Techniques pour montrer la terminaison

La terminaison est une propriété indécidable.

Indécidabilité de la terminaison

Soient $a_1, a_2, a_3, \ldots$ une numérotation de tous les algorithmes sur les entiers. On définit les fonctions suivantes :

$\mathtt{end}(i, n) \equiv 1$ si $a_i(n)$ termine
$\mathtt{end}(i, n) \equiv 0$ si $a_i(n)$ $\neg$ termine

$\mathtt{Diag}(i) \equiv$ si $\mathtt{end}(i, i) = 1$ alors boucler
sinon s'arreter avec un résultat

Pour tout i, $\mathtt{Diag}(i)$ termine ssi $a_i(i)$ ne termine pas.

Mais il y a un a_j tel que $\mathtt{Diag} = a_j$. Nous avons donc

$Diag(j)$ termine ssi $a_j(j)$ termine, ce qui donne

$a_j(j)$ termine ssi $a_j(j)$ ne termine pas.

Quel est l'erreur dans cette demonstration ?

Techniques pour montrer la terminaison

- Par ordres de réduction
  - Interprétation
  - Ordres polynômiaux
- Par paires de dépendance
- Par ordre produit
- Par ordre lexicographique
- Par ordre multi-ensemble
- Par ordres de simplification
  - Résultat général
  - Exemple : les ordres récursifs sur les chemins
- Par ajournement
- Par projection

Terminaison par ordres de réduction

Un ordre strict $\succ$ sur $\mathcal{T}(\mathcal{X}, \Sigma)$ est un ordre de réduction ssi

- chaque symbole $f \in \Sigma$ est monotone par rapport à $\succ$
- $\succ$ est stable par substitution
- $\succ$ est bien fondé

Théorème : Un système de réécriture $\mathcal{R}$ termine ssi il existe un ordre de réduction $\succ$ t.q. $l \succ r$ pour toute règle $l \to r \in \mathcal{R}$.

Interprétation comme ordre de réduction

Soit $\mathcal{A}$ une Σ-algèbre et soit $\succ_{\mathcal{A}}$ un ordre strict bien fondé sur le domain de $\mathcal{A}$.

Définition : La relation $\succ$ sur $\mathcal{T}(\mathcal{X}, \Sigma)$ est donnée par :

$s \succ t$ ssi $\Phi(s) \succ_{\mathcal{A}} \Phi(t)$ pour tout homomorphisme $\Phi : \mathcal{T}(\mathcal{X}, \Sigma) \to \mathcal{A}$

Théorème : Si pour tout $f \in \Sigma$, l'interprétation $f^{\mathcal{A}}$ est monotone par rapport à $\succ_{\mathcal{A}}$, alors $\succ$ est un ordre de réduction.

Ordres polynômiaux comme ordres de réduction

Un $\mathbb{N}$-polynôme n-aire P est un polynôme à n arguments $X_1, \ldots, X_n$ ayant de coefficients dans $\mathbb{N}$.

Une Σ-algèbre polynomiale $\mathcal{P}_{\mathbb{N}}$ est définie par :

- Son domain est un sous-ensemble de $\mathbb{N}^+$
- Pour chaque $f \in \Sigma$ d'arité n, il existe un $\mathbb{N}$-polynôme n-aire P_f t.q. $f^{\mathcal{P}_{\mathbb{N}}}(a_1, \ldots, a_n) = P_f(a_1, \ldots, a_n)$.

Un $\mathbb{N}$-polynôme n-aire P est complètement monotone ssi toute variable X_i $(1 \leq i \leq n)$ de P apparaît au moins une fois dans la définition de P avec un coefficient non nul.

Les ordres polynômiaux comme ordres de réduction

Théorème : Soit $\mathcal{P}_{\mathbb{N}}$ une Σ-algèbre polynomiale. Si chaque $f^{\mathcal{P}_{\mathbb{N}}}$ est spécifiée par un polynôme P_f complètement monotone, alors l'ordre $\succ$ associé à $\succ_{\mathcal{P}_{\mathbb{N}}}$ est un ordre de réduction.

Terminaison par paires de dépendance

Soit $\mathcal{R}$ un système de réécriture.

