Nondeterminism and Analog Computation: towards a characterization of **NP**

Jacques Dreyfus

Computer Science Laboratory of École Polytechnique (LIX)

September 26, 2025

Overview

- State of the art :

Overview

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])

Overview

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])

Overview

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])
- First result :
  - Extending [Thi18] to characterize **NP**

Overview

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])
- First result :
  - Extending [Thi18] to characterize **NP**
- Second result :
  - Unification of approaches via the length of the curve
  - Existence of a computable canonical representative of an analytic function

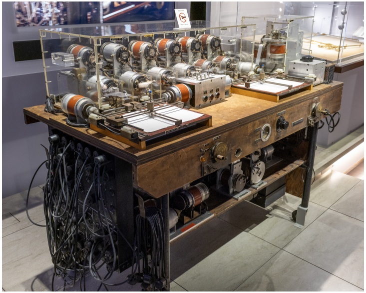


Figure 1: A differential analyser

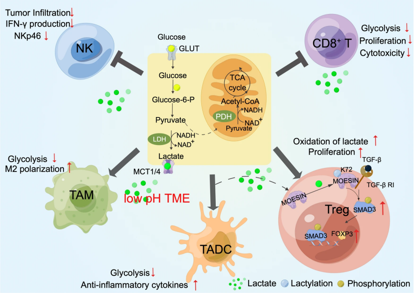


Figure 2: A natural model ([SLH22])

- 1941 : *General Purpose Analog Computer (GPAC)* ([Sha41])
- Association of basic blocks $(k, +, -, \times, \int)$ to build circuits

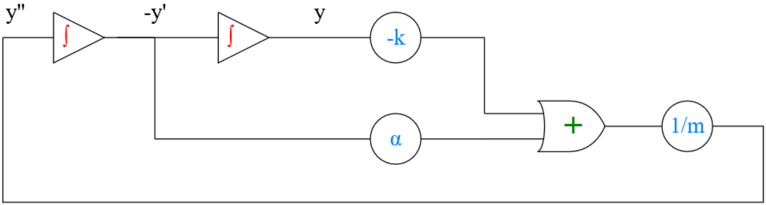


Figure 3: A damped harmonic oscillator

$$y'' = \frac{1}{m}(-ky - \alpha y')$$

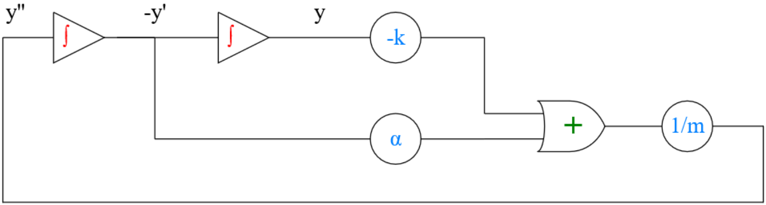


Figure 3: A damped harmonic oscillator

$$y'' = \frac{1}{m}(-ky - \alpha y')$$

- Function **generated** by a GPAC : $y' = p(y), \quad p \in \mathbb{R}[X]$

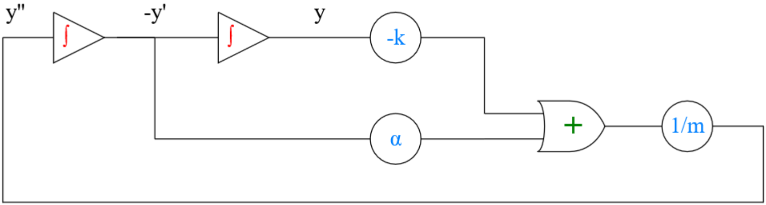


Figure 3: A damped harmonic oscillator

$$y'' = \frac{1}{m}(-ky - \alpha y')$$

- Function **generated** by a GPAC : $y' = p(y), \quad p \in \mathbb{R}[X]$
- It is rather the *trace* of the computation...

