

Logique et Calculabilité

INF551

$$\exists \Rightarrow \forall$$

Dr. Stéphane Lengrand,

`Stephane.Lengrand@Polytechnique.edu`

Cours IV

Les fonctions calculables



Vu de près : un algorithme

Vu de loin : une fonction **calculable**

Posons la question : **quelles fonctions sont calculables ?**

Comment répondre ?

On sait programmer ceci, et cela, ...

On sait composer les programmes comme ceci, et comme cela ...

“Et c’est tout”

C’est la définition inductive d’un ensemble de fonctions

I. La calculabilité sur les entiers

F_n ensemble des fonctions **partielles** de $\mathbb{N}^n$ dans $\mathbb{N}$

$$F = \bigcup_n F_n$$

Fonctions calculables

= un sous-ensemble de F inductivement défini comme le plus petit ensemble...

Plus petit ensemble...

qui contient

1. les fonctions $x_1, \dots, x_n \mapsto x_i$ "projections"
2. les fonctions $x_1, \dots, x_n \mapsto 0$ "fonctions constantes nulles"
3. la fonction $x \mapsto x + 1$ "fonction successeur"

et qui est clos par

1. composition
2. définition par récurrence
3. minimisation

La composition

A partir de fonctions $g_1, \dots, g_m$ de $\mathbb{N}^n$ dans $\mathbb{N}$ et h de $\mathbb{N}^m$ dans $\mathbb{N}$
construire la fonction

$$x_1, \dots, x_n \mapsto h(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))$$

La récurrence

A partir de fonctions g de $\mathbb{N}^{n-1}$ dans $\mathbb{N}$ et h de $\mathbb{N}^{n+1}$ dans $\mathbb{N}$
construire la fonction f définie par

$$f(x_1, \dots, x_{n-1}, 0) = g(x_1, \dots, x_{n-1})$$

$$f(x_1, \dots, x_{n-1}, y + 1) = h(x_1, \dots, x_{n-1}, y, (f(x_1, \dots, x_{n-1}, y)))$$

La minimisation

A partir de la fonction g de $\mathbb{N}^{n+1}$ dans $\mathbb{N}$
construire la fonction f définie par

$$f(x_1, \dots, x_n) = y$$

si y est le plus petit entier t.q. $g(x_1, \dots, x_n, y) = 0$

Et s'il n'en y a pas ?

Les domaines de définition

Projections, nulles, successeur : totales

f composée de $g_1, \dots, g_m$ avec h est définie en $p_1, \dots, p_n$
si $g_1, \dots, g_m$ définies en $p_1, \dots, p_n$
et h définie en $g_1(p_1, \dots, p_n), \dots, g_m(p_1, \dots, p_n)$

f définie par récurrence à partir de g et h est définie en $p_1, \dots, p_{n-1}, 0$
si g définie en $p_1, \dots, p_{n-1}$

f définie par récurrence à partir de g et h est définie en $p_1, \dots, p_{n-1}, q + 1$
si f définie en $p_1, \dots, p_{n-1}, q$
et h définie en $p_1, \dots, p_{n-1}, q, f(p_1, \dots, p_{n-1}, q)$

f définie par minimisation de g est définie en $p_1, \dots, p_n$
s'il existe q tel que : g définie et non nulle en $p_1, \dots, p_n, r$ pour tout $r < q$
et g définie et nulle en $p_1, \dots, p_n, q$

Les domaines de définition

Toutes les constructions préservent la totalité sauf la minimisation

Si g totale mais ne s'annule jamais

alors f construite par minimisation n'est pas définie en 0

On calcule $g(0, 0)$, $g(0, 1)$, $g(0, 2)$, $g(0, 3)$, ...

