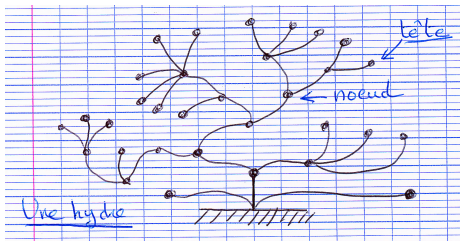
Hydra Ludica, une preuve d'impossibilité de prouver (simplement)

Pierre Castéran, Univ. Bordeaux et LaBRI

Banyuls, Janvier 2018



www.labri.fr/∼casteran/CoqArt/le_teaser

Le théorème idéal

- Son énoncé est simple et très accessible.

Le théorème idéal

- Son énoncé est simple et très accessible.
- Il a l'air faux (au moins surprenant).
- Il permet la discussion de diverses techniques de formalisation et de preuve.

Le théorème idéal

- Son énoncé est simple et très accessible.
- Il a l'air faux (au moins surprenant).
- Il permet la discussion de diverses techniques de formalisation et de preuve.

La preuve idéale

- Utilise des fonctions simples à tester (par `Compute`).
- Illustre des techniques variées : récursions complexes, preuves par réflexion, paramétricité, classes de types, unicité de preuves d'égalité, etc.
- Utilise des bibliothèques de Coq déjà existantes.

Les hydres de Kirby et Paris [3]

Définitions

Une *hydre* est un monstre mythologique en forme d'arbre à branchement fini. On appelle *tête* tout sommet sans descendant.

