Hydra Ludica : Une preuve d'impossibilité de prouver simplement

Pierre Castéran

Hydra Ludica : Une preuve d'impossibilité de prouver simplement *

Pierre Castéran

Univ. Bordeaux, LaBRI, CNRS, INP Bordeaux,
pierre.casteran@u-bordeaux.fr

Résumé

Les jeux d'hydre (aussi appelés batailles d'hydre), dus aux mathématiciens L. Kirby et J. Paris, forment un exemple de système de transitions dont la terminaison est difficile à démontrer. Cette difficulté de prouver est exprimée par ces auteurs sous forme d'un méta-théorème de l'arithmétique de Peano. Nous en présentons une adaptation en Coq sous forme d'une preuve d'impossibilité d'utiliser des relations bien fondées trop simples. Ce développement s'appuie sur une représentation finitaire des ordinaux inférieurs à ϵ_0 sous forme normale de Cantor.

1 Introduction

Les preuves formelles d'impossibilité permettent de se pencher sur la structure des preuves, la pertinence d'hypothèses, et d'étudier la puissance d'expression d'un formalisme.

De nombreux exemples se trouvent en théorie des langages (application des lemmes d'itération [13]), en algorithmique distribuée [3, 1, 6], etc. Ces preuves partagent fréquemment la même structure : une preuve par l'absurde, où l'hypothèse d'une solution à un problème donné permet de construire un contre-exemple. Dans le cas d'un langage formel dont on veut prouver la non-reconnaissabilité, un lemme d'itération permet, à partir d'un hypothétique automate reconnaissant ce langage, de construire un mot accepté par l'automate mais en dehors du langage considéré. De la même façon, prouver qu'une classe de systèmes de calculs locaux ne peut pas résoudre le problème de l'élection se fait en construisant, pour tout algorithme de cette classe, un graphe et une exécution désignant deux sommets élus de ce graphe au lieu d'un seul. Nous nous intéressons dans cet article à une espèce particulière de preuve d'impossibilité : la non-existence de preuves simples d'un théorème donné.

En 1982, les mathématiciens Laurie Kirby et Jeff Paris ont publié un article [10] contenant entre autres :

1. La description d'un jeu mathématique : le combat d'Hercule contre l'hydre. La particularité d'une bataille d'hydre est que ce monstre a la capacité d'augmenter de taille à chaque round. À l'instar des suites de Goodstein, étudiées dans le même article, les batailles d'hydres peuvent avoir une durée qui dépasse notre intuition.
2. La preuve d'un théorème *a priori* surprenant : Hercule gagne toujours contre l'hydre. L'adaptation en Coq de cette preuve se trouve dans la contribution sur les notations d'ordinaux [5].
3. Un second théorème établissant que la preuve du premier théorème ne *peut pas* être simple. L'objet de cet article est la mécanisation de ce résultat.

*Ce travail a bénéficié de l'aide des projets ANR Impex et ESTATE

Dans une première partie, nous rappelons les règles des jeux d'hydre, ainsi que la preuve de leur terminaison. Puis nous montrons comment formaliser avec les constructions de Coq une version faible du second théorème de Kirby et Paris. Enfin, nous discutons des prolongements possibles de ce développement.

2 Hydres et batailles d'hydre

Définition 1. *Une* hydre *est un monstre mythologique en forme d'arbre à branchement fini. Nous appelons* tête *toute feuille de l'arbre, et* pied *la racine de cet arbre. La longueur de la suite d'arêtes menant du pied à un sommet est appelée* hauteur *de ce sommet.*

La partie gauche de la figure 1 représente une hydre de hauteur 4 et comportant 5 têtes.

2.1 Règles du jeu

Un jeu d'hydre se joue à deux joueurs, Hercule et l'hydre, sous la forme d'une suite de *tours*, *reprises*, ou encore *rounds* [1]. Le jeu se termine par la victoire d'Hercule lorsque l'hydre est réduite à une tête.

À chaque tour, Hercule coupe une tête de l'hydre :

1. Si cette tête est de hauteur 1, aucune réaction.
2. Si la tête est de hauteur ≥ 2 :
   (a) On considère le sous-arbre issu du grand-père de la tête coupée (sur les dessins, la partie de l'hydre dont les têtes sont tristes).
   (b) Soit i un entier naturel. On ajoute i copies de cette sous-hydre à la même place ; l'entier i est appelé *facteur de réplication* du tour considéré.

Remarquons, que, si un sommet de l'hydre a un seul fils réduit à une tête, et que celle-ci est coupée, alors ce sommet devient à son tour une tête.

Les figures de 1 à 3 représentent le début d'un combat. L'emplacement d'où une tête a été enlevée est représenté par une arête en pointillé. Au premier tour, une tête de hauteur 1 est coupée, et l'hydre ne réagit pas. Au deuxième tour, l'hydre ajoute 4 copies de la zone blessée. Le facteur de réplication au troisième tour est de 2. Il est clair que l'hydre n'augmente jamais de hauteur lors d'un combat ; en revanche, sa taille peut devenir très grande.

FIGURE 1 – Premier tour d'une bataille

1. Ce mot d'origine anglaise est tout à fait admis en français. Nous utiliserons indifféremment ces trois mots dans cet article.