L'ensemble de symboles définis de $\mathcal{R}$ est donné par :
$\mathcal{D} = \{f \mid f(l_1, \ldots, l_n) \rightarrow\ r \in \mathcal{R}\}$.

L'ensemble de symboles constructeurs de $\mathcal{R}$ est donné par :
$\mathcal{C} = \Sigma \setminus \mathcal{D}$.

Une paire de dépendance d'une règle $l \rightarrow r \in \mathcal{R}$ est une paire de la forme $\langle l, f(\vec{s})\rangle$, où $f(\vec{s})$ est un sous-terme de r et $f \in \mathcal{D}$.

L'ensemble $PD(\mathcal{R})$ des paires de dépendance d'un système $\mathcal{R}$ est l'union des paires de dépendance de toutes les règles de $\mathcal{R}$.

Réécriture dans $PD(\mathcal{R})$

Observation :

1. Si $t \models\!\!\Rightarrow_{\mathcal{R}} v$, alors $t \rightarrow_{\mathcal{R}} v$.
2. Si $t \Rightarrow_{\mathcal{R}} v$, alors $t \rightarrow_{\mathcal{R}} v$.
3. Si $u \models\!\!\Rightarrow_{PD(\mathcal{R})} v$, alors il existe un terme t et une position $p \in Pos(t)$ t.q. $u \models\!\!\Rightarrow_{\mathcal{R}} t[v]_p$ (donc $u \rightarrow_{\mathcal{R}} t[v]_p$).

Suite de dépendance

Une suite de dépendance de $\mathcal{R}$ est une suite $u_0, v_0, u_1, v_1, \ldots$ où

$$u_0 \Rightarrow^*_{\mathcal{R}} v_0 \models\!\!\Rightarrow_{PD(\mathcal{R})} u_1 \Rightarrow^*_{\mathcal{R}} v_1 \models\!\!\Rightarrow_{PD(\mathcal{R})} \Rightarrow^*_{\mathcal{R}} u_2 \ldots$$

à laquelle on peut lui associer une $\mathcal{R}$-séquence de réduction

$$u_0 \rightarrow^*_{\mathcal{R}} v_0 \models\!\!\Rightarrow_{\mathcal{R}} v'_0[u_1]_{p_0} \rightarrow^*_{\mathcal{R}} v'_0[v_1]_{p_0} \models\!\!\Rightarrow_{\mathcal{R}} v'_0[v'_1[u_2]_{p_1}]_{p_0} \rightarrow^*_{\mathcal{R}} ..$$

Corollaire : (Complétude) Si $\mathcal{R}$ termine, alors toute suite de dépendance de $\mathcal{R}$ est finie.

Correction de la méthode

Lemme : Soit $\mathcal{R}$ un système qui ne termine pas. Alors tout terme non fortement normalisable contient un sous-terme non fortement normalisable $f(\vec{u})$ où $f \in \mathcal{D}$ et $\vec{u}$ est un vecteur de termes fortement normalisables.

Lemme : Si toute suite de dépendance de $\mathcal{R}$ est finie et le vecteur de termes $\vec{u}$ est fortement normalisable, alors pour toute $f \in \mathcal{D}$, $f(\vec{u})$ est fortement normalisable.

Théorème : (Correction) Si toute suite de dépendance de $\mathcal{R}$ est finie, alors $\mathcal{R}$ termine.

Critère de terminaison par paires de dépendances

Théorème : Un système de réécriture $\mathcal{R}$ termine s'il existe un préordre $\succsim$ stable par substitutions et monotone t.q. sa partie strict $\succ$ soit stable par substitutions et bien fondée et t.q.

– $l \succsim r$ pour toute règle $l \to r \in \mathcal{R}$
– $s \succ t$ pour toute paire de dépendance $\langle s, t \rangle$

Optimisation de la méthode

Soit $\mathcal{D} \subseteq \Sigma$ l'ensemble de symboles définis d'un système $\mathcal{R}$.

L'ensemble de symboles marqués de $\mathcal{R}$ est $\check{\mathcal{D}} = \{\check{f} \mid f \in \mathcal{D}\}$.

On travaille maintenant avec les termes sur $\Sigma \cup \check{\mathcal{D}}$.