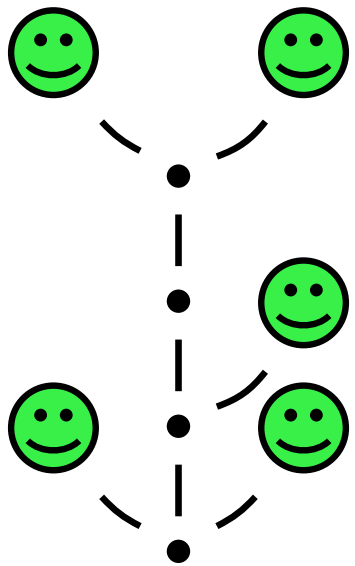


FIGURE – L'hydre Hy

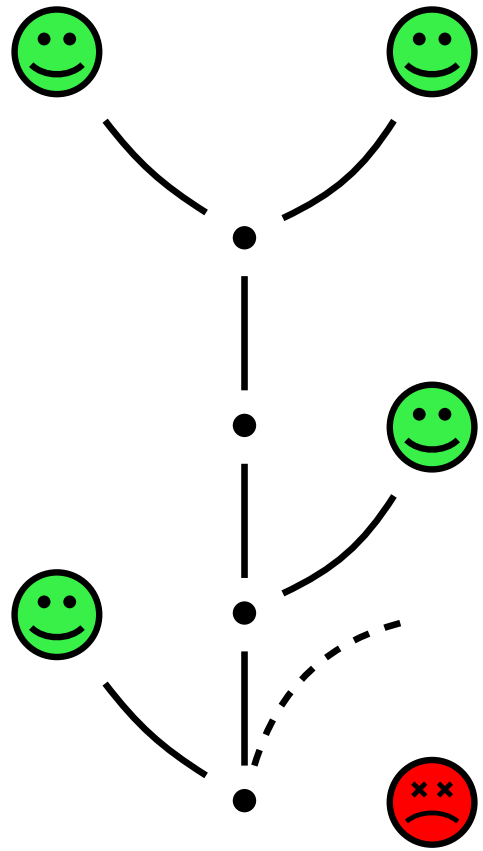


FIGURE – L'état de of Hy après un tour

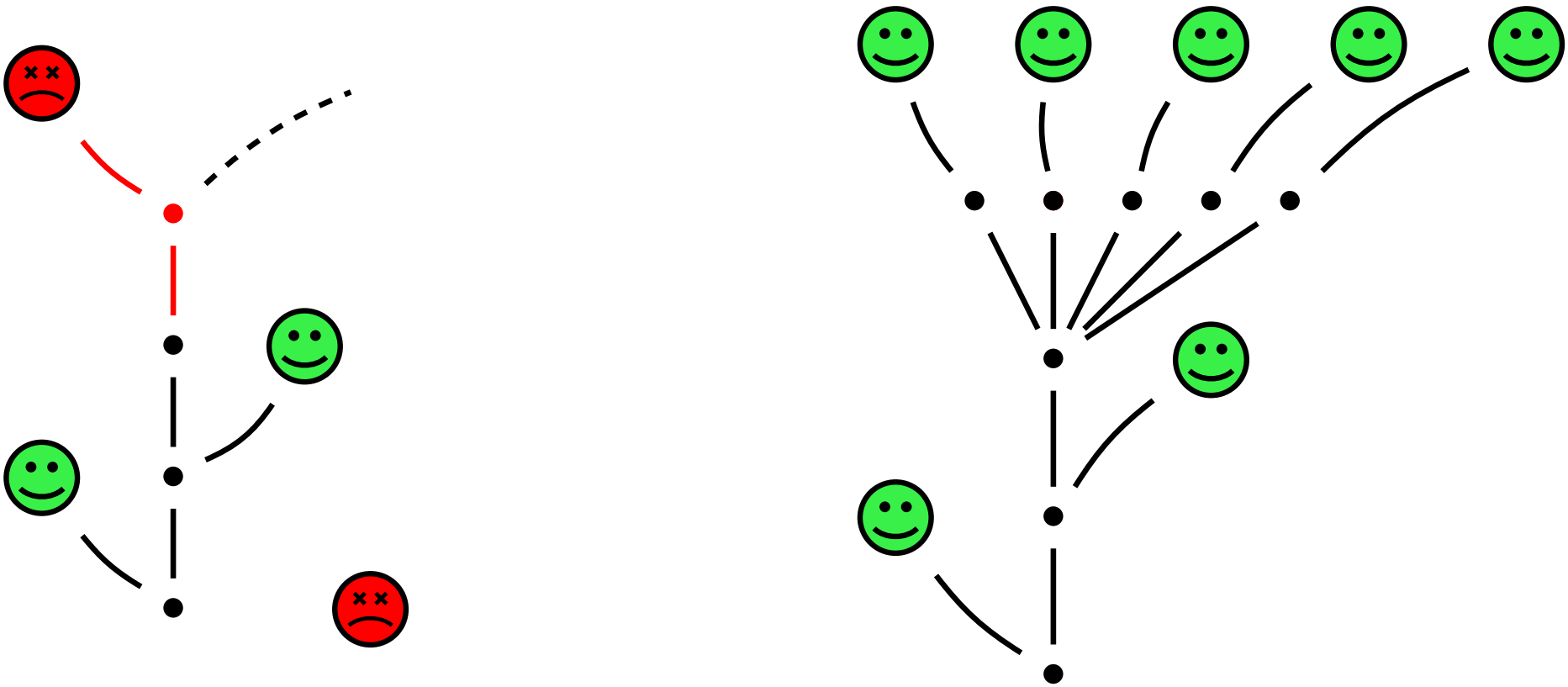
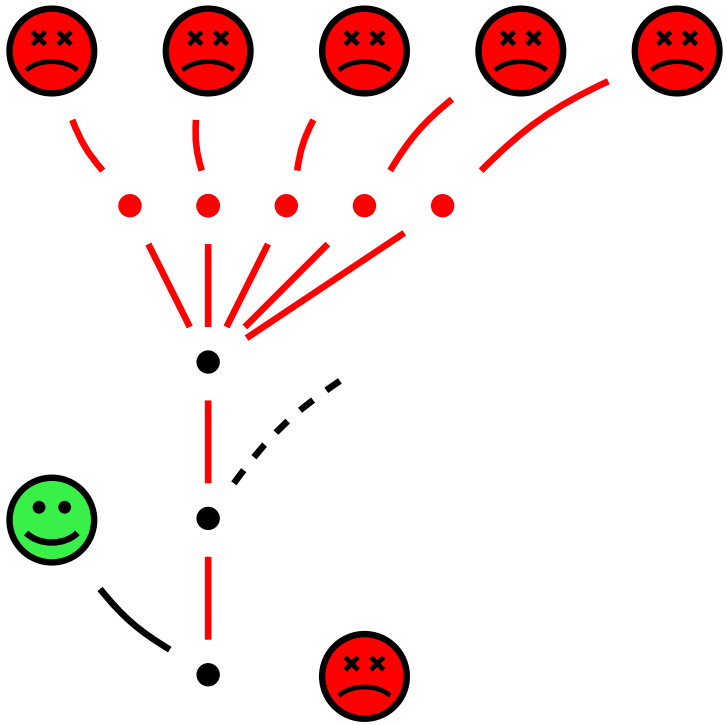


