Les Σ-algèbres et les algèbres de termes

Les signatures et les termes finis

Définition :[Signature] Une signature est constituée de deux ensembles:

- un ensemble fini $S = \{s_1, \ldots, s_k\}$ de symboles de *sortes*
- un ensemble non vide de symboles de fonction t.q. chaque $f \in \Sigma$ possède une arité $s_1 * \ldots * s_n, s$.

Définition :[Σ-algèbre] Etant donnée une signature Σ, une Σ-algèbre A est donnée par

- un ensemble A_{s_i} pour toute sorte s_i de Σ (cet ensemble est appelé le “support” de s_i)
- pour chaque symbole de fonction $f \in \Sigma$ d'arité $s_1 * \ldots * s_n, s$, une fonction $f^A : A_{s_1} \times \ldots \times A_{s_n} \to A_s$, appelée interprétation de f.

Exemple : a faire…

Définition :[Les termes sur une signature Σ] Soit Σ une signature, et $\mathcal{X}$ une famille d'ensembles $\mathcal{X}_s$ de variables pour chaque sorte s de Σ. L'ensemble $\mathcal{T}_\Sigma(\mathcal{X})$ de termes sur $\mathcal{X}$ et Σ est défini par :

- Toute variable $x \in \mathcal{X}_s$ est un terme de sorte s dans $\mathcal{T}_\Sigma(\mathcal{X})$
- Si f est d'arité $s_1 * \ldots * s_n, s$, et $t_1, \ldots, t_n$ sont dans $\mathcal{T}_\Sigma(\mathcal{X})$ de sorte s_1, … s_n respectivement, alors $f(t_1, \ldots, t_n)$ est un terme de sorte s dans $\mathcal{T}_\Sigma(\mathcal{X})$

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 $\mathcal{T}_\Sigma(\emptyset)$ ou $\mathcal{T}(\Sigma)$.

Exercice : Vérifiez que:

- Les termes sur la signature Σ et variables $\mathcal{X}$, $\mathcal{T}_\Sigma(\mathcal{X})$, forment bien une Σ-algèbre (A_{s_i} est l'ensemble de termes de sorte s_i, et $f^{\mathcal{A}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$). Cette algèbre est aussi dite algèbre syntaxique.

- Les termes clos $\mathcal{T}(\Sigma)$ forment bien une Σ-algèbre: (A_{s_i} est l'ensemble de termes clos de sorte s_i $f^{\mathcal{A}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$). Cette algèbre est aussi dite algèbre syntaxique close.

Dans la suite, par simplicité, on travaillera souvent sur des algèbres mono-sortées (i.e. ayant une seule sorte, que l'on peut alors ne pas indiquer explicitement).

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.

- $\epsilon \in \mathbb{N}^*$
- 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 :

- $\epsilon \in Pos(t)$
- 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 :

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

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 $p \not\leq_{pref} q$.

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 :

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

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

- $t[v]_\epsilon = v$
- $f(t_1, \ldots, t_n)[v]_{i.p} = f(t_1, \ldots, t_i[v]_p, \ldots, t_n)$

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

Soit R une relation 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.

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).

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 $\widehat{\sigma} : \mathcal{T}_{\Sigma}(\mathcal{X}) \to \mathcal{A}$, 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 $\mathcal{T}_\Sigma(\mathcal{X})$ en $\mathcal{T}_\Sigma(\mathcal{X})$.

Une substitution close est un morphisme de $\mathcal{T}_\Sigma(\mathcal{X})$ 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 finie 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 $VarIm(\theta)$ est l'ensemble $\bigcup_{x \in Dom(\theta)} Var(\theta(x))$.

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

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.

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.

La logique équationnelle

Équations : syntax et sémantique

Une Σ-équation est une paire de termes noté $s \doteq t$.

Une Σ-algèbre $\mathcal{A}$ est un modèle d'une Σ-équation $s \doteq t$, noté $\mathcal{A} \models s \doteq t$, ssi pour toute $\mathcal{A}$-assignation σ on a $\widehat{\sigma}(s) = \widehat{\sigma}(t)$.

