

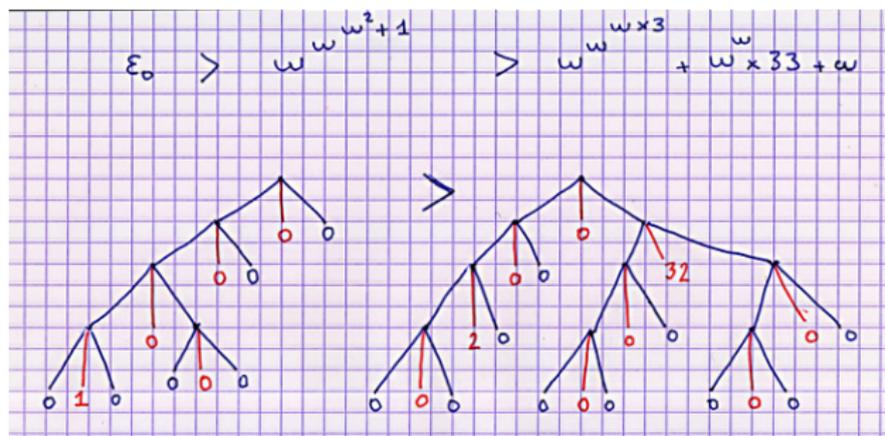
Opérateurs de description en *Coq*

Pierre Castéran¹

¹Méthodes Formelles, LaBRI

Le contexte : Travail sur les preuves de terminaison et les ordinaux

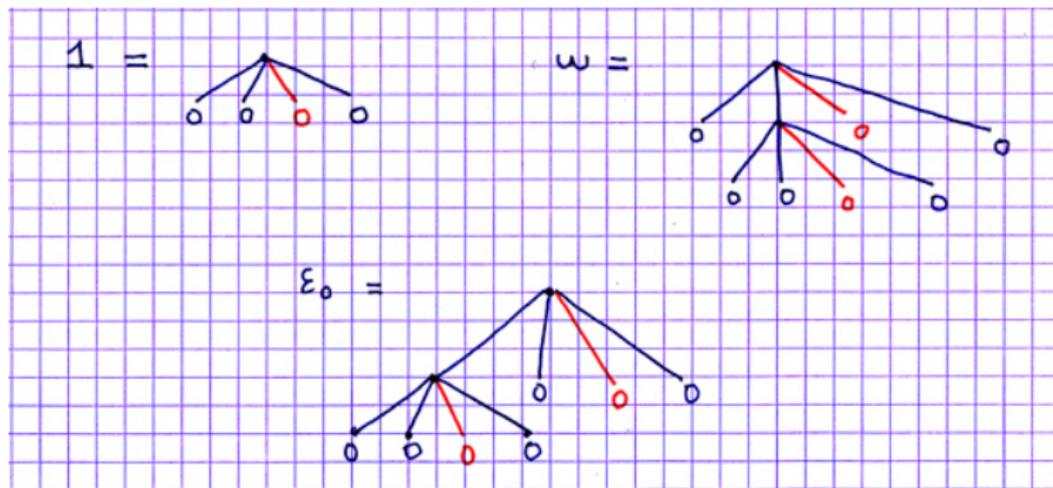
- Preuve de terminaison des suites de Goodstein et des batailles d'Hydre, utilisant des ordinaux en forme normale de Cantor :



- ▶ On définit un ordre total, décidable, bien fondé (preuve par plongement dans le rpo),
- ▶ une arithmétique (successeur, addition, multiplication, exponentiation),
- ▶ on associe à toute hydre ou toute suite de Goodstein un ordinal,
- ▶ on prouve que la suite des ordinaux associés est strictement décroissante.

