Bounded Arithmetic and ODE

Rui Li

June 20, 2025

Contents

Polynomial-time computation

Polynomial Hierarchy

Decision problems:

$$
\begin{aligned}
\Sigma_0^p &:= \mathsf{P} \\
\Sigma_1^p &:= \mathsf{NP} \\
\Sigma_{i+1}^p &:= \mathsf{NP}^{\Sigma_i^b}
\end{aligned}
$$

Functional classes:

$$
\square_{i+1}^p := \mathsf{FP}^{\Sigma_i^b}
$$

Cobham

Definition

f is said to be definable using bounded recursion on notation (BRN) from h, g_0, g_1 with the bound k if

$$\begin{array}{rcl} f(0,y) & = & g(y) \\ f(s_0(x),y) & = & g_0(x,y,f(x,y)) \\ f(s_1(x),y) & = & g_1(x,y,f(x,y)) \\ f(x,y) & < & k(x,y) \end{array}$$

where $s_0(x) = 2x$ and $s_1(x) = 2x+1$.

Fact

$$\text{FP} \quad = \quad [\ 0, s_0, s_1, \#, \text{comp}, \text{BRN}\ ]$$

Functional algebra of polynomial hierarchy

Definition

f is defined by bounded minimization (BMIN) from g if

$$f(x,y) \quad = \quad \mu i < x[g(i,y) = 0]$$

- $\square_i^p$:

$$[\ 0, S, +, \times, \#, \text{comp}, \text{BRN}, \text{BMIN} : \text{rk}(\text{BMIN}) < i\ ]$$

- PH:

$$[\ 0, S, +, \times, \#, \text{comp}, \text{BRN}, \text{BMIN}\ ]$$

Language of bounded arithmetic

Language:

$$0, S, +, \times, \#$$

Bounded arithmetical hierarchy:

- $\Sigma_0^b = \Pi_0^b = \Delta_0^b$: Boolean combination of atomic formulas:
- $\Sigma_{i+1}^b := \exists x \leq t\, \Pi_0^b$
  $\Pi_{i+1}^b := \exists x \leq t\, \Sigma_0^b$
- $\exists x \leq |t|$ and $\forall x \leq |t|$ do not change the logical complexity

Bounded arithmetic I

Definition (S^i_2)

- BASIC;
- Σ^b_i-*PIND:*

$$\frac{\Gamma, \phi(\lfloor \frac{x}{2} \rfloor) \ \vdash \ \Delta, \phi(x)}{\Gamma, \phi(0) \ \vdash \ \Delta, \phi(t)}$$

Lemma

$$f \in \square^p_i \quad \Leftrightarrow \quad S^i_2 \vdash \text{“}f \textit{ is total”}$$

Discrete ordinary differential equations

Discrete linear ODE I

Definition (Discrete ODE)

$$
\begin{aligned}
f(0,y) &= g(y) \\
\frac{\partial\ f(x,y)}{\partial\ l(x)} &= f(2x,y) - f(x,y)
\end{aligned}
$$

Discrete linear ODE II

Definition (L-ODE)

$$\frac{\partial f}{\partial l}(x,y) \quad = \quad \alpha(x,y) \times f(x,y) + \beta(x,y)$$

Lemma

$$\mathsf{FP} \quad = \quad [\, \mathsf{BASIC}, \mathsf{comp}, \mathsf{sign}, L\text{-}\mathit{ODE} \,]$$

Discrete linear ODE III

FP $\supseteq$ [BASIC, COMP, sign, L-ODE]:

- Let p be the polynomial bounding the computation time of α;
- Compute $\hat{f}$:

$$x \mapsto \langle f(0), f(\lfloor \frac{x}{2^{|x|}} \rfloor), f(\lfloor \frac{x}{2^{|x|-1}} \rfloor), \ldots, f(\lfloor \frac{x}{2} \rfloor), f(x) \rangle$$

- Its computational time is bounded by q s.t.

$$q(x) + p(x) \leq q(2x)$$

- So $f \in$ FP.