On dit aussi que $s \doteq t$ est valide pour $\mathcal{A}$.

Une Σ-algèbre $\mathcal{A}$ est un modèle d'un ensemble de Σ-équations $\mathcal{E}$, noté $\mathcal{A} \models \mathcal{E}$, ssi $\mathcal{A}$ est un modèle de toute équation de $\mathcal{E}$.

On dit aussi que $\mathcal{E}$ est valide pour $\mathcal{A}$.

Consequénce sémantique

Soit $\mathcal{E}$ un ensemble de Σ-équations et $s \doteq t$ une Σ-équation quelconque.

L'équation $s \doteq t$ est une consequénce logique de l'ensemble $\mathcal{E}$, noté $\mathcal{E} \models s \doteq t$, ssi tout modèle de $\mathcal{E}$ est aussi un modèle de $s \doteq t$.

La théorie équationnelle engendrée par $\mathcal{E}$ est l'ensemble $\doteq_{\mathcal{E}} = \{(s,t) \in \mathcal{T}_\Sigma(\mathcal{X}) \times \mathcal{T}_\Sigma(\mathcal{X}) \mid \mathcal{E} \models s \doteq t\}$.

Exercice : Montrer que la relation $\doteq_{\mathcal{E}}$ est une congruence sur $\mathcal{T}_\Sigma(\mathcal{X})$.

Règles syntaxiques pour le raisonnement équationnel

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \text{ (axiome)} \qquad \frac{}{s \doteq s} \text{ (réflexivité)}$$

$$\frac{s \doteq t}{t \doteq s} \text{ (symétrie)} \qquad \frac{s \doteq t \quad t \doteq u}{s \doteq u} \text{ (transitivité)}$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \text{ (substitution)} \qquad \frac{s \doteq t}{u[s]_p \doteq u[t]_p} \text{ (contexte)}$$

Dérivation

Une dérivation de l'équation $s \doteq t$ à partir d'un ensemble $\mathcal{E}$ est un arbre d'équations t.q.

- La racine est $s \doteq t$

- Si E est une feuille, alors $E \in \mathcal{E}$ ou E est une équation $s \doteq s$.
- Si $E_1, \ldots, E_n$ sont les fils de E, alors E est obtenue à partir de $E_1, \ldots, E_n$ par une règle syntaxique.

L'équation $s \doteq t$ est dérivée à partir de $\mathcal{E}$, noté $\mathcal{E} \vdash s \doteq t$, ssi il existe une dérivation de $s \doteq t$ à partir de $\mathcal{E}$.

La relation $\leftrightarrow^*_{\mathcal{E}}$

$$\frac{s \doteq t \in \mathcal{E}}{\sigma(s) \rightarrow_{\mathcal{E}} \sigma(t)} \ (\forall \sigma) \qquad\qquad \frac{s \rightarrow_{\mathcal{E}} t}{u[s]_p \rightarrow_{\mathcal{E}} u[t]_p} \ (\forall u \forall p)$$

$\leftrightarrow_{\mathcal{E}}$ est la fermeture symétrique de $\rightarrow_{\mathcal{E}}$
$\leftrightarrow^*_{\mathcal{E}}$ est la fermeture réflexive, symétrique et transitive de $\rightarrow_{\mathcal{E}}$

À propos de $\leftrightarrow^*_{\mathcal{E}}$

Exercice : Montrer que $\leftrightarrow^*_{\mathcal{E}}$ est une congruence sur $\mathcal{T}_\Sigma(\mathcal{X})$.

Exercice : Montrer que $\mathcal{E} \vdash s \doteq t$ ssi $s \leftrightarrow^*_{\mathcal{E}} t$.

Lemme de substitution (i)

Soit $\mathcal{A}$ une Σ-algèbre, σ une $\mathcal{A}$-assignation et θ une substitution. Alors pour tout terme $t \in \mathcal{T}_\Sigma(\mathcal{X})$ on a

$$\sigma(\theta(t)) = \sigma'(t)$$

où $\sigma'(x) = \sigma(\theta(x))$ pour toute variable $x \in \mathcal{X}$.

