

Réécriture

Ordre sur les preuves

version du April 4, 2006 – 20 h 16

Rappel

$$E_\infty = \bigcup_{i \geq 0} E_i \qquad R_\infty = \bigcup_{i \geq 0} R_i$$

$$E_\omega = \bigcup_{i \geq 0} \bigcap_{j \geq i} E_j \qquad R_\omega = \bigcup_{i \geq 0} \bigcap_{j \geq i} R_j$$

Petite histoire d'une preuve

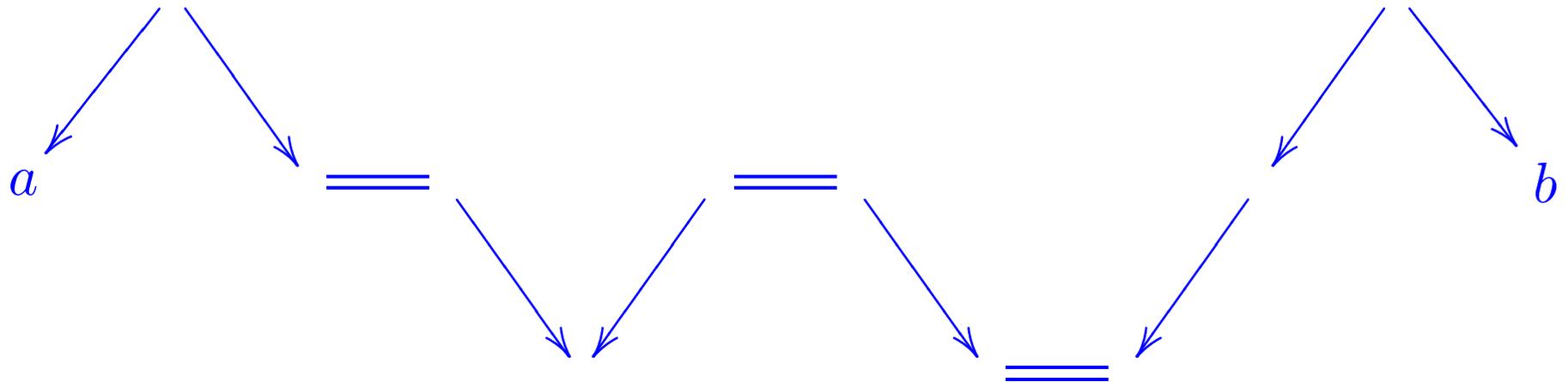
Les preuves de $a = b$

Considérons les preuves équationnelles possibles de l'égalité de deux termes $a = b$.

Au niveau (E_0, R_0) (avec $R_0 = \emptyset$) c'est une preuve complètement par identités.

$$a \equiv b$$

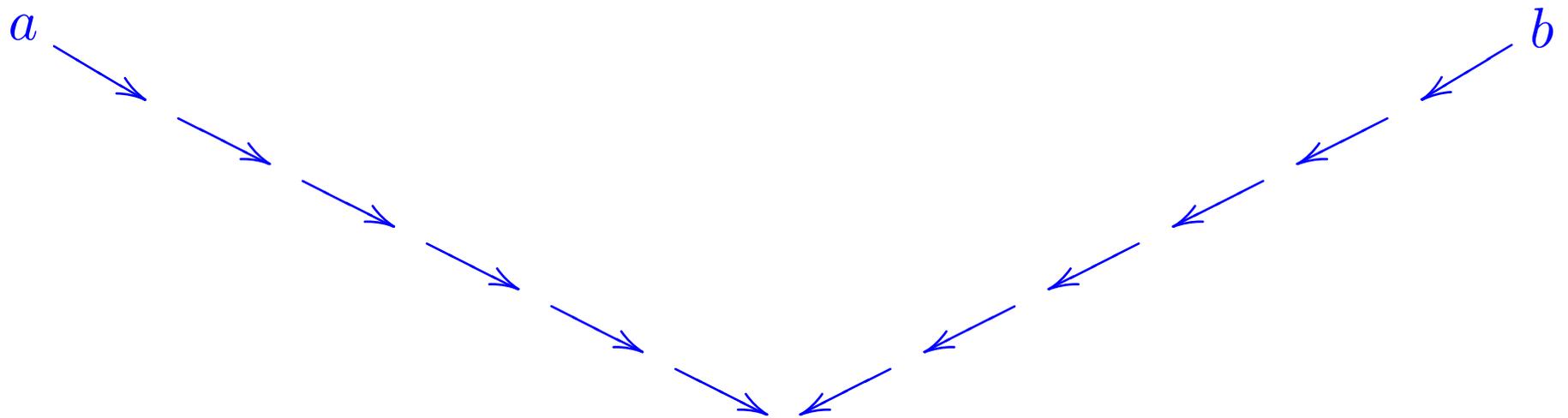
alors qu'au niveau (E_i, R_i) pour un i quelconque, c'est une preuve hétérogène.



