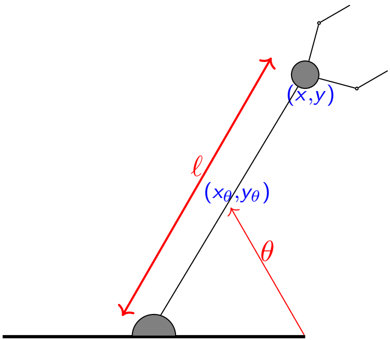
Solvability of Matrix-Exponential Equations

Joël Ouaknine, Amaury Pouly, João Sousa-Pinto,
James Worrell

University of Oxford

Example: 2D robot



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

Discretized actions:

- rotate arm by ψ
- change arm length by δ

$\rightarrow$ Linear transformations:

$$u \leftarrow Au$$

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:

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

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
- controllability

Related work in the discrete case

Input: $A, C \in \mathbb{Q}^{d \times d}$ matrices

Output: $\exists n \in \mathbb{N}$ such that $A^n = C$?

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

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

Related work in the discrete case

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

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

Related work in the discrete case

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

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

Related work in the discrete case

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

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

Related work in the discrete case

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

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

Related work in the discrete case

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

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

Related work in the discrete case

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

Input: $A_1, \dots, A_k, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $C \in \langle$semi-group generated by $A_1, \dots, A_k\rangle$?

Semi-group: $\langle A_1, \dots, A_k\rangle =$ all finite products of $A_1, \dots, A_k$
Examples:

$$A_1 A_3 A_2 \quad A_1 A_2 A_1 A_2 \quad A_3^8 A_2 A_1^3 A_3^{42}$$

Related work in the discrete case

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: $C \in \langle$semi-group generated by $A_1, \ldots, A_k\rangle$?
✓ Decidable if A_i commute × Undecidable in general

Semi-group: $\langle A_1, \ldots, A_k\rangle$ = all finite products of $A_1, \ldots, A_k$
Examples:

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

Recap on linear differential equations

Let $x : \mathbb{R}_+ \to \mathbb{R}^n$ function, $A \in \mathbb{Q}^{n \times n}$ matrix

$$x(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Linear differential equation:

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

Recap on linear differential equations

Let $x : \mathbb{R}_+ \to \mathbb{R}^n$ function, $A \in \mathbb{Q}^{n\times n}$ matrix

$$x(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Linear differential equation:

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

Examples:

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

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

$$\begin{cases} x_1'(t) = x_2(t) \\ x_2'(t) = -x_1(t) \end{cases}$$

$$\rightsquigarrow \begin{cases} x_1(t) = \sin(t) \\ x_2(t) = \cos(t) \end{cases}$$

Recap on linear differential equations

Let $x : \mathbb{R}_+ \to \mathbb{R}^n$ function, $A \in \mathbb{Q}^{n\times n}$ matrix

$$x(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Linear differential equation:

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

Examples:

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

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

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

$$\rightsquigarrow \begin{cases} x_1(t) = \sin(t) \\ x_2(t) = \cos(t) \end{cases}$$

Recap on linear differential equations

Let $x : \mathbb{R}_+ \to \mathbb{R}^n$ function, $A \in \mathbb{Q}^{n\times n}$ matrix

$$x(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Linear differential equation:

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

General solution form:

$$x(t) = \exp(At)x_0$$

$$\text{where } \exp(M) = \sum_{n=0}^{\infty} \frac{M^n}{n!}$$

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

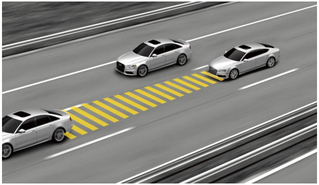
Input: $A, C \in \mathbb{Q}^{d\times d}$ matrices
Output: $\exists t \in \mathbb{R}$ such that $e^{At} = C$? ✓ Decidable (PTIME)

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

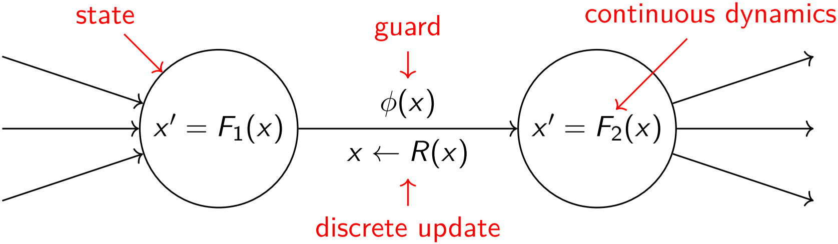
Example: $\exists t, u \in \mathbb{R}$ such that

