Preuves de terminaison par variants

Pierre Castéran, Université de Bordeaux et LaBRI

Grenoble, 31 août 2017

Introduction : Le charme des preuves d'impossibilité

- Les preuves 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.
- Nombreux exemples : théorie des langages, algorithmique distribuée (preuves en Coq : C. et V. Filou, S. Tixeuil, X. Urbain et al.), etc.
- Dans cet exposé, on présente un exemple de *preuve d'impossibilité de prouver simplement* (pour le moment dans un cadre non-distribué, non-déterministe).

Les hydres de Kirby et Paris [2]

Définition

Une hydre est un monstre mythologique en forme d'arbre à branchement fini.

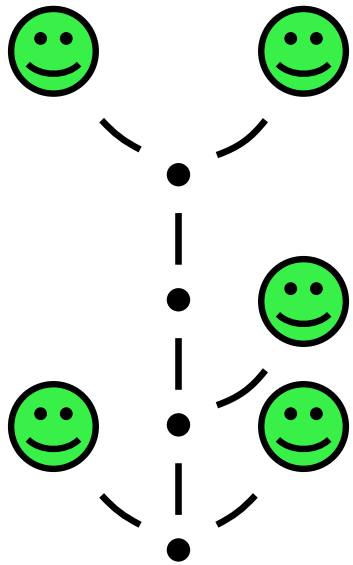


FIGURE : L'hydre Hy

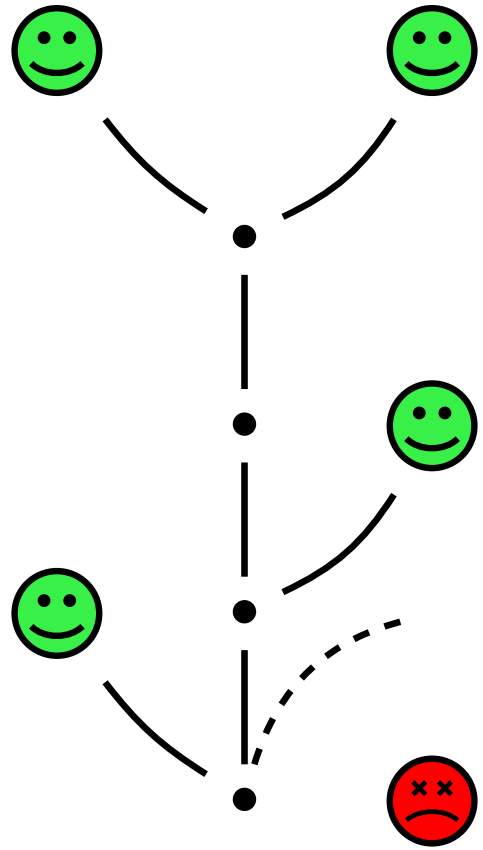


FIGURE : L'état de of Hy après un tour

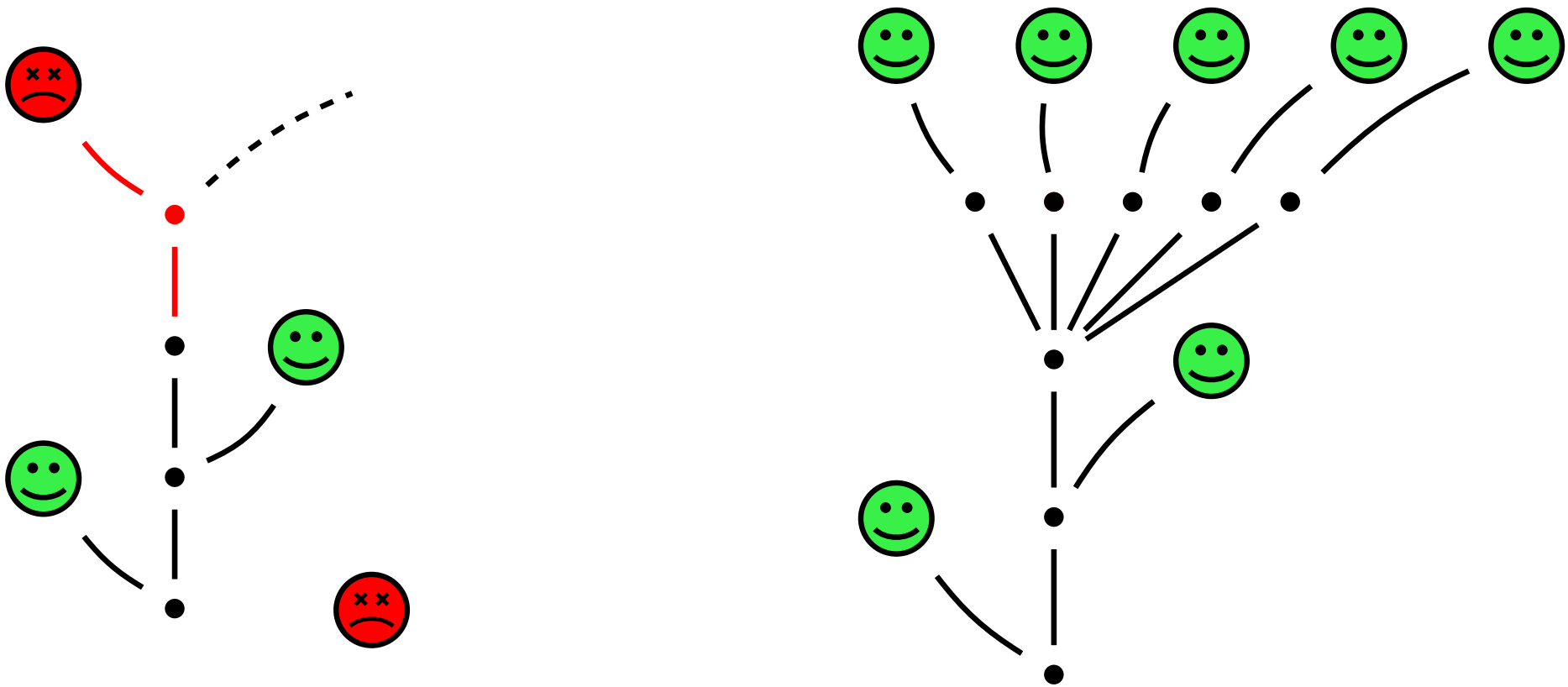
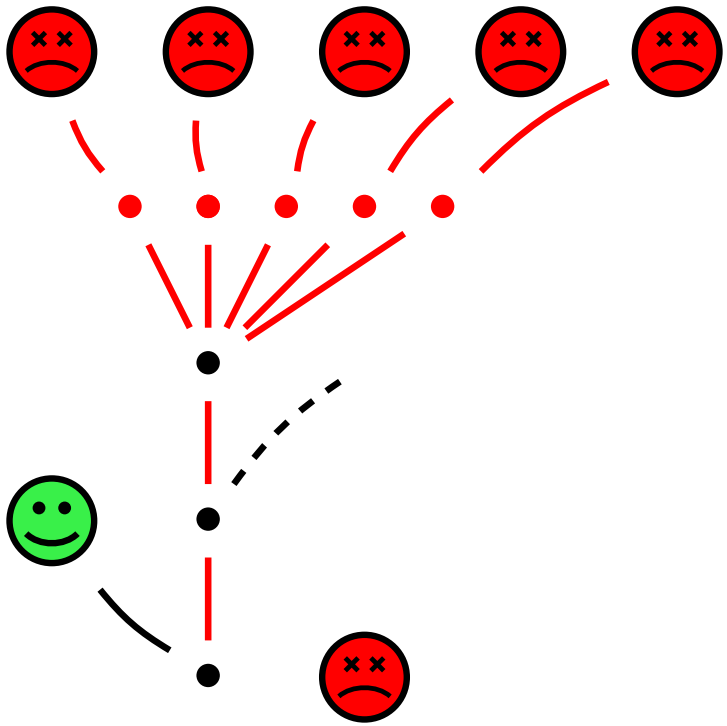


