Les algèbres de termes

Les signatures et les termes finis

Une signature Σ est un ensemble non vide de symboles de fonction t.q. chaque $f \in \Sigma$ possède une arité n.

Soit $\mathcal{X}$ un ensemble de variables et Σ une signature. L'ensemble $\mathcal{T}(\mathcal{X}, \Sigma)$ de termes sur $\mathcal{X}$ et Σ est définie par :

- Toute variable $x \in \mathcal{X}$ est un terme dans $\mathcal{T}(\mathcal{X}, \Sigma)$
- Si f est d'arité n, et $t_1, \ldots, t_n$ sont dans $\mathcal{T}(\mathcal{X}, \Sigma)$, alors $f(t_1, \ldots, t_n)$ est un terme dans $\mathcal{T}(\mathcal{X}, \Sigma)$

On note $Var(t)$ l'ensemble de variables du terme t. Un terme t est clos si $Var(t) = \emptyset$. L'ensemble de termes clos est noté $\mathcal{T}(\emptyset, \Sigma)$ ou $\mathcal{T}(\Sigma)$.

Les suites d'entiers, les positions d'un terme

L'ensemble $\mathbb{N}^*$ de suites sur $\mathbb{N}$ est le plus petit ensemble t.q.

- $\Lambda \in \mathbb{N}^*$
- Si $i \in \mathbb{N}$ et $p \in \mathbb{N}^*$, alors $ip \in \mathbb{N}^*$

L'ensemble $Pos(t)$ de positions d'un terme t est un sous-ensemble de $\mathbb{N}^*$ défini par :

- $\Lambda \in Pos(t)$
- Si $t = f(t_1, \ldots, t_n)$ et $p \in Pos(t_i)$, alors $ip \in Pos(t)$ pour tout $1 \leq i \leq n$.

La relation $\leq_{pref}$ sur les suites d'entiers

L'opération de concatenation sur deux positions de $\mathbb{N}^*$ est définie par induction comme suit :

$$\begin{array}{rcl} \Lambda.q & = & q \\ (ip).q & = & i(p.q) \end{array}$$

La relation préfixe $\leq_{pref}$ sur $\mathbb{N}^* \times \mathbb{N}^*$ est définie par :
$p \leq_{pref} q$ ssi $\exists r \in \mathbb{N}^*$ t.q. $p.r = q$

Les positions p et q sont incompatibles ou parallèles, noté $p \bowtie q$, ssi $p \not\leq_{pref} q$ et $p \not\leq_{pref} q$.

Définition alternative de terme

Un terme t est une fonction partielle de $\mathbb{N}^*$ vers $\Sigma \cup \mathcal{X}$ t.q.

- $t(\Lambda)$ est défini
- Si $t(p)$ est défini, alors pour tout $q \leq_{pref} p$, $t(q)$ est aussi défini.
- Si $t(p) = x$, alors pour tout $p <_{pref} s$, $t(s)$ n'est pas défini.
- Si $t(p) = f$ et f est d'arité n, alors pour toute position $p.i$ t.q. $1 \leq i \leq n$, $t(p.i)$ est aussi défini.

Le domain d'une terme t, noté $Dom(t)$ est l'ensemble $\{p \in \mathbb{N}^* \mid t(p) \text{ est défini}\}$. Si $Dom(t)$ est fini, alors t est un terme fini (dit simplement terme). Si $Dom(t)$ est infini, alors t est un terme infini.

Les sous-termes d'un terme

Soit t un terme. L'ensemble $ST(t)$ de sous-termes de t est défini par :

- $ST(x) = \{x\}$.
- $ST(f(t_1, \ldots, t_n)) = \{f(t_1, \ldots, t_n)\} \cup \{v \mid v \in ST(t_i)\}$.

L'ensemble de sous-termes stricts d'un terme t est l'ensemble de sous-termes auquel on a enlevé t.

On écrit $t \trianglerighteq s$ (resp. $t \triangleright s$) si s est un sous-terme (resp. strict) de t.

Sous-terme à une position

Soit t un terme et $p \in Pos(t)$. Le sous-terme de t à la position p, noté $t|_p$, est défini par récurrence sur p par :

- $t|_\Lambda = t$.
- $f(t_1, \ldots, t_n)|_{iq} = t_i|q$.

