Des omégas dans le Vouvray

- Exemples de terminaison lente
- Structure des preuves de terminaison
- Coq et le langage mathématique

Exemples de terminaison lente

Les suites de Goodstein et des problèmes similaires (batailles d'Hydre) présentent les caractéristiques suivantes:

- Propriétés faciles à énoncer, dures à prouver (parfois assez contre-intuitives:)
- Les preuves de ces propriétés mêlent inférences et calculs

Suites de Goodstein: un exemple

$$\begin{aligned} 42 &= 2^5 + 2^3 + 2 \\ &= 2^{(2^2+1)} + 2^{2+1} + 2 \end{aligned}$$

Suites de Goodstein: un exemple

$$
\begin{aligned}
42 &= 2^5 + 2^3 + 2 \\
&= 2^{(2^2+1)} + 2^{2+1} + 2 \\
\bullet \quad &= 3^{(3^3+1)} + 3^{3+1} + 3 - 1 \\
&= 3^{(3^3+1)} + 3^{3+1} + 2
\end{aligned}
$$

Suites de Goodstein: un exemple

$$
\begin{aligned}
42 &= 2^5 + 2^3 + 2 \\
&= 2^{(2^2+1)} + 2^{2+1} + 2 \\
\bullet \quad &\quad 3^{(3^3+1)} + 3^{3+1} + 3 - 1 \\
&= 3^{(3^3+1)} + 3^{3+1} + 2 \\
\bullet \quad &\quad 4^{(4^4+1)} + 4^{4+1} + 1
\end{aligned}
$$

Suites de Goodstein: un exemple

$$
\begin{aligned}
42 &= 2^5 + 2^3 + 2 \\
&= 2^{(2^2+1)} + 2^{2+1} + 2 \\
\bullet \quad &\quad 3^{(3^3+1)} + 3^{3+1} + 3 - 1 \\
&= 3^{(3^3+1)} + 3^{3+1} + 2 \\
\bullet \quad &\quad 4^{(4^4+1)} + 4^{4+1} + 1 \\
\bullet \quad &\quad 5^{(5^5+1)} + 5^{5+1}
\end{aligned}
$$

- $$\begin{aligned} & 6^{(6^6+1)} + 6^{6+1} - 1 \\ = \quad & 6^{(6^6+1)} + 6^6 \times 5 + \\ & 6^5 \times 5 + 6^4 \times 5 + \cdots + 6 \times 5 + 5 \end{aligned}$$

  (120607 chiffres binaires)