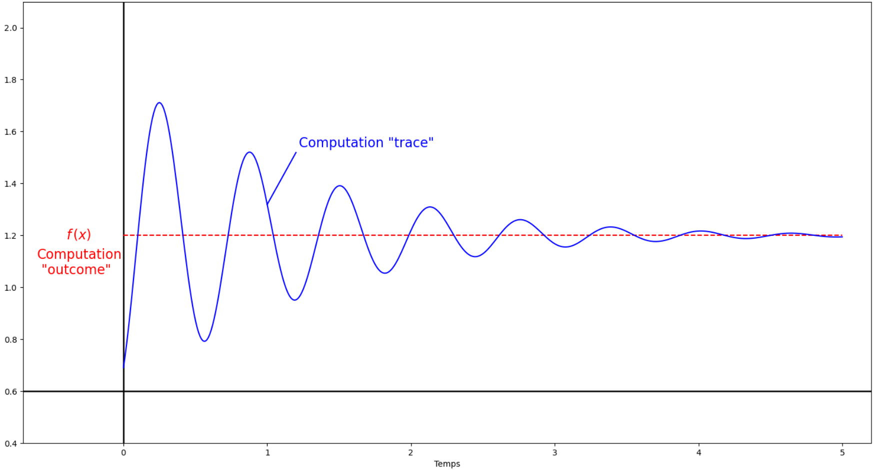


Figure 4: Computation outcome v. Computation trace

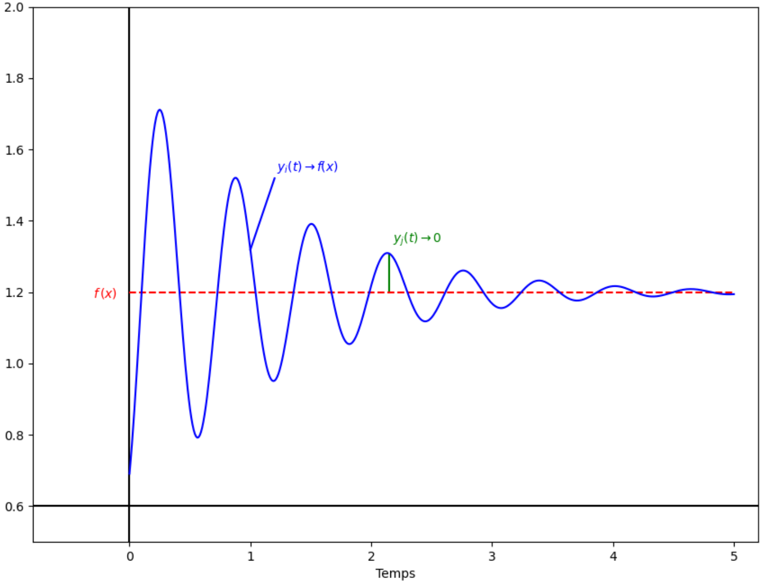
Definition

$f:[a,b]\to\mathbb{R}$ is **GPAC-computable** iff there exists $p:\mathbb{R}^{n+1}\to\mathbb{R}^n$ a polynomial, $p_0\in\mathbb{R}[X]$, $\alpha_1,\ldots,\alpha_{n-1}\in\mathbb{R}_c$ such that for $x\in[a,b]$, if $y\in\mathbb{R}^n$ is the solution of

$$Y'=p(Y,t)$$

with initial condition $Y_0=(\alpha_1,\ldots,\alpha_{n-1},p_0(x))$, we have :

$$\exists\,(i,j)\text{ such that }\begin{cases}\lim\limits_{t\to\infty} y_j(t)=0\\ |f(x)-y_i(t)|\leq y_j(t)\end{cases}$$


2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0
1
2
3
4
5
Temps
$y_i(t) \to f(x)$
$y_j(t) \to 0$
$f(x)$

Theorem ([BCGH06])

f is GPAC-computable

$$\Longleftrightarrow$$

f is computable in the sense of computable analysis

Theorem ([BCGH06])

$$f \text{ is GPAC-computable} \iff f \text{ is computable in the sense of computable analysis}$$

Proof (idea).

$\Rightarrow$ We can effectively solve polynomial systems (e.g. Euler's method)

Theorem ([BCGH06])

f is GPAC-computable

$$\Longleftrightarrow$$

f is computable in the sense of computable analysis

Proof (idea).

