# Lemme de Kruskal et un critère de terminaison.

Frédéric Valet

25 janvier 2015

**Définition 1.** *Un pré-ordre sur un ensemble $D$ est une relation binaire $\leq$ vérifiant les conditions de réflexivité et de transitivité. Un beau pré-ordre $\prec$ (ou pré-bel-ordre) sur cet ensemble est un pré-ordre tel que pour toute suite infinie $(s_i)_{i\in\mathbb{N}}$ de $D$, il existe un couple $i < j$ tel que $s_i \prec s_j$.*

**Proposition 2.** *Si $\prec$ est un pré-ordre sur $D$, alors on a équivalence entre :*
- *$\prec$ est un beau pré-ordre.*
- *Pour toute suite infinie $(s_i)_{i\in\mathbb{N}}$ de $D$, il existe une fonction $\phi : \mathbb{N} \to \mathbb{N}$ injective et croissante telle que la sous-suite $(s_{\phi(i)})_i$ soit strictement croissante :*

$$\forall i \in \mathbb{N} \ , \ s_{\phi(i)} \prec s_{\phi(i+1)}.$$

*Démonstration.* La seconde caractérisation implique facilement la première. Montrons qu'un pré-bel ordre nous permet de définir une sous-suite strictement croissante. Soit donc $(s_i)_i$ une suite dans $D$, on pose :

$$B := \{i \in \mathbb{N} \, ; \, \forall i < j \ , \ s_i \not\prec s_j\}.$$

Cet ensemble contient les éléments ne pouvant pas être le début d'une suite croissante. Deux cas se présentent : si $B$ est de cardinal infini, alors la suite dés éléments de $B$ ne peuvent pas respecter la condition du beau-pré ordre. Donc $B$ est de cardinal fini. On pose $M$ une borne supérieure de $B \subset \mathbb{N}$ ; en considérant la suite $(s_i)_{M\leq i}$, par hypothèse du beau-pré ordre, il existe un couple $(i, j)$ avec $M < i < j$ tel que $s_i \prec s_j$. Puisque $M < j$, cela implique que $s_j \notin B$, donc il existe un élément $s_{j'}$ avec $j < j'$ et $s_j \prec s_{j'}$. Puis on continue cette récurrence, ce qui nous permet de trouver la suite infinie strictement croissante. □

**Théorème 3.** ***de Higman*** *Soit $\prec$ un beau-pré ordre sur $D$. Alors on définit la relation $\trianglelefteq$ suivante sur $D^*$, ensemble des mots sur $D$ :*
- *pour $\epsilon$ le mot vide : $\epsilon \trianglelefteq \epsilon$.*
- *si $s \trianglelefteq t$ et $b \in D$ alors $s \trianglelefteq b \cdot t$.*
- *si $a \prec b$ et $s \trianglelefteq t$ alors $a \cdot s \trianglelefteq b \cdot t$.*

*C'est un beau-pré ordre.*

*Démonstration.* Supposons par l'absurde, que le pré-ordre $\trianglelefteq$ ne soit pas un beau-pré-ordre. Par la définition du beau-pré-ordre, il existe une suite infinie de mots $(s_i)_i$ telle que pour tout $i < j$, $s_i \not\trianglelefteq s_j$. On note :

$$E := \{(s_i)_{i\in\mathbb{N}} \ , \ \forall i < j \ , \ s_i \not\trianglelefteq s_j\}.$$

Cet ensemble admet un élément minimal, dans le sens où une suite $(s_i)_i$ est inférieure à une autre $(t_i)_i$ s'il existe un $i_0$ tel que :

$$\forall i < i_0 \ , \ |s_i| = |t_i| \text{ et } |s_{i_0}| \leq |t_{i_0}|.$$

Cette manière de comparer ressemble à l'ordre lexicographique sur les longueurs des mots. On remarque qu'aucun mot ne peut être le mot vide.
On note donc $(s_i)_i$ une suite minimisante. Soit $a_i$ la première lettre du mot $s_i = a_i \cdot w_i$, et ce pour chaque $i$. Puisque l'ordre $\prec$ est un pré-bel-ordre, on peut extraire une sous-suite $(a_{\phi(i)})_i$, qui soit strictement croissante pour $\prec$. Soit à présent la suite de mots :

$$(x_i)_{i\in\mathbb{N}} := s_0, s_1, \cdots, s_{\phi(0)-1}, w_{\phi(0)}, w_{\phi(1)}, w_{\phi(2)}, \cdots$$