Lemme de substitution (ii)

Considérons la Σ-algèbre $\mathcal{T}_\Sigma(\mathcal{X})^{\leftrightarrow^*_{\mathcal{E}}}$.

Soit σ une $\mathcal{T}_\Sigma(\mathcal{X})^{\leftrightarrow^*_{\mathcal{E}}}$-assignation et θ une substitution t.q $\sigma(x) = [\theta(x)]$ pour toute variable $x \in \mathcal{X}$. Alors pour tout terme $t \in \mathcal{T}_\Sigma(\mathcal{X})$ on a

$$\sigma(t) = [\theta(t)]$$

Le modèle $\mathcal{T}_\Sigma(\mathcal{X})^{\leftrightarrow^*_{\mathcal{E}}}$

Exercice : L'algèbre $\mathcal{T}_\Sigma(\mathcal{X})^{\leftrightarrow^*_{\mathcal{E}}}$ est un modèle de $\mathcal{E}$.

Théorème d'adéquation (Birkhoff 1933)

(Correction) Si $\mathcal{E} \vdash s \doteq t$, alors $\mathcal{E} \models s \doteq t$.

(Complétude) Si $\mathcal{E} \models s \doteq t$, alors $\mathcal{E} \vdash s \doteq t$.

Ce premier théorème de Birkhoff nous dit que la derivabilité syntaxique et la conséquence sémantique coincident, dans la logique équationnelle.

Un deuxième théorème de Birkhoff nous donne les propriétés intrinseques de la classe de Σ-algèbres qui sont les modèles d'une théorie équationnelle donnée.

Définition :[Produit direct de Σ-algèbres] Soit $A_1, \ldots, A_k$ une famille finie de Σ-algèbres. Le produit direct P de $A_1, \ldots, A_k$ est la Σ-algèbre définie comme suit:

- $P_{s_i} = A_{1s_i} \times \ldots \times A_{ks_i}$
- pour f de signature $s_1 * \ldots * s_n, s$ on définit f^P comme

$$f^P(< a_1^1, \ldots, a_k^1 >, \ldots, < a_1^n, \ldots, a_k^n >) = \\ < f^{A_1}(a_1^1, \ldots, a_1^n), \ldots, f^{A_k}(a_k^1, \ldots, a_k^n) >$$

Exercice : Vérifier que le produit direct de k Σ-algèbres est bien une Σ-algèbre.

Définition :[Variété] Une classe $\mathcal{K}$ de Σ-algèbres est une variété si ell'est *close* par les opérations suivantes:

sousalgèbre (i.e., si $A \in \mathcal{K}$, et B est une sousalgèbre de A, alors $B \in \mathcal{K}$)

image homomorphe (i.e., si $A \in \mathcal{K}$, B une Σ-algèbre, et $B = \Phi(A)$ pour un homomorphisme Φ, alors $B \in \mathcal{K}$))

produit direct (i.e., si $A_1, \ldots, A_k \in \mathcal{K}$ est P est le produit direct de $A_1, \ldots, A_k$, alors $P \in \mathcal{K}$

Définition :[Classe des modèles] On note $\mathcal{M}od(\mathcal{E})$ la classe des Σ-algèbres qui satisfont les équations $\mathcal{E}$ (les modèles de $\mathcal{E}$).

Théorème :[Birkhoff, 1935] Une classe $\mathcal{K}$ de Σ-algèbres est $\mathcal{M}od(E)$ pour un quelque ensemble d'équations $\mathcal{E}$) ssi ell'est une variété.

L'application la plus intéressante du théorème de Birkhoff est la preuve que certaines opérations ne sont pas axiomatisables par le biais d'une théorie équationnelle.

Exercice : Vérifié que la conditionnelle stricte définie par les équations conditionnelles suivantes n'est pas axiomatisable par une théorie équationnelle.

$$\begin{array}{lcll} ITE(b, e1, e2) & = & \perp & \text{si } b = \perp \text{ ou } e1 = \perp \text{ ou } e2 = \perp \\ ITE(true, e1, e2) & = & e1 & \\ ITE(false, e1, e2) & = & e2 & \end{array}$$