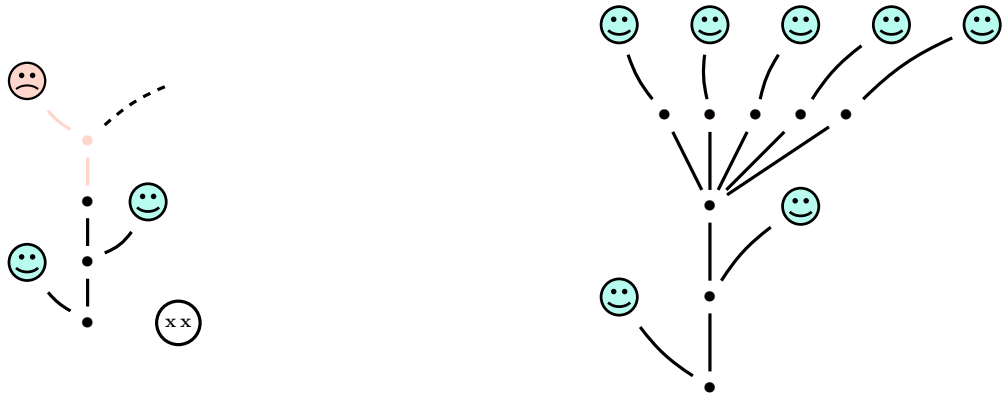

FIGURE 2 – Le deuxième tour

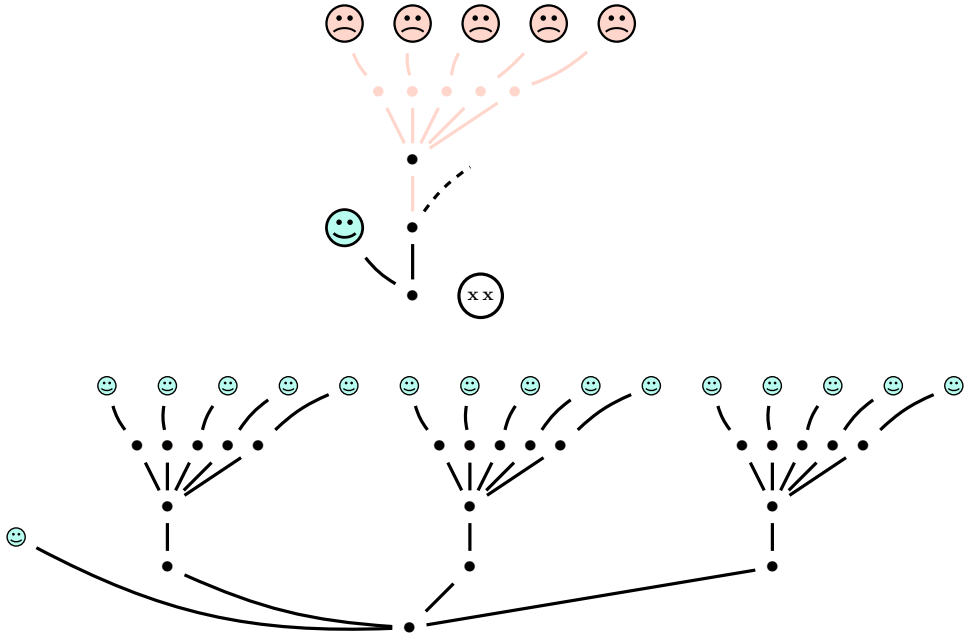

FIGURE 3 – Troisième reprise

Un combat peut durer *très* longtemps : considérons la petite hydre de la figure 4, et supposons qu'Hercule choisit toujours de couper la tête la plus à droite parmi les plus basses, et qu'au i-ème tour, le facteur de réplication soit de i. Alors, par comparaison avec la suite de Goodstein [10, 5] issue de 4, nous pouvons prouver que la bataille prendra plus de $3 \times 2^{402653211} - 1$ tours.

2.2 Le théorème de terminaison

L'article de Kirby et Paris de 1982 contient une preuve d'un théorème a priori étonnant.

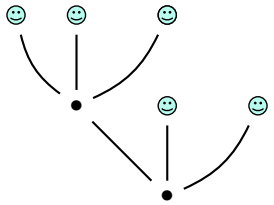

FIGURE 4 – L'hydre associée à la suite de Goodstein issue de 4

Théorème 1. *Quelles que soient les stratégies d'Hercule (choix d'une tête) et de l'hydre (choix du nombre de réplications), Hercule finit par gagner.*

2.2.1 Rappels sur les nombres ordinaux

La preuve du théorème 1 utilise les *nombres ordinaux*. Du point de vue mathématique, un ordinal est un représentant d'une classe d'équivalence (pour l'isomorphisme d'ordres) de relations d'ordre strict, totales et bien fondées. D'un point de vue ensembliste, un ordinal α est un ensemble dont les éléments sont les ordinaux strictement inférieurs à α. La relation $<$ sur les ordinaux est bien fondée, et l'ordre large $\leq$ associé est total.

Un ordinal α est un *ordinal successeur* s'il existe un ordinal β tel que α est le plus petit ordinal strictement supérieur à β. Un ordinal λ est un *ordinal limite* s'il est la borne supérieure d'une suite strictement croissante d'ordinaux.

Un ordinal est soit 0, soit un ordinal limite, soit un ordinal successeur. Cette division en cas, ainsi que la tactique de preuve par récurrence bien-fondée (aussi appelée *récurrence transfinie*) structurent de nombreuses preuves sur les ordinaux.

Par respect de la tradition, les ordinaux seront appelés α, β, γ, etc. On réservera la méta-variable λ aux ordinaux limites.