FIGURE : Le second tour



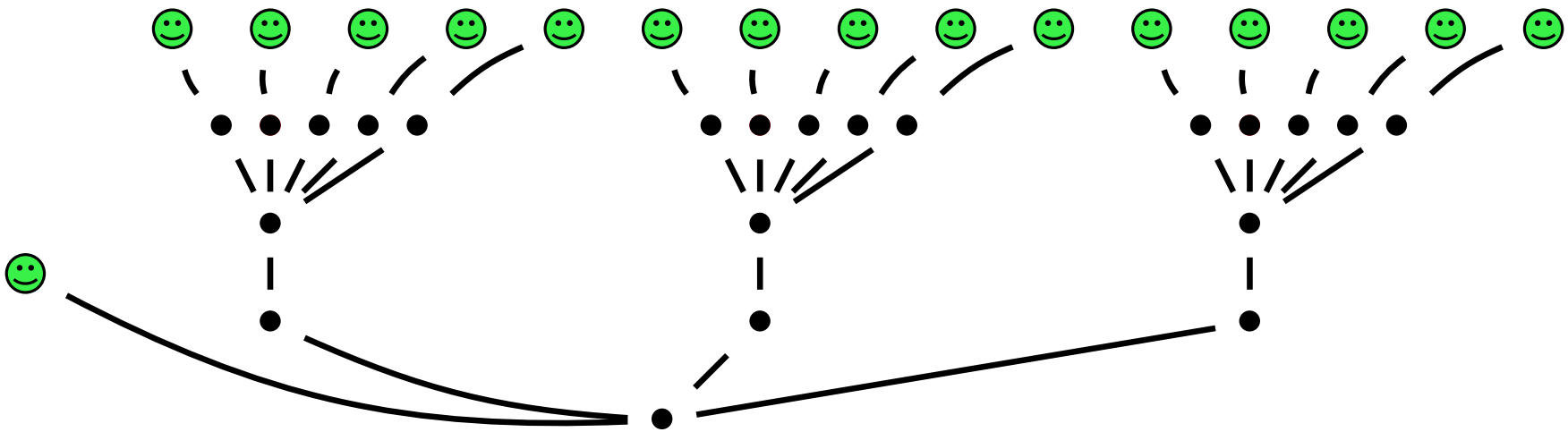


FIGURE : À la fin de la troisième reprise

Notion de stratégie

Hercule

Choix d'une tête à couper

L'hydre

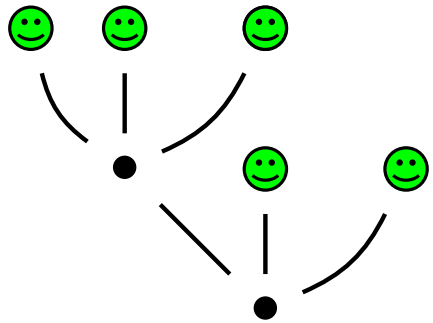
Choix du nombre de réplications de la partie étêtée

Théorème (Kirby et Paris, 1982)

Toute bataille d'hydre se termine par la victoire d'Hercule. Mais ça peut prendre du temps...

Exemple

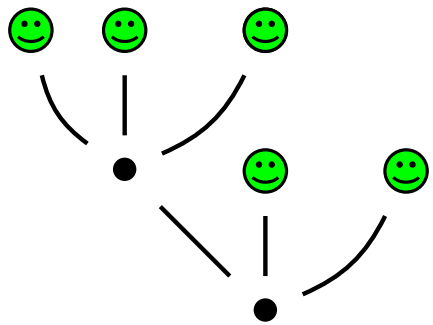
On considère l'hydre ci-dessous :



On suppose qu'Hercule choisit toujours la tête la plus basse possible, et que l'hydre augmente son facteur de réplication de 1 à chaque tour.

Exemple

On considère l'hydre ci-dessous :



On suppose qu'Hercule choisit toujours la tête la plus basse possible, et que l'hydre augmente son facteur de réplication de 1 à chaque tour.
Au 20000-ème tour, l'hydre a une taille de 9236 noeuds. Il faut plus de $3 \times 2^{402653211} - 1$ tours pour la vaincre.

Terminaison des systèmes de transition

```
Section Definitions.
 Variable E: Type.
 Variable tr : relation E. (* transition *)

 Definition terminates  :=  well_founded (flip tr).
```

Note

`flip` *tr* est la notation Coq pour tr^{-1}.

On peut associer une classe à la notion de *variant* :

```
Variables (T: Type)
          (lt : relation T)
          (m : E -> T).
Infix "<" := lt.

Class Variant :=
   {
     wf : well_founded lt;
     decr : forall x y, tr x y -> m y < m x
   }.
```

Preuve sur machine de la victoire d'Hercule

En suivant la preuve papier de K. et P. , mécanisation en Coq [3] :

- Représentation des ordinaux $< \epsilon_0$ par des arbres finis (forme normale de Cantor).
- Preuve de bonne fondation de l'ordre $<$ sur cette représentation.
- Un peu d'arithmétique sur les ordinaux.
- Tactiques associées à la preuve par récurrence transfinie et la trichotomie : zéro, ordinal successeur, ordinal limite.