Discrete linear ODE IV

$\mathrm{FP} \subseteq [\,\mathrm{BASIC}, \mathrm{COMP}, \mathrm{sign}, L\text{-ODE}\,]$:

- Represent every FP function on a model of computation (RAM);
- Represent the transition of machine states using ODE:

$$\frac{\partial f}{\partial l}(t, x) \quad = \quad \sum_{l} \mathrm{next}_l \times \bar{\mathrm{sg}}(f(t, x) - l) \times (\prod_{i}(\mathrm{sg}(f(t, x) - i)))$$

Proof: FP $\subseteq L$-ODE I

- Let $q_i(x)$ be the state of $M_f(x)$ at i-th step. Define

$$f_0(x,t) \quad := \quad \langle q_0(x), \ldots, q_{|t|}(x)\rangle$$

- Let p be polynomial bounding the computation time of $M_f(x)$, then the following operation is polynomial:

$$f(x) \quad \mapsto \quad f_0(x, 10^{p(|x|)})$$

- Define f_0 using L-ODE:

$$\langle q_0(x), \ldots, q_{|t|}(x), q_{|t|+1}(x)\rangle \quad = \quad \alpha(x,t) \times \langle q_0(x), \ldots, q_{|t|}(x)\rangle + \beta(x,t)$$

Proof: FP $\subseteq L$-ODE II

How to define α and β:

- Let last configuration of $f_0(x,t)$ be

$$q_{|t|}(x) \quad = \quad \langle s, w, i\rangle(x, |t|)$$

- Assume the last configuration of $f_0(x, 2t)$ can be defined by the following cases:

$$\langle s, w, i\rangle(x, |t|+1) \quad = \quad \begin{cases} q_a & \text{if } s(x,|t|) = s_a \\ q_b & \text{if } s(x,|t|) = s_b \end{cases}$$

- Then it can be represented by the following L-ODE:

$$\begin{aligned} & \langle q_0(x), \ldots, q_{|t|}(x), q_{|t|+1}(x)\rangle \\ = \; & [(s(x,|t|) =_? s_a] \times (\langle q_0(x), \ldots, q_{|t|}(x)\rangle \times 10^{|q_a|} + q_a) \\ & + [(s(x,|t|) =_? s_b] \times (\langle q_0(x), \ldots, q_{|t|}(x)\rangle \times 10^{|q_b|} + q_b) \end{aligned}$$

A more concise proof: FP $\subseteq$ L-ODE I

- Define

$$\hat{f}(x,y) \quad := \quad \begin{cases} \text{the first } p(|y|)\text{-many bits of } f(x) & \text{if } |y| \le |f(x)| \\ f(x) & \text{otherwise} \end{cases}$$

- $\hat{f}(x,2y)$ concatenates the $p(|y|)+1,\dots,p(|y|+1)$-th bits of $f(x)$ to $\hat{f}(x,y)$:

$$\hat{f}(x,2y) \quad = \quad \hat{f}(x,y)@\langle b_{p(|y|)+1},\dots,b_{p(|y|+1)}\rangle$$

- We obtain α and β:

$$\begin{aligned} \alpha(x,y) &= 10^{p(|y|+1)-p(|y|)} \\ \beta(x,y) &= \langle b_{p(|y|)+1}(x),\dots,b_{p(|y|+1)(x)}\rangle \end{aligned}$$

A more concise proof: FP $\subseteq$ L-ODE II

Are α and β always in FP?

- $\alpha(x, y) :=$ the number of additional bits

$$y \quad \mapsto \quad \begin{cases} p(|y|+1) - p(|y|) & \text{if } p(|y|+1) \leq |f(x)| \\ |f(x)| - p(|y|) & \text{if } p(|y|) \leq |f(x)| < p(|y|+1) \\ 0 & \text{otherwise} \end{cases}$$

- $\beta(x, y) :=$ the operation of computing the i-th of the additional bits

$$(x, i) \quad \mapsto \quad b_i(x)$$

Another ODE I

Definition (t-ODE)

$$f(t(x), y) \quad = \quad \alpha(x, y) \times f(x, y) + \beta(x, y)$$

where t can be a (multi)-function satisfying:

- $t(x) \geq 2x$;
- t *is left-invertible:* $t^{-1} \circ t =$ *id;*
- $t, t^{-1} \in$ FP.

Another ODE II

Lemma

Fix a multi-function t in FP*. Then every function f in* $\mathsf{FP}^{\mathsf{NP}}$ *can be represented using t-ODE with*

$$f(t(x), y) \quad =_{\max} \quad \alpha(x, y) \times f(x, y) + \beta(x, y)$$

where $\alpha, \beta \in \mathsf{FP}^{\mathsf{NP}}$.

Bounded arithmetic and witnessing functions

Bounded arithmetic I

Lemma

Let f be expressed as a Σ_i^b-formula ϕ_f.
Then, f is in $\square_i^p$ iff $S_2^i \vdash \forall x \, \exists y \, \phi_f(x, y)$.

