Modèles de calcul

Xavier Urbain

2023-2024

Motivations

TIME magazine, avril 1984, citant un éditeur de magazine sur le logiciel :

« *Put the right kind of software into a computer, and it will do whatever you want it to. There may be limits on what you can do with the machines themselves, but there are no limits on what you can do with software.* »

Motivations

Quelques définitions. . .

Quelques paradoxes :

- Zénon — infini ?
- Russel, Berry — existence ?

Proposition finitisme :

- Nombre fini d'objets,
- Nombre fini de règles de construction

$\rightsquigarrow \mathbb{R}$? . . . échec

Motivations

Quelques définitions. . .

Quelques paradoxes :

- Zénon — infini ?
- Russel, Berry — existence ?

Proposition formalisme :

- finitisme
- + constructions telles que
  - Théorie obtenue cohérente — Pas d'obtention de φ et $\neg\varphi$

$\rightsquigarrow$ Programme de Hilbert (fondation des mathématiques) On veut arithmétique non contradictoire + « vrai = prouvable » $\rightsquigarrow$ échec

Motivations

Procédure effective : texte fini sur alphabet fini indiquant sans ambiguïté les actions mécaniques à effectuer — sans réfléchir ni comprendre

Calculabilité :

- Preuve ?
- Calcul ?
- Construction ?

Déf. du mécanisme d'une preuve. . .

Pas tout faire ! ex : $\mathbb{N} \to \{0, 1\}$

Motivations

Amusons-nous :

$$\mathcal{B}(n) = \max\{[\mathrm{p}()] \mid \mathrm{p} \in \mathcal{L}, |\mathrm{p}| \le n\}$$

($\mathcal{B}(1)$ en ocaml ?)

```
let b = (* code de ℬ, de taille 𝒯 *)

let c =
    let b = ··· in
    (b (5 * 𝒯)) + 1
```


Motivations

Trois grands modèles :

- Machines de Turing (Turing 36, Post 36)
- Fonctions récursives (Gödel 31, Kleene ~40, Ackermann ~40)
- λ-calcul (Church ~30)
  $\rightsquigarrow$ λ-calculs typés (Church ~40. . .)

Machines de Turing

Alan Mathison Turing (1912–1954)

MT : automate + ruban (lect./écr.)

Machine de Turing $\mathscr{M}$: $(V, \mathbb{B}, Q, q_0, F, T)$

- V vocabulaire de $\mathscr{M}$
- $\mathbb{B} \in V$ caractère blanc
- Q états de $\mathscr{M}$
- $F \subseteq Q$ états finals
- $q_0 \in Q$ état initial
- $T : Q \times V \to V \times \{\triangleleft, \triangledown, \triangleright\} \times Q$

Bande (ruban) : séquence infinie de symboles de V dont nombre fini $\neq \mathbb{B}$

Configuration : état + valeurs de bande + position de tête (w_1, q, w_2)

Bande : $\ldots \mathbb{B} w_1 w_2 \mathbb{B} \ldots$ Tête sur premier caractère de w_2

Machines de Turing — exécution

Exécution sur u $\rightsquigarrow$ Configuration de départ : (ϵ, q_0, u)

Sur $(v, q, \alpha w)$ (évt $\alpha = \mathbb{B}$ et $w = \epsilon$)

- Si $T(q,\alpha) = (\beta, \triangleright, q')$ alors $(v\beta, q', w)$
- Si $T(q,\alpha) = (\beta, \triangledown, q')$ alors $(v, q', \beta w)$
- Si $T(q,\alpha) = (\beta, \triangleleft, q')$ alors :
  - Si $v = v_1\gamma$ alors $(v_1, q', \gamma\beta w)$
  - Si $v = \epsilon$ alors $(\epsilon, q', \mathbb{B}\beta w)$
- Si $T(q,\alpha)$ indéfini : arrêt

C_1 à C_2 en un pas : $C_1 \to_{\mathscr{M}} C_2$ Arrêt sur C : $C \to_{\mathscr{M}} \perp$

Machines de Turing — langage

Pour $V_t \subset V$ (sans $\mathbb{B}$),

$\mathcal{L}_{V_t}(\mathscr{M}) = \{w \in V_t^\star \mid (\epsilon, q_0, w) \to^\star_{\mathscr{M}} (u, q, v) \to_{\mathscr{M}} \perp, \quad q \in F\}$

q_0	$\mathbb{B}$	$1 \triangleright q_1$
	1	$1 \triangleright \perp$
q_1	$\mathbb{B}$	$\mathbb{B} \triangleright q_2$
	1	$1 \triangleright q_1$
q_2	$\mathbb{B}$	$1 \triangleleft q_2$
	1	$1 \triangleleft q_0$