- Définition d'un variant associant à toute hydre un ordinal $< \epsilon_0$
- Preuve que ce variant décroît strictement à chaque reprise du combat.

Forme normale de Cantor :

$$\omega^{(\omega^\omega + \omega^2 \times 8 + \omega)} + \omega^\omega + \omega^4 + 6$$

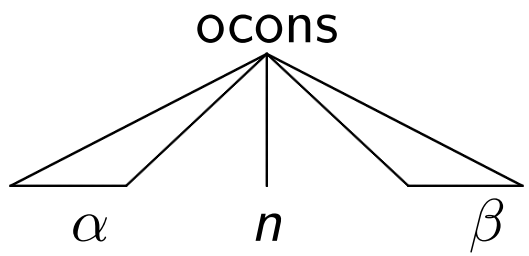
FIGURE : Un ordinal en forme normale de Cantor

Tout ordinal $< \epsilon_0$ est représenté sous forme d'arbre fini :

0

zero

$\omega^\alpha \times (n+1) + \beta$



On a bien une représentation *finie* des ordinaux inférieurs à ϵ_0. *Donc :* pas besoin d'axiomes, possibilités de calculer, de décider, etc.

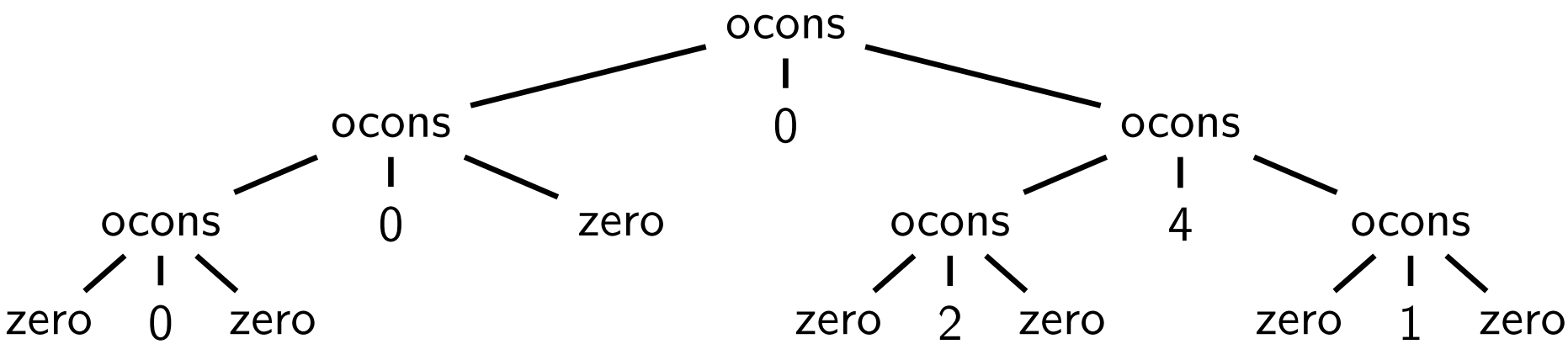


FIGURE : L'arbre associé à l'ordinal $\omega^\omega + \omega^3 \times 5 + 2$

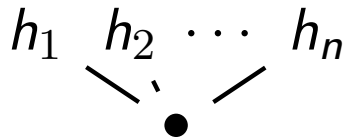
Définition d'un variant m

On définit récursivement la fonction m sur le type des hydres :

cas de base

$$m(\text{☺}) = 0$$

cas général : Soit h de la forme suivante



$m(h) = \omega^{m(h_1)} \oplus \omega^{m(h_2)} \oplus \cdots \oplus \omega^{m(h_n)}$ ($\oplus$: somme dite *d'Hessenberg*, strictement monotone et commutative)

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 $[0..\alpha[$ pour les batailles d'hydre
3. On construit une hydre h telle que $m(h) > m(h)$

Structure de la preuve

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

Problème

On ne sait rien sur m, à part l'hypothèse que c'est un variant. Seule la connaissance des ordinaux et des règles des combats d'hydre peut nous aider 😡.