Extension de ce travail

On peut représenter des ordinaux plus grands à l'aide de *la forme normale de Veblen* :



Quelques difficultés

- ▶ Représentation compacte, mais peu intuitive

Inductive T2: Set :=

| zero : T2

| cons : T2 → T2 → nat → T2.

cons a b n c == $\psi(a, b) \times (n + 1) + c$

- ▶ la relation d'ordre total associée est définie de façon inductive par 7 cas, genre :

lt_4 : $\forall \alpha_1 \alpha_2 \beta_1 \beta_2 n_1 n_2 \gamma_1 \gamma_2,$

$\alpha_2 < \alpha_1 \rightarrow$

cons $\alpha_1 \beta_1 0$ zero < $\beta_2 \rightarrow$

cons $\alpha_1 \beta_1 n_1 \gamma_1 <$ cons $\alpha_2 \beta_2 n_2 \gamma_2$

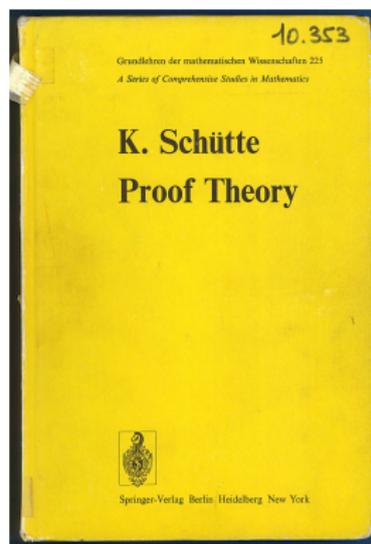
L'exemple de l'addition

```

Fixpoint plus (alpha beta : T2) {struct alpha}:T2 :=
  match alpha,beta with
  | zero, y => y
  | x, zero => x
  | cons a b n c, cons a' b' n' c' =>
    (match compare (cons a b 0 zero)
      (cons a' b' 0 zero)
    with | Lt => cons a' b' n' c'
         | Gt => (cons a b n (c + (cons a' b' n' c')))
         | Eq  => (cons a b (S(n+n')) c'))
    end)
  end
where "alpha + beta" := (plus alpha beta): g0_scope.

```

Afin de valider une telle représentation, il est nécessaire de prendre une référence mathématique :



Une Définition axiomatique des ordinaux dénombrables

Ax. I. \mathbb{O} is a set well-ordered by a relation $<$.

Ax. II. Every bounded subset of \mathbb{O} is denumerable. That is: if, given $M \subset \mathbb{O}$ there exists $\alpha \in \mathbb{O}$ such that $\xi < \alpha$ for all $\xi \in M$, then M is a finite or denumerably infinite set.

Ax. III. Every denumerable subset of \mathbb{O} is bounded. That is: for each finite or denumerably infinite set $M \subset \mathbb{O}$ there exists $\alpha \in \mathbb{O}$ such that $\xi < \alpha$ for all $\xi \in M$.

Corollary: \mathbb{O} is an infinite, but not denumerable set.

Validation de la représentation des ordinaux

- ▶ Etablir un morphisme injectif des représentations en forme normale de Cantor ou Veblen (ou autres) vers l'ensemble des ordinaux dénombrables (par exemple selon Schütte)
- ▶ Première étape, traduire en *Coq* cette théorie axiomatique.
- ▶ L'analyse du discours de Schütte fait apparaître deux notions récurrentes :
 - ▶ fonctions partielles,
 - ▶ définitions de constantes à partir de preuves [classiques] d'existence.

Représentation de fonctions partielles en *Coq* : un exemple

$$\frac{Y \text{ dénombrable} \quad X \subseteq Y}{\sqcup X \leq \sqcup Y}$$

Les axiomes de Schütte permettent de définir la borne supérieure d'une partie *dénombrable* de \mathbb{O} .

Représentation de fonctions partielles en *Coq* : un exemple

$$\frac{Y \text{ dénombrable} \quad X \subseteq Y}{\sqcup X \leq \sqcup Y}$$

\sqcup : Ensemble OT \rightarrow option OT

```

∀ X Y, denumerable Y → Included X Y →
  match  $\sqcup$  X,  $\sqcup$  Y with
  | Some x, Some y => x ≤ y
  | _, _ => True
end

```

Représentation de fonctions partielles en *Coq* : un exemple

$$\frac{Y \text{ dénombrable} \quad X \subseteq Y}{\sqcup X \leq \sqcup Y}$$

\sqcup : $\forall X, \text{denumerable } X \rightarrow \text{OT}$

$\forall X Y (D : \text{denumerable } Y)(H: \text{Included } X Y),$
 $\sqcup X (\text{denumerable_included } X Y D H) \leq \sqcup Y D$

Représentation de fonctions partielles en *Coq* : un exemple

$$\frac{Y \text{ dénombrable} \quad X \subseteq Y}{\sqcup X \leq \sqcup Y}$$

`is_⊔`: Ensemble OT → OT → Prop

`∀ X Y x y, denumerable Y → Included X Y →
 is_⊔ X x → is_⊔ Y y →
 x ≤ y`

Représentation de fonctions partielles en *Coq* : un exemple

$$\frac{Y \text{ dénombrable} \quad X \subseteq Y}{\sqcup X \leq \sqcup Y}$$

Require Import Epsilon.