- $6^{(6^6+1)} + 6^{6+1} - 1$

  $= 6^{(6^6+1)} + 6^6 \times 5 +$

  $6^5 \times 5 + 6^4 \times 5 + \cdots + 6 \times 5 + 5$

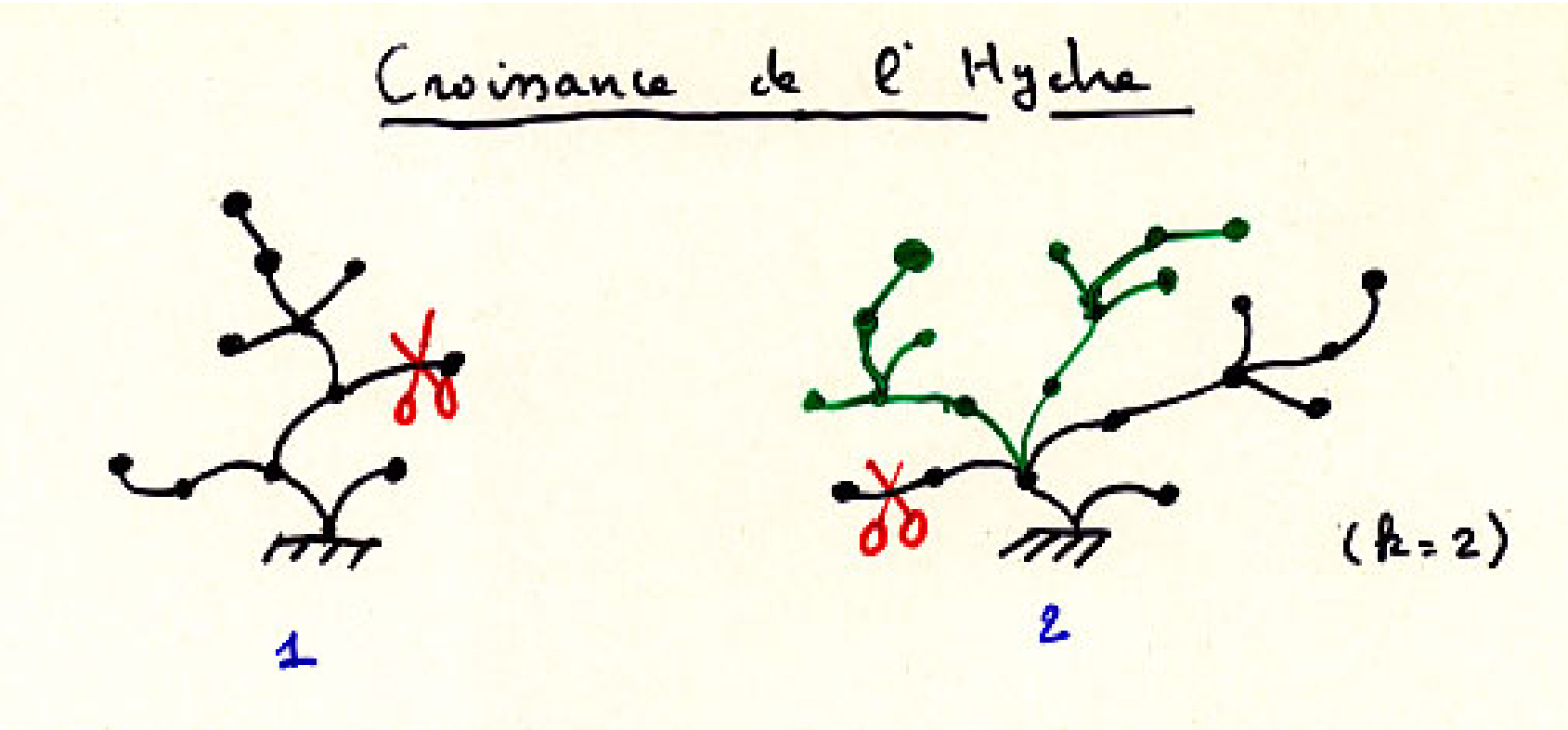
  (120607 chiffres binaires)