Puisque $|w_{\phi(0)}| < |s_{\phi(0)}|$, la suite $(x_i)_i$ est plus petite que la suite $(s_i)_i$, donc cette suite n'appartient pas à $E$. Il existe donc deux indices $i < j$ tels que $x_i \trianglelefteq x_j$. On a vu qu'on ne pouvait pas avoir $j < \phi(0)$. Si $i < \phi(0) \leq j$, alors $s_i \trianglelefteq w_j$, et par définition de $\trianglelefteq$, $s_i \trianglelefteq s_j$, ce qui est absurde. Donc $\phi(0) \leq i < j$ ; on a $w_i \trianglelefteq w_j$ et $a_i \prec a_j$ par extraction de la sous-suite, donc $s_i \trianglelefteq s_j$, ce qui est absurde. □

On peut définir à présent l'ordre de plongement :

**Définition 4.** *Soit $\Sigma$ une signature, muni d'un pré-bel ordre $\prec$. L'ordre de plongement, noté $\trianglelefteq$, et dont le symbole ne sera associé plus qu'au plongement, est défini sur l'ensemble des termes $T = T(\Sigma)$ par :*

- *Soient $s, b_1, \cdots, b_n$ des termes et $t$ un symbole de fonctions d'arité $n$ .*
  *Si pour un $i$ en particulier, on a $s \trianglelefteq b_i$, alors $s \trianglelefteq t(b_1, \cdots, b_n)$.*
- *Soient deux termes $s(a_1, \cdots, a_m)$ et $t(b_1, \cdots, b_n)$.*
  *Si $s \prec t$ et il existe une sous-suite croissante $\{j_1, \cdots, j_m\}$ de $[|1, n|]$ telle que pour tout $i \leq n$, $a_i \trianglelefteq b_{j_i}$, alors on a $s(a_1, \cdots, a_m) \trianglelefteq t(b_1, \cdots, b_n)$.*

L'ordre de plongement est un pré-ordre.

**Théorème 5.** ***de Kruskal*** *Étant donné un pré-bel-ordre $\prec$ sur une signature $\Sigma$, le plongement $\trianglelefteq$ est un pré-bel-ordre sur les termes $T(\Sigma)$.*

*Démonstration.* Comme dans la preuve du lemme de Higman, on suppose que le plongement n'est pas un pré-bel-ordre. Soit $E$ l'ensemble des suites de termes $(s_i)_i$ vérifiant $\forall i < j$ , $s_i \not\trianglelefteq s_j$. On choisit une suite minimale : $(s_i)_i$ est inférieure $(s'_i)_i$ s'il existe $i_0$ tel que :

$$\forall i < i_0 \ , \ |s_i| = |s'_i| \text{ et } |s_{i_0}| < |s'_{i_0}|,$$

où cette fois-ci on compare deux suites similairement à l'ordre lexicographique sur les hauteurs des termes. De même, le mot vide ne peut être dans la suite.
Posons pour chaque $i$, $s_i := t_i(a^i_1, \cdots, a^i_{r_i})$ ; on peut définir une sous suite $(t_{\phi(i)})_i$ qui soit strictement croissante pour $\prec$.
On considère à présent, sur l'alphabet $\mathcal{A}$ (qui est dénombrable) constitué des lettres :

$$(a_1^{\phi(1)}, \cdots, a_{r_{\phi(1)}}^{\phi(1)}, \cdots, a_1^{\phi(i)}, \cdots, a_{r_{\phi(i)}}^{\phi(i)}, \cdots).$$

Montrons que $\trianglelefteq$ est un pré-bel-ordre sur $\mathcal{A}$. Si ce n'en était pas un, on peut considérer une suite $r = (r_1, \cdots, r_i, \cdots)$ telle que pour tout $i < j$, $r_i \not\trianglelefteq r_j$. Cette propriété tient aussi pour toute sous-suite. De plus, il existe deux indices $i < j$ tels que $r_i$ (respectivement $r_j$) soit le sous-terme d'un élément $s_p$ (respectivement $s_q$) avec $p < q$. En effet, $r$ doit contenir une infinité de de termes différents, mais chaque terme $s_i$ ne contient qu'un nombre fini de termes. On peut itérer ce procédé, et on trouve une sous-suite $r' = (r'_1, \cdots, r'_i, \cdots)$ de $r$ telle que pour $i < j$, le terme $r'_i$ (respectivement $r'_j$) soit le sous-terme d'un terme $s_p$ (respectivement $s_q$) avec $p < q$. Soit $n$ l'indice du premier terme $s_n$ admettant $r'_1$ comme sous-terme. Si $n = 1$, alors $r'$ contredit la minimalité de la suite $s$. On a donc $n \geq 2$, et cette fois-ci, la suite :

$$(s_1, \cdots, s_{n-1}, r'_1, \cdots, r'_i, \cdots)$$

contredit la minimalité de $s$ (il faut faire par disjonction de cas, comme dans le lemme de Higman). On a donc conclu que $\trianglelefteq$ est un pré-bel-ordre sur l'alphabet $\mathcal{A}$.