Intuition f non définie en p = le calcul de $f(p)$ ne termine pas

(à suivre)

Exemples

$$x \mapsto x + 2$$

$$x, y \mapsto x + 1$$

L'addition, la multiplication, la fonction factorielle, la fonction prédécesseur

Le “et” booléen ($\&\&$), la négation booléenne ($!$), le “ou” booléen ($||$), le “if then else”

La soustraction limitée

La fonction caractéristique de $\leq$

La fonction caractéristique de $=$

Le quotient

Le reste

La fonction inverse d'une fonction calculable

Les programmes

Ensemble des fonctions calculables : définition inductive

Une fonction est calculable si et seulement si **il existe une dérivation de cette fonction**

Programme = dérivation d'une fonction calculable (le programme **calcule** la fonction)

= arbre étiqueté par les noms des règles $\pi_i^n, Z^n, Succ, \circ_m^n, Rec^n, \mu^n$

Remarque : $\neq$ programmes peuvent calculer la même fonction

$\circ_1^1(Succ, Succ) ?$

$\mu^1(\pi_1^2) ?$

Un programme f **termine** en $p_1, \dots, p_n$

si la fonction calculée est définie en $p_1, \dots, p_n$

La décidabilité

Un ensemble $A \subseteq \mathbb{N}$ est **décidable** si sa fonction caractéristique est calculable

i.e. s'il existe une fonction calculable f t.q. $f(x) = 1$ si $x \in A$ et $f(x) = 0$ sinon

Un ensemble A est **semi-décidable** s'il existe une fonction calculable f t.q. $f(x) = 1$ si $x \in A$ et f n'est pas définie en x sinon

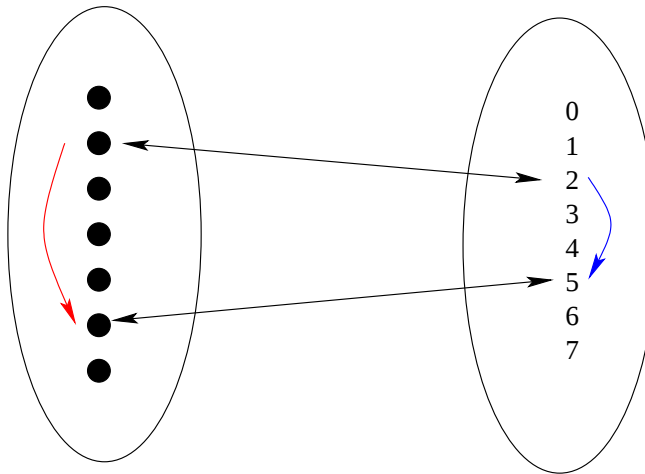
Exemple : l'ensemble des nombres pairs

II. La calculabilité sur les listes et les arbres

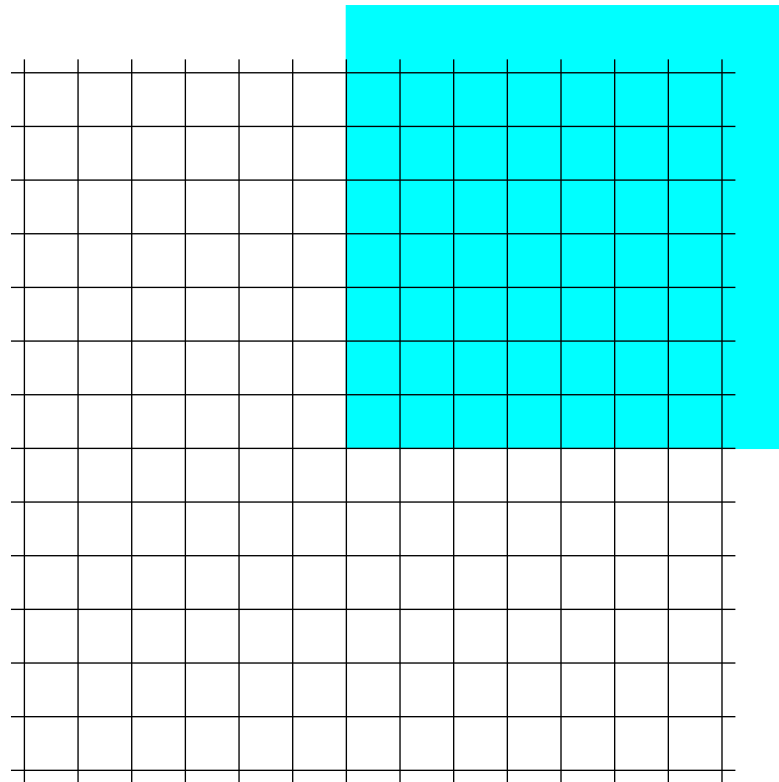
On veut étendre la calculabilité à d'autres types de données : listes, arbres,...