Une paire de dépendance marquée d'une règle $f(\vec{l}) \to r \in \mathcal{R}$ est une paire $\langle \check{f}(\vec{l}), \check{g}(\vec{s}) \rangle$, où $g(\vec{s})$ est sous-terme de r et $f \in \mathcal{D}$.

On remplace la notion de suite de dépendance par suite de dépendance marquée (utiliser paires de dépendance marquées à la place de paires de dépendance).

Lemme : Soit $\mathcal{R}$ un système de réécriture. Alors, toute suite de dépendance est finie ssi toute suite de dépendance marquées est finie.

Théorème : Un système de réécriture $\mathcal{R}$ termine s'il existe un préordre $\succsim$ stable par substitutions et monotone t.q. sa partie strict $\succ$ soit stable par substitutions et bien fondée et t.q.

- $l \succsim r$ pour toute règle $l \rightarrow r \in \mathcal{R}$
- $s \succ t$ pour toute paire de dépendance marquée $\langle s, t \rangle$

Terminaison par ordre produit

Le produit cartésien de n ensembles $\mathcal{A}_1 \ldots \mathcal{A}_n$ est l'ensemble de n-uplets $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n = \{(a_1, \ldots, a_n) \mid a_i \in \mathcal{A}_i\}$.

Si chaque $\mathcal{A}_i$ est muni d'une rélation de préordre $\gtrsim_i$, alors l'ordre produit est défini par

$(a_1, \ldots, a_n) \gtrsim_\times (b_1, \ldots, b_n)$ ssi $a_i \gtrsim_i b_i$ pour tout $i = 1 \ldots n$

Lemme : La rélation $\gtrsim_\times$ est bien fondée si toute relation $\gtrsim_i$ est bien fondée.

Ordre lexicographique sur le produit de 2 ensembles

Soit $>_{A_i}$ un ordre sur l'ensemble $\mathcal{A}_i$.

$$(x, y) >_{lex} (x', y') \text{ ssi } (x >_{A_1} x') \text{ ou } (x = x' \text{ et } y >_{A_2} y')$$

Exemple :

$$(4, "abc") >_{lex} (3, "abc") >_{lex} (2, "abcde") >_{lex} (2, "bcde") >_{lex} (2, "e") >_{lex} (1, "e") >_{lex} (0, \epsilon)$$

Ordre lexicographique sur le produit de n ensembles

Si chaque $>_{A_i}$ est un ordre strict sur l'ensemble $\mathcal{A}_i$, alors $>_{lex}$ est un ordre strict qui permet de comparer deux n-uplets de la manière suivante :

$$(x_1, \ldots, x_n) >_{lex} (x'_1, \ldots, x'_n) \text{ ssi } \quad \exists 1 \leq j \leq n$$
$$(x_j >_{A_j} x'_j \text{ and } \forall 1 \leq i < j \;\; x_i = x'_i)$$

Théorème : Tout ordre $>_{A_i}$ sur $\mathcal{A}_i$ est bien fondé ssi l'ordre lexicographique $>_{lex}$ sur $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n$ est bien fondé.

Ordre lexicographique (suite)

Avertissement : $>_{lex}$ n'est pas l'ordre du dictionaire ! !

Exemple :

$$
\begin{array}{lcl}
\text{Ackerman}(0,n) & = & n+1 \\
\text{Ackerman}(m+1,0) & = & \text{Ackerman}(m,1) \\
\text{Ackerman}(m+1,n+1) & = & \text{Ackerman}(m,\text{Ackerman}(m+1,n))
\end{array}
$$

Ordres multi-ensembles

Soit $\mathcal{A}$ un ensemble. Un multi-ensemble de base $\mathcal{A}$ est une fonction $\mathcal{M} : \mathcal{A} \rightarrow \mathbb{N}$.

Le multi-ensemble $\mathcal{M}$ est fini si $\mathcal{M}(x) > 0$ seulement pour un nombre fini d'éléments de $\mathcal{A}$.

Notation : $\{\!\{a, a, b\}\!\}$.

Soient $\mathcal{M}$ et $\mathcal{N}$ deux multi-ensembles. Le multi-ensemble union est définie par $\mathcal{M} \uplus \mathcal{N}(a) = \mathcal{M}(a) + \mathcal{N}(a)$.