$\Rightarrow$ We can effectively solve polynomial systems (e.g. Euler's method)

$\Leftarrow$ We can simulate TM with polynomial systems. How can we iterate a (transition) function with such a system ?

Theorem ([BCGH06])

f is GPAC-computable

$$\Longleftrightarrow$$

f is computable in the sense of computable analysis

Proof (idea).

$\Rightarrow$ We can effectively solve polynomial systems (e.g. Euler's method)

$\Leftarrow$ We can simulate TM with polynomial systems. How can we iterate a (transition) function with such a system ?

- "Branicky's trick" ([Bra95])

$$y' = (b - y)^3 \qquad \text{"}y \leftarrow b\text{"}$$

Theorem ([BCGH06])

f is GPAC-computable

$$\Longleftrightarrow$$

f is computable in the sense of computable analysis

Proof (idea).

$\Rightarrow$ We can effectively solve polynomial systems (e.g. Euler's method)

$\Leftarrow$ We can simulate TM with polynomial systems. How can we iterate a (transition) function with such a system ?

- "Branicky's trick" ([Bra95])

$$y' = (b-y)^3 \qquad \text{"}y \leftarrow b\text{"}$$

$$\begin{cases} z_1' = (f(z_2) - z_1)^3 \phi(t) & \text{"}z_1 \leftarrow f(z_2)\text{"} \\ z_2' = (z_1 - z_2)^3 \phi(\text{-}t) & \text{"}z_2 \leftarrow z_1\text{"} \end{cases}$$

$\square$

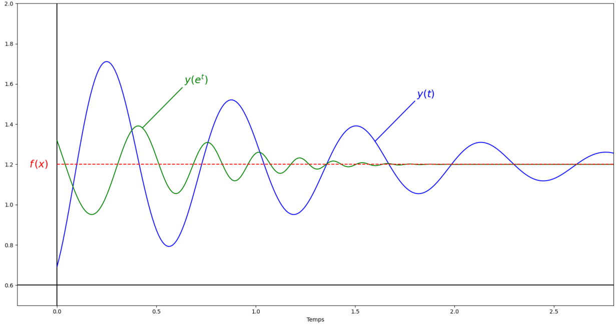
- Computability ✓

- Computability ✓
- Complexity ?

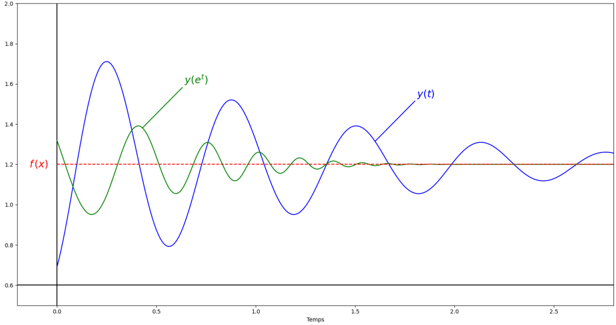
- Computability ✓
- Complexity ?
    - Computation time ?

- Computability ✓
- Complexity ?
  - Computation time ? ✗ (Arbitrary reparametrization of time, not robust)

- Computability ✓
- Complexity ?
  - Computation time ? ✗ (Arbitrary reparametrization of time, not robust)

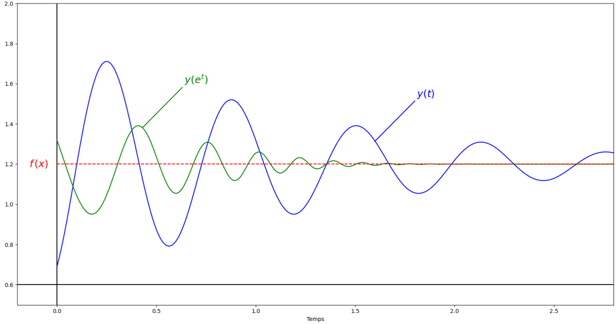


- Computability ✓
- Complexity ?
  - Computation time ? ✗ (Arbitrary reparametrization of time, not robust)