on peut recommencer à chaque fois

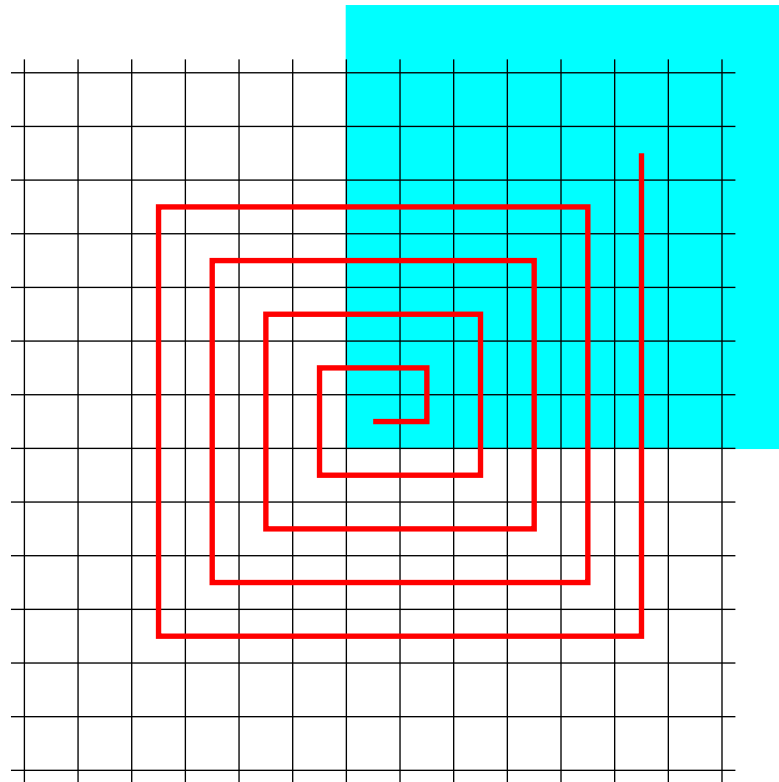
ou alors on peut numéroter les données (une idée de hacker)



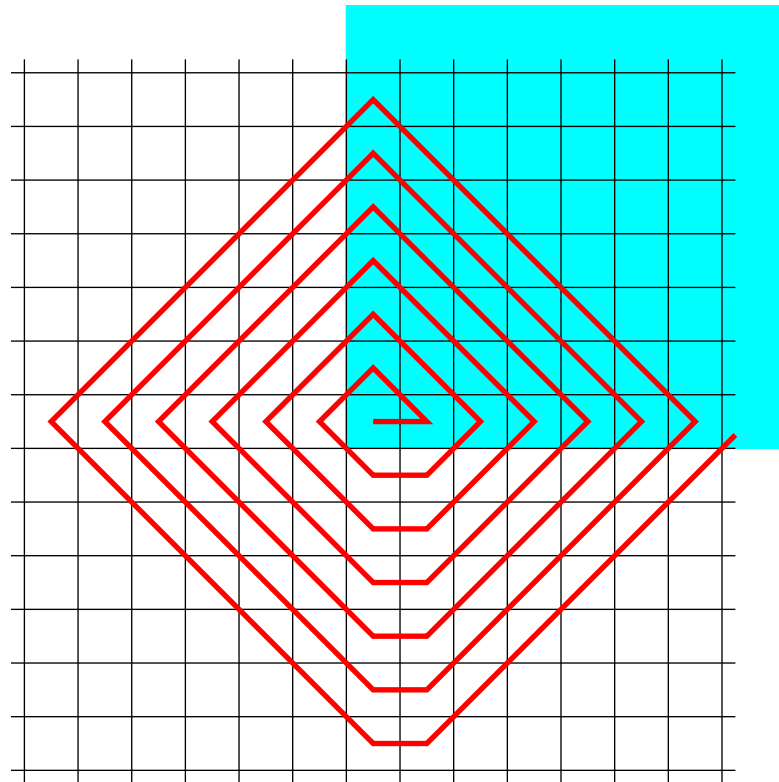
Un outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$