\sqcup : Ensemble OT \rightarrow OT

$\forall X Y, \text{denumerable } Y \rightarrow \text{Included } X Y \rightarrow$
 $\sqcup X \leq \sqcup Y.$

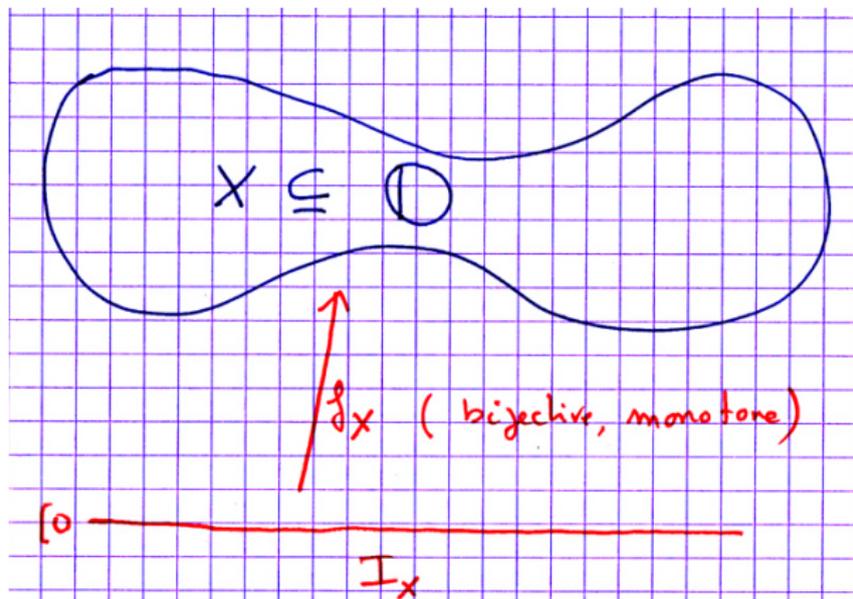
Définitions globales à partir de preuves d'existence

Considérons la définition de l'addition dans \mathbb{O} :

« $\alpha + \beta$ est le β -ième ordinal supérieur ou égal à α »

- ▶ Cette définition est une application d'une fonction d'énumération de l'ensemble des éléments de \mathbb{O} supérieurs ou égaux à α ,
- ▶ En général, la locution « le β -ième élément de X » n'est pas partout définie.

Fonctions d'énumération



Le texte ci-dessous construit une fonction g point par point. Ce lemme est utilisé par la suite dans une construction (par induction transfinie) d'une fonction d'énumération de tout sous-ensemble de \mathbb{O} .

Lemma 3. *If every proper segment of a set $B \subset \mathbb{O}$ has an ordering function then B also has an ordering function.*

Proof. Let $f_\beta : A_\beta \rightarrow B(\beta)$ be an ordering function of $B(\beta)$ for each proper segment $B(\beta)$ of B . By Ax. II the set $B(\beta)$ is denumerable. Since f_β is bijective, A_β is also denumerable and therefore a proper \mathbb{O} -segment. Therefore to each ordinal $\beta \in B$ there is an ordinal $g(\beta)$ such that $A_\beta = \mathbb{O}(g(\beta))$. g is a map from B into \mathbb{O} .