  $\ldots$

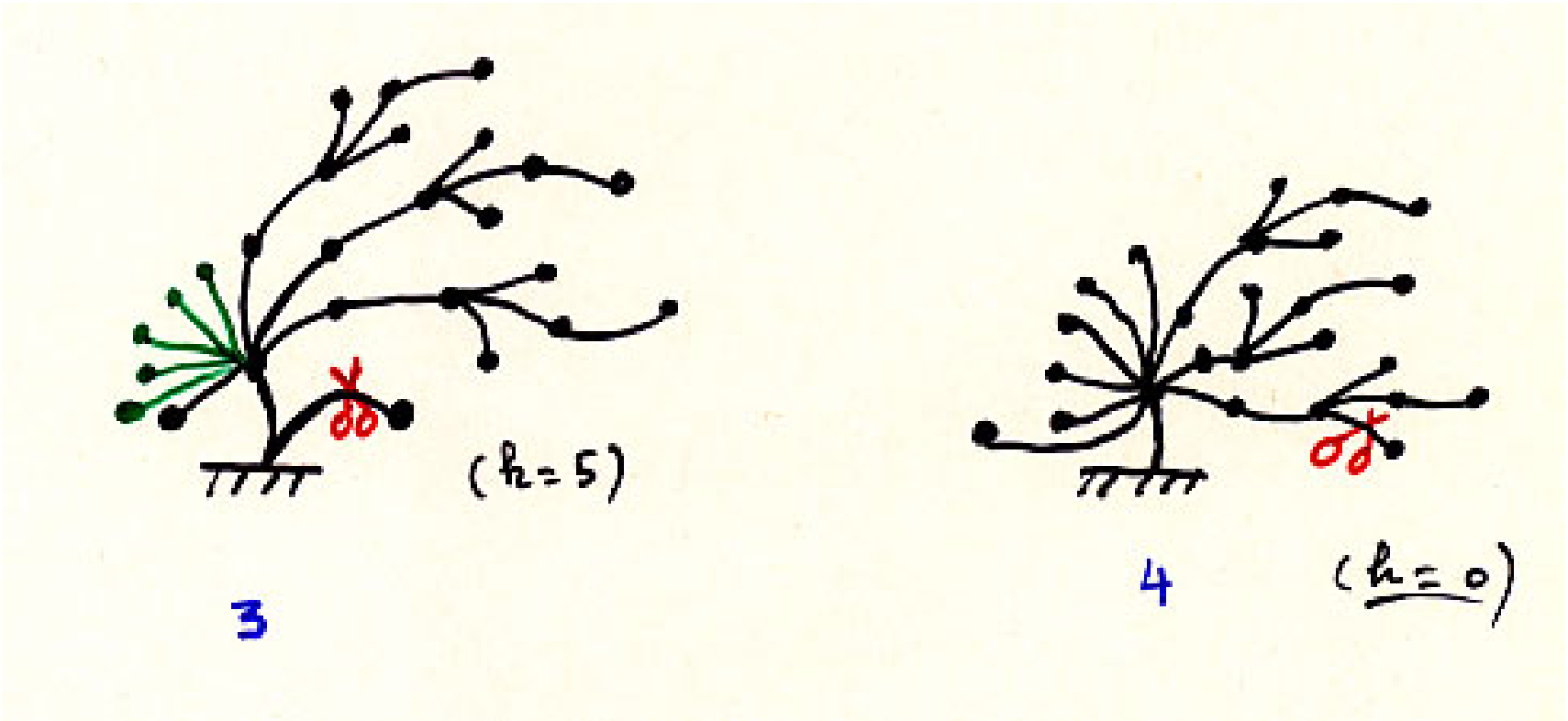
- $11^{(11^{11}+1)} + 11^{11} \times 5 +$

