Journée en l'honneur de Patrick Cegielski

Recursion theory, complexity and discrete differential equations

Arnaud Durand
joint work with Olivier Bournez

June 28, 2022

Outline

Patrick

- The mathematician

Patrick

- The mathematician

Patrick

- The mathematician

C. R. Acad. Sci. Paris, t. 315, Série I, p. 1431-1434, 1992

Informatique théorique/*Computer Science*

Indécidabilité de la théorie des entiers naturels munis d'une énumération des premiers et de la divisibilité

Patrick CEGIELSKI et Denis RICHARD

- The colleague (and political activist)

Patrick

- The mathematician
- The colleague (and political activist)
- The mentor

Patrick

- The mathematician
- The colleague (and political activist)
- The mentor

Introduction

- Implicit complexity : machine independent way to talk about complexity
- Usual means :
  - (finite) model theory
  - recursion
  - proof complexity
  - linear logic, proof theory
  - rewriting

Introduction

- In this talk: a Discrete Ordinary Differential Equations (ODE) point of view of complexity classes
- Pro: Natural way to express properties of many systems in applied science
- Pro: Very active field of maths, abundant literature
- Pro: Have widely studied discrete counterparts based on *finite differences*
- Pro: Analogy between definition by recursion and finite differences
- Cons: Is there more than an analogy?

Outline

Primitive recursive functions

Let $p \in \mathbb{N}$, $g : \mathbb{N}^p \to \mathbb{N}$ and $h : \mathbb{N}^{p+2} \to \mathbb{N}$.
The function $f = \mathrm{REC}(g, h) : \mathbb{N}^{p+1} \to \mathbb{N}$ is defined by primitive recursion from g and h if:

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(x+1, \mathbf{y}) = h(f(x, \mathbf{y}), x, \mathbf{y}) \end{cases}$$

- High complexity functions
- How to restrict the recursion scheme to lower complexity?

Bounded recursion

Let $g : \mathbb{N}^p \to \mathbb{N}$, $h : \mathbb{N}^{p+2} \to \mathbb{N}$ and $i : \mathbb{N}^{p+1} \to \mathbb{N}$.
The function $f = \mathrm{BR}(g, h) : \mathbb{N}^{p+1} \to \mathbb{N}$ is defined by bounded recursion from g, h and i if

$$\begin{aligned} f(0, \mathbf{y}) &= g(\mathbf{y}) \\ f(x+1, \mathbf{y}) &= h(f(x, \mathbf{y}), x, \mathbf{y}) \end{aligned}$$

under the condition that:

$$f(x, \mathbf{y}) \leq i(x, \mathbf{y}).$$

$O(|x|)$ "steps" to evaluate $f(x)$, control of the growth by some already known function
Key ingredient to capture elementary functions and Grzegorczyk's hierarchy

Recursion on notation (Cobham)

Consider $\mathbf{s}_0, \mathbf{s}_1 : \mathbb{N} \to \mathbb{N}$

$$\mathbf{s}_0(x) = 2 \cdot x \text{ and } \mathbf{s}_1(x) = 2 \cdot x + 1.$$

Definition

Function f defined by bounded recursion on notations, i.e. BRN, from functions g, h_0, h_1 et k when:

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(\mathbf{s}_0(x), \mathbf{y}) = h_0(x, \mathbf{y}, f(x, \mathbf{y})) \text{ for } x \neq 0 \\ f(\mathbf{s}_1(x), \mathbf{y}) = h_1(x, \mathbf{y}, f(x, \mathbf{y})) \\ f(x, \mathbf{y}) \leq k(x, \mathbf{y}) \end{cases}$$

Cobham's approach

$\mathscr{F}_P$ smallest subset of primitive recursive functions

- Containing basis functions :
  Function$\mathbf{0}$, projections p_i^k, successor functions $\mathbf{s}_0(x) = 2 \cdot x$ and $\mathbf{s}_1(x) = 2 \cdot x + 1$, "smash" function $x \sharp y = 2^{|x| \times |y|}$
- Closed by composition
- Closed by bounded recursion on notations

Cobham (62) : $\mathscr{F}_P$ is equal to $\mathbf{FP}$, the class of polynomial time computable functions

Why does it capture FP?