Exercice : Montrer la propriété suivante : Si $p.q \in Pos(t)$, alors $t|_{p.q} = (t|_p)_q$

Remplacement

Le remplacement du sous-terme $t|_p$ par un terme v, noté $t[p \leftarrow v]$ ou $t[v]_p$, est défini comme suit :

- $t[v]_\Lambda = v$
- $f(t_1, \ldots, t_n)[v]_{ip} = f(t_1, \ldots, t_i[v]_p, \ldots, t_n)$

Exercice : Montrer les propriétés suivantes :

- Si $p \in Pos(s)$ et $q \in Pos(t)$, alors $(s[t]_p)|_{p.q} = t_q$ et $(s[t]_p)[r]_{p.q} = s[t[r]_q]_p$.
- Si $p.q \in Pos(s)$, alors $(s[t]_{p.q})|_p = (s|_p)[t]_q$ et $(s[t]_{p.q})[r]_p = s[r]_p$.
- Si $p, q \in Pos(s)$ et $p \bowtie q$, alors $(s[t]_p)|_q = s|_q$ et $(s[t]_p)[r]_q = (s[r]_q)[t]_p$.

Σ-algèbres

Une Σ-algèbre $\mathcal{A}$ est définie par :

– Un ensemble $\mathbf{A}$ non vide appelé domain de discours

– Pour chaque $f \in \Sigma$ d'arité n, une fonction $f^{\mathcal{A}} : \mathbf{A^n} \mapsto \mathbf{A}$, appelée interprétation de f.

Exemple : L'algèbre syntaxique $\mathcal{T}(\mathcal{X}, \Sigma)$: $\mathbf{A}$ est l'ensemble de termes sur $\mathcal{X}$ et Σ et $f^{\mathcal{A}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Exemple : L'algèbre syntaxique close $\mathcal{T}(\Sigma)$: $\mathbf{A}$ est l'ensemble de termes clos sur Σ et $f^{\mathcal{A}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Sous-algèbres

Une Σ-algèbre $\mathcal{A}_1$ est une sous-algèbre de la Σ-algèbre $\mathcal{A}_2$ ssi

- $\mathbf{A_1} \subseteq \mathbf{A_2}$
- pour tout $n \geq 0$, pour tout symbole $f \in \Sigma$ d'arité n et pour tout $a_1, \ldots, a_n \in \mathbf{A_1}$ on a $f^{\mathcal{A}_1}(a_1, \ldots, a_n) = f^{\mathcal{A}_2}(a_1, \ldots, a_n)$.

Congruences

Une relation R sur une Σ-algèbre $\mathcal{A}$. On dit que $f \in \Sigma$ est monotone par rapport à R ssi pour tout $i = 1 \ldots n$, $a_i \; R \; a_i'$ implique $f^{\mathcal{A}}(a_1, \ldots, a_i, \ldots, a_n) \; R \; f^{\mathcal{A}}(a_1, \ldots, a_i', \ldots, a_n)$.

Une congruence $\sim$ sur une Σ-algèbre est une relation d'équivalence (réflexive, symétrique, transitive), t.q. tout symbole $f \in \Sigma$ est monotone par rapport à $\sim$.

Notation : $S/_{\sim}$ est l'ensemble de classes d'équivalence d'une Σ-algèbre S modulo une congruence $\sim$ sur S.

Exercice : Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble $\mathcal{A}$ et soit a un élément quelconque de $\mathcal{A}$. Montrer que pour tout $x, y \in \mathcal{A}$ si $[x] \cap [y] \neq \emptyset$, alors $[x] = [y]$.

Exercice : Soit $\mathcal{T}$ la relation sur les entiers définie par $a\mathcal{T}b$ ssi 5 est un diviseur de $a - b$. Montrer que $\mathcal{T}$ est une relation d'équivalence, et qu'elle est une congruence par rapport aux deux fonctions suivantes :

$$i(a) = 7 \times a \qquad \text{et} \qquad p(a, b) = (2 \times a) + (3 \times b)$$

Exercice : Soit $\mathcal{S}$ une relation déquivalence quelconque sur les entiers naturels. Montrer que si $\mathcal{S}$ est une *congruence* par rapport à $+$, alors $\mathcal{S}$ est une *congruence* par rapport à $\times$.

L'algèbre quotient

Si $\sim$ est une congruence sur une Σ-algèbre $\mathcal{A}$, alors $\mathcal{A}^{\sim}$ est une Σ-algèbre, dite algèbre quotient sur $\mathcal{A}$ t.q.

