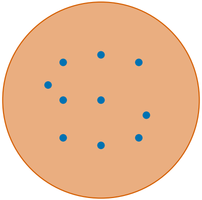
Invariants

invariant = overapproximation of the reachable states

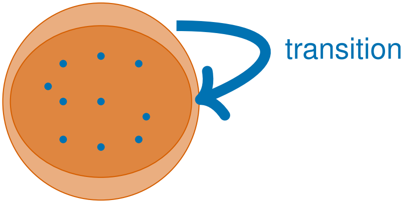


Invariants

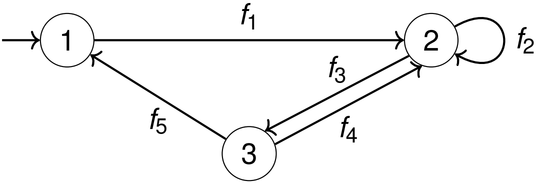
invariant = overapproximation of the reachable states



inductive invariant = invariant preserved by the transition relation

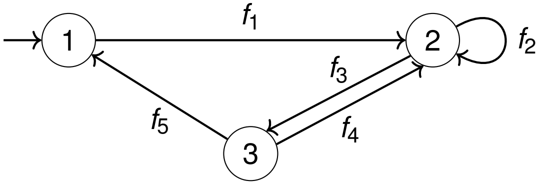


Inductive invariants: example



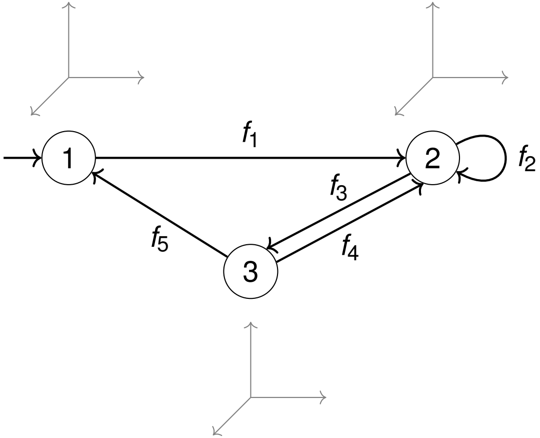
Inductive invariants: example

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



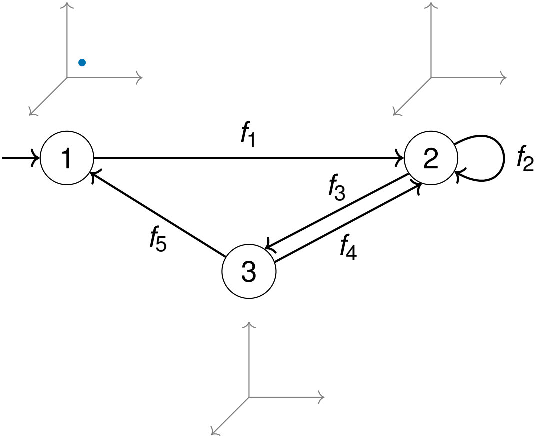
Inductive invariants: example

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



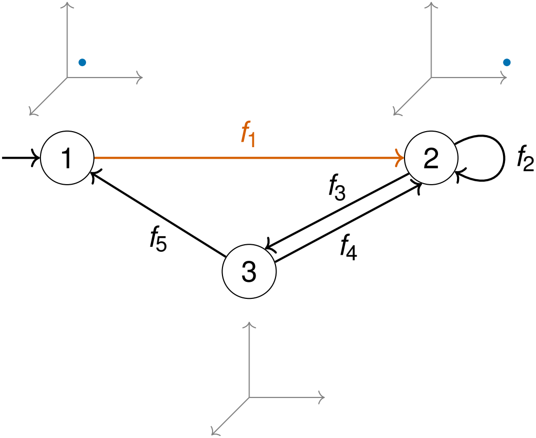
Inductive invariants: example

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



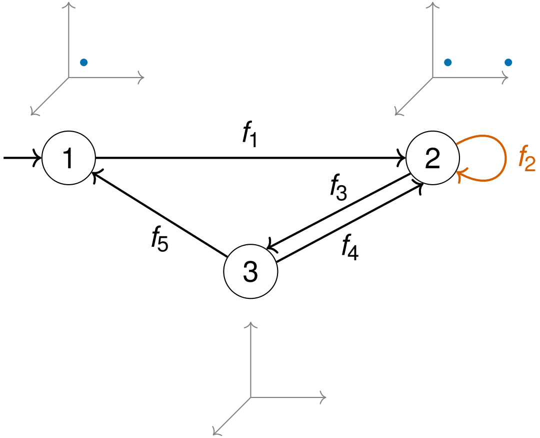
Inductive invariants: example

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



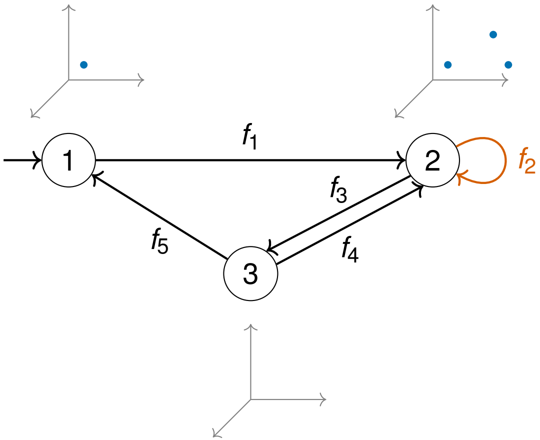
Inductive invariants: example

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



