Ce n'est jamais terminé . . .

Pierre Castéran, LaBRI
Laurent Bienvenu, LaBRI
Hervé Hocquard, LaBRI

27 juin 2019

Quelques exemples

Nous allons présenter quelques exemples d'algorithmes dans lesquels la preuve de terminaison est assez subtile.

- Un compte à rebours infernal,
- Fonction d'Ackermann,
- Le combat d'Hercule contre l'Hydre.

t	A	B	C
0	2	2	5

t	A	B	C
0	2	2	5
1	2	2	4

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0
6	2	1	5
7	2	1	4

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0
6	2	1	5
7	2	1	4
...	...	...	...

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0
6	2	1	5
7	2	1	4
...	...	...	...
11	2	1	0
...	...	...	...

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0
6	2	1	5
7	2	1	4
...	...	...	...
11	2	1	0
...	...	...	...
...	1	36	77

t	A	B	C
0	2	2	5
1	2	2	4
2	2	2	3
3	2	2	2
4	2	2	1
5	2	2	0
6	2	1	5
7	2	1	4
...	...	...	...
11	2	1	0
...	...	...	...
...	1	36	77

Quand ce compte va-t'il s'arrêter ? D'ailleurs, s'arrêtera-t'il ?

Peut-être pas si infernal que ça...

La suite va finir par atteindre la configuration

t	A	B	C
?	0	0	0

On utilise le théorème suivant :

Toute suite infinie de nombres entiers naturels dont chaque terme est inférieur ou égal au précédent finit par devenir stationnaire.

$1256, 1256, 1010, 1009, 1008, 479, 478, 477, 35, 35, 35, \ldots, 35, \ldots$

Ce résultat (bonne fondation de $\mathbb{N}$) se prouve par récurrence sur le premier item de la suite.

Supposons que le compteur ne s'arrête jamais.

Supposons que le compteur ne s'arrête jamais.

t	A	B	C
0	2	2	5
1	2	2	4
...			
12	1	36	77
...			

Le compteur `A` prend la valeur 2, puis 1, puis (peut-être) 0. Par le théorème précédent, il va stationner en une valeur a.

t	A	B	C
...	a	y	...
...	a	y'	...
...			
...	a	b	z
...	a	b	z'
...			
...	a	b	c
...	a	b	c
...	a	b	c
...			

Lorsque `A` devient fixe, B va se mettre à décroître, et atteindre une valeur fixe b. De même pour `C` et c.

Forcément, $a = b = c = 0$, le compteur s'arrête donc.

La fonction d'Ackermann

La fonction d'Ackermann de deux entiers naturels est définie par :

$$acker(m,n) = \begin{cases} n+1 & \text{si } m = 0 \\ acker(m-1,1) & \text{si } n = 0 \\ acker(m-1, acker(m,n-1)) & \text{sinon} \end{cases}$$

Algorithme de la fonction d'Ackermann

Algorithme 1 : AckermannRecursif(m,n)

Données : Deux entiers m et n

si *m=0* **alors**
  retourner n+1;
sinon si *n=0* **alors**
  retourner AckermannRecursif(m-1,1);
sinon
  retourner AckermannRecursif(m-1,AckermannRecursif(m,n-1));