Le premier ordinal infini est l'ordinal limite ω. L'ordinal ϵ_0 est le premier ordinal α vérifiant l'égalité $\alpha = \omega^\alpha$. Certains ordinaux dénombrables : ω, ω^2, ω^ω, ϵ_0, Γ_0, ont une représentation sous forme de termes finis permettant le calcul et rendant la comparaison décidable. Dans cet article nous utilisons la *forme normale de Cantor* pour représenter l'ensemble des ordinaux inférieurs à ϵ_0. Sauf mention contraire, tous les ordinaux mentionnés dans cet article seront inférieurs à ϵ_0.

2.2.2 Structure de la preuve du théorème de terminaison

La preuve de terminaison de toute bataille d'hydre de [10] s'articule de la façon suivante :

1. On considère une *mesure* associant à toute hydre h un ordinal inférieur à ϵ_0. Cette mesure est définie récursivement de la façon suivante :
   — Si h est une tête, alors $m(h) = 0$
   — Si h est formée d'un pied et des sous-hydres $h_1, h_2, \ldots, h_n$, alors

   $$m(h) = \omega^{m(h_1)} \oplus \omega^{m(h_2)} \oplus \cdots \oplus \omega^{m(h_n)}$$

   où $\oplus$ est la somme commutative et strictement monotone d'ordinaux, appelée *somme d'Hessenberg* ou *somme naturelle*.
2. On prouve que, si h se transforme en h' en un round, alors $m(h') < m(h)$.

3. L'ordre $<$ sur les ordinaux étant bien fondé, on en déduit que toute bataille est finie. De par les règles vues en 2.1, toute bataille se termine forcément par la victoire d'Hercule.

L'article de N. Dershowitz et G. Moser « The Hydra Battle Revisited » [7] décrit de façon très complète les preuves à propos des batailles d'hydre. Il cite également une classe de batailles d'hydres plus vaste, où les hydres peuvent augmenter de hauteur, tout en garantissant la terminaison de toutes les batailles, prouvée grâce à l'ordinal Γ_0.

L'article de Will Sladek « The Termite and the Tower » [16] propose quelques explications très lisibles sur une preuve très similaire : la terminaison des suites de Goodstein, et l'utilisation des ordinaux dans cette preuve.

2.3 Preuve en Coq du théorème de terminaison

La preuve de terminaison de toutes les batailles d'hydre fait partie d'une contribution écrite avec Évelyne Contejean [5]. Cette preuve contient une partie générique sur les notations d'ordinaux, notamment la forme normale de Cantor. Tout ordinal inférieur à ϵ_0 est représenté par un terme fini d'un type inductif appelé `T1`, repris de la bibliothèque écrite par P. Manolios et D. Vroon pour ACL2 [11].

```
(** * Cantor "pre" Normal form
     After Manolios and Vroon's work on ACL2

T1 is the type of terms used for representing Cantor normal form.
The term (ocons a n b) is intended to represent the ordinal
omega^a * (S n)  + b
*)

Inductive T1 : Set  :=
| zero : T1
| ocons : T1 -> nat -> T1 -> T1.
```

Sur ce type, nous définissons un ordre bien fondé et les opérations usuelles : somme, produit, exponentiation de base ω. La somme d'Hessenberg ne fait pas partie de la contribution de 2006, mais a été ajoutée depuis pour simplifier nos preuves.

Les hydres sont représentées comme des arbres dont chaque sommet possède un nombre fini mais quelconque de fils. Dans la définition suivante, les types `Hydra` et `Hydrae` sont respectivement associés aux hydres et aux suites finies d'hydres :

```
Inductive Hydra : Set :=
| node :  Hydrae -> Hydra
with Hydrae : Set :=
| hnil : Hydrae
| hcons : Hydra -> Hydrae -> Hydrae.

Notation head := (node hnil).
```

2.3.1 Représentation des règles de combat

Notre formalisation des règles de bataille d'hydre se fait sous la forme d'une relation binaire sur le type `Hydra` exprimant la transformation associée à chaque reprise. Soit $i \geq 0$, on note $h \underset{i}{\longrightarrow} h'$ la transformation de h en h' telle que :

— soit la tête coupée est de hauteur 1 et la valeur de i est non pertinente,
— soit cette tête est de hauteur ≥ 2 et i est le facteur de réplication associé.

Dans nos preuves, nous utiliserons quelques relations définies à partir de $\underset{i}{\longrightarrow}$:

$\longrightarrow$ (`-1->` dans les scripts Coq) : oubli du paramètre i

$\overset{+}{\underset{i}{\longrightarrow}}$: fermeture transitive de $\underset{i}{\longrightarrow}$

$\overset{+}{\longrightarrow}$ (`-+->` dans les scripts Coq) : fermeture transitive de $\longrightarrow$

2.3.2 Preuve formelle de terminaison

La formalisation en Coq de la preuve de terminaison suit fidèlement la preuve mathématique de l'article de 1982. Nous en décrivons ci-dessous la structure principale :

— Bibliothèque sur les formes normales de Cantor. La bonne fondation de l'ordre sur les ordinaux est prouvée de façon directe (preuve d'accessibilité) mais aussi de façon beaucoup plus concise en appliquant un développement d'Évelyne Contejean sur l'ordre récursif des chemins (*r.p.o.*)
— Définition et propriétés de la somme d'Hessenberg.
— Description des jeux d'hydre et preuve de terminaison proprement dite.