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(\mathbf{s}_0(x), \mathbf{y}) = h_0(x, \mathbf{y}, f(x, \mathbf{y})) \text{ for } x \neq 0 \\ f(\mathbf{s}_1(x), \mathbf{y}) = h_1(x, \mathbf{y}, f(x, \mathbf{y})) \\ f(x, \mathbf{y}) \leq k(x, \mathbf{y}) \end{cases}$$

Why does it capture FP?

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(\mathbf{s}_0(x), \mathbf{y}) = h_0(x, \mathbf{y}, f(x, \mathbf{y})) \text{ for } x \neq 0 \\ f(\mathbf{s}_1(x), \mathbf{y}) = h_1(x, \mathbf{y}, f(x, \mathbf{y})) \\ f(x, \mathbf{y}) \leq k(x, \mathbf{y}) \end{cases}$$

- f is defined from h_0, h_1 and k.
- If $|k(x, \mathbf{y})|$ is polynomial in $|x| + |y|$, then so is $|f(x, \mathbf{y})|$
- Hence, inner terms do not grow too fast!

Why does it capture FP?

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(\mathbf{s}_0(x), \mathbf{y}) = h_0(x, \mathbf{y}, f(x, \mathbf{y})) \text{ for } x \neq 0 \\ f(\mathbf{s}_1(x), \mathbf{y}) = h_1(x, \mathbf{y}, f(x, \mathbf{y})) \\ f(x, \mathbf{y}) \leq k(x, \mathbf{y}) \end{cases}$$

- $|\mathbf{s}_1(x)| = |\mathbf{s}_0(x)| = |x| + 1$
- Then the number of induction steps is in $O(|x|)$.

Going further: syntactic restriction, ramified recursion

- Cobham's work was the starting point of numerous attempts to capture complexity classes by recursion algebras
- Generalize to $\mathbf{L}, \mathrm{NC}^i, \mathrm{AC}^i$ classes
- Alternative approaches that do not require to bound the function *a priori*.
  - Predicative recursion (Bellantoni, Cook)
  - Ramified recurrence (Leivant, Leivant-Marion)
  - ....

Outline

Discrete derivative

Definition

Let $f : \mathbb{N} \to \mathbb{Z}$, the discrete derivative (a.k.a finite difference) is defined as:

$$\Delta \mathbf{f}(x) = \mathbf{f}(x+1) - \mathbf{f}(x).$$

When $f : \mathbb{N}^p \to Z^q$, set:

$$\frac{\partial \mathbf{f}(x, \mathbf{y})}{\partial x} = \mathbf{f}(x+1, \mathbf{y}) - \mathbf{f}(x, \mathbf{y})$$

.

Sometimes use $\mathbf{f}'(x)$ instead of $\Delta(\mathbf{f}(x))$

Discrete integral

Definition (Discrete Integral)

we write $\int_a^b \mathbf{f}(x)\delta x$ as a synonym for

$$\int_a^b \mathbf{f}(x)\delta x = \sum_{x=a}^{x=b-1} \mathbf{f}(x)$$

with the conventions: $\int_a^a \mathbf{f}(x)\delta x = 0$ and $\int_a^b \mathbf{f}(x)\delta x = -\int_b^a \mathbf{f}(x)\delta x$ when $a > b$.

It follows easily by the telescope formula that:

Theorem (Fundamental Theorem of Finite Calculus)

Let $\mathbf{F}(x)$ be some function. Then, $\int_a^b \mathbf{F}'(x)\delta x = \mathbf{F}(b) - \mathbf{F}(a)$.

