4. Incalculabilité – diagonalisation

Bruno Grenet

Université Grenoble Alpes – IM²AG
L3 Informatique
UE Modèles de calcul – Machines de Turing

https://membres-ljk.imag.fr/Bruno.Grenet/MCAL-MT.html

Introduction

Thèse de Church-Turing

Tout ce qui est *calculable* est calculable par machine de Turing

Rappels

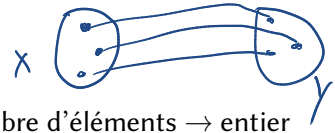
- Une fonction f est calculable si $f = f_{\mathcal{M}}$ pour une machine de Turing $\mathcal{M}$
- Un langage L est reconnaissable si $L = L(\mathcal{M})$ pour une machine de Turing $\mathcal{M}$
  décidable si χ_L est calculable

- Il existe des fonctions *incalculables* ? des langages *irreconnaissables* ? *indécidables* ?
- Qu'est-ce que ça veut dire ?

Table des matières

Table des matières

Cardinal d'un ensemble



Définition intuitive

- Le *cardinal* d'un ensemble fini est son nombre d'éléments $\rightarrow$ entier

Qu'est-ce que le cardinal d'un ensemble infini ?

L'outil de base : la bijection

- Bijection entre X et Y : à chaque $x \in X$ correspond un *unique* $y \in Y$ *et réciproquement*
- Formellement : $f : X \rightarrow Y$ telle que
  - pour tout $x, x' \in X$, $x \neq x' \implies f(x) \neq f(x')$ *injectivité*
  - pour tout $y \in Y$, il existe $x \in X$ telle que $f(x) = y$ *surjectivité*
- Équivalent : il existe une *réciproque* $f^{-1} : Y \rightarrow X$

La bonne définition !

Deux ensembles X et Y ont le même cardinal s'il existe une bijection entre X et Y

Ensembles finis

Deux définitions

- Intuitive: le cardinal d'un ensemble fini X est son nombre d'éléments
- Formelle : X et Y ont même cardinal s'il existe une bijection entre X et Y

Lemme

Un ensemble X a n éléments si et seulement s'il est en bijection avec $\{1, \dots, n\}$

($\Rightarrow$) $X = \{x_1, \dots, x_n\}$ $\quad f : X \longrightarrow \{1, \dots, n\}$, $x_i \longmapsto i$

($\Leftarrow$) Il existe une bijection $f : X \longrightarrow \{1, \dots, n\}$.

- $\forall x \in X,\ f(x) \in \{1, \dots, n\}$
- $\forall x \neq y \in X,\ f(x) \neq f(y)$
- $\forall i \in \{1, \dots, n\},\ \exists x \text{ tq } f(x) = i$

$\Big\}$ $X = \{x_1, \dots, x_n\}$ où $f(x_i) = i$ $\quad (x_i = f^{-1}(i))$

Ensembles dénombrables

Définition

Un ensemble infini X est **dénombrable** s'il est de même cardinal que les entiers naturels $\mathbb{N}$

- Autrement dit, s'il existe une bijection $f : \mathbb{N} \to X$

Exemples

- Ensemble $\mathbb{P}$ des entiers *pairs* positifs :

$$f : \mathbb{N} \to \mathbb{P}$$
$$n \mapsto 2n$$

- Ensemble $\mathbb{Z}$ des entiers relatifs :

$$f(n) = k \in \mathbb{Z}$$

$$f(n) = (-1)^n \lceil n/2 \rceil$$

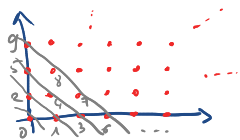
Numérotation

Lemme

- Un ensemble infini X est dénombrable si et seulement s'il existe une fonction *injective* $n : X \to \mathbb{N}$ $\qquad (x \neq y \Rightarrow n(x) \neq n(y))$
- Autrement dit, si on peut *numéroter* les éléments de X

Exemples

- Ensemble $\mathbb{N}^2$ des paires d'entiers :



→ bijection

- Ensemble Σ^* des mots sur un alphabet fini :

si $\Sigma = \{0,1\}$, $w \to$ entier qu'il ~~représente~~ en binaire → $\left.\begin{matrix} 01 \\ 1 \\ 001 \end{matrix}\right\} \to$ entier 1

$w \to$ entier qui s'écrit $1w$ en binaire : injectif.