  $11^5 \times 5 + 11^4 \times 5 + \cdots + 11 \times 5$

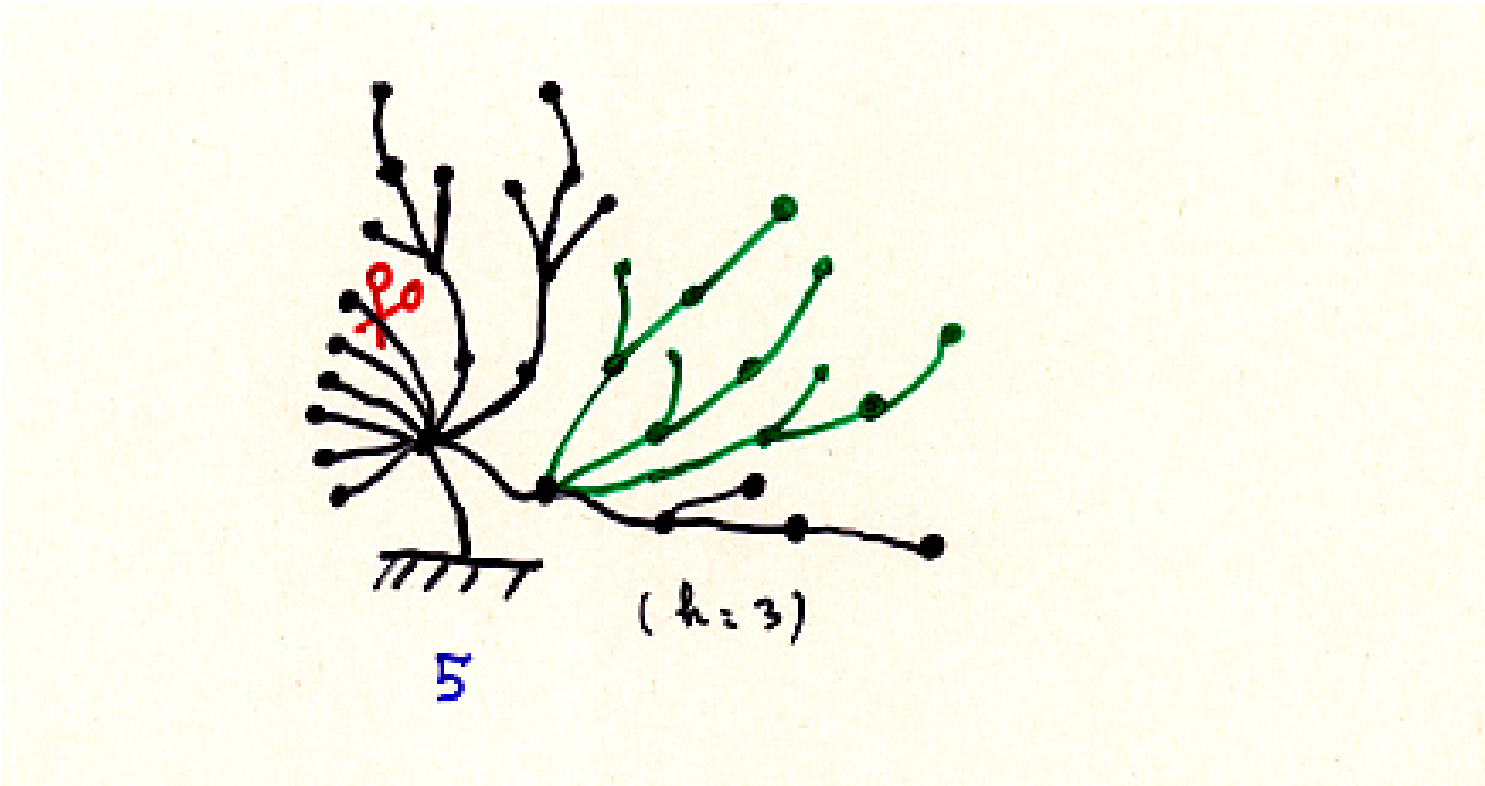
Hercule et l'Hydre



Hercule et l'Hydre (suite)



Hercule et l'Hydre (suite)



Résultats (Kirby et Paris)

1. La suite de Goodstein issue de 4 a pour longueur $3 \times 2^{402653211} - 1$ (vérifié en *Coq*)
2. Toute suite de Goodstein finit par atteindre 0 (vérifié en *Coq*)
3. Quelques soient les stratégies (récursives) de l'Hydre et d'Hercule, ce dernier finit par vaincre le monstre (vérifié en *Coq*)
4. Ces résultats ne peuvent pas être montrés dans l'arithmétique de Peano

Structure des preuves de terminaison

Les deux preuves de terminaison (suites de Goodstein et batailles d'hydre) utilisent les ordinaux inférieurs à ϵ_0.

- Bibliothèque sur l'ordinal ϵ_0,
- Attribution d'une mesure adaptée à ces problèmes de terminaison,
- Preuve que cette mesure décroît strictement à chaque étape,

Bibliothèque sur les notations d'ordinaux

- Termes pour les ordinaux $< \epsilon_0$ (Γ_0, etc.)
- Notion de forme normale
- Ordre linéaire (décidable)
- Preuve de bonne fondation (pour ϵ_0)
- Ordre sur les multi-ensembles (pour ϵ_0)
- Arithmétique ($+$, $-$, $\times$, $\hat{}$)