Discrete integral and basics of integration

Not surprisingly, basic notions from the continous setting adapts easily:

- derivation of a composition (chain rule), integration by parts, etc
- Example of the Product rule:
  $(\mathbf{f}(x) \cdot \mathbf{g}(x))' = \mathbf{f}(x+1) \cdot \mathbf{g}'(x) + \mathbf{f}(x)' \cdot \mathbf{g}(x)$
- Let $\mathbf{f}$ be some function, $\mathbf{C}$ some constant. Then the function

$$\mathbf{F}(x) = \mathbf{C} + \sum_{x=0}^{x-1} \mathbf{f}(x)$$

  is such that $\mathbf{F}'(x) = \mathbf{f}(x)$ and $\mathbf{F}(0) = \mathbf{C}$. As expected, $\mathbf{F}$ is called a primitive of $\mathbf{f}(x)$.

Discrete Ordinary Differential Equation (ODE)

Discrete ODE: System of equations of the form, where h is some function:

$$\frac{\partial \mathbf{f}(x, \mathbf{y})}{\partial x} = \mathbf{h}(\mathbf{f}(x, \mathbf{y}), x, \mathbf{y}), \tag{1}$$

With initial value $\mathbf{f}(0, \mathbf{y}) = \mathbf{g}(\mathbf{y})$: Initial Value Problem (IVP) or a Cauchy Problem.

Integral form:

$$\mathbf{f}(x, \mathbf{y}) = \mathbf{f}(0, \mathbf{y}) + \int_0^x \mathbf{h}(\mathbf{f}(x, \mathbf{y}), x, \mathbf{y}) \delta x.$$

- Hence, a discrete ODE always have a solution $f : \mathbb{N}^p \to \mathbb{Z}^q$
- Not always true if one wants $f : \mathbb{Z}^p \to \mathbb{Z}^q$

Linear system of discrete ODE

Some popular kind of equation...

Linear ODE: system of the form

$$\begin{cases} \mathbf{f}'(x, \mathbf{y}) = \mathbf{A}(x, \mathbf{y}) \cdot \mathbf{f}(x, \mathbf{y}) + \mathbf{B}(x, \mathbf{y}) \\ \mathbf{f}(0, \mathbf{y}) = \mathbf{G}(\mathbf{y}) \text{ (initial conditions)} \end{cases}$$

For matrices $\mathbf{A}$ and vectors $\mathbf{B}$ and $\mathbf{G}$.

- Well known and simple kind of system
- Easy to solve in the continous setting

Linear system of discrete ODE

Easy to see that solution is of the form:

$$\mathbf{f}(x,\mathbf{y}) = \left(\overline{2}^{\int_0^x \mathbf{A}(t,\mathbf{y})\delta t}\right)\cdot\mathbf{G}(\mathbf{y}) + \int_0^x \left(\overline{2}^{\int_{u+1}^x \mathbf{A}(t,\mathbf{y})\delta t}\right)\cdot\mathbf{B}(u,\mathbf{y})\delta u.$$

Or, alternatively:

$$\mathbf{f}(x,\mathbf{y}) = \sum_{u=-1}^{x-1}\left(\prod_{t=u+1}^{x-1}(1+\mathbf{A}(t,\mathbf{y}))\right)\cdot\mathbf{B}(u,\mathbf{y})$$

with the conventions that $\prod_x^{x-1}\kappa(x) = 1$ and $\mathbf{B}(-1,\mathbf{y}) = \mathbf{G}(\mathbf{y})$
Computational content is clear: the solution can be computed

Examples of linear ODE: bounded sum and product

Arithmetic is used freely below.
Let $g : \mathbb{N}^{p+1} \to \mathbb{N}$,

- Let $f(x, \mathbf{y}) = \sum_{z<x} g(z, \mathbf{y})$ for $x \neq 0$, and 0 for $x = 0$.
  Function f is the unique solution of :

$$\begin{cases} \frac{\partial f(x,\mathbf{y})}{\partial x} = g(x, \mathbf{y}) \\ f(0, \mathbf{y}) = 0 \end{cases}$$

