

Réécriture.

Définition 1. Soit \rightarrow une relation binaire sur un ensemble E . Le 2-uplet (E, \rightarrow) est un *SRA*, pour *système de réécriture abstraite*.

Soit $x_0 \in E$. Une *divergence* issue de x_0 est une suite $(x_i)_{i \in \mathbb{N}}$ telle que, pour tout i , on a $x_i \rightarrow x_{i+1}$.

La relation \rightarrow est *terminante* ou *termine* si et seulement si, quel que soit $x \in E$, il n'y a pas de divergence issue de x .

La relation \rightarrow diverge s'il existe une divergence.

Exemple 1. En général, une relation réflexive est divergente.

Théorème 1. Une relation (E, \rightarrow) est terminante si et seulement si elle satisfait le *principe d'induction bien fondée (PIBF)* suivant :

Pour tout prédicat \mathcal{P} sur E , si pour tout $x \in E$

$$\left[\forall y \in E, x \rightarrow y \text{ implique } \mathcal{P}(y) \right] \text{ implique } \mathcal{P}(x)$$

alors, pour tout $x \in E$, $\mathcal{P}(x)$.

En particulier, dans le principe d'induction bien fondée, on demande que les feuilles (les éléments sans successeurs) vérifient le prédicat.

Preuve. \triangleright « PIBF \implies terminaison ». Montrons que, quel

que soit $x \in E$,

$\mathcal{P}(x)$: « il n'y a pas de divergence issue de x ».

Soit $\text{Next}(x) = \{y \in E \mid x \rightarrow y\}$. On suppose que, pour tout $y \in \text{Next}(x)$, on a $\mathcal{P}(y)$. On en déduit $\mathcal{P}(x)$ car, sinon, une divergence ne passerait pas par $y \in \text{Next}(x)$. Par le principe d'induction bien fondée, on en déduit

$$\forall x \in E, \mathcal{P}(x),$$

autrement dit, la relation \rightarrow termine.

- ▷ « \neg PIBF \implies diverge », par contraposée. On suppose qu'il existe un prédicat \mathcal{P} tel que,

$$\forall x, (\forall y, x \rightarrow y \text{ implique } \mathcal{P}(y)) \text{ implique } \mathcal{P}(x),$$

et que l'on n'ait pas, $\forall x \in E, \mathcal{P}(x)$ autrement dit qu'il existe $x_0 \in E$ tel que $\neg\mathcal{P}(x_0)$.

Intéressons-nous à $\text{Next}(x_0) = \{y \in E \mid x_0 \rightarrow y\}$. Si, pour tout $y \in \text{Next}(x_0)$ on a $\mathcal{P}(y)$ alors par hypothèse $\mathcal{P}(x_0)$, ce qui est impossible. Ainsi, il existe $x_1 \in \text{Next}(x_0)$ tel que $\neg\mathcal{P}(x_1)$. On itère ce raisonnement, ceci crée notre divergence.

□

Remarque 1. L'induction bien fondée s'appelle aussi l'induction *noethérienne*, en référence à Emmy Noether, mathématicienne allemande du IX–Xème siècle.

Une application de ce principe d'induction est le *lemme de König*.

Définition 2. ▷ Un arbre est *fini* s'il a un nombre fini de nœuds (*infini* sinon).

- ▷ Un arbre est à *branchement fini* si tout nœud a un nombre fini d'enfants immédiats.
- ▷ Une branche est *infinie* si elle contient un nombre infini de nœuds.

Lemme 1 (Lemme de König). Si un arbre est à branchement fini est infini alors il contient une branche infinie.

Preuve. On considère E l'ensemble des nœuds de l'arbre, et on définit la relation \rightarrow par : on a $x \rightarrow y$ si y est enfant immédiat de x . On montre qu'un arbre à branchement fini sans branche infinie (*i.e.* la relation \rightarrow termine) est fini. On choisit la propriété $\mathcal{P}(x)$: « le sous-arbre enraciné en x est fini. »

Montrons que, quel que soit x , $\mathcal{P}(x)$ et pour ce faire, utilisons le principe d'induction bien fondée puisque la relation \rightarrow termine. On doit montrer que, si $\forall y \in \text{Next}(x), \mathcal{P}(y)$ implique $\mathcal{P}(x)$. Ceci est vrai car l'embranchement est fini. \square

1 Liens avec les définitions inductives.

On considère E l'ensemble inductif défini par la grammaire suivante :

$$t ::= F \mid N(t_1, k, t_2).$$

C'est aussi le plus petit point fixe de l'opérateur f associé (par le théorème de Knaster–Tarski).

On définit la relation \rightarrow binaire sur E par : on a $x \rightarrow y$ si et seulement si on a $x = N(y, k, z)$ ou $x = N(z, k, y)$.