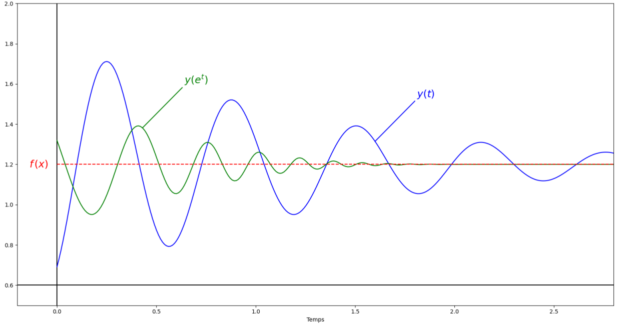
  - Curve length ? (invariant by reparametrization)

- Computability ✓
- Complexity ?
  - Computation time ? ✗ (Arbitrary reparametrization of time, not robust)



  - Curve length ? (invariant by reparametrization) ✓

- Computability ✓
- Complexity ?
  - Computation time ? ✗ (Arbitrary reparametrization of time, not robust)



  - Curve length ? (invariant by reparametrization) ✓

Theorem ([Pou15])

f is (classically) polynomial-time computable

$$\Longleftrightarrow$$

f is GPAC-computable by a GPAC of polynomial length

Another characterization with analytic functions by [Thi18]

Another characterization with analytic functions by [Thi18]

- Representation for analytic functions ?

Another characterization with analytic functions by [Thi18]

- Representation for analytic functions ?
- Coefficents alone are not enough... ✗

Another characterization with analytic functions by [Thi18]

- Representation for analytic functions ?
- Coefficents alone are not enough... ✗

Theorem ([Mü95])

In general, evaluation of a power series is not computable from its coefficients.

Another characterization with analytic functions by [Thi18]

- Representation for analytic functions ?
- Coefficents alone are not enough... ✗

Theorem ([Mü95])

In general, evaluation of a power series is not computable from its coefficients.

- We need more information

$f : [0,1] \to \mathbb{R}$ analytic.

Definition

A name for f consists of $(A, K, (a_{m,n})_{m \leq 2K, n \geq 0})$ such that :

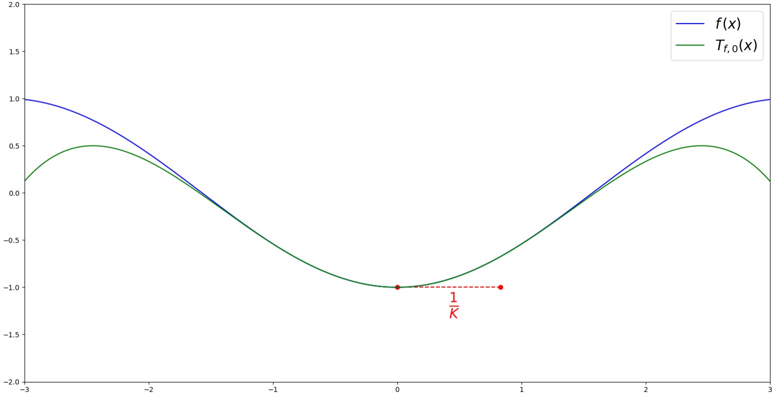
- $a_{m,n}$ is the n-th Taylor's coefficient of f around $\frac{m}{2K}$
- $|a_{m,n}| \leq AK^n$

$f : [0,1] \to \mathbb{R}$ analytic.

Definition

A name for f consists of $(A, K, (a_{m,n})_{m \leq 2K, n \geq 0})$ such that :