Preuve

($\Rightarrow$) Dénombrable $\Leftrightarrow \exists$ bij $f : X \to \mathbb{N}$ or une bijection est injective

($\Leftarrow$) On suppose qu'on a $n : X \to \mathbb{N}$ inj.

On définit $f : X \to \mathbb{N}$

$x \mapsto \min\{k : \forall y \text{ tq } n(y) < n(x),\ f(y) \neq k\}$

Représentation finie

Théorème

- Un ensemble infini X est dénombrable si et seulement s'il existe une fonction de codage $\langle\cdot\rangle : X \to \Sigma^*$ où Σ est un alphabet fini ($\textit{injective} : x \neq y \implies \langle x\rangle \neq \langle y\rangle$)
- On peut choisir $\Sigma = \{0, 1\}$

Preuve

($\Rightarrow$) X dénombrable $\Rightarrow \exists$ bijection $f : X \to \mathbb{N}$

Or Σ^* est dénombrable donc $\exists\, g : \mathbb{N} \to \Sigma^*$

donc $g \circ f : X \to \Sigma^*$ est une bijection, donc injective.

($\Leftarrow$) On supp qu'il existe $\langle\cdot\rangle : X \to \Sigma^*$. Or il existe une bijection $g^{-1} : \Sigma^* \to \mathbb{N}$. Donc $g^{-1}(\langle\cdot\rangle) : X \to \mathbb{N}$ est injective.

Exemples et non-exemples

Proposition

Les ensembles suivants sont dénombrables :

- ensemble $\mathbb{Q}$ des rationnels → "9/9" $\in \{0,1,/\}^*$
- ensemble des graphes → les sommets et les arêtes
- ensemble des arbres binaires
- ensemble des tableaux d'entiers "[0;3;12;1;0;7;8]" $\in \{0,1,2,\dots,9,;,[,]\}^*$

Preuve

Chaque élément a une représentation finie.

Remarque

La preuve précédente ne s'applique pas aux ensembles suivants :

- ensemble $\mathbb{R}$ des nombres réels
- ensemble $\mathcal{L}$ de tous les langages $L \subset \{0,1\}^*$
- ensemble des fonctions $f : \{0,1\}^* \to \{0,1\}^*$

Ensembles indénombrables

Définition

Un ensemble infini X est **indénombrable** s'il n'y a pas de bijection $f : \mathbb{N} \to X$

Théorème

L'ensemble $\mathcal{L} = \{L : L \subset \{0,1\}^*\}$ des *langages* est indénombrable

Argument intuitif

- Pour décrire $L \in \mathcal{L}$, il faut dire pour chaque mot $w \in \{0,1\}^*$ si $w \in L$ ou $w \notin L$
- Comme il y a une infinité de mots dans $\{0,1\}^*$, la description de L est infinie

Argument mais pas preuve

- On a montré qu'il existe une description infinie de chaque langage
- Il faut montrer qu'il n'en existe pas de finie

Preuve du théorème : *argument diagonal*

- $\{0,1\}^*$ est dénombrable : on peut numéroter les mots w_0, w_1, …
- On suppose $\mathcal{L}$ dénombrable : on peut numéroter les langages L_0, L_1, …
- On construit $L \notin \mathcal{L}$: contradiction

	w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	w_{11}	w_{12}	w_{13}	w_{14}	w_{15}	w_{16}	w_{17}	w_{18}	w_{19}	w_{20}	w_{21}	w_{22}	w_{23}	w_{24}	…
L_0	0	0	0	1	0	1	1	0	0	0	1	0	1	0	1	0	0	0	1	0	1	0	0	1	0	
L_1	0	1	0	0	0	1	0	0	1	0	1	1	1	0	1	1	1	0	1	0	1	1	0	0	0	
L_2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	
L_3	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0	
⋮																										
L	1	0	1	1	…																					

- $w_i \in L \Leftrightarrow w_i \notin L_i$
- Pour tout i $L \neq L_i$. Donc $L \notin \mathcal{L}$.