- son domain est $\mathcal{A}/_{\sim}$
- pour chaque $f \in \Sigma$, $f^{\mathcal{A}^{\sim}}([a_1], \ldots, [a_n]) = [f^{\mathcal{A}}(a_1, \ldots, a_n)]$.

Homomorphismes, endomorphismes, isomorphismes

Soit $\mathcal{A}$ et $\mathcal{B}$ deux Σ-algèbres. Un homomorphisme (ou morphisme) est une fonction $\Phi : \mathcal{A} \to \mathcal{B}$ t.q. pour tout $n \geq 0$, pour tout symbole $f \in \Sigma$ d'arité n et pour tout $a_1, \ldots, a_n \in \mathbf{A}$ on a

$$\Phi(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\Phi(a_1), \ldots, \Phi(a_n))$$

Un endomorphisme sur une Σ-algèbre $\mathcal{A}$ est un morphisme de $\mathcal{A}$ sur elle même. Un isomorphisme est un morphisme bijectif (injectif et surjectif).

Exemple : $\Phi : \mathrm{Z} \rightarrow \{2.z \mid z \in \mathrm{Z}\}$ t.q. $\Phi(z) = z + z$.

Exercice : Soit Φ la fonction suivante :

$$\begin{array}{lcl} \Phi(a) & = & 2 \\ \Phi(f(t)) & = & \Phi(t) \\ \Phi(g(t)) & = & \Phi(t) + 1 \\ \Phi(h(s,t)) & = & \Phi(s) + \Phi(t) \end{array}$$

Définir une Σ-algèbre $\mathcal{B}$ t.q. Φ soit un homomorphisme entre l'algèbre syntaxique clos $\mathcal{T}(\{a, f, g, h\})$ et $\mathcal{B}$.

Algèbres initiale

Une Σ-algèbre $\mathcal{I}$ est initiale dans $\mathcal{K}$ ssi pour toute Σ-algèbre $\mathcal{A} \in \mathcal{K}$ il existe un unique morphisme $\Phi : \mathcal{I} \to \mathcal{A}$.

Assignations

Soit $\mathcal{A}$ une Σ-algèbre et soit $\mathcal{X}$ un ensemble de variables.

Une $\mathcal{A}$-assignation est une application $\sigma : \mathcal{X} \to \mathcal{A}$.

Théorème : Pour toute $\mathcal{A}$-assignation $\sigma : \mathcal{X} \to \mathcal{A}$, il existe un unique morphisme $\widehat{\sigma} : \mathcal{T}(\mathcal{X}, \Sigma) \to \mathcal{A}$, t.q.

$$\begin{array}{lcl} \widehat{\sigma}(x) & = & \sigma(x) \\ \widehat{\sigma}(f(t_1, \ldots, t_n)) & = & f^{\mathcal{A}}(\widehat{\sigma}(t_1), \ldots, \widehat{\sigma}(t_n)) \end{array}$$

Notation : On confond σ et $\widehat{\sigma}$

Substitutions

Une substitution est un endomorphisme de $\mathcal{T}(\mathcal{X}, \Sigma)$ en $\mathcal{T}(\mathcal{X}, \Sigma)$.

Une substitution close est un morphisme de $\mathcal{T}(\mathcal{X}, \Sigma)$ en $\mathcal{T}(\Sigma)$.

Le domaine d'une substitution θ est l'ensemble $Dom(\theta) = \{x \in \mathcal{X} \mid \theta(x) \neq x\}$.

Une substitution est fini si son domain est fini. Dans ce cas, on note $\theta = \{x_1/t_1, \ldots, x_n/t_n\}$ si $\theta(x_i) = t_i$ pour tout $1 \leq i \leq n$.

L'image d'une substitution est l'ensemble $Im(\theta) = \{\theta(x) \mid x \in Dom(\theta)\}$. On note $VarIm(\theta)$ l'ensemble $\bigcup_{x \in Dom(\theta)} Var(\theta(x))$.

Un renommage θ est une substitution bijective de $Dom(\theta)$ sur $VarIm(\theta)$.

Stabilité par substitution

Une relation R sur $\mathcal{T}(\mathcal{X}, \Sigma)$ est stable par substitution ssi $t \; R \; t'$ implique $\theta(t) \; R \; \theta(t')$ pour toute substitution θ.

Unification

Deux termes s et t sont unifiables ss'il existe une substitution t.q. $\theta(s) = \theta(t)$ (θ est donc un unificateur de s et t).