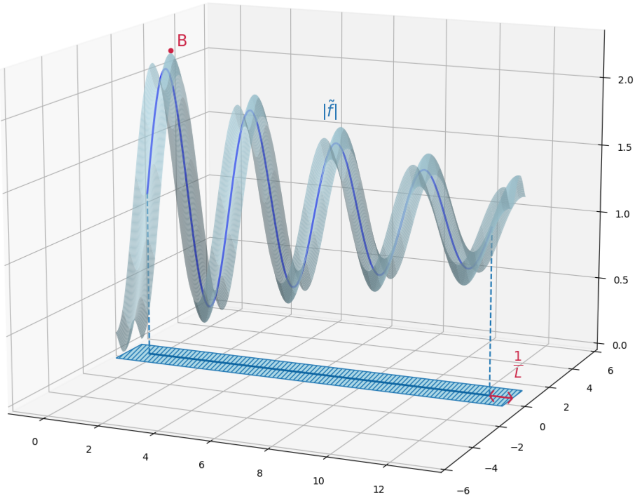
- $a_{m,n}$ is the n-th Taylor's coefficient of f around $\frac{m}{2K}$
- $|a_{m,n}| \leq AK^n$



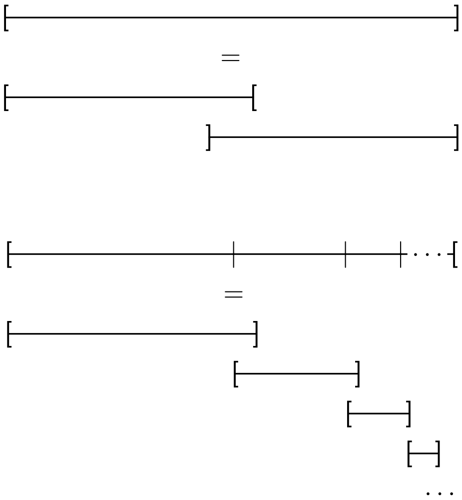
- A name gives a bound on the convergence radius and allows to bound partial sums $\rightarrow$ makes evaluation computable $\checkmark$

- A name gives a bound on the convergence radius and allows to bound partial sums $\rightarrow$ makes evaluation computable $\checkmark$
- N.B: another possibility for the name : some domain on which f admits a complex analytic extension without any pole

- A name gives a bound on the convergence radius and allows to bound partial sums $\rightarrow$ makes evaluation computable $\checkmark$
- N.B: another possibility for the name : some domain on which f admits a complex analytic extension without any pole



- More natural to talk about analytic functions on open intervals



Theorem ([Thi18])

$F : [0,1] \to \mathbb{R}$ analytic, A, K the parameters of its name.
The solution of $y' = F(y)$ (with initial condition $y_0 \in [0,1]$) can be approximated up to 2^{-n} in a time polynomial in $(n + A + K)$.

Theorem ([Thi18])

$F : [0,1] \to \mathbb{R}$ analytic, A, K the parameters of its name.
The solution of $y' = F(y)$ (with initial condition $y_0 \in [0,1]$) can be approximated up to 2^{-n} in a time polynomial in $(n + A + K)$.

- Link with [Pou15] (characterization by the GPAC) ?

Theorem ([Thi18])

$F : [0,1] \to \mathbb{R}$ analytic, A, K the parameters of its name.
The solution of $y' = F(y)$ (with initial condition $y_0 \in [0,1]$) can be approximated up to 2^{-n} in a time polynomial in $(n + A + K)$.

- Link with [Pou15] (characterization by the GPAC) ?
- Extension to **NP** ?

How can one add nondeterminism in a polynomial system ?

How can one add nondeterminism in a polynomial system ?

Lemma (Definition of NP by certificate)

$$L \in \mathbf{NP} \iff \exists L' \in \mathbf{P} \text{ such that } \forall x,$$
$$x \in L \iff \exists w, |w| \leq poly(|x|) \text{ and } (x, w) \in L'$$

Modification of Branicky's trick :

$$\begin{cases} z_1' = (f(z_2, A(t)) - z_1)^3 \phi(t) \\ z_2' = (z_1 - z_2)^3 \phi(\text{-}t) \end{cases}$$

Modification of Branicky's trick :

$$\begin{cases} z_1' = (f(z_2, A(t)) - z_1)^3 \phi(t) \\ z_2' = (z_1 - z_2)^3 \phi(\text{-}t) \end{cases}$$