FIGURE – Le second tour



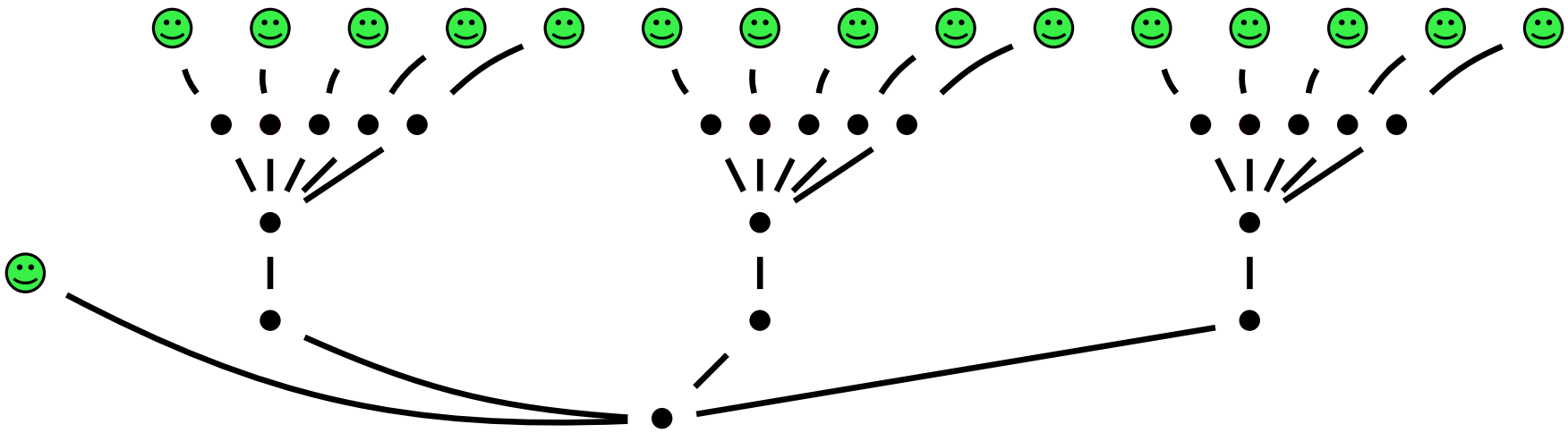


FIGURE – À la fin de la troisième reprise : Hy"'

À chaque tour,

1. Hercule choisit une tête et la coupe.
2. L'hydre choisit un nombre de copies de la partie ététée (si la tête est à distance > 1 du pied).

À chaque tour,

1. Hercule choisit une tête et la coupe.
2. L'hydre choisit un nombre de copies de la partie ététée (si la tête est à distance > 1 du pied).

Théorème (Kirby et Paris, 1982)

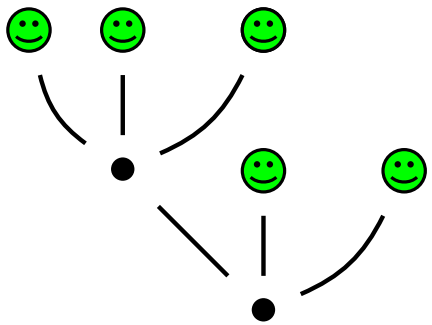
Toute bataille d'hydre se termine par la victoire d'Hercule.

À chaque tour,

1. Hercule choisit une tête et la coupe.
2. L'hydre choisit un nombre de copies de la partie ététée (si la tête est à distance > 1 du pied).