D'après le lemme de Higman, on peut étendre ce pré-bel-ordre aux mots sur l'alphabet $\mathcal{A}$. En particulier, les mots $w_i := a_1^{\phi(i)}, \cdots, a_{r_\phi(i)}^{\phi(i)}$ définis pour chaque $i$ sont des mots de $\mathcal{A}*$. On peut donc extraire de la suite $(w_i)_i$ deux termes $w_i$ et $w_j$ avec $i < j$ tels que $w_i \trianglelefteq w_j$. Cependant, grâce à la première extraction sur $(t_i)_i$, on a obtenu (en utilisant la transitivité) que $t_i \trianglelefteq t_j$. Donc en composant, on obtient $s_i \trianglelefteq s_j$, ce qui est absurde. □

On a le corollaire immédiat suivant :

**Corollaire 6.** *Si la signature $\Sigma$ est finie et est munie d'un pré-bel-ordre, alors de toute suite infinie de termes $(s_i)_i$, on peut extraire deux termes $s_i$ et $s_j$ tels que $i < j$ et $s_i \trianglelefteq s_j$.*

**Définition 7.** *Soit $\Sigma$ une signature.*
*Un ordre de réduction $<$ sur les termes $T(\Sigma)$ est un ordre bien fondé, qui soit clos par substitution (si $s < t$ alors pour $\sigma$ une substitution, $\sigma(s) < \sigma(t)$)et compatible avec les opérations (si $C$ est un contexte, c'est-à-dire un terme avec un "trou", et si $s < t$ alors $C[s] < C[t]$).*
*Un ordre de simplification $<$ est un ordre sur les termes, clos par substitution, compatible avec les opérations et vérifiant :*

$$\forall f \in \Sigma^{(n)}, \forall i \leq n \ , \ x_i < f(x_1, \cdots, x_n).$$

*Un système de réduction terminant $R$ est dit simplifiant s'il existe un ordre de simplification $<$ tel que :*

$$\forall t, t' \text{ termes vérifiant } t \to_R t' \text{ alors } t' < t.$$

**Proposition 8.** *Soit $<$ un ordre de simplification sur $T(\Sigma)$. Si $\Sigma$ est finie, alors $<$ est bien fondée.*

Remarque : La bien-fondaison nous permet d'avoir un ordre de réduction, qui lui va nous donner automatiquement la terminaison du système de réécriture.

*Démonstration.* Supposons par l'absurde qu'il existe une suite infinie $(s_i)_i$ de termes décroissante pour l'ordre de simplification $<$ : pour tout $i$, $s_i > s_{i+1}$.
A $i$ fixé, supposons que $s_{i+1}$ contienne une variable $x$ n'ayant aucune occurrence dans $s_i$. Alors en posant $\sigma = [s_i/x]$, alors :

$$s_i = \sigma(s_i) > \sigma(s_{i+1}) = C[s_i],$$

où $C$ est le contexte tel que $s_{i+1} = C[s_i]$. Donc $s_i > C[s_i]$, ce qui contredit la définition de l'ordre de simplification.
Ainsi quelque soit $i$, $s_{i+1}$ n'a que des variables de $s_i$. Donc dans cette suite, il n'y a qu'un nombre fini de variables. On peut considérer maintenant ces variables comme étant des constantes. La nouvelle signature est donc finie. La suite $(s_i)_i$ est donc une suite de termes clos, sans variables. Par la proposition précédente, il existe $i < j$ tel que $s_i \trianglelefteq s_j$. $s_i$ se plonge dans $s_j$, et cela nous donne $s_i < s_j$ (se fait par induction, ou par un dessin). Ceci contredit la décroissance de $(s_i)_i$. □

# Références


[1] Hubert Comon et Jean-Pierre Jouannaud. Les termes en logique et en programmation. http ://www.lsv.ens-cachan.fr/ comon/cours.html, Décembre 1997.

[2] Jean H. Gallier. What's so special about kruskal's theorem and the ordinal t0 ? a survey of some results in proof theory. *University of Pennsylvania, Scholarly Commons*, page 6, September 1993.

[3] Terese. *Term Rewriting Systems.* Cambridge Tracts in Theoretical Computer sciences, 2003.