Forme normale de Cantor

On peut représenter tous les ordinaux inférieurs à (*i.e.* éléments de) ϵ_0 à l'aide de la forme normale de Cantor:

$$\begin{aligned} \alpha &= \omega^{\alpha_1} \times n_1 + \omega^{\alpha_2} \times n_2 + \ldots \omega^{\alpha_p} \times n_p \\ \text{avec} \quad & \alpha > \alpha_1 > \alpha_2 > \cdots > \alpha_p \\ & n_i > 0 \end{aligned}$$

On représente $\omega^\alpha \times (n+1) + \beta$ par cons α n β.

```
Inductive T1 : Set :=
| cons : T1 → nat → T1 → T1
| zero : T1.
```

Ordre sur T1, formes normales

```
zero < cons a n b
a < a' →  cons a n b < cons a' n' b'
n < n' →  cons a n b < cons a n' b'
b < b' →  cons a n b < cons a n b'
```

```
nf zero
nf a →  nf (cons a n zero)
a' < a →  nf a →  nf(cons a' n' b)→
          nf(cons a n (cons a' n' b)).
```

Bonne fondation d'ϵ_0

La restriction de $<$ aux termes en forme normale est bien fondée. Notons que ce résultat ne peut se prouver par une simple induction structurelle, genre:

- 0 est accessible
- Soient α et β accessibles, et o=cons α n β en forme normale. Montrons que o est accessible.

L'hypothèse de récurrence est inexploitable (o a des antécédents de la forme cons α' n' β', avec $\beta \leq \alpha'$ et $\beta \leq \beta'$).

La triple induction

Lemme :

$$\forall \alpha,\ \mathrm{Acc}(\alpha) \Rightarrow \mathit{nf}(\alpha) \Rightarrow \underbrace{\forall n\ \beta,\ \mathit{nf}(\beta) \Rightarrow \beta < \omega^{\alpha} \Rightarrow \mathrm{Acc}(\mathtt{cons}\ \alpha\ n\ \beta)}_{Q(\alpha)}$$

Preuve (par récurrence sur l'accessibilité de α): Soit α accessible et en forme normale, tel que

$$\forall \alpha', \mathit{nf}(\alpha') \Rightarrow \alpha' < \alpha \Rightarrow Q(\alpha')$$

(1) Pour tout β en forme normale tel que $\beta < \omega^{\alpha}$, on a $\mathrm{Acc}(\beta)$. (En effet β s'écrit sous la forme $\mathtt{cons}\ \alpha'\ n'\ \beta'$, avec $\beta' < \omega^{\alpha'}$ et $\alpha' < \alpha$.)

La triple induction

Lemme :

$$\forall \alpha,\ \mathrm{Acc}(\alpha) \Rightarrow \mathit{nf}(\alpha) \Rightarrow \underbrace{\forall n\ \beta,\ \mathit{nf}(\beta) \Rightarrow \beta < \omega^{\alpha} \Rightarrow \mathrm{Acc}(\mathtt{cons}\ \alpha\ n\ \beta)}_{Q(\alpha)}$$

Preuve (par récurrence sur l'accessibilité de α): Soit α accessible et en forme normale, tel que

$$\forall \alpha', \mathit{nf}(\alpha') \Rightarrow \alpha' < \alpha \Rightarrow Q(\alpha')$$

(2) On finit la preuve du lemme (par récurrence sur n et sur l'accessibilité de β fraîchement établie.)

Un schéma utile (Yves Bertot)

```
(∀ x y z,
  (∀ t, RA t x →
      ∀ y' z', Acc RB y' → Acc RC z' → P t y' z') →
  (∀ t, RB t y → ∀ z', Acc RC z' → P x t z') →
  (∀ t, RC t z → P x y t) →
      P x y z) →
∀ x y z, Acc RA x →  Acc RB y →  Acc RC z →
   P x y z.
```

Application à $P\ \alpha\ n\ \beta\ = \mathrm{Acc}(\mathrm{cons}\ \alpha\ n\ \beta)$.