- Let $f(x, \mathbf{y}) = \prod_{z<x} g(z, \mathbf{y})$ for $x \neq 0$, and 1 for $x = 0$.
  Function f is the unique solution of :

$$\begin{cases} \frac{\partial f(x,\mathbf{y})}{\partial x} = f(x, \mathbf{y}) \cdot (g(x, \mathbf{y}) - 1) \\ f(0, \mathbf{y}) = 1 \end{cases}$$

Outline

Back to primitive recursion

One can obviously rewrite p.r. schemas using discrete ODE
Main part :

$$\begin{cases} f(0,\mathbf{y}) = & g(\mathbf{y}) \\ f(x+1,\mathbf{y}) = & h(f(x,\mathbf{y}),x,\mathbf{y}) \\ = & f(x,\mathbf{y}) + (-f(x,\mathbf{y}) + h(f(x,\mathbf{y}),x,\mathbf{y})) \end{cases}$$

Hence, setting $h_0(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y}) = -f(x,\mathbf{y}) + h(f(x,\mathbf{y}),x,\mathbf{y})$,
$\mathbf{f}(x,\mathbf{y})$ is solution of

$$\frac{\partial \mathbf{f}(x,\mathbf{y})}{\partial x} = h_0(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y})$$

So easy. This is just rephrasing...

Recursion on notation (Cobham)

What about complexity classes? Recall Cobham:

$$\begin{cases} f(0, \mathbf{y}) = g(\mathbf{y}) \\ f(\mathbf{s}_0(x), \mathbf{y}) = h_0(x, \mathbf{y}, f(x, \mathbf{y})) \text{ for } x \neq 0 \\ f(\mathbf{s}_1(x), \mathbf{y}) = h_1(x, \mathbf{y}, f(x, \mathbf{y})) \\ f(x, \mathbf{y}) \leq k(x, \mathbf{y}) \end{cases}$$

- Two successors do not fit well with a derivation approach
- bounding by function k is not very natural either

Objective: get rid of these two features and replace them by more ODE friendly restrictions

Derivation along a function

Given function $\mathcal{L}$, consider the equation:

$$\mathbf{f}(x+1,\mathbf{y}) = \mathbf{f}(x,\mathbf{y}) + (\mathcal{L}(x+1,\mathbf{y}) - \mathcal{L}(x,\mathbf{y})) \cdot \mathbf{h}(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y})$$

The value of f changes only when the value of $\mathcal{L}$ changes.

Consequence: only as many values to consider to compute $f(x,\mathbf{y})$ as the number of times $\mathcal{L}(t,\mathbf{y})$ changes between $t=0$ and $t=x$...

Application: if $\mathcal{L}(x,\mathbf{y})$ is the logarithm function $\ell(x)$ then only a logarithmic in x number of values

Derivation along a function

$\mathbf{f}(x+1,\mathbf{y}) = \mathbf{f}(x,\mathbf{y}) + (\mathcal{L}(x+1,\mathbf{y}) - \mathcal{L}(x,\mathbf{y})) \cdot \mathbf{h}(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y})$
means :

$$\frac{\partial \mathbf{f}(x,\mathbf{y})}{\partial x} = \frac{\partial \mathcal{L}(x,\mathbf{y})}{\partial x} \cdot \mathbf{h}(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y})$$

Definition ($\mathcal{L}$-ODE)

Let $\mathcal{L} : \mathbb{N}^{p+1} \to \mathbb{Z}$. The open equation will be written as:

$$\frac{\partial \mathbf{f}(x,\mathbf{y})}{\partial \mathcal{L}} = \frac{\partial \mathbf{f}(x,\mathbf{y})}{\partial x} \frac{\partial x}{\partial \mathcal{L}(x,\mathbf{y})} = \mathbf{h}(\mathbf{f}(x,\mathbf{y}),x,\mathbf{y}) \qquad (2)$$

Inspired by the classical formula:

$$\frac{\delta f(x,\mathbf{y})}{\delta x} = \frac{\delta f(x,\mathbf{y})}{\delta \mathcal{L}(x,\mathbf{y})} \cdot \frac{\delta \mathcal{L}(x,\mathbf{y})}{\delta x}.$$