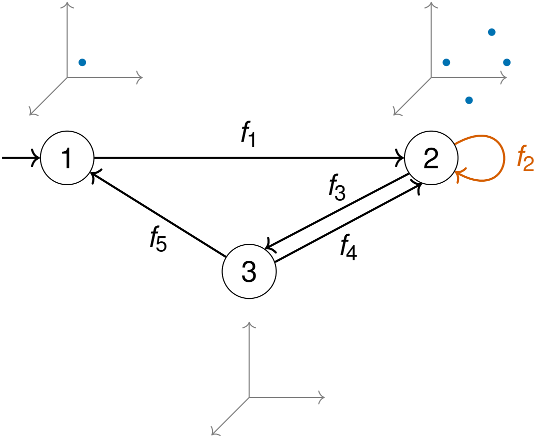
Inductive invariants: example

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



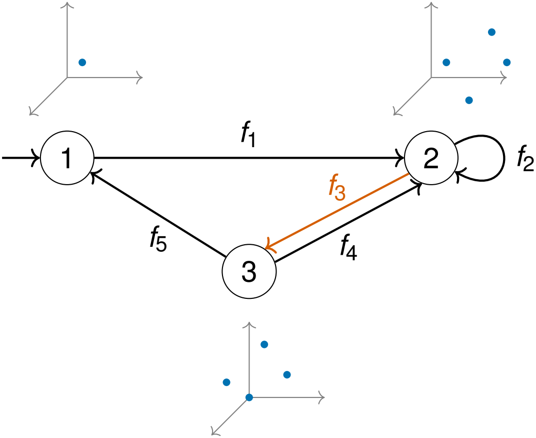
Inductive invariants: example

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



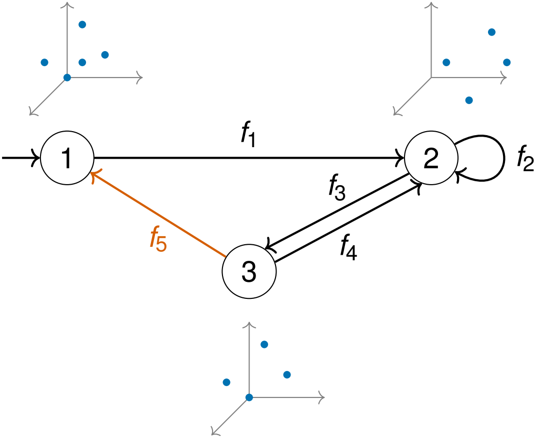
Inductive invariants: example

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



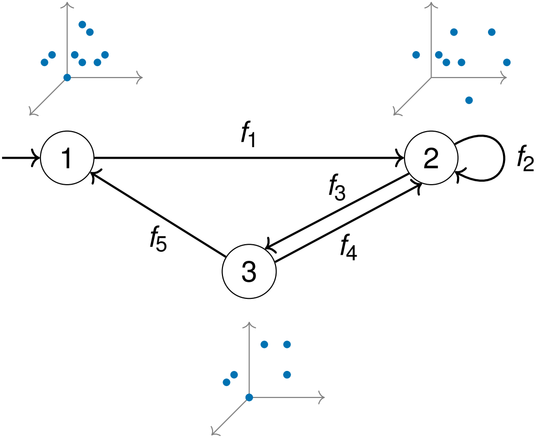
Inductive invariants: example

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



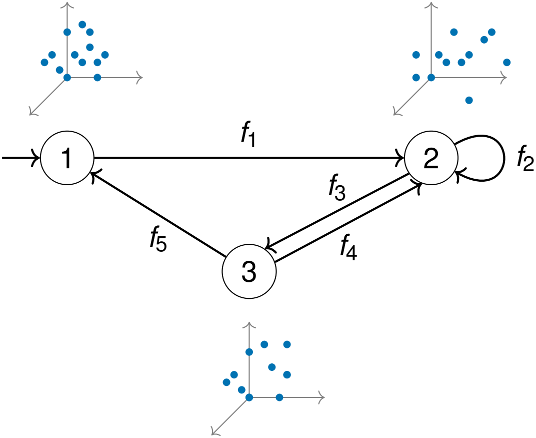
Inductive invariants: example

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



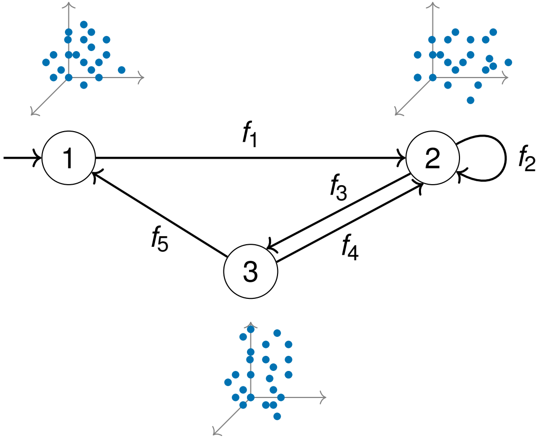
Inductive invariants: example

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



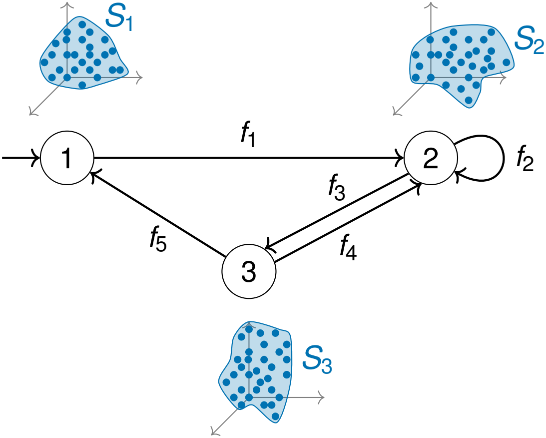
Inductive invariants: example

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



Inductive invariants: example

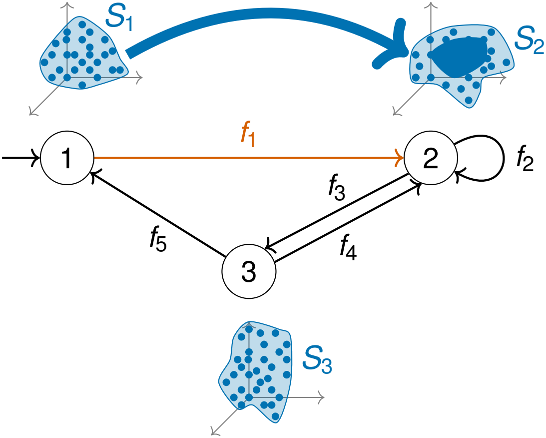
x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