Difficult direction: if f is provably total in S_2^1, then $f \in \mathrm{FP}$.

Easy direction: if $f \in \mathrm{FP}$, then f is provably total in S_2^1.

Bounded arithmetic II

- The following are Δ_1^b predicates:
  - $\mathsf{Seq}(w)$: w is a sequence;
  - $l(w) = x$: the length of w is x;
  - $w(i) = x$: x is the i-th element of w is x if $i \le l(w)$, otherwise $x = 0$;
- Then, we can express that w is computation of the TM M_f on input x:

$$\mathsf{Comp}_f(w, x)$$

- The totality of f can then be expressed as:

$$\forall x \, \exists w \, \mathsf{Comp}_f(w, x)$$

- It can be proved by Σ_1^b-PIND because w is bounded:

$$w \;\le\; \max(w)\#l(w)$$

Polynomial Hierarchy and ODE

ODE characterization of $\mathrm{FP}^{\mathrm{NP}}$ I

Definition (h-ODE)

Fix a multi-function h. Then, f is defined from α and β via h-ODE:

$$f(h(x), y) \quad =_{\max} \quad \alpha(x, y) \times f(x, y) + \beta(x, y)$$

Lemma

Every function in $\mathrm{FP}^{\mathrm{NP}}$ *can be represented by* FP-*ODE.*

ODE characterization of $\square_i^p$ I

Lemma

$$\square_{i+1}^p \quad = \quad [\ \square_i^p, \text{comp}, \square_i^p\text{-}\mathit{ODE}\ ]$$

- Define the theory

$$S_2^1(\bar{f}) := S_2^1 + \text{“}f \text{ is total”}$$

  where every f is a function definable by $\square_i^p$-ODE using with $g_1, g_2 \in \square_i^p$:

$$f(h(x)) \quad = \quad g_1(x) \times f(x) + g_2(x)$$

- Show that $S_2^1(\bar{f})$ is a conservative extension of S_2^{i+1}.

ODE characterization of $\square_i^p$ II

- Suppose $S_2^1(\bar{f})$ proves

$$\Gamma \vdash \Delta$$

- Let f be the function satisfying

$$\mathsf{Wit}^{i+1}_{\bigwedge \Gamma}(w, x) \;\rightarrow\; \mathsf{Wit}^{i+1}_{\bigvee \Delta}(f(w, x), x)$$

- Let h be provably total in $\square_i^p$ and α, β be provably total in $\square_{i+1}^p$. Then, f can be defined as

$$f(h(x)) \quad = \quad \alpha(x) \times f(x) + \beta(x)$$

From induction scheme to ODE

Objectives

ODE $\longleftrightarrow$ Bounded theories

$$\frac{\partial f}{\partial |h|}(x) = F(x, f(x)) \quad \longleftrightarrow \quad \Sigma_j^b \vdash \forall \Sigma_i^b$$

ODE $\leftarrow$ Bounded theories I

$j < i$:

- $S_2^{i-1} \vdash \forall\Sigma_i^b \quad \Rightarrow \quad \Box_i^p[\mathsf{wit}, O(\log)]$;
- $S_2^{i-2} \vdash \forall\Sigma_i^b \quad \Rightarrow \quad \Box_i^p[\mathsf{wit}, O(1)]$.

ODE $\leftarrow$ Bounded theories II

$j > i$:

- $S_2^{i+1} \vdash \forall\Sigma_i^b \quad \Rightarrow$ the projection of PLS$^{\Sigma_i^p}$ functions:

  E.g., suppose ϕ is Σ_1^b and S_2^2-provably total, then there exists PLS problem (F, N, C) s.t.

  $$S_2^2 \vdash \forall x\, \forall y\, (\forall z\, N(x,z) \wedge F(x,z) \rightarrow C(x,z) \leq C(y,z)) \rightarrow \mathsf{Wit}_\phi(x,y)$$

- The $S_2^j \vdash \forall\Sigma_i^b$ where $j > i+1$ is more complicated...

ODE $\rightarrow$ Bounded theories

?

Reference

- Bournez, Durand, *A characterization of functions over the integers computable in polynomial time using discrete differential equations*.
- Buss, *The witness function method and provably recursive functions of Peano arithmetic*.
- Krajicek, *Bounded arithmetic, propositional proofs and complexity theory*.
- Kentel, *The complexity of optimization problems*.
- Clote, Kranakis, *Boolean Functions and Computation Models*.