On sait que la relation \rightarrow termine. En effet, l'ensemble des arbres finis est un point fixe de la fonction f , donc E ne contient que des arbres finis.

Le principe d'induction bien fondée nous dit que, pour \mathcal{P} un prédicat sur E , pour montrer $\forall x, \mathcal{P}(x)$, il suffit de montrer que, quel que soit x , si $(\forall y, x \rightarrow y$ implique $\mathcal{P}(y))$ alors $\mathcal{P}(x)$. Autrement dit, il suffit de

montrer que $\mathcal{P}(\mathbb{E})$ puis de montrer que, si $\mathcal{P}(t_1)$ et $\mathcal{P}(t_2)$ alors on a que $\mathcal{P}(\mathbb{N}(t_1, k, t_2))$.

On retrouve le principe d'induction usuel.

Ce même raisonnement, on peut le réaliser quel que soit l'ensemble inductif, car la relation de « sous-élément » termine toujours puisque il n'y a que des éléments finis dans l'ensemble inductif.

2 Établir la terminaison.

Théorème 2. Soient $(B, >)$ un SRA terminant, et (A, \rightarrow) un SRA. Soit $\varphi : A \rightarrow B$ un *plongement*, c'est à dire une application vérifiant

$$\forall a, a' \in A, \quad a \rightarrow a' \text{ implique } \varphi(a) > \varphi(a').$$

Alors, la relation \rightarrow termine.

Théorème 3. Soient (A, \rightarrow_A) et (B, \rightarrow_B) deux SRA.

Le *produit lexicographique* de (A, \rightarrow_A) et (B, \rightarrow_B) est le SRA, que l'on notera $(A \times B, \rightarrow_{A \times B})$, défini par

$$(a, b) \rightarrow_{A \times B} (a', b') \text{ ssi } \begin{cases} (1) a \rightarrow_A a' \text{ (et } b' \text{ quelconque)} \\ \text{ou} \\ (2) a = a' \text{ et } b \rightarrow_B b' \end{cases} .$$

Alors, les relations (A, \rightarrow_A) et (B, \rightarrow_B) terminent si et seulement si la relation $(A \times B, \rightarrow_{A \times B})$ termine.

Preuve. \triangleright « \implies ». Supposons qu'il existe une divergence pour $(A \times B, \rightarrow_{A \times B})$:

$$(a_0, b_0) \rightarrow_{A \times B} (a_1, b_1) \rightarrow_{A \times B} (a_2, b_2) \rightarrow_{A \times B} \dots .$$

Dans cette divergence,

- soit on a utilisé (1) une infinité de fois, et alors en projetant sur la première composante et en ne conservant que les fois où l'on utilise (1), on obtient une divergence \rightarrow_A ;
- soit on a utilisé (1) un nombre fini de fois, et alors à partir d'un certain rang N , pour tout $i \geq N$, on a l'égalité $a_i = a_N$, et donc on obtient une divergence pour \rightarrow_B :

$$b_N \rightarrow_B b_{N+1} \rightarrow_B b_{N+2} \rightarrow \dots$$

- ▷ « \Leftarrow ». On montre que, si on a une divergence pour \rightarrow_A alors on a une divergence pour $\rightarrow_{A \times B}$ (on utilise (1) une infinité de fois) ; puis que si on a une divergence pour \rightarrow_B alors on a une divergence pour $\rightarrow_{A \times B}$ (on utilise (2) une infinité de fois).

□

3 Application à l'algorithme d'unification.

On note $(\mathcal{P}, \sigma) \rightarrow (\mathcal{P}', \sigma')$ la relation définie par l'algorithme d'unification (on néglige le cas où $(\mathcal{P}, \sigma) \rightarrow \perp$).

On note $|\mathcal{P}|$ la somme des tailles (vues comme des arbres) des contraintes de \mathcal{P} et $|\text{Vars } \mathcal{P}|$ le nombre de variables.

On définit $\varphi : (\mathcal{P}, \sigma) \mapsto (|\text{Vars } \mathcal{P}|, |\mathcal{P}|)$.

Rappelons la définition de la relation \rightarrow dans l'algorithme d'unification :

1. $(\{f(t_1, \dots, t_k) \stackrel{?}{=} f(u_1, \dots, u_n) \sqcup \mathcal{P}, \sigma\}) \rightarrow (\{t_1 \stackrel{?}{=} u_1, \dots, t_k \stackrel{?}{=} u_k\} \cup \mathcal{P}, \sigma)$;
2. $(\{f(t_1, \dots, t_k) \stackrel{?}{=} g(u_1, \dots, u_n) \sqcup \mathcal{P}, \sigma\}) \rightarrow \perp$ si $f \neq g$;
3. $(\{X \stackrel{?}{=} t\} \sqcup \mathcal{P}, \sigma) \rightarrow (\mathcal{P}[t/X], [t/X] \circ \sigma)$ où $X \notin \text{Vars}(t)$;

4. $(\{X \stackrel{?}{=} t\} \sqcup \mathcal{P}, \sigma) \rightarrow \perp$ si $X \in \text{Vars}(t)$ et $t \neq X$;
5. $(\{X \stackrel{?}{=} X\} \sqcup \mathcal{P}, \sigma) \rightarrow (\mathcal{P}, \sigma)$.