S_1, S_2, S_3 are the reachable states

Inductive invariants: example

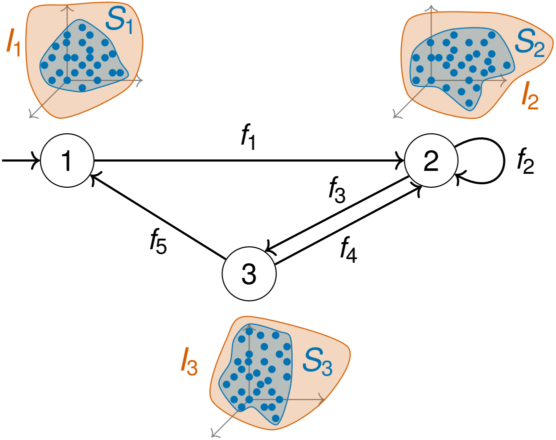
x, y, z range over $\mathbb{Q}$ $\qquad f_i : \mathbb{R}^3 \to \mathbb{R}^3$



S_1, S_2, S_3 is also an inductive invariant

Inductive invariants: example

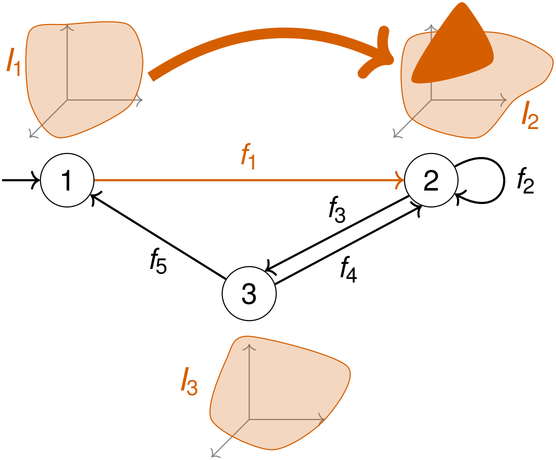
x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



I_1, I_2, I_3 is an invariant

Inductive invariants: example

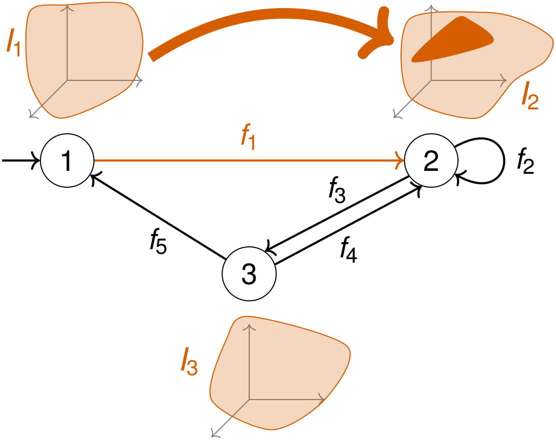
x, y, z range over $\mathbb{Q}$ $f_i : \mathbb{R}^3 \to \mathbb{R}^3$



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

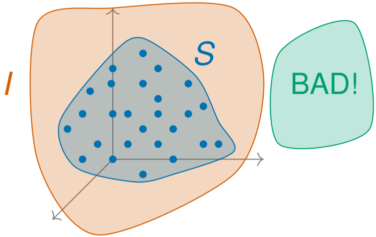
Inductive invariants: example

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

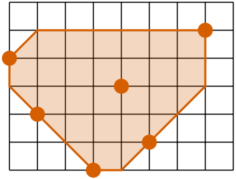
Why Invariants?



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.***

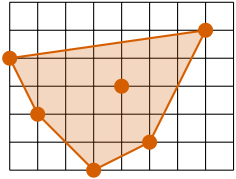
D. Beyer, T. Henzinger, R. Majumdar, and A. Rybalchenko
Invariant Synthesis for Combined Theories, 2007

Which invariants?



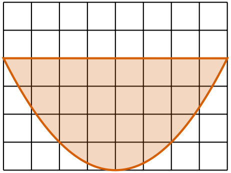
Octagons

$\leqslant$



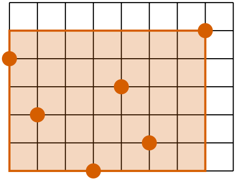
Polyhedrons

$\leqslant$

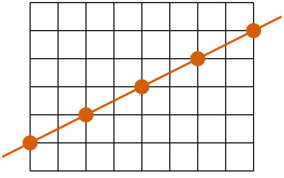


Semialgebraic sets

$\rotatebox{90}{$\leqslant$}$ $\rotatebox{90}{$\leqslant$}$ $\rotatebox{90}{$\leqslant$}$