Discrete $\ell()$-ODE schemas

What about the smallest classes of functions

- that contains $\mathbf{0}$, $\mathbf{1}$, projections π_i^p, the length $\ell(x)$, functions $x+y$, $x-y$, $x \times y$, the sign function $\mathrm{sg}(x)$
- that is closed under composition and $\ell()$-ODE schemata.
- Good: the number of step to compute the solution of a $\ell()$-ODE is bounded linearly in the length of x
- Bad: It is easily seen that the solution of

$$\frac{\partial f(x)}{\partial \ell(x)} = f(x) \cdot (f(x) - 1) \tag{3}$$

  is a fast growing function (output is exponential in size)

So we know how to control the number of steps but not the size of objects

Back to linear systems

Linear ODE: system of the form

$$\begin{cases} \mathbf{f}'(x, \mathbf{y}) = \mathbf{A}(x, \mathbf{y}) \cdot \mathbf{f}(x, \mathbf{y}) + \mathbf{B}(x, \mathbf{y}) \\ \mathbf{f}(0, \mathbf{y}) = \mathbf{G}(\mathbf{y}) \text{ (initial conditions)} \end{cases}$$

For matrices $\mathbf{A}$ and vectors $\mathbf{B}$ and $\mathbf{G}$. Recall that:

$$\mathbf{f}(x, \mathbf{y}) = \sum_{u=-1}^{x-1} \left(\prod_{t=u+1}^{x-1} (1 + \mathbf{A}(t, \mathbf{y})) \right) \cdot \mathbf{B}(u, \mathbf{y})$$

Using convention: $\prod_{x}^{x-1} \kappa(x) = 1$ and $\mathbf{B}(-1, \mathbf{y}) = \mathbf{G}(\mathbf{y})$

Linear system alone are also too powerful.... But if one reduces the number of steps drastically then the size of the output may become controlable

Towards capturing FP

- Idea: combine linearity and derivation along some particular function $\mathcal{L}$ i.e. systems :

$$\frac{\partial \mathbf{f}(x, \mathbf{y})}{\partial \mathcal{L}} = \mathbf{h}(\mathbf{f}(x, \mathbf{y}), x, \mathbf{y}), \tag{4}$$

  where
  - h is "linear"
  - $\mathcal{L}$ has a polylogarithmic number of values (such has the $\ell()$ function)

$\mathbb{DL}$

Definition ($\mathbb{DL}$)

Let $\mathbb{DL}$ be the smallest subset of functions,

- that contains $\mathbf{0}$, $\mathbf{1}$, projections π_i^p, the length $\ell(x)$, functions $x+y$, $x-y$, $x \times y$, the sign function $\mathrm{sg}(x)$
- closed under composition (when defined) and linear length-ODE scheme:

$$\frac{\partial \mathbf{f}(x, \mathbf{y})}{\partial \ell} = \mathbf{u}(\mathbf{f}(x, \mathbf{y}), x, \mathbf{y}) \quad \text{and } \mathbf{f}(0, \mathbf{y}) = \mathbf{g}(\mathbf{y})$$

where $\mathbf{u}$ is *essentially linear* in $\mathbf{f}(x, \mathbf{y})$.

A characterization of FP

Theorem

$\mathbb{DL} = \mathbf{FP}$

Proof of ($\subseteq$): Roughly speaking

- The derivation along $\ell(x)$ (or any $\mathcal{L}$ with polylog "jumps") permits to control the number of steps
- Linearity of the system permits to control the size of the output

Proof of ($\supseteq$): By a direct expression of a polynomial computation of a register machine.

Conclusion, questions and work in progress

- Short tour on the expressive and computational power of discrete ODE
- Appears
  - to be a convenient tool for algorithm design
  - to elegantly capture complexity notions
- Extend the work to other classes (**FPSPACE**, $\mathbf{NP}$, circuit classes)
- Smaller derivation steps and allowing errors
- Generalize to the continuous setting