Appliquons le plongement pour montrer que \rightarrow termine. On s'appuie sur le fait que le produit $(\mathbb{N}, >) \times (\mathbb{N}, >)$ est terminant (produit lexicographique).

Dans 1, $|\text{Vars } \mathcal{P}|$ ne change pas et $|\mathcal{P}|$ diminue. Puis dans 3, $|\text{Vars } \mathcal{P}|$ diminue. Et dans 5, on a $|\text{Vars } \mathcal{P}|$ qui décroît ou ne change pas, mais $|\mathcal{P}|$ diminue. Dans les autres cas, on arrive, soit sur \perp .

On en conclut que l'algorithme d'unification termine.

4 Multiensembles.

Définition 3. Soit A un ensemble. Un *multiensemble* sur A est la donnée d'une fonction $M : A \rightarrow \mathbb{N}$. Un multiensemble M est *fini* si $\{a \in A \mid M(a) > 0\}$ est fini.

Le multiensemble vide, noté \emptyset , vaut $a \mapsto 0$.

Pour deux multiensembles M_1 et M_2 sur A , on définit

- ▷ $(M_1 \cup M_2)(a) = M_1(a) + M_2(a)$;
- ▷ $(M_1 \ominus M_2)(a) = M_1(a) \ominus M_2(a)$ où l'on a $(n + k) \ominus n = k$ mais $n \ominus (n + k) = 0$.

On note $M_1 \subseteq M_2$ si, pour tout $a \in A$, on a $M_1(a) \leq M_2(a)$.

La *taille* de M est $|M| = \sum_{a \in A} M(a)$.

On note $x \in M$ dès lors que $x \in A$ et que $M(x) > 0$.

Exemple 2. Si on lit $\{1, 1, 1, 2, 3, 4, 3, 5\}$ comme un multiensemble M , on obtient que $M(1) = 3$, et $M(2) = 1$, et $M(3) = 2$, et $M(4) = 1$, et $M(5) = 1$, et finalement pour tout autre entier n , $M(n) = 0$.

Définition 4 (Extension multiensemble.). Soit $(A, >)$ un SRA. On lui associe une relation notée $>_{\text{mul}}$ définie sur les multiensembles finis sur A en définissant $M >_{\text{mul}} N$ si et seulement s'il existe X, Y deux multiensembles sur A tels que

- ▷ $\emptyset \neq X \subseteq M$;
- ▷ $N = (M \ominus X) \cup Y$ ¹
- ▷ $\forall y \in Y, \exists x \in X, x > y$.

Les multiensembles X et Y sont les « témoins » de $M >_{\text{mul}} N$.

Exemple 3. Dans $(\mathbb{N}, >)$, on a

$$\{1, 2, \underbrace{5}_X\} >_{\text{mul}} \{1, 2, \underbrace{4, 4, 4, 3, 3, 3, 3}_Y\}.$$

Théorème 4. La relation $>$ termine si et seulement si $>_{\text{mul}}$ termine.

Preuve. ▷ « \Leftarrow ». Une divergence de $>$ induit une divergence de $>_{\text{mul}}$.

▷ « \Rightarrow ». On se donne une divergence pour $>_{\text{mul}}$:

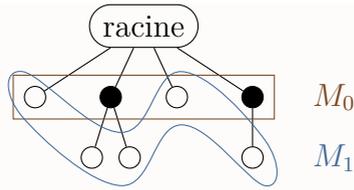
$$M_0 >_{\text{mul}} M_1 >_{\text{mul}} M_2 >_{\text{mul}} \dots ,$$

et on montre que $>$ diverge. À chaque $M_i >_{\text{mul}} M_{i+1}$ correspondent X_i et Y_i suivant la définition de $>_{\text{mul}}$.

On sait qu'il y a une infinité de i tel que $Y_i \neq \emptyset$. En effet, si au bout d'un moment Y_i est toujours vide alors $|M_i|$ décroît strictement, impossible.

Représentons cela sur un arbre.

1. C'est ici la soustraction usuelle : il n'y a pas de soustraction qui « pose problème ».



On itère le parcours en obtenant un arbre à branchement fini, qui est infini (observation du dessin) donc par le lemme de König il a une branche infinie. Par construction d'enfant de a correspond à $a > a'$, d'où divergence pour $>$.

□