Cette preuve prend plus de 4500 lignes de script Coq. Remarquons que les deux premières parties sont génériques et seule la troisième concerne les hydres. Il est cependant naturel de se demander si toute cette complexité est nécessaire pour prouver ce théorème de terminaison. L'article de Kirby et Paris apporte la réponse suivante :

Théorème 2. *La terminaison de toutes les batailles d'hydre ne peut pas se prouver dans l'arithmétique de Peano.*

3 Le théorème d'impossibilité

Le théorème 2 est un très beau résultat, mais dont l'énoncé pourrait ne pas trop parler à l'utilisateur de Coq, habitué à l'ordre supérieur et peu disposé à accepter des restrictions sur les règles logiques à utiliser. Nous proposons alors l'énoncé suivant, qui explicite la nécessité de considérer l'ordinal ϵ_0 dans la preuve de terminaison :

Théorème 3. *Soit α un ordinal strictement inférieur à ϵ_0 ; la terminaison de toutes les batailles d'hydre ne peut pas se prouver à l'aide d'une mesure des hydres vers l'intervalle $[0, \alpha[$.*

Notation Pour abréger les énoncés, nous noterons $P(\alpha)$ la propriété énoncée par le théorème 3.

Définition 2. *Par la suite, nous appellerons* variant *toute mesure vers un ensemble bien fondé qui décroit strictement à chaque reprise.*

3.1 Le cas de l'ordinal ω^2

La preuve du théorème 3 pour $\alpha < \epsilon_0$ quelconque est assez technique. Aussi nous présentons d'abord le cas $\alpha = \omega^2$, beaucoup plus simple, mais qui possède la même structure globale de preuve que le cas général, notamment la distinction entre ordinaux zéro, successeurs et limites.

L'ordinal ω^2, vu comme ensemble, est représenté par le produit cartésien $\mathbb{N} \times \mathbb{N}$ muni de l'ordre lexicographique usuel. L'ordinal $\omega \times i + j$ est alors représenté par le couple d'entiers (i, j). Les couples de la forme $(i, 0)$ $(i > 0)$ représentent les ordinaux limites, et les couples (i, j) $(j > 0)$ les ordinaux successeurs.

Notre preuve de $P(\omega^2)$ possède la structure suivante :

1. On plonge ω^2 dans l'ensemble des hydres par la fonction ι qui à tout couple (i, j) associe l'hydre composée de i tentacules de longueur 2 et j tentacules de longueur 1. Par exemple, la figure 5 représente l'hydre $\iota(3, 5)$.
2. On prouve, pour *n'importe quel variant m à valeur dans ω^2*, l'inégalité : $\forall \beta < \omega^2,\ \beta \leq m(\iota(\beta))$.
   La preuve se fait par récurrence bien-fondée sur ω^2 :
   Soit $\beta = (i, j)$ tel que l'inégalité ci-dessus est vérifiée pour tout couple strictement inférieur à β.
   — Si $\beta = (0, 0)$, l'inégalité est triviale.
   — Si $j > 0$, alors l'hydre $\iota(i, j)$ se tranforme en un round en $\iota(i, j - 1)$ (par perte d'une tête). Comme m est un variant, nous avons $m(\iota(i, j)) > m(\iota(i, j - 1))$, d'où $m(\iota(i, j)) > (i, j - 1)$ (par hypothèse de récurrence), et donc $m(\iota(i, j)) \geq (i, j)$.
   — Si $i > 0$ et $j = 0$, alors $(i, 0)$ est la limite de la suite $(i - 1, k)$ $(k \in \mathbb{N})$.
   Il suffit alors de montrer que $m(\iota(i, 0))$ est strictement supérieur à $(i-1, k)$ pour tout k. Or pour tout k, il suffit d'un round pour transformer l'hydre $\iota(i, 0)$ en $\iota(i - 1, k)$. Comme m est un variant, et par hypothèse de récurrence, nous avons $m(\iota(i, 0)) > m(\iota(i - 1, k)) \geq (i - 1, k)$ pour tout k. Par passage à la limite, nous obtenons enfin $m(\iota(i, 0)) \geq (i, 0)$.
3. Considérons l'hydre h_{ω^2} de la figure 6. Sa mesure $m(h_{\omega^2})$ est un couple (i, j). En deux reprises, h_{ω^2} se transforme en $\iota(i, j)$: dans un premier temps, nous obtenons une hydre avec $i + 1$ tentacules de longueur 2. Au round suivant, on remplace le plus à droite de ces tentacules par j tentacules de longueur 1. Pour tout variant m, on aura alors $m(h_{\omega^2}) > m(\iota(i, j)) = m(\iota(m(h_{\omega^2})))$.
4. En appliquant les deux étapes précédentes, nous obtenons l'inégalité suivante qui contredit l'irréflexivité de l'ordre strict $>$ sur ω^2 :

$$m(h_{\omega^2}) > m(\iota(m(h_{\omega^2}))) \geq m(h_{\omega^2})$$

3.2 Un schéma de preuve générique

Afin de mettre en valeur la structure de notre preuve d'impossibilité, indépendamment des propriétés spécifiques de tel ou tel ordinal α, nous abstrayons cette structure par une classe paramétrée par le type du variant considéré. En premier lieu, nous associons une classe à la notion de variant bien fondé. Soit une relation $<$ sur un type t. Toute instance de la classe suivante prouve la bonne fondation de $\longrightarrow^{-1}$, et donc la terminaison de toutes les batailles d'hydre.