Théorème (Kirby et Paris, 1982)

Toute bataille d'hydre se termine par la victoire d'Hercule. Mais ça peut prendre du temps... : une simulation sur l'hydre ci-dessous a demandé plus de $3 \times 2^{402653211} - 1$ rounds.



Preuve sur machine de la victoire d'Hercule [1]

- Représentation des ordinaux $< \epsilon_0$ par des arbres finis (forme normale de Cantor).
- Un peu d'arithmétique sur les ordinaux.
- Preuves de bonne fondation de l'ordre $<$ sur cette représentation, tactique de preuve par récurrence transfinie, etc.

```
Compute compare (omega ^ omega ^ omega)
                (omega ^ (omega * 42 + 566) * 25).
```

```
= GT : comparison
```

- Définition d'une mesure m (*variant*) associant à toute hydre un ordinal $< \epsilon_0$

- Si h est une tête, alors $m(h) = 0$
- Si h est formée d'un pied relié aux 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 d'ordinaux, appelée *somme d'Hessenberg* ou *somme naturelle*.

```
Compute compare (m Hy) (m Hy''').
```

```
= GT : comparison
```

Il « suffit » alors de prouver que si h se transforme en h' en un tour, alors $m(h') < m(h)$

Taille de la preuve

- Bibliothèque sur ϵ_0 : 7264 lignes
- Batailles d'hydres et terminaison : 925 lignes

Question :

Aurait-on pu faire plus simple ?

Preuves de difficulté de prouver

Second théorème de Kirby et Paris

La preuve de terminaison de toutes les batailles d'hydre n'est pas démontrable dans l'arithmétique de Peano.

Preuves de difficulté de prouver

Second théorème de Kirby et Paris

La preuve de terminaison de toutes les batailles d'hydre n'est pas démontrable dans l'arithmétique de Peano.

Remarque

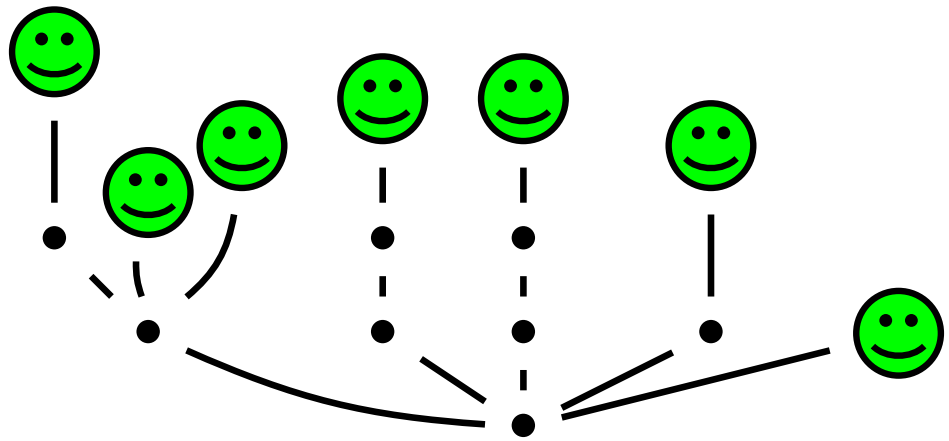
Ce très beau résultat ne parle pas vraiment à l'utilisateur de systèmes à base de logique d'ordre supérieur.
On souhaite en prouver une variante :

La terminaison des batailles d'hydre ne peut pas se prouver à l'aide d'un variant défini dans $[0..\alpha[$ *avec* $\alpha < \epsilon_0$.

Structure de la preuve

1. Soit $\alpha < \epsilon_0$ un ordinal.
2. On suppose qu'il existe un variant m à valeurs dans $[0..\alpha[$ avec $\alpha < \epsilon_0$ pour les batailles d'hydre.
3. On construit une hydre h telle que $m(h) > m(h)$
4. Mais c'est impossible !