Pour se faire la main ...

Avant d'attaquer la preuve pour un ordinal quelconque $\alpha < \epsilon_0$, on peut s'entraîner avec ω, ω^2, ω^ω, etc.
La structure de la preuve sera plus lisible que dans le cas général.

Par exemple, étudions le cas d'ω^2.

L'ordinal ω^2 est isomorphe au produit cartésien $\mathbb{N} \times \mathbb{N}$ muni de l'ordre lexicographique strict.

Preuve de l'insuffisance d'ω^2

1. Supposons qu'il existe un variant m à valeurs dans $\mathbb{N} \times \mathbb{N}$ pour notre problème de terminaison.
2. On définit une injection ι associant à tout couple (i, j) l'hydre comportant i bras de longueur 2 et j bras de longueur 1.

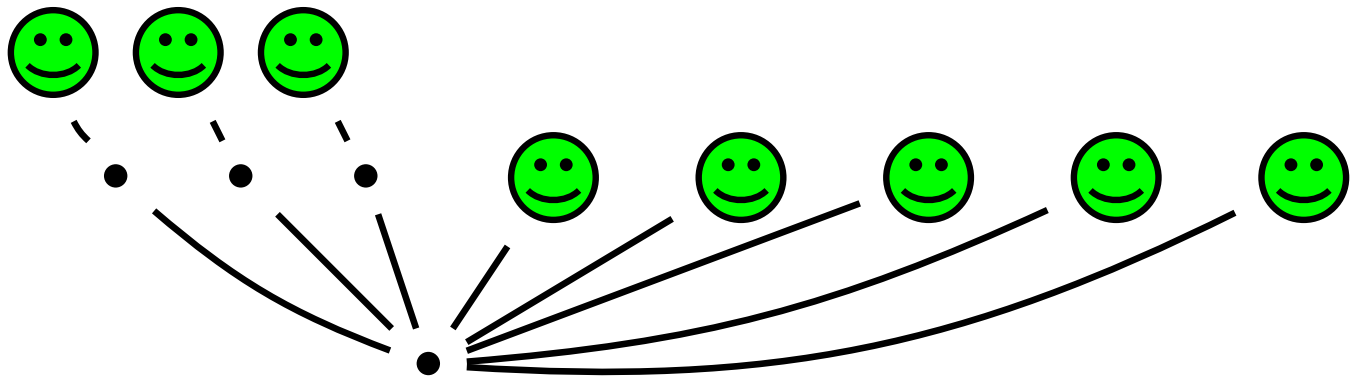


FIGURE : The hydra $\iota(3, 5)$

Soit alors l'hydre h_{ω^2}.

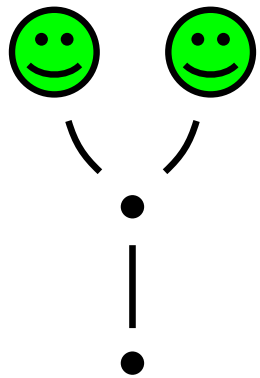


FIGURE : h_{ω^2}

Soit $(i,j) = m(h_{\omega^2})$; on remarque qu'en 2 rounds, h_{ω^2} se transforme en $\iota(i,j)$ (en passant par $\iota(i+1,0)$).
Donc $m(h_{\omega^2}) > m(\iota(m(h_{\omega^2})))$.

Il reste à prouver que pour tout (i,j) on a $m(\iota(i,j)) \geq (i,j)$, ce qui impliquera l'inégalité $m(\iota(m(h_{\omega^2}))) \geq m(h_{\omega^2})$, et, par transitivité, $m(h_{\omega^2}) > m(h_{\omega^2})$.