Car certaines identités ne sont plus présentes et il faut les remplacer par des réécritures.

Les preuves de $a = b$ (suite)

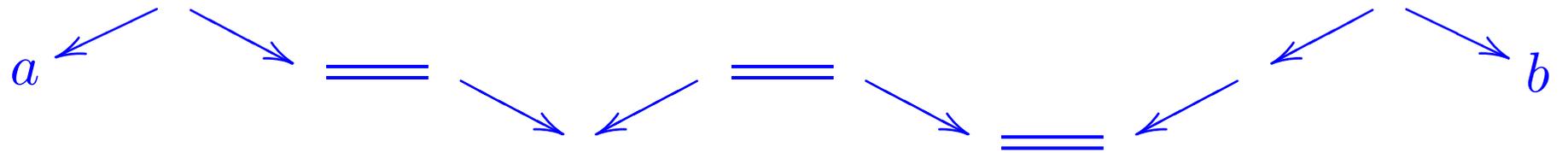
En fait ce qu'on souhaite c'est une preuve complètement par réécriture (une preuve en vallée).



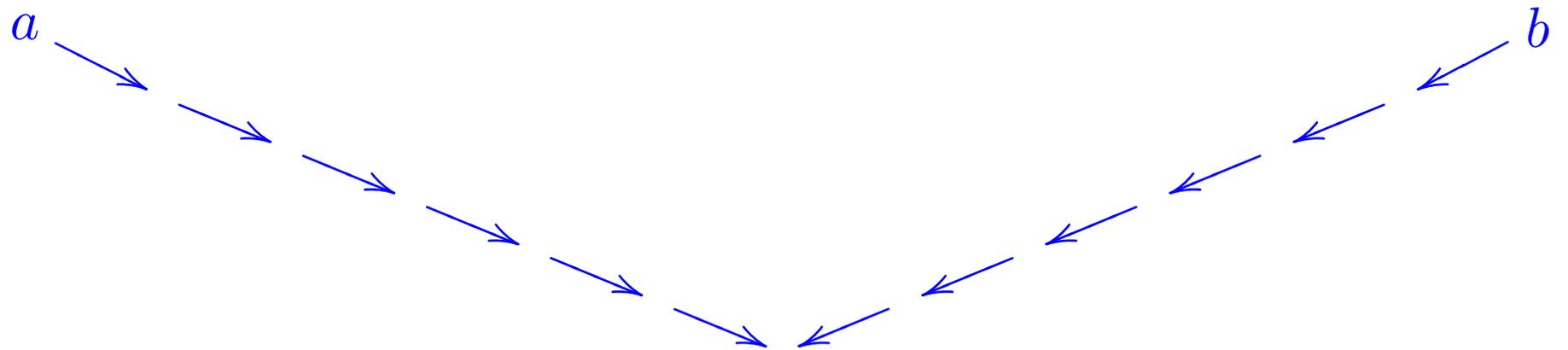
Début



Milieu



Fin



Il faut montrer que pour tout couple tel que $a =_{E_0} b$, il y a une **preuve de réécriture** dans R_ω , c'est-à-dire qu'il existe un c tels que

$$a \xrightarrow[R_\omega]{*} c \xleftarrow[R_\omega]{*} b$$

Il faut donc voir comment les preuves se transforment.