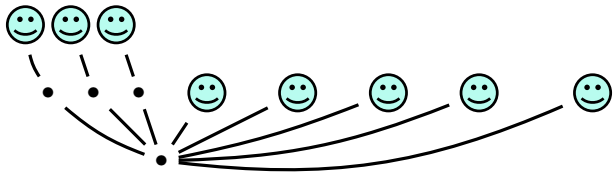

FIGURE 5 – L'hydre $\iota(3,5)$

FIGURE 6 – L'hydre h_{ω^2}

```
Class WfVariant (m: Hydra -> t) :=
  {
    wf : well_founded lt;
    decr : forall h h', h -1->  h' -> m h' < m h
  }.
```

Si l'on veut montrer qu'un ordre bien fondé $<$ ne permet pas de prouver la terminaison des batailles d'hydre, il suffit de montrer qu'il n'existe aucune instance de la classe `WfVariant` pour cet ordre. La classe suivante généralise la preuve de la section 3.1, et notamment l'usage de ses deux inégalités contradictoires.

```
Context (S: StrictOrder lt).
Infix "<" := lt.

Let le := clos_refl _ lt.
Infix "<=" := le.

Class TooSimple :=
 {
  iota : t -> Hydra;
  too_simple_1 :  forall m (V: WfVariant lt m) alpha,
                   alpha <= m (iota alpha);
  h: Hydra;
  too_simple_2 : forall m (V: WfVariant lt m),
                  h -+-> iota (m h)
  }.
```

Si l'on peut créer une instance de `TooSimple`, alors, pour tout variant m : `Hydra` $\to t$, on peut prouver $m(h) > m(\iota(m(h))) \geq m(h)$, et par conséquent `False`. La preuve de la section 3.1 est bien une instance de cette classe.

3.3 Preuve générale d'impossibilité

Nous avons alors à construire une instance de `TooSimple` pour le type $t = \{\beta : \texttt{T1} | \beta < \alpha\}$, où α est un ordinal quelconque strictement inférieur à ϵ_0. Nous donnons ci-dessous les étapes principales de cette preuve.

3.3.1 Plongement de $[0, \epsilon_0[$ dans `Hydra`

On définit récursivement une injection ι associant une hydre à tout ordinal $\beta < \epsilon_0$.

— $\iota(0) = \texttt{head}$

— Soit $\beta = \omega^{\beta_1} \times n_1 + \cdots + \omega^{\beta_p} \times n_p$ en forme normale de Cantor. Alors $\iota(\beta)$ est l'hydre formée d'un pied relié à n_1 copies de $\iota(\beta_1)$, ..., n_p copies de $\iota(\beta_p)$.

Par exemple, la figure 7 montre l'hydre associée à l'ordinal $\omega^{\omega+2} + \omega^\omega \times 2 + \omega + 1$.

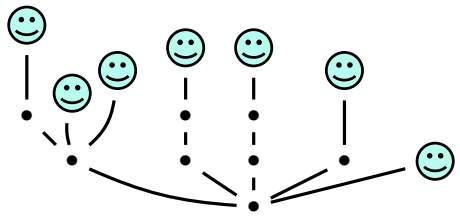

FIGURE 7 – L'hydre $\iota(\omega^{\omega+2} + \omega^\omega \times 2 + \omega + 1)$

3.3.2 La « machinerie » de Ketonen et Solovay

L'article de J. Ketonen et R. Solovay « Rapidly growing Ramsey functions » [9] est cité à l'appui des preuves de [10]. Une partie de cet article est consacrée à l'étude systématique de la relation $<$ sur l'intervalle $[0, \epsilon_0]$.

Les auteurs définissent la notion de « suite canonique ». Soit $\alpha < \epsilon_0$ un ordinal, et i un entier positif. On définit l'ordinal $\{\alpha\}(i)$ par récursion structurelle sur les formes normales de Cantor :

$$\begin{aligned}
\{0\}(i) &= 0 \\
\{\alpha+1\}(i) &= \alpha \\
\{\omega^{\beta+1}\}(i) &= \omega^\beta \times i \\
\{\omega^\lambda\}(i) &= \omega^{\{\lambda\}(i)} \quad (\lambda \textit{ ordinal limite}) \\
\{\omega^{\beta+1} \times n\}(i) &= \omega^{\beta+1} \times (n-1) + \omega^\beta \times i \quad (n \geq 2) \\
\{\omega^\lambda \times n\}(i) &= \omega^\lambda \times (n-1) + \omega^{\{\lambda\}(i)} \quad (n \geq 2,\ \lambda \textit{ ordinal limite}) \\
\{\omega^\alpha \times n + \beta\}(i) &= \omega^\alpha \times n + \{\beta\}(i) \quad (n \geq 1,\ 0 < \beta)
\end{aligned}$$

Notons que la définition ci-dessus diffère de celle, plus concise, de [9]. Notre définition, par sa récursion structurelle sur le type `T1`, simplifie le calcul des $\{\alpha\}(i)$ par l'évaluateur de Coq.

Par exemple, les égalités suivantes se prouvent par la simple tactique `reflexivity`.

$$\{\omega^\omega\}(4) = \omega^4 \qquad \{\omega^{\omega+2}\}(6) = \omega^{\omega+1} \times 6$$

.

L'intérêt des suites canoniques tient en les deux énoncés ci-dessous, prouvés dans [9].