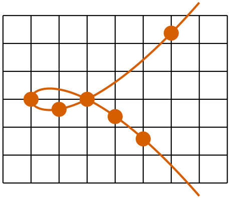


Intervals



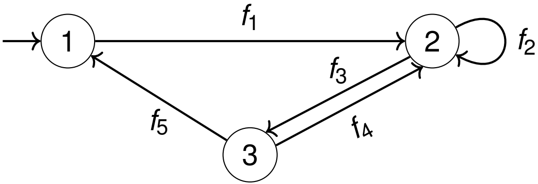
Affine/linear sets

$\leqslant$



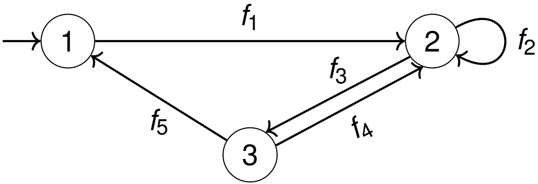
Algebraic sets =
polynomial equalities

Affine programs



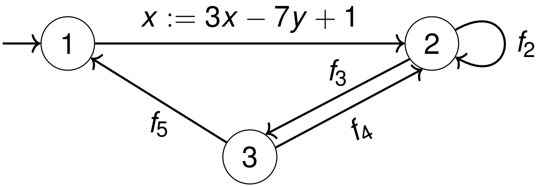
Affine programs

- Nondeterministic branching (no guards)



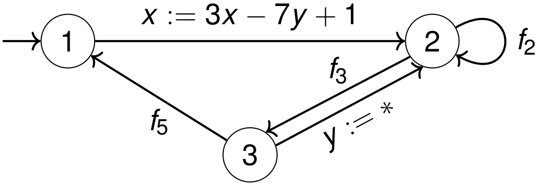
Affine programs

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



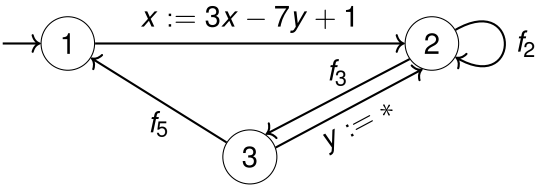
Affine programs

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



Affine programs

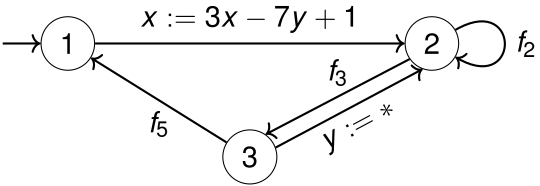
- Nondeterministic branching (no guards)
- All assignments are affine
- Allow nondeterministic assignments ($x := *$)



- 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

Karr's Algorithm

Affine Relationships Among Variables of a Program*

Michael Karr

Received May 8, 1974

Summary. Several optimizations of programs can be performed when in certain regions of a program equality relationships hold between a linear combination of the variables of the program and a constant. This paper presents a practical approach to detecting these relationships by considering the problem from the viewpoint of linear algebra. Key to the practicality of this approach is an algorithm for the calculation of the "sum" of linear subspaces.

Theorem (Karr 76)

There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, its strongest affine inductive invariant.

Discovering Affine Equalities Using Random Interpretation

Sumit Gulwani George C. Necula
University of California, Berkeley
{gulwani,necula}@cs.berkeley.edu

ABSTRACT

We present a new polynomial-time randomized algorithm for discovering affine equalities involving variables in a program.

Keywords

Affine Relationships, Linear Equalities, Random Interpretation, Randomized Algorithm

Some polynomial invariants

A Note on Karr's Algorithm

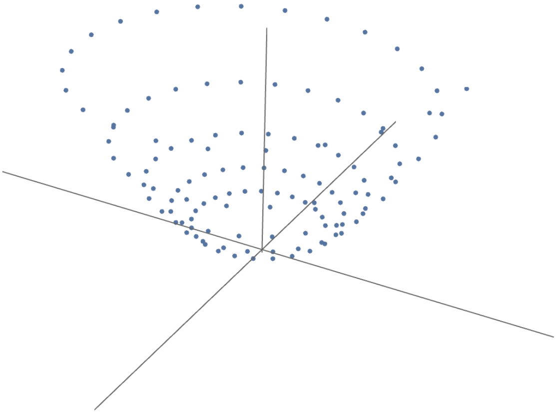
Markus Müller-Olm[1⋆] and Helmut Seidl[2]

Abstract. We give a simple formulation of Karr's algorithm for computing all affine relationships in affine programs. This simplified algorithm runs in time $\mathcal{O}(nk^3)$ where n is the program size and k is the number of program variables assuming unit cost for arithmetic operations. This improves upon the original formulation by a factor of k. Moreover, our re-formulation avoids exponential growth of the lengths of intermediately occurring numbers (in binary representation) and uses less complicated elementary operations. We also describe a generalization that determines all polynomial relations up to degree d in time $\mathcal{O}(nk^{3d})$.

Theorem (ICALP 2004)

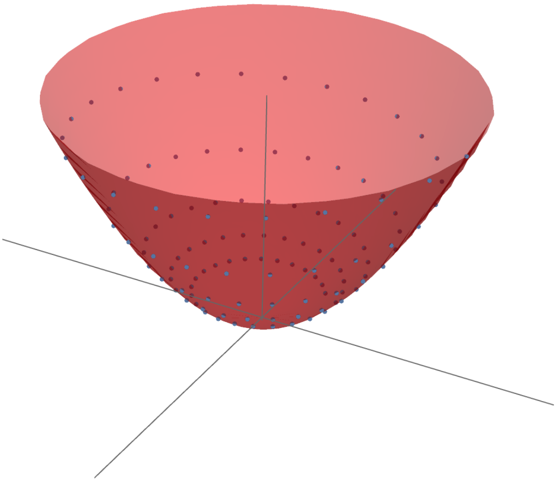
There is an algorithm which computes, for any given affine program over $\mathbb{Q}$, all its polynomial inductive invariants up to any ***fixed degree*** *d.*