Pour cela, on transforme chaque étape de preuve **en une étape de preuve plus simple** et on montre en se servant d'un ordre noethérien adéquat que le processus de transformation termine.

Un ordre sur les preuves

Le coût d'une preuve

Une preuve où les termes intermédiaires sont $a_1, \dots, a_k, a_{k+1}, \dots, a_n$ est associée au multiensemble $\{a_1 \mathcal{L}_1 a_2, \dots, a_k \mathcal{L}_k a_{k+1}, \dots\}$.

Chaque \mathcal{L}_k représente soit

$$= \quad \rightarrow \quad \leftarrow.$$

On va attribuer à chaque preuve un **coût**.

Auparavant on attribue un **coût** à **chaque étape élémentaire**.

Le **coût d'une preuve** est le **multiensemble des coûts** de chacune de ses étapes élémentaires.

Le coût d'une étape élémentaire

Le **coût** d'une étape élémentaire $a \mathcal{L} b$ est un triplet (M, l, r) .

Le coût d'une paire (suite)

On attribue les coûts de la façon suivante :

- si $a_k \mathcal{L}_k a_{k+1}$ est de la forme $a_k = a_{k+1}$, le coût est $(\{\{a_k, a_{k+1}\}\}, -, -)^a$,
- si $a_k \mathcal{L}_k a_{k+1}$ est de la forme $a_k \rightarrow a_{k+1}$, le coût est $(\{\{a_k\}\}, l, r)$, où l est le membre gauche de la règle de réécriture employée et r est le membre droit de la règle de réécriture employée.
- si $a_k \mathcal{L}_k a_{k+1}$ est de la forme $a_k \leftarrow a_{k+1}$, le coût est $(\{\{a_{k+1}\}\}, l, r)$, où l est le membre gauche de la règle de la réécriture employée et r est le membre droit de la règle de réécriture employée.

^a _ signifie qu'on n'attache pas d'importance à ce champ.

La comparaison des coûts de paires

Pour la première composante (M), c'est l'extension multiensemble de l'ordre sur les termes.

Pour la deuxième composante (l), c'est l'ordre d'enchâssement.

Pour la troisième composante (r), c'est l'ordre sur les termes.

Ainsi

- l'ordre sur les coûts termine.
- l'ordre sur les preuves termine.

L'enchâssement

La relation d'enchâssement \trianglelefteq (en anglais encompassment) est définie par

$$s \trianglelefteq t$$

si et seulement si

$$\exists p \in Pos(s) \cdot \exists \sigma \in Sub(T(\Sigma, V)) \cdot s|_p = \sigma(t)$$

$\trianglelefteq \cap \triangleright$ est =.

▶ est la relation $\underline{\triangleright} \cap \not\sim$ (où \sim est le renommage des variables), elle termine.

L'ordre sur les preuves

L'ordre sur les preuves s'écrit :

$$\mathcal{P} \succ_C \mathcal{P}'$$

Deux preuves sont équivalentes si elles prouvent la même identité.

Décroissance des preuves

Chaque transition fait décroître les preuves.

Si la transition est **Delete**. Si cette transition affecte une étape $a_k \mathcal{L}_k a_{k+1}$ de la preuve alors cette étape disparaît et le coût de la preuve diminue.

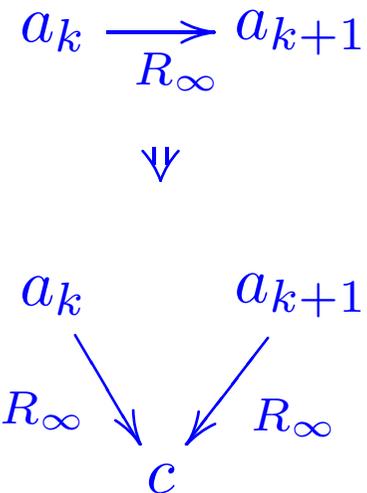
$$\dots a_k \equiv a_{k+1} \dots$$



$$\dots a_k \dots$$

Décroissance des preuves

Si la transition est **Compose**.