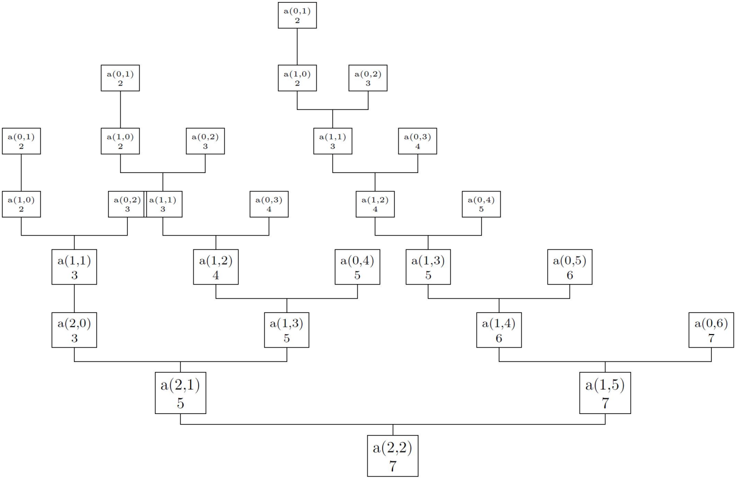


Figure: Arbre des appels pour `acker(2,2)=7`

La fonction d'Ackermann

$acker(m, n)$ fait deux appels récursifs :

- à $acker(m, n-1)$
- à $acker(m-1, N)$ pour un certain N potentiellement très grand

La fonction d'Ackermann

$acker(m, n)$ fait deux appels récursifs :

- à $acker(m, n-1)$
- à $acker(m-1, N)$ pour un certain N potentiellement très grand

Les deux couples $(m, n-1)$ et $(m-1, N)$ sont plus petits que (m, n) pour l'ordre du compte à rebours infernal.

La fonction d'Ackermann

$acker(m, n)$ fait deux appels récursifs :

- à $acker(m, n-1)$
- à $acker(m-1, N)$ pour un certain N potentiellement très grand

Les deux couples $(m, n-1)$ et $(m-1, N)$ sont plus petits que (m, n) pour l'ordre du compte à rebours infernal.

Donc l'algorithme va s'arrêter !

Batailles d'Hydre

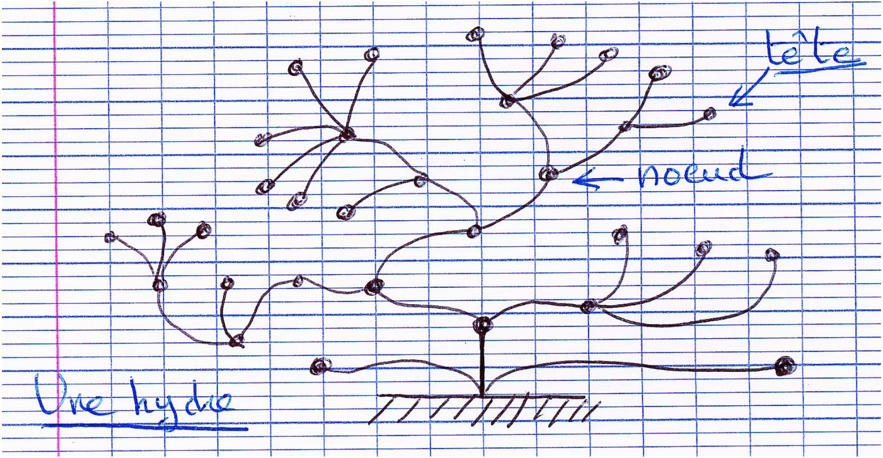
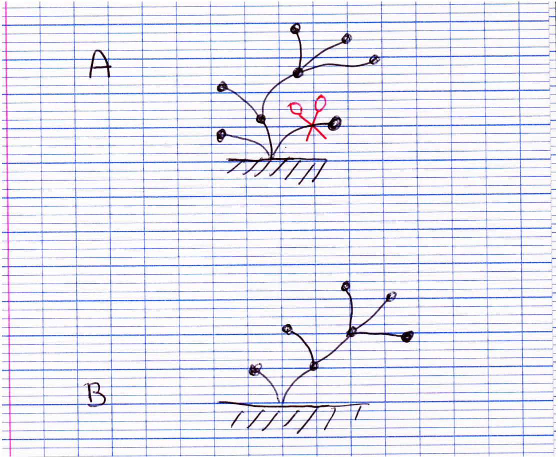
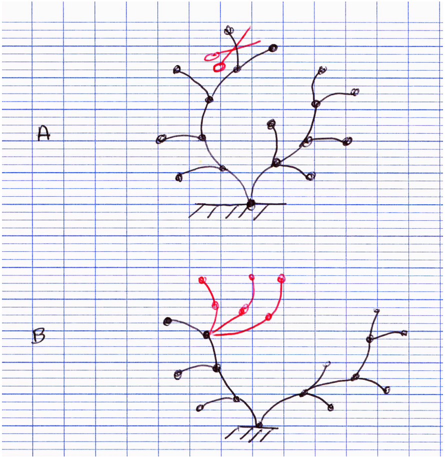