Why fixed degree is not enough



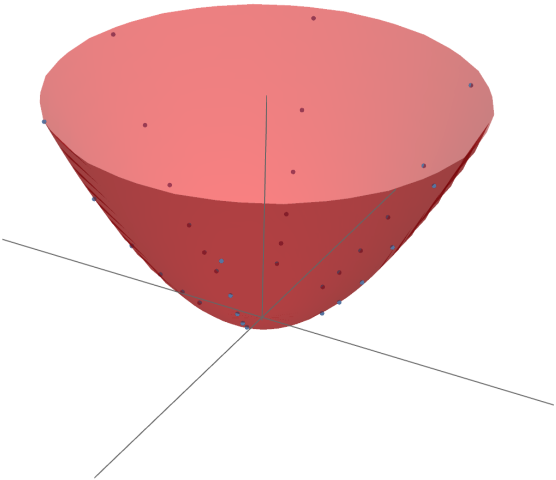
Why fixed degree is not enough

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



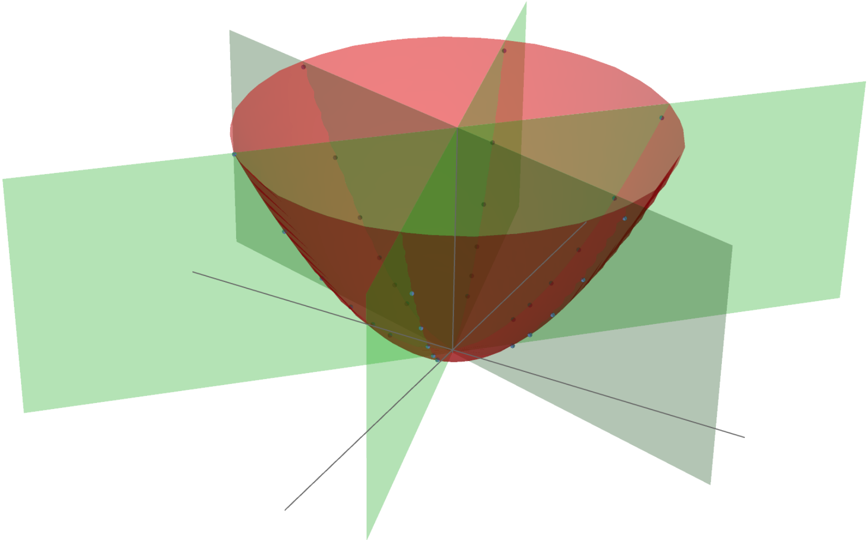
Why fixed degree is not enough

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



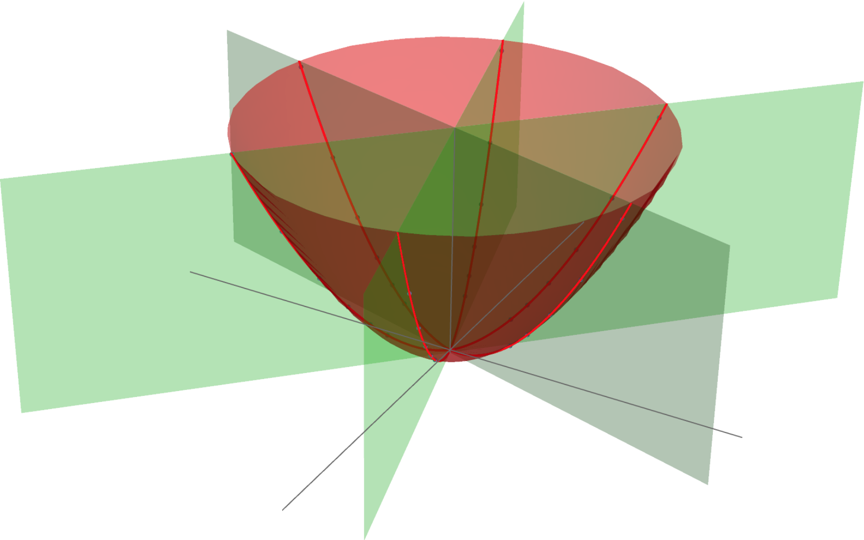
Why fixed degree is not enough

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



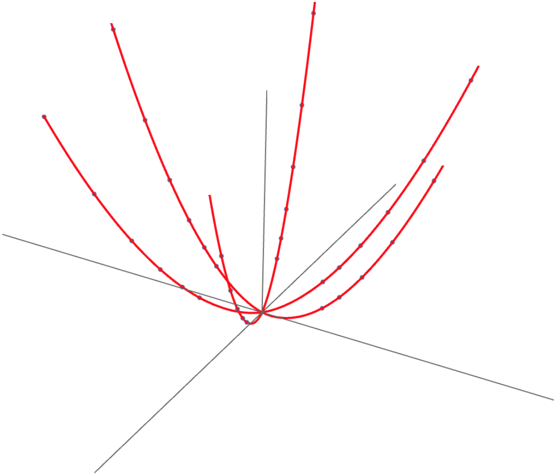
Why fixed degree is not enough

- 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 $(x - y)(10y + x)(y + 10x) = 0$



Main result

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

There is an algorithm which computes, for any given affine program over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

Main result

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

There is an algorithm which computes, for any given affine program over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

- strongest polynomial invariant $\iff$ smallest algebraic set

Main result

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

There is an algorithm which computes, for any given affine program over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

- strongest polynomial invariant $\iff$ smallest algebraic set
- Thus our algorithm computes all polynomial relations that always hold among program variables at each program location, in all possible executions of the program

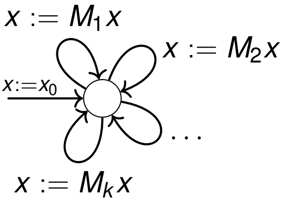
Main result

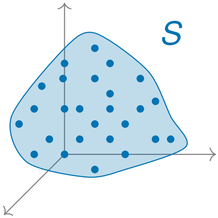
Theorem (Hrushovski, Ouaknine, P., Worrell, 2018)

There is an algorithm which computes, for any given affine program over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

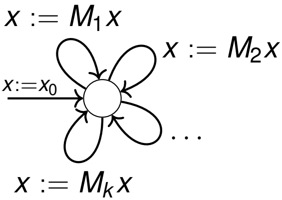
- strongest polynomial invariant $\iff$ smallest algebraic set
- Thus our algorithm computes all polynomial relations that always hold among program variables at each program location, in all possible executions of the program
- We represent this using a finite basis of polynomial equalities