La composition de deux substitutions θ et τ est définie par $(\theta \circ \tau)(x) = \widehat{\theta}(\tau(x))$ pour toute variable $x \in \mathcal{X}$.

Soient θ et τ deux substitutions. θ est une instance de τ (ou τ est plus générale que θ) ss'il existe une substitution ρ t.q. pour toute variable $x \in \mathcal{X}$, $(\rho \circ \tau)(x) = \theta(x)$.

Soit $\mathcal{S}$ un ensemble de substitutions. Une substitution $\theta \in \mathcal{S}$ est principale ssi toute substitution $\tau \in \mathcal{S}$ est une instance de θ.

Unificateur principal

Théorème : Soit $\mathcal{E}$ l'ensemble (non vide) d'unificateurs de deux termes s et t. Alors il existe un unificateur $\theta \in \mathcal{E}$ appelé unificateur principal t.q. pour tout $\tau \in \mathcal{E}$, θ est plus général que τ. De plus, cet unificateur principal est unique à renommage près.

Exemple :

Une substitution θ est idempotente ssi $\theta \circ \theta = \theta$.

Théorème : Si s et t sont unifiables, alors il existe un unificateur principal de s et t qui est idempotent.

Mais comment construire cette unificateur ?

Vers un algorithme d'unification

- La construction d'un système d'équations à partir d'un problème d'unification
- Les règles pour transformer le système d'équations
- L'algorithme d'unification
- L'interprétation du résultat de l'algorithme

Les systèmes d'équations

Définition : Une équation est une paire de termes de la forme $s \doteq t$. On dit qu'elle est unifiable ssi les termes s et t le sont.

Définition : Un système/problème d'équations E est un ensemble d'équations. On dit qu'il est unifiable ssi il existe une substitution qui est unificateur de toutes les équations de E. Cette substitution est appelée solution de E.

On s'intéresse aux systèmes d'équations finis qu'on notera $\{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}$.

Les formes résolues

Définition : Un système d'équations E est en forme résolue ssi il est de la forme $\{\alpha_1 \doteq t_1, \ldots, \alpha_n \doteq t_n\}$, où

- toutes les variables α_i sont distinctes ($i \neq j$ implique $\alpha_i \neq \alpha_j$)
- aucune α_i n'apparaît dans un t_j ($\forall i, \alpha_i \notin \bigcup_{1 \leq j \leq n} Var(t_j)$)

Notation : Si E est un système en forme résolue $\{\alpha_1 \doteq t_1, \ldots, \alpha_n \doteq t_n\}$ on note $\vec{E}$ la substitution $\{\alpha_1/t_1, \ldots, \alpha_n/t_n\}$.

Les règles de transformation

$$\frac{E \cup \{s \doteq s\}}{E} \quad \text{(effacer)} \qquad \frac{E \cup \{t \doteq \alpha\} \quad t \notin \mathcal{X}}{E \cup \{\alpha \doteq t\}} \quad \text{(orienter)}$$

$$\frac{E \cup \{f(s_1, \ldots, s_n) \doteq f(t_1, \ldots, t_n)\}}{E \cup \{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}} \quad \text{(décomposer)}$$

$$\frac{E \cup \{\alpha \doteq s\} \quad \alpha \in Var(E) \quad \alpha \notin Var(s)}{E\{\alpha/s\} \cup \{\alpha \doteq s\}} \quad \text{(remplacer)}$$

L'algorithme d'unification d'un système E

1. On démarre avec un système d'équations E
2. On applique les règles de transformation tant qu'on peut, on obtient un nouveau système P
3. Si le système P est en forme résolue
   - alors renvoyer $\vec{P}$
   - sinon échec

Vers la correction et la complétude de l'algorithme

Lemme :

1. L'algorithme termine.
2. Si σ est un unificateur d'une forme résolue P, alors $\sigma = \sigma\vec{P}$.
3. Si une règle transforme un problème P dans un problème S, alors les solutions de P et S sont les mêmes.

Correction et complétude de l'algorithme

Théorème : (Correction) Si l'algorithme trouve une substitution $\vec{S}$ pour le problème P, alors P est unifiable et $\vec{S}$ est un unificateur principal de P.

Autrement dit,

Si P n'est pas unifiable, l'algorithme échoue.

Théorème : (Complétude) Si le système P est unifiable, alors l'algorithme calcule l'unificateur principal de P.

Autrement dit,

Si l'algorithme échoue, alors le système P n'est pas unifiable.