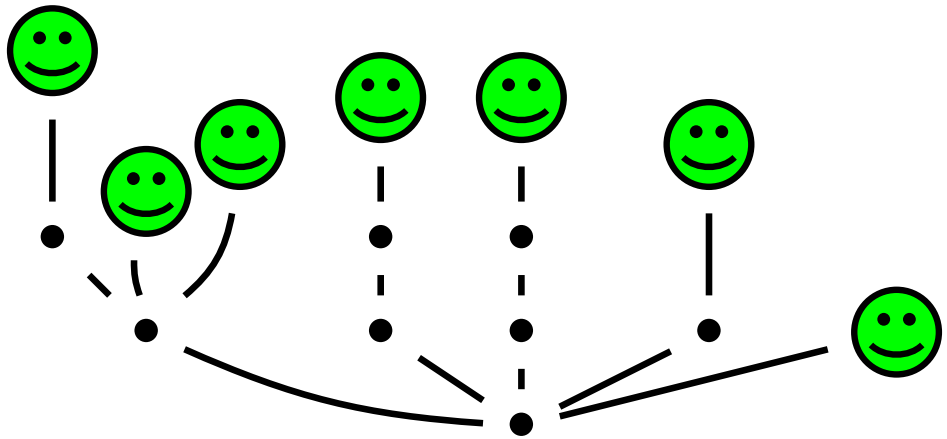
- Preuve par récurrence transfinie sur ω^2. On suppose que pour tout couple $(k,l) < (i,j)$ on a $m(\iota(k,l)) \geq (k,l)$
  - Si $i = j = 0$ la propriété est triviale.
  - Si $j > 0$ (*ordinal successeur*) : $\iota(i,j)$ se transforme en $\iota(i,j-1)$; donc $m(\iota(i,j)) > m(\iota(i,j-1)) \geq (i,j-1)$, donc $m(\iota(i,j)) \geq (i,j)$
  - (voir diapo suivante)

- Supposons $i > 0 \wedge j = 0$. Le couple (i, j) est la limite de tous les couples $(i - 1, k)$ où $k \in \mathbb{N}$.
  - Pour tout k l'hydre $\iota(i, 0)$ *peut* se transformer en $\iota(i - 1, k)$: *Un bras de longueur 2 est remplacé par k bras de longueur 1*
  - Pour tout k, donc, on a $m(\iota(i, 0)) > m(\iota(i - 1, k)) \geq (i - 1, k)$
  - Donc $m(\iota(i, 0)) \geq (i, 0)$.

- On a donc bien eu recours à une preuve par récurrence transfinie et une étude de cas : ordinal 0, successeur ou limite.
- La structure de la preuve d'impossibilité pour tout ordinal inférieur à ϵ_0 sera la même, mais va nécessiter beaucoup plus d'outils, et une connaissance plus fine de la structure d'ordre sur ϵ_0.

Preuve générale

1. Soit α un ordinal inférieur à ϵ_0.
2. Supposons qu'il existe un variant m à valeurs dans $[0..\alpha[$ pour prouver la terminaison des batailles d'hydre.
3. On définit une injection ι associant une hydre à tout $\beta < \epsilon_0$. Cette injection est pratiquement l'identité : La figure ci-dessous montre l'hydre associée à l'ordinal $\omega^{\omega+2} + \omega^\omega \times 2 + \omega + 1$



La preuve possède la même structure que pour ω^2 :

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse $m(h_\alpha) < \alpha$.
- On prouve que h_α se transforme 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 $\beta < \alpha$.

La preuve possède la même structure que pour ω^2 :

- On considère l'hydre $h_\alpha = \iota(\alpha)$.
- Par hypothèse $m(h_\alpha) < \alpha$.
- On prouve que h_α se transforme 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 $\beta < \alpha$.

Remarque

On travaille toujours sous la seule hypothèse que m est un variant. Donc pas d'argument de monotonie de m, ou autre affirmant que la mesure d'une hydre est supérieure à celle de ses filles ...

Les outils de Ketonen et Solovay [1]

Suites canoniques d'ordinaux

On définit les fonctions suivantes (pour tout $i \geq 1$), par récursion simple sur la notation en forme normale de Cantor :

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

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

$\{\omega^{\omega} + \omega\}(4) = \omega^{\omega} + 4$ $\quad$ $\{\omega^{\omega} \times 2\}(4) = \omega^{\omega} + \omega^4$

Si Hercule coupe la tête la plus à droite et la plus proche du pied, et l'hydre crée i copies de la partie blessée (si possible), alors l 'hydre $\iota(\beta)$ se transforme en un round en $\iota(\{\beta\}(i))$

Notation

Soit $i \geq 1$. On note $\underset{i}{\rightarrow}$ la fermeture transitive de la relation associée à la transformation de α en $\{\alpha\}(i)$.