Figure: Une hydre

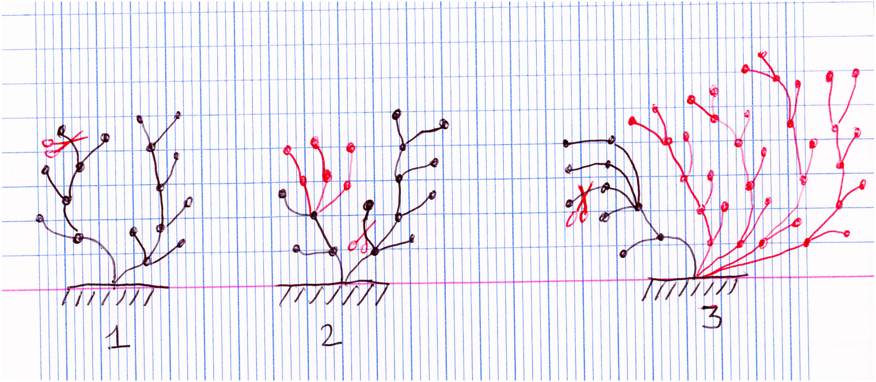
Décapitation : premier cas



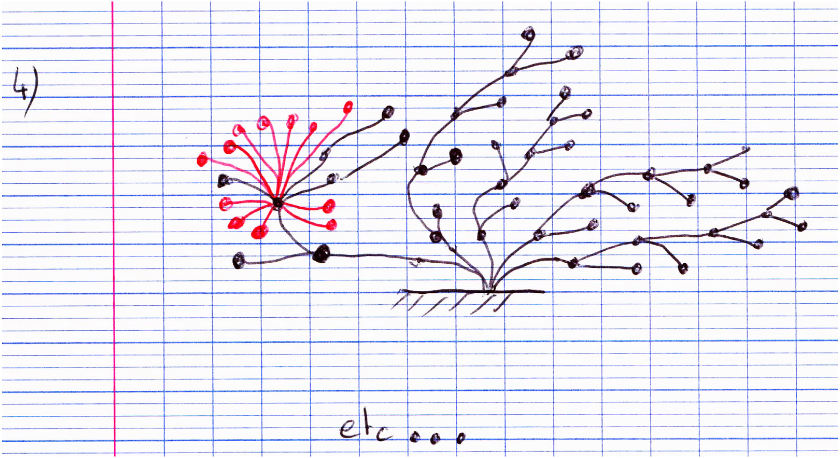
Décapitation : second cas



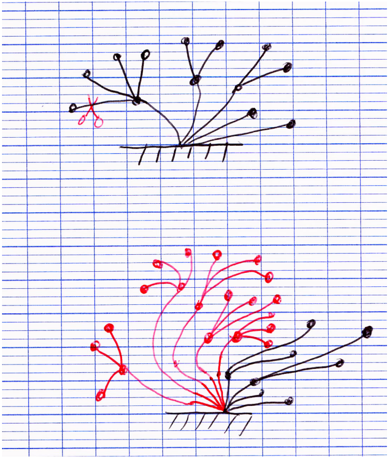
Un combat (début)