On définit une injection ι associant une hydre à tout ordinal $\beta < \epsilon_0$. Cette injection est pratiquement l'identité : La figure ci-dessous montre l'hydre associée à l'ordinal $\omega^{\omega+2} + \omega^\omega \times 2 + \omega + 1$



Les outils de Ketonen et Solovay [2]

Suites canoniques d'ordinaux

On definit pour tout $i \geq i$ et tout $\alpha < \epsilon_0$ l'ordinal $\{\alpha\}(i)$ (noté aussi $d\, i\, \alpha$) tel que :

$$\begin{aligned} \{\alpha+1\}(i) &= \alpha \\ \lambda &= \sup_{i\in\mathbb{N}} \{\{\lambda\}(i)\} \quad (\lambda \textit{ ordinal limite}) \end{aligned}$$

```
Example ex : d 42 (omega^omega^omega) = omega^omega^42.
Proof. reflexivity. Qed.
```

Remarque

La notion de limite s'exprime bien sous forme fonctionnelle ...

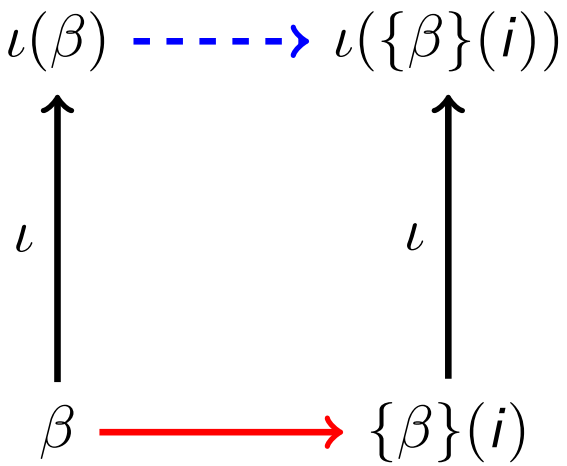
```
Lemma d_limit_strong lambda :
  nf lambda ->
  is_limit lambda  ->
  forall beta, beta < lambda ->
   {i:nat | beta < d i lambda < lambda}.
```

Suites canoniques et combats

$$\beta \longrightarrow \{\beta\}(i)$$

Considérons un élément $\{\beta\}(i)$ de la suite canonique associée à β.

Suites canoniques et combats

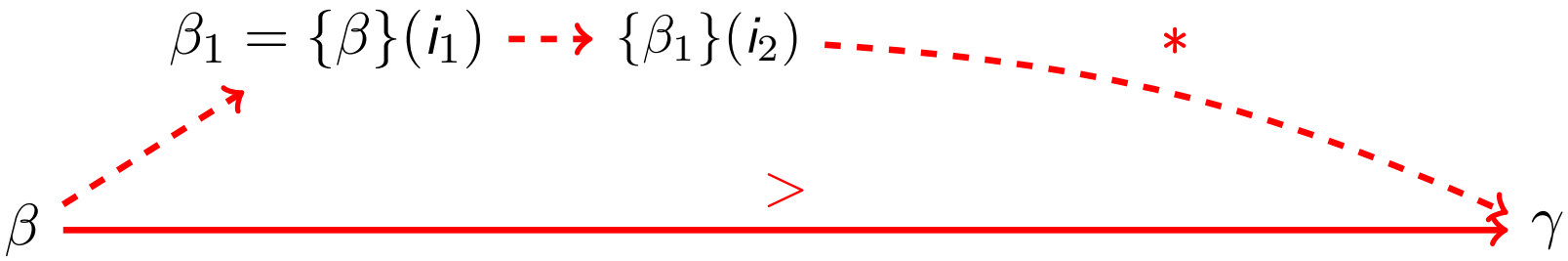


Considérons un élément $\{\beta\}(i)$ de la suite canonique associée à β. On lui associe un round où Hercule coupe la tête la plus à droite de l'hydre, et celle-ci réplique avec un facteur de i.