Lemme 1. *Soit λ un ordinal limite. Alors λ est la limite de la suite strictement croissante $\{\lambda\}(i)$ $(i \in \mathbb{N})$.*

Théorème 4. *Soient deux ordinaux α et β tels que $\beta < \alpha < \epsilon_0$. Alors il existe un entier i et une suite d'ordinaux $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_n = \beta$ telle que $\alpha_{k+1} = \{\alpha_k\}(i)$ pour tout $k < n$.*

3.3.3 Fin de la preuve

La relation entre les suites canoniques et les batailles d'hydre fait l'objet du lemme suivant :

Lemme 2. *Soit $0 < \alpha < \epsilon_0$ et $i \geq 1$ un entier. Alors $\iota(\alpha)$ se transforme en un round en $\iota(\{\alpha\}(i))$. Par conséquent, si $\beta < \alpha < \epsilon_0$, alors il existe une bataille transformant $\iota(\alpha)$ en $\iota(\beta)$.*

La première partie de ce lemme se prouve en construisant un round où Hercule coupe la plus à droite des têtes les plus basses de l'hydre, et l'hydre réagit avec un facteur de réplication de $i - 1$. En second lieu, le théorème 4 nous permet de finir la preuve.

Nous avons désormais tous les ingrédients pour construire une preuve de $P(\alpha)$, avec $\alpha < \epsilon_0$ quelconque. Soit m un variant quelconque à valeurs dans le type $\{\beta : \texttt{T1} \mid \beta < \alpha\}$.

On prouve d'abord l'inégalité $m(\beta) \geq \beta$ pour tout $\beta < \alpha$. Comme pour le cas de ω^2, on procède par récurrence bien fondée sur β, en considérant les trois cas $\beta = 0$, β ordinal successeur, et β ordinal limite. Seul ce dernier cas est non-trivial :

1. β est la limite (borne supérieure) de la suite canonique $\{\beta\}(i)$ $(i \in \mathbb{N})$.
   (a) Soit donc $\gamma < \beta$. Il existe un indice i tel que $\gamma < \{\beta\}(i)$.
   (b) Par le lemme 2, l'hydre $\iota(\beta)$ se transforme en un round en $\iota(\{\beta\}(i))$.
   (c) Comme m est un variant, nous avons $m(\iota(\beta)) > m(\iota(\{\beta\}(i)))$.
   (d) Par l'hypothèse de récurrence, nous avons $m(\iota(\{\beta\}(i))) \geq \{\beta\}(i) > \gamma$, donc $m(\iota(\beta)) > \gamma$.
2. L'ordinal $m(\iota(\beta))$ est donc strictement supérieur à tout ordinal γ strictement inférieur à β. Comme l'ordre $\leq$ est total, nous en déduisons l'inégalité $m(\iota(\beta)) \geq \beta$.

Considérons l'hydre $h = \iota(\alpha)$. Il reste à prouver l'inégalité $m(h) > m(\iota(m(h)))$.

1. Par hypothèse sur m, $m(h)$ est strictement inférieur à α.
2. En appliquant le théorème 4 de Ketonen et Solovay, on décompose l'inégalite $m(h) < \alpha$ en une suite d'applications de la fonction $\{\_\}(i)$ pour un certain i. Mais par le lemme 2, à cette suite s'associe une bataille transformant l'hydre $h = \iota(\alpha)$ en l'hydre $\iota(m(h))$.

Nous pouvons donc construire une instance de `TooSimple` pour l'ordre sur $\{\beta : T1 \mid \beta < \alpha\}$ et par conséquent avons prouvé $P(\alpha)$.

3.3.4 Remarques

L'analyse de cette preuve montre qu'aucune hypothèse supplémentaire sur le variant m n'est nécessaire. Seule la structure (alternance d'ordinaux successeurs et de limites) des ordinaux inférieurs à ϵ_0, ainsi que la relation entre suites canoniques et rounds de bataille, sont utilisées.

Remarquons également le caractère « constructif » de cette preuve : étant donnés un ordinal α et un hypothétique variant m à valeurs dans $[0, \alpha[$, on peut construire une bataille où l'hydre $\iota(m(\alpha))$ se transforme en elle-même au bout d'un nombre non nul de reprises.

Comme pour la preuve de la section 3.1, le choix d'un facteur de réplication dans une bataille est contrôlé par le traitement des ordinaux limites. Pour un ordinal β donné, la preuve commence par l'introduction d'un ordinal $\gamma < \beta$ quelconque, et introduit une dépendance entre γ et un approximant $\{\beta\}(i)$ strictement supérieur à γ. C'est cet indice i qui sera utilisé dans le round transformant $\iota(\beta)$ en $\iota(\{\beta\}(i))$. Notre preuve construit bien une bataille d'hydre, mais sans qu'on puisse ajouter une contrainte de la forme « le facteur de réplication est toujours 42 », ou « le facteur de réplication augmente de 1 à chaque tour ».

Dans notre développement, la preuve du lemme 1 et du théorème 4 de [9] a demandé 1803 lignes de vernaculaire Coq, pour 3 pages de discours mathématique. Nous savons gré à J. Ketonen et R. Solovay d'avoir proposé un découpage en lemmes très détaillé qu'il a suffi de suivre. Beaucoup de nos lemmes sont juste des reformulations directes des énoncés de [9]. L'application des théorèmes de Ketonen et Solovay au problème spécifique des hydres nous a demandé 740 lignes supplémentaires.

Ce ne sont cependant pas des traductions mot à mot. Les auteurs de cet article sont des mathématiciens, raisonnant en termes d'ensembles. En revanche, nous travaillons sur une représentation d'ordinaux par des termes finis, et avons privilégié l'écriture de fonctions calculables par `Compute` ou faciles à extraire. Citons à titre d'exemple les suites canoniques, et la fonction qui associe à un ordinal limite λ et un ordinal $\beta < \lambda$, un indice i tel que $\beta < \{\lambda\}(i)$. Le fait de pouvoir tester ces fonctions nous a permis d'avoir une vision plus « concrète » des objets mathématiques impliqués.