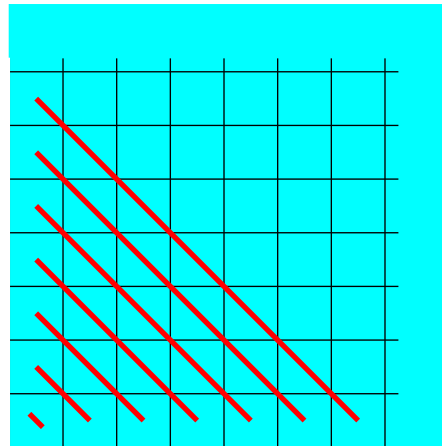
Un outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$



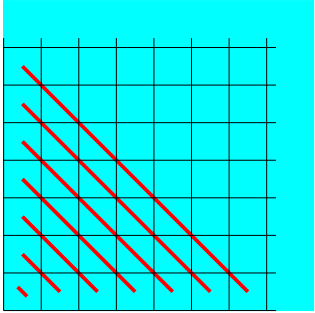
Un outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$



Un outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$



Un outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$



Point (n, p) sur la ligne $n + p$

Avant cette ligne $1 + 2 + \dots + (n + p) = (n + p)(n + p + 1)/2$ points

(numérotés de 0 à $(n + p)(n + p + 1)/2 - 1$)

Le numéro du point (n, p) est

$$(n + p)(n + p + 1)/2 + p$$

Un (meilleur) outil : une bijection entre $\mathbb{N}^2$ et $\mathbb{N}^*$

On ajoute 1

Le numéro du point (n, p) , noté $n; p$, est

$$(n; p) = (n + p)(n + p + 1)/2 + p + 1$$

La fonction ; (de $\mathbb{N}^2$ dans $\mathbb{N}$) est calculable

Ses deux réciproques hd et tl (de $\mathbb{N}$ dans $\mathbb{N}$) également

La calculabilité sur les listes

$$\ulcorner a_1, a_2, \dots, a_n \urcorner = (a_1; (a_2; (\dots; (a_n; 0))))$$

Definition: f est calculable

si la fonction (de $\mathbb{N}^n$ dans $\mathbb{N}$) qui à $\ulcorner l_1 \urcorner, \dots, \ulcorner l_n \urcorner$ associe $\ulcorner f(l_1, \dots, l_n) \urcorner$ est calculable

$cons : x, l \mapsto (x, l)$ est calculable

$hd, tl, sub, length, \dots$

l'accès au i ème élément

Une application : la récurrence bien fondée

$$f(0) = f(1) = 1, f(n) = f(n-1) + f(n-2)$$

Calculable ?

Plus généralement récurrence qui utilise non seulement $f(n-1)$ mais tous les $f(p)$ pour $p < n$

La fonction F t.q.

$$F(n) = \ulcorner f(0), f(1), f(2), \dots, f(n) \urcorner = (f(0); f(1); f(2); \dots; f(n); 0)$$

a un schéma de récurrence dans lequel $F(n)$ est défini en fonction de $F(n-1)$

Généralisons à d'autres types de données

Fonctions de $\mathcal{C}$ dans $\mathcal{D}$ avec $\mathcal{C}, \mathcal{D}$ finis ou dénombrables

Calculabilité définie à partir d'injections dans $\mathbb{N}$ ($\ulcorner \cdot \urcorner^{\mathcal{C}}$ et $\ulcorner \cdot \urcorner^{\mathcal{D}}$) :

$f : \mathcal{C} \longrightarrow \mathcal{D}$ calculable si
$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ \ulcorner x \urcorner^{\mathcal{C}} & \mapsto & \ulcorner f(x) \urcorner^{\mathcal{D}} \end{array} \text{ calculable}$$