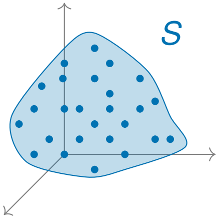
At the edge of decidability





At the edge of decidability



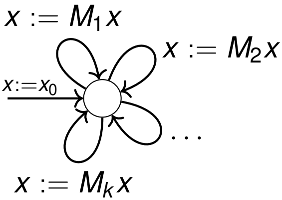


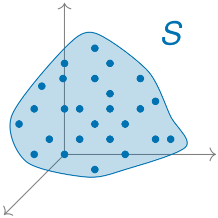
Theorem (Markov 1947[§])

There is a fixed set of 6×6 *integer matrices* $M_1, \dots, M_k$ *such that the reachability problem "*y *is reachable from* x_0*?" is undecidable.*

[§]Original theorems about semigroups, reformulated with affine programs.

At the edge of decidability





Theorem (Markov 1947§)

There is a fixed set of 6×6 *integer matrices* $M_1, \dots, M_k$ *such that the reachability problem "y is reachable from x_0?" is undecidable.*

Theorem (Paterson 1970*)

The mortality problem "0 is reachable from x_0 with $M_1, \dots, M_k$?" is undecidable for 3×3 *matrices.*

§Original theorems about semigroups, reformulated with affine programs.

Zariski closure of finitely generated groups

Our algorithm relies on this result:

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 which computes, for any given affine program over $\mathbb{Q}$ using only invertible transformations, its strongest polynomial inductive invariant.

Equivalently, compute the Zariski closure of a finitely generated groups of matrices.

From groups to semigroup

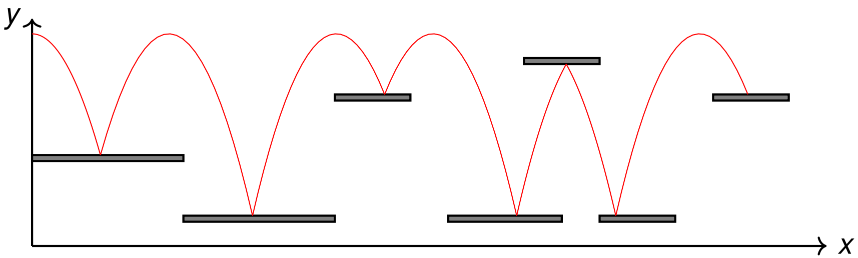
Theorem (Hrushovski, Ouaknine, P., Worrell, 2018)

There is an algorithm that computes the Zariski closure of any finitely semigroup of matrices (with algebraic coefficients), given its generators as inputs.

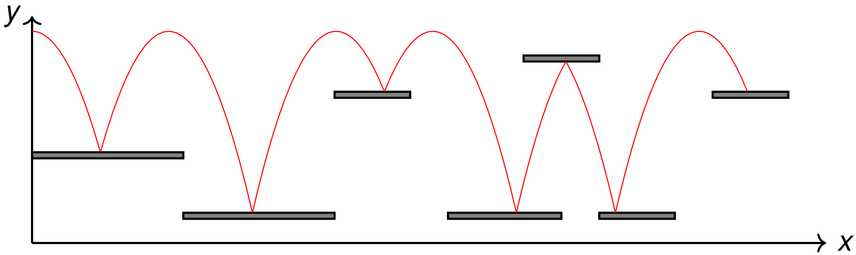
Corollary

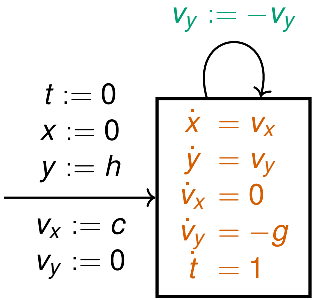
Given an affine program, we can compute for each location the ideal of all polynomial relations that hold at that location.

Going hybrid: a bouncing ball



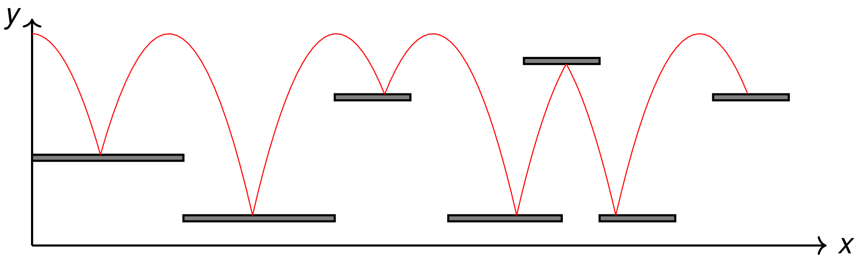
Going hybrid: a bouncing ball

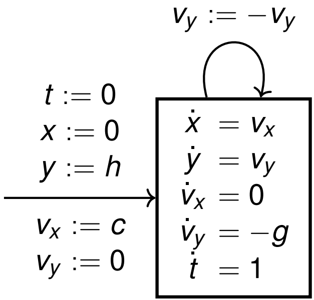




- affine program: collision
- $+$ linear differential equation: mechanics
- $=$ linear hybrid automaton

Going hybrid: a bouncing ball





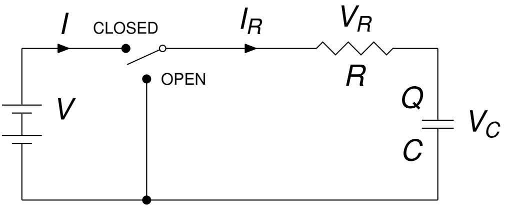
- affine program: collision
- \+ linear differential equation: mechanics
- = linear hybrid automaton

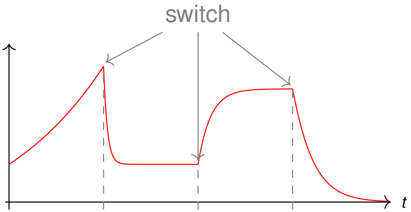
Invariants:

- $v_x = c$
- $x = tc$
- $v_y^2 + 2g(y - h) = 0$

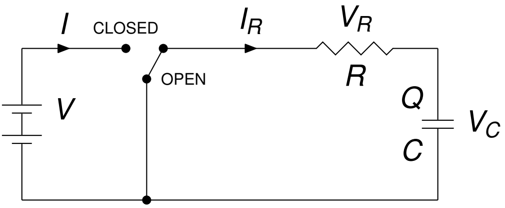
recover conservation of energy!