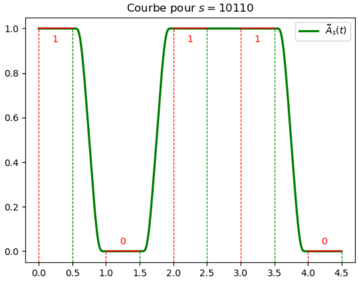


Figure 5: Ideal $A(t)$

Modification of Branicky's trick :

$$\begin{cases} z_1' = (f(z_2, A(t)) - z_1)^3 \phi(t) \\ z_2' = (z_1 - z_2)^3 \phi(\text{-}t) \end{cases}$$

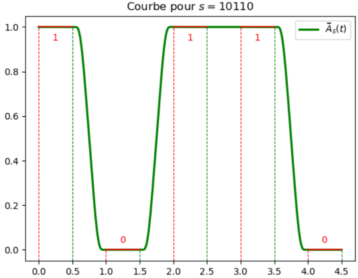


Figure 5: Ideal $A(t)$

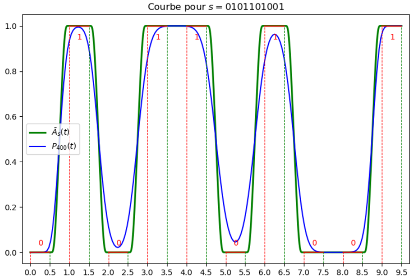


Figure 6: Analytic $A(t)$

- The certificate must be of polynomial size!

- The certificate must be of polynomial size!

Theorem

*One can explicit a polynomial whose degree and coefficients are **quadratic in T** that approximates $A(t)$ at a given precision on $[0, T]$.*

Proof.

Use Bernstein polynomials. □

- The certificate must be of polynomial size!

Theorem

One can explicit a polynomial whose degree and coefficients are ***quadratic in T*** *that approximates $A(t)$ at a given precision on $[0, T]$.*

Proof.

Use Bernstein polynomials. $\square$

- The existence of the certificate then means the existence of a polynomial in a certain class of polynomials.

Link between the two characterizations of **P** ([Pou15]/[Thi18]) ?

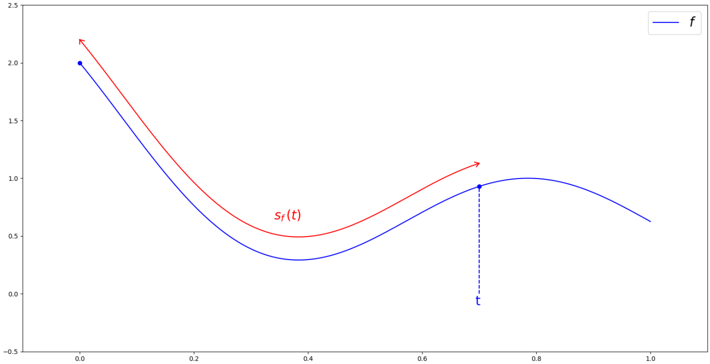
Link between the two characterizations of **P** ([Pou15]/[Thi18]) ?

Definition (*Abscisse curviligne*)

$f \in \mathcal{C}^1([0,1],\mathbb{R})$, $L = \operatorname{len}(f)$. We call *abscisse curviligne* of f:

$$\begin{array}{rccc} s_f : & [0,1] & \longrightarrow & [0,L] \\ & x & \longmapsto & \operatorname{len}_{[0,x]}(f) \end{array}$$

That is: $s_f(t) = \int_0^t \sqrt{1+f'(x)^2}\,dx$



Theorem (Link name/length of the curve)

$f : [0,1] \to \mathbb{R}$ analytic. From a name of f, one can compute a name for s_f in polynomial time (and A_{s_f}, K_{s_f} are themselves polynomial in A_f, K_f).

Theorem (Link name/length of the curve)

$f : [0,1] \to \mathbb{R}$ analytic. From a name of f, one can compute a name for s_f in polynomial time (and A_{s_f}, K_{s_f} are themselves polynomial in A_f, K_f).

- Consequence : one can compute $\mathrm{len}(f) = s_f(1)$ from a name of f, and its value is polynomial in the parameters of f.

Canonical representative of a computable function $f : [a, b] \to \mathbb{R}$?

Canonical representative of a computable function $f : [a, b] \to \mathbb{R}$?