En toute rigueur, la calculabilité dépend des injections, mais deux injections

$\ulcorner \cdot \urcorner, \ulcorner \cdot \urcorner' : \mathcal{C} \longrightarrow \mathbb{N}$ donnent la même notion de calculabilité pour $\mathcal{C}$ si $\ulcorner x \urcorner \mapsto \ulcorner x \urcorner'$ et sa réciproque (de $\mathbb{N}$ dans $\mathbb{N}$) sont calculables

1 seule notion de calculabilité pour $\mathcal{C}$ **ensemble fini**

En pratique, aucune ambiguïté pour nos types de données...

1 seule notion de calculabilité pour les listes d'entiers

...tel que l'accès au i ème élément est calculable

$$\begin{array}{ccc} f : & \mathbb{N}^n & \longrightarrow \mathcal{D} \\ & (a_1, a_2, \dots, a_n) & \mapsto f(a_1, a_2, \dots, a_n) \end{array} \quad \text{calculable}$$

ssi

$$\begin{array}{ccc} & \mathbb{N} & \longrightarrow \mathcal{D} \\ (a_1; (a_2; (...; (a_n; 0)))) & \mapsto & f(a_1, a_2, \dots, a_n) \end{array} \quad \text{calculable}$$

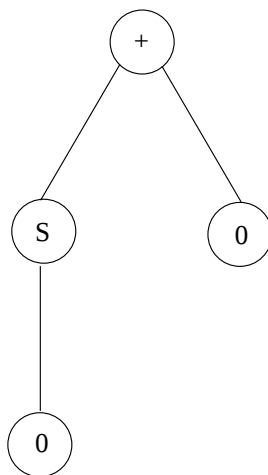
ssi

$$\begin{array}{ccc} \text{Listes} & \longrightarrow & \mathcal{D} \\ a_1, a_2, \dots, a_n & \mapsto & f(a_1, a_2, \dots, a_n) \end{array} \quad \text{calculable}$$

1 seule notion de calculabilité pour les arbres...

...tel que l'accès aux contenus des noeuds est calculable

D'abord : arbres étiquetés par des éléments d'un ensemble fini



On les numérote arbitrairement : $\ulcorner 0 \urcorner = 12$, $\ulcorner S \urcorner = 13$, $\ulcorner + \urcorner = 14$

Puis on numérote chaque arbre : $\ulcorner f(t_1, \dots, t_n) \urcorner = (\ulcorner f \urcorner; \ulcorner t_1 \urcorner; \dots; \ulcorner t_n \urcorner; 0)$

La calculabilité pour les arbres est **indépendante du choix de la numérotation**
(changement de numérotation calculable)

1 seule notion de calculabilité pour les arbres...

...tel que l'accès aux contenus des noeuds est calculable

Plus généralement : arbres étiquetés dans un ensemble infini dénombrable

Arbres 1-articulé = ensemble d'étiquettes fini

Arbres $(n + 1)$ -articulé = ens. d'étiquettes n -articulé

Exemples : propositions, séquents, démonstrations

1 seule notion de calculabilité pour les **arbres k-articulés** ($k \geq 1$)

tel que l'accès aux contenus des noeuds est calculable

$$\ulcorner f(t_1, \dots, t_n) \urcorner^k = (\ulcorner f \urcorner^{k-1}; (\ulcorner t_1 \urcorner^k; (\dots; (\ulcorner t_n \urcorner^k; 0))))$$

avec $\ulcorner \cdot \urcorner^0$ n'importe quelle injection de l'ensemble fini dans $\mathbb{N}$

III. L'élimination de la récurrence

Ensemble des fonctions calculables inductivement défini par

- les fonctions $x_1, \dots, x_n \mapsto x_i$
 - les fonctions $x_1, \dots, x_n \mapsto 0$
 - la fonction $x \mapsto x + 1$
-
- la composition
 - la définition par récurrence
 - la minimisation

Ensemble $\mathcal{C}$ inductivement défini par

- les fonctions $x_1, \dots, x_n \mapsto x_i$
- les fonctions $x_1, \dots, x_n \mapsto 0$
- la fonction $x \mapsto x + 1$
- l'addition
- la multiplication
- la fonction caractéristique de $\leq$
- la composition

- la minimisation

même ensemble ?