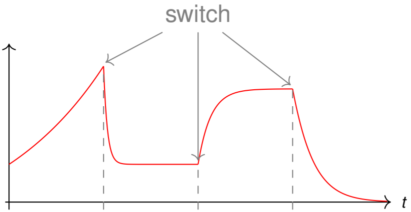
Example: RC circuit





Example: RC circuit

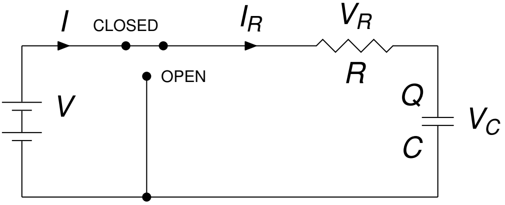


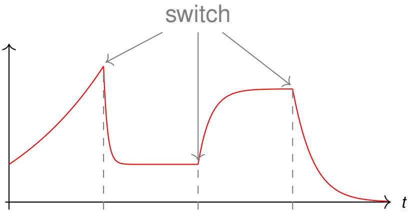


OPEN

$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

Example: RC circuit





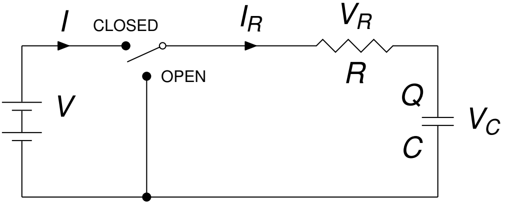
OPEN

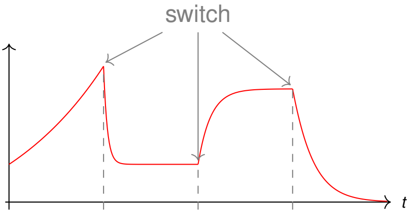
$$\boxed{\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

CLOSED

$$\boxed{\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}}$$

Example: RC circuit





OPEN

$$\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

OPEN → CLOSED:

$$\begin{aligned} I &:= \frac{1}{R}(V - V_C) \\ I_R &:= \frac{1}{R}(V - V_C) \\ V_R &:= V - V_C \end{aligned}$$

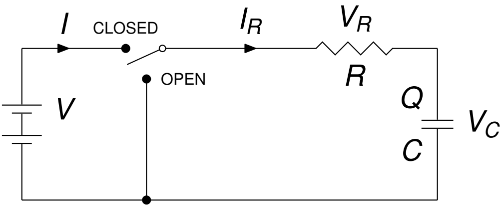
CLOSED → OPEN:

$$\begin{aligned} I &:= 0 \\ I_R &:= -\frac{1}{R} V_C \\ V_R &:= -V_C \end{aligned}$$

CLOSED

$$\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

Example: RC circuit



Invariants

OPEN	CLOSED
$Q = CV_C$	$Q = CV_C$
$V_R = RI_R$	$V_R = RI_R$
$I = 0$	$I = I_R$
$V_R = -V_C$	$V_R = V - V_C$

OPEN

$$\begin{aligned} \dot{I} &= 0 \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

OPEN → CLOSED:

$$\begin{aligned} I &:= \frac{1}{R}(V - V_C) \\ I_R &:= \frac{1}{R}(V - V_C) \\ V_R &:= V - V_C \end{aligned}$$

CLOSED → OPEN:

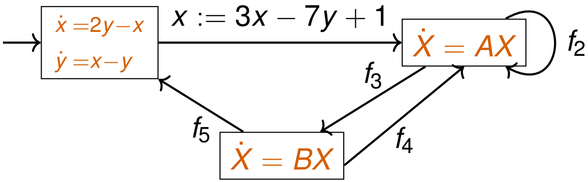
$$\begin{aligned} I &:= 0 \\ I_R &:= -\frac{1}{R} V_C \\ V_R &:= -V_C \end{aligned}$$

CLOSED

$$\begin{aligned} \dot{I} &= -\frac{1}{RC} I_R \\ \dot{I}_R &= -\frac{1}{RC} I_R \\ \dot{V}_R &= -\frac{1}{C} I_R \\ \dot{Q} &= I_R \\ \dot{V}_C &= \frac{1}{C} I_R \end{aligned}$$

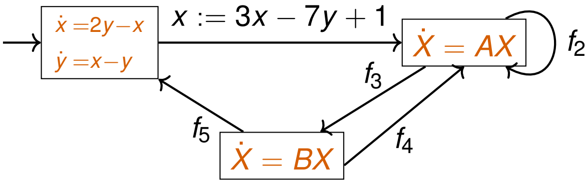
Linear Hybrid Automata

- Nondeterministic branching (no guards)
- All assignments are affine
- Linear differential equations in each location



Linear Hybrid Automata

- Nondeterministic branching (no guards)
- All assignments are affine
- Linear differential equations in each location



- More general than affine programs
- More general than linear differential equations

From affine programs to hybrid automata

Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

There is an algorithm that computes, for any given guard-free linear hybrid automaton over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

From affine programs to hybrid automata

Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

There is an algorithm that computes, for any given guard-free linear hybrid automaton over $\overline{\mathbb{Q}}$, its strongest polynomial inductive invariant.