Ordre et batailles

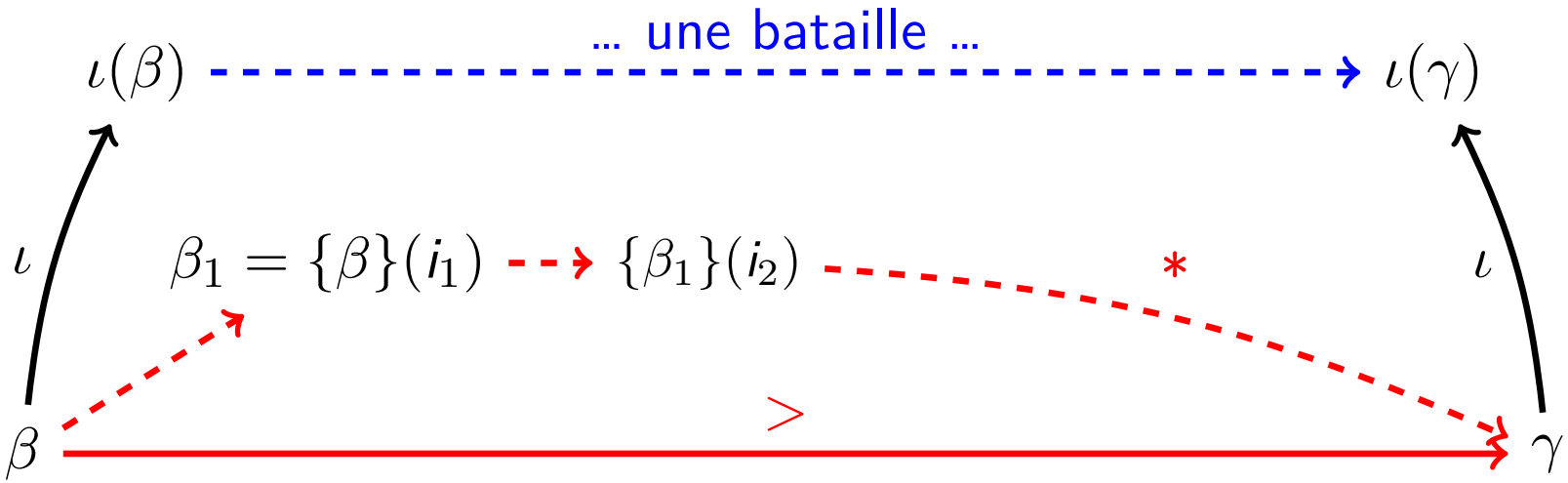
Soient $\gamma < \beta < \epsilon_0$

Ordre et batailles



Ketonen et Solovay [2] *(preuve par récurrence transfinie sur β)*

Ordre et batailles



La preuve, en 8 lignes

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse, $m(h_\alpha) < \alpha$.

La preuve, en 8 lignes

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse, $m(h_\alpha) < \alpha$.
- L'hydre h_α se transforme alors en $\iota(m(h_\alpha))$, ce qui implique l'inégalité $m(h_\alpha) > m(\iota(m(h_\alpha)))$.

La preuve, en 8 lignes

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse, $m(h_\alpha) < \alpha$.
- L'hydre h_α se transforme alors en $\iota(m(h_\alpha))$, ce qui implique l'inégalité $m(h_\alpha) > m(\iota(m(h_\alpha)))$.
- D'autre part, on prouve l'inégalité $m(\iota(\beta)) \geq \beta$, pour tout $\beta < \alpha$ (par récurrence transfinie sur β).

La preuve, en 8 lignes

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse, $m(h_\alpha) < \alpha$.
- L'hydre h_α se transforme alors en $\iota(m(h_\alpha))$, ce qui implique l'inégalité $m(h_\alpha) > m(\iota(m(h_\alpha)))$.
- D'autre part, on prouve l'inégalité $m(\iota(\beta)) \geq \beta$, pour tout $\beta < \alpha$ (par récurrence transfinie sur β).
- On en conclut l'inégalité stricte $m(h_\alpha) > m(\iota(m(h_\alpha))) \geq m(h_\alpha)$.
- D'où `False` 

Conclusion et Perspectives

Aspects importants

- Interface calcul/preuve.
- Infini potentiel/infini actuel.
- Maths discrètes/programmation (*e.g.* limites)

Travaux futurs

En fonction des stratégies respectives d'Hercule et de l'hydre, évaluation de l'hyper-complexité des durées de batailles et de la preuve de terminaison.

- Fonctions à croissance rapide [a] (hiérarchie de Wainer).
- Ensembles α-grands

a. Très rapide.


P. C. and Évelyne Contéjean.
On ordinal notations.
User Contributions to the Coq Proof Assistant, 2006.


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


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