Machines de Turing — langage

Pour $V_t \subset V$ (sans $\mathbb{B}$),

$\mathcal{L}_{V_t}(\mathscr{M}) = \{w \in V_t^\star \mid (\epsilon, q_0, w) \to^\star_{\mathscr{M}} (u, q, v) \to_{\mathscr{M}} \perp, \quad q \in F\}$

$$\mathscr{M} = (\overbrace{\{a,b\}}^{V_t} \cup \{X\}, \mathbb{B}, Q = \{q_0, \ldots, q_f\}, q_0, F = \{q_f\}, T)$$

$T =$

q_0	$\mathbb{B}$	$\mathbb{B} \triangledown q_f$
	a	$a \triangleright q_1$
q_1	a	$a \triangleright q_1$
	b	$X \triangleleft q_2$
q_2	a	$X \triangleright q_3$
	X	$X \triangleleft q_2$

q_3	X	$X \triangleright q_3$
	b	$X \triangleleft q_2$
	$\mathbb{B}$	$\mathbb{B} \triangleleft q_4$
q_4	X	$X \triangleleft q_4$
	$\mathbb{B}$	$\mathbb{B} \triangledown q_f$

Machines de Turing — langage

Pour $V_t \subset V$ (sans $\mathbb{B}$),

$\mathcal{L}_{V_t}(\mathscr{M}) = \{w \in V_t^\star \mid (\epsilon, q_0, w) \to^\star_{\mathscr{M}} (u, q, v) \to_{\mathscr{M}} \perp, \quad q \in F\}$

q_0	$\mathbb{B}$	$1 \triangleright q_1$
	1	$1 \triangleleft q_2$
q_1	$\mathbb{B}$	$1 \triangleright q_2$
	1	$1 \triangleright q_1$

q_2	$\mathbb{B}$	$1 \triangleright q_3$
	1	$\mathbb{B} \triangleleft q_4$
q_3	$\mathbb{B}$	$1 \triangleleft q_0$
	1	$1 \triangleleft q_3$
q_4	$\mathbb{B}$	$1 \triangleright \perp$
	1	$\mathbb{B} \triangleleft q_0$

47176870 étapes, 1 : 4098, B : 8191

Machines de Turing — décision

$w \in L?$ donnée : w, question : caract. de L

Problème de décision :

- Décidable si $\exists \mathscr{M}$ t.q.arrêt en temps fini $\forall w$ et sur acceptant ssi $w \in L$
- Semi-décidable si $\exists \mathscr{M}$ t.q. arrêt en temps fini et acceptant si $w \in L$
  non acceptant ou pas d'arrêt si $w \notin L$
- Co-semi-décidable si décision pour $\overline{L}$ semi-décidable

$\in L?$ décidable $\leadsto$ L récursif (réc.)

$\in L?$ semi-décidable $\leadsto$ L récursivement énumérable (r.é.)

$\leadsto$ L r.é. tel que $\exists \mathscr{M}$ reconnaissant L et s'arrêtant toujours : réc.

- $\exists?$ programme (une MT) pour répondre à : $w, L \mapsto w \in L?$
- $\exists? L$ récursif ? $\exists? L$ r.é. non réc. ? $\exists? L$ non r.é. ?

Machines de Turing — fonction

Reconnaître, ok... mais avec quelque-chose sur la bande ?

Pour $V_1 \subset V$ et $V_2 \subset V$, sans $\mathbb{B}$, fonction $f : V_1^\star \to V_2^\star$ calculée par $\mathscr{M}$: pour $w \in V_1^\star$

- Arrêt : $(\epsilon, q_0, w) \to^\star_{\mathscr{M}} (w_1, q, u\alpha v) \to_{\mathscr{M}} \perp$, $u \in V_2^\star$, $\alpha \notin V_2$ $\quad f(w) = u$
- Pas d'arrêt sur w : $f(w)$ non défini

Passage à n arguments ? $f(w_1, \ldots, w_n) \leadsto (\epsilon, q_0, w_1\mathbb{B}w_2\mathbb{B}\ldots\mathbb{B}w_n) \to \cdots$

f Turing calculable si $\mathscr{M}$ calcule f

Machines de Turing — fonction

Exemple : multiplication par 2 dans $\mathbb{N}$ (modulo abus de notation)

$T =$

q_0	$x \in [0\cdots9]$	$x \triangleright q_0$
	$\mathbb{B}$	$\mathbb{B} \triangleleft q_{pr}$
q_{pr}	$x \in [0\cdots4]$	$[\![2x]\!] \triangleleft q_{pr}$
	$x \in [5\cdots9]$	$[\![2x-10]\!] \triangleleft q_r$
q_r	$x \in [0\cdots4]$	$[\![2x+1]\!] \triangleleft q_{pr}$
	$x \in [5\cdots9]$	$[\![2x-9]\!] \triangleleft q_r$
	$\mathbb{B}$	$1 \triangleleft q_\perp$

Et hop on vérifie que ça marche pour $7035\ldots$

Machines de Turing — thèse de Church

Procédure effective : texte fini sur alphabet fini indiquant sans ambiguïté les actions mécaniques à effectuer sans réfléchir ni comprendre

« Thèse » de Church : fonctions calculables = Turing calculables