La triple induction (fin)

On termine la preuve par récurrence structurelle:

- zero est trivialement accessible,
- Le lemme précédent permet de montrer que si α et β sont accessibles, et si `cons` α n β est en forme normale, alors ce dernier terme est accessible. Notons que l'accessibilité de β est "reprouvée" dans le lemme.

Conséquences On obtient la récurrence et la récursion transfinies.

Réminiscences Cette preuve rappelle par sa structure la preuve de normalisation forte du λ-calcul simplement typé (termes réductibles). Voir aussi les preuves de terminaison des *po.

Toute suite de Goodstein est finie

On associe à tout item de la suite de Goodstein un ordinal (inférieur à ϵ_0) tel que cette suite est strictement décroissante.

$$
\begin{array}{cc}
2 & \omega^3 = \omega^{\omega+1} \\
3 & \omega^\omega \times 2 + \omega^2 \times 2 + \omega \times 2 + 2 \\
4 & \omega^\omega \times 2 + \omega^2 \times 2 + \omega \times 2 + 1 \\
5 & \omega^\omega \times 2 + \omega^2 \times 2 + \omega \times 2 \\
\multicolumn{2}{c}{\dots} \\
N & \omega^\omega \times 2 \\
N+1 & \omega^\omega + \sum_{i=N}^{0} \omega^i \times N
\end{array}
$$

Preuve de la victoire d'Hercule

On associe à toute Hydre H un ordinal $o(H) < \epsilon_0$:

- A toute tête est associé 0
- A toute hydre de la forme $\bullet(H_1, H_2, \ldots, H_n)$, on associe la somme naturelle (associative, commutative et strictement monotone) $\omega^{o(H1)} \oplus \omega^{o(H_2)} \ldots \oplus \omega^{o(H_n)}$.

On prouve que $o(H)$ décroît strictement à chaque étape. Cette preuve utilise des multi-ensembles d'ordinaux.

Γ_0

```
Inductive T2 : Set :=
  zero : T2
| cons : T2 → T2  → nat → T2 → T2.
```

Abréviations :

$$\begin{aligned} \psi(\alpha, \beta) &= \text{cons } \alpha \ \beta \ 0 \ \text{zero} \\ \epsilon_\alpha &= \psi(\psi(\text{zero}, \text{zero}), \alpha) \end{aligned}$$

ordre sur T2

1: $\texttt{zero} < \texttt{cons}\ \alpha\ \beta\ n\ \gamma$

2: $\gamma < \gamma' \rightarrow$
$\texttt{cons}\ \alpha\ \beta\ n\ \gamma < \texttt{cons}\ \alpha\ \beta\ n\ \gamma'$

3: $\beta < \beta' \rightarrow$
$\texttt{cons}\ \alpha\ \beta\ n\ \gamma < \texttt{cons}\ \alpha\ \beta'\ n'\ \gamma'$

4: $\texttt{n} < n' \rightarrow$
$\texttt{cons}\ \alpha\ \beta\ n\ \gamma < \texttt{cons}\ \alpha\ \beta\ n'\ \gamma'$

ordre sur T2 (suite)

5: α < α' $\rightarrow$
β < cons α' β' 0 zero $\rightarrow$
cons α β n γ < cons α' β' n' γ'

6: α' < α $\rightarrow$
cons α β 0 zero < β' $\rightarrow$
cons α β n γ < cons α' β' n' γ'

7: α' < α $\rightarrow$
cons α β n γ < cons α' (cons α β 0 zero) n' γ'

- ordre linéaire, décidable ((Longue) preuve en *Coq*)
- bonne fondation : à faire.

Travail à faire

- Extension de la bibliothèque à Γ_0 (partiellement réalisée), Λ, etc.
- Lien avec les outils utilisant des ordres récursifs de chemins:
  - Goodstein (preuve par *po)
  - Hydre (preuve par *po)
  - ϵ_0, Γ_n, Λ, etc ...
- structure de ces preuves de terminaison (inductions)
- semi?-automatisation des calculs
- ordres de terminaison?
- preuve de Kirby et Paris?