Lemme

Si $\alpha \underset{i}{\rightarrow} \beta$, alors $\iota(\alpha) \xrightarrow{+} \iota(\beta)$.

Propriétés [1]

- Si λ est un ordinal limite, alors λ est la borne supérieure des $\{\lambda\}(i)$.
- Toute transformation élémentaire de α en $\{\alpha\}(i)$ peut se simuler par une suite de transformations $\alpha \underset{j}{\rightarrow} \{\alpha\}(i)$ (avec $i < j$).
- Si $i \leq j$, alors $\underset{i}{\rightarrow} \subseteq \underset{j}{\rightarrow}$
- Si $\beta < \alpha$, il existe un $i \geq 1$ tel que $\alpha \underset{i}{\rightarrow} \beta$ (ce qui se traduit par une suite de reprises avec un facteur de réplication constamment égal à i).

Une fois qu'on a mécanisé toute la « machinerie de Ketonen et Solovay », notre preuve est assez simple :

1. Comme $\alpha > m(h_\alpha)$, l'hydre h_α se transforme en $h' = \iota(m(h_\alpha)))$.
2. On a donc $m(h) > m(h')$ (car m est un variant)
3. Reste à prouver $m(h') \geq m(h)$.
4. Comme précédemment, on généralise en $\forall \beta < \epsilon_0,\ m(\iota(\beta) \geq \beta$.

On prouve cette propriété par récurrence transfinie sur β. Le seul cas nouveau est celui des ordinaux limites :

- Si λ est un ordinal limite, alors λ est la borne supérieure de tous les $\{\lambda(i)\}$.

On prouve cette propriété par récurrence transfinie sur β. Le seul cas nouveau est celui des ordinaux limites :

- Si λ est un ordinal limite, alors λ est la borne supérieure de tous les $\{\lambda(i)\}$.
  - Soit $\gamma < \lambda$, alors γ est dominé par un $\{\lambda\}(i)$.
  - On a donc $\lambda > \{\lambda\}(i) > \gamma$
  - L'hydre $\iota(\lambda)$ se transforme alors en $\iota(\gamma)$
  - Par hypothèse de récurrence, on a $m(\iota(\gamma)) \geq \gamma$, donc $m(\iota(\lambda)) > \gamma$
- On a donc, par passage à la limite, $m(\iota(\lambda)) \geq \lambda$.

On obtient donc notre contradiction $m(h) > m(h)$ 

Remarques générales

- Les preuves d'impossibilité nous permettent d'explorer la puissance des outils de démonstration
- L'exemple de l'hydre présente un double intérêt :
  - Le theorème de terminaison a un énoncé simple, mais surprenant
  - Le second théorème de [2] permet de formaliser la notion de difficulté d'une preuve
- Mettre une preuve complète dans un répertoire demande d'unifier des notations et définitions parfois hétérogènes de la littérature
- La mécanisation pour un assistant de preuve est l'occasion de transformer des éléments du discours mathématique usuel genre *il suffit de considérer le cas ...* en procédures informatiques (tactiques)

- Les lemmes sur les suites canoniques $\{\alpha\}(i)$ et les relations $\underset{i}{\rightarrow}$ sont ceux de [1].
- Les démonstrations restent fondamentalement les mêmes, avec certains changements :
  - Utilisation de structures de données plutôt que des ensembles
  - Utilisation de tactiques, de calculs, de la bibliothèque standard
  - Suppression de notions auxiliaires devenues superflues.

Taille des scripts

- Ketonen-Solovay : 1803 lignes
- Lemmes d'impossibilité :
  - ω : 115 lignes
  - ω^2 : 280 lignes
  - α quelconque $< \epsilon_0$: 621 lignes

Travaux futurs

- Dans notre preuve, on utilise le fait qu'à chaque reprise, l'hydre peut choisir son nombre de réplications.
- Or, l'article de Kirby et Paris considère aussi le cas ou l'hydre n'est pas libre de choisir ce nombre. Il reste donc à prouver que si ce nombre est contrôlé (par exemple, augmente de 1 à chaque tour), l'ordinal ϵ_0 reste le variant le plus simple pour la preuve de terminaison.
- Outils mathématiques à mécaniser :
  - Fonctions à croissance rapide,
  - Ensemble α-grands
- Trouver des exemples dans le distribué ?


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.


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