Ordres multi-ensembles

Soit $\succ$ un ordre strict. La relation $\succ_{mul}$ associée est donnée par la fermeture transitive de la relation $\succ^1_{mul}$:

$\mathcal{M} \uplus \{\!\{x\}\!\} \succ^1_{mul} \mathcal{M} \uplus \{\!\{y_1, \ldots, y_n\}\!\}$, où $n \geq 0$ et $\forall i, x \succ y_i$.

Exemple : $\{\!\{5, 3, 1, 1\}\!\} \succ_{mul} \{\!\{4, 3, 3, 1\}\!\}$.

Exercice : Si $\succ$ est un ordre strict, alors $\succ_{mul}$ est un ordre strict.

Théorème : Soit $\succ$ un ordre strict sur $\mathcal{A}$, alors $\succ$ est bien fondé ssi $\succ_{mul}$ est bien fondé.

Les ordres de simplification

Un préordre de simplification sur $\mathcal{T}(\mathcal{X}, \Sigma)$ est un préordre $\succsim$ t.q.

1. Les symboles de Σ sont monotone par rapport à $\succsim$
2. $\succsim$ est stable par substitutions
3. $t \trianglerighteq u$ implique $t \succsim u$

Le plongement

La relation de plongement sur $\mathcal{T}(\mathcal{X}, \Sigma)$ est définie par $s \trianglerighteq_{emb} t$ ssi l'une de ces conditions est vérifiée

- $s = x = t$ pour $x \in \mathcal{X}$
- $s = f(s_1, \ldots, s_n)$ et $t = f(t_1, \ldots, t_n)$ et $\forall i \; s_i \trianglerighteq_{emb} t_i$
- $s = f(s_1, \ldots, s_n)$ et il existe j t.q. $s_j \trianglerighteq_{emb} t$

Remarque :

- Si $s \trianglerighteq t$, alors $s \trianglerighteq_{emb} t$.
- $\triangleright_{emb}$ est bien fondé.

Beaux préordres

Un préordre $\succsim$ sur un ensemble $\mathcal{A}$ est un beau préordre ssi pour toute suite infinie $s_1, s_2, s_3, \ldots$ de $\mathcal{A}$, il existe $i < j$ t.q. $s_i \precsim s_j$.

Un préordre $\succsim$ sur un ensemble *fini* $\mathcal{A}$ est toujours un beau préordre.

Lemmes pour le théorème de Kruskal

Lemme : $\gtrsim$ est un beau préordre sur $\mathcal{A}$ ssi pour toute suite infinie $s_1, s_2, s_3, \ldots$ de $\mathcal{A}$, il y a une infinité d'indices $i_1 < i_2 < i_3 < \ldots$ t.q. $s_{i_1} \lesssim s_{i_2} \lesssim s_{i_3} \lesssim \ldots$.

Lemme : Si chaque $\gtrsim_i$ est un beau préordre sur $\mathcal{A}_i$, alors l'ordre produit $\gtrsim_\times$ est un beau préordre sur $\mathcal{A}_1 \times \ldots \times \mathcal{A}_n$.

Théorème de Kruskal

Théorème : Soit Σ une signature finie et $\mathcal{X}$ un ensemble fini de variables. Alors $\trianglerighteq_{emb}$ est un beau préordre.

Lemme : Si $\succsim$ est un préordre de simplication sur $\mathcal{T}(\mathcal{X}, \Sigma)$, alors $s \trianglerighteq_{emb} t$ implique $s \succsim t$.

Terminaison par ordres de simplification

Lemme : Soit Σ une signature finie. Si $\succ$ est un ordre de simplication sur $\mathcal{T}(\mathcal{X}, \Sigma)$, alors il est un ordre de réduction (donc bien fondé).

La preuve utilise le théorème de Kruskal et le fait que $\trianglelefteq_{emb} \subseteq \precsim$ pour tout préordre de simplification.

Et la réciproque ?

Soit $\mathcal{R} = f(f(x)) \to\ f(g(f(x)))$.

Ce système termine (exercice), et donc $\to^+_{\mathcal{R}}$ est un ordre de réduction. Supposons que $\to^+_{\mathcal{R}}$ soit aussi un ordre de simplification. Alors $f(g(f(x))) \trianglerighteq_{emb} f(f(x))$ impliquerait $f(g(f(x))) \to^+ f(f(x)) \to^+ f(g(f(x)))$, ce qui contredit la terminaison.