Coq et le langage mathématique

Cette partie du travail en cours s'attache à l'écriture de types les plus conformes possible à l'écriture mathématique usuelle (pour faciliter la compréhension des énoncés de theorèmes et spécifications de programmes).

Problèmes rencontrés:

- fonctions partielles,
- définitions interactives de fonctions compliquées,
- définitions "inductives" rejetées par *Coq*

Exemples

```
Parameter sup : ∀ A (X:Ensemble A), denumerable X → A.

Parameter denumerable_incl : ∀ A (X Y: Ensemble A),
   Included _ X Y → denumerable Y → denumerable X.

Lemma sup_mono : ∀ A (X Y: Ensemble A)
                 (H : denumerable Y)
                 (H0 :Included A X Y),
                 sup X (denumerable_incl H0 H) ≤
                 sup Y H.
```

Autres exemples

- “ Tout ensemble d'ordinaux $X \subseteq \mathbb{O}$ a une unique fonction d'énumération (*i.e.* une bijection d'un segment initial de $\mathbb{O}$ vers X) ”
- “ On définit $+\alpha$ comme la fonction d'énumération de l'ensemble des ordinaux $\geq \alpha$”
- “ Si α est un ordinal, on définit l'ensemble $\mathrm{Cr}(\alpha)$ par
  - $\mathrm{Cr}(0)$ est l'ensemble des “additifs principaux”
  - si $0 < \alpha$, alors $\mathrm{Cr}(\alpha)$ est l'ensemble des ordinaux points-fixes communs à toutes les fonctions d'énumération des $\mathrm{Cr}(\beta)$ pour $\beta < \alpha$ ”

Travail en cours

- Bibliothèque autour de l'opérateur ϵ de Hilbert:
  - Exemple:

```
Definition pred (n:nat) :=
  epsilon inh_nat (fun p ⇒ p+1 = n)

Lemma pred_lt : ∀ n, 0 < n → pred n < n.
```

  - Opérateur de description (ι)
  - Tactiques d'élimination, de réécriture (avec l'opérateur de description)
  - Étude des problèmes posés par la déclaration d'ϵ et son axiomatisation : logique classique, prédicativité, etc.

Influence d'epsilon sur la logique

- A partir d'ϵ on peut dériver $(A \to B) \vee (B \to A)$ pour toutes propositions A et B, d'où : $\sim A \vee \sim\sim A$,
- Si on déclare ϵ extensionnel:

$$\frac{\forall a, P\ a \Leftrightarrow Q\ a \quad \exists a, P\ a}{\epsilon_P = \epsilon_Q}$$

  Alors on a le tiers exclu (`or` et `sumbool`),
- Avec `-impredicative-set`, on dérive $2 = 3$.

Légère adaptation de la récursion à la Balaa-Bertot aux fonctions partielles:

- `cr_fun :`
  `∀ α : OT,`
  `(∀ β : OT, β < α → Ensemble OT) →`
  `ordinal α → Ensemble OT`

- `Definition critical :`
  `∀ α, (ordinal α) → Ensemble OT :=`
  `OFix (fun (_:OT) => Ensemble OT) cr_fun`

- Preuve que cr_fun est extensionnelle:

$$(\forall\, x, f\, x = g\, x) \rightarrow \mathit{cr\_fun}\, f = \mathit{cr\_fun}\, g$$

- Equations de point fixe,
- Régles d'introduction, d'élimination
- Abréviation :

```
Definition Cr (α : OT) : Ensemble OT :=
    fun β ⇒ ∃ H: ordinal α, critical  H β.
```

- Preuves : exemple :

```
∀ α β, α ≤ β → Cr β ⊆ Cr α
```

Conclusions, directions de travail

- Comparaison de preuves de bonne fondations, mise en facteur?
- Degré d'automatisation des calculs sur les ordinaux,
- Ecriture de tactiques spécialisées,
- Spécifications “lisibles”.