Autres ensembles indénombrables

Théorème

Les ensembles suivants sont indénombrables :

- l'ensemble des fonctions $f : \{0,1\}^* \to \{0,1\}$
- l'ensemble des fonctions $f : \Sigma^* \to \Sigma^*$
- l'ensemble $[0,1]$ des réels entre 0 et 1
- l'ensemble $\mathbb{R}$ des nombres réels

Remarque

- Tous ces ensembles ont le même cardinal (= sont en bijection)
- On peut trouver des ensembles encore plus gros fonctions $f : \mathbb{R} \to \mathbb{R}$

Preuve

- $f \mapsto L_f = \{ w : f(w) = 1 \}$ est bijective.
- l'ensemble des $f : \Sigma^* \to \Sigma^*$ "contient" l'ensemble des $f : \{0,1\}^* \to \{0,1\}$.
- bijection : $x \in [0,1] \mapsto$ "langage des bits de x"
- $[0,1] \subset \mathbb{R}$.

Bilan

Il existe plusieurs *tailles* d'infini

Ensembles dénombrables

- *Plus petits* ensembles infinis
- Caractérisations :
  - en bijection avec $\mathbb{N}$ ou autre ensemble dénombrable
  - chaque élément possède une description finie
- Exemples : $\{0,1\}^*$, $\mathbb{Q}$, graphes, suites finies d'entiers, …

Ensembles indénombrables

- Ensembles de taille *strictement supérieure* à celle de $\mathbb{N}$
- Caractérisations :
  - pas de bijection avec un ensemble dénombrable
  - en bijection avec un ensemble indénombrable
- Exemples :
  - $\mathbb{R}$, langages $\subset \{0,1\}^*$, fonctions $f : \Sigma^* \to \Sigma^*$, suites infinies d'entiers, …
  - fonctions $f : \mathbb{R} \to \mathbb{R}$, suites infinies de réels, …

Pour aller plus loin

Tailles d'infini

- Il existe une infinité de tailles d'infini différentes
- Existe-t-il une taille intermédiaire entre $\mathbb{N}$ et $\mathbb{R}$?
  - Question mathématiquement *indémontrable*

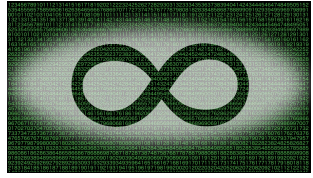


Table des matières

Nombre d'algorithmes

Combien y a-t-il d'algorithmes différents ?

Rappel

- Formalisation : algorithme = machine de Turing
  - ou machine RAM, ou programme dans un langage donné, ou …
- Question : combien y a-t-il de machines de Turing ?

Théorème

L'ensemble des algorithmes est dénombrable

Preuve

- Chaque machine de Turing possède une description finie
  - Chaque machine RAM, chaque programme, … possède une description finie

Conséquence

- On peut numéroter les algorithmes : A_0, A_1, A_2, …

Description binaire d'une machine de Turing

Rappel

- $\mathcal{M} = (Q, \Sigma, q_0, \delta)$
- Il suffit de représenter $\delta = \{(q, x, q', y, \leftrightarrow), \dots\}$

Avec un grand alphabet

- Alphabet : $\Gamma = Q \sqcup \Sigma \sqcup \{\leftarrow, \rightarrow\}$
- Transition : mot $qxq'y \leftrightarrow$ de 5 lettres sur l'alphabet Γ
- Table δ : concaténation des transitions
  - pas besoin de symbole de séparation