$\text{cout}(a_k \rightarrow a_{k+1}) = (\{\{a_k\}\}, s, t) > \text{cout}(a_k \rightarrow c) = (\{\{a_k\}\}, s, u)$ parce que $\{\{a_k\}\} = \{\{a_k\}\}$, $s = s$ et $t > u$,

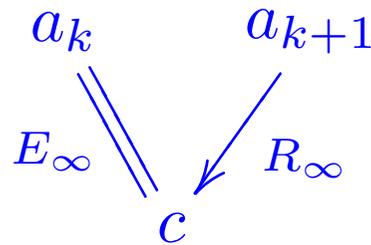
et

$\text{cout}(a_k \rightarrow a_{k+1}) > \text{cout}(c \leftarrow a_{k+1})$ parce que $\{\{a_k\}\} \gg \{\{a_{k+1}\}\}$.

Décroissance des preuves

Si la transition est **Simplify**.

$$a_k \xlongequal[E_\infty]{} a_{k+1}$$



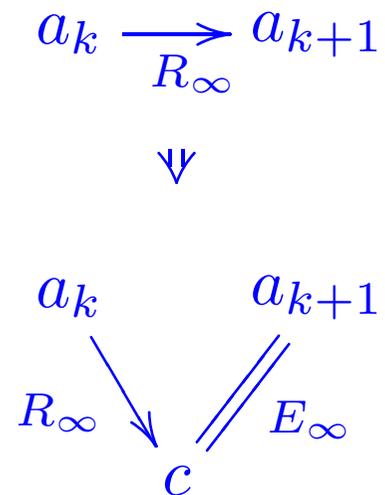
$\text{cout}(a_k = a_{k+1}) > \text{cout}(a_k = c)$ parce que $\{\{a_k, a_{k+1}\}\} \gg \{\{a_k, c\}\}$

et

$\text{cout}(a_k = a_{k+1}) > \text{cout}(c \leftarrow a_{k+1})$ parce que $\{\{a_k, a_{k+1}\}\} \gg \{\{a_{k+1}\}\}$.

Décroissance des preuves

Si la transition est **Collapse**.



$\text{cout}(a_k \rightarrow a_{k+1}) = (\{\{a_k\}\}, s, t) > \text{cout}(a_k \rightarrow c) = (\{\{a_k\}\}, l, r)$ parce que $\{\{a_k\}\} = \{\{a_k\}\}$, et ou bien ou bien $s \blacktriangleright l$ ou bien $s = l$ et $t > r$.

et

$\text{cout}(a_k \rightarrow a_{k+1}) > \text{cout}(c = a_{k+1})$ parce que $\{\{a_k\}\} \gg \{\{c, a_{k+1}\}\}$.

Décroissance des preuves

Si la transition est **Orient**.

$$a_k \stackrel{=}{R_\infty} a_{k+1}$$

\Downarrow

$$a_k \xrightarrow{R_\infty} a_{k+1}$$

$\text{cout}(a_k = a_{k+1}) > \text{cout}(a_k \rightarrow a_{k+1})$ parce que $\{\{a_k, a_{k+1}\}\} \gg \{\{a_k\}\}$.

Décroissance des preuves

Comment décroître un pic ? $a_{k-1} \xleftarrow{R_\infty} a_k \xrightarrow{R_\infty} a_{k+1}$

Sans nuire à la généralité, on peut supposer que le pic est un pic dans R_ω soit $a_{k-1} \xleftarrow{R_\omega} a_k \xrightarrow{R_\omega} a_{k+1}$.

Sinon ce pic disparaît par l'une des transitions **Compose** ou **Collapse** déjà vues.