L'opérateur de description indéfinie et ses dérivés

`Logic.ClassicalEpsilon (requires Classical)`

Axiom `constructive_indefinite_description` :
`forall (A : Type) (P : A→Prop),`
`(exists x, P x) → { x : A | P x }.`

`epsilon` : $\forall A: \text{Type}, \text{inhabited } A \rightarrow (A \rightarrow \text{Prop}) \rightarrow A.$

`epsilon_spec`
`: $\forall (A : \text{Type}) (i : \text{inhabited } A) (P : A \rightarrow \text{Prop}),$`
 `$(\exists x : A, P x) \rightarrow P (\text{epsilon } i P)$`

Opérateurs dérivés

hilbert/Epsilon.v

```
Definition iota (A:Type)(i : inhabited A)
              (P: A→Prop) : A :=
  epsilon i (unique P).
```

```
Definition the_fun (i : inhabited B)(D : A→Prop)
                 (R:A→B→Prop)
                 (pi : ∀ a, D a → ∃!b, R a b)
                 : A→B :=
  fun a:A ⇒ iota i (fun (b:B) ⇒ D a ∧ R a b).
```

Un exemple : la définition de l'addition

```

Definition alpha_th (B: Ensemble OT):=
  epsilon
  (inhabits (fun alpha => alpha))
  (fun f =>
    ordering_function f (the_ordering_segment B) B).

```

```

Lemma alpha_th_ok
  :  $\forall$  B : Ensemble OT,
    Included B ordinal ->
    ordering_function (alpha_th B)
      (the_ordering_segment B) B

```

Définition de l'addition (suite)

```
Definition plus alpha : OT → OT :=  
  alpha_th (ge alpha).
```

```
Notation "alpha + beta " := (plus alpha beta) : ord_scope.
```

Tactiques associées

```

  /*Une fonction  $f$  normale sur  $X$ 
  est une fonction d'énumération continue de  $\mathbb{O}$  dans  $X$ */

```

```

Lemma normal_plus_alpha :  $\forall \alpha$ , ordinal  $\alpha \rightarrow$ 
                          normal (plus  $\alpha$ ) (ge  $\alpha$ ).

```

Proof.

```

  intros; unfold plus; epsilon_e (alpha_th (ge  $\alpha$ )).

```

.

```

alpha : Well_Orders.M ON
H : ordinal alpha
=====
∃ x : OT → OT,
  ordering_function x (the_ordering_segment (ge alpha))
                    (ge alpha)

```

subgoal 2 is:

```

∀ x : OT → OT,
  ordering_function x (the_ordering_segment (ge alpha))
                    (ge alpha) →
  normal x (ge alpha)

```

Suite de la preuve, utilisant le théorème suivant :

« Si $X \subseteq \mathbb{O}$ est non borné et clos par \sqcup , alors toute fonction d'énumération de X est normale. »

Respect de la structure du discours mathématique

denumerable and therefore a proper \mathbb{O} -segment. Therefore to each ordinal $\beta \in B$ there is an ordinal $g(\beta)$ such that $A_\beta = \mathbb{O}(g(\beta))$. g is a map from B into \mathbb{O} .

Section beta_fixed.

Variable beta : OT.

Hypothesis beta_B : In B beta.

...

Definition g := iota inh_OT

(fun o \Rightarrow ordinal o \wedge
A_beta = members o).

End beta_fixed.

Lemma g_def : $\forall \beta : OT, \text{In } B \beta \rightarrow$

A_beta $\beta = \text{members } (g \beta)$.

Bilan provisoire

- ▶ L'opérateur de description indéfinie permet de décrire facilement les fonctions partielles, et des constructions classiques du discours mathématique
- ▶ Les énoncés de théorèmes ne demandent pas d'adaptation,
- ▶ La traduction de certaines définitions peut donner lieu à des expressions complexes (opérateurs de description emboîtés, points-fixes de fonctions mutuellement récursives), **mais** il suffit d'en dériver les égalités paraphrasant ces définitions.

Non incompatibilité avec le *Coq* usuel, moyennant quelques précautions :

- ▶ incompatibilité avec l'imprédicativité de Set,
- ▶ transformation de $P \vee Q$ en $\{P\} + \{Q\}$ (en utilisant *epsilon*),
- ▶ transformation de $P \vee \neg P$ en $\{P\} + \{\neg P\}$ (en utilisant seulement *iota*)
- ▶ Utilisation du système de modules : Le module *EPSILON0* est en « *Coq* pur ». Le lemme ci-dessous établit la relation entre une représentation effective de l'ordinal ω , et sa définition mathématique classique.

Lemma omega_omega : inject EPSILON0.omega = omega.

À faire :

- ▶ Considérer d'autres corpus,
- ▶ Structures syntaxiques adaptées (cf le travail de Pierre Corbineau)
- ▶ Développer plus de tactiques spécialisées.