Certains lemmes et définitions de [9] ont disparu de notre adaptation. Par exemple, les auteurs définissent une relation « α concorde avec β » utilisée comme condition de certains lemmes intermédiaires, et définie par « α et β sont en forme normale de Cantor, et tous les termes de β sont inférieurs ou égaux aux termes de α ». En fait, les schémas de récurrence créés auparavant dans [5] génèrent des buts où cette condition est automatiquement remplie. Nous avons donc une preuve complète du lemme 1 et du théorème 4 fortement inspirée de [9], mais compatible avec « l'esprit Coq ».

4 Perspectives

4.1 Représentations des ordinaux dans un assistant de preuve

Les ordinaux sont utiles pour la construction de preuves formelles de totalité de fonctions récursives. Parmi les formalisations existantes, on peut considérer l'utiisation de *notations d'ordinaux* représentant des ordinaux dénombrables comme ϵ_0, Γ_0 sous forme de termes finis permettant le calcul effectif d'expressions arithmétiques et la comparaison d'ordinaux par une fonction booléenne [11, 5, 8].

L'implémentation de ces opérations peut alors être validée en prouvant leur correction par rapport à une définition mathématique : définition axiomatique [4, 8] ou définition des ordinaux comme quotients de bons ordres pour la relation d'isomorphismes d'ordres [12].

Il serait intéressant, comme cela a été fait pour l'arithmétique dans la bibliothèque standard, de rendre compatibles tous ces modules en unifiant les noms de théorèmes, et tant que possible, en définissant des fonctions de traduction d'un formalisme vers l'autre. Par exemple, nous avons défini une « coercion » des ordinaux en forme normale de Cantor vers l'ensemble des ordinaux dénombrables au sens de Schütte. On peut alors disposer de plusieurs vues d'un même objet.

4.2 Étude des stratégies de l'hydre

Rappelons que les preuves des sections 3.1 et 3.3 construisent des batailles d'hydre dans lesquelles le facteur de réplication est quelconque à chaque étape : l'hydre doit pouvoir choisir ce nombre à chaque tour. Or, la lecture de l'article de Kirby et Paris suggère que nous pouvons prouver le théorème 3 en considérant des batailles où le nombre de réplications de l'hydre est *contrôlé*, le cas classique étant une augmentation de 1 à chaque reprise du combat. Il reste donc à prouver que, dans ce dernier cas, l'ordinal ϵ_0 reste le co-domaine de variant le plus simple pour la preuve de terminaison.

L'article de Ketonen et Solovay propose des outils mathématiques permettant d'étudier systématiquement les facteurs de réplications utilisés dans une bataille. Soient un ordinal $\alpha < \epsilon_0$ et une suite finie d'entiers strictement croissante $s = i_1 < i_2 < \cdots < i_n$. On calcule $\alpha_1 = \{\alpha\}(i_1), \ldots, \alpha_n = \{\alpha_{n-1}\}(i_n)$. La suite s est dite α-*grande* si $\alpha_n = 0$. Autrement dit, si l'hydre $\iota(\alpha)$ réagit avec les facteurs de réplication de la suite s et Hercule coupe toujours la tête la plus à droite parmi les plus basses [2], la bataille est terminée au bout de n reprises.

Notons que Ketonen et Solovay définissent plutôt une notion d'*ensemble* α-grand, mais dont l'énumération se fait toujours dans l'ordre croissant des éléments. Notre implémentation (encore très partielle) de cette notion en Coq a pu bénéficier des définitions et lemmes de la bibliothèque standard de Coq sur les listes triées. Dans ce cas encore, nos définitions peuvent s'écarter de celles de [9], mais les notions principales restent les mêmes.

Toujours en considérant la même stratégie d'Hercule, et si l'hydre $\iota(\alpha)$ réagit avec un facteur de réplication de i, puis $i+1, i+2, \ldots$, la fin de la bataille sera prévue pour le plus petit entier k tel que l'intervalle $[i, k]$ soit α-grand. La fonction F_α qui à i associe l'entier k est une fonction *à croissance rapide*. Les propriétés de ces fonctions sont étudiées dans [9] et servent à prouver le théorème 2 de [10] pour toute stratégie récursive de l'hydre. Notre projet est de prouver en Coq une version du théorème 3 pour cette stratégie, avec pour effet collatéral l'écriture de modules sur les « grands » ensembles et les fonctions à croissance rapide. Ces fonctions d'une complexité monstrueuse échappent totalement au test ; seule la preuve permet d'en capter les propriétés. L'article de S. Schmitz [14] présente un ensemble d'applications de ces fonctions à l'étude de la complexité.

2. Des expérimentations en OCaML nous ont persuadé que, dans la mesure ou l'hydre augmente strictement son nombre de réplications à chaque reprise, cette stratégie est la pire pour Hercule. Négliger les têtes les plus hautes les rend beaucoup plus dangereuses au fur et à mesure que le nombre de réplications augmente.

5 Conclusion

Les suites de Goodstein et les batailles d'hydre ont pour intérêt de pallier le caractère trop abstrait des preuves d'incomplétude à la Gödel. Montrer qu'un théorème donné n'est pas prouvable en arithmétique de Peano, ou nécessite l'ordinal ϵ_0 est plus « simple » que considérer la prouvabilité en général.