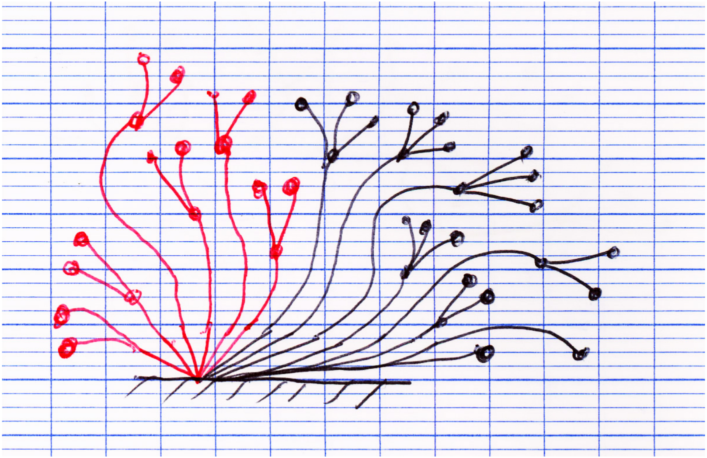


Un combat (suite)



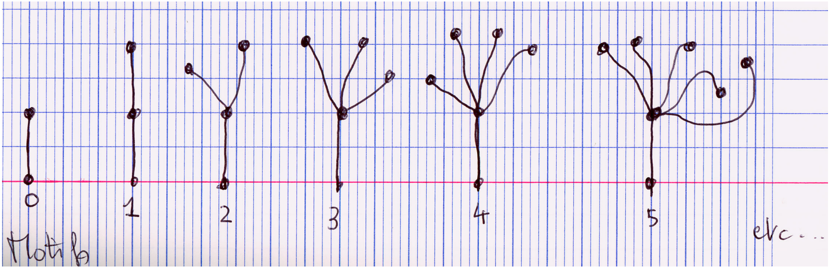
Étude d'une espèce particulière d'hydre (tentacules de longueur ≤ 2)



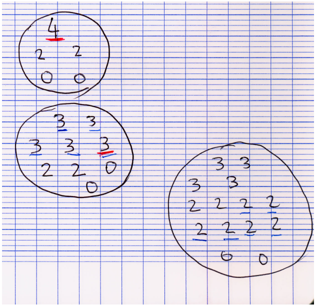


On prouve qu'Hercule finit toujours par vaincre une telle hydre.

Pour ce faire, on commence par associer un nombre entier à chaque motif élémentaire :



On constitue des « sacs »[1] de nombres entiers naturels :

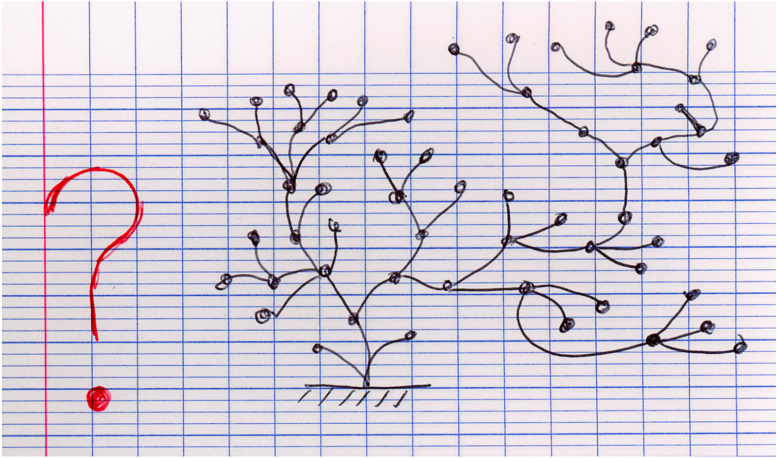


On considère la relation engendrée par le remplacement d'un élément d'un sac par un nombre quelconque d'entiers strictement inférieurs.

1. Aussi appelés *multi-ensembles*.

- L'ensemble des sacs est bien fondé pour cette relation (c'est un compte à rebours infernal à k compteurs, k étant la plus grande valeur).
- A chaque tour d'une bataille d'hydre, le sac associé à l'hydre « diminue ».

Et pour une hydre quelconque ?

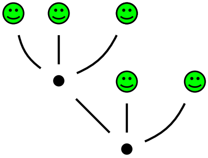


Théorème (Kirby et Paris, 1982)

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

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 se fait en plus de $10^{10^{30}}$ rounds !.



Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$

$$\omega,$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega + 1,$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$
$$\omega+\omega,$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$
$$\omega+\omega, \omega+\omega+1, \omega+\omega+2, \ldots$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$
$$\omega+\omega, \omega+\omega+1, \omega+\omega+2, \ldots$$
$$\ldots$$
$$\omega^{\omega}, \ldots, \omega^{\omega^{\omega}}, \ldots$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$
$$\omega+\omega, \omega+\omega+1, \omega+\omega+2, \ldots$$
$$\ldots$$
$$\omega^{\omega}, \ldots, \omega^{\omega^{\omega}}, \ldots$$
$$\epsilon_0 = \omega^{\omega^{\omega^{\omega^{\cdots}}}}$$

Cantor : les ordinaux

$$0, 1, 2, 3, 4, \ldots, n, n+1, \ldots$$
$$\omega, \omega+1, \omega+2, \ldots$$
$$\omega+\omega, \omega+\omega+1, \omega+\omega+2, \ldots$$
$$\ldots$$
$$\omega^{\omega}, \ldots, \omega^{\omega^{\omega}}, \ldots$$
$$\epsilon_0 = \omega^{\omega^{\omega^{\omega^{\cdots}}}}, \epsilon_0 + 1, \ldots,$$

La classe des ordinaux, comme les entiers, est bien fondée.

On se fait la main avec ω ($\mathbb{N}$)

Pourquoi recourir aux ordinaux ?

On se fait la main avec ω ($\mathbb{N}$)

Pourquoi recourir aux ordinaux ?

1. Supposons qu'il existe un variant à valeurs dans $\mathbb{N}$ pour notre problème de terminaison.
2. On définit une injection ι associant à tout entier i l'hydre composée d'un pied et $i + 1$ têtes.

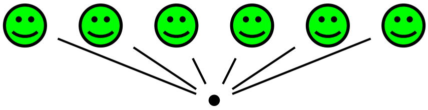


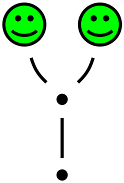
Figure: L'hydre $\iota(5)$

On considère alors l'hydre h_ω ci-dessous :

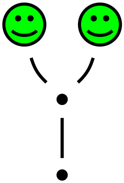
On considère alors l'hydre h_ω ci-dessous :

Il faut nécessairement lui attribuer un convergent $\geq \omega$

Qui de celle-ci ?

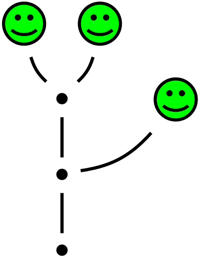


Qui de celle-ci ?

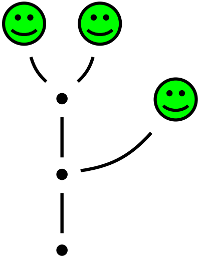


Convergent : ω^2

Et celle-ci ?



Et celle-ci ?



Convergent : ω^{ω^2+1}

Terminaison et ordinaux

- A chaque fois qu'on coupe une tête, le convergent décroît strictement (en tant qu'ordinal)
- Or la classe des ordinaux est bien fondée (pas de suite infinie strictement décroissante)
- Le convergent finit donc par se stabiliser sur une valeur, qui ne peut être que 0, ce qui correspond à une hydre vaincue.

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 (arithmétique, quantification sur les entiers récurrence 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 (arithmétique, quantification sur les entiers récurrence simple).

Remarque

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

Remarque pour les mathématiciens

La complexité des trois problèmes de terminaison précédents peut se mesurer à l'aide des ordinaux de Cantor :

Compte à rebours : ω^3

Hydre dont les tentacules sont de longueur ≤ 2 : ω^ω

Hydre quelconque : ϵ_0 (plus grand que ω^ω, ω^{ω^ω}, $\omega^{\omega^{\omega^\omega}}$, ...)