Chaque ensemble est clos par les règles de l'autre

$+$, $\times$, $\chi_{\leq}$ calculables (facile)

$\mathcal{C}$ clos par récurrence ?

g et h dans $\mathcal{C}$

f construite par récurrence à partir de g et h

dans $\mathcal{C}$?

$\mathcal{C}$ clos par récurrence ?

$r = f(x_1, \dots, x_{n-1}, y)$ ssi

il existe une suite $s_0, \dots, s_y$ t.q.

$$s_0 = g(x_1, \dots, x_{n-1})$$

$$s_1 = h(x_1, \dots, x_{n-1}, 0, s_0)$$

...

$$s_{k+1} = h(x_1, \dots, x_{n-1}, k, s_k)$$

...

et $r = s_y$

Il existe une suite ?

Codons la par un entier

Le codage des suites

Avec la fonction $;$, codage des suites $cons, hd, tl, nth$

Ça commence bien $;$, $cons, hd, tl$ appartiennent à $\mathcal{C}$

Mais comment montrer que nth appartient à $\mathcal{C}$? (pas de récurrence)

Une autre codage : la fonction β de Gödel

$$\beta(k, l, i) = l \bmod (k(i + 1) + 1)$$

Pour toute suite finie $s_0, \dots, s_y$, il existe deux entiers k, l tel que pour tout i ,
 $s_i = \beta(k, l, i)$

La récurrence

Une fonction de $\mathcal{C}$ qui à $x_1, \dots, x_{n-1}, y, k, l$ et i associe le nombre 1 ssi $i < y$ et $h(x_1, \dots, x_{n-1}, i, \beta(k, l, i)) = \beta(k, l, i + 1)$ et 0 sinon.

Une fonction de $\mathcal{C}$ qui à $x_1, \dots, x_{n-1}, y, k, l$ et r associe l'entier 0 si $g(x_1, \dots, x_{n-1}) = \beta(k, l, 0)$
pour tout $i < y$, $h(x_1, \dots, x_{n-1}, i, \beta(k, l, i)) = \beta(k, l, i + 1)$
et $\beta(k, l, y) = r$.

Soit une la fonction de $\mathcal{C}$ qui à $x_1, \dots, x_{n-1}, y$ associe le plus petit j t.q. la fonction précédente s'annule en $x_1, \dots, x_{n-1}, y, hd(hd(j)), tl(hd(j)), tl(j)$

Quelques complications techniques (f^*) : poly

Que retenir ?

Une définition **équivalente** des fonctions calculables en 8 règles

Trois fonctions de bases de plus, en l'échange de la récurrence

IV. L'indécidabilité du problème de l'arrêt

Théorème

L'ens. des couples d'entiers (p, q) t.q. $p = \lceil f \rceil$ et f termine en q
est indécidable

Preuve par l'absurde

On suppose l'existence d'un programme h qui termine toujours t.q.

$$\begin{aligned} h(p, q) &= 1 \text{ si } p = \ulcorner f \urcorner \text{ et } f \text{ termine en } q \\ h(p, q) &= 0 \text{ sinon} \end{aligned}$$

On fabrique

$$k = \circ_1^1(\mu^1(\pi_1^2), \circ_2^1(h, \pi_1^1, \pi_1^1))$$

$$\begin{aligned} k \text{ ne termine pas en } p \text{ si } p = \ulcorner f \urcorner \text{ et } f \text{ termine en } p \\ k \text{ termine en } p \text{ sinon} \end{aligned}$$

k termine en $\ulcorner k \urcorner$ si et seulement si k ne termine pas en $\ulcorner k \urcorner$

Contradiction.

La suite

En PC : La fonction d'Ackermann

La prochaine fois : le théorème de Church

Questions?