L'énoncé des deux théorèmes de Kirby et Paris — surtout le premier — est suffisamment simple pour être compris d'un large public. Nous avons utilisé les jeux d'hydre dans des cadres divers : l'opération *Maths en Jeans* pour un public lycéeen, un cours de programmation fonctionnelle en Licence d'Informatique. Par ailleurs, nombreux sont les sites offrant des animations de batailles d'hydre ; citons parmi ceux-ci la page d'Andrej Bauer [2]. Le premier théorème est déjà surprenant, et le second fournit des éléments d'analyse sur la difficulté de prouver. Ce dernier pourrait cependant ne pas étonner ceux/celles pour qui *toute* démonstration est difficile.

L'utilisation d'un système de notation d'ordinaux (forme normale de Cantor) nous a permis de rendre « concrètes » certaines notions liées aux ordinaux : comparaison, opérations arithmétiques, suites canoniques, implémentées sous forme de fonctions que l'utilisateur peut appliquer. Par exemple, si $\alpha < \lambda$ et λ est un ordinal limite, on peut définir une fonction qui calcule le i-ème ordinal strictement compris entre α et λ, pour toute valeur de i. La notion d'*infini potentiel* est bien capturée par la notion de fonction.

Enfin, l'adaptation du discours mathématique : omissions d'étapes "faciles", utilisation d'ensembles, etc., à l'univers de Coq : tactiques, types inductifs, etc., est en soi un sujet d'intérêt.

L'intérêt du travail présenté est profondément lié aux caractéristiques de Coq que nous souhaitons mettre en valeur : preuves par calcul, classes de types, etc. Cette notion de classe nous a permis de construire une famille de preuves indexée par un ordre bien fondé quelconque, et de raisonner sur la nécessaire complexité de cet ordre.

État actuel du développement Les preuves décrites dans cet article sont disponibles dans leur état actuel à l'adresse suivante : `http://www.labri.fr/perso/casteran/hydra-ludica/`.

Ce développement a été mis au point sous la version `V8.7` de Coq. Nous avons inclus une version modernisée de la contribution [5] ainsi que la présentation axiomatique des ordinaux dénombrables d'après Schütte [15]. Nous avons également débuté une formalisation des ensembles et suites α-grands. Une documentation de ce développement est en cours de rédaction et est disponible à l'adresse ci-dessus.

Remerciements L'auteur remercie vivement les relecteurs anonymes pour leurs nombreux commentaires sur une première version de cet article, ainsi que les membres de l'équipe « Méthodes Formelles » du LaBRI pour leurs remarques lors de présentations détaillées de ce travail.

Références

[1] C. Auger, Z. Bouzid, P. Courtieu, S. Tixeuil, and X. Urbain. Certified Impossibility Results for Byzantine-Tolerant Mobile Robots. In *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, volume 8255 of *LNCS*, page 15, Osaka, Japon, November 2013.

[2] Andrej Bauer. The hydra game. math.andrej.com/2008/02/02/the-hydra-game.

[3] Pierre Castéran and Vincent Filou. Tasks, types and tactics for local computation systems. *Stud. Inform. Univ.*, 9(1) :39–86, 2011.

[4] Pierre Castéran. Utilisation en Coq de l'opérateur de description. In *Actes des Journées Francophones des Langages Applicatifs*, 2007. http ://jfla.inria.fr/2007/actes/index.html.

[5] Pierre Castéran and Évelyne Contéjean. On ordinal notations. User Contributions to the Coq Proof Assistant, 2006.

[6] Pierre Courtieu, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. Impossibility of gathering, a certification. *Inf. Process. Lett.*, 115(3) :447–452, 2015.

[7] Nachum Dershowitz and Georg Moser. The hydra battle revisited. In Hubert Comon-Lundh, Claude Kirchner, and Hélène Kirchner, editors, *Rewriting, Computation and Proof : Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of His 60th Birthday*, pages 1–27. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[8] José Grimm. Implementation of three types of ordinals in Coq. Research Report RR-8407, INRIA, 2013.

[9] Jussi Ketonen and Robert Solovay. Rapidly growing Ramsey functions. *Annals of Mathematics*, 113(2) :267–314, 1981.

[10] Laurie Kirby and Jeff Paris. Accessible independence results for Peano arithmetic. *Bulletin of the London Mathematical Society*, 14 :725–731, 1982.

[11] Panagiotis Manolios and Daron Vroon. Ordinal arithmetic : Algorithms and mechanization. *Journal of Automated Reasoning*, 34(4) :387–423, May 2005.

[12] Michael Norrish and Brian Huffman. Ordinals in HOL : Transfinite arithmetic up to (and beyond) ω_1. In Sandrine Blazy and Christine Paulin-Mohring and David Pichardie, editor, *International Conference on Interactive Theorem Proving*, pages 133–146, Rennes, France, July 2013. Springer.

[13] Marcus Vinícius Midena Ramos, Ruy J. G. B. de Queiroz, Nelma Moreira, and José Carlos Bacelar Almeida. Formalization of the pumping lemma for context-free languages. *CoRR*, abs/1510.04748, 2015.

[14] Sylvain Schmitz. Complexity hierarchies beyond elementary. *CoRR*, abs/1312.5686, 2013.

[15] Kurt Schutte. *Proof theory / Translation from the German by J. N. Crossley.* Springer-Verlag Berlin ; New York, 1977.

[16] Will Sladek. The Termite and the Tower : Goodstein sequences and provability in PA. http ://-citeseerx.ist.psu.edu/showciting ?cid=337283, 2007.