For systems with purely continuous dynamics, *i.e.* no discrete transitions, called switching systems:

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

There is no algorithm that computes the strongest algebraic inductive invariant for the class of switching systems with equality guards.

From hybrid automata to affine programs

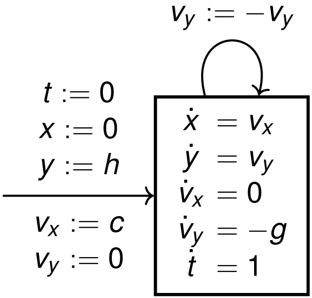
Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

There is an algorithm that computes, for any given ***guard-free linear hybrid automaton*** *over $\mathbb{Q}$, an* ***affine program*** *over $\mathbb{Q}$ that has the same polynomial inductive invariants.*

From hybrid automata to affine programs

Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

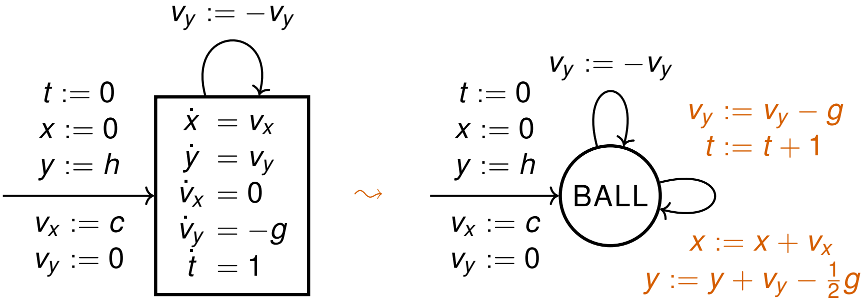
There is an algorithm that computes, for any given ***guard-free linear hybrid automaton*** *over $\mathbb{Q}$, an* ***affine program*** *over $\mathbb{Q}$ that has the same polynomial inductive invariants.*



From hybrid automata to affine programs

Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

*There is an algorithm that computes, for any given **guard-free linear hybrid automaton** over $\mathbb{Q}$, an **affine program** over $\mathbb{Q}$ that has the same polynomial inductive invariants.*



Linear Differential Equations

For $x(t) \in \mathbb{R}^n$ and A rational matrix, consider

$$\dot{x} = Ax$$

The solution is

$$x(t) = e^{At}x(0)$$

where e^X is the matrix exponential.

Linear Differential Equations

For $x(t) \in \mathbb{R}^n$ and A rational matrix, consider

$$\dot{x} = Ax$$

The solution is

$$x(t) = e^{At}x(0)$$

where e^X is the matrix exponential. Recall that:

- strongest algebraic invariant = smallest algebraic set
- smallest algebraic set containing X = Zariski closure $\overline{X}$ of X

Lemma

Let A be a rational matrix, there exists B an algebraic matrix such that $\overline{\langle B \rangle} = \overline{\langle e^A \rangle} = \overline{\{e^{At} : t \in \mathbb{R}\}}$.

Linear Differential Equations

For $x(t) \in \mathbb{R}^n$ and A rational matrix, consider

$$\dot{x} = Ax$$

The solution is

$$x(t) = e^{At} x(0)$$

where e^X is the matrix exponential. Recall that:

- strongest algebraic invariant = smallest algebraic set
- smallest algebraic set containing X = Zariski closure $\overline{X}$ of X

Lemma

Let A be a rational matrix, there exists B an algebraic matrix such that $\overline{\langle B \rangle} = \overline{\langle e^A \rangle} = \overline{\{e^{At} : t \in \mathbb{R}\}}$.

- obvious candidate $B = e^A$ is not algebraic
- "reverse-engineer" B algebraic to encode some multiplicative relations between the eigenvalues

Complexity of computing the Zariski closure

How expensive is it to compute this strongest invariant ?

$$\boxed{\text{linear hybrid}} \xrightarrow{\text{reduce}} \boxed{\text{semigroup}} \xrightarrow{\text{reduce}} \boxed{\text{group}}$$

Complexity of computing the Zariski closure

How expensive is it to compute this strongest invariant ?

$$\boxed{\text{linear hybrid}} \xrightarrow{\text{reduce}} \boxed{\text{semigroup}} \xrightarrow{\text{reduce}} \boxed{\text{group}}$$

Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm that computes the Zariski closure of any finitely group of matrices, given its generators as inputs.

No complexity bounds. It is not clear it is even elementary.

Complexity of computing the Zariski closure

How expensive is it to compute this strongest invariant ?

$$\boxed{\text{linear hybrid}} \xrightarrow{\text{reduce}} \boxed{\text{semigroup}} \xrightarrow{\text{reduce}} \boxed{\text{group}}$$

Theorem (Derksen, Jeandel and Koiran, 2004)

There is an algorithm that computes the Zariski closure of any finitely group of matrices, given its generators as inputs.

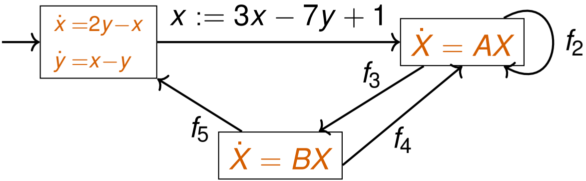
No complexity bounds. It is not clear it is even elementary.

Theorem (Nosan, P., Schmitz, Shirmohammadi, Worrell, 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.

Summary

- invariant = overapproximation of reachable states
- invariants allow verification of safety properties
- guard-free linear hybrid automata:
  - nondeterministic branching, no guards, affine assignments
  - linear differential equations



Theorem (Majumdar, Ouaknine, P., Worrell, 2020)

There is an algorithm that computes, for any given guard-free linear hybrid automaton over $\mathbb{Q}$, its strongest polynomial inductive invariant.