Exemple : Les ordres récursifs sur les chemins

Soit $\gtrsim_\Sigma$ un préordre bien fondé sur Σ. On associe à chaque symbole $f \in \Sigma$ un statut dans l'ensemble $\{LEX, MUL\}$ t.q. si $f \sim g$, alors

- f et g ont le même statut,
- et si en plus leur statut est LEX, alors f et g ont la même arité.

L'ordre $\succ_{rpo}$

Soit $\succsim_\Sigma$ un préordre bien fondé sur une signature finie Σ. L'ordre récursifs sur les chemins est donné par $s \succ_{rpo} t$ ssi

1. [sous-terme] $s = f(s_1, \ldots, s_n)$ et $\exists i$ t.q. $s_i \succ_{rpo} t$ ou $s_i = t$ ou
2. [Deux symboles] $s = f(s_1, \ldots, s_n)$, $t = g(t_1, \ldots, t_m)$ et l'une des conditions suivantes est vérifiée
   (a) [précédence] $f \succ_\Sigma g$ et pour tout j, $s \succ_{rpo} t_j$
   (b) [multi-ensemble] $f \sim_\Sigma g$ ont un statut MUL et $\{\!\{s_1, \ldots, s_n\}\!\}(\succ_{rpo})_{mul}\{\!\{t_1, \ldots, t_m\}\!\}$.
   (c) [lexicographique] $f \sim_\Sigma g$ ont un statut LEX et $(s_1, \ldots, s_n)(\succ_{rpo})_{lex}(t_1, \ldots, t_m)$ et pour tout j, $s \succ_{rpo} t_j$

Est-il bien défini ?

Remarques

- Si tous les symboles ont statut LEX l'ordre s'appelle lpo.
- Si tous les symbols ont statut MUL l'ordre s'appelle mpo.
- Cette définition de rpo, ainsi que le théorème de Kruskal, peuvent être etendus à une signature Σ infinie munie d'un beau préordre. (ref. Simple Termination Revisited - A. Middeldorp et H. Zantema)

Propriétés de $\succ_{rpo}$

Théorème : La relation $\succ_{rpo}$ est bien fondée.

Propriétés de $\succ_{rpo}$ (suite)

Lemme : La relation $\succ_{rpo}$ est un ordre strict.

Lemme : La relation $\succ_{rpo}$ est un ordre de simplification.

Corollaire : La relation $\succ_{rpo}$ est un ordre de réduction (donc bien fondé).

Terminaison par ajournement

Soit $\mathcal{R}$ et $\mathcal{S}$ deux relations.

$\mathcal{R}$ peut être ajourné par rapport à $\mathcal{S}$ ssi pour tout s, t, u t.q. $s \longrightarrow_{\mathcal{R}} t \longrightarrow_{\mathcal{S}} u$ il existe v t.q. $s \longrightarrow^{+}_{\mathcal{S}} v \longrightarrow^{*}_{\mathcal{R}\cup\mathcal{S}} u$.

Théorème : Soient $\mathcal{R}$ et $\mathcal{S}$ deux relations bien fondées t.q. $\mathcal{R}$ peut être ajourné par rapport à $\mathcal{S}$. Alors la relation $\mathcal{R} \cup \mathcal{S}$ est aussi bien fondée.

Corollaire : Si $\mathcal{R}$ est bien fondé, alors $\mathcal{R} \cup \triangleright$ est bien fondé.

Terminaison par projection

Théorème : Pour $i = 1, 2$, soit $\mathcal{R}_i$ une relation sur O t.q.

1. $\mathcal{R}_2$ termine
2. il existe une relation $\mathcal{S}$ sur O' et une interprétation $\mathcal{T} : O \to O'$ t.q. :
   - $a \longrightarrow_{\mathcal{R}_1} b$ implique $\mathcal{T}(a) \longrightarrow^+_{\mathcal{S}} \mathcal{T}(b)$,
   - $a \longrightarrow_{\mathcal{R}_2} b$ implies $\mathcal{T}(a) \longrightarrow^*_{\mathcal{S}} \mathcal{T}(b)$.

Alors, si $\mathcal{S}$ termine, $(\mathcal{R}_1 \cup \mathcal{R}_2)$ termine aussi.