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

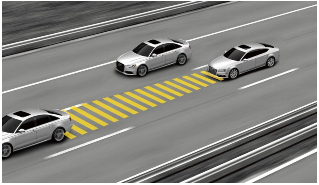
Hybrid/Cyber-physical systems



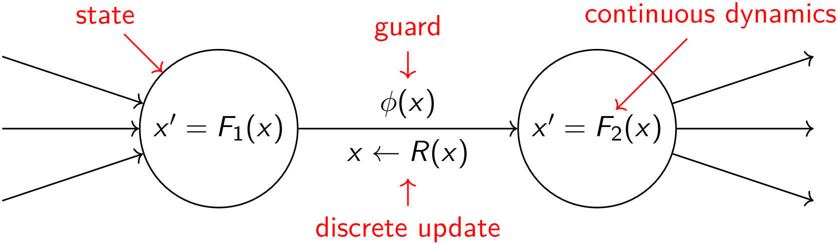
- physics: continuous dynamics
- electronics: discrete states



Hybrid/Cyber-physical systems



- physics: continuous dynamics
- electronics: discrete states



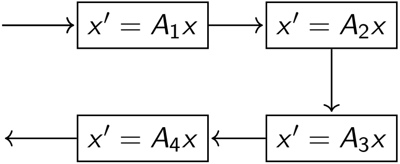
Some classes:

- $F_i(x) = 1$: timed automata
- $F_i(x) = c_i$: rectangular hybrid automata
- $F_i(x) = A_i x$: linear hybrid automata

Typical questions

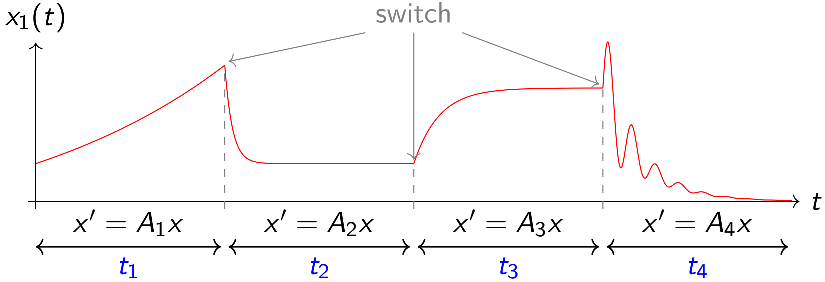
- reachability
- safety
- controllability

Switching system

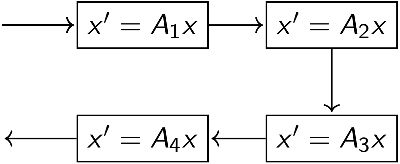


Restricted hybrid system:

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

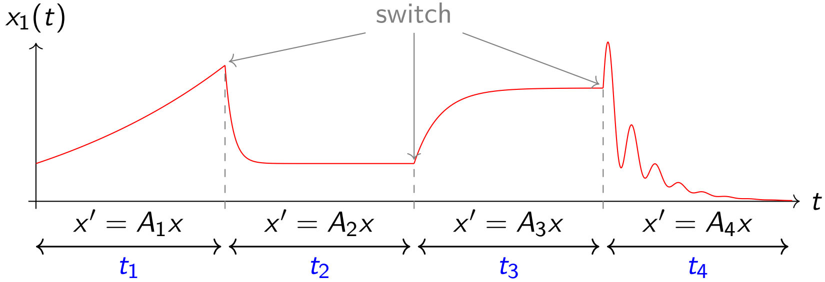


Switching system



Restricted hybrid system:

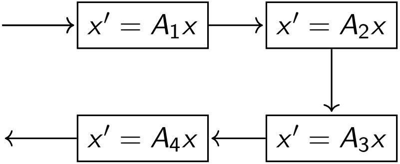
- linear dynamics
- no guards (nondeterministic)
- no discrete updates



Dynamics:

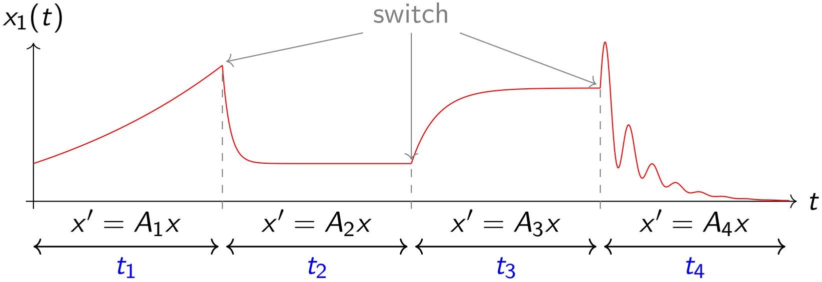
$$e^{A_4 t_4} e^{A_3 t_3} e^{A_2 t_2} e^{A_1 t_1}$$

Switching system



Restricted hybrid system:

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

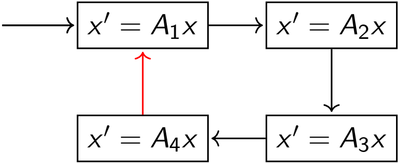


Problem:

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

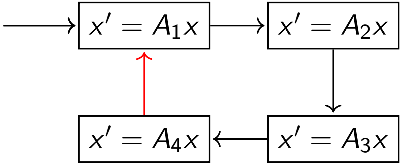
What we control: $t_1, t_2, t_3, t_4 \in \mathbb{R}_+$

Switching system

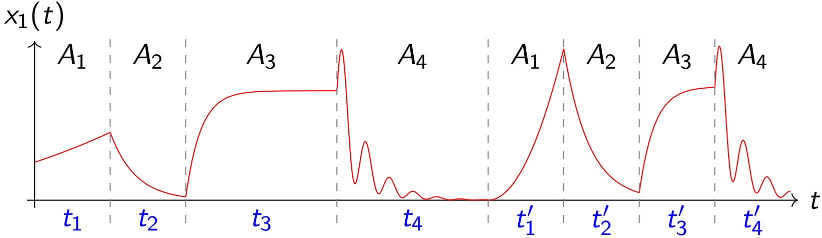


What about a loop ?

Switching system



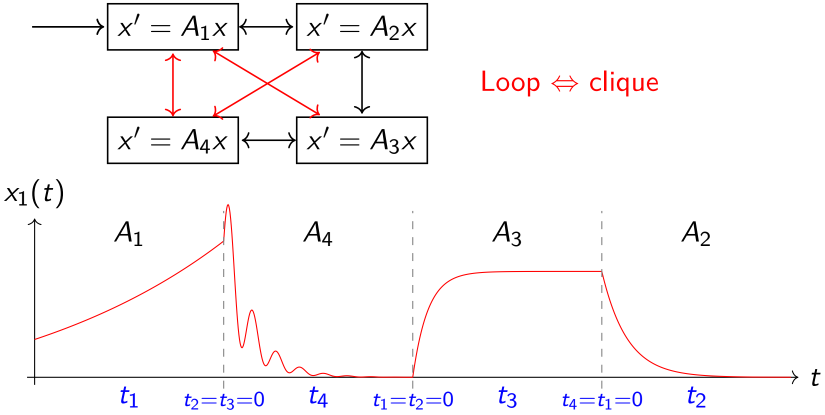
What about a loop ?



Dynamics:

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

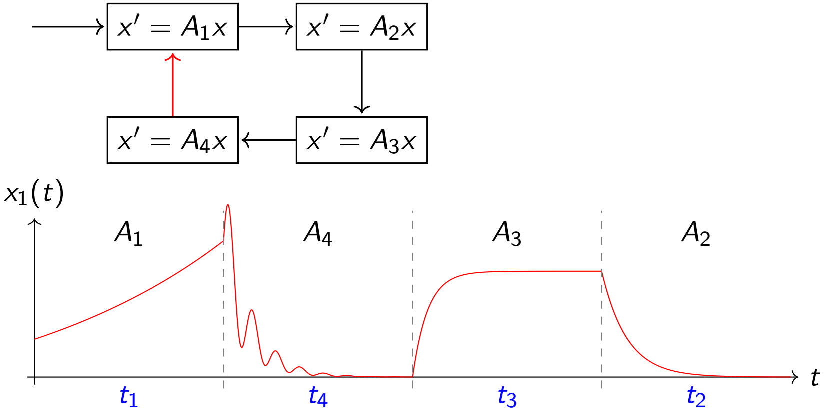
Switching system



Remark:

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

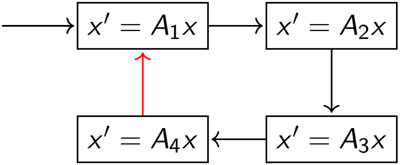
Switching system

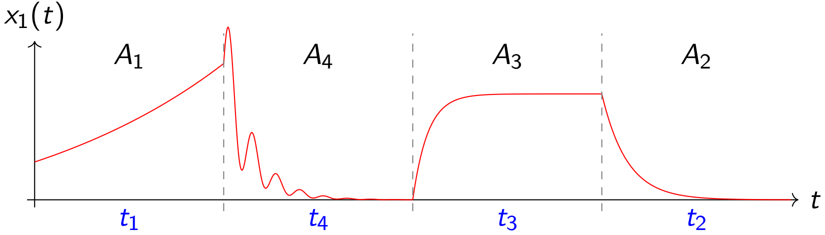


Dynamics:

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

Switching system





Problem:

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

where

$$\mathcal{G} = \langle \text{semi-group generated by } e^{A_i t} \text{ for all } t \geqslant 0 \rangle$$

Main results

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

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

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

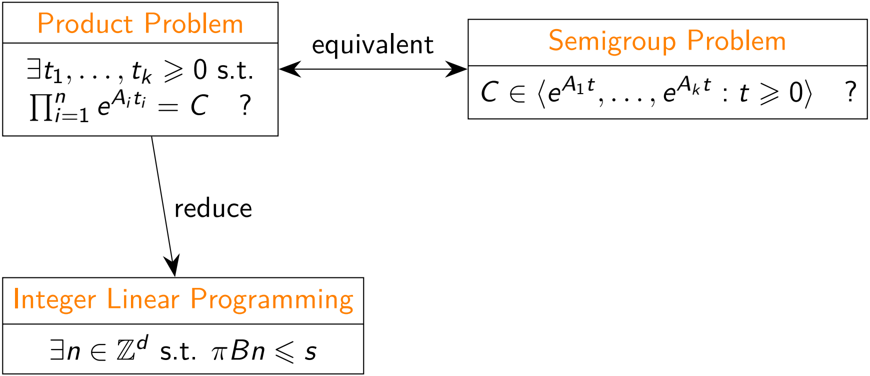
$$C \in \langle \text{semigroup generated by } e^{A_1 t}, \ldots, e^{A_k t} : t \geqslant 0 \rangle \quad ?$$

Theorem

Both problems are:

- Undecidable in general
- Decidable when all the A_i commute

Some words about the proof (commuting case)



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

⟷ 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

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

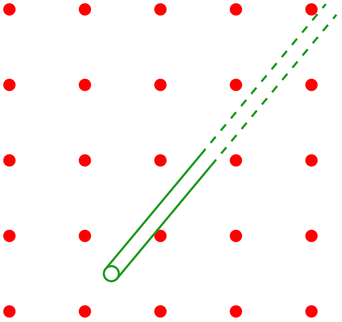
Integer Linear Programming

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

where s is a linear form in logarithms of algebraic numbers

Key ingredient: Diophantine approximations

- Finding integer points in cones: Kronecker's theorem



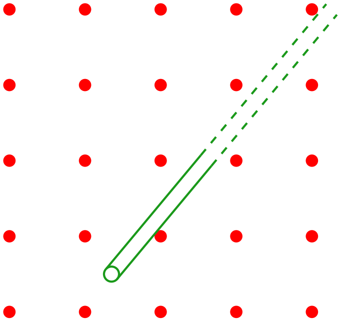
Integer Linear Programming

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

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 →

Semigroup Problem

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

Hilbert's Tenth Problem

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

↑ reduce (Hilbert's Tenth Problem → Product Problem)

Theorem (Matiyasevich)

Hilbert's Tenth Problem is undecidable

Conclusion

- Continuous extension of discrete matrix power problems studied by Lipton, Cai, Potapov, ...
- Motivated by verification, synthesis and controllability problems for cyber-physical systems
- (Un-)decidability results achieved with number-theoretic tools and integer linear programming