Décroissance des preuves

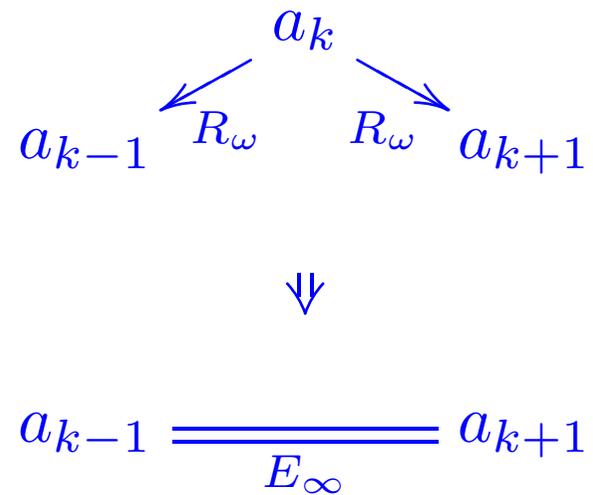
Comment décroître un pic ?

Deux cas :

1. il s'agit d'une paire critique de R_ω ,
2. il s'agit de deux règles qui s'appliquent sans superposition.

Comment décroître un pic ?

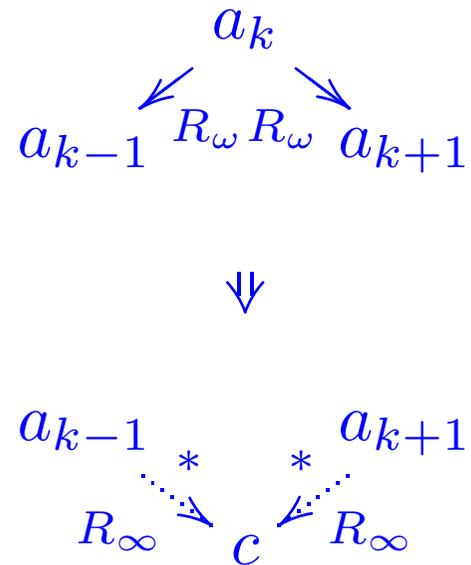
Pour le cas 1, grâce à l'équité, on sait qu'une transition **Deduce** va s'appliquer tôt ou tard et



et on remarque que $\{a_k\} \gg \{a_{k-1}, a_{k+1}\}$

Comment décroître un pic ?

Pour le cas 2, sans le besoin d'aucune transition cette preuve a, à l'étape i , une preuve d'un coût moindre.



En effet, $\{a_k\}$ domine toutes les étapes de réécriture de

$$a_{k-1} \xrightarrow{*} c \xleftarrow{*} a_{k+1}.$$

Théorème :

Le contrôle de la complétion est supposé équitable.

Si il existe une preuve \mathcal{P} dans $E_\infty \cup R_\infty$

qui n'est pas une preuve de réécriture

alors il existe dans $E_\infty \cup R_\infty$ une preuve \mathcal{P}'
équivalente à \mathcal{P} telle que $\mathcal{P} \succ_C \mathcal{P}'$.

Théorème :

Le contrôle de la complétion est supposé équitable.

Si il existe une preuve \mathcal{P} dans $E_\infty \cup R_\infty$

qui n'est pas une preuve de réécriture

alors il existe dans $E_\infty \cup R_\infty$ une preuve \mathcal{P}'
équivalente à \mathcal{P} telle que $\mathcal{P} \succ_C \mathcal{P}'$.

Par les résultats précédents, si la preuve \mathcal{P} n'est pas une preuve par réécriture, elle peut-être réduite.

Corollaire:

Le contrôle de la complétion est supposé équitable.

- Si il existe une preuve \mathcal{P} dans $E_\infty \cup R_\infty$
alors il existe une **preuve de réécriture équivalente** dans R_ω .
- R_ω est **canonique**, c-à-d est **confluent**, **terminant** et **interréduit**.
- Si R_ω est fini alors **le problème du mot** dans E_0 est **décidable**.