Avec un alphabet binaire

- On représente $\mathcal{M}$ sur l'alphabet Γ
- On représente chaque lettre de Γ par un mot binaire
  - Numérotation $\Gamma = \{\gamma_0, \gamma_1, \dots, \gamma_{n-1}\}$
  - $\gamma_i \to \text{BIN}_\ell(i)$ avec $\ell = 1 + \lfloor \log n \rfloor$

Conséquence

Deux faits

- L'ensemble des algorithmes est dénombrable
- L'ensemble des langages (resp. des fonctions) est indénombrable

Théorème

- Il existe des langages $L \subset \{0,1\}^*$ qui ne sont pas reconnaissables
- Il existe des langages $L \subset \{0,1\}^*$ qui ne sont pas décidables
- Il existe des fonctions $f : \{0,1\}^* \to \{0,1\}^*$ qui ne sont pas calculables

Preuve

- Un langage est reconnaissable s'il existe un algo A tq $A(w) = 1 \iff w \in L$
- L'ensemble des langages reconnaissables est dénombrable.
- Si tous les langages étaient reconnaissables, l'ensemble des langages serait dénombrable

Conclusion

Tout n'est pas calculable

- Il existe beaucoup plus de langages ou de fonctions que d'algorithmes
- Donc il existe des langages et fonctions sans algorithme
- On peut même dire, dans un sens précis, que :
  - *presque aucun* langage n'est reconnaissable
  - *presque aucun* langage n'est décidable
  - *presque aucune* fonction n'est calculable

Remarque

- Le théorème ne donne *aucun exemple* !
- On en verra dans le prochain cours

Bonus 1 : nombres algébriques

Définition

Un nombre complexe z est *algébrique* s'il existe un polynôme $p \in \mathbb{Z}[x]$ tel que $p(z) = 0$

Exemples

- Entiers, rationnels, $\sqrt{2}$ (x^2-2) $\varphi = \frac{1}{2}(1+\sqrt{5})$ (x^2-x-1), $e^{3i\pi/7}$ $(x^6-x^5+x^4-x^3+x^2-x+1)$, …
- $\sqrt[5]{3} - 3i\sqrt[3]{13} \simeq 1,24573 - 7,05400i$ $(x^{30}-18x^{25}+616005x^{24}+135x^{20}+454611690x^{19}+151784864010x^{18}-540x^{15}+8349331770x^{14}-213105949070040x^{13}+18700047030896010x^{12}+1215x^{10}+20723640210x^9+2042948377142595x^8+1026632581996190 9490x^7+1151932247126709664005x^6-1458x^5+6286947030x^4-372935410872570x^3+4796562063424826565x^2-207347804482807739520 90x+28383840955651551463016730)$
- $1.752347726449668\ldots$ $(x^5-10x+1)$
- Contre-exemples : π, e, $\sin(1)$, $\ln(2)$, $\log_2(3)$, …

Théorème

L'ensemble des nombres algébriques est dénombrable

Preuve

Description : le polynôme + suffisamment de décimales pour distinguer des autres racines

Bonus 2 : nombres réels calculables

Définition

Un nombre $x \in \mathbb{R}$ est *calculable* s'il existe un algorithme qui, étant donné n, calcule les n premières décimales de x

Exemples

- Nombres algébriques
- π, e, $\sin(1)$, $\ln(2)$, $\log_2(3)$, …
- Contre-exemples : ???

Théorème

- L'ensemble des nombres réels calculables est dénombrable
- *Presque tous* les nombres réels sont incalculables

Bonus 3 : nombres réels définissables

Définition informelle

Un nombre $x \in \mathbb{R}$ est *définissable* s'il possède une description finie

Exemples

- N'importe quel nombre que je peux décrire…
- Contre-exemple : par définition, je ne peux en décrire aucun…

Théorème

- L'ensemble des nombres définissable est dénombrable
- Presque aucun nombre réel n'est définissable !

Remarque

- Nécessite une définition *formelle* de définissable
- Paradoxe sinon : « le plus petit nombre positif non définissable »

Pour aller plus loin