- First attempt:

$$\frac{1}{A} f\left(\frac{x}{K}\right) \quad \text{(defined on } [aK, bK])$$

  - Computable, admits for parameters $(A', K') = (1, 1)$ ✓

Canonical representative of a computable function $f : [a, b] \to \mathbb{R}$?

- First attempt:
$$\frac{1}{A} f\left(\frac{x}{K}\right) \quad \text{(defined on } [aK, bK])$$
    - Computable, admits for parameters $(A', K') = (1, 1)$ ✓
    - $f : [a, b] \to [0, 1], x \mapsto \sin(x)$ et $g : [a/2, b/2] \to [0, 1], x \mapsto \sin(2x)$ do not have the same representative... ✗

Canonical representative of a computable function $f : [a,b] \to \mathbb{R}$?

- First attempt:

$$\frac{1}{A} f\left(\frac{x}{K}\right) \quad \text{(defined on } [aK, bK])$$

  - Computable, admits for parameters $(A', K') = (1,1)$ ✓
  - $f : [a,b] \to [0,1], x \mapsto \sin(x)$ et $g : [a/2, b/2] \to [0,1], x \mapsto \sin(2x)$ do not have the same representative... ✗

- Second attempt:

$$\frac{1}{A}(f \circ s_f^{-1})\left(\frac{x}{4K}\right) \quad \text{(defined on } [0, \mathrm{len}(f)K])$$

  - Computable, admits for prameters $(A', K') = (1,1)$ ✓

Canonical representative of a computable function $f : [a,b] \to \mathbb{R}$?

- First attempt:
$$\frac{1}{A} f\left(\frac{x}{K}\right) \quad \text{(defined on } [aK, bK])$$
  - Computable, admits for parameters $(A', K') = (1,1)$ ✓
  - $f : [a,b] \to [0,1], x \mapsto \sin(x)$ et $g : [a/2, b/2] \to [0,1], x \mapsto \sin(2x)$ do not have the same representative... ✗

- Second attempt:
$$\frac{1}{A}(f \circ s_f^{-1})\left(\frac{x}{4K}\right) \quad \text{(defined on } [0, \mathrm{len}(f)K])$$
  - Computable, admits for prameters $(A', K') = (1,1)$ ✓
  - f and g have the same representative! ✓

- State of the art :

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])
- First result :
  - Extending [Thi18] to characterize **NP**

- State of the art :
  - A characterization of **P** by polynomial differential systems ([Pou15])
  - A characterization of **P** by analytic functions ([Thi18])
- First result :
  - Extending [Thi18] to characterize **NP**
- Second result :
  - Unification of approaches via the length of the curve
  - Existence of a computable canonical representative of an analytic function

Olivier Bournez, Manuel Campagnolo, Daniel Graça, and Emmanuel Hainry.
The general purpose analog computer and computable analysis are two equivalent paradigms of analog computation.
pages 631–643, 05 2006.

Michael S. Branicky.
Universal computation and other capabilities of hybrid and continuous dynamical systems.
Theoretical Computer Science, 138(1):67–100, 1995.
Hybrid Systems.

Norbert Th. Müller.
Constructive aspects of analytic functions.
In *Proc. Workshop on Computability and Complexity in Analysis*, volume 190 of *Informatik-Berichte*, pages 105–114. FernUniversität Hagen, 1995.

Amaury Pouly.
Continuous models of computation: from computability to complexity.
PhD thesis, École Polytechnique, Universidade do Algarve, 2015.
Thèse de doctorat dirigée par Bournez, Olivier Informatique Palaiseau, Ecole polytechnique 2015.

Claude E. Shannon.
Mathematical theory of the differential analyzer.
Journal of Mathematics and Physics, 20(1-4):337–354, 1941.

Shuang Shang, Jing Liu, and Fang Hua.
Protein acylation: mechanisms, biological functions and therapeutic targets.
Signal Transduction and Targeted Therapy, 7(1):396, 2022.

Holger Thies.
Uniform computational complexity of ordinary differential equations with applications to dynamical systems and exact real arithmetic.
PhD thesis, Université de Tokyo, 2018.